1. Introduction (Giới thiệu)

Tài liệu này được xây dựng nhằm mô tả các yêu cầu phần mềm và hệ thống cho dự án IOT-Smart-Doorlock-with-RFID-and-OTP-using-ESP32. Mục tiêu chính là định nghĩa rõ ràng các chức năng, đặc điểm kỹ thuật, ràng buộc và phạm vi của hệ thống, từ đó làm cơ sở cho việc thiết kế, lập trình, kiểm thử và triển khai.

Dự án hướng đến việc nâng cao tính bảo mật và tính tiện dụng của hệ thống khóa cửa truyền thống, thông qua cơ chế xác thực hai lớp.

Hệ thống sẽ cho phép người dùng mở khóa cửa thông qua hai cách:

- Xác thực RFID – quẹt thẻ RFID hợp lệ.
- Xác thực OTP – nhập mã OTP được gửi tới email hoặc ứng dụng di động.
- Xác thực PIN - nhập mã PIN đã được thiết lập từ trước

Nếu một trong ba cách được xác thực, cửa sẽ được điều khiển mở thông qua relay hoặc servo motor, sau đó tự động khóa lại sau một khoảng thời gian.

2. System Features (Các tính năng hệ thống / Functional Requirements)

2.1. Mở khóa bằng RFID

- **Mô tả:** Hệ thống sử dụng module RFID RC522 để đọc thẻ RFID. Nếu thẻ hợp lệ (được admin đăng ký), cửa sẽ mở.
- **Input:** Thẻ RFID đưa gần đầu đọc.
- **Xử lý:** ESP32 đọc UID thẻ, so sánh với danh sách đã lưu.
- **Output:**
    - Nếu hợp lệ → mở khóa.
    - Nếu không hợp lệ → hiển thị lỗi và từ chối truy cập.
- **Điều kiện thành công:** Thẻ đúng, UID khớp.
- **Điều kiện thất bại:** Thẻ không có trong danh sách, lỗi đọc.

2.2. Mở khóa bằng OTP

- **Mô tả:** Người dùng có thể mở khóa bằng cách nhập OTP được gửi qua email/app.
- **Input:** Yêu cầu mở khóa → hệ thống sinh OTP và gửi cho người dùng. Người dùng nhập OTP trên keypad hoặc app.
- **Xử lý:**
    - Sinh OTP ngẫu nhiên.
    - Lưu tạm trong bộ nhớ ESP32.
    - So sánh OTP nhập với OTP lưu, đồng thời kiểm tra thời gian hiệu lực (ví dụ 30 giây).

- **Output:**
    - OTP đúng và còn hạn → mở khóa.
    - OTP sai hoặc hết hạn → từ chối truy cập.

- **Điều kiện thành công:** OTP trùng khớp và trong thời gian hợp lệ.
- **Điều kiện thất bại:** OTP sai, hết hạn, lỗi gửi email.

2.3. Mở khóa bằng PIN

- **Mô tả:** Người dùng có thể mở khóa bằng cách nhập mã PIN cố định trên keypad.
- **Input:** Mã PIN được nhập qua keypad.
- **Xử lý:** So sánh PIN nhập với mã PIN đã lưu trong bộ nhớ hệ thống.
- **Output:**
    - PIN đúng → mở khóa.
    - PIN sai → từ chối, báo lỗi.
- **Điều kiện thành công:** PIN đúng.
- **Điều kiện thất bại:** PIN sai, nhập sai quá số lần cho phép.

2.4. Điều khiển khóa cửa

- **Mô tả:** Sau khi xác thực thành công bằng một trong các phương thức (RFID, OTP, PIN), hệ thống sẽ điều khiển relay hoặc servo motor để mở cửa.
- **Input:** Tín hiệu xác thực thành công.
- **Xử lý:** Xuất tín hiệu đến relay/servo để mở khóa.
- **Output:** Cửa mở, sau thời gian định sẵn (ví dụ 5 giây) tự động khóa lại.
- **Điều kiện thành công:** Relay/servo hoạt động đúng.
- **Điều kiện thất bại:** Lỗi cơ khí, mất nguồn.

