TRƯỜNG ĐẠI HỌC BÁCH KHOA

ĐẠI HỌC QUỐC GIA TPHCM

----------❀❀❀----------

BÁO CÁO BÀI TẬP LỚN

THIẾT KẾ HỆ THỐNG NHÚNG

Chủ đề: IOT Smart Doorlock with RFID and OTP using ESP32

Giảng viên: Bùi Quốc Bảo

Nhóm 3

Thành viên	*MSSV*
Trần Quốc Nam	*2212161*
Đặng Quốc Khánh	*2211503*

Năm học: 2025 - 2026

MỤC LỤC

CHƯƠNG 1: TỔNG QUAN

1.1. Vấn đề (Problem)

Các loại khóa cơ truyền thống bộc lộ nhiều hạn chế về an ninh (dễ bị cắt phá, sao chép chìa) và bất tiện khi sử dụng (quên chìa, mất chìa). Việc quản lý ra vào tại các khu vực cần bảo mật hoặc nhà trọ, văn phòng gặp nhiều khó khăn.

1.2. Ý nghĩa (Significance)

Đồ án thiết kế hệ thống khóa cửa điện tử sử dụng công nghệ thẻ từ RFID và mật khẩu số giúp nâng cao tính bảo mật, loại bỏ sự phụ thuộc vào chìa khóa cơ, đồng thời tạo tiền đề cho việc tích hợp quản lý từ xa qua Internet (IoT).

1.3. Ứng dụng (Application)

Mặc dù đây là một mô hình đồ án môn học, nhưng hệ thống khóa cửa thông minh (Smart Door Lock) được thiết kế với độ hoàn thiện cao, có tính ứng dụng thực tiễn rộng rãi trong đời sống và công nghiệp:

- Hệ thống an ninh nhà ở (Smart Home): Thay thế ổ khóa cơ truyền thống tại các căn hộ chung cư, nhà phố thông minh, giúp gia chủ không cần mang theo chùm chìa khóa cồng kềnh.
- Kiểm soát ra vào văn phòng (Access Control): Ứng dụng tại các công ty, phòng họp hoặc khu vực hạn chế (như phòng Server, kho tài liệu) để chỉ cho phép nhân viên có thẻ từ hoặc mật khẩu được cấp quyền mới được phép ra vào.
- Quản lý khu nhà trọ, khách sạn (Hospitality): Giúp chủ nhà trọ quản lý người thuê dễ dàng. Khi khách trả phòng, chỉ cần xóa mã thẻ/mật khẩu trên hệ thống mà không cần tốn chi phí thay toàn bộ ổ khóa như khóa cơ.
- Tủ đồ cá nhân (Smart Locker): Ứng dụng cho hệ thống tủ gửi đồ tại siêu thị, phòng Gym, hồ bơi, tăng tính an toàn và tiện lợi cho khách hàng.

- Giáo dục và Nghiên cứu: Sản phẩm là mô hình trực quan để sinh viên nghiên cứu về lập trình hệ thống nhúng, các chuẩn giao tiếp (SPI, I2C, GPIO) và kỹ thuật điều khiển thiết bị ngoại vi trên nền tảng ESP32.

1.4. Mục tiêu (Objective)

Xây dựng hoàn thiện hệ thống khóa cửa thông minh với các chức năng:

- Mở khóa bằng thẻ từ RFID.
- Mở khóa bằng mật khẩu (Keypad).
- Hiển thị trạng thái trên màn hình LCD.
- Hệ thống hoạt động ổn định với nguồn 12V, điều khiển chốt cửa điện từ (Solenoid Lock).

CHƯƠNG 2: TỔNG QUAN HỆ THỐNG

2.1. Requirements

2.1.1. Functional Requirement

ID	Requirement Description
FR1	**Mở khóa bằng RFID**
FR2	**Mở khóa bằng OTP (One-Time Password)**
FR3	**Mở khóa bằng PIN**
FR4	**Quản lý mở khóa**

FR1 – Hệ thống cho phép người dùng mở khóa bằng thẻ RFID

- FR1.1. Hệ thống phải cho phép mở khóa bằng thẻ RFID hợp lệ.
- FR1.2. Hệ thống phải lưu trữ và quản lý danh sách thẻ RFID được phép sử dụng.
- FR1.3. Khi quét thẻ không hợp lệ, hệ thống phải từ chối và hiển thị cảnh báo.

FR2 – Hệ thống cho phép người dùng mở khóa bằng OTP (One-Time Password)

- FR2.1. Hệ thống phải sinh OTP ngẫu nhiên và có thời hạn sử dụng (< 60 giây).
- FR2.2. OTP phải được gửi đến người dùng qua ứng dụng di động/Telegram/email tùy cấu hình.
- FR2.3. Hệ thống chỉ mở khóa khi OTP nhập vào khớp và còn hiệu lực.

FR3 – Hệ thống cho phép người dùng mở khóa bằng PIN

- FR3.1. Hệ thống phải cho phép người dùng nhập PIN cố định để mở khóa.
- FR3.2. Người dùng có thể thay đổi PIN thông qua giao diện quản lý.
- FR3.3. Khi nhập sai PIN nhiều lần liên tiếp, hệ thống phải khóa tạm thời và cảnh báo.

FR4 – Quản lý mở khóa

- FR4.1. Hệ thống phải điều khiển khóa điện tử (servo/relay) để mở hoặc đóng.
- FR4.2. Hệ thống phải ghi lại log sự kiện.
- FR4.3. Hệ thống phải cho phép reset và cập nhật firmware qua OTA (Over-The-Air).

2.1.2. Non-Functional Requirements

ID	Requirement Description
NFR1	Thời gian phản hồi khi quét RFID, nhập OTP hoặc PIN không vượt quá 2 giây.
NFR2	Hệ thống phải hoạt động liên tục 24/7 với tỉ lệ lỗi < 1%.
NFR3	Dữ liệu OTP/PIN phải được mã hóa khi truyền, và giao tiếp phải sử dụng HTTPS/TLS.
NFR4	Hệ thống phải tiêu thụ điện năng thấp, có thể dùng pin/UPS trong trường hợp mất điện.
NFR5	Hệ thống phải dễ mở rộng để tích hợp thêm cảm biến (camera, vân tay, cảm biến cửa…).

NFR1 – Thời gian phản hồi

- NRF1.1: RFID/OTP/PIN phải được xử lý trong ≤ 2 giây.
- NRF1.2: Nếu vượt ngưỡng thì hệ thống phải ghi log sự kiện lỗi.

