

ĐẠI HỌC QUỐC GIA TP HCM
TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN



Môn: VẬT LÝ CHO CÔNG NGHỆ THÔNG TIN

BÁO CÁO

ĐỒ ÁN CUỐI KỲ:

KHÓA CỬA THÔNG MINH

Sinh viên thực hiện: 21127076 – Doãn Anh Khoa

21127143 – Nguyễn Minh Quân

21127537 – Phạm Sĩ Phú

Giảng viên hướng dẫn: Thầy Cao Xuân Nam

Thầy Đặng Hoài Thương

Tp.HCM, ngày 22 tháng 8 năm 2023

MỤC LỤC

I.	Thông tin tổng quan	3
II.	Bảng phân chia công việc.....	3
III.	Mô tả sản phẩm	6
1.	Chức năng của toàn hệ thống.....	6
2.	Sơ đồ truyền nhận dữ liệu	8
IV.	Bản thiết kế 3D	10
V.	Giao diện web và mô tả chức năng.....	15
1.	Tab SIGN IN và tab LOGOUT.....	15
2.	Tab HOME.....	16
3.	Tab HISTORY	17
4.	Tab SECURITY	18
VI.	Giải thích flow NodeRED (mô tả cấu hình/code các Node chính)	19
1.	Đăng nhập vào website	19
2.	Xem các thông tin của thiết bị.....	23
3.	Xem danh sách lịch sử truy cập khóa cửa.....	24
4.	Tạo mật khẩu động và điều khiển thiết bị từ xa.....	27
5.	Đăng xuất khỏi website.....	30
VII.	Nguồn tham khảo	31

I. Thông tin tổng quan

Mã nhóm: NHÓM 4

Thông tin các thành viên:

STT	Họ tên	MSSV
1	Doãn Anh Khoa	21127076
2	Nguyễn Minh Quân (nhóm trưởng)	21127143
3	Phạm Sĩ Phú	21127537

Tên sản phẩm: KHÓA CỬA THÔNG MINH

II. Bảng phân chia công việc

Mục	Công việc	Thành viên phụ trách
A. Chuẩn bị	1. Lên ý tưởng sản phẩm và kế hoạch thực hiện lâu dài.	Nguyễn Minh Quân
	2. Tìm nguồn tham khảo sản phẩm.	Nguyễn Minh Quân
	3. Lập danh sách thiết bị cần thiết.	Doãn Anh Khoa
	4. Tìm hiểu giá thành, mua thiết bị và vật dụng liên quan.	Phạm Sĩ Phú
B. Thiết kế 3D	1. Vẽ phác thảo hình dáng bên ngoài (khung sản phẩm).	Doãn Anh Khoa
	2. Vẽ cấu trúc bên trong sản phẩm (vẽ chi tiết các thiết bị).	Phạm Sĩ Phú

C. Thiết kế sản phẩm thực tế		1. Vẽ chi tiết mạch điện (phân bố dây, thiết bị hợp lý).	Doãn Anh Khoa
		2. Lắp mạch điện thực tế theo cấu trúc bản vẽ.	Nguyễn Minh Quân
		3. Chế tạo sản phẩm thực tế (làm khung sản phẩm, ghép khung và mạch với nhau).	Phạm Sĩ Phú
D. Lập trình	Mạch Arduino Uno R3	1. Lập trình cảm biến vân tay (nhận vân tay, tìm kiếm vân tay, lưu trữ/xóa vân tay).	Nguyễn Minh Quân
		2. Lập trình nhận bàn phím số khi chạy toàn bộ hệ thống.	
		3. Lập trình nhận nút nhấn.	
		4. Lập trình hiển thị nội dung giao tiếp ra màn hình LCD (truy cập đúng/sai/khẩn cấp, cài đặt, tín hiệu kết nối).	
		5. Lập trình các chức năng (admin, thêm mật khẩu, xóa mật khẩu, thêm vân tay, xóa vân tay) của phần cài đặt.	
		6. Lập trình truyền/nhận tín hiệu với mạch Wemos (giao thức UART).	
	Mạch Wemos D1 R2 (ESP-8266)	1. Lập trình âm thanh cho buzzer.	Doãn Anh Khoa
		2. Lập trình truyền tín hiệu cho relay (đóng/ngắt khóa điện).	
		3. Lập trình truyền/nhận dữ liệu với mạch Uno (giao thức UART).	
		4. Lập trình kết nối mạch với Wifi.	
		5. Lập trình kết nối MQTT Server, truyền/nhận dữ liệu với website qua MQTT.	
		6. Lập trình gửi Http Request (gửi request đến IFTTT trong trường hợp khẩn cấp).	

	Website, Cloud, IFTTT	1. Lập trình xử lý các flow trong NodeRED.	Phạm Sĩ Phú
		2. Thiết kế giao diện website.	
		3. Lập trình truyền/nhận dữ liệu qua MQTT Server giữa website và thiết bị.	
		4. Quản lý lưu trữ dữ liệu trên cloud.	
		5. Lập trình truyền/nhận dữ liệu từ website lên cloud và ngược lại.	
		6. Lập trình truyền “http request” từ website lên IFTTT, gửi thông báo cho người dùng.	
E. Báo cáo cuối kỳ		1. Quay video demo sản phẩm.	Nguyễn Minh Quân
			Phạm Sĩ Phú
			Doãn Anh Khoa
		2. Mô tả chức năng toàn bộ hệ thống.	Nguyễn Minh Quân
		3. Vẽ sơ đồ truyền nhận dữ liệu giữa các đối tượng và chú thích.	Doãn Anh Khoa
		4. Trình bày và chú thích bản thiết kế 3D.	Doãn Anh Khoa
		5. Trình bày giao diện web và chức năng của web.	Phạm Sĩ Phú
			Doãn Anh Khoa
		6. Giải thích flow NodeRED.	Phạm Sĩ Phú
			Doãn Anh Khoa
Tỷ lệ % công việc từng thành viên:			
Nguyễn Minh Quân: 34%; Doãn Anh Khoa: 32%; Phạm Sĩ Phú: 34%			

III. Mô tả sản phẩm

1. Chức năng của toàn hệ thống

a. Chức năng của thiết bị:

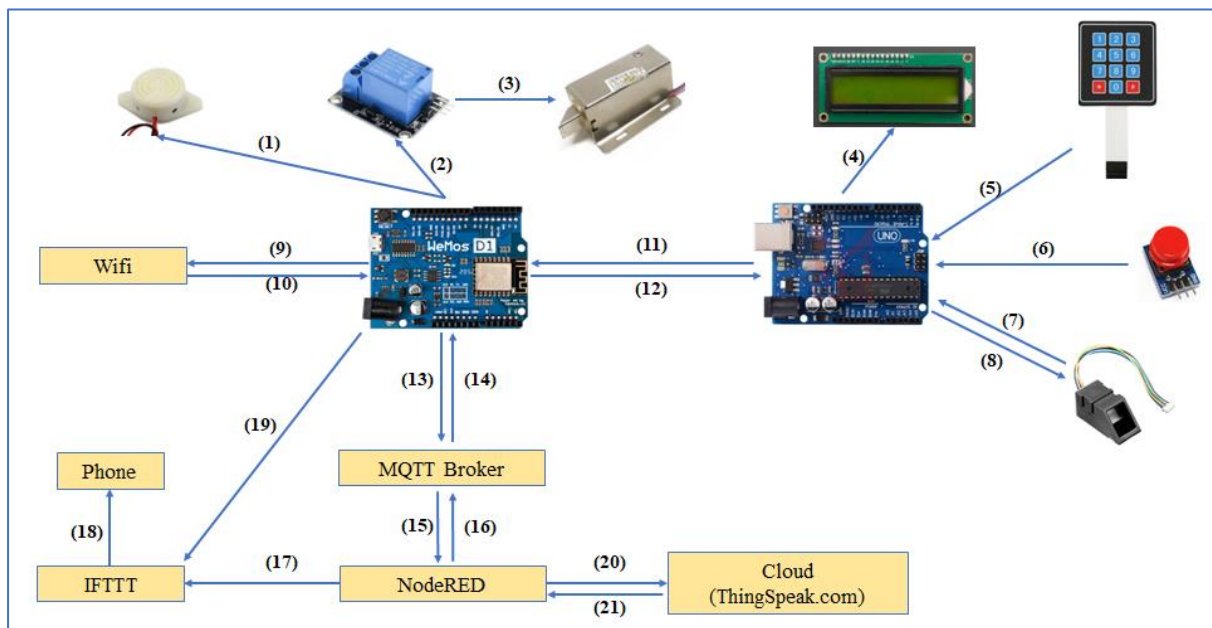
- Có thể chủ động mở khóa cửa từ phía bên trong bằng cách nhấn vào nút nhấn.
- Ở phía bên ngoài sẽ có 1 màn hình LCD, cảm biến vân tay và bàn phím số.
- Người dùng có thể mở khóa cửa bằng vân tay bằng cách đưa ngón tay vào cảm biến hoặc nhập mật khẩu bằng bàn phím số sau đó nhấn '#'. Khi truy cập thành công, màn hình LCD sẽ hiển thị cửa được mở khóa bằng phương thức nào và ID tương ứng.
- Người chủ sở hữu có thể thực hiện các cài đặt sau: Thêm mật khẩu số, Thêm vân tay người dùng, xóa mật khẩu số, xóa vân tay người dùng. Số lượng mật khẩu số tối đa là 5, số lượng vân tay tối đa là 20. Để truy cập vào được chức năng cài đặt cần nhấn tổ hợp phím '*' + '0' + '#' và nhập đúng mật khẩu admin.
- Mật khẩu admin cài đặt mặc định là "1234", mật khẩu này sẽ được cập nhật một lần duy nhất ở lần đầu tiên thêm mật khẩu số mới.
- Ở chức năng cài đặt, màn hình hiển thị những dòng lệnh cụ thể như sau:
 - 1: Thêm người dùng mới:
 - 1: Thêm vân tay
 - 2: Thêm mật khẩu
 - *: Quay lại màn hình trước đó
 - 2: Xóa người dùng:
 - 1: Xóa mật khẩu
 - 2: Xóa vân tay
 - *: Quay lại màn hình trước đó
 - *: Quay lại màn hình nhập mật khẩu
- Bình thường đèn màn hình sẽ tắt, khi có thao tác nhấn phím hoặc vân tay, đèn màn hình sẽ mở lên. Đèn màn hình LCD sẽ tắt khi nhấn 2 lần phím '*'.
- Khi truy cập thành công hoặc nhập sai mật khẩu/vân tay cũng sẽ có âm thanh đúng/sai tương ứng từ buzzer.

