ĐẠI HỌC QUỐC GIA TPHCM

TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN

KHOA CÔNG NGHỆ THÔNG TIN

Proposal

Nhập môn lập trình điều khiển thiết bị thông minh (AIoT)

Đồ án: Smart Door Lock System (SDLS)

Sinh viên:

Đinh Nguyễn Gia Bảo (22127027) (Trưởng nhóm)

Nguyễn Công Tuấn (22127436)

Hoàng Lê Minh Đăng (22127051)

Nguyễn Quang Sáng (22127364)

Giảng viên:

TS. Võ Hoài Việt

Ths. Đỗ Thị Thanh Hà

Ngày 4 tháng 6 năm 2025

MỤC LỤC

I. Tổng quan

1. Giới thiệu sản phẩm

Trong cuộc sống hiện đại, nhu cầu về **an ninh, tiện nghi và tự động hóa trong sinh hoạt hàng ngày** ngày càng trở nên cấp thiết. Các phương pháp khóa cửa truyền thống như dùng chìa khóa cơ thường gặp phải nhiều bất tiện như **dễ thất lạc**, **khó kiểm soát người ra vào**, và **khó tích hợp với các hệ thống thông minh khác trong nhà**. Bên cạnh đó, khi xã hội ngày càng phát triển theo hướng **Internet of Things (IoT)** và **nhà thông minh (Smart Home)**, việc ứng dụng công nghệ để cải thiện các chức năng cơ bản trong gia đình trở thành xu hướng tất yếu.

Xuất phát từ thực tế đó, nhóm chúng tôi nhận thấy sự cần thiết của một hệ thống **Khóa Cửa Thông Minh** – một giải pháp có khả năng **thay thế hoàn toàn phương pháp khóa truyền thống** bằng một hệ thống có tính năng **tự động**, **bảo mật cao**, và **dễ dàng tích hợp với các thiết bị thông minh khác**. Việc phát triển hệ thống này không chỉ giải quyết những hạn chế hiện tại mà còn mở ra cơ hội tạo nên một nền tảng **an toàn, hiện đại và đáng tin cậy** cho các ứng dụng nhà thông minh trong tương lai.

2. Ý nghĩa & Mục đích sản phẩm

Việc phát triển Hệ thống Khóa Cửa Thông Minh (SDLS) mang lại nhiều ý nghĩa quan trọng, không chỉ đối với người dùng cuối mà còn góp phần vào xu hướng phát triển công nghệ chung

2.1. Nâng cao An toàn và An ninh cho Ngôi nhà:

- Hệ thống cung cấp một lớp bảo vệ vượt trội so với khóa cơ truyền thống, vốn dễ bị sao chép chìa, bẻ khóa. Các phương thức xác thực hiện đại như nhận diện khuôn mặt, mã số, và điều khiển từ xa có giám sát giúp hạn chế tối đa nguy cơ đột nhập trái phép.
- Khả năng ghi lại lịch sử ra vào và gửi cảnh báo tức thời khi có dấu hiệu bất thường (như cố gắng mở khóa sai nhiều lần) giúp người dùng chủ động nắm bắt tình hình an ninh của ngôi nhà, ngay cả khi ở xa.

2.2. *Tối ưu hóa Sự Tiện lợi và Linh hoạt trong Cuộc sống Hàng ngày:*

- Loại bỏ hoàn toàn sự bất tiện của việc mang theo và bảo quản chìa khóa cơ, nỗi lo quên chìa hay mất chìa.
- Cho phép chủ nhà dễ dàng cấp quyền truy cập tạm thời hoặc theo lịch trình cho khách, người giúp việc, hoặc nhân viên giao hàng từ xa thông qua ứng dụng di động, mà không cần phải có mặt trực tiếp.
- Tự động hóa việc mở cửa giúp tiết kiệm thời gian và mang lại trải nghiệm sống tiện nghi, hiện đại hơn.

2.3. *Thúc đẩy Quá trình Hiện đại hóa và Xây dựng Nhà Thông minh (Smart Home):*

- SDLS không chỉ là một thiết bị độc lập mà còn là một thành phần quan trọng, có khả năng tích hợp và tương tác với các thiết bị thông minh khác trong hệ sinh thái nhà thông minh (ví dụ: tự động bật đèn khi chủ nhà về, kích hoạt hệ thống an ninh khi tất cả rời đi).
- Dự án góp phần phổ biến ứng dụng công nghệ Internet of Things (IoT) vào đời sống thực tiễn, mang lại những giá trị thiết thực và nâng cao chất lượng cuộc sống.

2.4. *Đáp ứng Nhu cầu Thực tiễn và Mang lại Giá trị Cộng thêm:*

- Trong bối cảnh công nghệ số phát triển mạnh mẽ, nhu cầu về các giải pháp tự động hóa, an toàn và thông minh ngày càng tăng. SDLS đáp ứng trực tiếp nhu cầu này, mang đến một giải pháp bảo mật tiên tiến và tiện ích.
- Sản phẩm hoàn thiện có tiềm năng thương mại hóa, đóng góp vào sự phát triển của thị trường thiết bị thông minh tại Việt Nam, đồng thời khẳng định năng lực ứng dụng và phát triển công nghệ của đội ngũ thực hiện.

Hệ thống Khóa Cửa Thông Minh (SDLS) nhằm cách mạng hóa an ninh và tiện nghi trong không gian sống, thay thế khóa truyền thống bằng giải pháp công nghệ cao tích hợp AI và IoT. Sản phẩm hướng đến xây dựng hệ sinh thái nhà thông minh an toàn, hiện đại, dễ dùng, đáp ứng nhu cầu tự động hóa và bảo mật. SDLS loại bỏ bất tiện của chìa khóa cơ, tạo nền tảng cho môi trường sống thông minh, kết nối, góp phần thúc đẩy hiện đại hóa ngôi nhà tại Việt Nam và nâng cao chất lượng cuộc sống.

Tóm lại, Hệ thống Khóa Cửa Thông Minh không chỉ giải quyết những hạn chế của phương pháp khóa truyền thống mà còn mở ra một kỷ nguyên mới về an ninh, tiện nghi và tự động hóa cho không gian sống, đóng góp tích cực vào việc xây dựng một cuộc sống thông minh và an toàn hơn.

3. Mục tiêu

Dự án Hệ thống Khóa Cửa Thông Minh (SDLS) tập trung vào 3 mục tiêu quan trọng và thực tế để đảm bảo tính hiệu quả, an ninh và khả năng triển khai trong môi trường nhà thông minh:

STT	Mục tiêu	Chỉ tiêu định lượng & Thời hạn
1	Xây dựng hệ thống nhận diện khuôn mặt có thể hoạt động ổn định trong điều kiện thực tế	Đạt độ chính xác ≥ 90% trong điều kiện ánh sáng tự nhiên, khoảng cách 0.5–1m, hoàn thành trong 2 tuần đầu triển khai
2	Tích hợp chức năng mở khóa từ xa thông qua ứng dụng web và điện thoại	Đảm bảo thời gian phản hồi ≤ 3 giây trong mạng ổn định, hoàn thành trong tuần thứ 3 của dự án
3	Thiết lập chế độ hoạt động ngoại tuyến bằng mật khẩu số, đảm bảo hệ thống vẫn mở khóa khi không có Internet	Thời gian mở khóa ≤ 2 giây, tỷ lệ thành công ≥ 95%, hoàn thành trong tuần thứ 4

Các mục tiêu trên được lựa chọn theo tiêu chuẩn SMART để đảm bảo rằng hệ thống không chỉ đạt được tính tự động, hiện đại, và thân thiện với người dùng, mà còn đáp ứng các yêu cầu thực tiễn về an ninh, độ tin cậy và khả năng triển khai trong môi trường gia đình thông minh.

4. Khó khăn và thách thức

1. Công nghệ Nhận diện Khuôn mặt:
   - Đạt độ chính xác cao (>90%) và tốc độ xử lý nhanh trong điều kiện ánh sáng thực tế đa dạng (ngày, đêm, ngược sáng).
   - Chống giả mạo hiệu quả bằng hình ảnh, video hoặc các kỹ thuật tinh vi khác.

2. Kết nối Mạng và Hoạt động Từ xa/Offline:
   - Đảm bảo kết nối từ xa ổn định, phản hồi nhanh (<3s) bất chấp biến động của mạng Internet.
   - Đồng bộ hóa dữ liệu và duy trì hoạt động tin cậy khi mất kết nối Internet (chế độ mật khẩu số).
3. Phát triển Hệ thống Phức tạp và Đa nền tảng:
   - Tích hợp nhiều công nghệ: nhận diện AI, lập trình nhúng (firmware), ứng dụng di động (Android), ứng dụng web, và quản lý backend.
   - Thiết kế giao diện người dùng (UI/UX) trực quan, dễ sử dụng trên cả di động và web.
4. Độ Tin cậy và Ổn định của Hệ thống:
   - Đảm bảo hệ thống hoạt động liên tục, chính xác 24/7 và xử lý tốt các tình huống lỗi (ví dụ: cảnh báo kịp thời <5s, không báo động giả).
   - Quản lý nguồn điện và độ bền của thiết bị phần cứng.

