

**BỘ GIÁO DỤC VÀ ĐÀO TẠO**  
**TRƯỜNG ĐẠI HỌC SƯ PHẠM KỸ THUẬT TP. HCM**  
**KHOA CÔNG NGHỆ THÔNG TIN**



**ĐỒ ÁN CUỐI KỲ**  
**MÔN VẬN VẬT KẾT NỐI**

**DESIGN AND IMPLEMENTATION OF DOOR ACCESS**  
**CONTROL AND SECURITY BASED ON IOT**

**GVHD:** ThS. Đinh Công Đoàn

**SVTH:**

- |                         |          |
|-------------------------|----------|
| 1. Trần Phúc Toàn       | 23110344 |
| 2. Nguyễn Thị Kim Oanh  | 23110372 |
| 3. Nguyễn Phạm Bảo Trân | 23110348 |

**Thành phố Hồ Chí Minh, Tháng 4 năm 2025**

## MỤC LỤC

<b>Danh mục từ viết tắt.....</b>	<b>1</b>
<b>LỜI CẢM ƠN.....</b>	<b>2</b>
<b>PHẦN MỞ ĐẦU.....</b>	<b>3</b>
<b>1.1. Tóm tắt ý tưởng nội dung báo cáo.....</b>	<b>3</b>
<b>1.2. Đặt vấn đề .....</b>	<b>3</b>
1.2.1 Tóm lược những nghiên cứu trong và ngoài nước .....	3
1.2.2. Một số tài liệu liên quan .....	5
1.2.3. Lí do chọn đề tài .....	6
1.2.4. Mục tiêu đề tài .....	7
1.2.5. Đối tượng nghiên cứu .....	7
1.2.7. Phương pháp nghiên cứu .....	9
1.2.8. Nội dung đề tài.....	9
<b>PHẦN NỘI DUNG.....</b>	<b>11</b>
<b>CHƯƠNG 1: GIỚI THIỆU .....</b>	<b>11</b>
1.1. Chức năng chính.....	11
1.2. Tính năng nổi bật.....	11
1.3. Ứng dụng thực tế.....	11
<b>CHƯƠNG 2: PHÂN TÍCH YÊU CẦU.....</b>	<b>14</b>
2.1. Yêu cầu hệ thống .....	14
2.2. Sơ đồ nguyên lý .....	15
2.3. Mô tả các bước của hệ thống.....	16
<b>CHƯƠNG 3: NHỮNG KIẾN THỨC LIÊN QUAN .....</b>	<b>17</b>
3.1. Servo motor SG90 .....	17
3.1.1 Thông số kỹ thuật .....	17
3.1.2. Chức năng các chân .....	18
3.2. RFID.....	19
3.2.1. Giới thiệu RFID .....	19

3.2.2.	Thông số kỹ thuật.....	19
3.3.	ESP32-DevKitC .....	20
3.3.1.	Ưu điểm.....	20
3.3.2.	Thông số kỹ thuật.....	20
3.4.	LCD 16x02 và Module I2C.....	21
3.4.1.	Giới thiệu LCD 16x02 .....	21
3.4.2.	Thông số kỹ thuật.....	21
3.4.3.	Chức năng các chân LCD .....	22
3.5	Module I2C.....	24
3.5.1.	Tại sao sử dụng Module I2C.....	24
3.5.2.	Thông số kỹ thuật .....	24
3.6.	Arduino .....	24
3.6.1.	Thông số kỹ thuật .....	25
3.7.	Khóa điện 12V.....	26
3.7.1.	Thông số kỹ thuật .....	27
3.7.2.	Chức năng Khóa điện .....	27
3.8.	Giới thiệu Module bàn phím ma trận 4x4 .....	27
3.9.	Cảm biến vân tay .....	28
3.9.1.	Thông số kỹ thuật .....	29
3.9.2.	Ứng dụng cảm biến vân tay .....	30
<b>CHƯƠNG 4:</b>	<b>ỨNG DỤNG .....</b>	<b>31</b>
4.1.	Mô tả các bước đi.....	31
4.1.1.	Cấp nguồn cho hệ thống .....	31
4.1.2.	Nhận diện người dùng.....	31
4.1.3.	Hiển thị thông tin .....	32
4.1.4.	Điều khiển truy cập.....	32
4.1.5.	Kết nối mạng qua ESP32S.....	32
4.1.6.	Các chức năng khác .....	32
4.2.	Sơ đồ mạch kết nối các phần, các mô đun .....	33
4.3.	Chi tiết các bước xây dựng ứng dụng.....	33
4.4.	Nguy cơ tiềm ẩn .....	38

4.4.1.	Nguy cơ về an ninh .....	38
4.4.2.	Nguy cơ về Khả năng sử dụng và Môi trường.....	39
4.5.	Cách khắc phục .....	39
4.5.1.	.Tăng cường an ninh .....	39
4.5.2.	Nâng cao Độ tin cậy Kỹ thuật và Vận hành.....	40
<b><i>PHẦN KẾT LUẬN.....</i></b>		<b><i>43</i></b>
<b>1. Kết quả đạt được.....</b>		<b>43</b>
<b>2. Ưu điểm.....</b>		<b>43</b>
<b>3. Nhược điểm.....</b>		<b>44</b>
<b>4. Hướng phát triển đề tài .....</b>		<b>44</b>
<b><i>TÀI LIỆU THAM KHẢO .....</i></b>		<b><i>46</i></b>

### Danh mục từ viết tắt

ST	Từ viết tắt	Ý nghĩa	Chú thích
1	RFID	Radio Frequency Identification	Nhận dạng qua tần số vô tuyến
2	LCD	Liquid Crystal Display	Màn hình tinh thể lỏng
3	LED	Inter-Integrated Circuit	Điốt phát quang
4	I2C	Integrator Development Environment	
5	IDE	Integrator Development Environment	Môi trường phát triển tích hợp
7	IC	Integrated Circuit	
8	I/O	Input/output	đầu vào/đầu ra
9	UART	Universal asynchronous receiver transmitter	
10	DSP	Digital Signal Processor	
12	SPI	Serial Peripheral Interface	Giao tiếp ngoại vi nối tiếp
13	IOT	Internet of Things	Mạng lưới vạn vật kết nối Internet
16	DDRAM	Display Data RAM	Bộ nhớ dữ liệu hiển thị
17	CGRAM	Character Generator RAM	Bộ nhớ tạo ký tự
18	AC	Address Counter	Bộ đếm địa chỉ
20	AI	Artificial Intelligence	Trí tuệ nhân tạo

## LỜI CẢM ƠN

Trong quá trình học tập và thực hiện đồ án, chúng em đã nhận được sự hỗ trợ, chỉ dẫn nhiệt tình từ quý Thầy Cô, các anh chị và bạn bè. Với tình cảm chân thành và sâu sắc, chúng em xin được bày tỏ lòng biết ơn đến tất cả những người đã đồng hành cùng chúng em trong hành trình này.

Trước hết, chúng em xin gửi lời tri ân sâu sắc đến quý Thầy Cô khoa Công nghệ thông tin và các Thầy Cô thuộc bộ môn Internet vạn vật đã tận tâm truyền đạt những kiến thức quý báu, tạo nền tảng vững chắc giúp chúng em có thể vận dụng vào thực tiễn và hoàn thành đồ án một cách trọn vẹn. Đặc biệt, chúng em xin gửi lời cảm ơn chân thành và sâu sắc đến Thầy Đinh Công Đoan, người đã không quản ngại thời gian và công sức, tận tình hướng dẫn, chỉ bảo và đồng hành cùng chúng em trong suốt quá trình nghiên cứu và thực hiện đồ án.

Chúng em cũng xin bày tỏ lòng biết ơn đến các anh chị và các bạn cùng khóa đã nhiệt tình chia sẻ kinh nghiệm, hỗ trợ kỹ thuật và đóng góp ý kiến quý báu. Sự hợp tác và tinh thần đoàn kết của tất cả mọi người đã giúp chúng em vượt qua nhiều khó khăn, thách thức để hoàn thành đồ án đúng tiến độ và đạt được kết quả tốt nhất.

Mặc dù đã nỗ lực hết mình, chúng em nhận thức rằng đồ án vẫn còn những hạn chế và thiếu sót nhất định. Với tinh thần cầu thị, chúng em rất mong nhận được những góp ý, chỉ dẫn từ quý Thầy Cô và các bạn để có thể tiếp tục hoàn thiện mô hình, nâng cao chất lượng đồ án và áp dụng những kinh nghiệm quý báu này vào các dự án tương lai.

Một lần nữa, chúng em xin gửi lời cảm ơn chân thành và sâu sắc đến tất cả những người đã đồng hành, hỗ trợ và tạo điều kiện thuận lợi để chúng em có thể hoàn thành tốt đồ án này. Những kiến thức và kinh nghiệm quý báu mà chúng em tích lũy được trong quá trình thực hiện đồ án sẽ là hành trang vô giá cho chúng em trên con đường học tập và phát triển sự nghiệp trong tương lai.

## PHẦN MỞ ĐẦU

### 1.1. Tóm tắt ý tưởng nội dung báo cáo

Báo cáo này trình bày một giải pháp đột phá trong lĩnh vực an ninh và kiểm soát truy cập: hệ thống kiểm soát cửa thông minh tích hợp công nghệ IoT tiên tiến, cho phép người dùng quản lý và điều khiển quyền truy cập thông qua lệnh thoại trên thiết bị di động. Vượt xa khỏi giới hạn của các hệ thống khóa cơ học truyền thống vốn chỉ hoạt động theo cơ chế cơ học đơn giản, giải pháp này mang đến nhiều ưu điểm vượt trội phù hợp với xu hướng số hóa hiện đại. Người dùng có thể thực hiện giám sát và quản lý từ xa không phụ thuộc vào khoảng cách địa lý, cho phép kiểm soát cửa ra vào từ bất kỳ đâu thông qua kết nối internet. Đặc biệt, hệ thống được thiết kế với giao diện web chạy trên máy chủ local, đồng thời có khả năng mở rộng truy cập từ internet thông qua công cụ ngrok, tạo điều kiện thuận lợi cho việc quản lý từ xa mà không cần cấu hình phức tạp.

Hệ thống còn được trang bị khả năng ghi nhật ký hoạt động theo thời gian thực, cung cấp thông tin chi tiết về mọi lượt ra vào kèm theo thời gian chính xác, giúp chủ sở hữu dễ dàng theo dõi và quản lý. Về phương thức xác thực, giải pháp này tập trung vào ba công nghệ bảo mật hiệu quả: cảm biến vân tay chính xác cho phép nhận diện nhanh chóng người dùng được ủy quyền, hệ thống mật khẩu số linh hoạt có thể dễ dàng thay đổi khi cần thiết, và công nghệ RFID tiện lợi cho phép truy cập nhanh chóng thông qua thẻ từ mà không cần tiếp xúc trực tiếp. Sự kết hợp đa dạng các phương thức xác thực này không chỉ nâng cao tính bảo mật, giảm thiểu rủi ro bị đột nhập trái phép mà còn mang lại sự linh hoạt chưa từng có trong việc quản lý quyền truy cập, đáp ứng toàn diện nhu cầu ngày càng cao của người dùng trong kỷ nguyên số hiện đại.

### 1.2. Đặt vấn đề

#### 1.2.1 Tóm lược những nghiên cứu trong và ngoài nước

- Công Nghệ Sinh Trắc Học Trong Hệ Thống Kiểm Soát Truy Cập:

Các nghiên cứu hiện đại đang tập trung mạnh mẽ vào việc tích hợp công nghệ sinh trắc học với các hệ thống điều khiển dựa trên IoT. Một nghiên cứu tiêu biểu đã phát triển hệ thống tích hợp nhận dạng vân tay với vi điều khiển Arduino và module GSM, tạo nên giải

pháp kiểm soát cửa từ xa an toàn và hiệu quả. Hệ thống này cho phép đăng ký vân tay, đối chiếu mẫu và giám sát trạng thái theo thời gian thực. Quá trình xác thực bao gồm các bước đăng ký vân tay, lưu trữ an toàn vào cơ sở dữ liệu, và sau đó so sánh với các mẫu đã lưu để xác định quyền truy cập.