- Ngoài ra khi cố gắng truy cập và sai 5 lần liên tục, buzzer sẽ phát ra âm thanh báo động trong 30 giây, đồng thời không cho phép truy cập các thiết bị trong 2 phút tiếp theo và gửi tín hiệu khẩn cấp cho chủ sở hữu.

b. Chức năng chính của Website và Cloud:

- Đăng nhập website để quản lý bằng tài khoản, mật khẩu đã được định sẵn.
- Website hiển thị thông tin cơ bản của thiết bị; hiển thị thiết bị truy cập gần nhất; hiển thị lịch sử mở khóa cửa thông qua phương thức nào và ID nào.
- Website còn có chức năng tạo 1 mật khẩu số ngẫu nhiên (dynamic password) và mật khẩu ấy có hiệu lực trong 3 phút.
- Ngoài ra website cho phép admin mở khóa cửa từ xa (remote) bằng cách nhập đúng mật khẩu admin của thiết bị.
- Cloud sẽ lưu trữ mỗi khi có dữ liệu mới (thời gian truy cập thành công mật khẩu số/vân tay, các ID người dùng), lưu trữ mật khẩu admin của thiết bị phục vụ cho việc mở cửa từ xa, lưu tài khoản và mật khẩu đăng nhập của website.

2. Sơ đồ truyền nhận dữ liệu



Chú thích:

- (1) Buzzer nhận tín hiệu digital (HIGH/LOW) từ mạch Wemos.
- (2) Relay nhận tín hiệu digital (HIGH/LOW) từ mạch Wemos.
- (3) Relay đóng/ngắt điện ở cổng COM, NC để mở/đóng khóa điện.
- (4) Màn hình LCD nhận tín hiệu bật/tắt đèn màn hình và nội dung chuỗi từ mạch Uno để in ra.
- (5) Mạch Uno nhận giá trị char từ trên Keypad.
- (6) Mạch Uno nhận tín hiệu digital (HIGH/LOW) từ Button.
- (7) Mạch Uno nhận vân tay người dùng và bộ nhớ trong Fingerprint.
- (8) Mạch Uno gửi lại vân tay lưu trữ về Fingerprint.
- (9) Mạch Wemos gửi SSID và mật khẩu để kết nối Wifi.
- (10) Mạch Wemos nhận tín hiệu từ Router/điểm truy cập để kết nối Wifi.
- (11) Mạch Wemos nhận dữ liệu từ mạch Uno bao gồm:
 - Ký tự tương ứng (báo hiệu các phương thức truy cập mở khóa).
 - Chuỗi ID tương ứng của mật khẩu số và vân tay khi truy cập thành công.
 - Ký tự tương ứng (báo hiệu truy cập sai).
 - Chuỗi mật khẩu (báo hiệu cập nhật mật khẩu admin).
- (12) Mạch Uno nhận dữ liệu từ mạch Wemos bao gồm:
 - Chuỗi thông báo đã kết nối wifi của ESP8266 để in trên LCD.

- Chuỗi thông báo điều khiển từ xa để in trên LCD.
 - Chuỗi chứa mật khẩu ngẫu nhiên tạo từ website.
 - Ký tự thông báo mật khẩu vừa tạo ngẫu nhiên không còn hợp lệ.
- (13) Mạch Wemos gửi dữ liệu tới MQTT Broker bao gồm:
- Chuỗi chứa mật khẩu admin mặc định “1234” khi setup.
 - Tín hiệu loại phương thức truy cập khóa thành công.
 - Chuỗi ID của mật khẩu số và vân tay khi truy cập thành công.
 - Chuỗi mật khẩu (báo hiệu cập nhật mật khẩu admin).
- (14) Mạch Wemos nhận dữ liệu từ MQTT broker bao gồm:
- Chuỗi thông báo để điều khiển mở cửa từ xa.
 - Chuỗi chứa mật khẩu ngẫu nhiên tạo từ website.
- (15) MQTT Broker gửi lên NodeRED các dữ liệu:
- Chuỗi chứa mật khẩu admin.
 - Tín hiệu loại phương thức truy cập khóa thành công.
 - Chuỗi ID của mật khẩu số và vân tay khi truy cập thành công.
- (16) MQTT Broker nhận từ NodeRED các dữ liệu:
- Chuỗi thông báo để điều khiển mở cửa từ xa.
 - Chuỗi chứa mật khẩu ngẫu nhiên tạo từ website.
- (17) NodeRED gửi “http request” lên IFTTT khi đăng nhập website thành công.
- (18) IFTTT gửi thông báo về điện thoại khi đăng nhập website thành công và khi có tín hiệu khẩn cấp.
- (19) Mạch Wemos gửi “http request” lên IFTTT khi có tín hiệu khẩn cấp.
- (20) NodeRED gửi chuỗi phương thức truy cập thành công, thời gian truy cập, mật khẩu admin của thiết bị, tài khoản mật khẩu đăng nhập website lên Cloud (ThingSpeak.com).
- (21) NodeRED đọc chuỗi phương thức truy cập thành công, thời gian truy cập, mật khẩu admin thiết bị, tài khoản mật khẩu đăng nhập website từ Cloud (ThingSpeak.com).

