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)

ID	Requirement Description
R1	**Mở khóa bằng RFID**
R1.1	Hệ thống phải cho phép mở khóa bằng thẻ RFID hợp lệ.
R1.2	Hệ thống phải lưu trữ và quản lý danh sách thẻ RFID được phép sử dụng.
R1.3	Khi quét thẻ không hợp lệ, hệ thống phải từ chối và hiển thị cảnh báo.
R2	**Mở khóa bằng OTP (One-Time Password)**
R2.1	Hệ thống phải sinh OTP ngẫu nhiên và có thời hạn sử dụng (<60 giây).
R2.2	OTP phải được gửi đến người dùng qua ứng dụng di động/Telegram/email tùy cấu hình.
R2.3	Hệ thống chỉ mở khóa khi OTP nhập vào khớp và còn hiệu lực.
R3	**Mở khóa bằng PIN**
R3.1	Hệ thống phải cho phép người dùng nhập PIN cố định để mở khóa.
R3.2	Người dùng có thể thay đổi PIN thông qua giao diện quản lý.
R3.3	Khi nhập sai PIN nhiều lần liên tiếp, hệ thống phải khóa tạm thời và cảnh báo.
R4	**Quản lý mở khóa**
R4.1	ESP32 phải điều khiển khóa điện tử (servor) để mở hoặc đóng.
R4.2	Hệ thống phải ghi lại log sự kiện (thẻ RFID được quét, OTP/PIN được nhập, trạng thái khóa).
R4.3	Hệ thống phải cho phép reset và cập nhật firmware qua OTA (Over-The-Air).

R1 – Hệ thống cho phép người dùng mở khóa bằng thẻ RFID
R1.1. Hệ thống phải cho phép mở khóa bằng thẻ RFID hợp lệ.

- Thẻ RFID phải nằm trong danh sách đã đăng ký.
- Khi quét đúng thẻ hợp lệ, khóa phải mở trong ≤ 2 giây.
- Hệ thống phải phát tín hiệu xác nhận (LED xanh/buzzer).

R1.2. Hệ thống phải lưu trữ và quản lý danh sách thẻ RFID được phép sử dụng.
- Danh sách thẻ lưu trong bộ nhớ.
- Số lượng thẻ tối thiểu hệ thống lưu được ≥ 50.

R1.3. Khi quét thẻ không hợp lệ, hệ thống phải từ chối và hiển thị cảnh báo.
- LED đỏ sáng và phát âm cảnh báo.
- Hiển thị thông báo "RFID không hợp lệ" màn hình LCD.
- Sau 3 lần quét sai liên tiếp, khóa tạm vô hiệu hóa trong 1 phút.

R2 – Hệ thống cho phép người dùng mở khóa bằng OTP (One-Time Password)

R2.1. Hệ thống phải sinh OTP ngẫu nhiên và có thời hạn sử dụng (< 60 giây).
- OTP dài 6 chữ số.
- Mỗi OTP chỉ dùng một lần.
- Hết hạn sau 60 giây kể từ khi sinh ra.

R2.2. OTP phải được gửi đến người dùng qua ứng dụng di động/Telegram/email tùy cấu hình.
- OTP gửi thành công trong ≤ 5 giây.
- Có thông báo "OTP đã được gửi" trên App.

R2.3. Hệ thống chỉ mở khóa khi OTP nhập vào khớp và còn hiệu lực.
- OTP hết hạn sẽ bị từ chối.
- Sau 3 lần nhập sai OTP liên tiếp → khóa tạm thời trong 2 phút.
- Mở khóa thành công phải có log sự kiện lưu lại.

R3 – Hệ thống cho phép người dùng mở khóa bằng PIN

R3.1. Hệ thống phải cho phép người dùng nhập PIN cố định để mở khóa.
- PIN dài 4–6 chữ số.
- Khi nhập đúng PIN, khóa mở trong ≤ 1 giây.
- Có tín hiệu xác nhận (LED xanh/buzzer).

R3.2. Người dùng có thể thay đổi PIN thông qua giao diện quản lý.
- Yêu cầu nhập PIN cũ hoặc OTP trước khi đổi.
- PIN mới không được trùng PIN cũ.
- Có thông báo xác nhận "PIN đã thay đổi thành công".