NFR2 – Độ tin cậy hệ thống

- NFR2.1: Hệ thống phải hoạt động liên tục 24/7 với uptime ≥ 99%.
- NFR2.2: Có cơ chế tự khởi động lại khi treo.
- NFR2.3: Khi mất mạng, RFID/PIN vẫn hoạt động offline.
- NFR2.4: Tuổi thọ phần cứng tối thiểu 2 năm.

NFR3 – Bảo mật dữ liệu

- NFR3.1: OTP/PIN phải được mã hóa (AES-128 trở lên).
- NFR3.2: Giao tiếp sử dụng HTTPS/TLS.
- NFR3.3: Không được lưu OTP dưới dạng plaintext.

NFR4 – Tiêu thụ năng lượng

- NFR4.1: Có pin/UPS dự phòng ≥ 4 giờ trong trường hợp mất điện.
- NFR4.2: Cảnh báo pin yếu hiển thị trên App.

NFR5 – Khả năng mở rộng

- NFR5.1: Hỗ trợ tích hợp thêm cảm biến (camera, vân tay, cảm biến cửa).
- NFR5.2: Cho phép giao tiếp mở rộng qua UART/I2C/SPI.
- NFR5.3: Có thể quản lý cảm biến bổ sung qua App/Web.

2.1. Use Case Modelling

Hệ thống được thiết kế với 3 kịch bản sử dụng chính: Mở khóa bằng mật khẩu, Mở khóa bằng thẻ từ và Xử lý khi nhập sai (Báo động).

- UC – 01: Mở khóa bằng Mật khẩu (Password Unlock)

- Mô tả: Người dùng nhập mật khẩu đã cài đặt trước thông qua bàn phím (Keypad) để mở khóa cửa.
- Các bước thực hiện:

  - Hệ thống ở trạng thái chờ, LCD hiển thị thông báo "Moi nhap mat khau".
  - Người dùng nhập các ký tự số trên Keypad 4x4.
  - LCD hiển thị ký tự * thay cho số thực để bảo mật.
  - Người dùng nhấn phím # để xác nhận.
  - Hệ thống kiểm tra mật khẩu. Nếu đúng:
  - Buzzer kêu 1 tiếng "bíp" ngắn.
  - Relay đóng mạch, Solenoid rút chốt mở cửa.
  - LCD hiển thị "Welcome Home".
  - Sau 5 giây, Solenoid tự động bung chốt để khóa lại.
- Yêu cầu: Hệ thống đã được cấp nguồn và mật khẩu đã được lưu trong bộ nhớ.

- UC – 02: Mở khóa bằng Thẻ RFID (RFID Unlock)

- Mô tả: Người dùng sử dụng thẻ từ hoặc móc khóa RFID đã đăng ký để chạm vào đầu đọc mở cửa nhanh chóng.
- Các bước thực hiện:
  - Hệ thống ở trạng thái chờ, module RFID liên tục phát sóng dò tìm thẻ.
  - Người dùng đưa thẻ vào phạm vi quét (2-5cm).
  - Đầu đọc RC522 đọc mã UID của thẻ và gửi về ESP32.
  - Hệ thống so sánh UID với danh sách hợp lệ. Nếu khớp:
  - Buzzer kêu 1 tiếng "bíp".
  - Relay kích hoạt Solenoid mở cửa.
  - LCD hiển thị "Card Accepted".
  - Cửa tự động khóa lại sau 5 giây.
- Yêu cầu: Thẻ RFID phải là thẻ hoạt động ở tần số 13.56MHz và đã được nạp UID vào Code.

- UC – 03: Xử lý truy cập trái phép (Access Denied)

- Mô tả: Hệ thống phản hồi khi người dùng nhập sai mật khẩu hoặc sử dụng thẻ từ không hợp lệ.
- Các bước thực hiện:
  - Người dùng nhập sai mật khẩu và nhấn #, hoặc quẹt thẻ chưa đăng ký.
  - Hệ thống kiểm tra thấy dữ liệu không trùng khớp.
  - Buzzer phát ra âm thanh cảnh báo (3 tiếng "bíp" dài hoặc kêu liên tục 1s).
  - LCD hiển thị thông báo lỗi "Wrong Password" hoặc "Invalid Card".
  - Relay không hoạt động, cửa vẫn ở trạng thái khóa.
  - Hệ thống quay lại trạng thái chờ sau 2 giây.
- Yêu cầu: Hệ thống hoạt động bình thường.

2.2. System Architecture

Kiến trúc hệ thống bao gồm các khối chính là Khối nguồn, Khối hiển thị, Khối vi điều khiển, Khối di chuyển, Khối cảm biến và Khối nạp code. Trong đó:

- Khối nguồn: Nguồn 12V, mạch ổn áp tạo nguồn 5V và mạch ổn áp tạo nguồn 3.3V.

- Khối hiển thị: Hiển thị thông qua LCD và thông báo bằng led và buzzer.

- Khối vi điều khiển: Thực hiện điều khiển các khối còn lại.

- Khối chấp hành : Nhận tín hiệu kích từ vi điều khiển để cấp nguồn cho khóa.

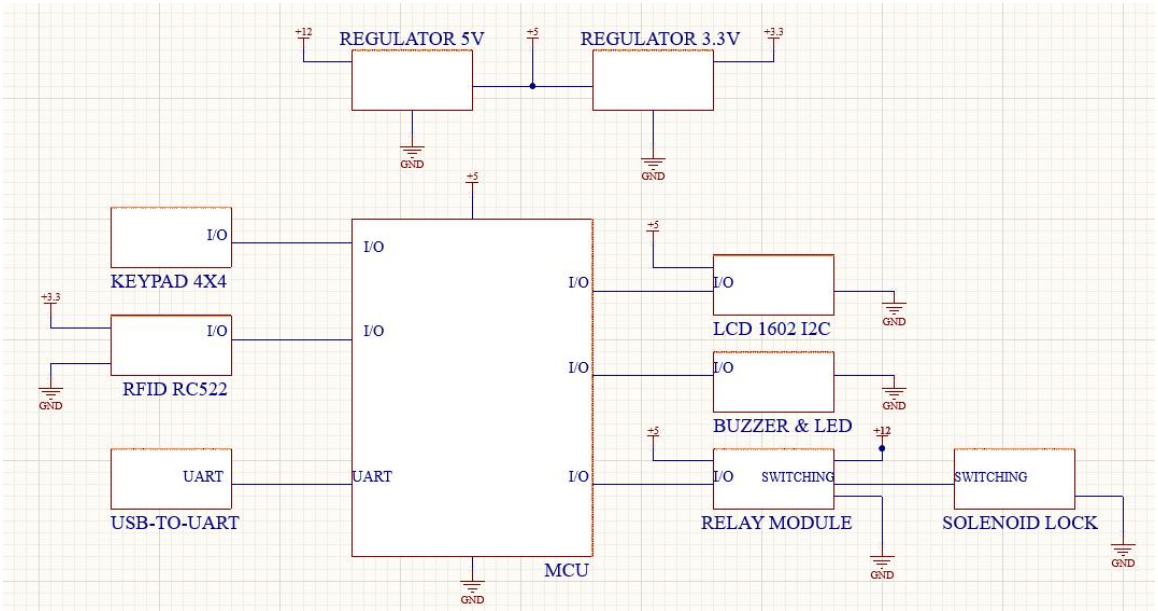
- Khối nhập liệu: Dùng để nhập dữ liệu vào.