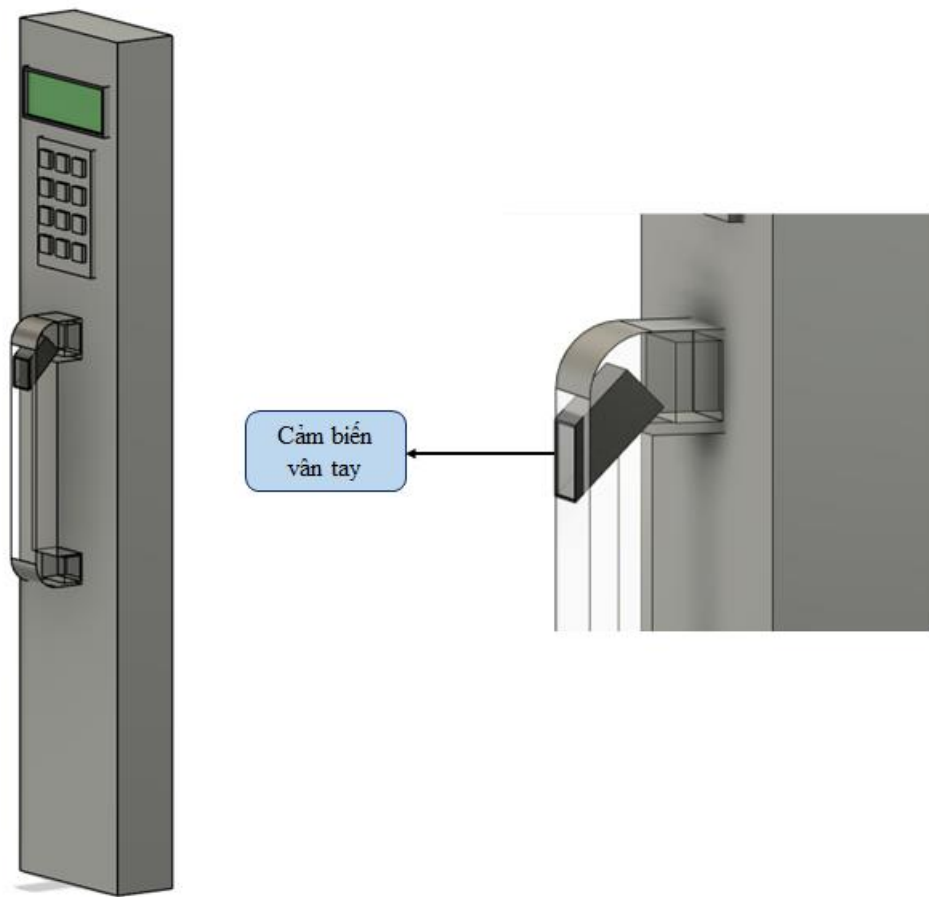
IV. Bản thiết kế 3D



Hình 1: Phần A của sản phẩm khi gắn lên cửa



Hình 2: Phần B của sản phẩm khi gắn lên cửa



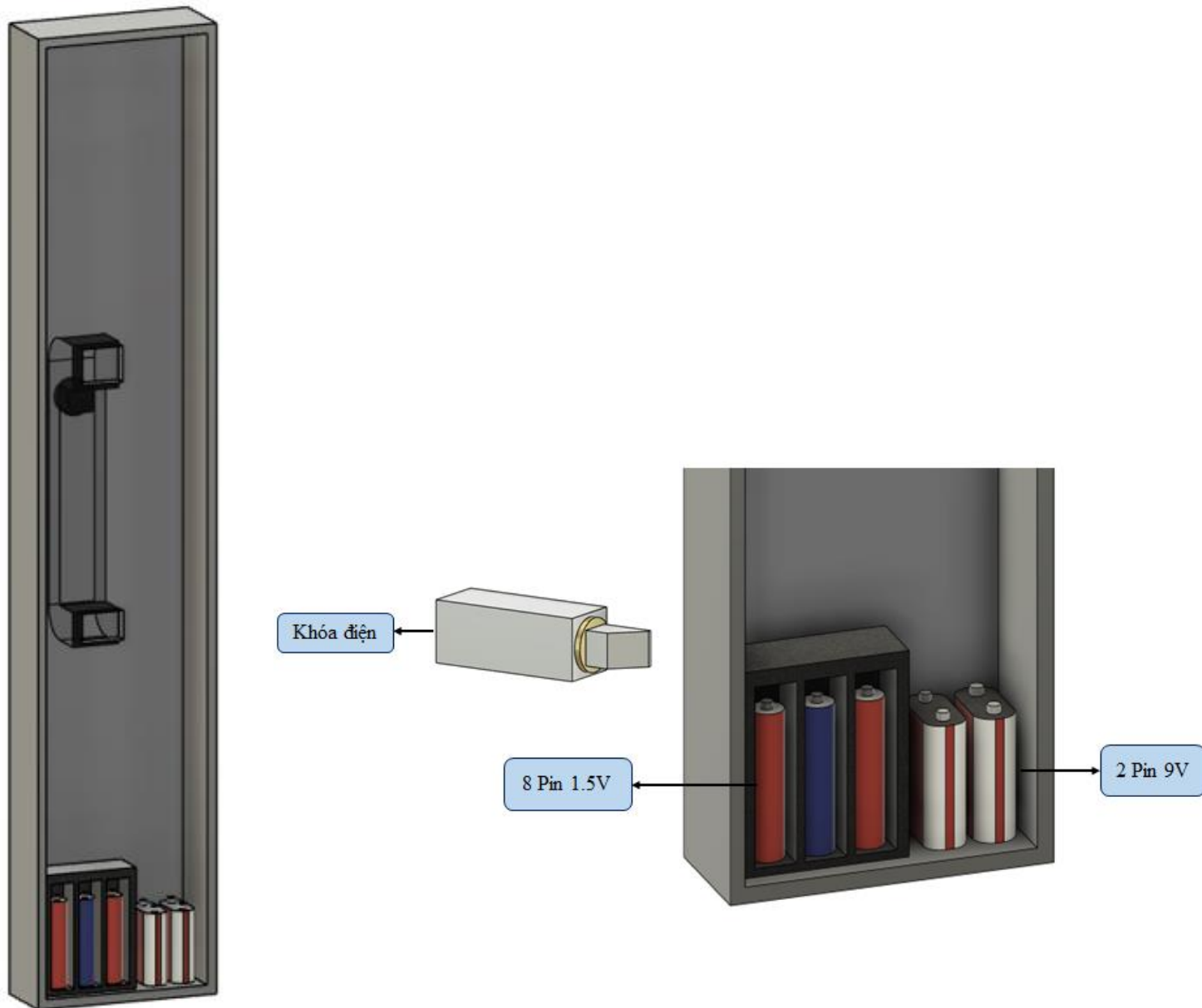
Hình 3: Mặt ngoài của phần A



Hình 4: Mặt trong của phần A



Hình 5: Mặt ngoài của phần B

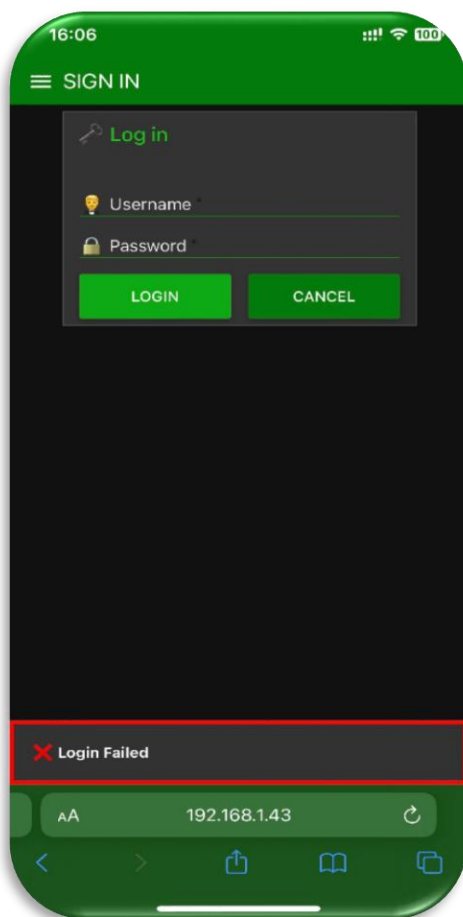


Hình 6: Mặt trong của phần B

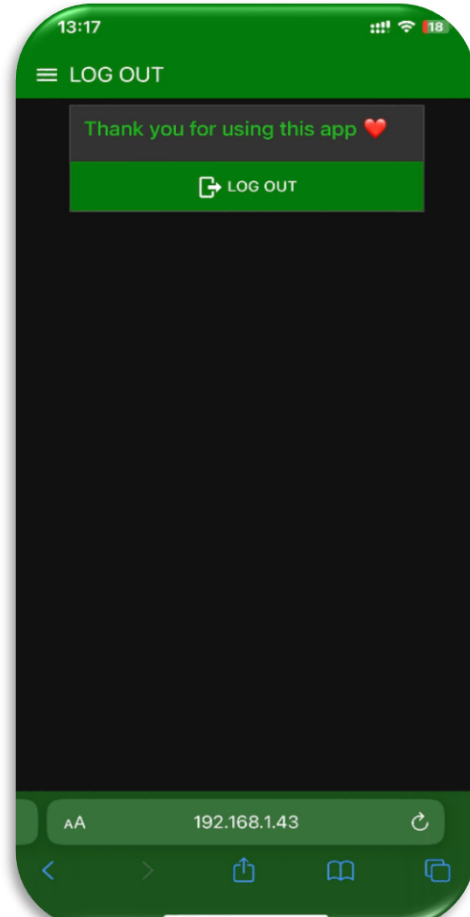
V. Giao diện web và mô tả chức năng

1. Tab SIGN IN và tab LOGOUT

- Giao diện chính:



Hình 6: Giao diện SIGN IN



Hình 7: Giao diện LOG OUT

- Chức năng của tab SIGN IN:

Cho phép người quản lý truy cập vào website

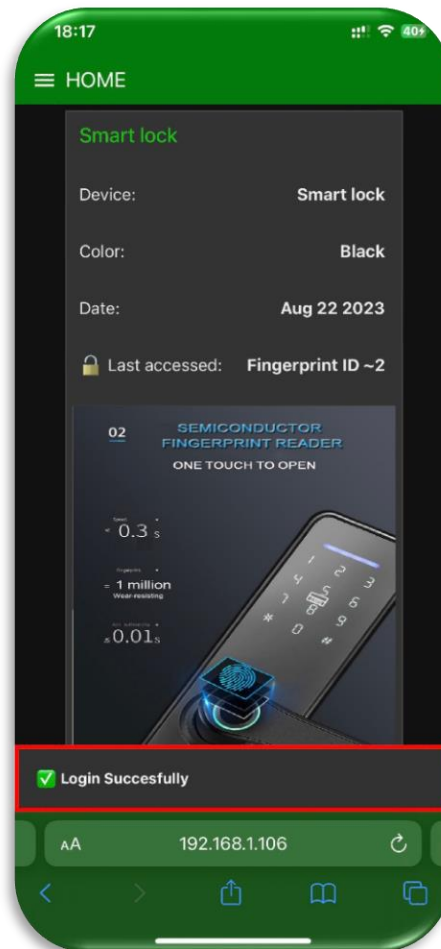
- ✓ Nếu nhập sai tên đăng nhập và mật khẩu: website sẽ hiển thị dòng thông báo “❌ Login Failed”.
- ✓ Ngược lại, sẽ thông báo “✅ Login Successfully” và cho phép sử dụng các tab chức năng bên trong website.