Công nghệ nhận dạng khuôn mặt cũng đang được ứng dụng rộng rãi trong các hệ thống kiểm soát cửa. Một nghiên cứu đã phát triển hệ thống dựa trên phương pháp PCA (Principal Component Analysis) để đo khoảng cách Euclidean trong hình ảnh khuôn mặt, từ đó kích hoạt cơ chế mở khóa cho chủ sở hữu được nhận diện. Tương tự, một hệ thống khác sử dụng ESP32-CAM đã được phát triển, kết hợp khả năng nhận dạng khuôn mặt với giám sát từ xa thông qua mạng IoT.

#### - Hệ Thống Kiểm Soát Qua Ứng Dụng Di Động và Nền Tảng Truyền Thông

Ứng dụng di động đang trở thành phương tiện kiểm soát phổ biến cho các hệ thống cửa thông minh. Một nghiên cứu mới đây đã phát triển hệ thống cửa thông minh có thể điều khiển qua tin nhắn WhatsApp, tận dụng sự kết hợp giữa IoT và nền tảng truyền thông quen thuộc<sup>[4]</sup>. Phương pháp này mang đến sự tiện lợi và linh hoạt cao cho người dùng trong việc quản lý truy cập từ xa.

Tại Ấn Độ, các nhà nghiên cứu đã phát triển hệ thống kiểm soát cửa dựa trên Android kết hợp với công nghệ IoT, cho phép chủ nhà giám sát từ xa trạng thái của cửa, đồng thời nhận thông báo khi có chuyển động đáng ngờ. Hệ thống này sử dụng giao thức MQTT cloud làm cầu nối truyền thông giữa điện thoại thông minh và cơ chế khóa cửa.

Một nghiên cứu khác đã phát triển hệ thống bảo mật nhà thông minh tích hợp cảnh báo và kiểm soát truy cập, cho phép không chỉ điều khiển cửa từ xa mà còn gửi hình ảnh của khách đến email của chủ nhà<sup>[6]</sup>. Hệ thống này sử dụng Raspberry Pi làm bộ điều khiển trung tâm, tiêu thụ ít năng lượng và có chi phí thấp.

Công nghệ Wi-Fi cũng được ứng dụng trong các hệ thống kiểm soát cửa, với một nghiên cứu đã phát triển hệ thống kiểm soát truy cập dựa trên IoT và Wi-Fi, cho phép người dùng điều khiển cửa từ xa trong phạm vi được cung cấp bởi điểm truy cập không dây.

#### - Nghiên Cứu và Ứng Dụng tại Việt Nam

Tại Việt Nam, nghiên cứu về nhà thông minh dựa trên IoT cũng đang được phát triển. Một nghiên cứu đã đề xuất mô hình nhà thông minh sử dụng ID để kiểm soát



truy cập, trong đó hệ thống đăng ID lên dịch vụ kiểm soát để so sánh với các ID được ủy quyền trong cơ sở dữ liệu<sup>[8]</sup>. Nghiên cứu này cũng thảo luận về các thành phần chính trong hệ thống nhà thông minh, bao gồm cảm biến, bộ xử lý và các phần mềm quản lý.

Gần đây nhất, một bài viết vào tháng 2/2025 đã thảo luận về ứng dụng IoT và AI trong trung tâm giám sát an ninh tại Việt Nam. Hệ thống này cho phép các thiết bị như camera, cảm biến và máy báo động hoạt động liên tục và gửi dữ liệu theo thời gian thực. Khi tích hợp với AI, dữ liệu này được xử lý nhanh chóng để phát hiện các bất thường, giảm thiểu cảnh báo giả và nâng cao độ chính xác trong phản ứng trước các sự cố an ninh.

#### - Xu Hướng Phát Triển và Triển Vọng Tương Lai

Xu hướng phát triển hệ thống kiểm soát truy cập cửa thông minh đang hướng tới các giải pháp mã nguồn mở, cho phép tích hợp với các hệ thống khác và tùy chỉnh theo nhu cầu cụ thể. Các hệ thống như Raspberry Pi và Arduino đang được sử dụng rộng rãi để xây dựng các hệ thống kiểm soát truy cập tùy chỉnh, với khả năng kết nối với cơ sở dữ liệu và giao tiếp với các thiết bị khác.

Trong tương lai, việc tích hợp IoT với các công nghệ mới nổi và đảm bảo khả năng mở rộng sẽ là ưu tiên hàng đầu. Ưu tiên cho các triển khai thực tế là rất quan trọng cho làn sóng đổi mới tiếp theo trong hệ thống kiểm soát truy cập<sup>[12]</sup>.

### 1.2.2. Một số tài liệu liên quan

Nhiều nghiên cứu trong và ngoài nước đã tập trung phát triển các hệ thống kiểm soát truy cập cửa thông minh dựa trên IoT, với các hướng tiếp cận đa dạng như tích hợp sinh trắc học, sử dụng nền tảng di động, truyền thông không dây và các giao thức bảo mật hiện đại.

Trong nghiên cứu của G. Mary Sowjanya và S. Nagaraju (2016), nhóm tác giả đã thiết kế và triển khai một hệ thống kiểm soát truy cập cửa sử dụng cảm biến vân tay, vi điều khiển và kết nối IoT. Hệ thống cho phép xác thực người dùng qua sinh trắc học, đồng thời gửi thông báo trạng thái cửa đến chủ nhà qua Internet, nâng cao mức độ an toàn và tiện lợi.

Ezeofor C. Joseph và cộng sự (2022) phát triển một hệ thống kiểm soát truy cập cửa dựa trên IoT, tích hợp với ứng dụng web cho phép giám sát và điều khiển cửa từ xa. Hệ

thống này sử dụng vi điều khiển ESP8266, cảm biến và giao diện web để quản lý quyền truy cập, đồng thời ghi lại nhật ký truy cập cho mục đích bảo mật.

Một số nghiên cứu khác tập trung vào việc kết hợp nhiều phương thức xác thực, như hệ thống khóa cửa thông minh sử dụng cả vân tay và bàn phím để tăng cường bảo mật. Các giải pháp này thường sử dụng nền tảng IoT để truyền dữ liệu thời gian thực lên các dịch vụ đám mây như Firebase, cho phép chủ nhà kiểm soát và theo dõi trạng thái cửa mọi lúc, mọi nơi.

Ngoài ra, các nghiên cứu mới còn thử nghiệm việc tích hợp IoT với các nền tảng nhắn tin phổ biến như WhatsApp để mở rộng khả năng điều khiển từ xa, hoặc sử dụng camera nhận diện khuôn mặt kết hợp với AI để tự động xác thực và ghi nhận hình ảnh người truy cập.

Các tài liệu này không chỉ tập trung vào thiết kế kỹ thuật mà còn đánh giá hiệu quả, độ tin cậy, khả năng mở rộng và các vấn đề bảo mật trong môi trường IoT, góp phần hoàn thiện các giải pháp kiểm soát truy cập cửa thông minh trong thực tiễn.

### **1.2.3. Lí do chọn đề tài**

Việc lựa chọn đề tài "Hệ thống kiểm soát truy cập và an ninh cửa dựa trên IoT" xuất phát từ nhiều yếu tố quan trọng trong bối cảnh phát triển công nghệ hiện nay.

Trước hết, an ninh và kiểm soát truy cập đang trở thành mối quan tâm hàng đầu cho cả môi trường dân cư và doanh nghiệp. Các phương pháp truyền thống như khóa cơ học không còn đáp ứng được nhu cầu bảo mật ngày càng cao, đặc biệt là khả năng quản lý từ xa và giám sát liên tục.

Sự phát triển mạnh mẽ của công nghệ IoT mở ra cơ hội lớn trong việc kết nối và điều khiển các thiết bị thông minh. Việc áp dụng IoT vào hệ thống kiểm soát cửa không chỉ nâng cao tính bảo mật mà còn mang lại trải nghiệm người dùng tiện lợi hơn thông qua đa dạng phương thức xác thực như vân tay, mặt khẩu và RFID.

Giải pháp này còn đáp ứng xu hướng số hóa và tự động hóa trong quản lý tòa nhà hiện đại. Bằng cách tích hợp giao diện web chạy trên máy chủ local và khả năng mở rộng truy cập từ internet thông qua ngrok, hệ thống mang lại tính linh hoạt cao trong quản lý, phù hợp với lối sống và làm việc di động hiện nay.

Đặc biệt, khả năng ghi nhật ký hoạt động theo thời gian thực của hệ thống giúp tăng cường tính minh bạch và trách nhiệm giải trình, đồng thời hỗ trợ việc phân tích và khắc phục sự cố khi cần thiết.

Với những lý do trên, đề tài này không chỉ có tính ứng dụng cao mà còn mang tính cấp thiết trong việc đáp ứng nhu cầu an ninh thông minh trong kỷ nguyên số.

#### **1.2.4. Mục tiêu đề tài**

- Mục tiêu tổng quát: Nghiên cứu, thiết kế và phát triển một hệ thống kiểm soát truy cập cửa thông minh dựa trên công nghệ IoT, tích hợp đa dạng phương thức xác thực và khả năng quản lý từ xa nhằm nâng cao tính bảo mật, tiện lợi và hiệu quả trong việc kiểm soát ra vào các khu vực cần bảo vệ.
- Mục tiêu cụ thể
  - Xây dựng hệ thống xác thực đa phương thức tích hợp công nghệ nhận dạng vân tay, mã số mật khẩu và thẻ RFID đảm bảo tính bảo mật cao.
  - Phát triển giao diện web chạy trên máy chủ local cho phép quản lý và cấu hình hệ thống một cách trực quan, dễ sử dụng.
  - Tích hợp khả năng truy cập từ xa thông qua ngrok, giúp người dùng có thể quản lý hệ thống từ bất kỳ đâu thông qua internet.
  - Thiết kế và triển khai hệ thống ghi nhật ký hoạt động theo thời gian thực, cung cấp thông tin chi tiết về các lượt ra vào.
  - Phát triển chức năng điều khiển bằng lệnh thoại trên thiết bị di động, tăng tính tiện lợi cho người dùng.
  - Xây dựng cơ chế cảnh báo và thông báo khi phát hiện truy cập trái phép hoặc bất thường.
  - Đảm bảo tính ổn định và độ tin cậy của hệ thống trong điều kiện hoạt động thực tế, bao gồm cả khả năng hoạt động khi mất kết nối internet.
  - Tối ưu hóa hiệu năng của hệ thống, giảm thiểu độ trễ trong quá trình xác thực và phản hồi.