- Khối nạp code: Dùng để nạp code vào khối vi điều khiển.

Hình 1: Sơ đồ kiến trúc

2.3. Block diagram

Block diagram thể hiện cách thức giao tiếp cũng như các khối nào nào là module input, các khối nào là module output.



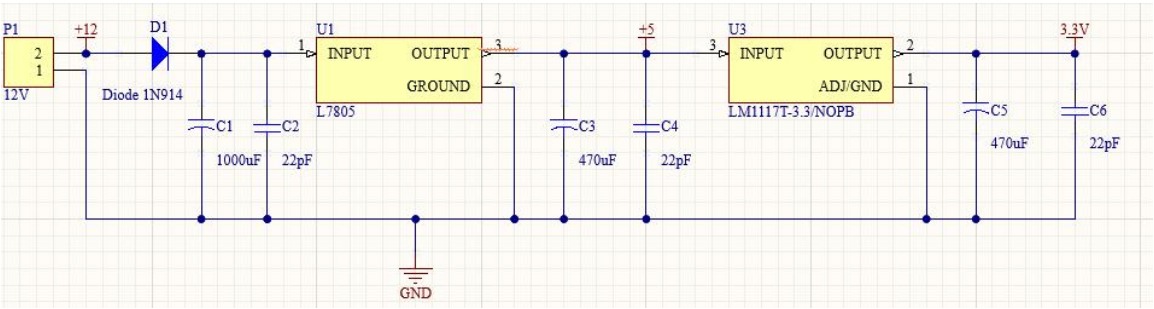
Hình 2: Sơ đồ khối

CHƯƠNG 3 THIẾT KẾ PHẦN CỨNG

3.1. Khối nguồn

Hệ thống sử dụng mô hình hạ áp tầng (Cascade) để đảm bảo ổn định nhiệt và hiệu suất.

- Đầu vào: 12V DC (cần thiết để Solenoid hoạt động mạnh).
- Tầng 1 (12V -> 5V): Sử dụng IC L7805 để cấp nguồn cho Relay, LCD, Buzzer. Có Diode bảo vệ chống ngược cực và tụ lọc nhiễu.
- Tầng 2 (5V -> 3.3V): Sử dụng IC AMS1117-3.3 để cấp nguồn cho ESP32 và module RFID (vì ESP32 và RFID hoạt động ở 3.3V, nếu cấp 5V sẽ cháy).

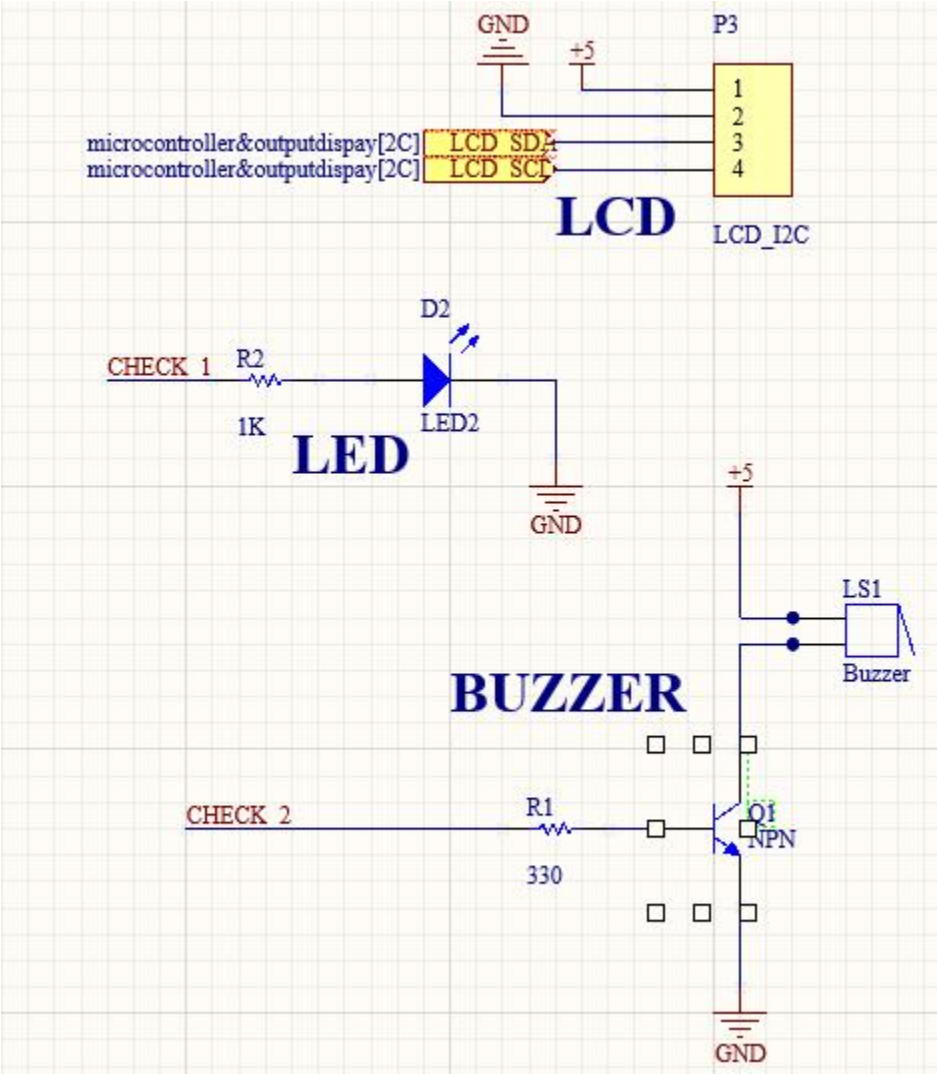


Hình 3: Khối nguồn

3.2. Khối hiển thị

- LCD 1602: Sử dụng giao tiếp I2C (chân SDA, SCL) giúp tiết kiệm chân GPIO của vi điều khiển.
- Buzzer: Sử dụng Transistor NPN (C1815/2N2222) để khuếch đại dòng điện từ chân GPIO, đảm bảo còi kêu to và bảo vệ vi điều khiển.
- Led: Sử dụng LED đơn (màu Xanh) kết nối nối tiếp với điện trở hạn dòng vào chân GPIO. Cung cấp phản hồi thị giác tức thời cho người dùng (Sáng