2.5. Quản lý admin

- **Mô tả:** Admin có quyền quản lý và cấu hình hệ thống.
- **Chức năng chính:**
    - Thêm/xóa thẻ RFID.
    - Đặt lại/đổi PIN.
    - Cấu hình email để nhận OTP.
    - Reset hệ thống khi cần.
- **Input:** Lệnh từ admin qua serial console hoặc app.
- **Output:** Xác nhận thay đổi thành công hoặc báo lỗi.

2.6. Ghi log và cảnh báo

- **Mô tả:** Hệ thống ghi lại nhật ký truy cập và gửi cảnh báo khi phát hiện hành vi bất thường.
- **Input:** Sự kiện truy cập (RFID, OTP, PIN đúng/sai).
- **Xử lý:**
    - Lưu dữ liệu UID/PIN/OTP, thời gian, trạng thái vào bộ nhớ.

    - Nếu nhập sai nhiều lần → gửi cảnh báo qua email/app.
- **Output:** Nhật ký truy cập và thông báo cảnh báo.

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

3.1. Hiệu năng (Performance Requirements)

- Thời gian xử lý yêu cầu mở khóa không vượt quá 2 giây từ khi người dùng quét thẻ RFID, nhập PIN, hoặc nhập OTP.
- Hệ thống có thể xử lý ít nhất 20 yêu cầu mở khóa liên tiếp/phút mà không bị treo hoặc chậm trễ.
- Dữ liệu OTP sinh ra và gửi đi phải được tạo trong vòng 1 giây.

3.2. Độ tin cậy (Reliability Requirements)

- Hệ thống duy trì hoạt động liên tục với thời gian khả dụng (uptime) ít nhất 99% trong điều kiện hoạt động chuẩn.
- Trong trường hợp mất kết nối Internet, hệ thống vẫn có thể mở khóa bằng RFID và PIN.
- Tự động phục hồi khi mất nguồn: khi có lại nguồn, hệ thống khởi động và hoạt động bình thường trong vòng 30 giây.

3.3. Bảo mật (Security Requirements)

- Mọi dữ liệu OTP và PIN truyền qua Internet phải được mã hóa (ví dụ: TLS/SSL).
- PIN và OTP không được lưu trữ ở dạng văn bản thuần (plain text), mà phải hash hoặc mã hóa.
- Hệ thống khóa tự động sau 3 lần nhập sai liên tiếp, yêu cầu chờ ít nhất 30 giây để thử lại.
- RFID phải sử dụng UID duy nhất, không cho phép thẻ chưa đăng ký mở khóa.

3.4. Tính khả dụng và dễ sử dụng (Usability Requirements)

- Giao diện quản lý (trên web/app) cần dễ hiểu, thao tác trực quan, hỗ trợ tiếng Anh và tiếng Việt.
- Đèn LED và còi báo hiệu trạng thái mở/khóa hoặc lỗi phải hiển thị rõ ràng.
- Người dùng bình thường có thể làm quen với thao tác mở khóa trong < 5 phút.

3.5. Khả năng bảo trì và mở rộng (Maintainability & Scalability)

- Mã nguồn được viết rõ ràng, có chú thích, hỗ trợ cập nhật firmware qua OTA (Over-The-Air).
- Hệ thống hỗ trợ mở rộng để thêm tính năng mới (ví dụ: mở khóa bằng vân tay, camera AI).
- Cấu hình thẻ RFID, PIN, và OTP có thể được cập nhật từ xa thông qua giao diện quản trị.

4. External Interface Requirements (Yêu cầu giao diện ngoài)

4.1. Giao diện người dùng (User Interface)

- **Ứng dụng di động/Web**:
  - Hiển thị trạng thái cửa (mở/đóng).
  - Cho phép nhập OTP để mở khóa.
  - Quản trị viên có thể thêm/xóa thẻ RFID, thay đổi PIN, xem nhật ký truy cập.
  - Hỗ trợ ngôn ngữ: Tiếng Việt, Tiếng Anh.
- **Màn hình LCD/OLED**:
  - Hiển thị hướng dẫn: "Quét thẻ RFID", "Nhập OTP/PIN", "Thành công/Thất bại".
  - Đèn LED và còi báo trạng thái (Xanh = thành công, Đỏ = thất bại, Vàng = đang xử lý).
- **Keypad**: nhập OTP và PIN.

