

IoT CHALLENGE 2023



Team VIKINGS

HOME AUTOMATION SYSTEM

Members:

Le Hung Viet

Tran Van Thinh

Trinh Thi Cuc

Mentor: Pham Anh Khang

Hanoi - 2023

TABLE OF CONTENTS

1. Introduction	3
1.1. Overview	3
1.2. Model.....	3
2. Components detail.....	5
2.1. Server.....	5
2.2. Devices	6
2.3. Facial recognition	7
2.4. Dashboard.....	8
3. Features	9
3.1. Smart Configuration	9
3.2. Control devices.....	9
3.3. Collect environmental data, power consumption.....	10
3.4. Security.....	11
3.5. Data management	14
4. Result and summary.....	15
5. User Manual	17
5.1. Connection Configuration	17
5.2. Open Dashboard	17
5.3. Control devices through dashboard.....	18
5.4. Download log file	19
5.5. Door control.....	19
5.6. Add / Delete user.....	20
5.7. Local control devices.....	21
5.8. File Management.....	22

TABLE OF FIGURES

Figure 1.1. System overview.....	3
Figure 2.1. Raspoberry Pi 4.....	5
Figure 2.2. Server diagram.....	6
Figure 2.3. Deep Learning Facial Recognition Model.....	8
Figure 3.1. Smart configuration diagram	9
Figure 3.2. Control devices diagram	9
Figure 3.3. Collect and send data to server	10
Figure 3.4. Data storage and visualization diagram.....	11
Figure 3.6. Pried door warning diagram	12
Figure 3.8. Delete user diagram	13
Figure 3.9. Generate chart from log file diagram	14
Figure 3.10. Manage file digram.....	14
Figure 4.1. Home Automation System model.....	15
Figure 4.1. Config display.....	17
Figure 4.2. Config UI.....	17
Figure 4.3. Log in screen.....	17
Figure 4.4. Dashboard Overview	18
Figure 4.5. Control Device UI.....	18
Figure 4.6. Choose date to download log file	19
Figure 4.7. Log file example.....	19
Figure 4.8. Unlock the door with Facial Recognition.....	20
Figure 4.9. Unlock the door from inside the home	20
Figure 4.10. Add & Delete user	21
Figure 4.11. Local control devices.....	21
Figure 4.12. File management screen	22

1. Introduction

1.1. Overview

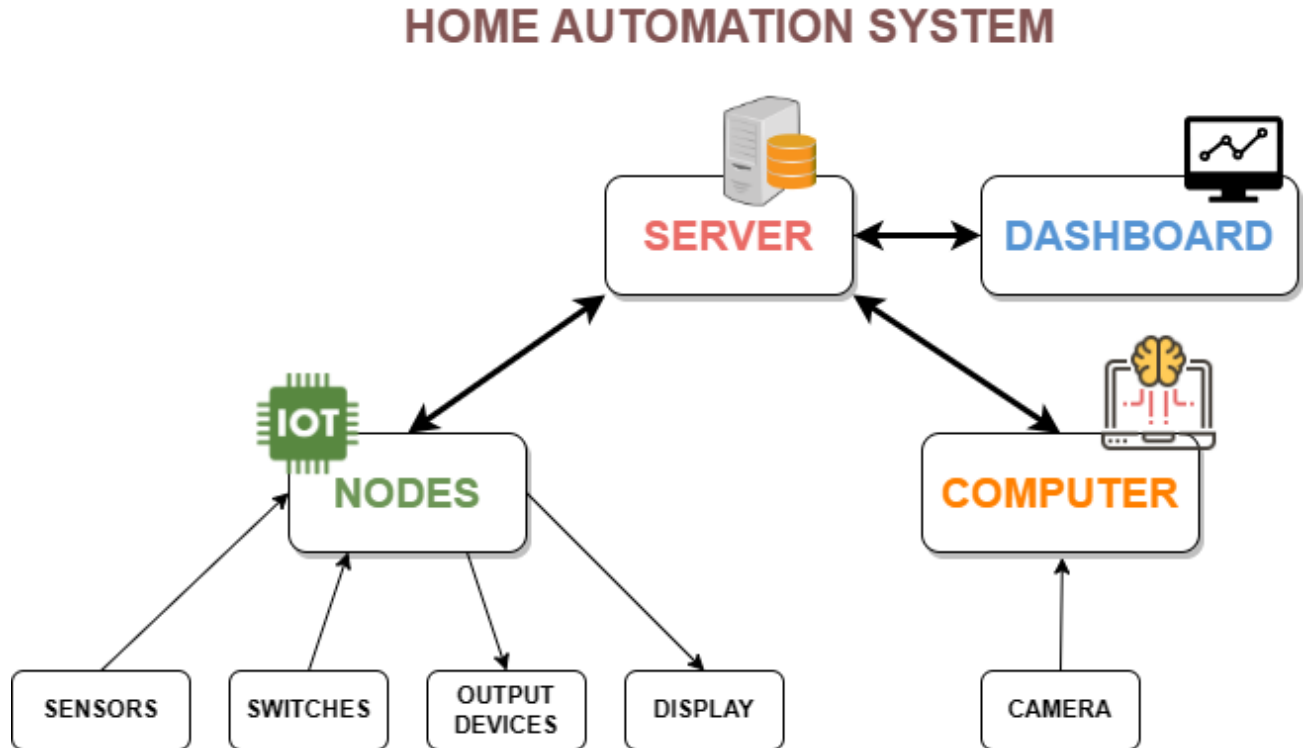


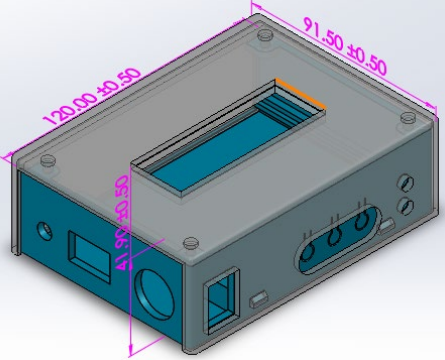
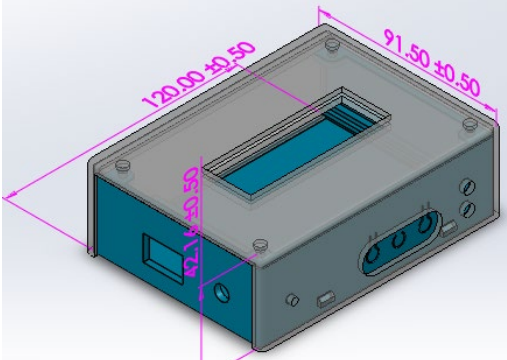
Figure 1.1. System overview

The "Home Automation System" comprises four primary components:

- Processing Block consists of a microcontroller, sensors, relays, and is tasked with the responsibilities of gathering data from sensors and switches, transmitting and receiving commands to/from the server, and issuing control commands to end devices
- Facial Recognition Block, comprising a computer and a camera, assumes the role of conducting facial recognition and relaying the outcomes to the server.
- The Server Block, equipped with a Raspberry Pi featuring MQTT Broker and Node-RED installations, serves as the central control hub. It handles the reception and transmission of data from controllers and computers while also functioning as a data storage repository.
- The Dashboard Block functions as the user interface for remotely controlling the entire system through a web app platform, powered by Node-RED

1.2. Model

Based on the homeowner's specific use case, there are two product versions to choose from: Viking_01 and Viking_02.