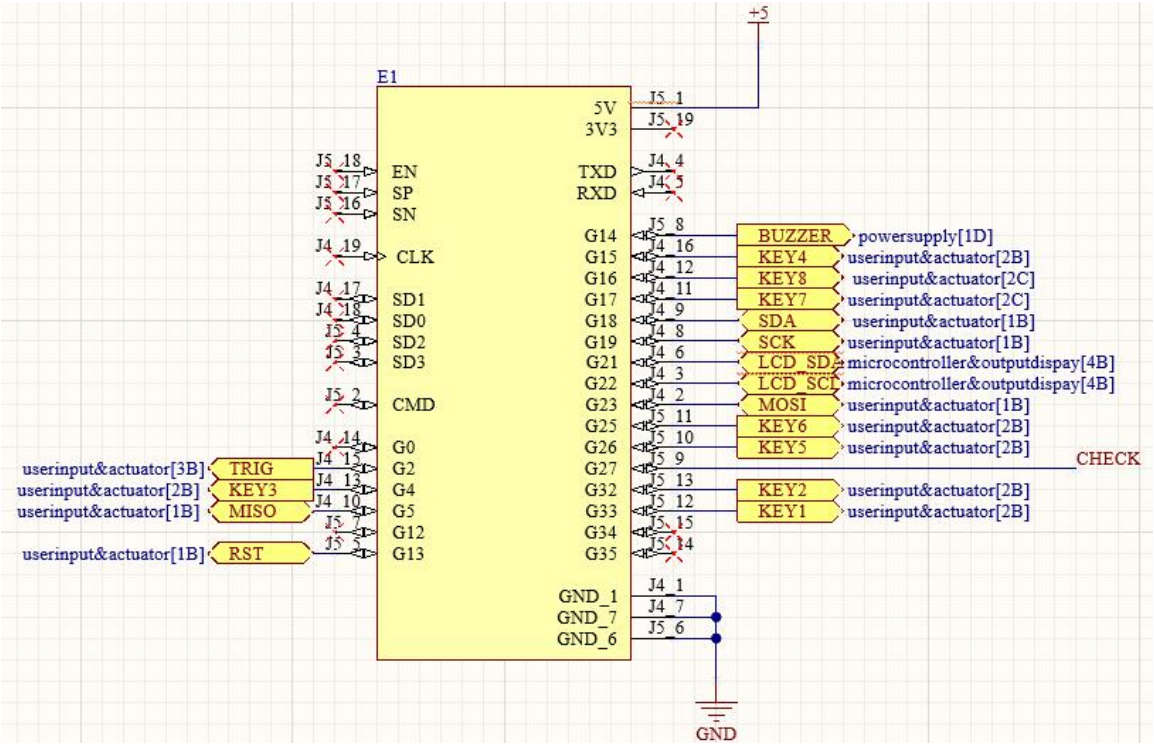
khi mở khóa thành công, tắt hoặc nhấp nháy khi khóa/báo lỗi) hỗ trợ cho màn hình LCD và còi Buzzer.



Hình 4: Khối hiển thị

3.3. Khối vi điều khiển

MCU: NodeMCU ESP32 được lựa chọn nhờ tốc độ xử lý cao (Dual-core 240MHz), bộ nhớ lớn và tích hợp sẵn Wi-Fi/Bluetooth cho các tính năng IoT mở rộng.

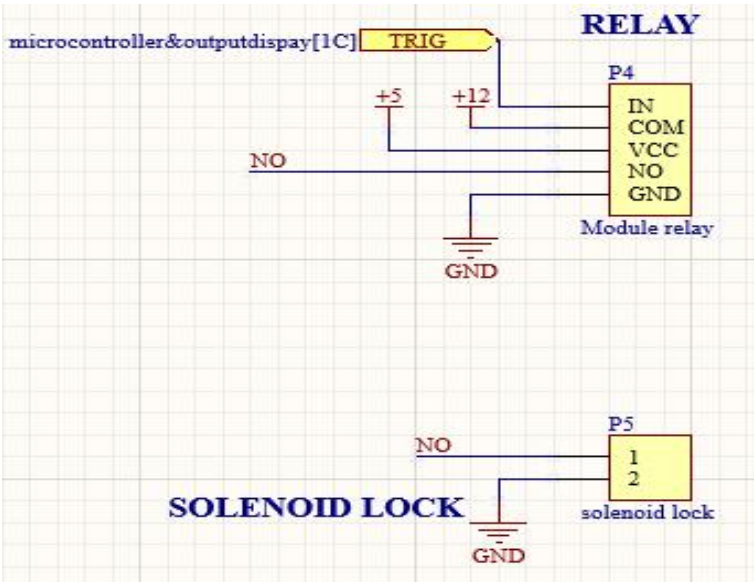


Hình 5: Khối vi điều khiển

3.4. Khối chấp hành

Đây là phần quan trọng nhất để đóng/mở cửa.