#### **1.2.5. Đối tượng nghiên cứu**

- Công nghệ Internet of Things (IoT) ứng dụng trong hệ thống kiểm soát truy cập:

- Kiến trúc hệ thống IoT phù hợp cho ứng dụng an ninh cửa
- Giao thức truyền thông và kết nối giữa các thiết bị trong hệ thống
- Giải pháp xử lý dữ liệu phân tán và tích hợp
- Các phương thức xác thực đa dạng:
  - Công nghệ nhận dạng vân tay và thuật toán so khớp
  - Hệ thống mật khẩu số và cơ chế bảo mật
  - Công nghệ RFID trong kiểm soát truy cập
- Hệ thống web server chạy local và công nghệ mở rộng truy cập từ xa:
  - Kiến trúc và phát triển web server nhẹ cho thiết bị IoT
  - Công nghệ ngrok và phương pháp tạo tunnel an toàn ra internet
  - Cơ chế xác thực và phân quyền trong truy cập từ xa
- Hệ thống lưu trữ và quản lý dữ liệu:
  - Cơ sở dữ liệu cho thiết bị IoT giới hạn tài nguyên
  - Phương pháp ghi nhật ký hoạt động theo thời gian thực
  - Giải pháp sao lưu và đồng bộ hóa dữ liệu
- Quy trình phát triển và kiểm thử hệ thống IoT cho an ninh:
  - Phương pháp thiết kế và triển khai cho thiết bị giới hạn tài nguyên
  - Kỹ thuật kiểm thử đảm bảo độ tin cậy của hệ thống
  - Quy trình đánh giá hiệu năng và tối ưu hóa

#### **1.2.6. Phạm vi nghiên cứu**

Nghiên cứu và phát triển hệ thống phần cứng: Tập trung vào việc lựa chọn, thiết kế và tích hợp các thành phần phần cứng chuyên dụng cho hệ thống kiểm soát truy cập, bao gồm bộ vi điều khiển trung tâm (như ESP32, Raspberry Pi), cảm biến vân tay có độ chính xác cao, đầu đọc thẻ RFID, bàn phím mật khẩu số, khóa điện từ, các cảm biến phụ trợ (cảm biến trạng thái cửa, cảm biến chuyển động), hệ thống cung cấp năng lượng và giải pháp dự phòng khi mất điện.

Phát triển kiến trúc phần mềm: Thiết kế và xây dựng kiến trúc phần mềm module hóa, bao gồm firmware cho bộ vi điều khiển, middleware xử lý logic kiểm soát truy cập, hệ thống quản lý cơ sở dữ liệu người dùng và nhật ký, giao diện web cho phép quản trị hệ thống, và các API giao tiếp giữa các thành phần.

Nghiên cứu giao thức kết nối và truyền thông: Đánh giá và lựa chọn các giao thức truyền thông phù hợp cho hệ thống IoT như MQTT, CoAP, HTTP/HTTPS, WebSocket, đảm bảo giao tiếp ổn định và hiệu quả giữa các thành phần trong hệ thống và với môi trường bên ngoài.

Phát triển thuật toán xác thực đa phương thức: Nghiên cứu và triển khai các thuật toán xử lý và so khớp vân tay, các cơ chế xác thực và quản lý mật khẩu, giao thức xử lý thẻ RFID, cùng với khả năng kết hợp các phương thức xác thực theo cấu hình linh hoạt.

Phát triển hệ thống web server local và truy cập từ xa: Xây dựng giải pháp web server nhẹ chạy trên thiết bị điều khiển trung tâm, tối ưu hóa cho tài nguyên giới hạn, tích hợp công nghệ ngrok hoặc tương tự để mở rộng khả năng truy cập từ xa qua internet một cách an toàn.

### **1.2.7. Phương pháp nghiên cứu**

Sử dụng các tài liệu trực tuyến về "kiểm soát truy cập cửa dựa trên IoT" kết hợp với việc thực hành lập trình và triển khai phần cứng để hiểu cách thức kết nối và hoạt động của các thiết bị hay đối tượng nghiên cứu sử dụng trong đề tài này. Phương pháp sẽ bao gồm:

- Tổng quan tài liệu về các hệ thống bảo mật IoT hiện có
- Tạo mẫu với vi điều khiển ESP32/ESP8266
- Kiểm tra các cơ chế xác thực khác nhau
- Đánh giá lỗ hổng bảo mật
- Đánh giá trải nghiệm người dùng

Dự án này sẽ chuyển đổi khái niệm bảng điều khiển thông minh ban đầu thành một hệ thống kiểm soát truy cập cửa và bảo mật toàn diện tận dụng công nghệ IoT.

### **1.2.8. Nội dung đề tài**

Đề tài được triển khai theo các nội dung chính như sau:

- Phần mở đầu: Khái quát sơ lược về đề tài
- Phần nội dung: Triển khai nội dung dự án
  - Chương 1: Giới thiệu đề tài
  - Chương 2: Phân tích yêu cầu
  - Chương 3: Những kiến thức liên quan
  - Chương 4: Ứng dụng

- Phần kết luận: Nhận xét, đánh giá hệ thống, nêu lên những ưu điểm, hạn chế và hướng phát triển trong

## **PHẦN NỘI DUNG**

### **CHƯƠNG 1: GIỚI THIỆU**

#### **1.1. Chức năng chính**

- Mở khóa bằng vân tay: Sử dụng cảm biến vân tay để xác thực người dùng, đảm bảo độ an toàn cao và tránh việc bị sao chép như chìa khóa truyền thống.
- Mở khóa bằng mật khẩu: Nhập mã PIN thông qua bàn phím điện tử, giúp người dùng dễ dàng truy cập mà không cần mang theo thiết bị.
- Mở khóa bằng thẻ RFID: Hệ thống hỗ trợ thẻ từ (RFID) giúp thao tác nhanh chóng, phù hợp với các văn phòng, cơ quan sử dụng thẻ nhân viên.
- Mở khóa từ xa qua Internet (Ngrok): Sử dụng dịch vụ ngrok để tạo đường dẫn công khai từ mạng cục bộ (localhost) lên Internet. Nhờ đó, người dùng có thể mở cửa từ xa thông qua điện thoại hoặc trình duyệt, dù không có mặt tại chỗ.

#### **1.2. Tính năng nổi bật**

- Đa dạng phương thức xác thực: Cho phép người dùng lựa chọn hoặc kết hợp nhiều cách mở khóa, tăng tính linh hoạt và bảo mật.
- Lưu trữ và quản lý người dùng: Có thể thêm/xóa dấu vân tay, mật khẩu hoặc thẻ RFID thông qua giao diện điều khiển.
- Giao diện điều khiển qua web/mobile: Kết hợp với ngrok và ứng dụng web giúp người dùng mở khóa, xem lịch sử truy cập từ xa.
- Bảo mật cao: Mỗi người dùng có một mã định danh riêng. Dữ liệu vân tay và mật khẩu được mã hóa.

#### **1.3. Ứng dụng thực tế**

Hệ thống kiểm soát truy cập và an ninh cửa dựa trên IoT mà chúng ta đang nói tới không chỉ là một sản phẩm công nghệ đơn lẻ, mà còn mang trong mình tiềm năng ứng dụng rộng lớn, có thể thay đổi cách thức quản lý ra vào tại nhiều loại hình không gian khác nhau. Đầu tiên và phổ biến nhất phải kể đến việc tích hợp vào nhà ở thông minh. Hệ thống này hoàn toàn có khả năng thay thế các loại khóa cửa truyền thống rườm rà bằng một giải pháp

khóa thông minh hiện đại. Nhờ đó, chủ nhà và các thành viên gia đình có thể mở cửa một cách tiện lợi chỉ bằng vân tay, thẻ RFID hoặc mã PIN cá nhân, loại bỏ nỗi lo quên hay mất chìa khóa. Hơn nữa, tính năng kết nối IoT cho phép chủ nhà cấp quyền truy cập tạm thời hoặc mở cửa từ xa cho khách hoặc người thân thông qua một ứng dụng di động, đồng thời ghi lại chi tiết lịch sử ra vào, giúp tăng cường khả năng giám sát an ninh ngôi nhà ngay cả khi không có mặt tại đó. Hệ thống cũng có thể được tích hợp sâu hơn vào mạng lưới nhà thông minh, tự động kích hoạt các ngữ cảnh khác như bật đèn, điều chỉnh nhiệt độ khi cửa được mở bởi người dùng hợp lệ.

Bên cạnh ứng dụng dân dụng, hệ thống rất phù hợp cho môi trường văn phòng và các cơ sở kinh doanh nhỏ. Tại đây, việc kiểm soát ai được phép ra vào, khi nào là yếu tố then chốt để đảm bảo an ninh và quản lý hiệu quả. Hệ thống cho phép hạn chế người lạ tiếp cận các khu vực quan trọng, chỉ cấp quyền truy cập cho nhân viên có thẩm quyền. Đặc biệt, bằng cách ghi lại thời gian ra vào của từng người dùng thông qua các phương thức xác thực, hệ thống có thể kiêm nhiệm chức năng quản lý chấm công một cách tự động và chính xác. Nó cũng giúp kiểm soát việc ra vào các phòng ban cụ thể như phòng máy chủ chứa dữ liệu nhạy cảm hay kho tài liệu mật. Việc sử dụng khóa điện tử thông minh thay thế chìa khóa vật lý truyền thống còn giúp giảm thiểu đáng kể chi phí liên quan đến việc sao chép, quản lý và xử lý khi mất chìa khóa, đồng thời giảm rủi ro an ninh khi nhân viên nghỉ việc.

Mở rộng ra các môi trường chuyên biệt hơn, hệ thống kiểm soát truy cập này cũng rất hữu ích trong các phòng thí nghiệm, xưởng sản xuất hay kho bãi và khu vực lưu trữ. Tại những nơi này, nhu cầu kiểm soát ra vào thường rất nghiêm ngặt do liên quan đến hóa chất nguy hiểm, thiết bị đắt tiền, hoặc các bí mật công nghệ cần được bảo vệ. Hệ thống đảm bảo rằng chỉ những người có thẩm quyền, được đào tạo và cấp quyền mới có thể tiếp cận các khu vực này, nâng cao sự an toàn và bảo mật. Đối với kho bãi, việc ghi lại lịch sử ra vào chi tiết còn hỗ trợ đắc lực cho công tác quản lý hàng hóa và kiểm kê.

Không chỉ giới hạn ở các không gian cố định lâu dài, hệ thống còn mang lại giải pháp quản lý linh hoạt cho các môi trường có lượng người ra vào thay đổi thường xuyên như trường học, thư viện hay các mô hình căn hộ cho thuê, homestay. Trong trường học, hệ thống có thể được sử dụng để kiểm soát ra vào phòng máy tính, phòng lab, thư viện, hoặc ký túc xá, phân quyền dựa trên vai trò (học sinh, sinh viên, giáo viên) và lịch trình cụ



thể. Đối với căn hộ cho thuê hay homestay, hệ thống cho phép người quản lý cấp quyền truy cập tạm thời cho khách thuê một cách dễ dàng qua mạng, và quan trọng là có thể thu hồi quyền truy cập ngay lập tức khi khách trả phòng mà không cần phải can thiệp trực tiếp vào ổ khóa hay lo ngại về việc khách giữ lại chìa khóa vật lý.

