DIPARTIMENTO DI INGEGNERIA
INFORMATICA, MODELLISTICA,
ELETTRONICA E SISTEMISTICA

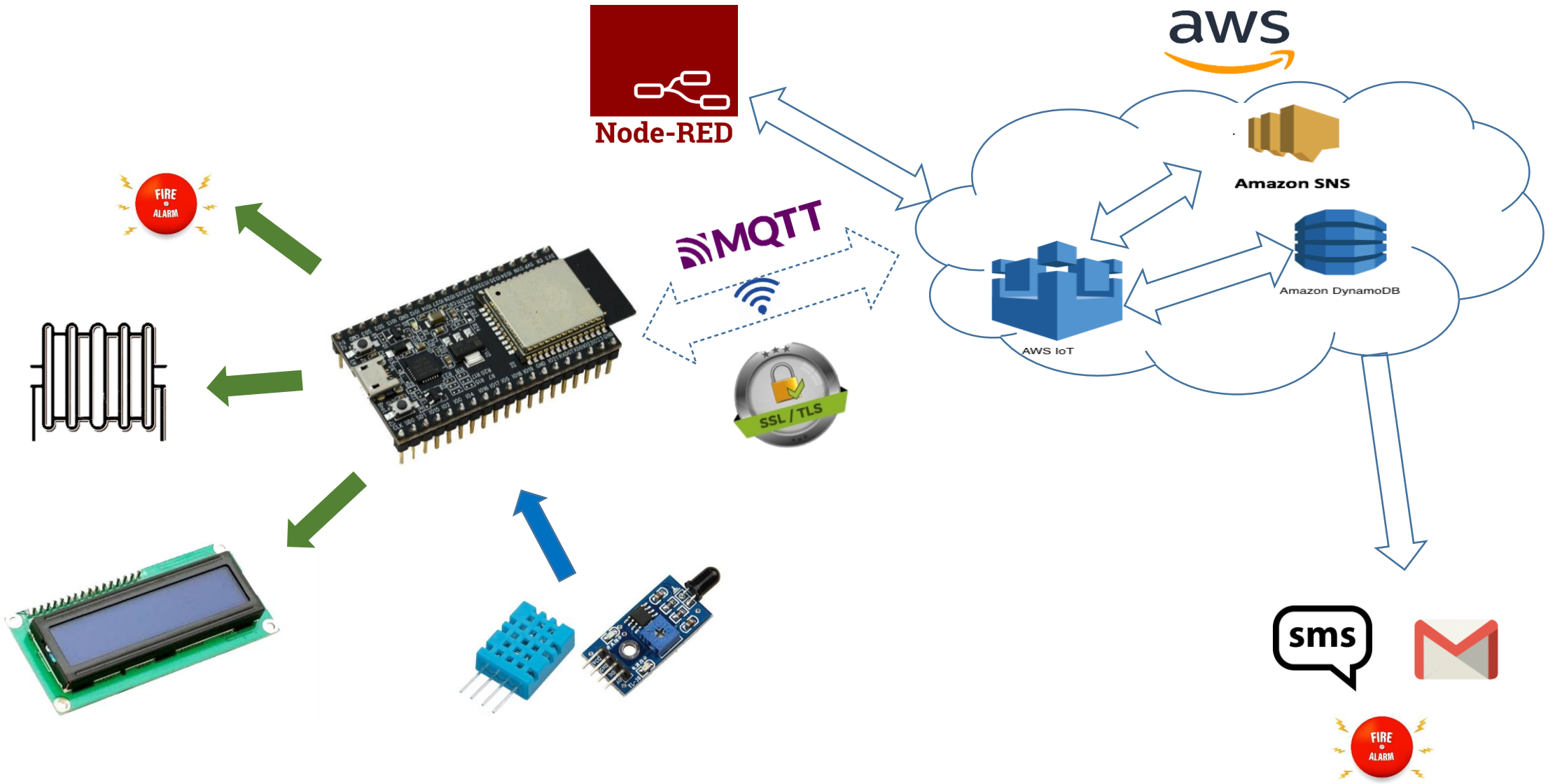
DIMES

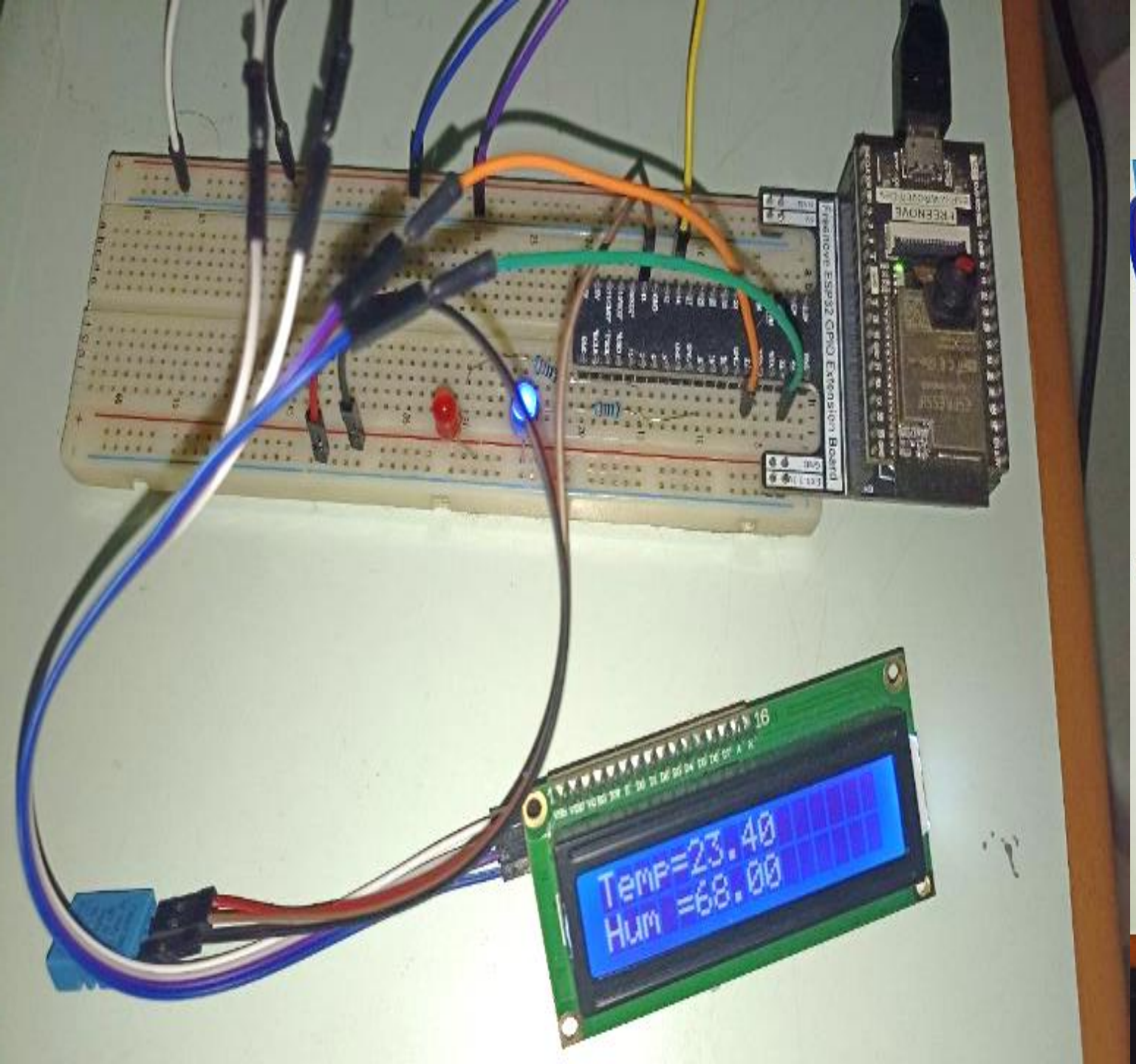
Secure IoT System

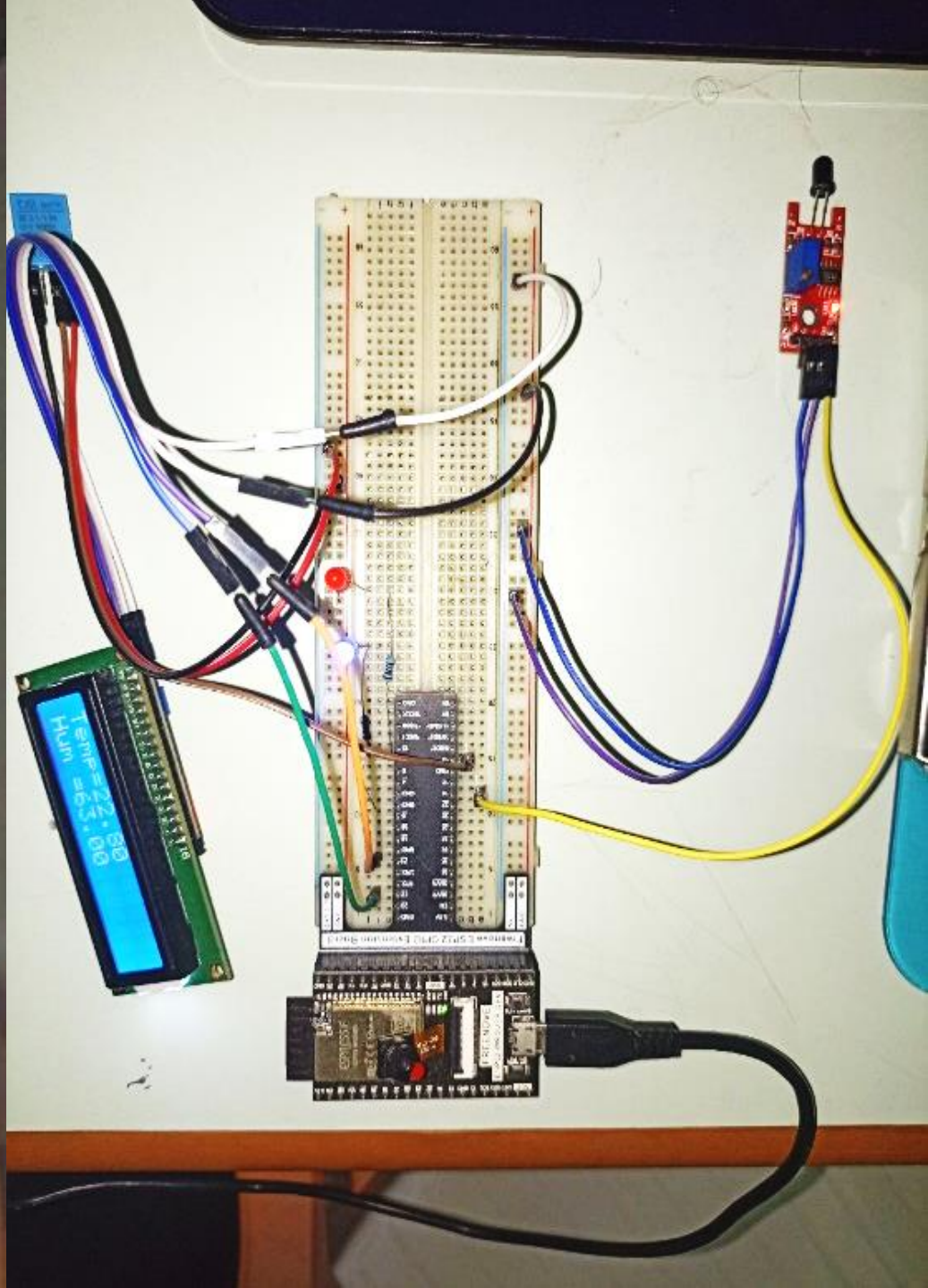
AHMAD MAHMOD

MOHAMAD ISSAM SAYYAF