- Chức năng của tab LOG OUT:

Sau khi sử dụng xong, người quản lý có thể đăng xuất để đảm bảo tính bảo mật cho website

2. Tab HOME

- Giao diện chính:



Hình 8: Giao diện HOME

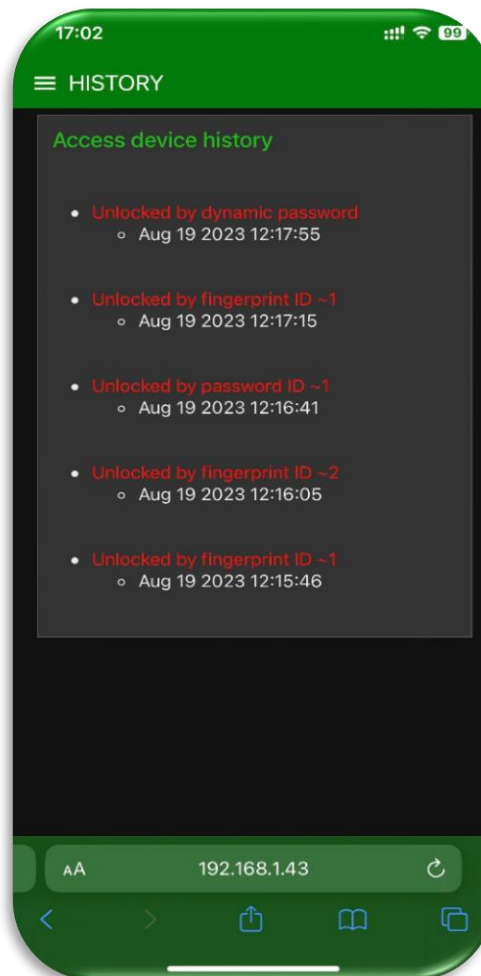
- Chức năng: đây là nơi giới thiệu các thông tin của thiết bị như tên, màu sắc và thời điểm truy cập website.

Bên cạnh đó, tab còn cung cấp cho người quản lý biết được phương thức gần nhất mở khóa cửa là gì

VD: lần mở khóa cửa gần nhất được thực hiện bằng vân tay có ID là 2 (như hình 8).

3. Tab HISTORY

- Giao diện chính:



Hình 9: Giao diện HISTORY

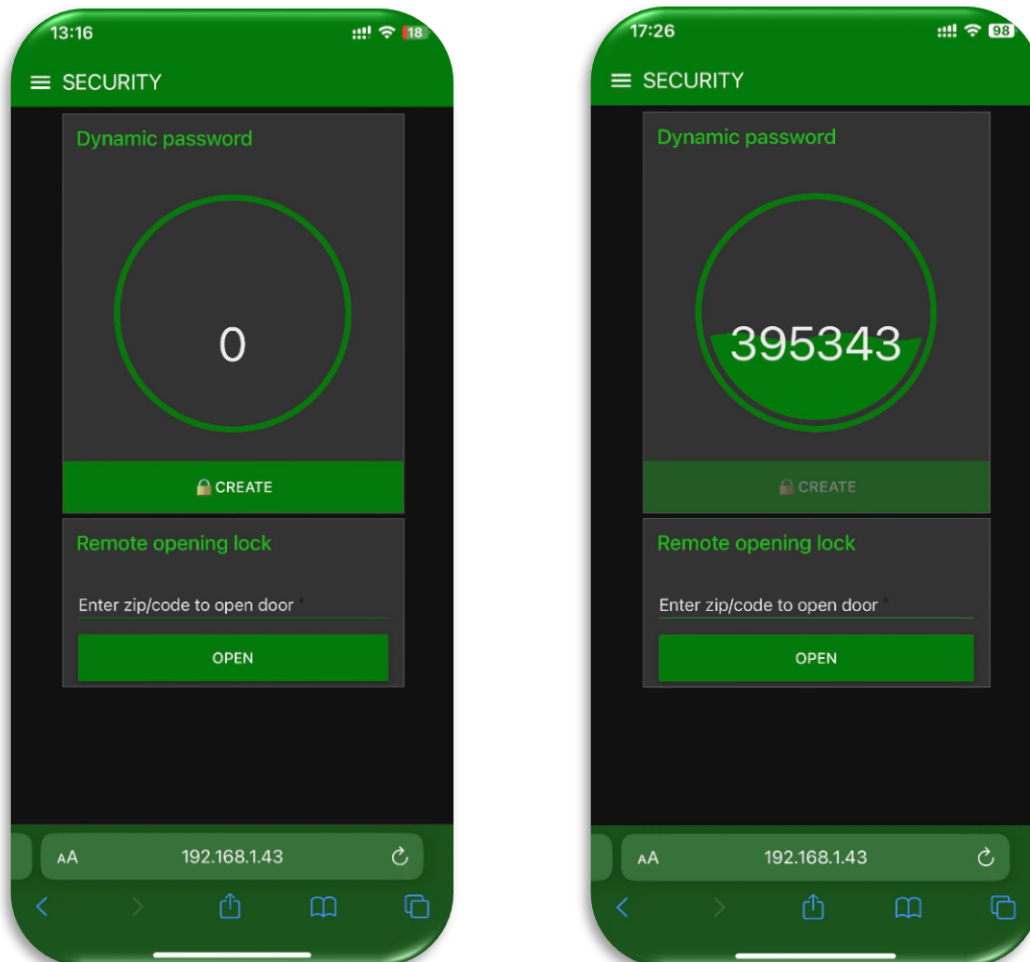
- Chức năng: giúp người quản lí có thể xem được lịch sử truy cập thiết bị, bao gồm các thông tin như sau:

- ✓ Phương thức truy cập:
 - Bàn phím số (vd: “Unlocked by password ID ~1”,...)
 - Vân tay (vd: “Unlocked by fingerprint ID ~2”,...)
 - Mật khẩu ngẫu nhiên (vd: “Unlocked by dynamic password”)
- ✓ Số ID nhận dạng của từng phương thức (vd: “ID ~1”, “ID ~2”, ...)
- ✓ Thời gian truy cập thiết bị thành công (vd: “Aug 19 2023 12:16:41”, ...)

4. Tab SECURITY

- Giao diện chính:

Bao gồm có 2 group: “Dynamic password” và ”Remote opening lock”.



Hình 10: Giao diện SECURITY

- Chức năng của group “Dynamic password”:

Trong trường hợp không có ai ở nhà mà người thân hay bạn bè muốn mở khóa cửa thì người quản lý sẽ ấn nút “CREATE” để tạo ra một mật khẩu ngẫu nhiên có hiệu lực trong vòng 3 phút cho phép họ nhập mật khẩu đó để vào nhà.

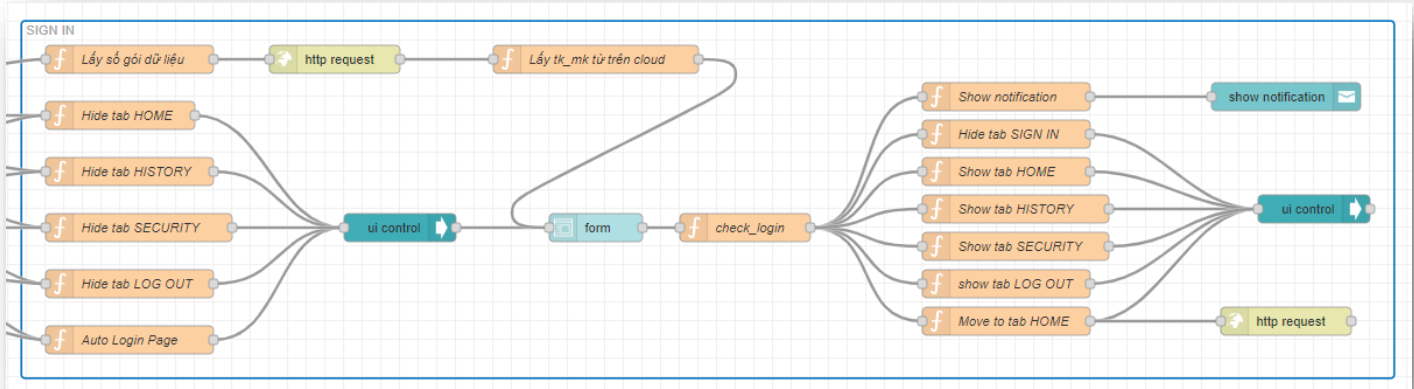
VD: “395343” (ở hình 4).

- Chức năng của group “Remote opening lock”:

Ngoài việc mở khóa trực tiếp bằng các phương thức thì website còn hỗ trợ việc mở khóa từ xa bằng mật khẩu admin được cài đặt trên thiết bị.