II. Phát biểu bài toán

1. Đầu vào - đầu ra

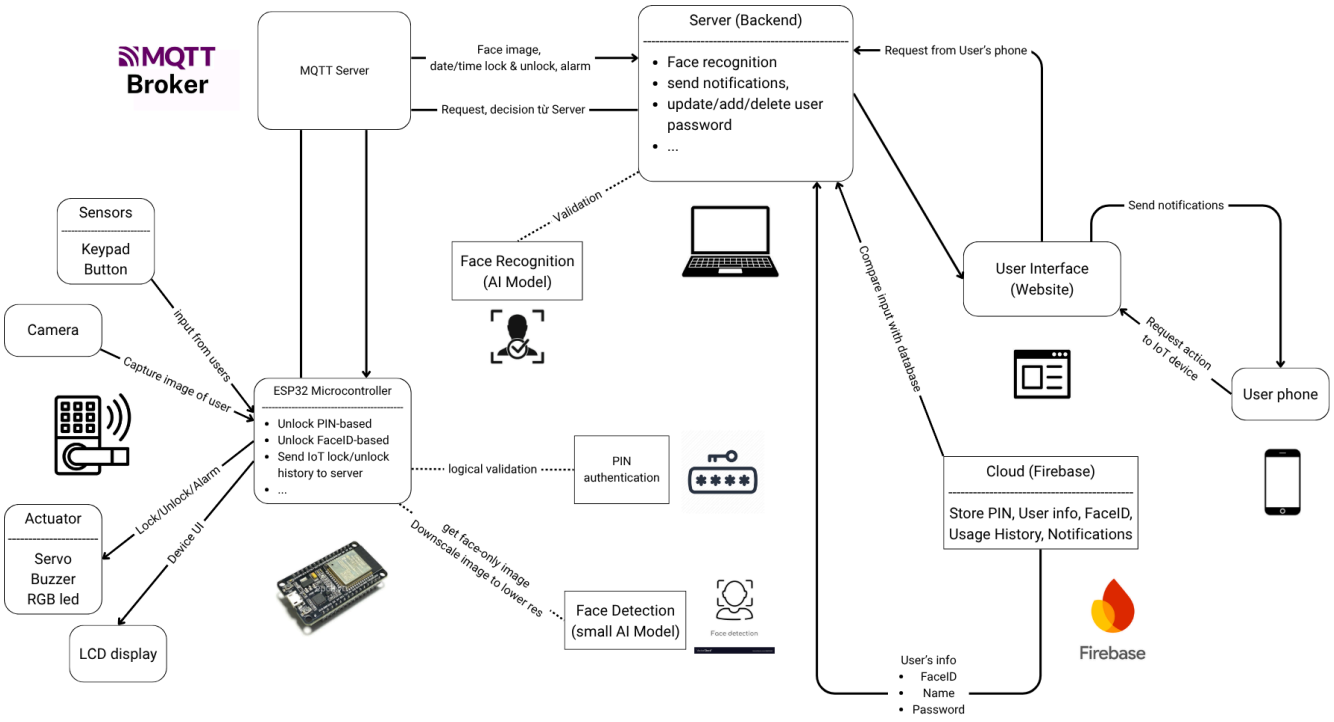
1.1. Input

- **Ảnh khuôn mặt người dùng**: Được chụp từ camera, lưu trữ dưới dạng ảnh RGB (ma trận 3 chiều có kích thước H×W×3).
- **Mã PIN từ bàn phím (keypad)**: Dữ liệu người dùng nhập vào, lưu dưới dạng chuỗi ký tự (String[]). Dùng để xác thực khi không sử dụng nhận diện khuôn mặt.
- **Lệnh điều khiển từ xa**: Được gửi từ ứng dụng điện thoại hoặc giao diện website. Dạng tín hiệu điều khiển (mở/khóa), biểu diễn bằng biến Boolean flag.

1.2. Output

- **Góc xoay của Servo motor**: Điều khiển phần cứng để mở hoặc khóa cửa. Giá trị góc dưới dạng Integer (VD: 0° để khóa, 90° để mở).
- **Trạng thái còi báo động (Buzzer)**: Kêu hay không tùy thuộc vào kết quả xác thực khuôn mặt. Dạng Boolean (True nếu có báo động, False nếu không).
- **Thông tin hiển thị trên LCD**: Phản hồi người dùng sau mỗi lần thao tác. Gồm các nội dung như: "Mở cửa thành công", "Mở cửa thất bại", "Cảnh báo: Không nhận diện được". Dạng dữ liệu: String.

2. Sơ đồ hệ thống (Framework)



Hình 1: Framework hệ thống Smart Door Lock System

2.1. ESP32 Microcontroller (Thiết bị điều khiển trung tâm)

ESP32 đóng vai trò là bộ điều khiển chính tại thiết bị cửa, tiếp nhận đầu vào từ các cảm biến (bàn phím, camera, nút nhấn), sau đó xử lý hoặc gửi dữ liệu lên máy chủ để xác thực. Nó điều khiển trực tiếp các thiết bị phần cứng như:

- **Servo motor** (để mở/đóng khóa),
- **Buzzer và LED RGB** (để thông báo trạng thái hoặc cảnh báo),
- **LCD** (để hiển thị hướng dẫn và phản hồi người dùng).

ESP32 hỗ trợ 2 phương thức xác thực:

- **Nhập mã PIN** (PIN-based unlocking),
- **Nhận diện khuôn mặt** (FaceID-based unlocking).

2.2. Camera và AI xử lý khuôn mặt

Khi có người dùng tiếp cận, camera sẽ chụp ảnh khuôn mặt. Ảnh được xử lý qua hai bước:

- **Face Detection**: Một mô hình AI nhẹ xác định vùng khuôn mặt trong ảnh và nén ảnh xuống độ phân giải thấp.

- **Face Recognition**: Một mô hình AI lớn hơn (trên server) sẽ thực hiện nhận dạng để xác định danh tính người dùng.

2.3. MQTT Broker

Hệ thống sử dụng giao thức **MQTT** để trao đổi dữ liệu giữa các thiết bị IoT (ESP32) và server. MQTT đảm bảo giao tiếp nhẹ, ổn định trong môi trường IoT, đồng thời hỗ trợ gửi các thông điệp như:

- Trạng thái khóa/mở,
- Yêu cầu xác thực,
- Gửi dữ liệu thời gian thực đến máy chủ

2.4. Backend Server (Máy chủ trung tâm)

Máy chủ thực hiện các chức năng chính:

- Xử lý xác thực khuôn mặt,
- So sánh mã PIN hoặc FaceID với cơ sở dữ liệu,
- Gửi thông báo đến người dùng,
- Quản lý cơ sở dữ liệu người dùng (thêm/sửa/xóa thông tin),
- Ghi nhận lịch sử truy cập

2.5. Firebase (Dịch vụ đám mây)

Firebase được sử dụng như nền tảng lưu trữ và đồng bộ dữ liệu theo thời gian thực. Nó bao gồm:

- Lưu thông tin người dùng: PIN, FaceID, tên, lịch sử truy cập,
- Quản lý quyền truy cập,
- Lưu trữ thông báo và trạng thái hệ thống.

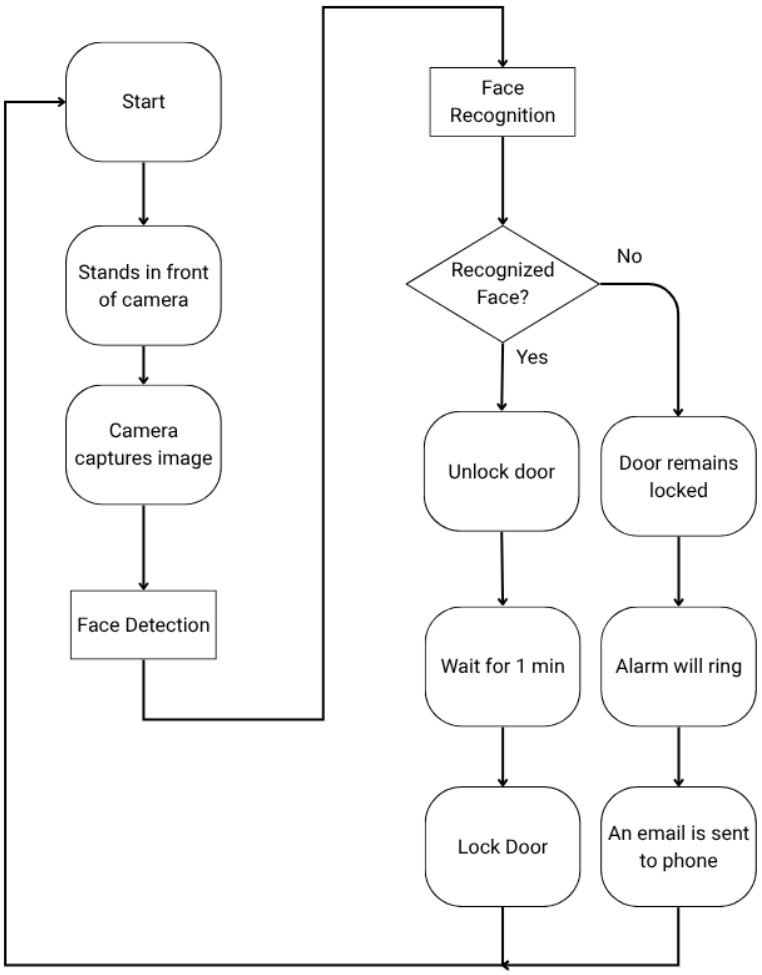
2.6. Giao diện người dùng (Website & Ứng dụng điện thoại)

Giao diện web hoặc ứng dụng di động cho phép người dùng:

- Theo dõi trạng thái cửa (đã khóa/chưa khóa),
- Mở khóa từ xa,
- Quản lý tài khoản người dùng và thông tin bảo mật,
- Nhận thông báo cảnh báo khi có truy cập trái phép.

3. Hệ thống Face Recognition

Hệ thống **Face Recognition** là thành phần cốt lõi trong giải pháp **Smart Door Lock**, cho phép nhận diện khuôn mặt người dùng để ra quyết định mở/khóa cửa một cách tự động và an toàn. Quá trình nhận diện được thiết kế theo pipeline xử lý gồm các bước chính: **phát hiện khuôn mặt (face detection)**, **nhận dạng khuôn mặt (face recognition)**, và **xử lý phản hồi điều khiển** dựa trên kết quả nhận dạng.



Hình 2: Sơ đồ luồng xử lý Face Recognition cho IoT device

Phát hiện người dùng: Khi có người đứng trước camera, hệ thống ESP32-CAM sẽ tự động kích hoạt việc chụp ảnh.

Face Detection: Ảnh được truyền qua một mô hình AI nhỏ thực hiện phát hiện vùng chứa khuôn mặt. Ảnh sẽ được **downscale** để giảm dung lượng, sau đó trích xuất phần khuôn mặt để gửi lên server xử lý tiếp theo.

Face Recognition: Mô hình nhận diện khuôn mặt (AI model lớn hơn) trên máy chủ sẽ so sánh ảnh khuôn mặt gửi đến với cơ sở dữ liệu người dùng (trên Firebase). Nếu khuôn mặt được nhận diện (kết quả trùng khớp trên ngưỡng xác định), hệ thống xác thực thành công.