Idea of The Project




Freenove ESP32 CAM Extension Board
FREENOVE
Temp=23.40
Hum =68.00


Temp=22.00
Hum =63.00

IoT Stack

Node-RED

AWS IOT

WPA2

SSL / TLS

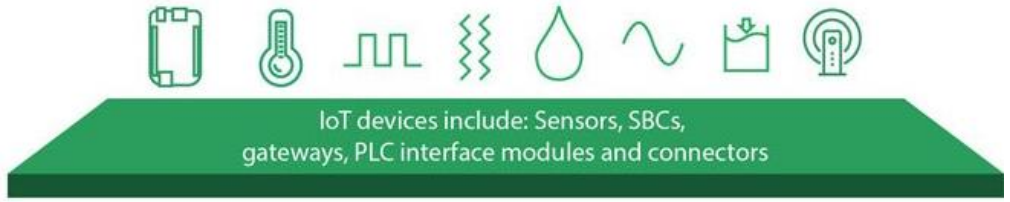
MQTT

ARDUINO

ESP32

IoT Stack

IoT Device (physical)



ESP32

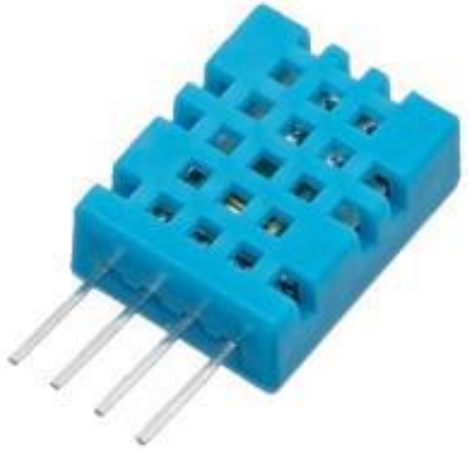
- ESP32 is designed for use in small, low-power devices, and is particularly well-suited for Internet of Things (IoT) applications. Some features of the ESP32 include:
  - Support for 802.11b/g/n Wi-Fi
  - Support for Bluetooth 4.2 and Bluetooth 5
  - A wide range of peripherals, including ADC, PWM, I2C, I2S, UART, and more

IoT Stack

IoT Device (physical)

DHT11 Sensor

- The DHT11 sensor measures both temperature and humidity and can communicate the data to a microcontroller using a single-wire digital interface.