R3.3. Khi nhập sai PIN nhiều lần liên tiếp, hệ thống phải khóa tạm thời và cảnh báo.
- Sau 5 lần sai → khóa vô hiệu hóa trong 5 phút.
- Buzzer kêu ngắn 3 lần, LED đỏ nhấp nháy.
- Ghi log sự kiện sai PIN.

R4 – Quản lý mở khóa

R4.1. Hệ thống phải điều khiển khóa điện tử (servo/relay) để mở hoặc đóng.
- Lệnh mở/đóng từ App → phản hồi trong ≤ 2 giây.
- Trạng thái khóa (mở/đóng) phải hiển thị trên LCD.
- Servo/relay phải hoạt động ổn định ≥ 50.000 chu kỳ.

R4.2. Hệ thống phải ghi lại log sự kiện.
- Log gồm: loại sự kiện (RFID/OTP/PIN), kết quả (thành công/thất bại), thời gian.
- Lưu tối thiểu 1000 sự kiện trong bộ nhớ.
- Có chức năng tải log xuống App.

R4.3. Hệ thống phải cho phép reset và cập nhật firmware qua OTA (Over-The-Air).
- Reset bằng nút cứng hoặc lệnh App.
- Firmware mới tải về phải được kiểm tra checksum.
- Khi cập nhật OTA, hệ thống vẫn đảm bảo an toàn (tự rollback nếu lỗi).

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

ID	Requirement Description
R5	Thời gian phản hồi khi quét RFID, nhập OTP hoặc PIN không vượt quá 2 giây.
R6	Hệ thống phải hoạt động liên tục 24/7 với tỉ lệ lỗi < 1%.
R7	Dữ liệu OTP/PIN phải được mã hóa khi truyền, và giao tiếp phải sử dụng HTTPS/TLS.
R8	Hệ thống phải tiêu thụ điện năng thấp, có thể dùng pin/UPS trong trường hợp mất điện.
R9	Hệ thống phải dễ mở rộng để tích hợp thêm cảm biến (camera, vân tay, cảm biến cửa…).

R5 – Thời gian phản hồi
- RFID/OTP/PIN phải được xử lý trong ≤ 2 giây.
- Nếu vượt ngưỡng thì hệ thống phải ghi log sự kiện lỗi.

R6 – Độ tin cậy hệ thống
- Hệ thống phải hoạt động liên tục 24/7 với uptime ≥ 99%.
- Có cơ chế tự khởi động lại khi treo.
- Khi mất mạng, RFID/PIN vẫn hoạt động offline.
- Tuổi thọ phần cứng tối thiểu 2 năm.

R7 – Bảo mật dữ liệu
- OTP/PIN phải được mã hóa (AES-128 trở lên).
- Giao tiếp sử dụng HTTPS/TLS.
- Không được lưu OTP dưới dạng plaintext.

R8 – Tiêu thụ năng lượng
- Có pin/UPS dự phòng ≥ 4 giờ trong trường hợp mất điện.
- Cảnh báo pin yếu hiển thị trên App.

R9 – Khả năng mở rộng
- Hỗ trợ tích hợp thêm cảm biến (camera, vân tay, cảm biến cửa).
- Cho phép giao tiếp mở rộng qua UART/I2C/SPI.
- Có thể quản lý cảm biến bổ sung qua App/Web.

4. Use case modelling

Use Case Name	**Unlock with RFID**
Use Case ID	UC01
Scope	IoT Smart Doorlock (hardware)
Primary Actor(s)	User
Stakeholders and Interests	User: wants to quickly unlock using an RFID card. System Owner: wants to ensure only valid cards can unlock the door.
Preconditions	The user has a registered valid RFID card.
Postconditions	The door unlocks if the card is valid. The event log is recorded.
Main Flow of Events	- The user swipes the RFID card. - The system reads the card ID. - The system compares the ID against the registered list. - If valid → the system controls the lock to open.
Alternative Flows	If the card is invalid → the system denies access, shows a warning, and logs the event. After 3 consecutive failures → the lock is disabled for 1 minute.
Exception Flows	RFID reader hardware failure → notify the user.
Includes	UC07 (Electronic Lock Control), UC05 (Event Logging).
Extends	None
Special Requirements	Response time < 2s (R5).
Assumptions	The RFID card has already been registered in the system.
Notes	Can be extended to support multiple RFID card types.
Author	
Date	

Use Case Name	**Unlock with OTP**
Use Case ID	UC02
Scope	IoT Smart Doorlock (hardware)
Primary Actor(s)	User
Stakeholders and Interests	User: wants to unlock securely without an RFID card. System Owner: wants OTP to be random, secure, and time-limited.