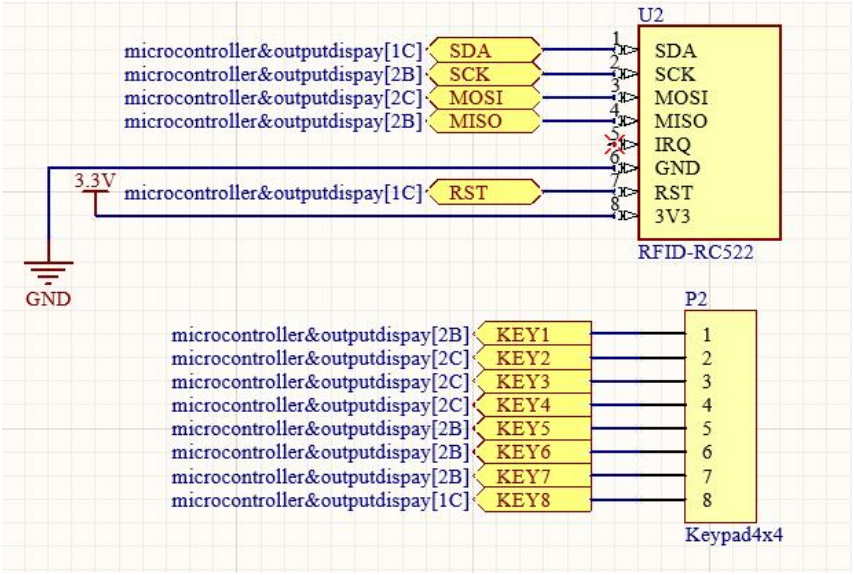
- Relay 5V: Đóng vai trò cách ly giữa vi điều khiển (3.3V) và khóa từ (12V).
- Solenoid Lock: Sử dụng nguồn 12V.



Hình 6: Khối chấp hành

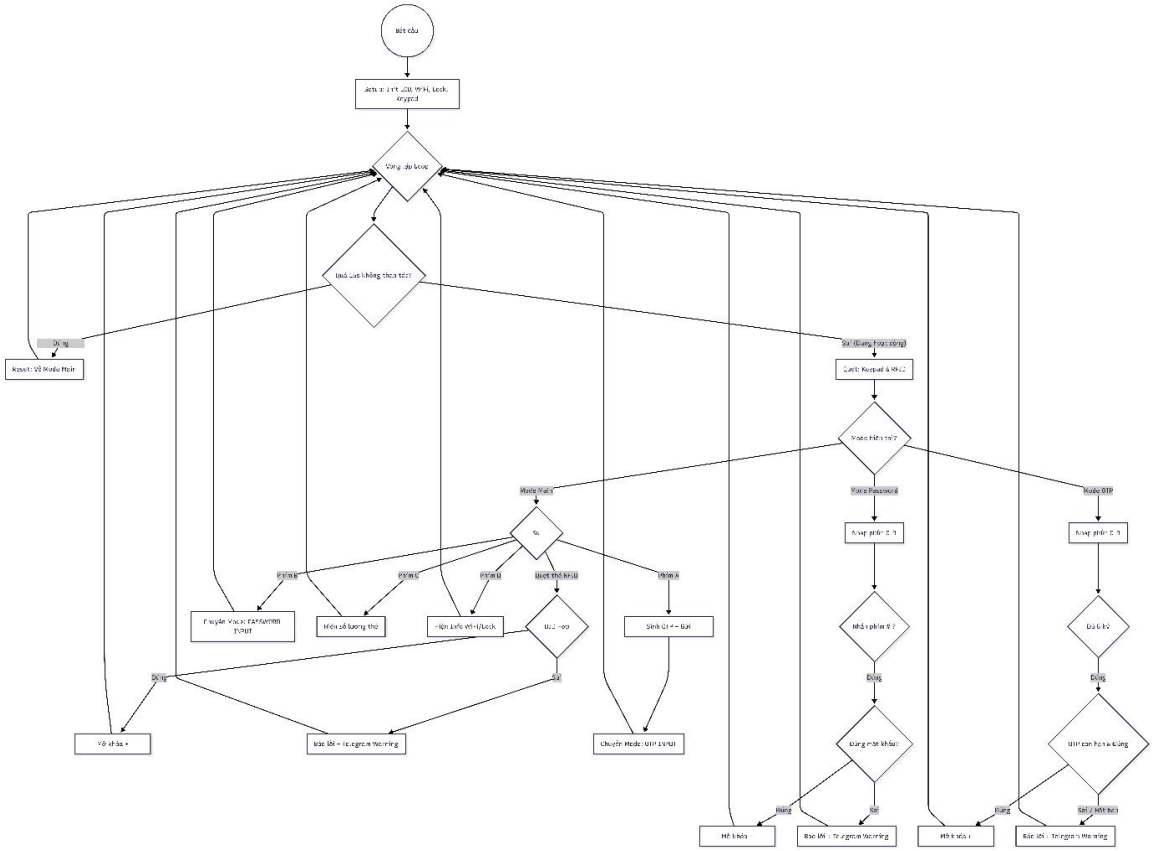
3.5. Khối nhập liệu

- RFID RC522: Giao tiếp qua chuẩn SPI (MOSI, MISO, SCK, SS) cho tốc độ đọc thẻ nhanh.
- Keypad 4x4: Kết nối 8 chân GPIO, sử dụng thư viện Keypad.h để quét ma trận phím.



Hình 7: Khối nhập liệu

CHƯƠNG 4: THIẾT KẾ PHẦN MỀM



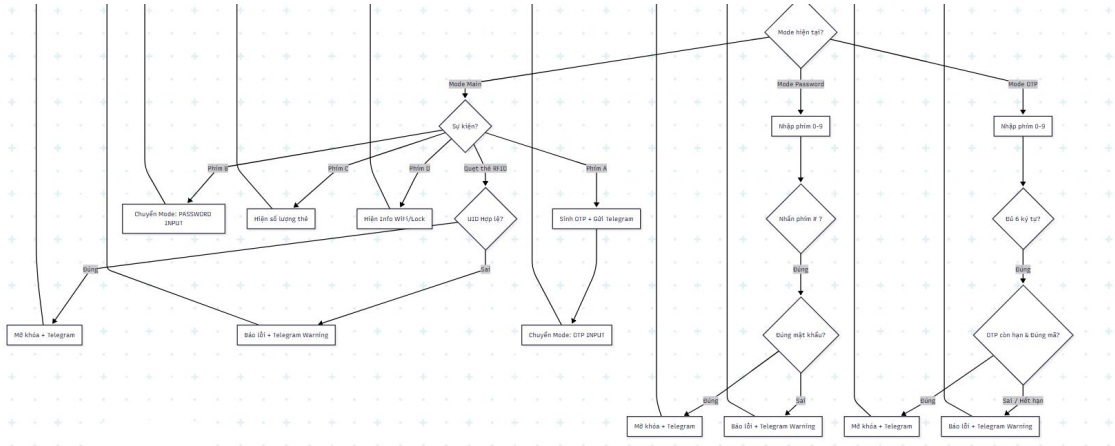
Hình 8: Flowchart của hệ thống

Dựa trên flowchart, hệ thống sẽ hoạt động theo luồng sau:

- Trạng thái SETUP (Khởi tạo): Khi bắt đầu (Start), hệ thống thực hiện khởi tạo các thành phần phần cứng bao gồm: màn hình LCD, kết nối WiFi, module khóa (Lock) và bàn phím (Keypad). Sau khi hoàn tất, hệ thống chuyển sang vòng lặp chính (Loop).
- Trạng thái CHECK TIMEOUT (Kiểm tra thời gian chờ): Trong vòng lặp, hệ thống liên tục kiểm tra thời gian không hoạt động. Nếu phát hiện quá 15 giây người dùng không thao tác, hệ thống thực hiện Reset: đưa giao diện về màn hình chính (Mode Main) và xóa các bộ đệm nhập liệu để bảo mật. Nếu hệ thống đang

được thao tác (thời gian < 15s), hệ thống chuyển sang trạng thái quét tín hiệu đầu vào (Scan Inputs).