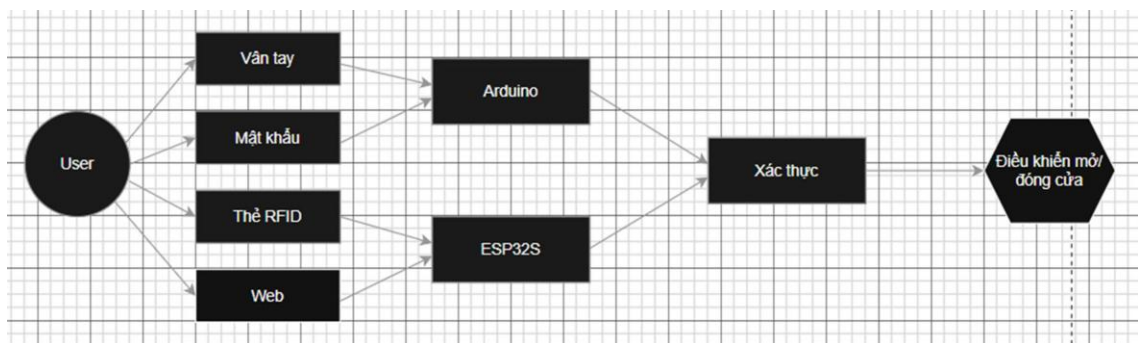
## CHƯƠNG 2: PHÂN TÍCH YÊU CẦU

### 2.1. Yêu cầu hệ thống

- Xác thực và kiểm soát truy cập: Hệ thống phải hỗ trợ nhiều phương thức xác thực người dùng để đảm bảo tính linh hoạt và bảo mật cao:
  - Xác thực sinh trắc học: Hệ thống phải có khả năng nhận dạng vân tay với độ chính xác tối thiểu 95%, thời gian phản hồi không quá 2 giây. Cảm biến vân tay cần có khả năng lưu trữ ít nhất 10 mẫu vân tay khác nhau.
  - Xác thực qua thẻ RFID: Hệ thống cần hỗ trợ đọc thẻ RFID chuẩn 13.56MHz (Mifare) với khoảng cách đọc tối thiểu 5cm. Mỗi thẻ RFID phải được liên kết với một ID người dùng duy nhất trong cơ sở dữ liệu.
  - Xác thực bằng mật khẩu: Bàn phím số phải cho phép người dùng nhập mật khẩu có độ dài 4-8 chữ số. Hệ thống cần hỗ trợ tính năng mật khẩu một lần (OTP) cho khách và mật khẩu khẩn cấp cho tình huống đặc biệt.
- Quản lý người dùng: Hệ thống cần cung cấp các chức năng quản lý người dùng toàn diện:
  - Đăng ký người dùng mới: Quản trị viên phải có khả năng thêm người dùng mới vào hệ thống, bao gồm thu thập dữ liệu vân tay, cấp phát thẻ RFID, và thiết lập mật khẩu ban đầu.
  - Xóa người dùng: Hệ thống phải cho phép xóa hoàn toàn thông tin của người dùng khỏi cơ sở dữ liệu khi cần thiết, với xác nhận bổ sung để tránh xóa nhầm.
  - Chỉnh sửa thông tin người dùng: Quản trị viên cần có khả năng cập nhật thông tin người dùng như tên, phân quyền, mật khẩu, hoặc cập nhật mẫu vân tay.
- Điều khiển cơ chế khóa: Hệ thống cần điều khiển cơ chế khóa một cách chính xác và an toàn:
  - Mở khóa tự động: Sau khi xác thực thành công, hệ thống phải tự động kích hoạt cơ chế mở khóa trong thời gian không quá 1 giây.
  - Khóa tự động: Hệ thống phải tự động khóa lại cửa sau một khoảng thời gian có thể cấu hình (mặc định là 7 giây).
  - Điều khiển từ xa: Quản trị viên phải có khả năng điều khiển khóa từ xa thông qua ứng dụng di động hoặc giao diện web trong trường hợp khẩn cấp.

- Yêu cầu về bảo mật
  - Mã hóa dữ liệu: Tất cả dữ liệu nhạy cảm (mẫu vân tay, mật khẩu) phải được mã hóa khi lưu trữ và truyền tải với chuẩn mã hóa tối thiểu AES-256.
  - Bảo vệ chống tấn công vật lý: Các thành phần phần cứng phải được bảo vệ trong vỏ chống phá hoại, với cảm biến phát hiện khi có nỗ lực mở vỏ trái phép.
- Giao diện phần cứng
  - Màn hình hiển thị: Hệ thống phải có màn hình LCD tối thiểu 16x2 ký tự hoặc màn hình OLED/TFT có độ phân giải đủ để hiển thị thông tin trạng thái và hướng dẫn người dùng.
  - Phản hồi âm thanh: Hệ thống phải cung cấp phản hồi âm thanh khác nhau cho các sự kiện như xác thực thành công, xác thực thất bại, hoặc cảnh báo.
  - Bàn phím: Bàn phím số phải có độ bền cao.
- Giao diện web: Hệ thống phải cho phép quản trị viên:
  - Xem trạng thái hệ thống theo thời gian thực
  - Quản lý người dùng (thêm, xóa, chỉnh sửa)
  - Xem nhật ký truy cập
  - Điều khiển khóa từ xa

## 2.2. Sơ đồ nguyên lý



Hệ thống kiểm soát ra vào thông minh (Door Access Control and Security System) ứng dụng công nghệ IoT được thiết kế để tăng cường bảo mật và tự động hóa việc mở/đóng cửa. Sơ đồ nguyên lý thể hiện một cách rõ ràng luồng dữ liệu từ người dùng đến các thiết bị xử lý, cho đến khi lệnh mở cửa được kích hoạt. Người dùng có thể tương tác với hệ thống thông qua nhiều hình thức xác thực như: quét vân tay, nhập mật khẩu, quét thẻ RFID, hoặc truy cập từ xa qua giao diện web.

Cụ thể, dữ liệu vân tay và mặt khẩu sẽ được gửi đến Arduino, đóng vai trò là bộ xử lý trung gian. Arduino thực hiện kiểm tra sơ bộ, sau đó chuyển thông tin đến khối xác thực trung tâm. Trong khi đó, các dữ liệu từ thẻ RFID và giao diện web sẽ được xử lý thông qua ESP32S, là vi điều khiển hỗ trợ kết nối Wi-Fi và giao tiếp mạng. Thiết bị này không chỉ tiếp nhận thông tin từ thẻ RFID, mà còn có thể đảm nhận chức năng điều khiển và xác thực từ xa thông qua các lệnh gửi qua trình duyệt hoặc ứng dụng di động.

Tất cả thông tin từ Arduino và ESP32S sau đó được đưa vào khối xác thực, nơi dữ liệu được kiểm tra và so sánh với cơ sở dữ liệu người dùng hợp lệ. Nếu xác thực thành công, hệ thống sẽ phát lệnh đến bộ điều khiển cơ cấu chấp hành để thực hiện thao tác mở hoặc đóng cửa. Cơ cấu này có thể là một module relay hoặc servo điều khiển khóa điện, kết hợp với còi báo để cảnh báo khi phát hiện truy cập sai hoặc hành vi bất thường.

### **2.3. Mô tả các bước của hệ thống**

- Cấp nguồn cho hệ thống
- Nhận diện người dùng
- Hiển thị thông tin
- Điều khiển truy cập
- Kết nối mạng qua ESP32S
- Các chức năng khác

## CHƯƠNG 3: NHỮNG KIẾN THỨC LIÊN QUAN

### 3.1. Servo motor SG90



*Hình 1: Động cơ servo SG90*

Động Cơ Servo SG90 là một loại động cơ servo phổ biến được sử dụng rộng rãi trong các ứng dụng điều khiển nhỏ và đơn giản như cánh tay robot, điều khiển mô hình, các hệ thống tự động hóa nhỏ và các dự án điện tử. Những ưu điểm chính của Servo SG90 bao gồm:

- Tốc độ phản ứng nhanh, chính xác
- Tích hợp sẵn driver điều khiển động cơ
- Dễ dàng điều khiển góc quay chính xác thông qua phương pháp điều độ rộng xung PWM
- Kích thước nhỏ gọn, phù hợp với các dự án có không gian hạn chế
- Tiêu thụ điện năng thấp
- Khả năng lắp đặt đơn giản

#### **3.1.1 Thông số kỹ thuật**

- Khối lượng: 9g (siêu nhẹ)
- Kích thước: 23mm × 12.2mm × 29mm
- Momen xoắn: 1.8kg/cm (lực xoắn đủ để di chuyển các đối tượng nhỏ)

- Tốc độ hoạt động: 60 độ trong 0.1 giây (phản hồi nhanh)
- Điện áp hoạt động: 4.8V (khoảng 5V, tương thích với hầu hết các vi điều khiển)
- Nhiệt độ hoạt động: 0°C – 55°C
- Góc quay: Thường là 180 độ ( $\pm 90$  độ từ vị trí trung tâm)
- Độ chính xác: Khoảng 1-2 độ trong điều kiện hoạt động bình thường
- Chu kỳ tín hiệu PWM: 20ms (50Hz)
- Độ rộng xung điều khiển: 1ms - 2ms (tương ứng với góc  $-90^\circ$  đến  $+90^\circ$ )

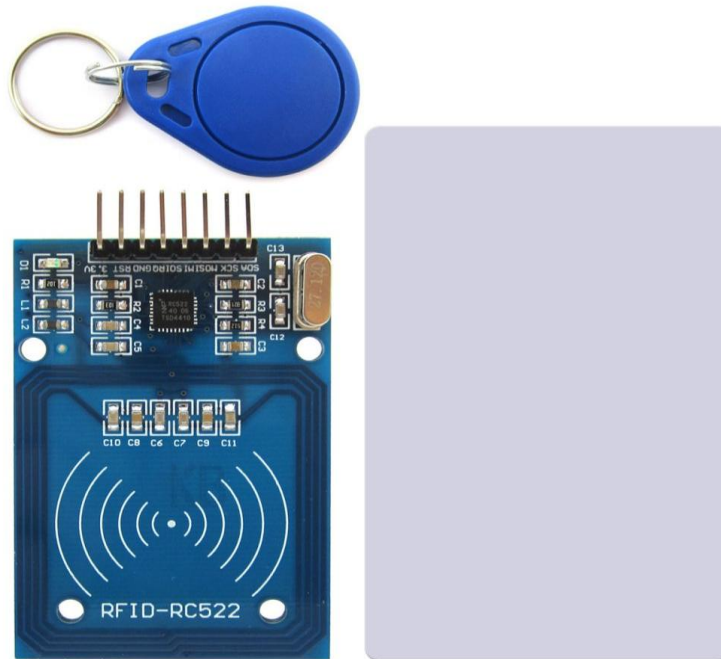
### ***3.1.2. Chức năng các chân***

Đối với Servo SG90, động cơ servo này bao gồm một đầu nối loại S phổ quát điều đó sẽ có thể phù hợp với hầu hết các thiết bị thương mại. Nó được tạo thành từ 3 dây với màu sắc xác định những gì mỗi dây được sử dụng để:

- Đỏ: là cấp nguồn dương hoặc Vcc (+)
- Nâu: là cấp nguồn âm (-) hay GND (nối đất)
- Cam: nó là cấp mang tín hiệu PPM (Điều chế vị trí xung) để điều khiển động cơ servo

## 3.2. RFID

### 3.2.1. Giới thiệu RFID



Hình 2: RC522 MFRC-522 RFID Module

**RFID (Radio Frequency Identification)** là công nghệ sử dụng sóng radio để truyền tải thông tin giữa nhãn (thẻ) và đầu đọc, giúp theo dõi và quản lý sản phẩm nhanh chóng. Nguyên Tuấn cung cấp dịch vụ **in thẻ RFID** với nhiều loại khác nhau, phù hợp với nhu cầu đa dạng của khách hàng

### 3.2.2. Thông số kỹ thuật

- Điện áp nuôi: 3.3V:
- Dung điện nuôi :13-26mA
- Tần số hoạt động: 13.56MHz
- Khoảng cách hoạt động: 0 – 60 mm
- Cổng giao tiếp: SPI, tốc độ tối đa 10Mbps
- Kích thước: 40mm X 60mm
- Có khả năng đọc và ghi

### 3.3. ESP32-DevKitC



*Hình 3: ESP32-DevKitC sử dụng module ESP-WROOM 1*

**ESP32-DevKitC sử dụng module ESP-WROOM-32** có SoC trung tâm là ESP32 tích hợp Wifi, Bluetooth.

Với ưu điểm là cách sử dụng dễ dàng, ra chân đầy đủ, tích hợp mạch nạp và giao tiếp UART CP2102, **ESP32-DevKitC** là lựa chọn số 1 cho các bạn bắt đầu nghiên cứu ESP32.

#### 3.3.1. Ưu điểm

Tiết kiệm chân cho vi điều khiển

Dễ dàng kết nối với LCD

#### 3.3.2. Thông số kỹ thuật

Module: ESP-WROOM-32

Flash: 4 MB

Nguồn cung cấp: 5V DC thông qua cổng micro USB.