	Vikings_01	Vikings_02
		
	ESP32 (4MB Flash, 520KB SRAM)	
Input	2 switches	2 buttons
Capacity	2 outputs (up to 220V - 500W)	2 outputs (up to 220V - 500W)
Power	12V	
Display	16x2 LCD	
Sensors	Temperature – Humidity sensor, GAS sensor, current sensor	Current sensor, IR sensor
Tính năng	Gather environmental data, power consumption, and control lighting through switches and monitor;	Gather power consumption data, establish lighting schedules for on/off cycles, automatic lighting, and facial recognition for door locking.

2. Components detail

2.1. Server

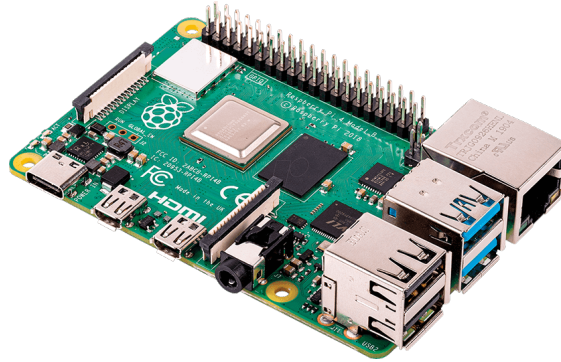


Figure 2.1. Raspoberry Pi 4

The Raspberry Pi 4 serves as the central hub of the system, responsible for controlling and monitoring devices through MQTT communication; manages logic, Dashboard via Node-RED.

Spec	Quad-core Cortex-A72, 4GB LPDDR4-3200 SDRAM, 32GB ROM
OS	Ubuntu Server 20.04
Platform	Node-RED: a visual tool that facilitates the creation and management of automation logic through a web browser.
Framework	NodeJS
MQTT broker	Mosquitto: an open-source MQTT broker that facilitates secure and reliable communication between devices and applications within the system, utilizing the MQTT protocol
Address	vikings.hopto.org (DDNS): Automatically updating the Raspberry Pi's public IP address whenever it changes, allows for accessing the system from anywhere on the Internet, eliminating the need to manually track the new IP address.

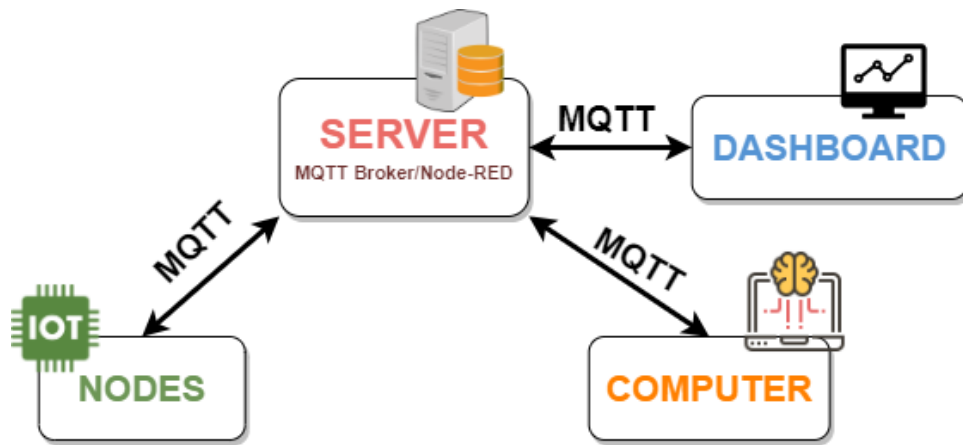


Figure 2.2. Server diagram

Security: Raspberry Pi is protected by fundamental system settings, using strong passwords, and consistently updating both the operating system and applications

Secure communication: MQTT is configured to employ a secure connection (MQTT over TLS/SSL) to enhance security when transmitting information between devices and servers. For data transmission and reception, an account and password are required to ensure proper verification..

Access management: Users access and manage devices by utilizing their designated account and password, with authorization granted based on three distinct levels:

- Administrator: provides full system privileges, including the ability to edit system logic.
- User: Users at this level possess access and operational rights within the control panel. They can view the logical system but do not possess editing capabilities.
- Guest: limited to viewing rights only and cannot perform any operational actions.

2.2. Devices

MCU ESP32	Dual-core Tensilica LX6, clock speed 80MHz – 240MHz; 512KB RAM; 4MB Flash memory
Relay	Utilize a Relay for managing devices operating at higher voltage levels than the microcontroller's output voltage
IR sensor	Uses infrared rays to detect people passing by and automatically turn on the lights.
MQ-2 GAS sensor	Measure the concentration of gas inside the house and gather signals using analog pins.

DHT22 sensor	Measures air temperature and humidity, transmitting signals to the microcontroller via the One-wire protocol
INA219 sensor	Measure voltage, power consumption, and current parameters, then transmit the data to the MCU using the I2C protocol.
Buzzer	Generate a beep and control it through the microcontroller's GPIO pin
LCD 16x2	Displays the device's current status, basic parameters, and communicates indirectly with the MCU through the I2C LCD16x02.
Servo SG90	Control rotation angle using the PWM mechanism, with the SG90 servo employed as an electric lock within the device

2.3. Facial recognition

Devices:

- Server: This is a central component of your system. It sends requests to the host and likely handles the processing of facial recognition.
- Webcam: This is the input device that captures raw frames in real-time. These frames typically contain images of faces.
- Host: This is where the webcam is connected. It receives requests from the server and is responsible for forwarding the raw frames captured by the webcam to the server for processing.

Programs:

- Deep Learning Model: This is an end-to-end model with pre-trained model of ArcFace with 98% accuracy that is trained to detect and extract features of faces from the raw frames captured by the webcam. The training process likely involves feeding the model with a large dataset of labeled facial images to learn to recognize faces accurately.

Pipeline:

- The webcam continuously captures raw frames (images) in real-time.
- The host receives requests from the server. These requests might include instructions to start processing frames.