- Trạng thái MODE MAIN (Màn hình chính): Hệ thống quét tín hiệu từ Keypad và RFID. Tại đây xử lý các sự kiện:
  - Quẹt thẻ RFID: Hệ thống kiểm tra UID. Nếu Đúng (hợp lệ), thực hiện mở khóa và gửi thông báo Telegram. Nếu Sai, báo lỗi truy cập và gửi cảnh báo Telegram.
  - Phím A: Hệ thống sinh mã OTP, gửi mã qua Telegram, sau đó chuyển trạng thái sang Mode OTP.
  - Phím B: Hệ thống chuyển trạng thái sang Mode Password.
  - Phím C: LCD hiển thị số lượng thẻ RFID hợp lệ đã lưu.
  - Phím D: LCD hiển thị thông tin trạng thái WiFi và trạng thái Khóa.
- Trạng thái MODE PASSWORD (Nhập mật khẩu): Người dùng nhập các phím số (0-9). Khi nhấn phím #, hệ thống kiểm tra mật khẩu:
  - Đúng: Thực hiện mở khóa và gửi thông báo Telegram.
  - Sai: Hệ thống hiển thị lỗi, báo động và gửi cảnh báo Telegram.
- Trạng thái MODE OTP (Nhập mã xác thực): Người dùng nhập các phím số. Khi bộ đệm đủ 6 ký tự, hệ thống tự động kiểm tra tính hợp lệ (mã đúng và còn thời hạn):
  - Đúng & Còn hạn: Thực hiện mở khóa và gửi thông báo Telegram.
  - Sai hoặc Hết hạn: Hệ thống từ chối truy cập, báo lỗi tương ứng và gửi cảnh báo Telegram.