Preconditions	The user has a valid account and OTP delivery is configured.
Postconditions	The door unlocks if the OTP is valid and not expired.
Main Flow of Events	- The user requests an OTP. - The system generates a random OTP (6 digits, expires after 60 seconds). - The OTP is sent via App/Telegram/email within ≤ 5 seconds. - The user enters the OTP. - If valid and within the time limit → the door unlocks.
Alternative Flows	If OTP is invalid → access denied. After 3 consecutive failures → the lock is disabled for 2 minutes.
Exception Flows	OTP delivery failure → notify the user on the App.
Includes	UC07 (Electronic Lock Control), UC05 (Event Logging).
Extends	UC04 (OTP Management).
Special Requirements	The user has internet connectivity.
Assumptions	The RFID card has already been registered in the system.
Notes	Can integrate with multiple OTP delivery channels.
Author	
Date	

Use Case Name	**Unlock with PIN**
Use Case ID	UC03
Scope	IoT Smart Doorlock (hardware)
Primary Actor(s)	User
Stakeholders and Interests	User: wants to easily unlock using a PIN code. System Owner: wants PINs to be secure and changeable.
Preconditions	The user has a valid PIN.
Postconditions	The door unlocks if the PIN is correct. The event log is recorded.
Main Flow of Events	- The user enters a PIN (4–6 digits). - The system verifies the PIN.

	- If correct → unlocks within ≤ 1 second, LED green/buzzer confirms.
Alternative Flows	If incorrect → deny access. After 5 consecutive failures → the lock is disabled for 5 minutes, red LED blinks, buzzer beeps 3 times.
Exception Flows	Keypad failure → notify the user via App.
Includes	UC07 (Electronic Lock Control), UC05 (Event Logging).
Extends	UC06 (PIN Management).
Special Requirements	PIN must be AES-128 encrypted.
Assumptions	The user has been assigned a valid initial PIN.
Notes	PIN can be changed via App/Web
Author	
Date	

Use Case Name	**OTP Management**
Use Case ID	UC04
Scope	IoT Smart Doorlock (hardware)
Primary Actor(s)	User, System
Stakeholders and Interests	User: wants to receive OTP quickly to unlock. System Owner: wants OTP to be generated correctly, securely, and expire on time.
Preconditions	The user has a valid account.
Postconditions	The OTP is generated, single-use, and expires after 60 seconds.
Main Flow of Events	- The user requests an OTP. - The system generates a random OTP (6 digits). - The OTP is sent to App/Telegram/email.
Alternative Flows	None.
Exception Flows	OTP delivery error → notify the user.
Includes	None
Extends	UC02 (Unlock with OTP).
Special Requirements	Each OTP is single-use only.
Assumptions	The system has internet connectivity.
Notes	Delivery channel can be configured.
Author	

Date	

Use Case Name	**Event Logging**
Use Case ID	UC05
Scope	IoT Smart Doorlock (hardware)
Primary Actor(s)	System, System Owner
Stakeholders and Interests	System Owner: wants to monitor all unlock attempts.
Preconditions	The system is functioning normally.
Postconditions	Event logs are stored in memory (≥ 1000 records). Logs can be downloaded via App.
Main Flow of Events	- Every unlock attempt (success/failure) is recorded. - Logs include: event type (RFID/OTP/PIN), result, timestamp. - User/System Owner can download logs via App/Web.
Alternative Flows	If memory is full → overwrite the oldest log.
Exception Flows	Memory failure → send alert to the user.
Includes	None
Extends	UC01, UC02, UC03.
Special Requirements	Logs must be downloadable through App/Web.
Assumptions	Sufficient storage is available.
Notes	Can be extended to cloud-based storage.
Author	
Date	

Use Case Name	**PIN Management**
Use Case ID	UC06
Scope	IoT Smart Doorlock (hardware)
Primary Actor(s)	User, System Owner
Stakeholders and Interests	User: wants to change PIN for security. System Owner: wants to ensure secure PIN change process.
Preconditions	User knows the old PIN or has OTP for verification.
Postconditions	The new PIN is stored and confirmed successfully.
Main Flow of Events	- User selects the PIN change function.