Flame Sensor

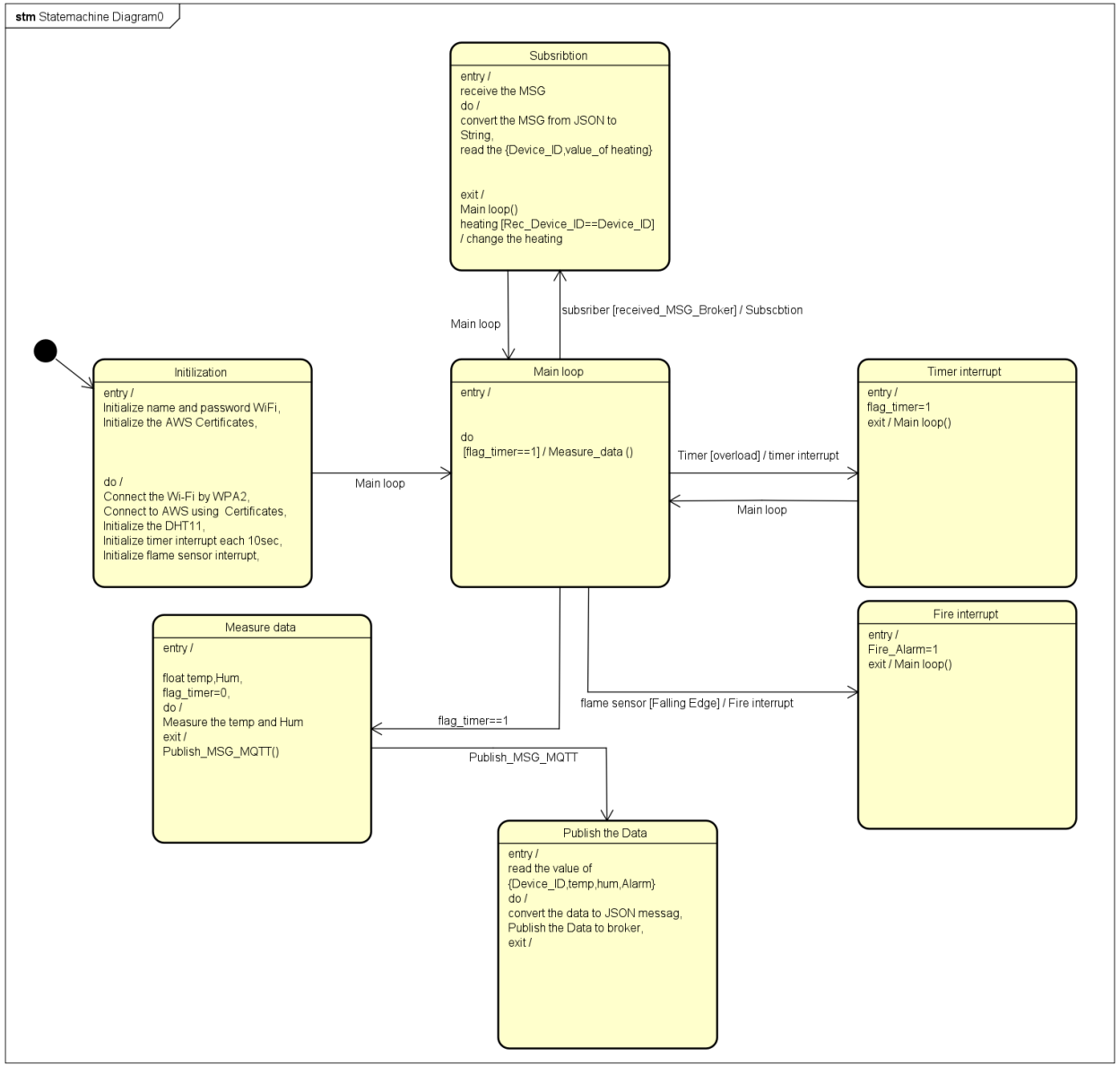
- A flame sensor is a device that is used to detect the presence of a flame or fire. These sensors use an infrared (IR) sensor to detect a flame's presence by measuring a fire's IR emissions.

IoT Stack

Device Software

ARDUINO

Languages used include: Linux, C, Perl, Python, Qt



IoT Stack

Communications

- WPA2 (Wi-Fi Protected Access II) is a security protocol used in Wi-Fi networks to encrypt the data transmitted over the air.
- It provides stronger security compared to its predecessor WPA, using AES encryption.
- WPA2 is the most commonly used security protocol for Wi-Fi networks and is recommended for home and small business use.

IoT Stack

Communications

- SSL (Secure Sockets Layer) and TLS (Transport Layer Security) are cryptographic protocols used to secure internet communications by encrypting data transmitted between a client (such as a web browser) and a server (such as a website).
- They are widely used to secure websites, email, and other internet services, and are designed to prevent eavesdropping, tampering, and message forgery.
- SSL/TLS certificates are issued by trusted third-party certificate authorities to verify the identity of the website owner.