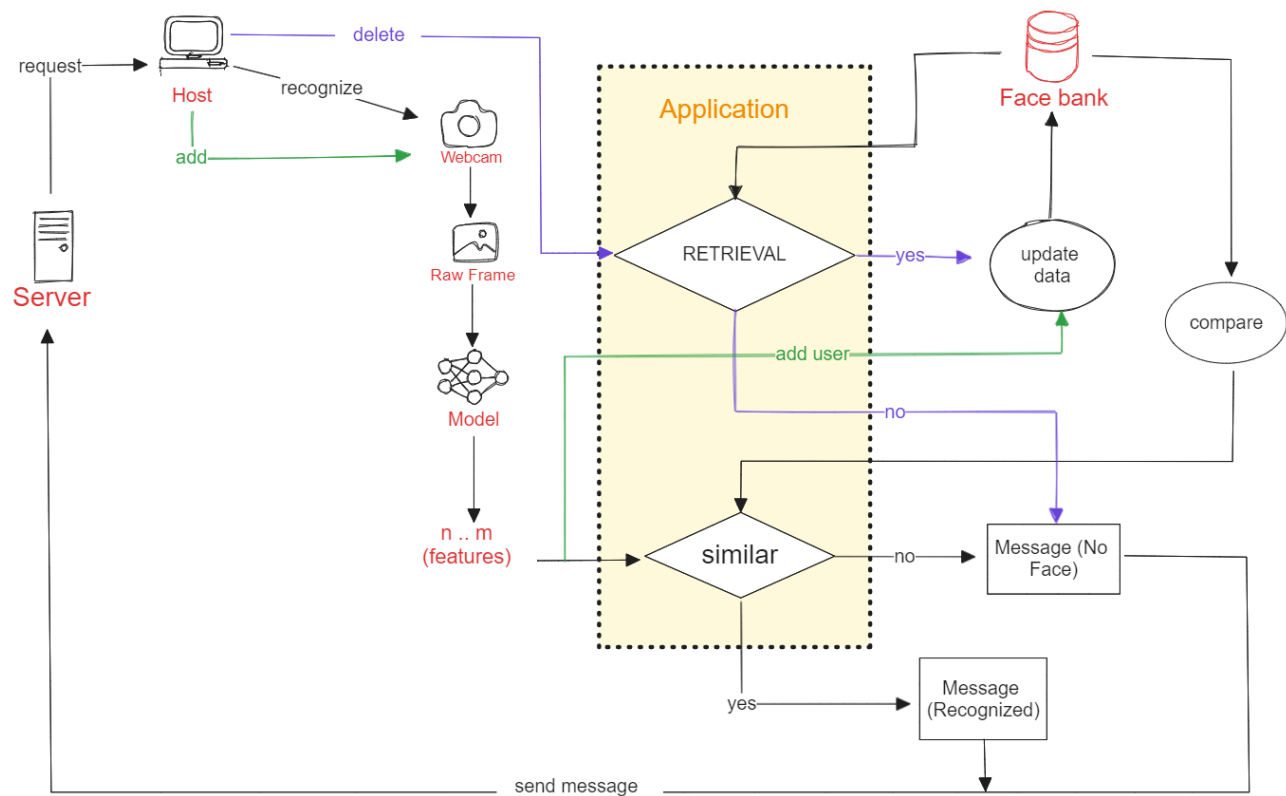


Figure 2.3. Deep Learning Facial Recognition Model

2.4. Dashboard

The system's dashboard is an intuitive and interactive interface constructed with Node-RED. It empowers users to seamlessly monitor and control their home through a web app, encompassing features such as:

- Displays indoor environmental parameters.
- Controls electrical equipment and provides real-time monitoring of their status
- Manages users with permission to unlock the door using Facial Recognition
- Stores and manages data

Users are required to have an account and password for accessing and utilizing the dashboard. This information is encrypted on the server to guarantee the security and integrity of the system

3. Features

3.1. Smart Configuration

This feature simplifies the process for users to modify WiFi and MQTT connection parameters via a web browser, all without requiring a system reset. It proves highly convenient during initial installation or when changing the installation location.

When "Smart Config" mode is activated, the ESP32 will function as a webserver and broadcast its own WiFi signal. Users can connect to this WiFi network using a web browser to initiate the installation process, as illustrated in the following diagram:

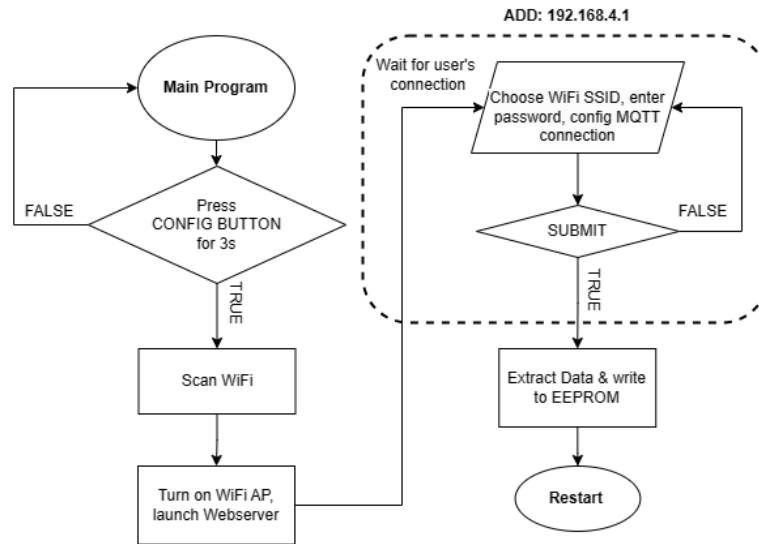


Figure 3.1. Smart configuration diagram

3.2. Control devices

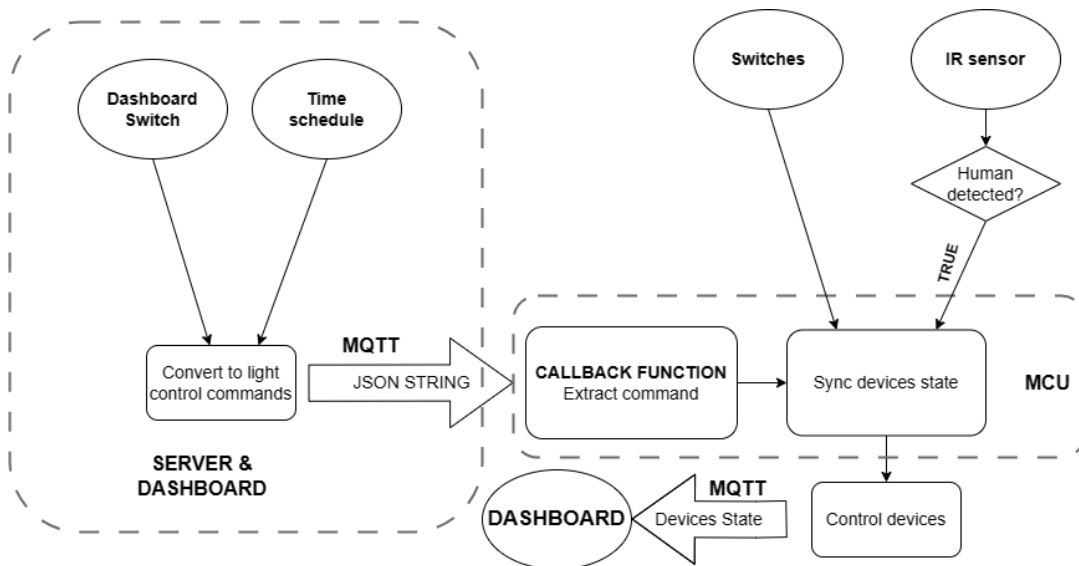


Figure 3.2. Control devices diagram

There are three methods to control the device: using the command in dashboard, utilizing physical switch buttons, and enabling automation by sensor status:

- Using dashboard: The dashboard will transmit a string command via MQTT to the MCU, where the MCU will compare and verify the command before controlling the device in accordance with the corresponding command.
- Using physical switch: Utilize the physical switch as a button to capture the signal and control the light device according to the button's status.
- Using sensor: Automatically activates based on sensor detection status.

3.3. *Collect environmental data, power consumption*

The device collects temperature, humidity, gas, and power consumption data and transmits it to the server in JSON format through the MQTT protocol. These parameters are subsequently analyzed and presented on a real-time chart for monitoring and visualization.

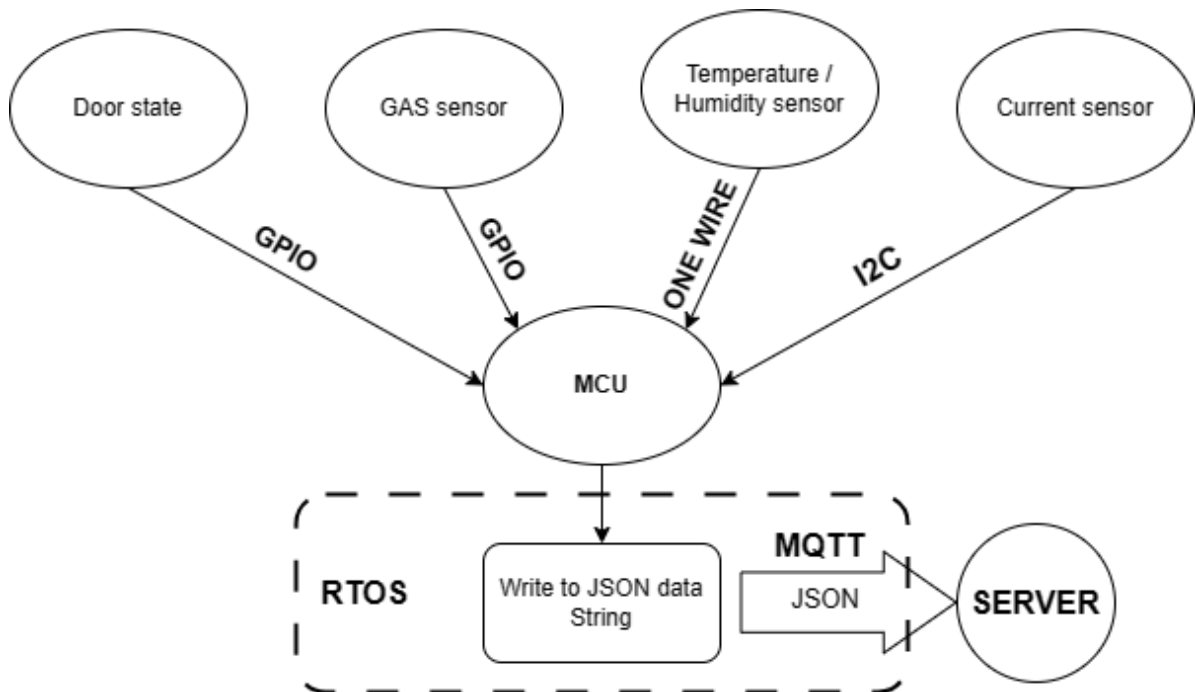


Figure 3.3. *Collect and send data to server*

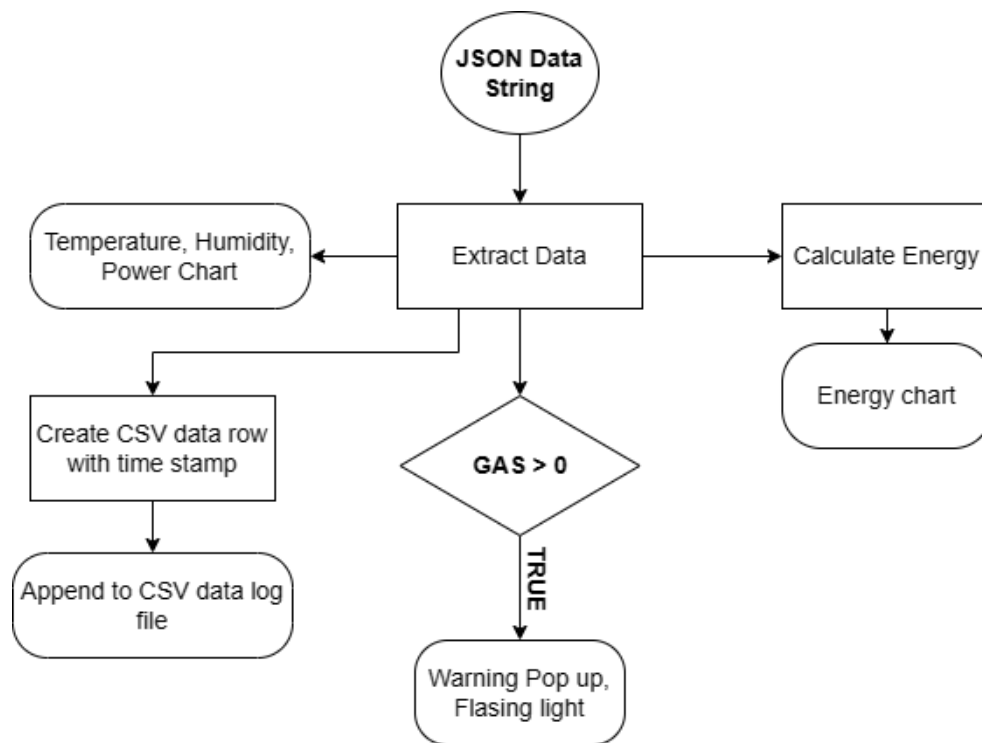


Figure 3.4. Data storage and visualization diagram

3.4. Security

3.4.1. Lock/unlock the door

The "Home Automation System" incorporates two door unlocking mechanisms and an automatic door locking mechanism that engages when the door is closed:

- When entering the house from outside, the system mandates face authentication to unlock the door. Users initiate this process by pressing a button and facing the camera. The system will automatically recognize the face and unlock the door if it matches the database.
- When going out from home, just press the unlock button inside the house without needing face authentication
- Whenever the door is closed, it is automatically locked and the door-pry detection feature will be activated.