Phản hồi điều khiển:

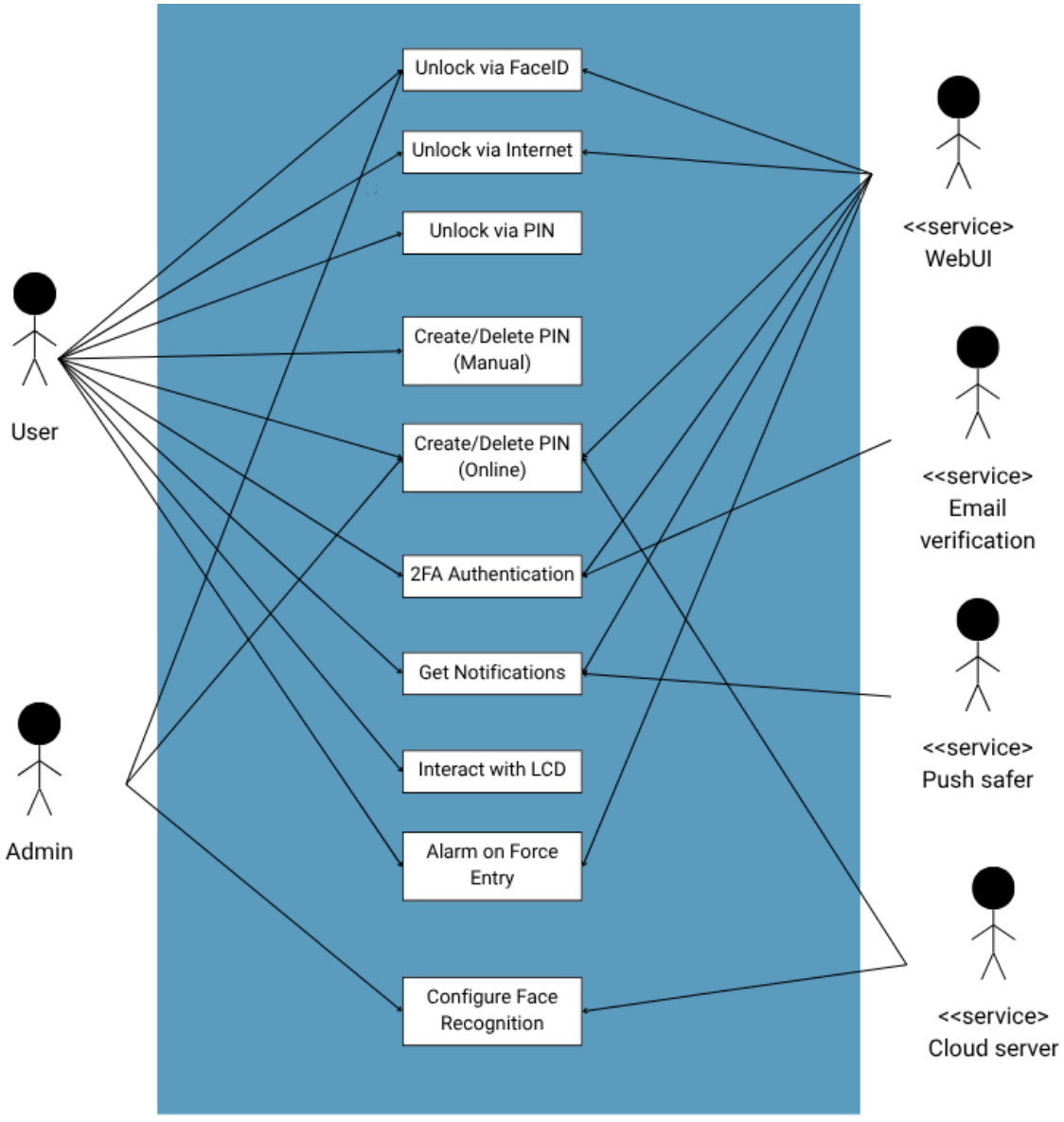
- Nếu xác thực thành công: Hệ thống điều khiển sẽ **mở khóa**. Sau khoảng thời gian 1 phút, hệ thống sẽ tự **khóa lại cửa** để đảm bảo an toàn.

- Nếu xác thực thất bại: Cửa vẫn được giữ ở trạng thái **đóng**. **Còi báo động (buzzer)** được kích hoạt. Một **thông báo (email hoặc tin nhắn)** sẽ được gửi đến điện thoại của chủ nhà qua Firebase để cảnh báo truy cập trái phép.

III. Đặc tả sản phẩm (Specifications)

1. Sơ đồ tính năng (Use-case model)

1.1 Actor model



1.2 Các tính năng chính của sản phẩm (Main use-case)

1.2.1 Điều khiển cửa ra vào

- **Mở/Đóng cửa tự động** thông qua xác thực khuôn mặt (Face Recognition).
- **Mở/Đóng cửa thủ công** bằng cách nhập mã PIN qua bàn phím (keypad).
- **Mở/Đóng cửa từ xa** thông qua giao diện web (Web UI / Internet-connected).

1.2.2 Quản lý mật khẩu

- **Tạo, sửa đổi, và xoá mã PIN/mật khẩu** của người dùng đã đăng ký.
- **Thiết lập mật khẩu trực tiếp** trên thiết bị qua bàn phím.

Thiết lập hoặc thay đổi mật khẩu từ xa qua giao diện web.

1.2.3 Bảo mật và an toàn hệ thống

- **Cảnh báo khi có tác động mạnh** lên thiết bị (force detection), còi báo động sẽ được kích hoạt.
- **Xác thực hai lớp (Two-factor Authentication)**: Kết hợp FaceID + PIN hoặc xác thực từ xa. **Lưu trữ dữ liệu trên cloud Firebase** và mã hóa dữ liệu truyền qua Internet (HTTPS/MQTT secure).

1.2.4 Giao tiếp và tương tác người dùng

- **LCD hiển thị hướng dẫn sử dụng** khi khởi động lần đầu hoặc sau khi thiết bị được reset.
- **Gửi thông báo thời gian thực** đến điện thoại người dùng về:
  - Lịch sử mở/đóng cửa,
  - Thay đổi mật khẩu,
  - Cảnh báo bảo mật.

1.3 List of actors

No.	Actor	Detailed Description
1	User	Người sử dụng cuối cùng của hệ thống Smart Door Lock. Có thể mở cửa bằng khuôn mặt, mã PIN hoặc giao diện web. Không có quyền truy cập vào cấu hình hệ thống hay dữ liệu quản trị.
2	Admin	Quản trị viên hệ thống. Có toàn quyền truy cập, bao gồm: quản lý cơ sở dữ liệu người dùng, cấu hình thiết bị, cập nhật mô hình AI, xem lịch sử truy cập, và thực hiện thao tác mở khóa từ xa thông qua giao diện quản lý.

1.4 List of services

No.	Actor	Service	Detailed Description
1	User	Face-based Unlocking	Cho phép người dùng mở cửa bằng cách nhận diện khuôn mặt thông qua camera.
2	User	PIN-based Unlocking	Cho phép người dùng nhập mã PIN trên keypad để mở khóa cửa (trường hợp nhận diện khuôn mặt thất bại).
3	User	Remote Unlock (Web)	Cho phép người dùng đã xác thực đăng nhập vào giao diện web có thể mở khóa từ xa.
4	Admin	Configure Face Recognition	Thêm/xóa hình ảnh người dùng, cập nhật dữ liệu khuôn mặt.
5	User/Admin	Web UI Interaction	Giao diện quản lý và điều khiển từ xa qua website
6	System	Push Notifications	Gửi thông báo truy cập, cảnh báo qua app hoặc điện thoại.

2. Use-case Specifications

2.1 Use-case: Đóng mở cửa thủ công

Use case Name	Mở/đóng mở cửa thủ công
Brief description	User sử dụng mật khẩu số hoặc chìa khóa để mở/đóng cửa mà không cần đến tính năng tự động hoặc kết nối Internet, đảm bảo hoạt động ngay cả khi mất điện
Actors	User: Người sử dụng hệ thống khóa cửa thông minh, bao gồm chủ nhà hoặc người được cấp quyền
Basic Flow	1. Bắt đầu: User tiếp cận cửa và sử dụng bàn phím số hoặc chìa khóa cơ học 2. Nhập mật khẩu (nếu sử dụng bàn phím số) - User nhập mật khẩu số trên bàn phím tích hợp - Hệ thống xác thực mật khẩu - Nếu đúng, khóa cửa được mở - Ghi lại lịch sử mở cửa vào cơ sở dữ liệu (nếu hệ thống được kết nối) - Nếu sai, từ chối mở cửa và yêu cầu nhập lại (giới hạn số lần nhập sai, ví dụ: 3 lần) 3. Sử dụng chìa khóa cơ học (nếu không dùng mật khẩu) - User sử dụng chìa khóa cơ học để mở khóa - Cửa được mở mà không cần xác thực qua hệ thống điện tử 4. Đóng cửa - User đóng cửa thủ công - Hệ thống tự động khóa lại (nếu được cấu hình) hoặc User khóa bằng chìa khóa cơ học 5. Kết thúc: Hệ thống trở về trạng thái chờ
Alternative Flows	A1: Nhập sai mật khẩu quá số lần cho phép - Hệ thống kích hoạt còi báo động - Gửi thông báo đến User (nếu có kết nối Wi-Fi) - Tạm khóa bàn phím số trong 5 phút để ngăn thử mật khẩu tiếp theo A2: Mất điện - Hệ thống chuyển sang chế độ pin dự phòng - User có thể sử dụng chìa khóa cơ học để mở/đóng cửa A3: Lỗi bàn phím số - User chuyển sang sử dụng chìa khóa cơ học để mở cửa
Pre-conditions	1. Hệ thống khóa cửa đã được cài đặt với bàn phím số hoặc ổ khóa 2. User đã được cấp mật khẩu số hoặc chìa khóa 3. Hệ thống có thể hoạt động bằng pin dự phòng trong trường hợp mất điện
Post-conditions	1. Cửa được mở hoặc đóng thành công theo cách thủ công 2. Lịch sử mở/đóng cửa được ghi lại (nếu hệ thống được kết nối) 3.Hệ thống trở về trạng thái chờ, sẵn sàng cho lần sử dụng tiếp theo