IoT Stack

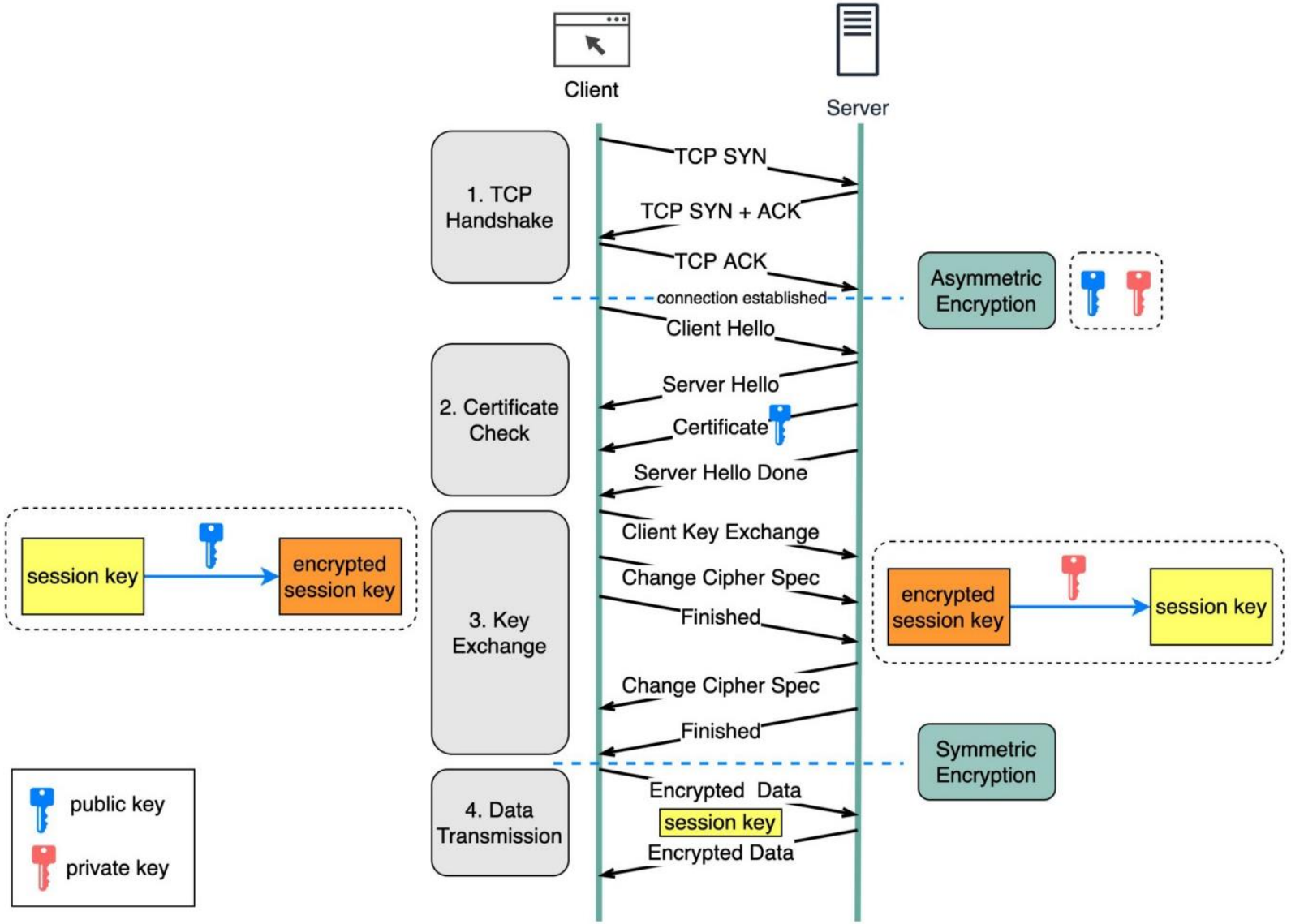
Communications

WPA2

SSL / TLS

MQTT

Wired, Bluetooth, WiFi, Zigbee, Thread,
LTE-M/NB-IoT/2G/3G/4G/5G cellular networks, LoRaWAN