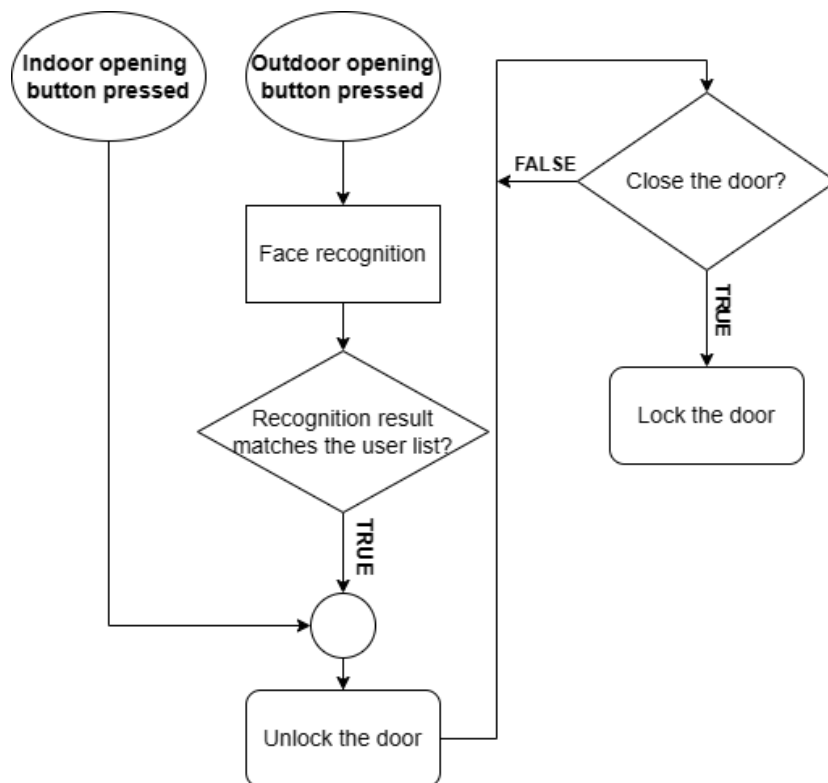


Figure 3.5. Door lock/unlock diagram

3.4.2. Pried door warning

- The detection and warning feature for door prying is automatically enabled when the door is closed. If the system detects an attempt to pry the door open, it will promptly send a notification to the server and email it to the homeowner.
- After the user presses the outside door open button for face authentication, the siren will deactivate, and the system will return to a ready state for normal operation.

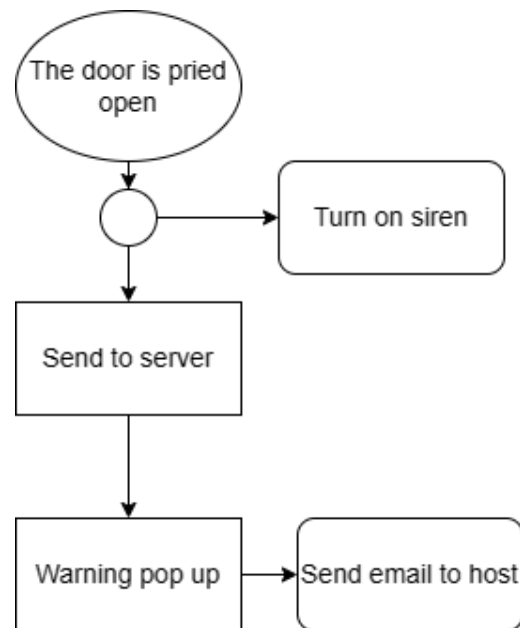


Figure 3.6. Pried door warning diagram

3.4.3. Add user with permission to unlock the door using Facial Recognition

- Homeowners have the capability to add individuals with permission to unlock the door using facial recognition through the dashboard.
- When receiving request to add new user from server, host will get their facial features and relevant information and store in the system. This thread interacts with the deep learning model to extract and save facial features for the new user.
- The list of usernames with this authorization is securely saved and encrypted into a system file to enhance security and prevent tampering.

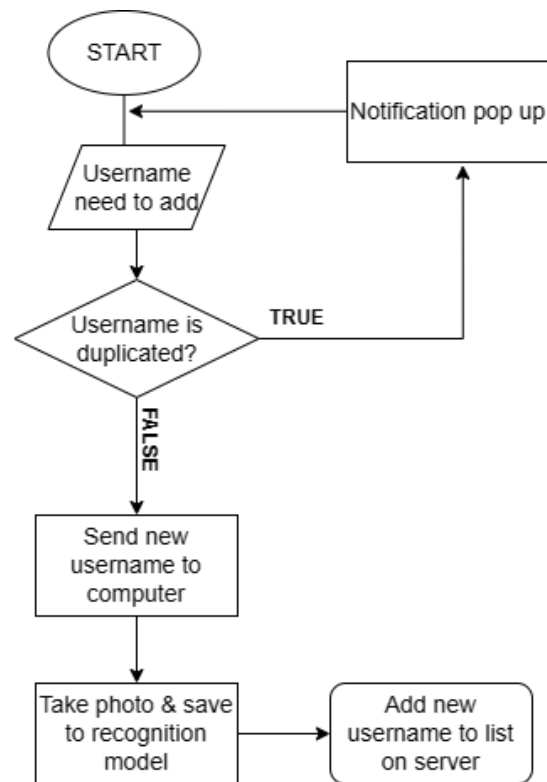


Figure 3.7. Add user diagram

3.4.4. Delete user with permission to unlock the door using Facial Recognition

- The list of usernames with permission to unlock via facial recognition is decoded and presented as a selector box.
- When deleting a username, the system simultaneously removes that username from the system file and the list of labels in the recognition model to maintain synchronization.

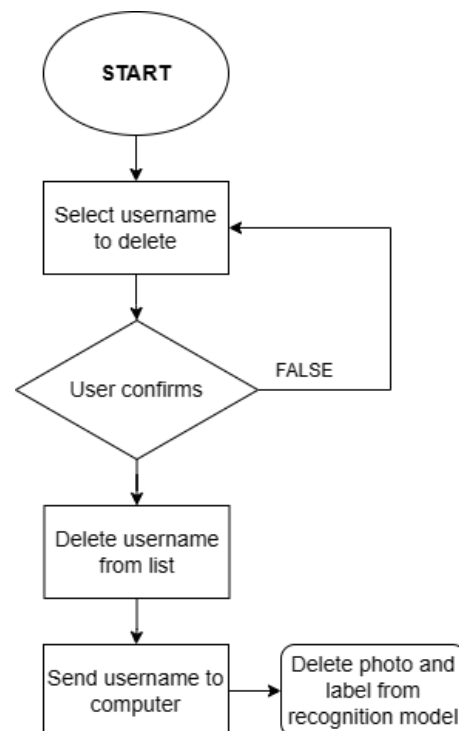


Figure 3.8. Delete user diagram

3.5. Data management

3.5.1. Generate chart from log file

To facilitate data analysis, we've implemented a feature that visualizes the recorded data on a daily basis through charts