2.2 Use-case: Đóng mở cửa tự động bằng khuôn mặt

Use case Name	Đóng mở cửa tự động bằng khuôn mặt
Brief description	User sử dụng mật khẩu số hoặc chìa khóa để mở/đóng cửa mà không cần đến tính năng tự động hoặc kết nối Internet, đảm bảo hoạt động ngay cả khi mất điện
Actors	User: Người sử dụng hệ thống khóa cửa thông minh, bao gồm chủ nhà hoặc người được cấp quyền Admin: Theo dõi và quản lý lịch sử đóng/mở cửa Hệ thống AI: Thực hiện nhận diện khuôn mặt hoặc hành vi bất thường
Basic Flow	1. Bắt đầu: User tiếp cận cửa, đứng trong phạm vi nhận diện của camera

	2. Nhận diện khuôn mặt: Hệ thống AI kích hoạt camera, quét và phân tích khuôn mặt của User 3. Xác thực: - Nếu khuôn mặt khớp với cơ sở dữ liệu: - Hệ thống tự động mở khóa cửa - Gửi thông báo qua website/ứng dụng đến User (nếu được cấu hình) - Nếu khuôn mặt không khớp: - Hệ thống từ chối mở cửa - Kích hoạt còi báo động (nếu phát hiện hành vi bất thường, ví dụ: cố ý mở khóa nhiều lần) 4. Đóng cửa - Sau khi User đi qua, hệ thống tự động đóng và khóa cửa sau một khoảng thời gian (ví dụ: 5 giây) - Ghi lại lịch sử đóng/mở cửa vào cơ sở dữ liệu 5. Kết thúc: Hệ thống trở về trạng thái chờ
Alternative Flows	A1: Mất điện - Hệ thống chuyển sang chế độ pin dự phòng - Nhận diện khuôn mặt vẫn hoạt động với hiệu suất tối ưu - Nếu pin yếu, gửi thông báo đến User qua Wifi (nếu còn kết nối) A2: Nhận diện khuôn mặt thất bại - Hệ thống yêu cầu User nhập mật khẩu số thủ công hoặc sử dụng xác thực 2 bước - Nếu nhập sai quá số lần (ví dụ: 3 lần), kích hoạt còi báo động và gửi thông báo đến User A3: Phát hiện hành vi bất thường - Hệ thống AI nhận diện hành vi bất thường (ví dụ: người lạ đứng quá lâu) - Kích hoạt còi báo động và gửi thông báo khẩn cấp tới User A4: Kết nối Wifi bị gián đoạn - Hệ thống hoạt động offline, sử dụng cơ sở dữ liệu cục bộ để nhận diện khuôn mặt - Lịch sử đóng/mở cửa được lưu cục bộ và đồng bộ khi Wi-Fi khôi phục
Pre-conditions	1. Hệ thống khóa cửa đã được cài đặt và kết nối với nguồn điện hoặc pin 2. Camera tích hợp trên khóa cửa hoạt động bình thường 3. Cơ sở dữ liệu khuôn mặt của User đã được đăng ký 4. Hệ thống AI đã được huấn luyện để nhận diện khuôn mặt 5. Kết nối Wifi ổn định (nếu sử dụng thông báo qua Internet)
Post-conditions	1. Cửa được mở hoặc đóng thành công 2. Lịch sử đóng/mở cửa được ghi lại (cục bộ hoặc đám mây) 3. Thông báo được gửi đến User (nếu được cấu hình) 4. Hệ thống trở về trạng thái chờ

2.3 Use-case: Đóng mở cửa thông qua Internet

Use case Name	Đóng mở cửa thông qua Internet
Brief description	User sử dụng mật khẩu số hoặc chìa khóa để mở/đóng cửa mà không cần đến tính năng tự động hoặc kết nối Internet, đảm bảo hoạt động ngay cả khi mất điện
Actors	User: Người sử dụng hệ thống, có quyền truy cập qua website/ứng dụng Admin: Quản lý cấu hình hệ thống và theo dõi lịch sử mở/đóng cửa Hệ thống AI: Xác thực yêu cầu mở cửa từ xa (nếu tích hợp xác thực 2 bước)
Basic Flow	1. Bắt đầu: User truy cập website hoặc ứng dụng di động của SDLS 2. Đăng nhập: User nhập thông tin đăng nhập (tên đăng nhập, mật khẩu) - Xác thực 2 bước (nếu được kích hoạt)

	- Hệ thống gửi mã OTP qua email hoặc tin nhắn SMS đến User - User nhập mã OTP để xác thực - Yêu cầu mở cửa - User chọn tùy chọn "Mở cửa" trên giao diện website/ứng dụng - Hệ thống kiểm tra quyền truy cập và gửi lệnh đến khóa cửa qua giao thức MQTT - Khóa cửa mở và gửi thông báo xác nhận đến User 3. Đóng cửa: - User chọn tùy chọn "Đóng cửa" hoặc hệ thống tự động đóng sau một khoảng thời gian (ví dụ: 5 giây) - Ghi lại lịch sử đóng/mở cửa vào cơ sở dữ liệu đám mây 4. Kết thúc: Hệ thống trở về trạng thái chờ
Alternative Flows	A1: Kết nối Wifi bị gián đoạn - Hệ thống thông báo lỗi kết nối đến User - User được khuyến nghị sử dụng chế độ thủ công (mật khẩu số hoặc chìa khóa cơ học) A2: Xác thực 2 bước thất bại - Hệ thống từ chối yêu cầu mở cửa nếu mã OTP sai hoặc hết hạn - User được yêu cầu thử lại hoặc liên hệ Admin A3: Phát hiện truy cập trái phép - Nếu phát hiện hành vi đăng nhập bất thường (ví dụ: nhiều lần nhập sai mật khẩu), hệ thống tạm khóa tài khoản và gửi thông báo đến Admin A4: Lỗi hệ thống từ xa - Nếu lệnh mở/đóng cửa không được thực thi, hệ thống gửi thông báo lỗi đến User
Pre-conditions	1. Hệ thống khóa cửa đã được kết nối với Wifi ổn định 2. User đã đăng ký tài khoản và được cấp quyền truy cập trên website/ứng dụng 3. Hệ thống hỗ trợ xác thực 2 bước (nếu được cấu hình) 4. Thiết bị di động hoặc máy tính của User có kết nối Internet
Post-conditions	1. Cửa được mở hoặc đóng thành công qua Internet 2. Lịch sử đóng/mở cửa được ghi lại trong cơ sở dữ liệu đám mây 3. Thông báo xác nhận được gửi đến User 4. Hệ thống trở về trạng thái chờ

2.4 Use-case: Tạo mật khẩu số thủ công

Use case Name	Tạo mật khẩu số thủ công
Brief description	User sử dụng bàn phím số để tự tạo hoặc chỉnh sửa mật khẩu số cho hệ thống khóa cửa, đảm bảo tính bảo mật và linh hoạt
Actors	User: Người sử dụng hệ thống, có quyền tạo hoặc thay đổi mật khẩu số của mình Admin: Người quản lý hệ thống, có quyền tạo hoặc chỉnh sửa mật khẩu số cho nhiều User Hệ thống AI: Xác thực quyền truy cập của User trước khi cho phép tạo mật khẩu (nếu tích hợp xác thực 2 bước)
Basic Flow	1. Bắt đầu: User tiếp cận bàn phím số trên khóa cửa hoặc đăng nhập vào website/ứng dụng SDLS 2. Xác thực quyền truy cập - Nếu sử dụng bàn phím số: User mật khẩu hiện tại - Nếu sử dụng website/ứng dụng: User đăng nhập bằng tài khoản và mật khẩu, có thể kèm xác thực 2 bước (OTP qua email/SMS) 3. Tạo mật khẩu - User nhập mật khẩu số mới (ví dụ: 4-8 chữ số) và xác nhận lại mật

	khẩu - Hệ thống kiểm tra tính hợp lệ của mật khẩu (độ dài, không trùng lặp với mật khẩu cũ) 4. Lưu mật khẩu - Mật khẩu được lưu vào cơ sở dữ liệu cục bộ của khóa hoặc đồng bộ lên đám mây (nếu có Wi-Fi) - Hệ thống ghi lại lịch sử tạo/chỉnh sửa mật khẩu vào cơ sở dữ liệu 5. Thông báo - Hệ thống xác nhận tạo mật khẩu thành công qua bàn phím (đèn báo/âm thanh) hoặc thông báo trên website/ứng dụng 6. Kết thúc: Hệ thống trở về trạng thái chờ
Alternative Flows	A1: Xác nhận mật khẩu thất bại - Hệ thống từ chối yêu cầu tạo mật khẩu - User được yêu cầu nhập lại mã quản lý hoặc mật khẩu hiện tại (giới hạn 3 lần) - Nếu nhập sai quá 3 lần, hệ thống tạm khóa bàn phím hoặc tài khoản trong 5 phút và gửi thông báo đến User/Admin A2: Mật khẩu không hợp lệ - Nếu mật khẩu không đáp ứng yêu cầu (quá ngắn, trùng mật khẩu cũ), hệ thống yêu cầu nhập lại mật khẩu mới A3: Mất kết nối Wi-Fi (nếu dùng website/ứng dụng) - Hệ thống lưu trữ mật khẩu cục bộ và đồng bộ khi Wi-Fi khôi phục - User có thể tạo mật khẩu qua bàn phím số thay thế A4: Mất điện - Hệ thống chuyển sang chế độ pin dự phòng - User có thể tạo mật khẩu qua bàn phím số
Pre-conditions	1. Hệ thống khóa cửa đã được cài đặt với bàn phím số hoặc kết nối với website/ứng dụng 2. User đã được cấp quyền truy cập để tạo hoặc chỉnh sửa mật khẩu 3. Kết nối Wifi ổn định (nếu tạo mật khẩu qua website/ứng dụng) 4. Hệ thống có cơ chế xác thực 2 bước (nếu được kích hoạt)
Post-conditions	1. Mật khẩu số mới được tạo và lưu trữ thành công 2. Lịch sử tạo/chỉnh sửa mật khẩu được ghi lại trong cơ sở dữ liệu 3. Thông báo xác nhận được gửi đến User (nếu có Wi-Fi) 4. Hệ thống trở về trạng thái chờ