	- User enters the old PIN or OTP for verification. - If verification succeeds → user enters a new PIN (different from the old one). - The system saves the new PIN and confirms with a message "PIN changed successfully".
Alternative Flows	If the new PIN matches the old one → notify error and request another PIN.
Exception Flows	Invalid verification or memory failure → deny change and notify via App.
Includes	UC05 (Event Logging).
Extends	UC03 (Unlock with PIN).
Special Requirements	PIN must be AES-128 encrypted.
Assumptions	User has permission to change PIN.
Notes	PIN change can be done via App or Web.
Author	
Date	

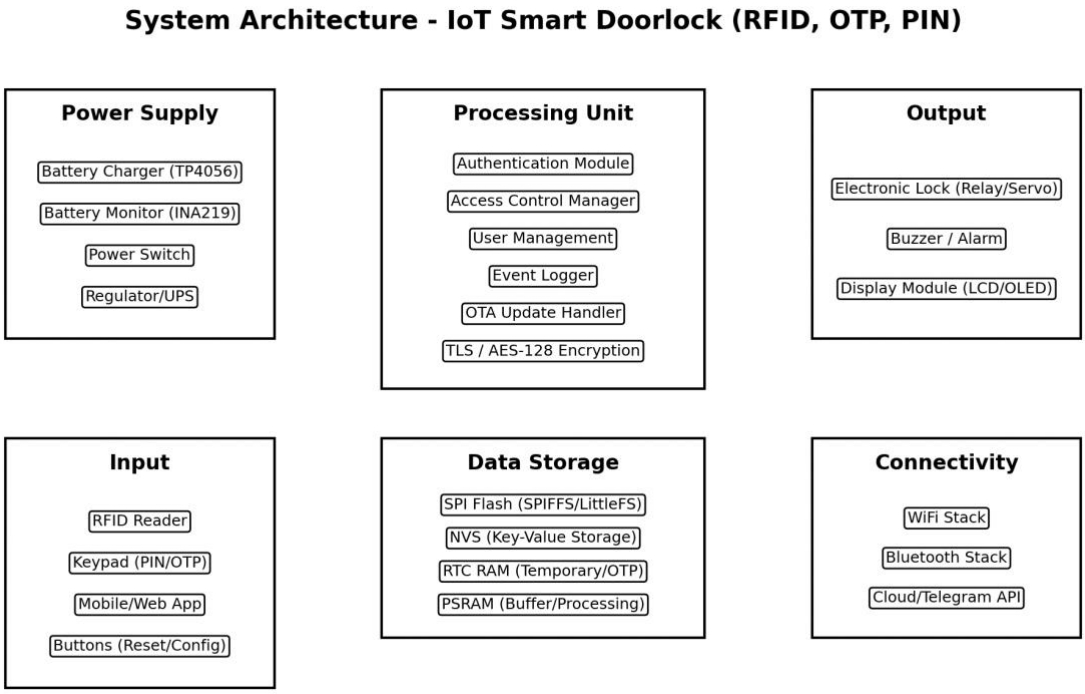
Use Case Name	**Electronic Lock Control**
Use Case ID	UC07
Scope	IoT Smart Doorlock (hardware)
Primary Actor(s)	User, System
Stakeholders and Interests	User: wants accurate and fast lock/unlock control. System Owner: wants reliable and durable lock hardware.
Preconditions	The system is ready and has stable power supply.
Postconditions	The lock changes state (open/close) and status is shown on LCD/App.
Main Flow of Events	- Receive lock/unlock command from App or valid RFID/OTP/PIN. - System drives servo/relay to change lock state. - Updated state is displayed on LCD and App.
Alternative Flows	Servo/relay jammed → retry. If still fails → send alert.
Exception Flows	Hardware failure → send critical error notification.
Includes	UC05 (Event Logging).