4.2. Giao diện phần cứng (Hardware Interface)

- ESP32 kết nối với:
  - RFID RC522 (SPI/I2C).
  - Relay/Servo motor (GPIO).
  - Keypad (GPIO).
  - LCD/OLED (I2C/SPI).
  - Buzzer + LED (GPIO).
- Nguồn cấp 5V–12V, có pin dự phòng.

4.3. Giao diện phần mềm (Software Interface)

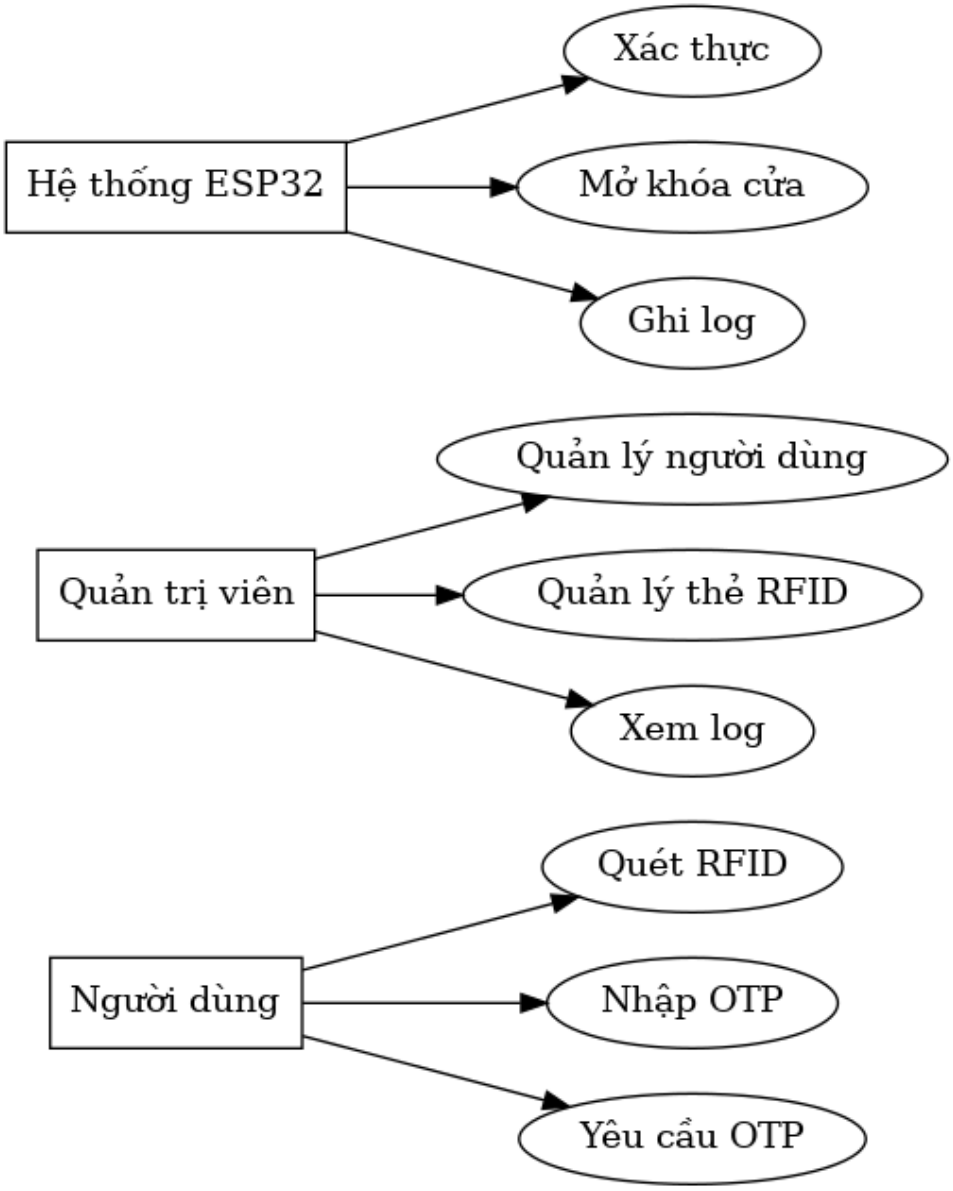
- **Firmware trên ESP32**: Arduino C++, thư viện WiFi, HTTPClient, MFRC522, Keypad, ArduinoJson.
- **Server/Cloud**: Backend (Node.js/Flask/Django), cơ sở dữ liệu MySQL/MongoDB.
- **Ứng dụng di động/Web**: React Native/Flutter/ReactJS, kết nối server qua REST API (HTTPS, JSON).