Tích hợp mạch nạp và giao tiếp UART CP2102.

Tích hợp ngoại vi: LED Status, BOOT, ENABLE.



Kích thước: 28.33 x 51.45mm

### 3.4. LCD 16x02 và Module I2C

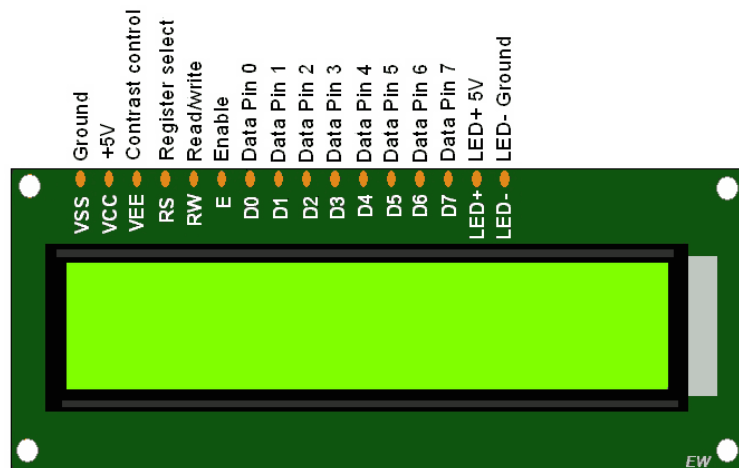
#### 3.4.1. Giới thiệu LCD 16x02



Hình 4: Màn hình LCD 1602

Ngày nay, thiết bị hiển thị LCD (Liquid Crystal Display) được sử dụng trong rất nhiều các ứng dụng của VDK. LCD có rất nhiều ưu điểm so với các dạng hiển thị khác: Nó có khả năng hiển thị kí tự đa dạng, trực quan (chữ, số và kí tự đồ họa), dễ dàng đưa vào mạch ứng dụng theo nhiều giao thức giao tiếp khác nhau, tốn rất ít tài nguyên hệ thống và giá thành rẻ ...

#### 3.4.2. Thông số kỹ thuật



Hình 5: LCD 1602 xanh lá 1

- Điện áp MAX : 7V
- Điện áp MIN : - 0,3V
- Hoạt động ổn định : 2.7-5.5V
- Điện áp ra mức cao : > 2.4
- Điện áp ra mức thấp : <0.4V
- Dòng điện cấp nguồn : 350uA - 600uA
- Nhiệt độ hoạt động : - 30 - 75 độ C

### 3.4.3. Chức năng các chân LCD

Chân số 1 - VSS : chân nối đất cho LCD được nối với GND của mạch điều khiển

- Chân số 2 - VDD : chân cấp nguồn cho LCD, được nối với VCC=5V của mạch điều khiển

- Chân số 3 - VE : điều chỉnh độ tương phản của LCD

- Chân số 4 - RS : chân chọn thanh ghi, được nối với logic "0" hoặc logic "1":

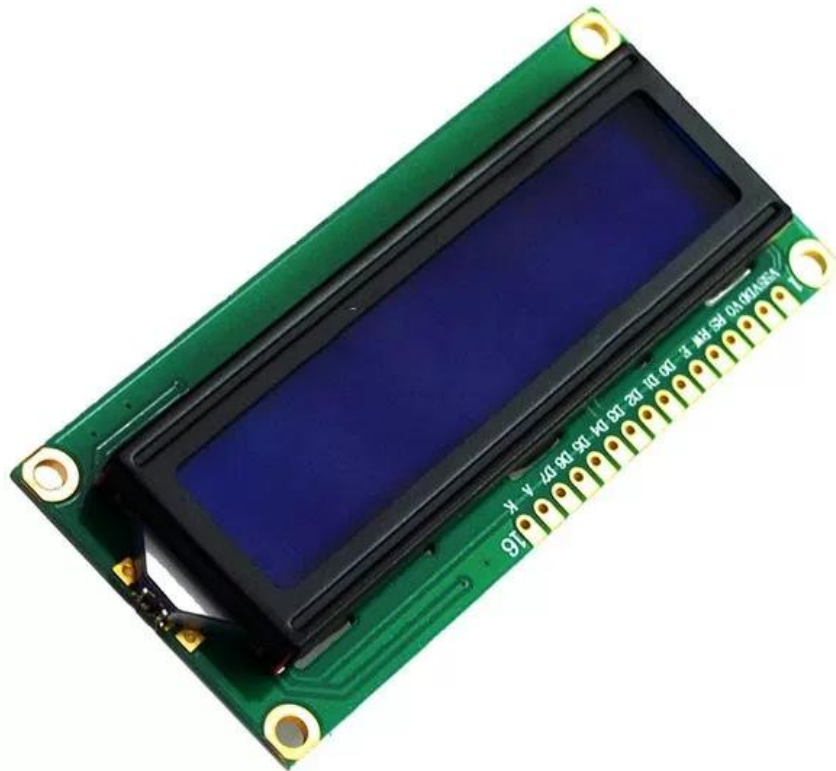
+ Logic "0": Bus DB0 - DB7 sẽ nối với thanh ghi lệnh IR của LCD (ở chế độ "ghi"- write) hoặc nối với bộ đếm địa chỉ của LCD (ở chế độ "đọc" - read)

Logic "1": Bus DB0 - DB7 sẽ nối với thanh ghi dữ liệu DR bên trong LCD

- Chân số 5 - R/W : chân chọn chế độ đọc/ghi (Read/Write), được nối với logic "0" để ghi hoặc nối với logic "1" đọc

- Chân số 6 - E : chân cho phép (Enable). Sau khi các tín hiệu được đặt lên bus DB0-DB7, các lệnh chỉ được chấp nhận khi có 1 xung cho phép của chân này như sau:

- + Ở chế độ ghi: Dữ liệu ở bus sẽ được LCD chuyển vào thanh ghi bên trong khi phát hiện một xung (high-to-low transition) của tín hiệu chân E
- + Ở chế độ đọc: Dữ liệu sẽ được LCD xuất ra DB0-DB7 khi phát hiện cạnh lên (low-to-high transition) ở chân E và được LCD giữ ở bus đến khi nào chân E xuống mức thấp



*Hình 6: CD 1602 Xanh dương 5v*

- Chân số 7 đến 14 - D0 đến D7: 8 đường của bus dữ liệu dùng để trao đổi thông tin với MPU. Có 2 chế độ sử dụng 8 đường bus này là: Chế độ 8 bit (dữ liệu được truyền trên cả 8 đường, với bit MSB là bit DB7) và Chế độ 4 bit (dữ liệu được truyền trên 4 đường từ DB4 tới DB7, bit MSB là DB7)
- Chân số 15 - A : nguồn dương cho đèn nền
- Chân số 16 - K : nguồn âm cho đèn nền

### 3.5 Module I2C

#### 3.5.1. Tại sao sử dụng Module I2C



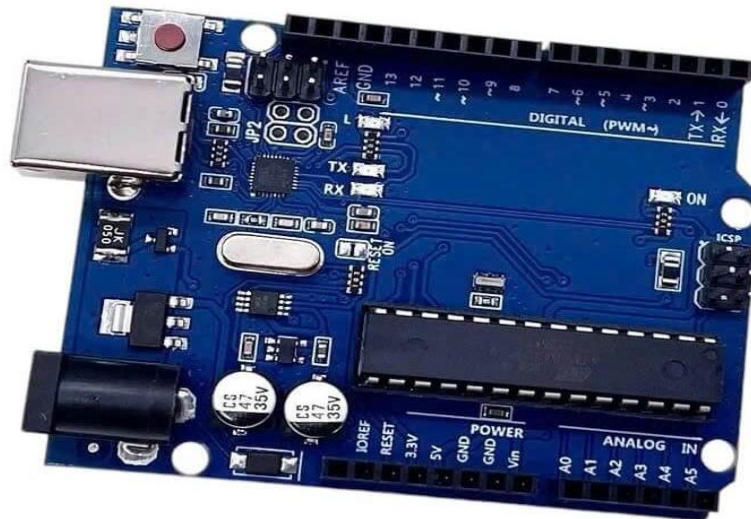
*Hình 7: Mạch Chuyển Đổi Giao Tiếp I2C Cho LCD 1*

Để sử dụng các loại LCD có driver là HD44780 (LCD 1602, LCD 2004, ...) cần có ít nhất 6 chân của MCU kết nối với các chân RS, EN, D7, D6, D5 và D4 để có thể giao tiếp với LCD. Nhưng với module chuyển giao tiếp LCD sang I2C, chúng ta chỉ cần hai chân (SDA và SCL) của MCU kết nối với hai chân (SDA và SCL) của module để có thể hiển thị thông tin lên LCD. Ngoài ra có thể điều chỉnh được độ tương phản bởi biến trở gắn trên module.

#### 3.5.2. Thông số kỹ thuật

- Điện áp hoạt động: 2.5-6V DC.
- Hỗ trợ màn hình: LCD1602,1604,2004 (driver HD44780).
- Giao tiếp: I2C.
- Địa chỉ mặc định: 0X27 (có thể điều chỉnh bằng ngắn mạch chân A0/A1/A2).
- Tích hợp Jump chót để cung cấp đèn cho LCD hoặc ngắt.
- Tích hợp biến trở xoay điều chỉnh độ tương phản cho LCD.

### 3.6. Arduino



*Arduino Uno R3 1*

**Arduino Uno** là một bo mạch vi điều khiển dựa trên chip Atmega328P. Uno có 14 chân I/O digital ( trong đó có 6 chân xuất xung PWM), 6 chân Input analog, 1 thạch anh 16MHz, 1 cổng USB, 1 jack nguồn DC, 1 nút reset.

Uno hỗ trợ đầy đủ những thứ cần thiết để chúng ta có thể bắt đầu làm việc.

Cầm board mạch trên tay, thông qua sơ đồ cấu trúc, chúng ta sẽ biết vùng cấp nguồn, các chân digital, chân analog, đèn báo hiệu, reset ... trên đó.

### **3.6.1. Thông số kỹ thuật**

Chip	Arduino
Chip điều khiển chính:	ATmega328P
Chip nạp và giao tiếp UART	ATmega16U2
Nguồn nuôi mạch	5VDC từ cổng USB hoặc nguồn ngoài cắm từ giắc tròn DC (nếu sử dụng nguồn ngoài từ giắc tròn DC Hshop.vn khuyên bạn nên cấp nguồn từ 6~9VDC để đảm bảo mạch hoạt động tốt, nếu bạn cắm 12VDC thì IC ổn áp rất nóng, dễ cháy và gây hư hỏng mạch).

Số chân Digital I/O	14 (trong đó 6 chân có khả năng xuất xung PWM)
Số chân PWM Digital I/O	6
Số chân Analog Input	6
Dòng điện DC Current trên mỗi chân I/O	20 mA
Dòng điện DC Current chân 3.3V	50 mA
Flash Memory	32 KB (ATmega328P), 0.5 KB dùng cho bootloader
SRAM	2 KB (ATmega328P)
EEPROM	1 KB (ATmega328P)
Clock Speed	16 MHz
LED_BUILTIN	13
Kích thước	68.6 x 53.4 mm

### 3.7. Khóa điện 12V



*Khóa cửa điện từ 12V 0.1*

Khóa chốt điện từ LY-03 đi kèm gá chốt, có chức năng hoạt động như một ổ khóa cửa sử dụng Solenoid để kích đóng mở bằng điện, được sử dụng nhiều trong nhà thông minh hoặc các loại tủ, cửa phòng, cửa kho,... Khóa chốt điện từ này sử dụng điện áp 12VDC, là loại thường đóng (cửa đóng) với chất lượng tốt, độ bền cao. Khóa có thể sử dụng chung với các mạch chức năng tạo thành một hệ thống thông minh.