VI. Giải thích flow NodeRED (mô tả cấu hình/code các Node chính)

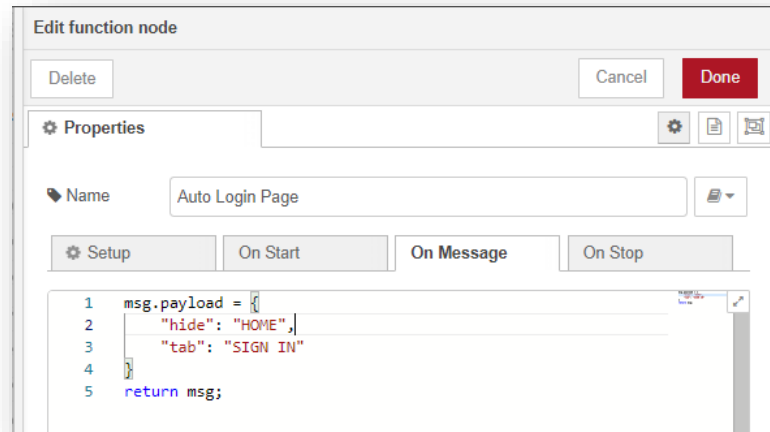
1. Đăng nhập vào website



Công dụng: là nơi để quản lí việc đăng nhập vào website.

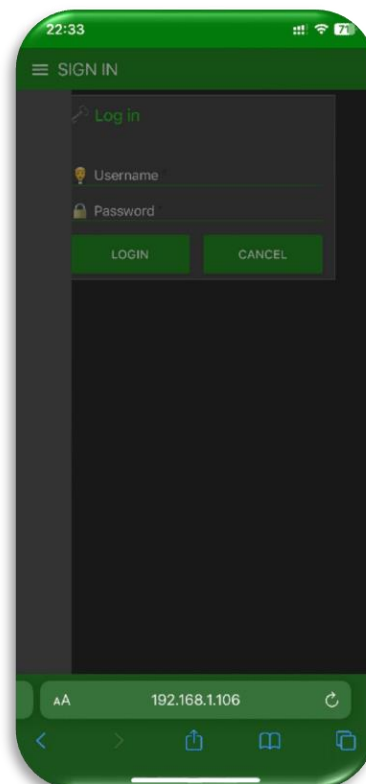
- Cụ thể hơn, khi bắt đầu chạy website, node function “*Auto Login Page*” sẽ dẫn đến giao diện log in. Bên cạnh đó những node function như “*Hide tab HOME*”, “*Hide tab HISTORY*”, “*Hide tab SECURITY*”, “*Hide tab LOG OUT*” giúp ẩn đi các tab chức năng trong thanh menu không cho người dùng truy cập vào khi chưa đăng nhập vào website. Những node function ẩn/ hiện tab trên đều được quản lý bởi node “*ui control*”.
- Việc lấy thông tin tài khoản hiện tại như tên đăng nhập và mật khẩu từ cloud sẽ luôn chạy khi khởi động website.
- Khi đăng nhập vào website thành công, node function “*Move to tab HOME*” sẽ luôn đưa người dùng đến với tab HOME đầu tiên và cho hiện những tab chức năng trong menu. Sau đó sẽ ẩn đi tab SIGN IN.

- ❖ Node function “*Auto Login Page*”:
 - “hide”: “HOME”: sử dụng yêu cầu ẩn tab HOME.
 - “tab”: “SIGN IN”: chuyển đến tab SIGN IN.

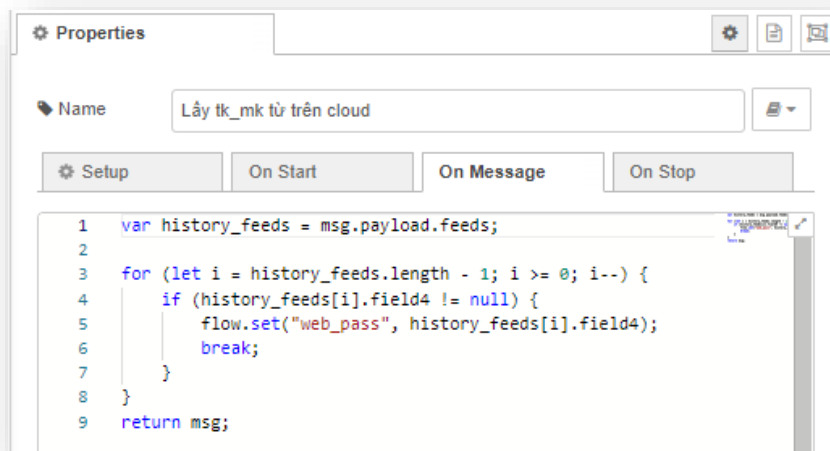


Công dụng: luôn giữ ở trang SIGN IN khi chưa đăng nhập vào website thành công.

- ❖ Node function “*Hide tab HOME*”, “*Hide tab HISTORY*”, “*Hide tab SECURITY*”, “*Hide tab LOG OUT*”:

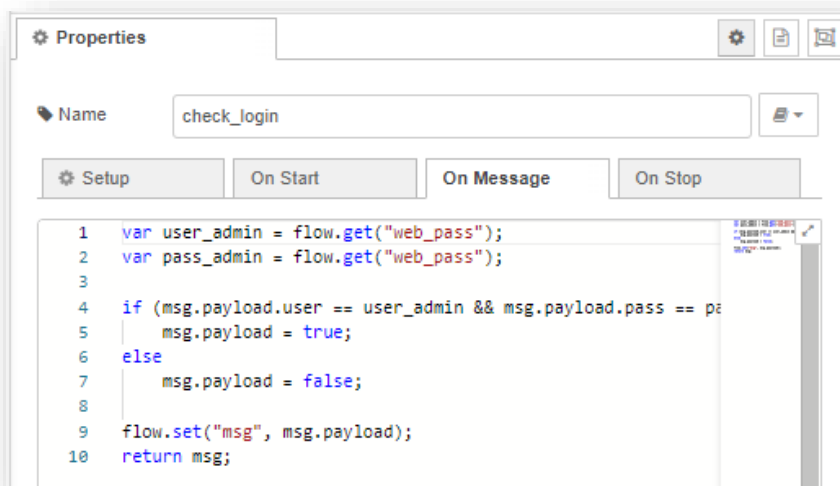


Công dụng: khi thực hiện đăng nhập tại trang SIGN IN, những node trên sẽ giúp ẩn đi các tabs chức năng khác trong thanh menu.

❖ Node function “*Lấy tk_mk từ trên cloud*”:Mô tả:

Đầu tiên, ta sẽ đi gán danh sách các gói dữ liệu hiện có trên cloud vào biến *history_feeds*, sau đó ta thực hiện công việc duyệt qua từng gói dữ liệu từ gói mới nhất đến gói cũ nhất để ta lấy được dữ liệu từ *field4* rồi ta gán vào flow “*web_pass*” để xét tính đúng / sai khi người dùng đăng nhập.

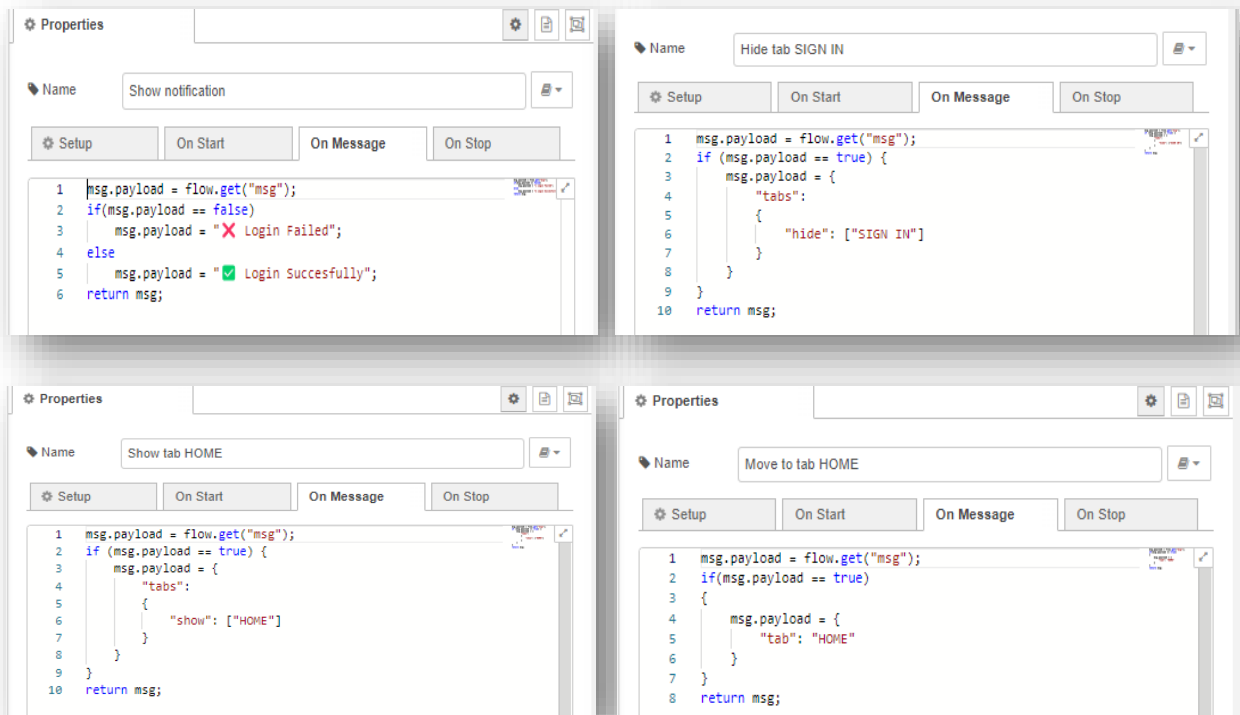
Lưu ý: khi thêm các gói dữ liệu sau, *field4* sẽ bằng *null* do tài khoản website chỉ được lưu cứng 1 lần ở trên cloud. Nên khi duyệt các gói dữ liệu ta sẽ lấy *field4* khác *null* đầu tiên tức là mật khẩu hiện tại của website.