2.5 Use-case: Tạo mật khẩu số thông qua Internet (qua website)

Use case Name	Tạo mật khẩu số thông qua Internet
Brief description	User sử dụng giao diện website/ứng dụng để tự tạo hoặc chỉnh sửa mật khẩu số cho hệ thống khóa cửa, đảm bảo tính bảo mật và linh hoạt
Actors	User: Người sử dụng hệ thống, có quyền tạo hoặc thay đổi mật khẩu số của mình Admin: Người quản lý hệ thống, có quyền tạo hoặc chỉnh sửa mật khẩu số cho nhiều User Hệ thống AI: Xác thực quyền truy cập của User trước khi cho phép tạo mật khẩu (nếu tích hợp xác thực 2 bước)
Basic Flow	1. Bắt đầu: User truy cập website SDLS qua trình duyệt. 2. Đăng nhập: - User nhập thông tin đăng nhập (tên đăng nhập, mật khẩu) - Nếu xác thực 2 bước được kích hoạt, hệ thống gửi mã OTP qua email hoặc SMS, và User nhập mã OTP để xác thực 3. Yêu cầu tạo mật khẩu: - User chọn tùy chọn "Tạo mật khẩu mới" trên giao diện website - User nhập mật khẩu số mới (ví dụ: 4-8 chữ số) hoặc chọn tùy chọn "Tạo mật khẩu tự động" để hệ thống AI tạo mật khẩu ngẫu nhiên

	- User xác nhận lại mật khẩu (nếu nhập thủ công) 4. Kiểm tra và lưu mật khẩu: - Hệ thống kiểm tra tính hợp lệ của mật khẩu (độ dài, không trùng với mật khẩu cũ) - Mật khẩu được lưu vào cơ sở dữ liệu đám mây và đồng bộ với khóa cửa qua giao thức MQTT - Hệ thống ghi lại lịch sử tạo/chỉnh sửa mật khẩu 5. Thông báo: - Hệ thống gửi thông báo xác nhận tạo mật khẩu thành công qua website và/hoặc email/SMS đến User - Nếu User tạo mật khẩu, thông báo cũng được gửi đến Admin 6. Kết thúc: Hệ thống trở về trạng thái chờ
Alternative Flows	A1: Đăng nhập hoặc xác thực 2 bước thất bại - Hệ thống từ chối yêu cầu tạo mật khẩu - User được yêu cầu nhập lại thông tin đăng nhập hoặc mã OTP (giới hạn 3 lần) - Nếu nhập sai quá 3 lần, hệ thống tạm khóa tài khoản trong 5 phút và gửi thông báo đến Admin A2: Mật khẩu không hợp lệ - Nếu mật khẩu không đáp ứng yêu cầu (quá ngắn, trùng mật khẩu cũ), hệ thống yêu cầu User nhập lại hoặc tạo mật khẩu tự động A3: Mất kết nối Wi-Fi - Hệ thống thông báo lỗi kết nối đến User - Mật khẩu được lưu trữ tạm thời trên website và đồng bộ khi kết nối Wi-Fi được khôi phục - User được khuyến nghị sử dụng bàn phím số để tạo mật khẩu thủ công A4: Lỗi hệ thống từ xa - Nếu lệnh tạo mật khẩu không được thực thi, hệ thống gửi thông báo lỗi đến User và đề xuất thử lại
Pre-conditions	1. Hệ thống khóa cửa đã được kết nối với Wifi ổn định 2. User đã đăng ký tài khoản và được cấp quyền truy cập trên website SDLS 3. Hệ thống hỗ trợ xác thực 2 bước (nếu được kích hoạt) 4. Thiết bị của User (máy tính, điện thoại) có kết nối Internet. 5. Cơ sở dữ liệu đám mây được cấu hình để lưu trữ và đồng bộ mật khẩu
Post-conditions	1. Mật khẩu số mới được tạo và lưu trữ thành công trong cơ sở dữ liệu đám mây và đồng bộ với khóa cửa. 2. Lịch sử tạo/chỉnh sửa mật khẩu được ghi lại. 3. Thông báo xác nhận được gửi đến User qua website, email hoặc SMS. 4. Hệ thống trở về trạng thái chờ.

2.6 Use-case: Còi báo động khi bị tác động lực mạnh

Use case Name	Còi báo động khi bị tác động lực mạnh
Brief description	Hệ thống khóa cửa thông minh kích hoạt còi báo động khi phát hiện tác động lực mạnh (ví dụ: cố ý phá khóa hoặc va đập mạnh), đồng thời gửi thông báo đến User để đảm bảo an toàn.
Actors	User: Người sử dụng hệ thống, nhận thông báo và theo dõi lịch sử báo động Admin: Người quản lý hệ thống, nhận thông báo và theo dõi lịch sử báo động
Basic Flow	1. Bắt đầu: Hệ thống AI liên tục giám sát tín hiệu từ cảm biến rung hoặc gia tốc trên khóa cửa 2. Phát hiện tác động lực mạnh: - Cảm biến ghi nhận lực tác động vượt ngưỡng cấu hình (ví dụ: rung mạnh, va đập)

	- Hệ thống AI xác định đây là hành vi bất thường (có thể là cố ý phá khóa) 3. Kích hoạt còi báo động: - Hệ thống kích hoạt còi báo động với âm lượng lớn (ví dụ: ≥80 dB) để cảnh báo tại chỗ - Còi kêu liên tục trong khoảng thời gian được cấu hình (ví dụ: 30 giây) 4. Gửi thông báo: - Hệ thống gửi thông báo khẩn cấp đến User qua website, ứng dụng, email hoặc SMS (nếu có kết nối Wi-Fi) - Thông báo bao gồm thời gian, vị trí (nếu có GPS), và chi tiết sự kiện 5. Ghi lịch sử: - Hệ thống ghi lại sự kiện báo động (thời gian, mức độ tác động) vào cơ sở dữ liệu cục bộ hoặc đám mây 6. Kết thúc: - Còi báo động tắt sau thời gian cấu hình hoặc khi User tắt thủ công - Hệ thống trở về trạng thái giám sát bình thường
Alternative Flows	A1: Tác động lực không vượt ngưỡng - Nếu cảm biến ghi nhận tác động nhưng không đủ mạnh (dưới ngưỡng cấu hình), hệ thống không kích hoạt còi mà chỉ ghi lại sự kiện vào lịch sử (để phân tích hành vi bất thường sau này) A2: Mất kết nối Wi-Fi - Hệ thống vẫn kích hoạt còi báo động tại chỗ - Thông báo được lưu trữ cục bộ và đồng bộ với website/ứng dụng khi Wi-Fi được khôi phục A3: Mất điện - Hệ thống chuyển sang chế độ pin dự phòng - Còi báo động và cảm biến rung vẫn hoạt động bình thường A4: User tắt còi thủ công - User sử dụng mã quản lý (code) trên bàn phím số hoặc website/ứng dụng để tắt còi - Hệ thống ghi lại hành động tắt còi vào lịch sử
Pre-conditions	1. Hệ thống khóa cửa đã được cài đặt với cảm biến rung hoặc gia tốc để phát hiện tác động lực mạnh 2. Còi báo động được tích hợp và hoạt động bình thường 3. Hệ thống được kết nối với nguồn điện hoặc pin dự phòng 4. Kết nối Wifi ổn định (nếu sử dụng thông báo qua website/ứng dụng) 5. Ngưỡng tác động lực mạnh (độ rung, gia tốc) đã được cấu hình trong hệ thống
Post-conditions	1. Còi báo động được kích hoạt và tắt đúng theo cấu hình hoặc yêu cầu 2. Thông báo khẩn cấp được gửi đến User (nếu có kết nối Wi-Fi) 3. Lịch sử sự kiện báo động được ghi lại trong cơ sở dữ liệu (cục bộ hoặc đám mây) 4. Hệ thống trở về trạng thái giám sát bình thường

2.7 Use-case: Bảo mật xác thực 2 bước

Use case Name	Bảo mật xác thực 2 bước
Brief description	Hệ thống yêu cầu User thực hiện xác thực hai bước (2FA) khi thực hiện các hành động nhạy cảm như mở/đóng cửa qua Internet, tạo mật khẩu, hoặc quản lý hệ thống, nhằm tăng cường bảo mật
Actors	User: Người sử dụng hệ thống, cần xác thực hai bước để thực hiện các hành động nhạy cảm qua website/ứng dụng
Basic Flow	1. Bắt đầu: User truy cập website hoặc ứng dụng SDLS để thực hiện hành động nhạy cảm (ví dụ: mở/đóng cửa qua Internet, tạo mật khẩu mới, hoặc thay đổi cấu hình)