4.4. Giao diện truyền thông (Communication Interface)

- Wi-Fi 802.11 b/g/n.
- Giao thức HTTP/HTTPS hoặc MQTT giữa ESP32 và server.
- Giao tiếp UART/I2C/SPI/GPIO giữa ESP32 và các module.

5. System Models (Mô hình hệ thống)

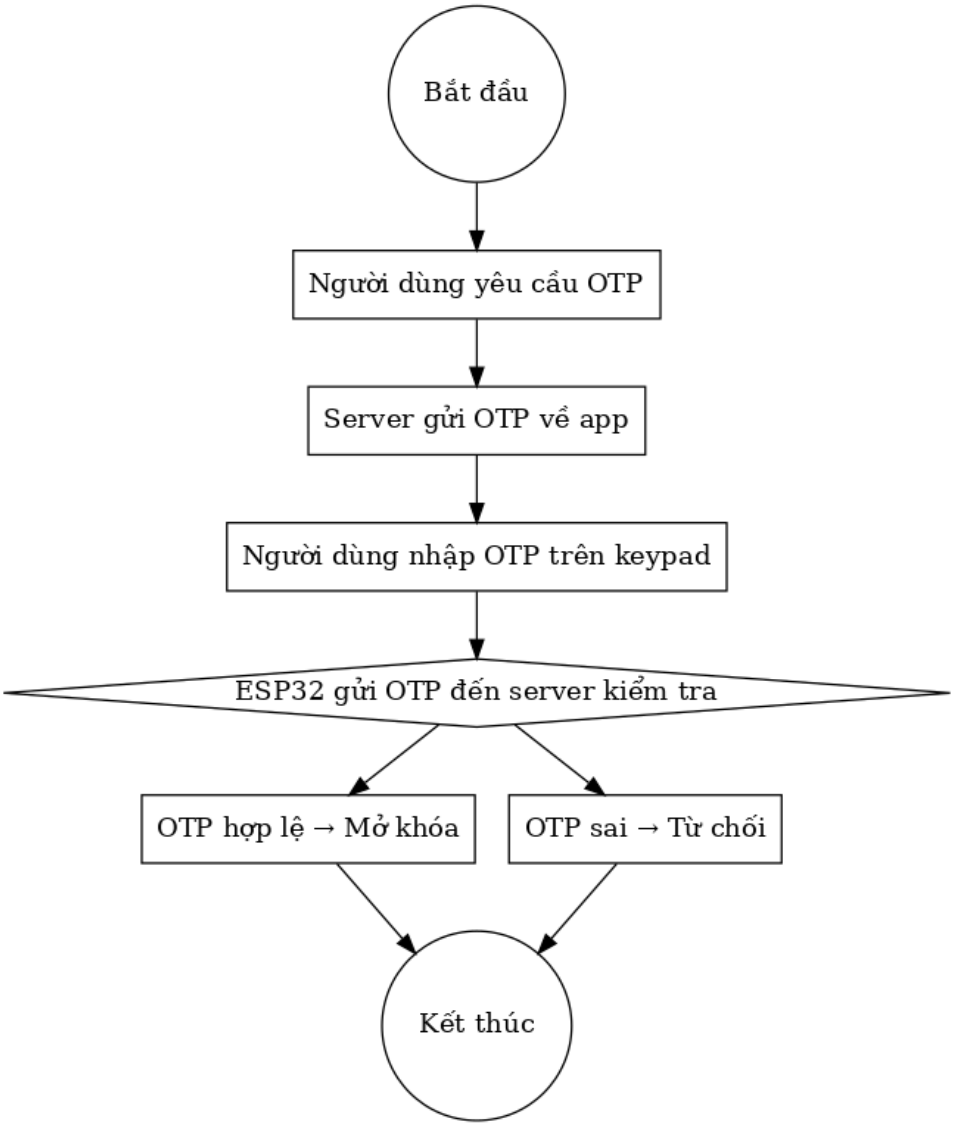
5.1. Use Case Diagram



Tác nhân chính:

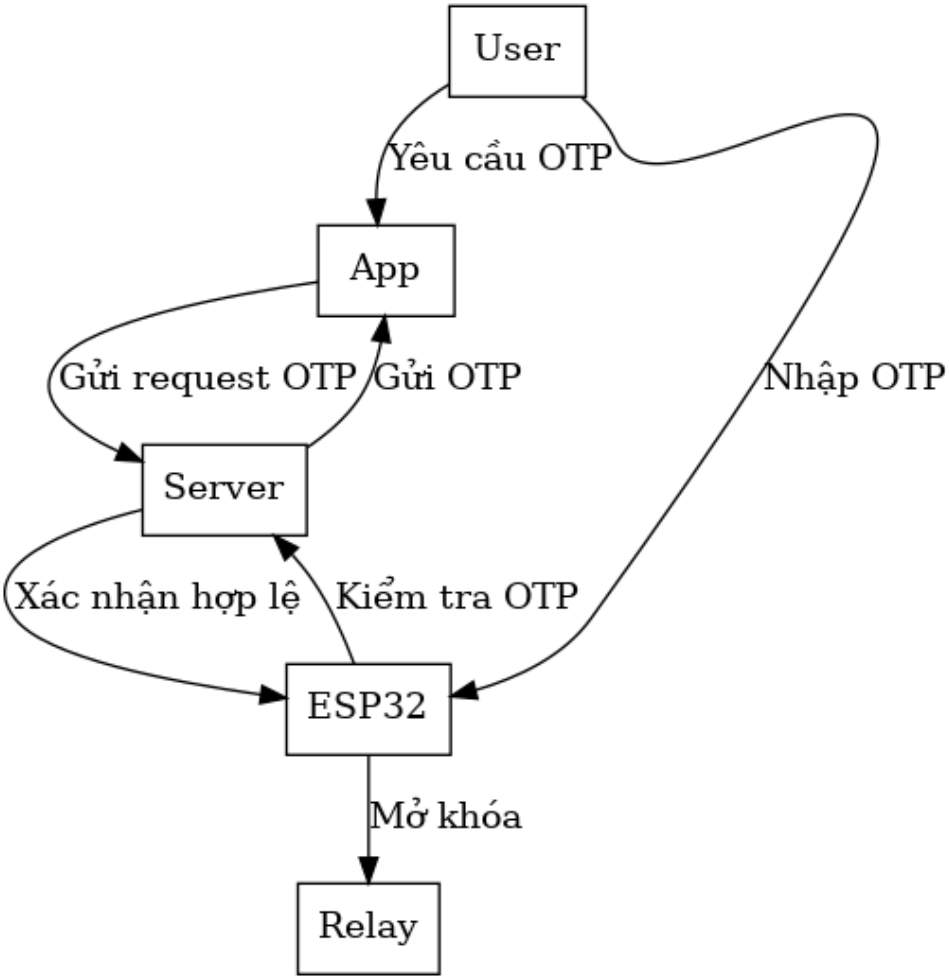
- Người dùng: mở khóa bằng RFID, OTP, PIN.
- Quản trị viên: quản lý thẻ RFID, thay đổi PIN, xem log.
- Hệ thống: xác thực, điều khiển relay, ghi nhật ký.