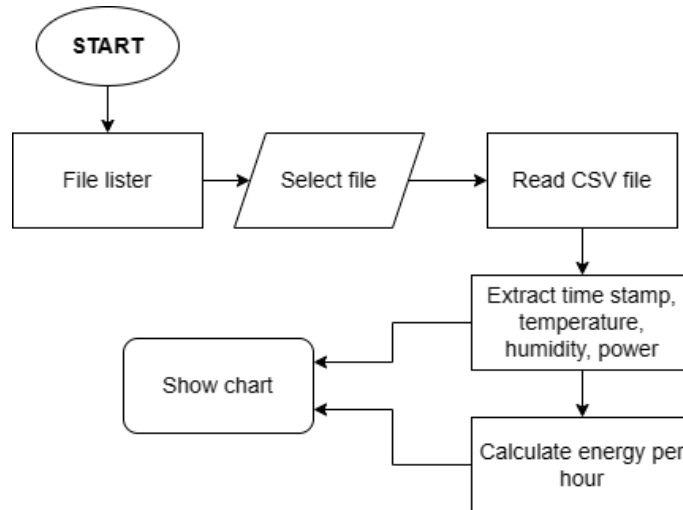


Figure 3.9. Generate chart from log file diagram

3.5.2. Delete log file

Users can manually delete log files, or the files will be automatically deleted if they exceed 30 days.

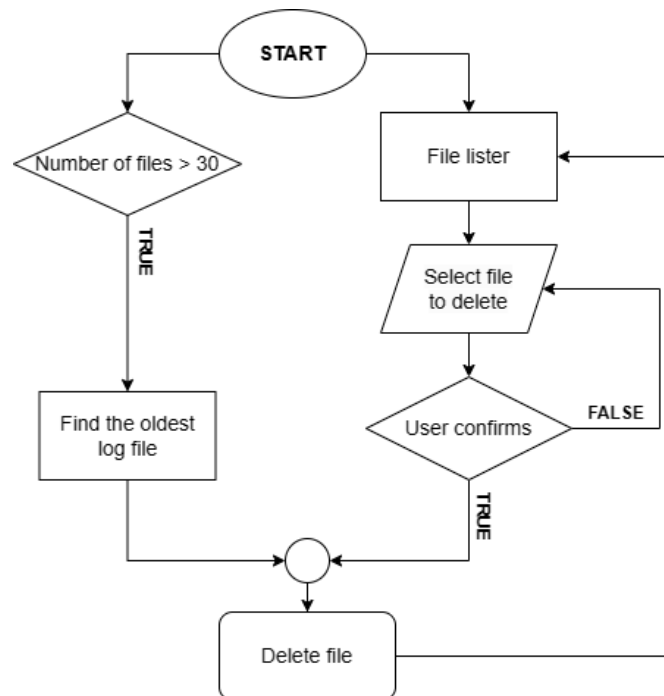


Figure 3.10. Manage file digram

4. Result and summary



Figure 4.1. Home Automation System model

Summary:

- We have successfully developed a system with all the basic features and components of a smart home
- The system meets the established criteria, operates reliably, and can be controlled and monitored via the internet
- The device is compatible with existing electrical appliances, easy to install and maintain
- The accuracy of the facial recognition model reaches 98% with a recognition time of approximately 1 second

5. User Manual

5.1. Connection Configuration

- Step 1: Press and hold the “config button” for three seconds and wait until the LCD screen displays “Please visit 192.168.4.1” as shown in the image below



Figure 4.1. Config display

- Step 2: Connect to the 'Home Automation System' Wi-Fi network.
- Step 3: Use any browser to access the page '192.168.4.1'. and enter the parameters as shown in the image below

The image shows a web-based configuration interface. On the left, the 'System Configuration' section has a 'Select network for ESP32' dropdown menu with a list of networks: P1602, P1602, 1602, P1702_2, 1603, P1702, P1702, Minh Tung, Juju, Ngan An, and Son Phong. Below this is a 'WIFI' section with 'SSID' and 'PASSWORD' input fields. On the right, the 'MQTT' section contains input fields for 'ADDRESS', 'USERNAME', 'PASSWORD', 'PORT', 'PUB TOPIC', and 'SUB TOPIC', along with a green 'SUBMIT' button. Orange arrows point from labels to the corresponding fields: 'Select WiFi network' to the dropdown, 'Enter WiFi password' to the password field, 'MQTT Broker Address' to the address field, 'MQTT password' to the password field, 'MQTT Publish Topic' to the pub topic field, 'MQTT username' to the username field, 'MQTT Port' to the port field, and 'MQTT Subscribe Topic' to the sub topic field.

Figure 4.2. Config UI

- Configuration is successful when the MCU resets and the green light is on.

5.2. Open Dashboard

To access the dashboard, visit the address vikings.hopto.org:1880/ui, you need to log in with user name and password.