	2. Đăng nhập bước 1: - User nhập thông tin đăng nhập (tên đăng nhập và mật khẩu) - Hệ thống kiểm tra thông tin đăng nhập, nếu đúng thì chuyển sang bước xác thực thứ hai 3. Gửi mã OTP: - Hệ thống AI tạo mã OTP ngẫu nhiên (ví dụ: chuỗi 6 chữ số, có hiệu lực trong 5 phút) - Mã OTP được gửi đến email hoặc số điện thoại đã đăng ký của User qua giao thức SMTP (email) hoặc SMS API 4. Xác thực bước 2: - User nhập mã OTP vào giao diện website/ứng dụng. - Hệ thống kiểm tra tính hợp lệ của mã OTP: - Nếu mã OTP đúng, hệ thống cho phép thực hiện hành động nhạy cảm - Nếu mã OTP sai, hệ thống yêu cầu nhập lại (giới hạn 3 lần) 5. Ghi lịch sử: - Hệ thống ghi lại sự kiện xác thực 2 bước (thành công hoặc thất bại) vào cơ sở dữ liệu đám mây 6. Thông báo: - Hệ thống gửi thông báo xác nhận xác thực thành công đến User qua website/ứng dụng - Nếu hành động nhạy cảm được thực hiện bởi User, thông báo cũng được gửi đến Admin 7. Kết thúc: Hệ thống cho phép hành động nhạy cảm được thực hiện và trở về trạng thái chờ
Alternative Flows	A1: Nhập sai mã OTP - Nếu User nhập sai mã OTP quá 3 lần, hệ thống tạm khóa tài khoản trong 5 phút và gửi thông báo đến Admin. - User có thể yêu cầu gửi lại mã OTP mới (giới hạn 3 lần gửi lại trong 10 phút) A2: Mất kết nối Wi-Fi - Hệ thống thông báo lỗi kết nối đến User. - Hành động nhạy cảm bị tạm hoãn, User được khuyến nghị sử dụng phương pháp xác thực thay thế (như mật khẩu số thủ công hoặc chìa khóa cơ học) A3: Mã OTP hết hạn - Nếu mã OTP không được nhập trong thời gian hiệu lực (5 phút), hệ thống yêu cầu User yêu cầu gửi mã OTP mới A4: Phát hiện truy cập bất thường - Nếu hệ thống AI phát hiện nhiều lần xác thực thất bại hoặc hành vi bất thường (ví dụ: đăng nhập từ thiết bị lạ), hệ thống tạm khóa tài khoản và gửi thông báo khẩn cấp đến Admin
Pre-conditions	1. Hệ thống khóa cửa đã được kết nối với Wifi ổn định để gửi/nhận thông báo OTP 2. User đã đăng ký tài khoản trên website/ứng dụng SDLS và cung cấp thông tin liên hệ (email hoặc số điện thoại) để nhận OTP 3. Hệ thống hỗ trợ giao thức gửi OTP (qua email hoặc SMS) được cấu hình sẵn 4. Thiết bị của User (máy tính, điện thoại) có kết nối Internet 5. Hệ thống đã được kích hoạt tính năng xác thực 2 bước trong cấu hình
Post-conditions	1. Xác thực 2 bước hoàn tất thành công, cho phép User thực hiện hành động nhạy cảm 2. Lịch sử xác thực được ghi lại trong cơ sở dữ liệu đám mây 3. Thông báo xác nhận được gửi đến User qua website, ứng dụng, email hoặc SMS 4. Hệ thống trở về trạng thái chờ

2.8 Use-case: LCD instruct người dùng Setup device khi khởi động lần đầu/sau khi reset

Use case Name	LCD instruct người dùng Setup device khi khởi động lần đầu/sau khi reset
Brief description	Hệ thống sử dụng màn hình LCD tích hợp để hướng dẫn User thực hiện các bước thiết lập ban đầu (như cấu hình Wifi, tạo mật khẩu, hoặc đăng ký khuôn mặt) khi khởi động lần đầu hoặc sau khi reset thiết bị, đảm bảo dễ sử dụng và vận hành ngay cả khi không có kết nối Internet
Actors	User: Người sử dụng hệ thống, thực hiện thiết lập ban đầu hoặc sau khi reset
Basic Flow	1. Bắt đầu: Hệ thống khởi động lần đầu hoặc được reset, màn hình LCD hiển thị thông báo chào mừng và hướng dẫn thiết lập ban đầu 2. Hiển thị hướng dẫn trên LCD: - LCD hiển thị các bước thiết lập, ví dụ: "Chọn ngôn ngữ", "Nhập mã quản lý mặc định", "Cấu hình Wi-Fi", "Tạo mật khẩu", "Đăng ký khuôn mặt" - User sử dụng bàn phím số để điều hướng và chọn các tùy chọn 3. Nhập mã quản lý mặc định: - User nhập mã quản lý mặc định (ví dụ: 0000) được cung cấp bởi nhà sản xuất - Hệ thống xác thực mã, nếu đúng thì cho phép tiếp tục thiết lập 4. Cấu hình Wifi (nếu có): - LCD hiển thị hướng dẫn nhập SSID và mật khẩu Wifi - User nhập thông tin Wifi qua bàn phím số - Hệ thống thử kết nối với Wi-Fi và hiển thị trạng thái kết nối (thành công hoặc thất bại) 5. Tạo mật khẩu quản lý mới: - LCD yêu cầu User nhập mật khẩu số mới (4-8 chữ số) và xác nhận lại - Hệ thống kiểm tra tính hợp lệ của mật khẩu và lưu vào cơ sở dữ liệu cục bộ 6. Đăng ký khuôn mặt (nếu có camera tích hợp): - LCD hướng dẫn User đứng trước camera để đăng ký khuôn mặt - Hệ thống AI quét và lưu dữ liệu khuôn mặt vào cơ sở dữ liệu 7. Hoàn tất thiết lập: - LCD hiển thị thông báo "Thiết lập hoàn tất" và hướng dẫn sử dụng cơ bản. - Hệ thống ghi lại sự kiện thiết lập vào cơ sở dữ liệu cục bộ. - Nếu có kết nối Wi-Fi, hệ thống đồng bộ dữ liệu thiết lập lên đám mây. 8. Kết thúc: Hệ thống chuyển sang trạng thái hoạt động bình thường.
Alternative Flows	A1: Nhập sai mã quản lý mặc định - LCD hiển thị thông báo lỗi và yêu cầu User nhập lại mã (giới hạn 3 lần) - Nếu nhập sai quá 3 lần, hệ thống tạm khóa bàn phím trong 5 phút và hiển thị thông báo trên LCD A2: Kết nối Wifi thất bại - LCD hiển thị thông báo lỗi kết nối và đề xuất thử lại hoặc bỏ qua bước cấu hình Wi-Fi - Hệ thống cho phép thiết lập offline, lưu dữ liệu cục bộ và đồng bộ khi Wi-Fi được kết nối sau này A3: Mật khẩu không hợp lệ - Nếu mật khẩu mới không đáp ứng yêu cầu (quá ngắn, trùng lặp), LCD hiển thị thông báo lỗi và yêu cầu nhập lại A4: Lỗi đăng ký khuôn mặt - Nếu camera không nhận diện được khuôn mặt (do ánh sáng yếu

	hoặc lỗi thiết bị), LCD hiển thị thông báo lỗi và đề xuất thử lại hoặc bỏ qua bước này A5: Mất điện trong quá trình thiết lập - Hệ thống chuyển sang chế độ pin dự phòng - LCD tiếp tục hiển thị hướng dẫn, nhưng nếu pin yếu, hệ thống lưu trạng thái thiết lập hiện tại và yêu cầu tiếp tục khi có nguồn điện
Pre-conditions	1. Hệ thống khóa cửa đã được cài đặt với màn hình LCD và bàn phím số hoạt động bình thường 2. Thiết bị đang ở trạng thái khởi động lần đầu hoặc vừa được reset về cài đặt gốc 3. Hệ thống được cung cấp nguồn điện hoặc pin dự phòng 4. User có thông tin cần thiết (như SSID/mật khẩu Wifi, mã quản lý mặc định) để thực hiện thiết lập
Post-conditions	1. Thiết bị được thiết lập thành công với các thông số như Wi-Fi, mật khẩu mới, và dữ liệu khuôn mặt (nếu có). 2. Lịch sử thiết lập được ghi lại trong cơ sở dữ liệu cục bộ hoặc đồng bộ lên đám mây (nếu có Wi-Fi). 3. LCD hiển thị trạng thái sẵn sàng và hệ thống chuyển sang chế độ hoạt động bình thường

2.9 Use-case: System gửi lịch sử mở cửa, thông báo thay đổi mật khẩu về điện thoại

Use case Name	System gửi lịch sử mở cửa, thông báo thay đổi mật khẩu về điện thoại
Brief description	Hệ thống gửi thông báo về lịch sử mở/đóng cửa và các thay đổi mật khẩu đến điện thoại của User hoặc Admin qua ứng dụng di động, email, hoặc SMS, đảm bảo người dùng được cập nhật kịp thời và tăng cường bảo mật
Actors	User: Người sử dụng hệ thống, nhận thông báo về lịch sử mở/đóng cửa và thay đổi mật khẩu Admin: Người quản lý hệ thống, nhận thông báo về tất cả các sự kiện mở/đóng cửa và thay đổi mật khẩu từ User
Basic Flow	1. Bắt đầu: Hệ thống ghi nhận sự kiện mở/đóng cửa hoặc thay đổi mật khẩu (thủ công, tự động, hoặc qua Internet) 2. Ghi lịch sử sự kiện: - Hệ thống AI lưu thông tin sự kiện (thời gian, loại sự kiện, danh tính User nếu có, phương thức xác thực) vào cơ sở dữ liệu cục bộ và đồng bộ lên đám mây (nếu có Wi-Fi) 3. Tạo thông báo: - Hệ thống AI tạo nội dung thông báo, ví dụ: - Lịch sử mở cửa: "Cửa được mở lúc 10:30 AM, ngày 31/05/2025, bởi [User/Khuôn mặt/Mật khẩu]." - Thay đổi mật khẩu: "Mật khẩu mới được tạo lúc 10:35 AM, ngày 31/05/2025, bởi [User/Admin]." 4. Gửi thông báo: - Hệ thống gửi thông báo đến điện thoại của User/Admin qua: - Push notification trên ứng dụng SDLS - Email thông qua giao thức SMTP - SMS thông qua API SMS (nếu được cấu hình) - Thông báo bao gồm chi tiết sự kiện và thời gian xảy ra 5. Xác nhận gửi: - Hệ thống ghi lại trạng thái gửi thông báo (thành công hoặc thất bại) vào cơ sở dữ liệu 6. Kết thúc: Hệ thống trở về trạng thái chờ, tiếp tục giám sát các sự kiện tiếp theo
Alternative Flows	A1: Mất kết nối Wi-Fi - Hệ thống lưu trữ thông báo cục bộ trong cơ sở dữ liệu