❖ Node function “*check_login*”:Mô tả:

Lấy thông tin tài khoản tên đăng nhập và mật khẩu website từ cloud vào 2 biến là *user_admin* và *pass_admin*. Nếu người dùng nhập đúng đồng

thời tên đăng nhập và mật khẩu thì ta sẽ gán *true* vào flow “*msg*”. Ngược lại nếu nhập sai ta gán *false*.

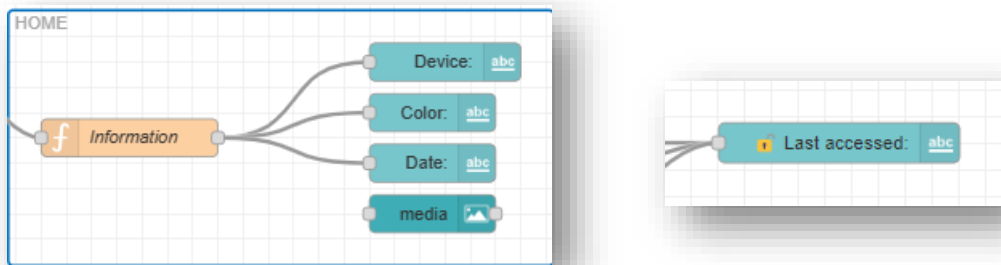
- ❖ Node function “*Show notification*”, “*Show tab HOME*”, “*Hide tab SIGN IN*”, “*Move to tab HOME*”:



Mô tả: ta lấy biến từ trong flow “*msg*” trước đó để kiểm tra điều kiện:

- ❖ *true*: đưa người dùng tới trang HOME và cho hiện các tab chức năng, ẩn đi tab SIGN IN và in ra thông báo đã đăng nhập thành công
- ❖ *false*: vẫn ở lại trang SIGN IN và in ra thông báo đăng nhập thất bại.

2. Xem các thông tin của thiết bị



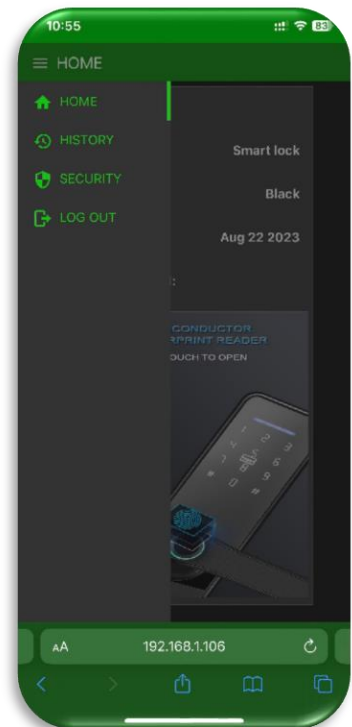
Công dụng: hiển thị thông tin của thiết bị thông qua và phương thức truy cập khóa cửa gần nhất.

❖ Node function “Information”

```

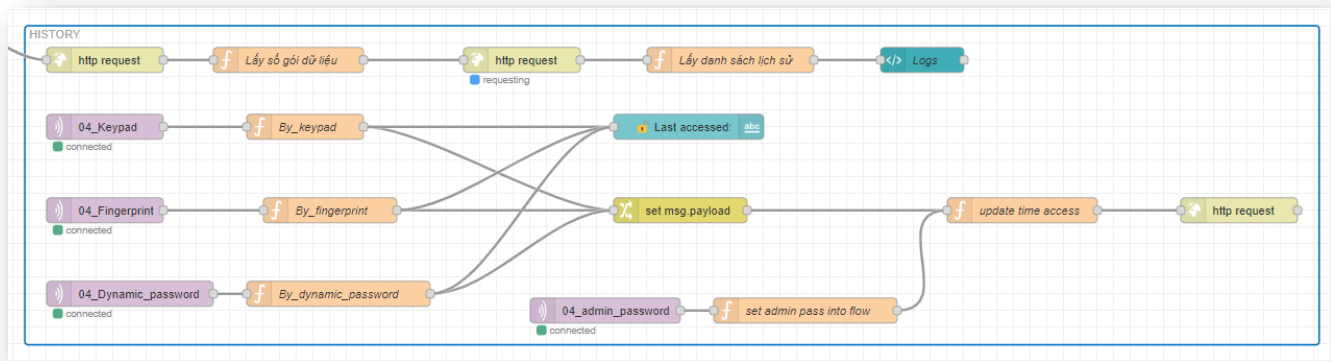
Name: Information
Setup On Start On Message On Stop
1 var date = new Date(msg.payload);
2
3 // Tên thiết bị
4 msg.name = "Smart lock";
5
6 // Màu
7 msg.color = "Black";
8
9 // Ngày tháng năm
10 msg.date = date.toString().slice(4, 16);
11
12
13 return msg;

```



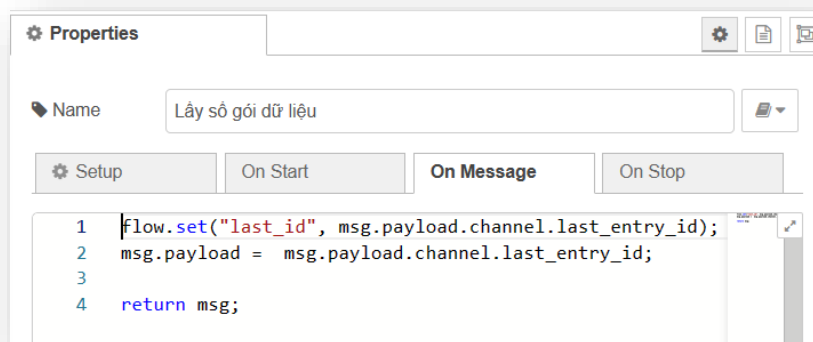
Mô tả: `msg.name`, `msg.color`, `msg.date` lần lượt chứa giá trị tên thiết bị, màu và thời gian người dùng đăng nhập truy cập vào website.

3. Xem danh sách lịch sử truy cập khóa cửa

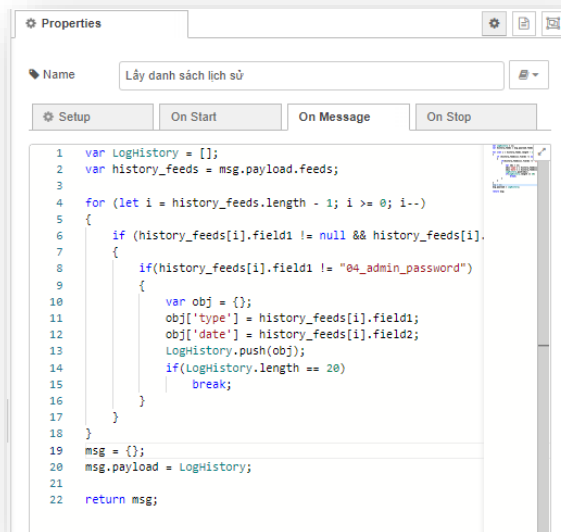


Công dụng: được tạo để đọc và lưu lịch sử từ cloud. Ngoài ra còn thể hiện lịch sử gần nhất trên website cho phép người quản lý thuận tiện theo dõi.

❖ Node function “Lấy số gói dữ liệu”



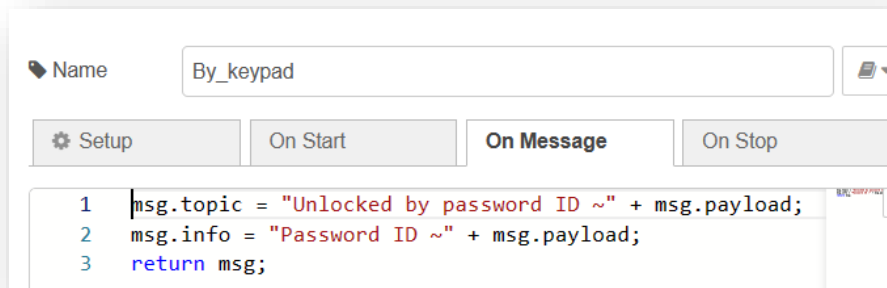
Mô tả: node “*http request*” trước node function để đọc dữ liệu từ cloud. Từ đó ta cần lấy số gói feeds từ trong mục “*channel.last_entry_id*”.