5.2. Activity Diagram – Quy trình mở khóa bằng OTP



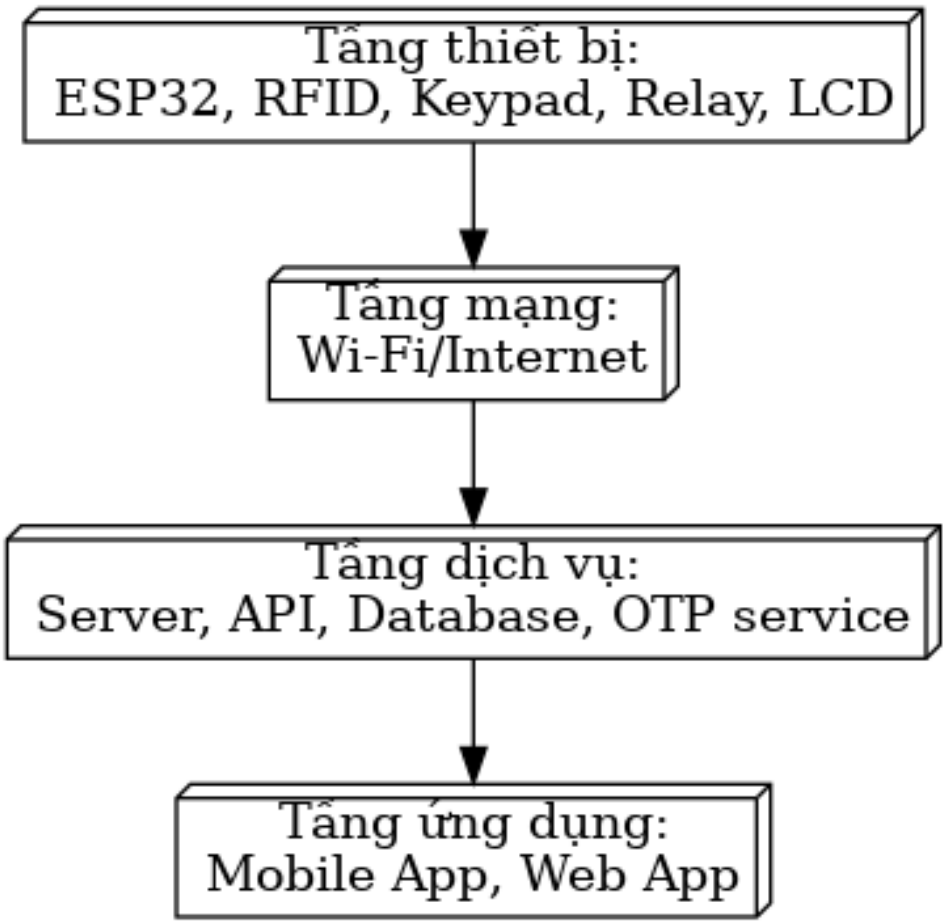
1. Người dùng yêu cầu OTP.
2. Server sinh OTP và gửi về app/email.
3. Người dùng nhập OTP tại keypad.
4. ESP32 gửi OTP lên server để kiểm tra.
5. Nếu đúng và hợp lệ → mở khóa + ghi log.
6. Nếu sai → báo lỗi và từ chối.

5.3. Sequence Diagram – Mở khóa bằng OTP



- Người dùng → App: yêu cầu OTP.
- App → Server: gửi request.
- Server → App: trả về OTP.
- Người dùng → ESP32: nhập OTP.
- ESP32 → Server: xác thực OTP.
- Server → ESP32: trả kết quả.
- ESP32 → Relay: mở khóa nếu hợp lệ.

5.4. Kiến trúc hệ thống



- **Tầng thiết bị**: ESP32, RFID, keypad, relay, LCD, buzzer.
- **Tầng mạng**: Wi-Fi.
- **Tầng dịch vụ**: Server, API, database, dịch vụ OTP.
- **Tầng ứng dụng**: Mobile app, Web app cho admin và user.

6. Appendices (Phụ lục)

6.1. Thuật ngữ

- RFID: Radio Frequency Identification.
- OTP: One-Time Password.
- PIN: Personal Identification Number.
- ESP32: Vi điều khiển hỗ trợ Wi-Fi/Bluetooth.
- API: Application Programming Interface.

6.2. Giả định & Ràng buộc

- Hệ thống cần mạng Wi-Fi để sử dụng OTP, nhưng vẫn mở được bằng RFID/PIN khi offline.
- OTP có hiệu lực trong 30–60 giây.

- Cửa tự động khóa lại sau thời gian định sẵn.
- Mỗi người dùng có tối đa 1 thẻ RFID và 1 PIN.
- Log lưu trữ tối thiểu 10.000 bản ghi.

6.3. Tài liệu tham khảo