Extends	UC01, UC02, UC03.
Special Requirements	Response ≤ 2s; servo/relay lifetime ≥ 50,000 cycles.
Assumptions	Servo/relay is properly installed and compatible.
Notes	Can be replaced with other electronic lock modules.
Author	
Date	

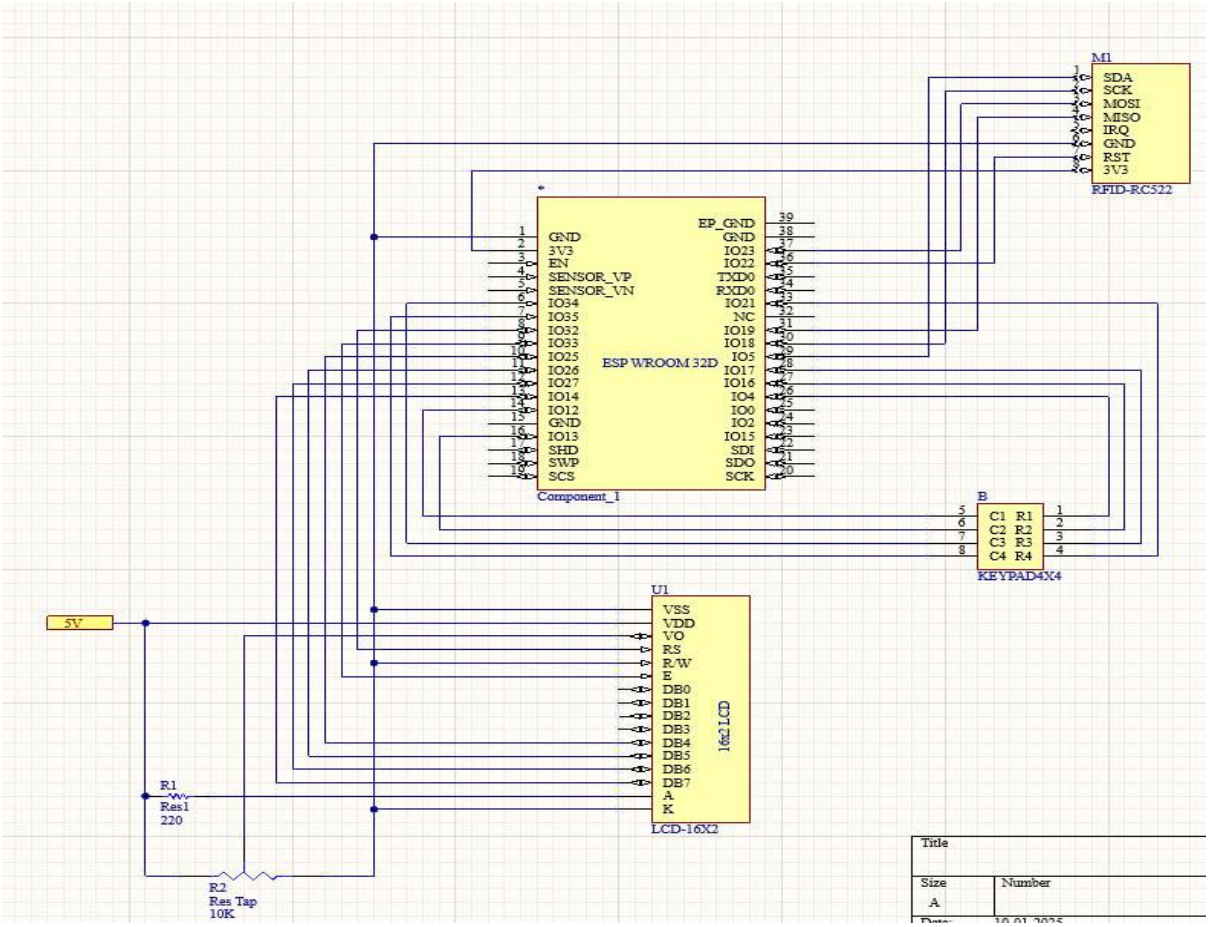
5. Use Case-Requirement Traceability Matrix

	UC01	UC02	UC03	UC04	UC05	UC06	UC07
R1.1	X						X
R1.2				X			
R1.3	X				X		
R2.1		X					
R2.2		X					
R2.3		X					X
R3.1			X				X
R3.2				X			
R3.3			X		X		
R4.1							X
R4.2				X			
R4.3					X		
R5	X	X	X				X
R6		X				X	X
R7							X
R8							X
R9				X			X

6. System architecture (Kiến trúc hệ thống)



7. Schematic (Sơ đồ)



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

8.1. 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.

8.2. 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.

8.3. 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).

8.4. 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.