❖ Node function “*Lấy danh sách lịch sử*”

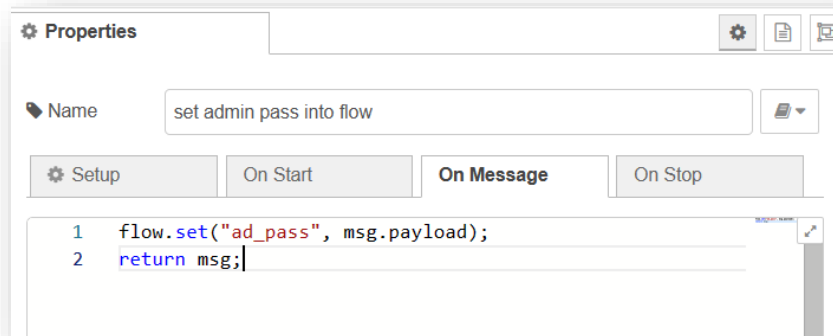
Mô tả: lấy danh sách lịch sử từ cloud để hiển thị lên website 20 phương thức gần nhất mở cửa như mật khẩu số, vân tay hay mật khẩu khuôn cấp.

Tạo mảng *LogHistory* để chứa 20 phương thức gần nhất mở cửa theo những cách đã liệt kê ở trên. Mỗi phần tử bao gồm 2 giá trị là *type* – dùng phương thức nào để mở cửa và *date* – thời gian lúc mở cửa, *type* và *date* được gán ở giá trị *field1* *field2* của gói feed.

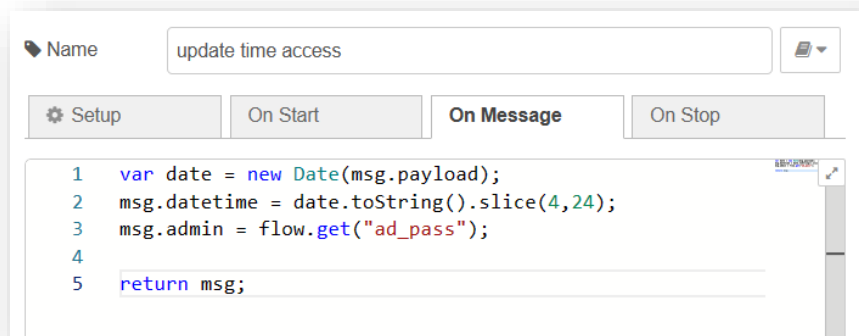
- ❖ Các node MQTT như “04_Keypad”, “04_Fingerprint” và “04_Dynamic_password”: nhận tín hiệu từ mạch ESP8266 khi mở cửa bằng mật khẩu số, dấu vân tay hay mật khẩu khuôn cấp.
- ❖ Node function “By_keypad”: nếu mở cửa bằng mật khẩu số, node sẽ nhận được tín hiệu từ mạch với giá trị là số ID – thứ tự của mật khẩu trong danh sách các mật khẩu hợp lệ hiện tại.



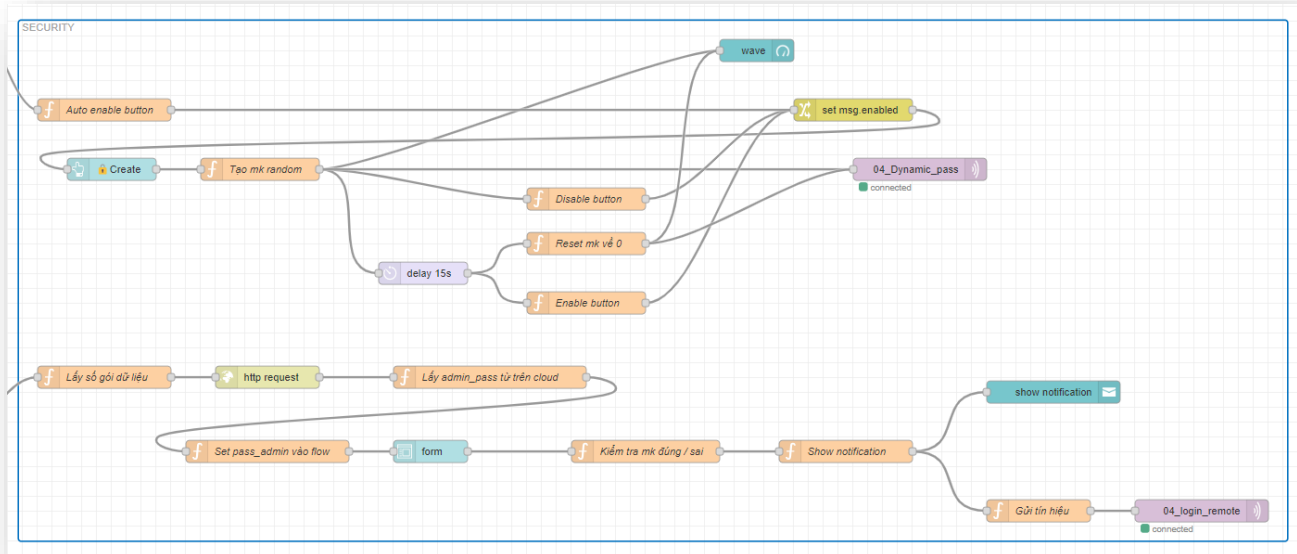
- Với *msg.topic* là dòng thông báo mở bằng mật khẩu số được dùng để lưu trên cloud.
 - Với *msg.info* là dòng thông báo trong tab HOME ở phần mở cửa gần nhất.
 - Tương tự như vậy với node “*By_fingerprint*”, “*By_dynamic_password*”.
- ❖ Node function “*set admin pass into flow*”: node “*04_admin_password*” sẽ nhận mật khẩu admin từ mạch ESP8266 truyền đến, gán mật khẩu admin vào flow “*ad_pass*”.



- ❖ Node function “*update time access*”: hàm để gán thời gian mở cửa vào *msg.datetime* và gán mật khẩu admin vào trong *msg.admin*. Sau đó sẽ lưu dữ liệu lên cloud thông qua node “*http request*” lưu lần lượt giá trị *field1*, *field2*, *field3* lần lượt là *msg.topic*, *msg.datetime* và *msg.admin*.

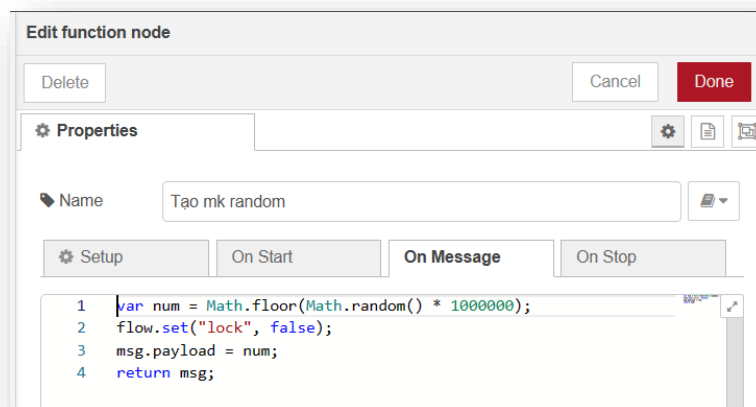


4. Tạo mật khẩu động và điều khiển thiết bị từ xa



Công dụng: tăng tính bảo mật cho khóa cửa, cụ thể trong group này có chức năng tạo khẩu cấp một mật khẩu số có hiệu lực trong vòng 3 phút và điều khiển mở khóa từ xa bằng cách nhập mật khẩu admin.

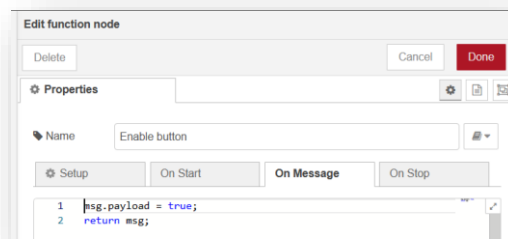
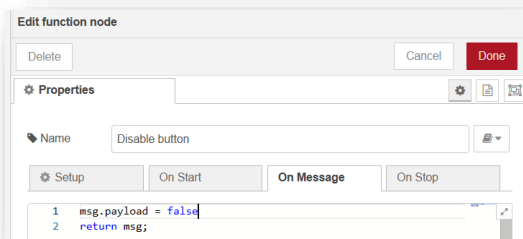
❖ Node function “*Tạo mk random*”:



Mô tả: Tạo ngẫu nhiên một dãy số có 6 chữ số làm thành mật khẩu khẩu cấp bằng cách làm tròn xuống giá trị của một số ngẫu nhiên nhân với 1000000 (như câu lệnh `Math.floor(Math.random() * 1000000)`).