#### **3.7.1. Thông số kỹ thuật**

Vật liệu: Thép không gỉ

Nguồn điện: 12V DC

Dòng điện làm việc: 0.35A

Công suất: 4.2W

Yêu cầu nguồn cấp: 12VDC/1A

Kích thước: L54 x D38 x H28

Thời gian cấp nguồn: Thời gian dài, Khi nhiệt độ < 78°C

Trọng lượng: 150g

#### **3.7.2. Chức năng Khóa điện**

Khóa/Mở cửa bằng điện:

Khi cấp nguồn 12V (thường là DC), chốt sẽ thu vào hoặc bật ra (tùy loại thường đóng hay thường mở), cho phép mở cửa.

Khi mất điện, cửa sẽ tự khóa lại (hoặc tự mở – tùy vào loại chốt sử dụng: Fail Safe hay Fail Secure).

Tích hợp với hệ thống điều khiển

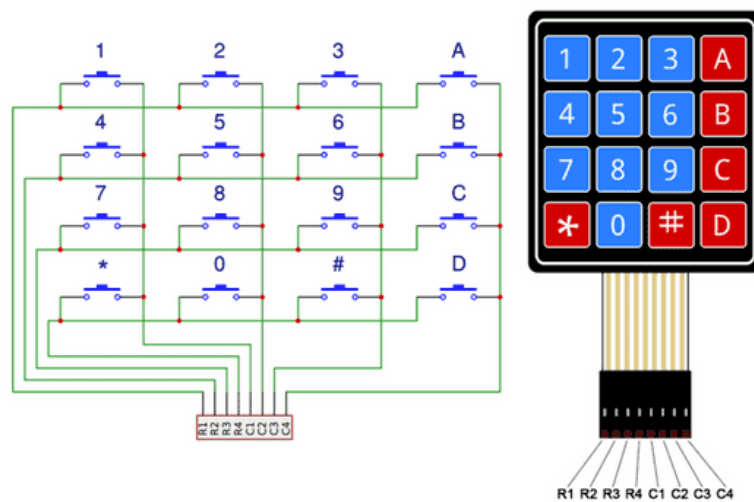
Tăng cường an ninh

Tiết kiệm năng lượng

### **3.8. Giới thiệu Module bàn phím ma trận 4x4**

Ma trận phím 4x4 gồm 16 nút bấm được kết nối thành 4 hàng và 4 cột





**Hình 6 Mô hình bàn phím 4x4**

Để đọc giá trị của phím bấm ta sẽ sử dụng thuật toán “quét phím”. Có 2 cách quét phím là quét theo cột hay quét theo hàng. Ở đây ta nói về quét hàng, quét cột cũng hoàn toàn tương tự.

Ta lần lượt xuất tín hiệu mức 0 ra các hàng (khi một hàng là mức 0 thì tất cả các hàng khác phải là mức 1). Sau đó kiểm tra các cột nếu cột nào có mức logic 0 thì phím có tọa độ hàng và cột đó được ấn.

### 3.9. Cảm biến vân tay





Cảm biến nhận dạng vân tay sử dụng giao tiếp UART TTL hoặc USB 1.1 để giao tiếp với Vi điều khiển hoặc kết nối trực tiếp với máy tính (thông qua mạch chuyển USB-UART hoặc giao tiếp USB 1.1). Cảm biến nhận dạng vân tay được tích hợp nhân xử lý nhận dạng vân tay phía trong, tự động gán vân tay với 1 chuỗi data và truyền qua giao tiếp UART ra ngoài nên hoàn toàn không cần các thao tác xử lý hình ảnh, đơn giản chỉ là phát lệnh đọc/ghi và so sánh chuỗi UART nên rất dễ sử dụng và lập trình.

Cảm biến nhận dạng vân tay có khả năng lưu nhiều vân tay cho 1 ID (1 người), thích hợp cho các ứng dụng bảo mật, khóa cửa, sinh trắc học,... Khu vực ứng dụng: Mô-đun vân tay được sử dụng rộng rãi, phù hợp với tất cả các hệ thống nhận dạng vân tay từ cao cấp đến thấp cấp.

### 3.9.1. Thông số kỹ thuật

Chip	Cảm biến vân tay
Điện áp cung cấp	DC 3.8 ~ 7.0V
Màu đèn nền	Xanh
Ánh sáng	ánh sáng dài / nhấp nháy
Dòng hoạt động hiện tại	<60mA
Dòng đỉnh	<85mA
Diện tích phần cảm biến	15 × 17mm
Phương pháp so khớp	Phương pháp so sánh (1: 1) Phương pháp tìm kiếm (1: N)
Loại mô hình	O40
Lưu trữ vân tay	240 vân tay
Mức độ an toàn	3 (từ thấp đến cao: 1,2,3,4,5)
Tỷ lệ chấp nhận sai (FAR)	<0,001% (Mức an toàn 3)
Tỷ lệ từ chối (FRR)	<1,0% (mức bảo mật là 3)
Giao tiếp	UART (mức logic TTL)
Tốc độ baud (UART)	(9600 × N) bps Trong đó N = 1 ~ 12 (mặc định N = 6, tức là 57600bps)

### ***3.9.2. Ứng dụng cảm biến vân tay***

Khóa vân tay, kết sắt, hộp súng, tài chính và các khu vực an ninh khác.

- Các lĩnh vực nhận dạng như hệ thống kiểm soát truy cập, IPC, máy POS , đào tạo lái xe và tham dự.
- Các khu vực quản lý như câu lạc bộ tư nhân, phần mềm quản lý và cấp phép.
- Người nhận Medicare, người nhận tiền hưu trí, thanh toán bằng vân tay và các lĩnh vực tài chính khác.
- Câu lạc bộ tư nhân, phần mềm quản lý, cấp phép và các lĩnh vực quản lý khác.
- Trong các hệ thống khóa cửa vân tay, kết sắt, khu vực tài chính và an ninh khác.
- Hệ thống kiểm soát ra vào, máy tính công nghiệp, đào tạo lái xe, chăm công và các lĩnh vực nhận dạng khác.

## CHƯƠNG 4: ỨNG DỤNG

### 4.1. Mô tả các bước đi

#### 4.1.1. Cấp nguồn cho hệ thống

Bước đầu tiên và quan trọng nhất là cung cấp nguồn điện cho toàn bộ hệ thống. Trung tâm điều khiển, bo mạch Arduino UNO, có thể nhận nguồn từ cổng USB (khi kết nối với máy tính hoặc bộ sạc USB) hoặc thông qua chân Vin, cho phép sử dụng các nguồn điện ngoài phù hợp. Mô-đun ESP32S, yêu cầu điện áp hoạt động 3.3V, được cấp nguồn thông qua một mạch chuyển đổi điện áp chuyên dụng để đảm bảo ổn định và an toàn. Các thiết bị ngoại vi khác như cảm biến vân tay AS608, mô-đun RFID RC522, màn hình LCD, relay điều khiển và bàn phím ma trận (keypad) sẽ được cấp nguồn trực tiếp từ các chân nguồn 5V hoặc 3.3V của Arduino, tùy thuộc vào yêu cầu của từng linh kiện, hoặc có thể sử dụng một nguồn phụ riêng nếu công suất tiêu thụ của hệ thống lớn.

#### 4.1.2. Nhận diện người dùng

Hệ thống cung cấp ba phương thức chính để người dùng đăng nhập và xác thực danh tính, tăng tính linh hoạt và bảo mật.

Sử dụng thẻ RFID (với mô-đun RC522): Người dùng sẽ đưa thẻ RFID của mình lại gần mô-đun RC522. Mô-đun này sẽ đọc mã định danh (ID) duy nhất của thẻ và truyền dữ liệu này đến Arduino UNO thông qua giao tiếp SPI tốc độ cao. Arduino sau đó sẽ so sánh ID nhận được với danh sách các ID thẻ được phép truy cập đã lưu trữ trong bộ nhớ hoặc cơ sở dữ liệu.

Sử dụng cảm biến vân tay (với cảm biến AS608): Người dùng đặt ngón tay lên bề mặt cảm biến vân tay AS608. Cảm biến sẽ chụp lại hình ảnh vân tay và xử lý sơ bộ. Dữ liệu đặc trưng của vân tay (template) sẽ được truyền đến Arduino qua giao tiếp UART. Arduino sẽ nhận dữ liệu này và tiến hành đối chiếu với các mẫu vân tay đã được đăng ký và lưu trữ trước đó để tìm sự trùng khớp.

Sử dụng bàn phím ma trận (Keypad 4x4): Người dùng sẽ nhập mã PIN cá nhân thông qua bàn phím. Arduino sẽ đọc các phím được nhấn, ghép lại thành một chuỗi mã PIN hoàn chỉnh. Sau đó, Arduino sẽ kiểm tra mã PIN vừa nhập này với mã PIN đúng đã được lập trình sẵn hoặc lưu trữ.

Hệ thống sẽ chờ đợi đầu vào từ một trong ba phương thức này.

#### **4.1.3. *Hiển thị thông tin***

Màn hình LCD 16x2 đóng vai trò là giao diện phản hồi chính cho người dùng, hiển thị các thông báo trạng thái và hướng dẫn trong suốt quá trình hoạt động. Các thông báo có thể bao gồm: "Mời nhập mã PIN", "Mời quét thẻ RFID", "Mời đặt ngón tay", "Đang xử lý...", "Xác thực thành công - Cửa mở", "Truy cập bị từ chối", "Vân tay không khớp", "ID thẻ không hợp lệ", "Mã PIN sai", v.v. Màn hình giúp người dùng biết được hệ thống đang ở trạng thái nào và cần thực hiện hành động gì tiếp theo.

#### **4.1.4. *Điều khiển truy cập***

Đây là bước thực thi kết quả của quá trình xác thực. Nếu bất kỳ phương thức xác thực nào (RFID, vân tay, hoặc mã PIN) trả về kết quả thành công, Arduino UNO sẽ kích hoạt bộ relay. Relay hoạt động như một công tắc điện tử công suất lớn, cho phép dòng điện chạy qua để cấp nguồn cho motor điều khiển cửa. Motor này có thể là động cơ servo để điều khiển góc mở/đóng chính xác hoặc động cơ DC để kéo/đẩy chốt cửa. Sau khi cửa được mở thành công và duy trì trạng thái mở trong một khoảng thời gian ngắn đã định (ví dụ vài giây), Arduino sẽ ngắt tín hiệu kích hoạt relay, làm cho relay chuyển về trạng thái ban đầu và ngắt nguồn cấp cho motor, dẫn đến việc cửa tự động đóng lại (hoặc cho phép người dùng đóng thủ công tùy thiết kế cơ khí).