	- Khi Wi-Fi được khôi phục, hệ thống đồng bộ và gửi tất cả thông báo chưa gửi đến User A2: Lỗi gửi thông báo - Nếu gửi thông báo qua ứng dụng, email, hoặc SMS thất bại (do lỗi API hoặc cấu hình), hệ thống thử lại tối đa 3 lần - Nếu vẫn thất bại, hệ thống ghi lại lỗi và thông báo cho Admin qua kênh liên lạc thay thế (nếu có) A3: User tắt thông báo - User/Admin có thể tắt một số loại thông báo (ví dụ: chỉ nhận thông báo thay đổi mật khẩu) qua cài đặt trên ứng dụng SDLS - Hệ thống vẫn ghi lại tất cả sự kiện vào cơ sở dữ liệu nhưng không gửi thông báo cho các loại bị tắt A4: Phát hiện sự kiện bất thường - Nếu hệ thống AI phát hiện sự kiện bất thường (ví dụ: nhiều lần mở cửa thất bại hoặc thay đổi mật khẩu từ thiết bị lạ), thông báo được gửi kèm nhãn "Khẩn cấp" để cảnh báo User
Pre-conditions	1. Hệ thống khóa cửa đã được kết nối với Wi-Fi ổn định để gửi thông báo 2. User đã đăng ký tài khoản trên ứng dụng SDLS hoặc cung cấp email/số điện thoại để nhận thông báo 3. Hệ thống hỗ trợ giao thức gửi thông báo qua ứng dụng (push notification), email (SMTP), hoặc SMS (API) 4. Thiết bị di động của User có cài đặt ứng dụng SDLS hoặc có thể nhận email/SMS 5. Hệ thống đã được cấu hình để ghi lại lịch sử mở/đóng cửa và các sự kiện thay đổi mật khẩu
Post-conditions	1. Thông báo về lịch sử mở/đóng cửa hoặc thay đổi mật khẩu được gửi thành công đến điện thoại của User 2. Lịch sử sự kiện được ghi lại trong cơ sở dữ liệu cục bộ hoặc đám mây 3. Hệ thống trở về trạng thái chờ, sẵn sàng ghi nhận và gửi thông báo cho các sự kiện tiếp theo

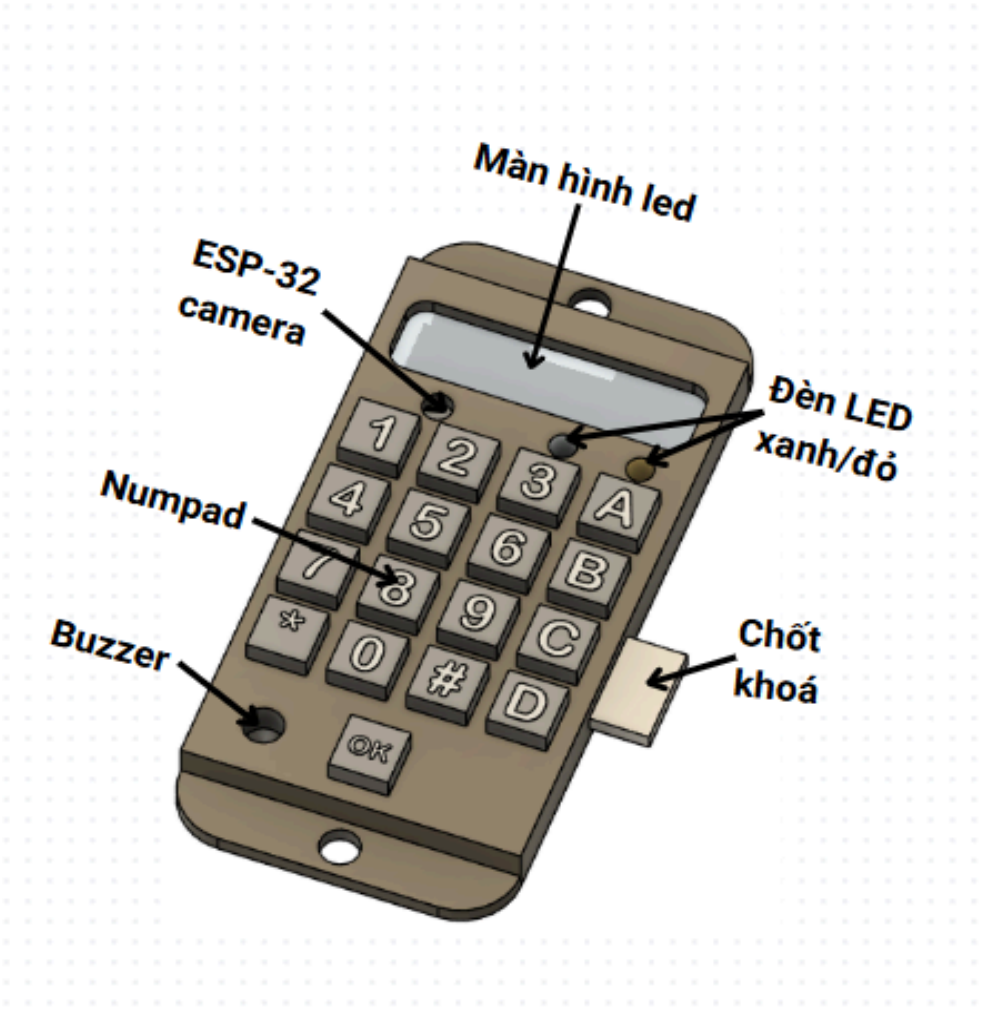
IV. Danh sách thiết bị

Budget list					
STT	**Tên sản phẩm**	**Đơn giá**	**Số lượng**	**Link**	**Chức năng**
1	Màn Hình LCD Text LCD2004 Xanh Lá	28,000	1	link	Màn hình dùng để tương tác với người dùng
2	Bàn Phím Ma Trận Nhựa mềm 4x4 Keypad	12,000	1	link	Thiết bị dùng để input mật khẩu
3	Mạch 1 Nút Nhấn Tact Switch 12x12mm	6,000	1	link	Thiết bị input để xác nhận mật khẩu
4	Kit phát triển Wifi BLE ESP32 Camera ESP32-CAM Development Board Ai-Thinker	225,000	1	link	Để triển khai tính năng Face Recognition
5	Còi Buzzer báo động 5VDC	3,000	1	link	Báo hiệu có trộm đang bẻ khoá.

6	Bộ 140 Dây Cắm Breadboard Nhiều Kích Cỡ (Pre-Formed Jumper Wire Kit)	25,000	1	link	Dùng để kết nối mạch điện với thiết bị.
7	Breadboard MB-102 400 lỗ 85x55x10mm	16,000	1	link	Dùng để kết nối mạch điện với thiết bị.
8	Bộ 3 loại LED màu 5mm thông dụng (3 kind 5mm Color Led)	9,000	1	link	Dùng để trang bị đèn LED, kiểm lỗi cho sản phẩm
9	Cảm biến âm thanh tích hợp AGC MAX9814 Microphone Amplifier Module	55,000	1	link	Xác thực giọng nói
10	Động cơ RC Servo 9G 360°	27,000	1	link	Dùng để đóng mở chốt khoá của thiết bị.
11	Cảm biến rung Piezoelectric Ceramic Vibration Sensor V2	35,000	1	Link	Phát hiện rung, chấn động, hoặc tác động lực mạnh lên cửa
12	Mạch chuyển USB UART CP2102 Mini	37,000	1	Link	Dùng để nạp code cho ESP32-cam
13	Kit phát triển Wifi BLE SoC ESP32 S3 WeAct ESP32-S3-B N16R8 (Espressif DevKitC-1 Compatible)	195,000	1	Link	Dùng để xử lý tín hiệu từ sensor và thực thi các decision logic cho actuator như buzzer, lcd hay servo
14	Nguồn Power Adaptor AC-DC 12V 1A OEM	50,000	1	Link	Cấp nguồn cho thiết bị
15	Chi phí phát sinh	50,000			
	Tổng tiền	773,000			

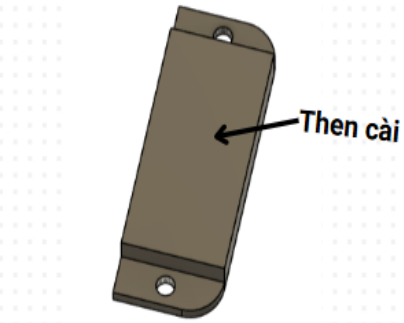
V. Bản vẽ thiết kế (Prototype)