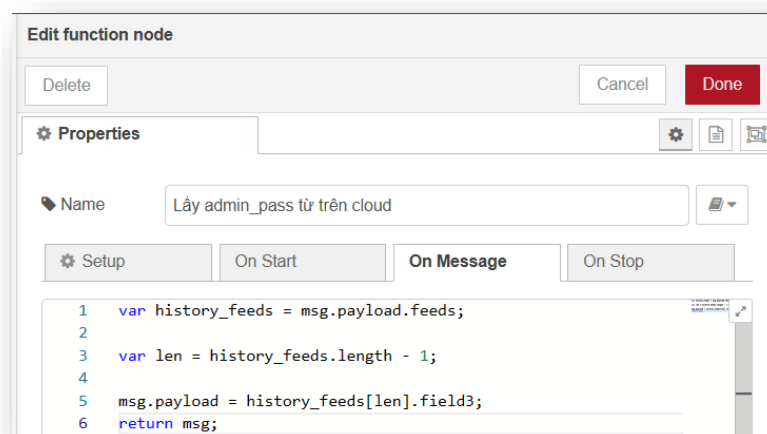
❖ Node MQTT out “04_Dynamic_pass”: mật khẩu vừa được tạo sẽ gửi đến node để truyền đến mạch ESP8266 để thêm mật khẩu hợp lệ mới.

❖ Node function “Disable button”:



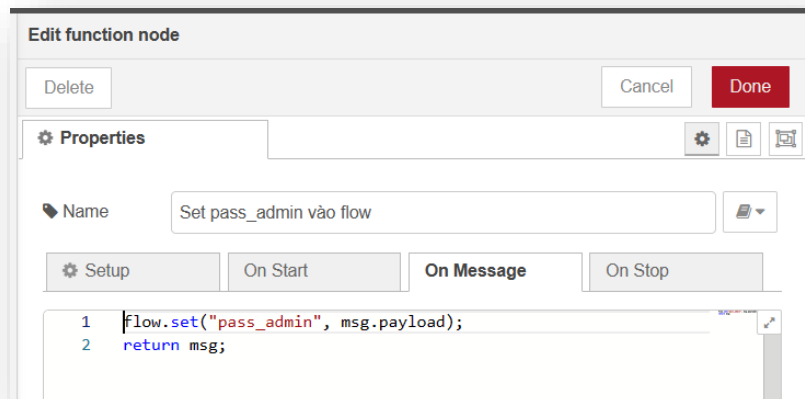
- Node dùng để gán giá trị `msg.payload` là `false` để ngăn việc tạo mật khẩu khẩn cấp liên tục. Tương tự vậy, ta cũng có node function “Enable button” hay “Auto enable button” để cho phép người dùng có thể ẩn tạo mật khẩu trở lại.
- Gói tin trạng thái của button gửi đến node change “set msg.enabled” để mở hoặc khóa việc ẩn tạo mật khẩu.

❖ Node function “lấy admin_pass từ trên cloud”:

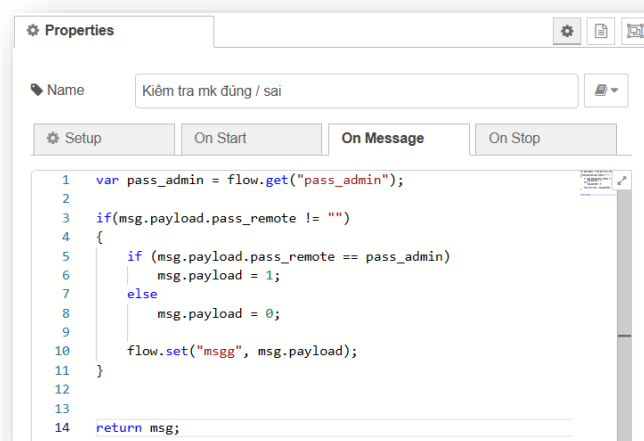


- Node để lấy mật khẩu admin có từ trên cloud.
- Gửi gói tin để đọc dữ liệu từ cloud qua node “http request”. Sau đó ta cần lấy ra những gói feed lưu vào biến `history_feeds`. Mật khẩu admin sẽ là giá trị `field3` của gói feed cuối cùng của dữ liệu từ cloud.

- ❖ Node function “Set pass_admin vào flow”: lưu mật khẩu admin mới lấy từ cloud vào flow “pass_admin”.

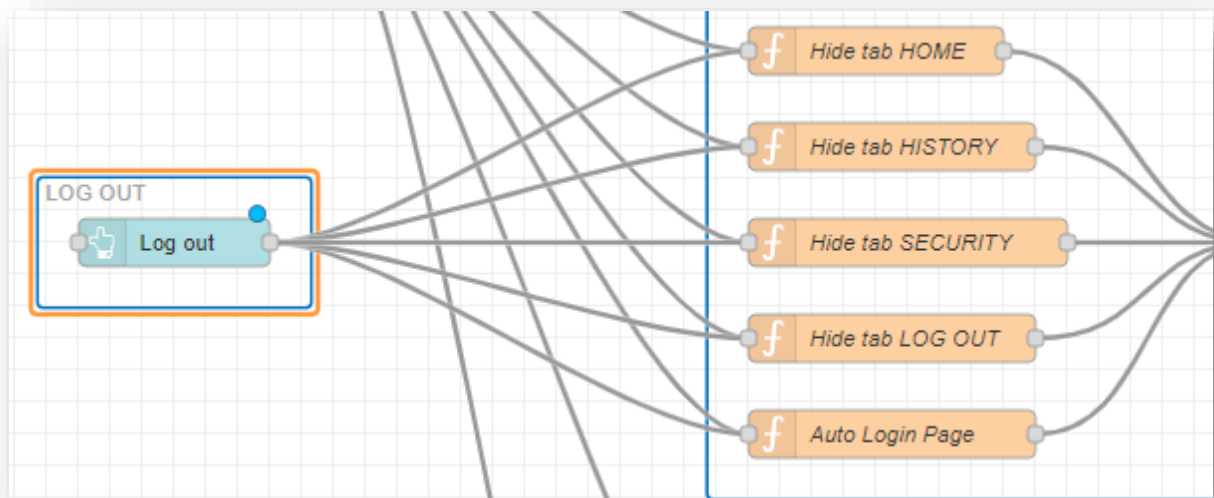


- ❖ Node function “Kiểm tra mk đúng / sai”



- Với chức năng điều khiển từ xa, người dùng cần phải nhập mật khẩu admin mới có thể mở cửa.
- Mật khẩu admin sẽ được lấy từ flow “Kiểm tra mk đúng / sai” để kiểm tra với người dùng nhập. Nếu như người dùng nhập đúng thì msg.payload là 1, ngược lại thì là 0.
- Giá trị được gán vào flow “msgg” để gửi thông báo trên web cho người dùng nhập sai hay đúng. Đồng thời cũng gửi tín hiệu tới node “04_login_remote” để truyền đến mạch ESP8226 rồi đến mạch Uno để in ra dòng thông báo trên thiết bị LCD.

5. Đăng xuất khỏi website



Công dụng: giúp người quản lý có thể đăng xuất để tăng tính an toàn cho website.

❖ Node button “*Log out*”

Sau khi ấn nút “*Log out*” để đăng xuất, website sẽ trở về lại trang SIGN IN và ẩn hết các tab HOME, HISTORY, SECURITY, LOG OUT trong thanh menu.

VII. Nguồn tham khảo

- Làm khóa vân tay đơn giản dùng cảm biến vân tay r305 và kit arduino nano:
<https://www.youtube.com/watch?v=b1DIAH9GfWA>
- How to make fingerprint door lock at home:
https://www.youtube.com/watch?v=SMmj_qAbyeM
- Arduino Keypad and LCD display:
https://www.youtube.com/watch?v=G2C6_Bp8cwk
- Hướng dẫn giao tiếp uart giữa board arduino với kit wifi esp8266:
<https://www.youtube.com/watch?v=X7CKYdUB2mw>
- Node-Red Dashboard tutorial:
<https://www.youtube.com/playlist?list=PLhaePTb701HSHPp6r3lbWdnUs8y98OHh>
- How to catch time in Node-Red:
<https://youtu.be/ZcekM0kpg4Y>
- Code kết nối Wifi: <https://dandelion-croissant-ad4.notion.site/Code-k-t-n-i-Wifi-tr-n-Wokwi-4055feb3a4844e56914a3ae5bff8a82a>
- Code kết nối MQTT Server: <https://dandelion-croissant-ad4.notion.site/Code-k-t-n-i-MQTT-Server-b708e215b4134638ae1eafe37a7650aa>
- Code gửi Http Request từ ESP: <https://dandelion-croissant-ad4.notion.site/Code-g-i-HttpRequest-t-ESP-fa27af5c3b0e4750b7d7e8dd1d81a6c3>