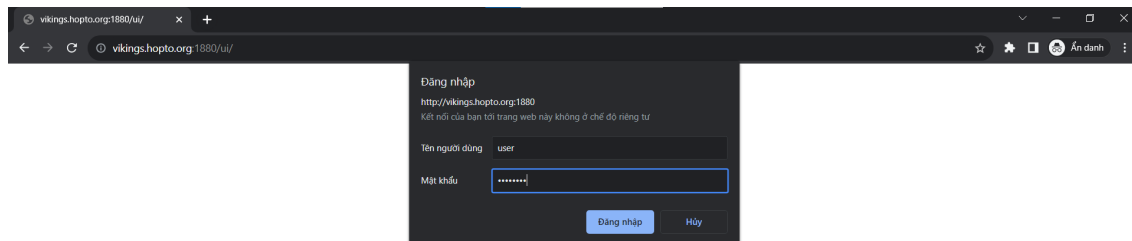


Figure 4.3. Log in screen

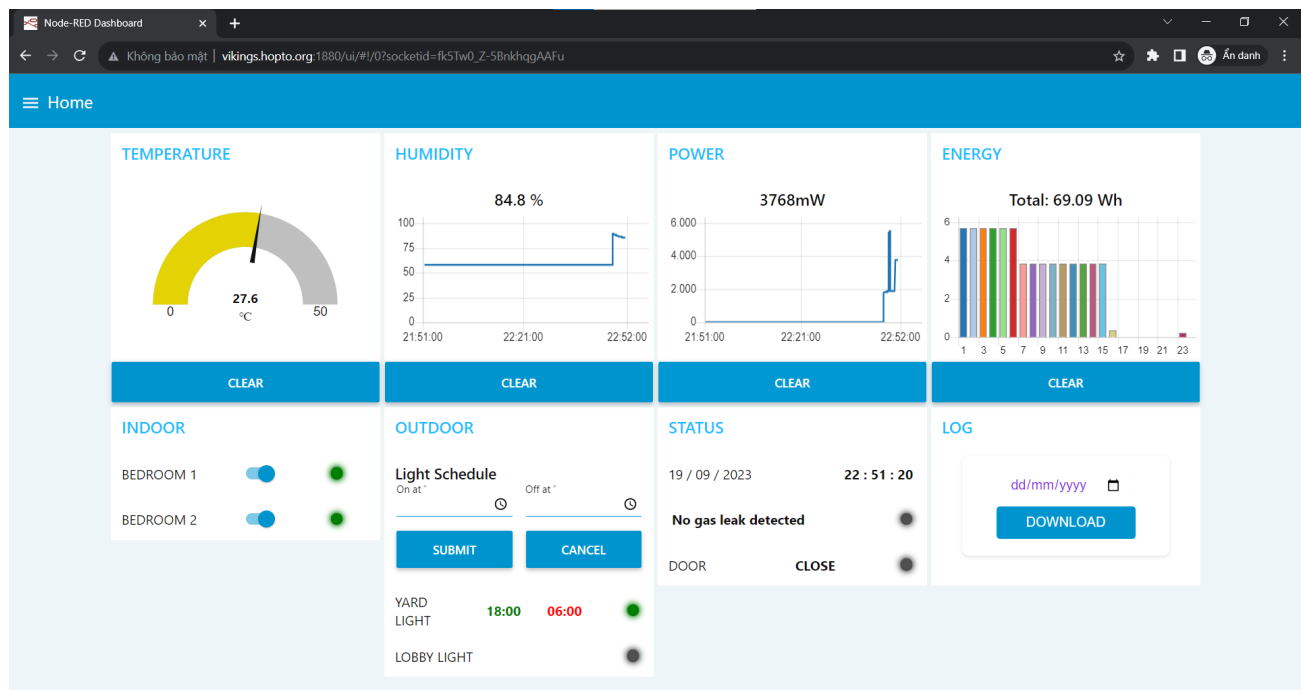


Figure 4.4. Dashboard Overview

5.3. Control devices through dashboard

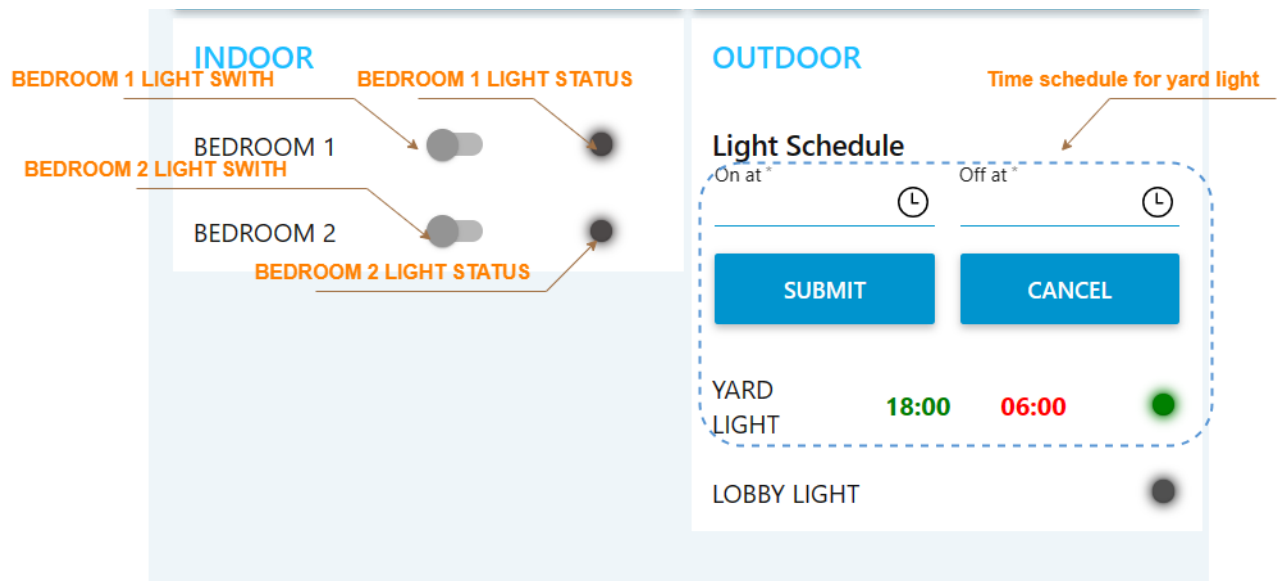


Figure 4.5. Control Device UI

From tab “Home” on Dashboard, the device can be controlled in two ways:

- Controlled by the button switch.
- Time schedule.

The device's status corresponds to the status light on Dashboard

5.4. Download log file

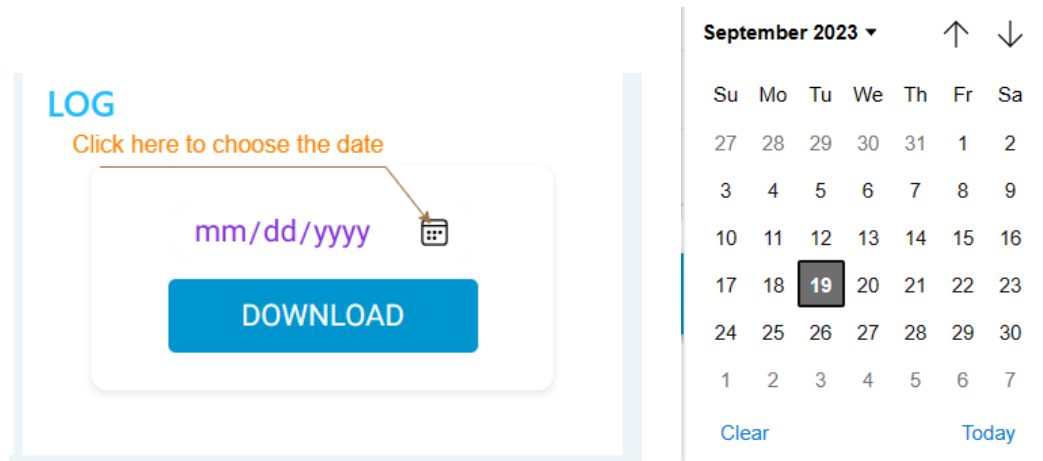


Figure 4.6. Choose date to download log file

A	B	C	D
timeStamp	Temperature	Humidity	Power
0:00:00	27.21	50.22	5733.43
0:05:00	27.26	50.06	5730.89
0:10:02	27.3	50.03	5713.37
0:15:00	27.24	50.32	5363.48
0:20:00	27.2	50.44	1914.32
0:25:00	27.2	50.1	1917.13
0:30:00	27.14	49.87	1920.82
0:35:00	27.02	49.81	1907.94
0:40:01	26.86	49.93	1904.69
0:45:00	26.72	50.06	1918.89
0:50:00	26.56	50.25	1923.05

Figure 4.7. Log file example

To retrieve data from previous days, go to the log section, select the desired date, and then press the **Download button**. The downloaded data will be in CSV format

****Note: The log file will be automatically deleted after 30 days.***

5.5. Door control

To unlock the door from the outside, you need to press the button located outside the door, as shown in the **Figure 4.8**. When the button is pressed, the camera will activate and verify the user's face, if it matches the authorized user, the door will unlock.