Thiết kế bên ngoài của ổ khoá



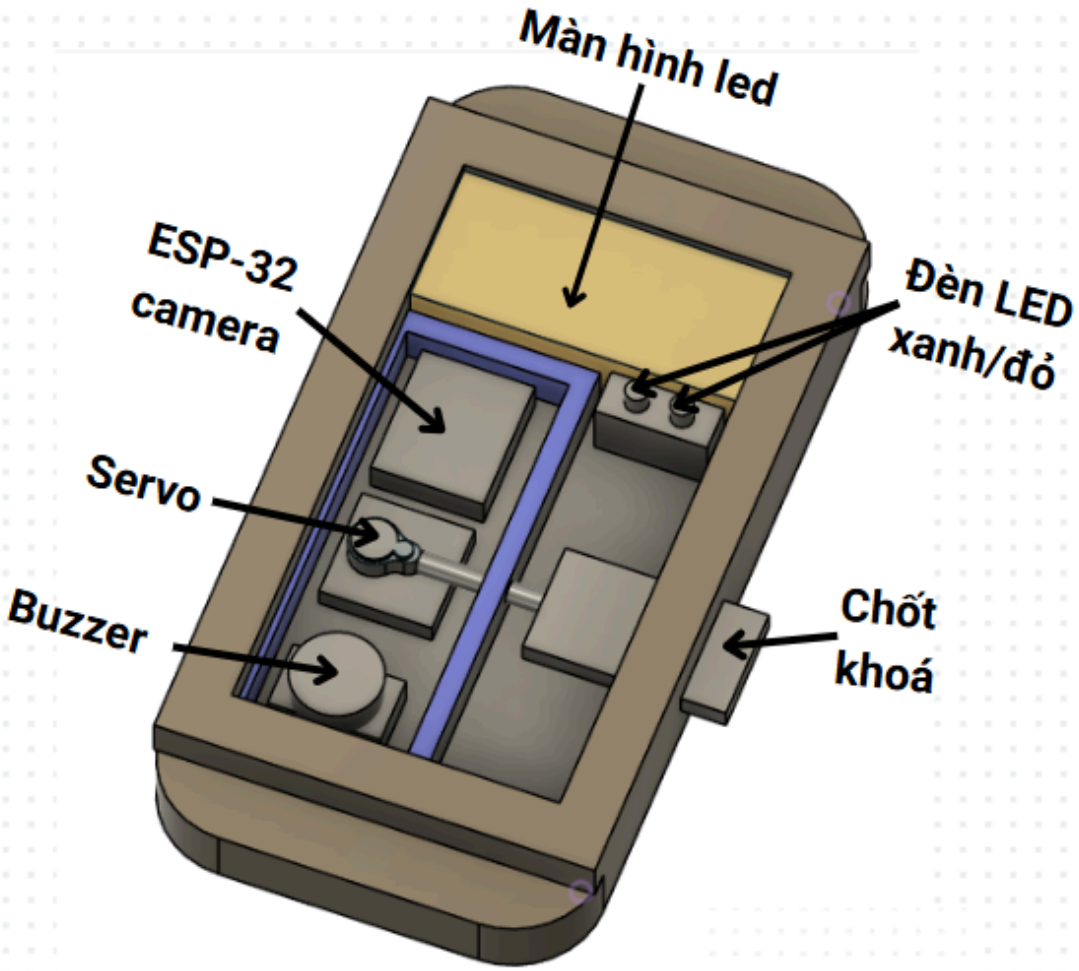
S

Hình 1: Hình dạng bên ngoài của thiết bị



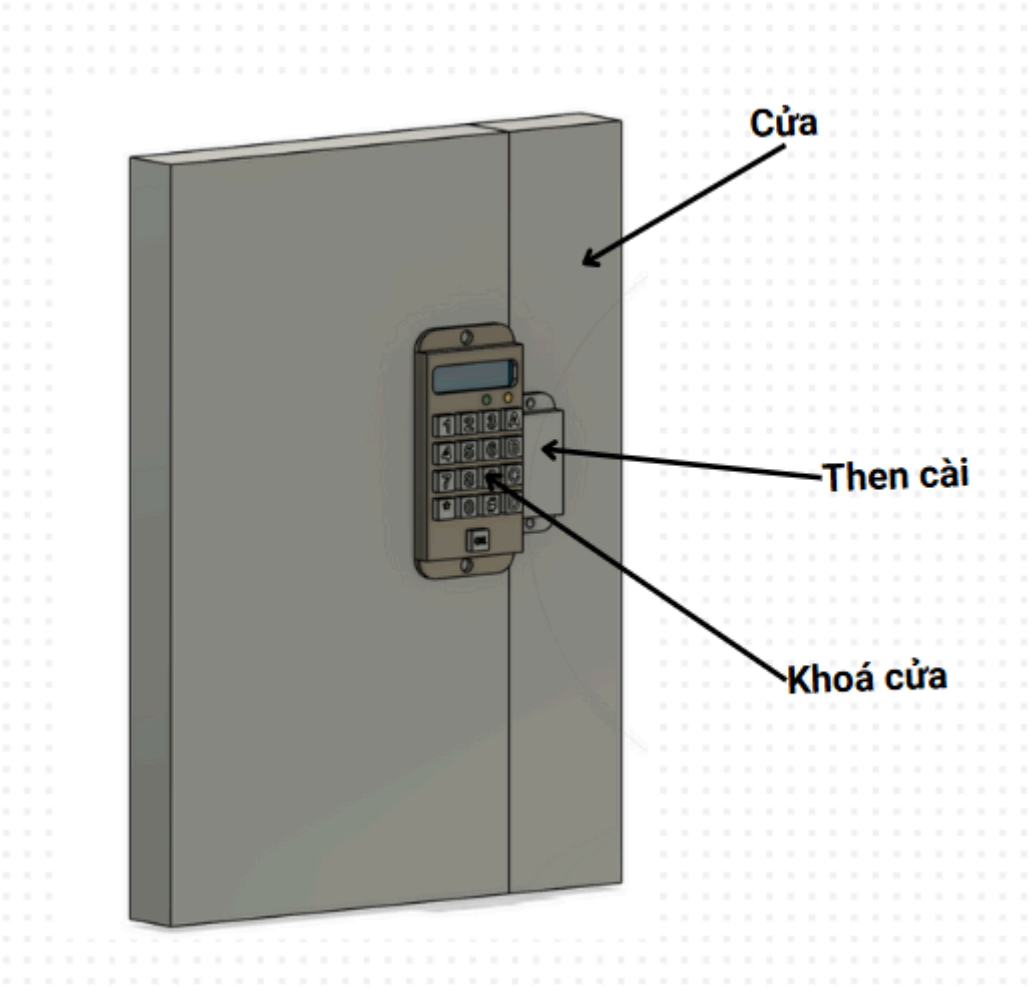
Hình 2: Then cài đi kèm với ổ khoá để khoá cửa

Kiến trúc bên trong của ổ khoá



Hình 3: Thiết kế bên trong của thiết bị

Ứng dụng của sản phẩm vào thực tiễn



Hình 4: Ổ khoá khi được gắn trên cửa

VI. Kế hoạch triển khai

Dự án Hệ thống Khóa Cửa Thông Minh (SDLS) được triển khai trong 10 tuần, chia thành 5 giai đoạn chính, từ lên ý tưởng, thiết kế, phát triển, tích hợp, đến kiểm thử và hoàn thiện. Kế hoạch đảm bảo tính khả thi, hiệu quả cho đồ án môn AIOT, đáp ứng các mục tiêu định lượng và mang lại sản phẩm thực tế.

Giai đoạn	Nhiệm vụ chính	Kết quả mong đợi	Start date	End date	Phân công
1. Lên ý tưởng và phân tích yêu cầu	Nghiên cứu nhu cầu khóa thông minh, AI/IoT. - Phân tích công nghệ phù hợp. - Xác định yêu cầu kỹ thuật và bảo mật.	Báo cáo yêu cầu hệ thống - Danh sách công nghệ sơ bộ - Kế hoạch phát triển ban đầu	17/05/2025	24/05/2025	- **Gia Bảo**: Phân tích use-case - **Quang Sáng**: Nghiên cứu AI/IoT - **Minh Đăng**: Tổng hợp yêu cầu kỹ thuật - **Công Tuấn**: Viết báo cáo tổng hợp
2. Thiết kế hệ thống	Chọn phần cứng và nền tảng phần mềm - Thiết kế sơ đồ hệ thống & luồng dữ liệu - Phác thảo giao diện người dùng	Danh sách phần cứng/phần mềm - Sơ đồ hệ thống chi tiết - Giao diện người dùng sơ bộ	25/05/2025	31/05/2025	- **Quang Sáng**: Thiết kế sơ đồ hệ thống - **Công Tuấn**: Chọn phần cứng - **Minh Đăng**: Thiết kế giao diện - **Gia Bảo**: Kiểm tra tổng thể
3. Phát triển hệ thống	Xây dựng mô-đun nhận diện khuôn mặt - Tích hợp điều khiển từ xa qua web/app - Phát triển giao diện người dùng	Mô-đun nhận diện hoạt động - Mở khóa từ xa qua MQTT - Giao diện hoạt động bản beta	01/06/2025	28/06/2025	- **Gia Bảo**: Xây dựng nhận diện khuôn mặt - **Quang Sáng**: Tích hợp MQTT + mở khóa từ xa - **Minh Đăng**: Thiết kế UI/UX web - **Công Tuấn**: Phát triển app & Firebase
4. Tích hợp và tối ưu	Tích hợp chế độ offline - Kết nối cảnh báo an ninh (buzzer, rung) - Tối ưu hiệu suất hệ thống	Chế độ offline ổn định - Cảnh báo hoạt động tốt - Báo cáo hiệu suất sơ bộ	29/06/2025	12/07/2025	- **Công Tuấn**: Logic offline & cảnh báo - **Gia Bảo**: Tích hợp toàn bộ hệ thống - **Minh Đăng**: Tối ưu UI/UX - **Quang Sáng**: Kiểm thử tích hợp

5. Kiểm thử và hoàn thiện	Thử nghiệm thực tế (nhiều điều kiện) - Tinh chỉnh giao diện, sửa lỗi - Hoàn tất báo cáo và tài liệu hướng dẫn	Hệ thống hoàn thiện - Báo cáo, hướng dẫn đầy đủ	13/07/2025	27/07/2025	- **Quang Sáng**: Kiểm thử tính năng - **Gia Bảo**: Xử lý lỗi logic - **Công Tuấn**: Viết tài liệu hướng dẫn - **Minh Đăng**: Hoàn thiện báo cáo trình bày

Đánh giá tổng thể về khả năng thành công của kế hoạch:

Tiêu chí	Tỷ lệ thành công ước tính
Thiết kế & phân tích yêu cầu	100% – đã hoàn thành rõ ràng
Thiết kế hệ thống phần cứng/mềm	95% – linh kiện phổ biến, đã xác định đầy đủ
Phát triển tính năng cốt lõi	90% – đã có mô-đun AI tham khảo, khả thi
Tích hợp & tối ưu	85% – cần phối hợp nhiều phần nhưng đã dự trù giải pháp
Kiểm thử & hoàn thiện	90% – có kế hoạch kiểm thử rõ và phân công cụ thể

VII. Tài liệu tham khảo

[1] P. Elechi, E. Okowa, and U. Ekwueme, *Facial Recognition Based Smart Door Lock System*, Department of Electrical/Electronic Engineering, Rivers State University, Nigeria.

[2] S. M. Siam, H. Ahn, L. Liu, S. Alam, H. Shen, Z. Cao, N. B. Shroff, B. Krishnamachari, M. Srivastava, and M. Zhang, "Artificial Intelligence of Things: A Survey," *arXiv preprint arXiv:2410.19998*, Oct. 2024.

[3] F. Mehta, *Face Recognition and Security System*, GitHub repository, [Online]. Available: https://github.com/fenilgmehta/Face-Recognition-and-Security-System

[4] Ars Futura, *Smart Lock*, GitHub repository, [Online]. Available: https://github.com/arsfutura/smart-lock

[5] B. Malbusca, *Facial Recognition RMSF*, GitHub repository, [Online]. Available: https://github.com/bmalbusca/FacialRecognition_RMSF