#### **4.1.5. *Kết nối mạng qua ESP32S***

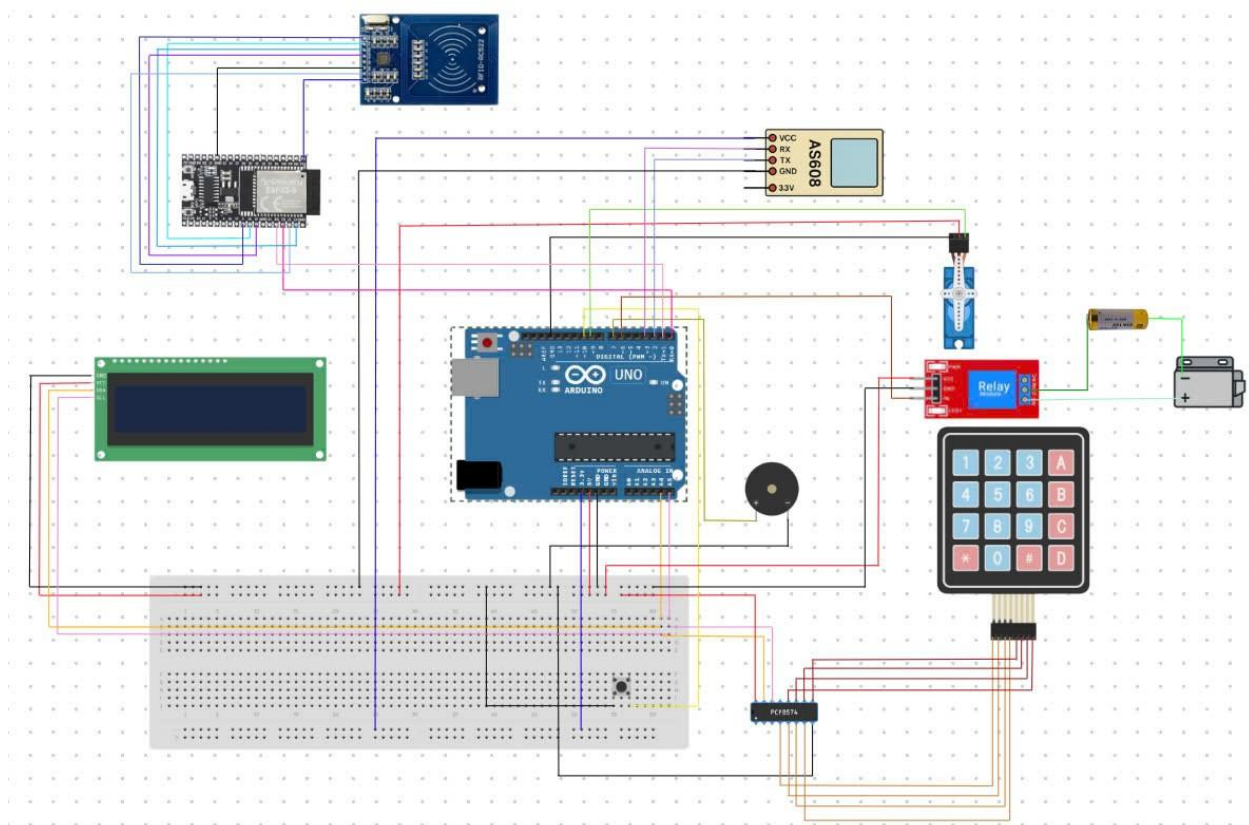
Mô-đun ESP32S được tích hợp vào hệ thống để cung cấp khả năng kết nối mạng (Wi-Fi). ESP32S giao tiếp với Arduino UNO thông qua giao tiếp nối tiếp UART. Sau khi quá trình xác thực diễn ra (thành công hay thất bại), Arduino có thể gửi thông tin về sự kiện này (như ID người dùng, thời gian, kết quả xác thực, phương thức sử dụng) đến ESP32S. ESP32S sau đó sẽ kết nối vào mạng Wi-Fi và gửi dữ liệu này lên một máy chủ (server) từ xa hoặc một nền tảng lưu trữ log trực tuyến. Chức năng này rất hữu ích cho việc giám sát từ xa (kiểm tra ai ra vào, khi nào) hoặc thậm chí cho phép điều khiển cửa từ xa thông qua một ứng dụng trên điện thoại hoặc giao diện web, tùy thuộc vào lập trình trên ESP32S và server.

#### **4.1.6. *Các chức năng khác***

Ngoài các chức năng cốt lõi trên, hệ thống còn bao gồm một số thành phần phụ trợ để cải thiện trải nghiệm người dùng và cung cấp thêm thông tin trạng thái. Buzzer (còi báo)

sẽ phát ra âm thanh để cảnh báo hoặc xác nhận hành động, ví dụ như tiếng bíp khi quét thẻ, tiếng kêu khác nhau cho xác thực thành công hoặc thất bại. Các đèn LED hoặc các mô-đun hiển thị trạng thái đơn giản khác được bố trí trên breadboard hoặc mạch có thể được sử dụng để chỉ báo trực quan trạng thái hoạt động hiện tại của hệ thống.

#### 4.2. Sơ đồ mạch kết nối các phần, các mô-đun



#### 4.3. Chi tiết các bước xây dựng ứng dụng

**Bước 1:** Đăng kí tài khoản và đưa esp32 ra internet bằng ngrok



# Hệ Thống Cửa Thông Minh

Vui lòng đăng nhập để tiếp tục

Tên đăng nhập

 Nhập tên đăng nhập


Mật khẩu

 Nhập mật khẩu

☐ Ghi nhớ đăng nhập

**Đăng nhập →**

© 2025 Smart Door Control System

 [Cấu hình WiFi](#) [Quên mật khẩu?](#) [Cần trợ giúp?](#)

**Bước 2:** Đăng nhập vào trang admin



## Hệ Thống Cửa Thông Minh

Vui lòng đăng nhập để tiếp tục

Tên đăng nhập



admin

Mật khẩu



.....

☒ Ghi nhớ đăng nhập

**Đăng nhập →**

© 2025 Smart Door Control System




[Cấu hình WiFi](#)

[Quên mật khẩu?](#)

[Cần trợ giúp?](#)

**Bước 3:** Vào trang quản trị hệ thống chúng ta có thể bấm nút “Mở cửa” thì trạng thái lúc đó sẽ mở và sau 7 giây thì trạng thái sẽ tự động chuyển qua trạng thái “Đã đóng”

## 1 Điều khiển cửa

 Trạng thái: Đã đóng

 Mở cửa

## Quản lý thẻ RFID


**ⓘ Lưu ý quan trọng:** Việc thêm, xóa và quản lý thẻ RFID, vân tay, và mã PIN phải được thực hiện trực tiếp thông qua giao diện vật lý của Arduino (bàn phím và màn hình LCD). Các chức năng này không có sẵn thông qua giao diện web.

**💡 Hướng dẫn:** Để quản lý thẻ RFID, vui lòng sử dụng menu Admin trên thiết bị Arduino bằng cách nhập mã PIN quản trị viên trên bàn phím.




**Bước 4:** Tiếp theo, chọn thêm người dùng, sau khi thêm người dùng thì sẽ xuất hiện dưới danh sách người dùng và có thể truy cập và dùng




## Quản lý người dùng

 Thêm người dùng

### Danh sách người dùng

Tên đăng nhập	Quyền hạn	Thao tác
admin	<b>Quản trị viên</b>	 Xóa
sin	Người dùng	 Xóa
sin235	<b>Quản trị viên</b>	 Xóa

## Nhật ký hoạt động

Thời gian	Người dùng	Hành động
 Lỗi khi tải nhật ký hoạt động		



## 4.4. Nguy cơ tiềm ẩn

### 4.4.1. Nguy cơ về an ninh

- Lỗi phần cứng:
  - Các cảm biến (RFID, vân tay, bàn phím) có thể bị hỏng do tác động môi trường (ẩm, bụi), hao mòn tự nhiên hoặc lỗi sản xuất.
  - Relay điều khiển cửa có thể bị cháy, kẹt hoặc hỏng do hoạt động quá tải hoặc liên tục trong thời gian dài.
  - Motor dùng để mở/đóng cửa có thể gặp sự cố.
  - Các bo mạch xử lý (Arduino, ESP32) hoặc bộ nguồn gặp trục trặc, hoạt động không ổn định.
- Lỗi phần mềm:
  - Lỗi trong logic xử lý xác thực (ví dụ: thuật toán so khớp vân tay không chính xác, sai sót khi kiểm tra mã PIN).
  - Lỗi trong giao tiếp giữa các module phần cứng (qua các giao thức như UART, SPI).
  - Lỗi quản lý bộ nhớ gây ra tình trạng treo hoặc khởi động lại đột ngột của thiết bị.
  - Lỗi liên quan đến thời gian (ví dụ: cửa mở quá lâu hoặc đóng quá nhanh).
  - Lỗi trong quá trình kết nối mạng, gửi hoặc nhận dữ liệu từ máy chủ.
- Sự cố mạng:
  - Mất kết nối Wi-Fi hoặc internet, ảnh hưởng đến khả năng ghi nhật ký hoạt động lên máy chủ, giám sát và điều khiển hệ thống từ xa.
  - Độ trễ mạng cao làm chậm phản hồi của hệ thống, gây khó chịu cho người dùng.
  - Sự cố nguồn điện:
    - Toàn bộ hệ thống ngừng hoạt động khi nguồn điện chính bị ngắt.
    - Nguồn cấp không đủ công suất để tất cả các thiết bị hoạt động ổn định, đặc biệt khi motor cửa hoạt động.

#### **4.4.2. Nguy cơ về Khả năng sử dụng và Môi trường**

- Lỗi người dùng:
  - Người dùng quên mã PIN, làm mất thẻ RFID, gặp khó khăn khi đặt ngón tay lên cảm biến vân tay do không quen hoặc cảm biến nhạy cảm với điều kiện tay (quá khô/ướt).
  - Thao tác sai cách dẫn đến làm hỏng thiết bị.
  - Yếu tố môi trường:
    - Nhiệt độ quá cao hoặc quá thấp, độ ẩm, bụi bẩn có thể ảnh hưởng đến hoạt động và tuổi thọ của các linh kiện điện tử, đặc biệt là cảm biến vân tay và các kết nối.
    - Hệ thống có thể bị hỏng do va đập vật lý hoặc rung động mạnh.
    - Khó khăn trong cài đặt và bảo trì:
    - Quy trình lắp đặt hệ thống phức tạp, đòi hỏi kiến thức kỹ thuật.
    - Khó khăn trong việc cập nhật phiên bản firmware hoặc sửa lỗi phần mềm khi hệ thống đã được lắp đặt cố định.
    - Việc quản lý người dùng (thêm, xóa, sửa) có thể rườm rà nếu không có giao diện quản lý thuận tiện.

#### **4.5. Cách khắc phục**

##### **4.5.1. Tăng cường an ninh**

- Đối với Xác thực:
  - Sử dụng các thuật toán băm mật mã (cryptographic hashing) để lưu trữ mã PIN thay vì lưu trữ mã PIN gốc.
  - Thiết lập giới hạn số lần thử nhập mã PIN hoặc quét vân tay/thẻ sai liên tiếp trước khi khóa tạm thời quyền truy cập từ phương thức đó.
  - Sử dụng các cảm biến vân tay có khả năng nhận diện tốt và thuật toán so khớp robust, đồng thời làm sạch bề mặt cảm biến định kỳ.
  - Áp dụng các loại thẻ RFID có lớp bảo mật và sử dụng các key riêng để truy cập dữ liệu trên thẻ, thay vì chỉ dựa vào UID dễ bị sao chép.
  - Cân nhắc áp dụng xác thực đa yếu tố (ví dụ: yêu cầu cả thẻ RFID và mã PIN) cho các khu vực an ninh cao.