Figure 4.8. Unlock the door with Facial Recognition

Unlocking the door will be easier from the inside, just press the door unlock button as shown in the **Figure 4.9**, and the door will be unlocked.

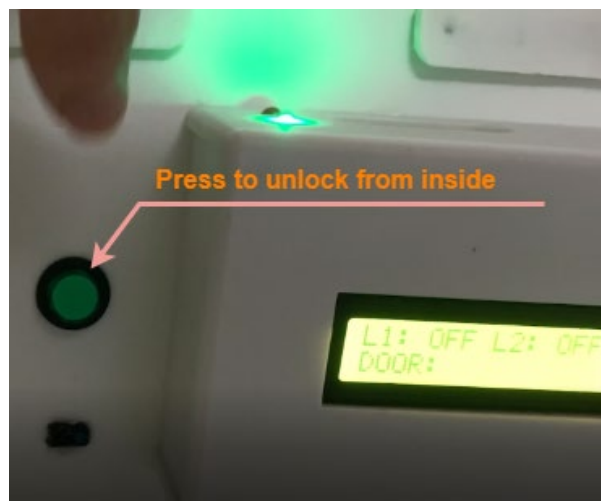
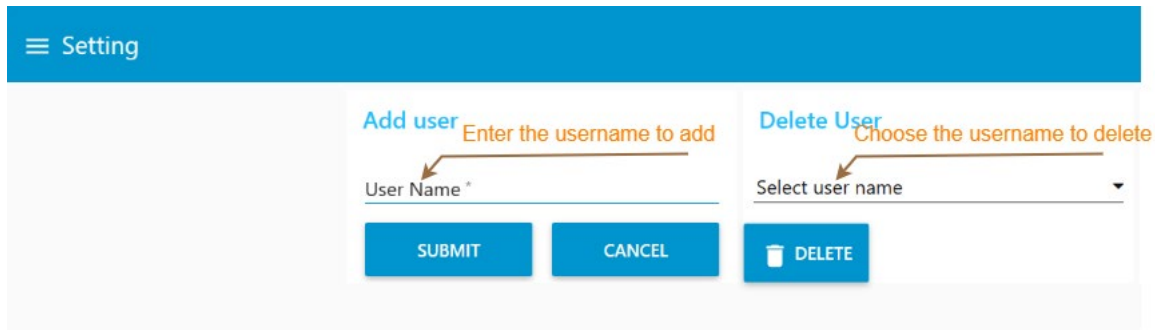


Figure 4.9. Unlock the door from inside the home

5.6. Add / Delete user

To add a new member's face, go to the Setting tab on the Dashboard. Enter the new member's name, place their face in front of the camera, and press submit. At this point, the face data collection process begins, please keep it steady until the 'add user successful' message appears.

To delete another member's face, go to the “DELETE” section, select the member's name from the list, and press delete. The data related to that member will be deleted, and they won't be able to unlock the door during the next recognition.



The screenshot shows a mobile application interface titled 'Setting'. It contains two main sections: 'Add user' and 'Delete User'. The 'Add user' section has a text input field labeled 'User Name *' with a red arrow pointing to it and the text 'Enter the username to add' above it. Below this field are two buttons: 'SUBMIT' and 'CANCEL'. The 'Delete User' section has a dropdown menu labeled 'Select user name' with a red arrow pointing to it and the text 'Choose the username to delete' above it. Below this dropdown is a button labeled 'DELETE' with a trash can icon.

Figure 4.10. Add & Delete user

5.7. Local control devices

To control the device without using the internet, there are two methods:

- Press the switch button next to the device (for the Viking_1 model).
- For the Viking_2 model, you can control the device automatically through the infrared sensor.



Figure 4.11. Local control devices

5.8. File Management

To facilitate better data analysis and provide a more visual representation, go to the File Manager tab on the Dashboard. Select the file you want to graph, then click “Graph”. The graph will be drawn and displayed according to the data type.

Furthermore, in the “File Manager” tab, you can refresh or delete files containing data from previous days

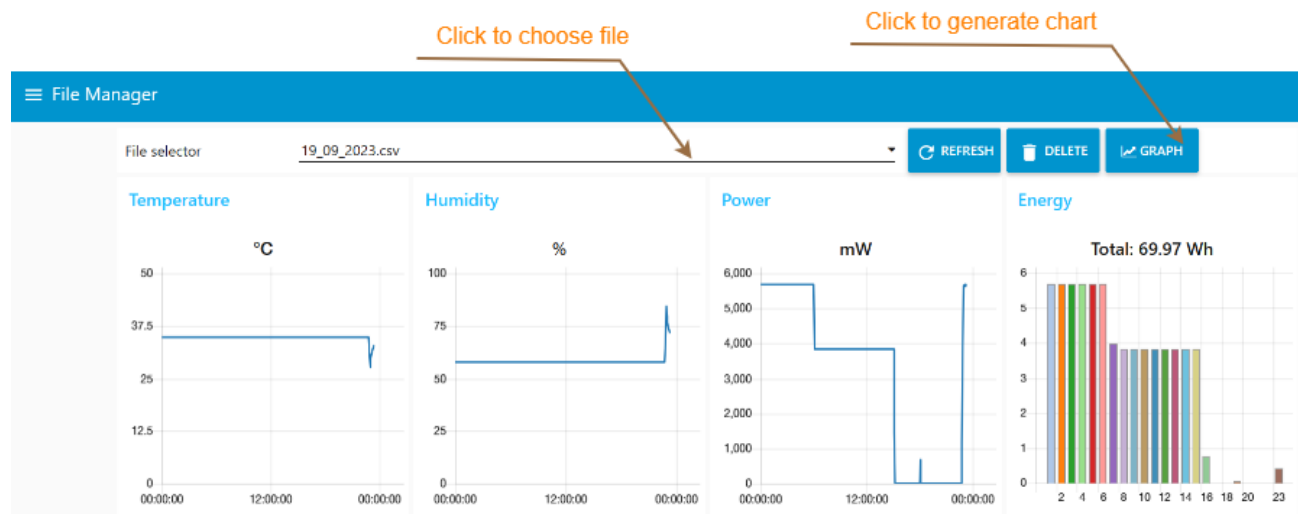


Figure 4.12. File management screen