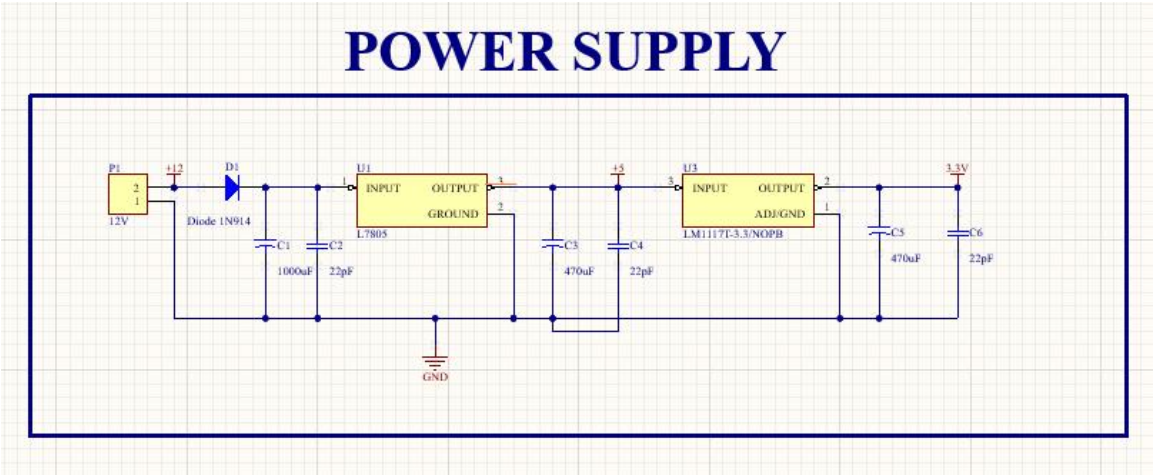


Hình 9: Ba nhánh MODE chính của hệ thống

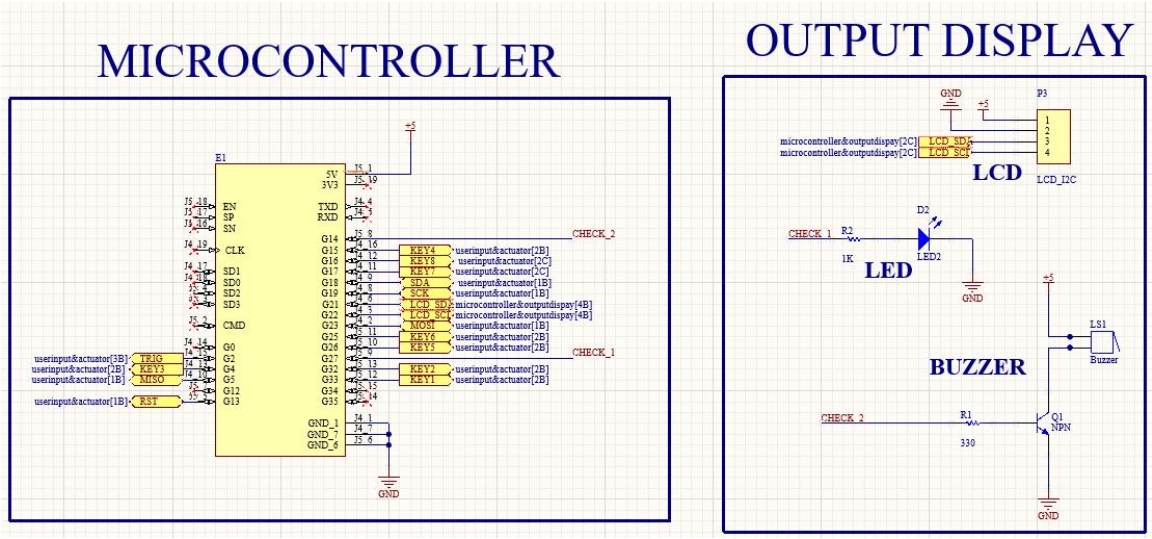
CHƯƠNG 5: KẾT QUẢ

5.1. Schematic

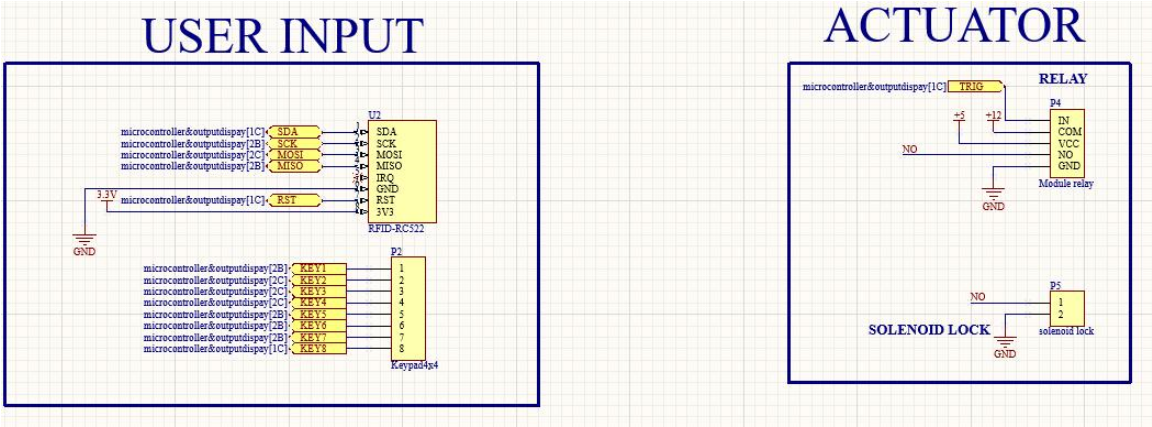
Schematic sẽ bao gồm các khối đã nêu trong thiết kế phần cứng.



Hình 10: Khối nguồn



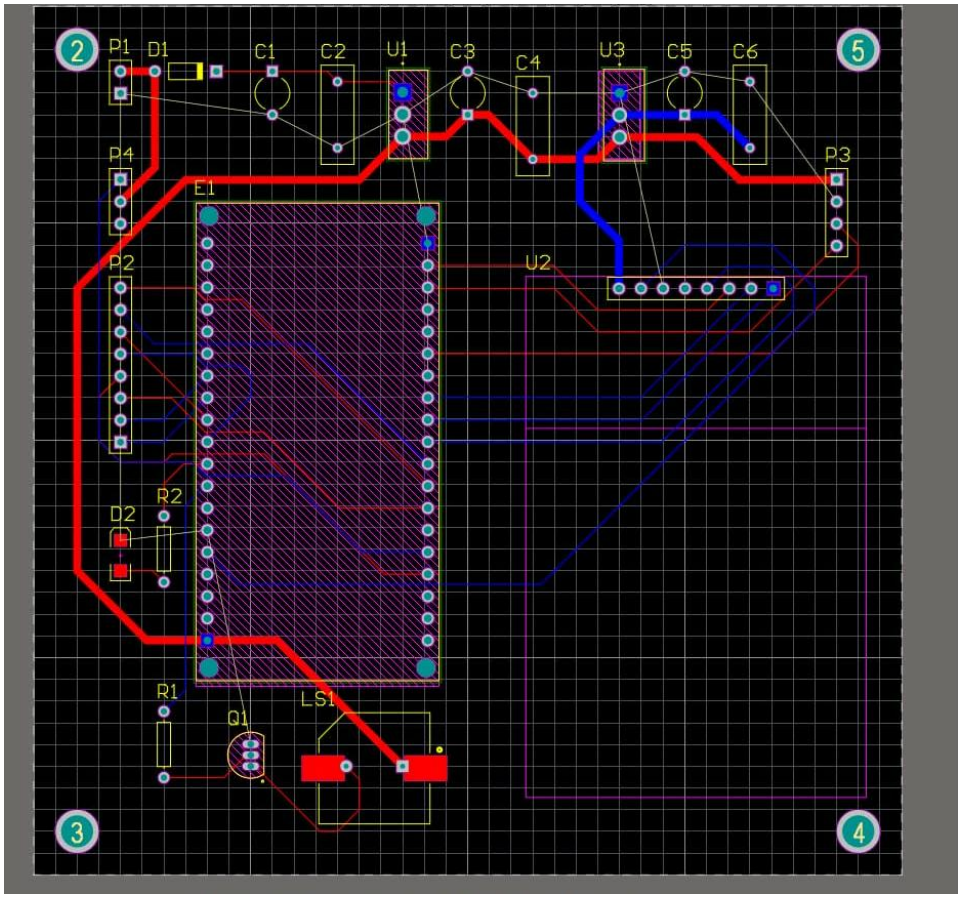
Hình 11: Khối vi điều khiển và khối hiển thị



Hình 12: Khối nhập liệu và khối chấp hành

5.2. Layout

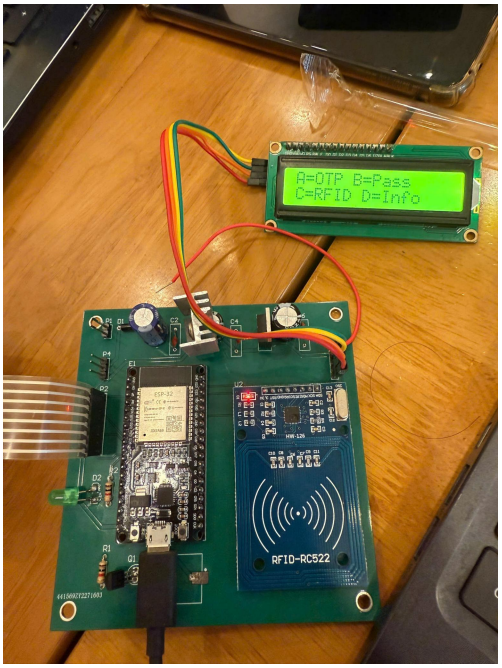
Nhóm thực hiện layout phần cứng theo kết cấu chi tiết như sau:



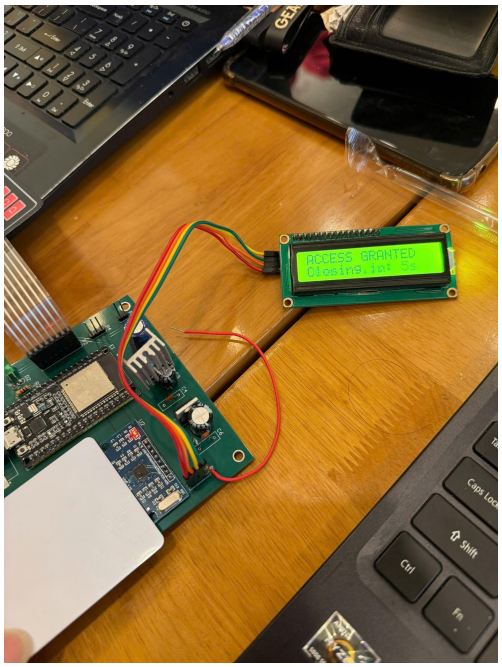
Hình 13: Layout của hệ thống

5.3. Kết quả dự án

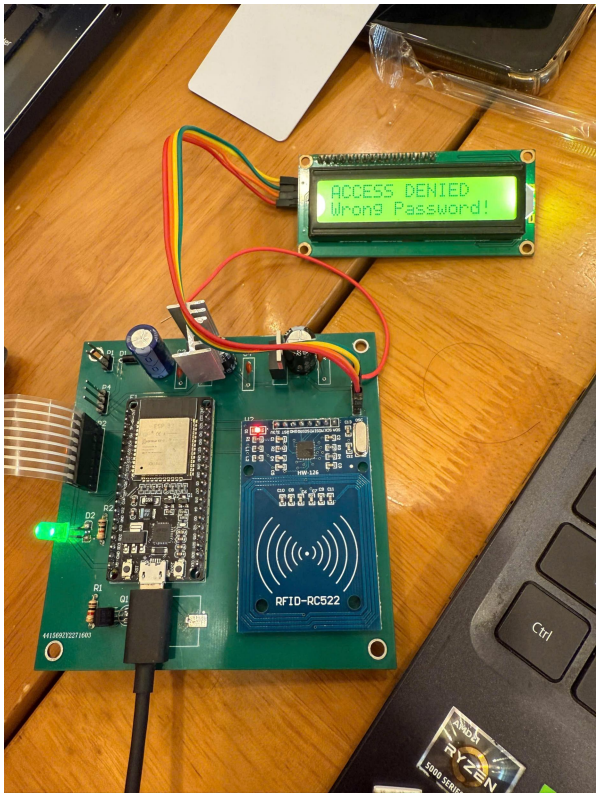
Sau khi thiết kế và xây dựng, kết quả dự án như sau:



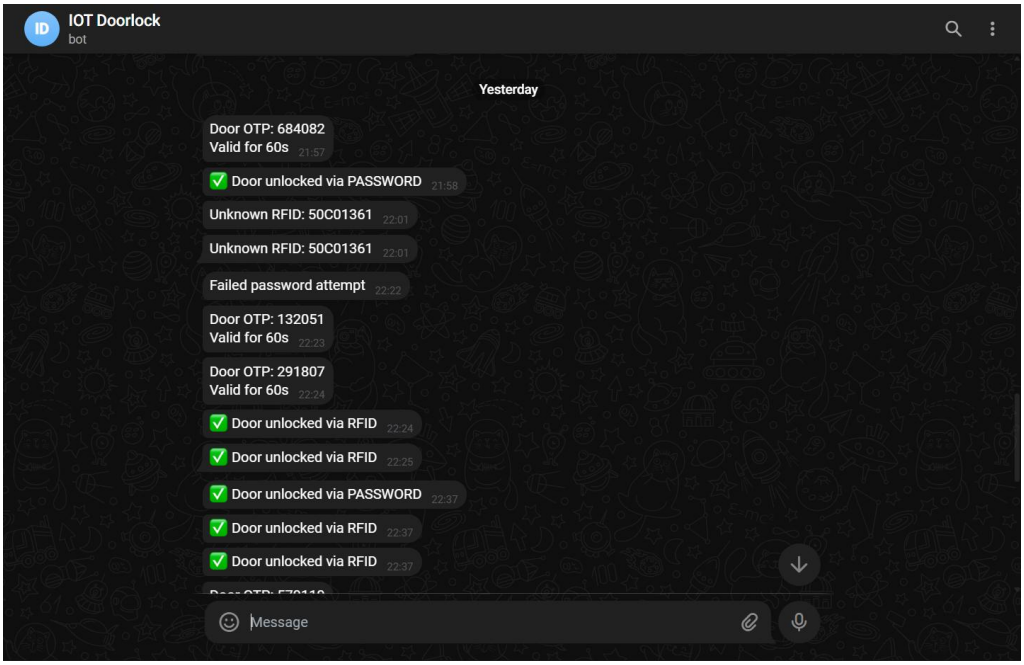
Hình 14: MODE của hệ thống



Hình 15: Màn hình LCD thể hiện khóa được mở trong 5s



Hình 16: LCD thể hiện cảnh báo khi nhập sai mật khẩu



Hình 17: Giao diện Telegram người dùng

CHƯƠNG 6 TỔNG KẾT

Nhóm đã thiết kế và thi công thành công hệ thống khóa cửa thông minh tích hợp công nghệ IoT, hoàn thành mục tiêu xây dựng một thiết bị hoạt động ổn định trên nền tảng vi điều khiển ESP32. Hệ thống đã khắc phục được những hạn chế về an ninh và sự bất tiện của các loại khóa cơ truyền thống thông qua việc tích hợp đa dạng phương thức xác thực và khả năng quản lý từ xa qua Internet, tạo tiền đề cho các ứng dụng Smart Home hiện đại.

Cụ thể, hệ thống đáp ứng tốt các yêu cầu chức năng và phi chức năng đã đề ra:

- Khả năng bảo mật và vận hành đa dạng: Hệ thống thực hiện mở khóa chính xác và nhanh chóng thông qua 3 phương thức: thẻ từ RFID, mật khẩu số (Keypad) và mã xác thực một lần (OTP), đảm bảo tính an toàn cao thay thế cho chìa khóa vật lý.
- Giao diện trực quan và giám sát IoT: Trạng thái cửa được hiển thị thời gian thực trên màn hình LCD và đồng bộ hóa thông báo về ứng dụng Telegram trên điện thoại, giúp người dùng dễ dàng theo dõi lịch sử ra vào và nhận cảnh báo truy cập trái phép tức thời.
- Tính năng tự động hóa: Hệ thống hoạt động theo quy trình khép kín với cơ chế tự động đóng chốt khóa sau 5 giây mở và tự động kích hoạt báo động (Buzzer) khi nhập sai dữ liệu nhiều lần, đảm bảo an ninh 24/7.