- Đối với Phần mềm và Firmware:
  - Thực hiện lập trình an toàn (secure coding), kiểm tra chặt chẽ các dữ liệu đầu vào và xử lý các trường hợp ngoại lệ.
  - Mã hóa dữ liệu nhạy cảm (PIN, ID người dùng, mẫu vân tay nếu lưu trữ trên thiết bị) trước khi ghi vào bộ nhớ flash hoặc EEPROM.
  - Triển khai cơ chế cập nhật firmware an toàn qua mạng (OTA - Over-The-Air) với chữ ký số để đảm bảo phiên bản cập nhật không bị giả mạo.
- Đối với Mạng và Giao tiếp:
  - Luôn sử dụng giao thức bảo mật Wi-Fi mạnh nhất hiện có (WPA2 hoặc WPA3) với mật khẩu phức tạp và duy nhất cho mạng của hệ thống.
  - Sử dụng các giao thức truyền dữ liệu an toàn được mã hóa khi giao tiếp với máy chủ.
  - Hạn chế các thông tin nhạy cảm truyền giữa Arduino và ESP32 qua UART, chỉ truyền những dữ liệu cần thiết và đã được xử lý bớt (ví dụ: trạng thái xác thực, không truyền mẫu vân tay thô).
  - Cấu hình tường lửa (firewall) trên mạng hoặc máy chủ để chỉ cho phép các kết nối từ địa chỉ IP hoặc cổng cụ thể.
  - Áp dụng xác thực mạnh mẽ cho các kết nối API hoặc MQTT đến máy chủ.
  - Triển khai cơ chế giới hạn tốc độ yêu cầu (rate limiting) trên máy chủ để chống tấn công DoS ở tầng ứng dụng.
- Đối với Vật lý:
  - Thiết kế và sử dụng vỏ hộp bảo vệ thiết bị chắc chắn, chống phá hoại, khó bị mở ra nếu không có công cụ chuyên dụng.
  - Lắp đặt các thành phần quan trọng như bo mạch điều khiển, relay, và motor ở những vị trí khuất, khó tiếp cận từ bên ngoài.
  - Cân nhắc thêm cảm biến phát hiện cạy phá vỏ hộp và tích hợp chức năng gửi cảnh báo đến người quản lý khi phát hiện can thiệp vật lý.

#### **4.5.2. Nâng cao Độ tin cậy Kỹ thuật và Vận hành**

- Đối với Phần cứng:

- Chọn các linh kiện điện tử, cơ khí (relay, motor) từ các nhà sản xuất uy tín, có thông số kỹ thuật phù hợp với tải và môi trường hoạt động dự kiến.
  - Tính toán kỹ lưỡng công suất nguồn điện cần thiết, sử dụng bộ nguồn ổn định và có các mạch bảo vệ (quá áp, quá dòng).
  - Thiết kế mạch in hoặc bố trí trên breadboard/testboard hợp lý, đảm bảo các kết nối chắc chắn, giảm thiểu nhiễu.
  - Thực hiện hiệu chuẩn hoặc kiểm tra định kỳ cho các cảm biến quan trọng.
- Đối với Phần mềm:
- Áp dụng các kỹ thuật lập trình phòng ngừa (defensive coding), kiểm tra giá trị trả về của các hàm, xử lý các tình huống lỗi (ví dụ: cảm biến không phản hồi, mất kết nối mạng).
  - Sử dụng bộ đếm thời gian giám sát (Watchdog timer) để tự động khởi động lại thiết bị nếu phần mềm bị kẹt.
  - Triển khai cơ chế thử lại (retry mechanism) cho các thao tác giao tiếp ngoại vi hoặc gửi dữ liệu qua mạng có khả năng thất bại tạm thời.
  - Xây dựng hệ thống ghi nhật ký hoạt động và lỗi chi tiết, có thể lưu trữ cục bộ hoặc gửi lên máy chủ để dễ dàng gỡ lỗi (debug) và theo dõi tình trạng hệ thống.
- Đối với Mạng:
- Thiết kế hệ thống có khả năng hoạt động ở chế độ ngoại tuyến cơ bản (chỉ xác thực cục bộ) nếu mất kết nối mạng, và lưu trữ nhật ký tạm thời để đồng bộ sau khi có mạng trở lại.
  - Triển khai cơ chế thông báo (ví dụ: gửi email, tin nhắn push notification qua ứng dụng di động) đến người quản lý khi hệ thống mất kết nối mạng.
  - Đối với Nguồn điện:
  - Sử dụng bộ nguồn dự phòng như pin hoặc bộ lưu điện nhỏ (mini UPS) để duy trì hoạt động của hệ thống trong một khoảng thời gian khi nguồn điện lưới bị ngắt.
  - Thiết kế hệ thống để thực hiện tắt máy an toàn (graceful shutdown) hoặc gửi cảnh báo khi nguồn pin dự phòng yếu.



## PHẦN KẾT LUẬN

### 1. Kết quả đạt được

Hiểu được cấu trúc, nguyên lý hoạt động và cách lập trình cho vi điều khiển ESP32S và Arduino trong ứng dụng IoT.

Nắm vững cách thức hoạt động và giao tiếp với các module/cảm biến cụ thể:

- Màn hình LCD 16x02 qua giao thức I2C.
- Bàn phím số (Keypad) thông qua IC mở rộng I/O PCF8574.
- Cảm biến vân tay AS608 (lấy và so sánh dữ liệu vân tay).
- Đầu đọc thẻ RFID RC522 (đọc UID thẻ).
- Module Relay 5V để điều khiển khóa điện.
- Động cơ Servo SG90 (mô phỏng/hỗ trợ cơ cấu khóa/chốt cửa).

Triển khai thành công hệ thống xác thực đa yếu tố, kết hợp RFID, vân tay và mã PIN để cấp quyền truy cập.

Xây dựng được project hoàn chỉnh trên Arduino IDE, biên dịch và nạp chương trình cho ESP32S và Arduino.

Sử dụng thành công dịch vụ Ngrok để tạo đường hầm (tunnel) bảo mật, thiết lập một endpoint công khai cho phép ESP32S nhận lệnh điều khiển và gửi trạng thái ra internet từ mạng cục bộ.

Xây dựng được chức năng ghi nhật ký truy cập cơ bản và hiển thị trạng thái hệ thống lên màn hình LCD.

### 2. Ưu điểm

Tăng cường An ninh: Hệ thống cung cấp nhiều lớp xác thực (RFID, Vân tay, Mã PIN), nâng cao đáng kể độ an toàn so với khóa cơ truyền thống.

Linh hoạt và Truy cập từ xa: Cho phép người dùng lựa chọn phương thức xác thực phù hợp tại chỗ. Cung cấp khả năng điều khiển (khóa/mở) và giám sát trạng thái cửa từ xa qua internet bằng cách truy cập vào địa chỉ endpoint được cung cấp bởi Ngrok thông qua trình duyệt web hoặc ứng dụng tùy chỉnh.

Khả năng Giám sát: Hệ thống ghi nhận lại lịch sử các lần truy cập, giúp người quản lý dễ dàng theo dõi (thông qua LCD hoặc truyền dữ liệu qua Ngrok).

### 3. Nhược điểm

Cấu hình WiFi Thủ công: Thông tin mạng WiFi (SSID và mật khẩu) đang được nhúng cứng trong code, yêu cầu phải sửa đổi và nạp lại chương trình mỗi khi muốn kết nối vào một mạng WiFi khác.

Giao diện Quản lý Cơ bản: Chức năng quản lý người dùng (thêm/xóa vân tay, thẻ RFID), xem nhật ký chi tiết còn hạn chế, chủ yếu thao tác trực tiếp hoặc qua giao diện đơn giản (Serial Monitor, LCD ). Giao diện điều khiển từ xa qua Ngrok (nếu có) cũng có thể còn đơn giản.

Bảo mật Chuyên sâu: Chưa đi sâu vào các giải pháp bảo mật nâng cao như mã hóa dữ liệu truyền qua tunnel Ngrok (ngoài mã hóa TLS mặc định của Ngrok), chống tấn công replay, bảo vệ vật lý chống giả mạo cảm biến.

Độ trễ: Có thể có độ trễ nhất định khi điều khiển từ xa do tín hiệu phải đi qua nhiều lớp mạng và dịch vụ Ngrok.

Không có điều khiển giọng nói: Hệ thống hiện tại không hỗ trợ điều khiển bằng giọng nói.

### 4. Hướng phát triển đề tài

Một hướng quan trọng là cải thiện khả năng sử dụng và quản lý. Điều này bao gồm việc xây dựng cơ chế cấu hình WiFi linh hoạt (qua WiFi Manager, SmartConfig,...) để dễ dàng kết nối thiết bị mà không cần sửa code. Song song đó, phát triển một giao diện Web hoặc ứng dụng di động chuyên nghiệp là cần thiết để quản lý người dùng (thêm, xóa, sửa), xem lịch sử truy cập chi tiết, cấu hình các tham số hệ thống và điều khiển cửa từ xa một cách trực quan. Giao diện này đóng vai trò trung tâm trong việc vận hành hệ thống sau khi lắp đặt.

Để đảm bảo hệ thống hoạt động ổn định và an toàn qua mạng, cần tập trung vào độ tin cậy của kết nối từ xa và nâng cao bảo mật. Điều này đòi hỏi nghiên cứu các giải pháp thay thế hoặc bổ sung cho Ngrok nhằm có endpoint ổn định hơn (như dịch vụ tunneling trả phí, tự host, DDNS, nền tảng IoT chuyên dụng) và xử lý tự động khi địa chỉ endpoint thay đổi. Quan trọng là thêm cơ chế hoạt động ngoại tuyến cho các chức năng xác thực cơ bản khi mất internet. Về bảo mật, cần triển khai xác thực mạnh hơn cho các lệnh điều khiển từ



xa (dùng token, mật khẩu), mã hóa dữ liệu nhạy cảm lưu trữ trên thiết bị và nghiên cứu biện pháp chống tấn công replay.

Cuối cùng, mở rộng các tính năng cốt lõi sẽ làm tăng giá trị của hệ thống. Có thể tích hợp camera để chụp ảnh người truy cập khi có sự kiện, thêm cảm biến phát hiện cửa bị phá hoại hoặc mở trái phép để tăng cường an ninh, và gửi thông báo đẩy (push notification) đến điện thoại người dùng khi có sự kiện quan trọng (truy cập, cảnh báo). Việc tối ưu hóa mã nguồn để giảm độ trễ và tăng hiệu năng xử lý cũng là một phần của hướng phát triển này.

## TÀI LIỆU THAM KHẢO

1. S., K., S, R., A, K., & M, K. (2025). Biometric and IoT Integration for Secure and Remote Door Access Control Using Fingerprint Recognition and GSM Technology. *E3S Web of Conferences*.
2. Widiartha, K., & Ekayana, A.A. (2020). Design of IOT based facial recognition door access control locker services at tourist attractions in Bali. *Journal of Physics: Conference Series*, 1516.
3. Badashah, D.S., Usha, N.S., Reddy K, B., & G, L. (2022). Automatic Door Access Control System Based on Facial Recognition Using ESP32-CAM. *International Journal for Research in Applied Science and Engineering Technology*.
4. Nasution, A.B., Nugroho, A.Y., Gunawan, H., & Sari, R.E. (2024). Development of an IoT Based Smart Door System with Access Control via WhatsApp. *Indonesian Journal of Applied and Industrial Sciences (ESA)*.
5. Agarwal, A., et al. (2023, August 8). IoT-based Door Security System using IoT Technology. Research Square. <https://assets-eu.researchsquare.com/files/rs-3163015/v1/8736f19b-9002-4729-ade9-88db04b9c300.pdf>
6. Piarsa, I. N., et al. (2024, October). IoT-Based Smart Door Lock System with Fingerprint and Keypad Access. *Journal-ISI*, 11, 2097.
7. Anonymous. (2024, May 31). Door Security System for Home Monitoring Based on IoT. Granthaalayah Publication.
8. Anonymous. (2024, August 28). IoT Door Locking a Review. Semantic Scholar.
9. Anonymous. (2022, May 31). Automatic Door Access Control System Based on Facial Recognition Using ESP32-CAM. Semantic Scholar.
10. Anonymous. (n.d.). IoT Based Door Access Control System Using ESP32CAM. Semantic Scholar.
11. Anonymous. (2023, February 1). Access Control for IoT: A Survey of Existing Research, Dynamic Policies and Future Directions. NCBI.
12. Sowjanya, G. M., & Nagaraju, S. (2016). Design and implementation of door access control and security system based on IoT. 2016 International Conference on Inventive Computation Technologies (ICICT), 2, 1-4.