IoT Stack

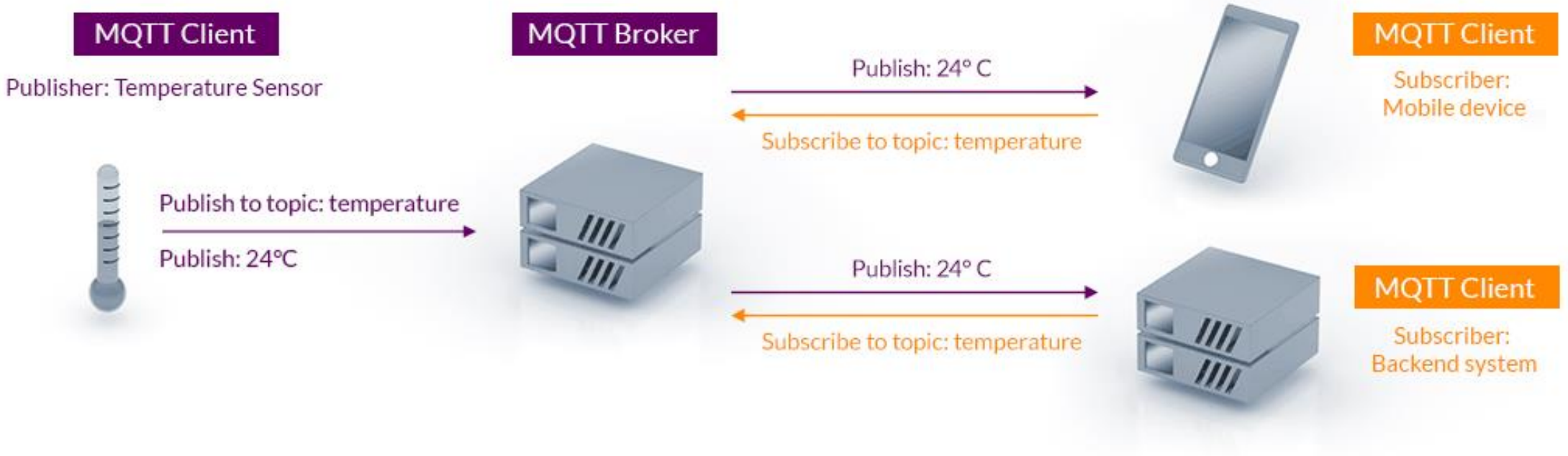
Communications

- MQTT (Message Queuing Telemetry Transport) is a lightweight, publish-subscribe network protocol used for Internet of Things (IoT) and Machine-to-Machine (M2M) communications.
- It is designed to be efficient and low-overhead, making it ideal for use in resource-constrained devices and low-bandwidth networks.
- MQTT operates on a Publish/Subscribe model, where clients subscribe to topics to receive messages, and publish messages to topics.
- The server, known as a broker, routes the messages between clients and ensures reliable delivery.
- MQTT is commonly used for real-time monitoring and control of IoT devices and systems.

MQTT

IoT Stack

Communications

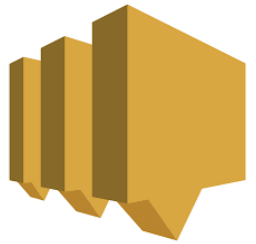


IoT Stack

Cloud Platform

AWS IoT

- AWS IoT is a cloud platform that allows devices to securely connect and interact with cloud applications and other devices.
- The platform supports MQTT as a communication protocol for IoT devices, allowing for efficient and low-overhead data transmission.
- By using AWS IoT, you can easily store the data from IoT devices in Amazon DynamoDB, and use SNS to trigger actions such as sending SMS messages and emails.
- This allows you to build a comprehensive and scalable IoT solution that can perform real-time monitoring, data processing, and alerting.



SNS

AWS IoT

DynamoDB

IoT Stack

Cloud Platform

aws | Services | Search [Alt+S] | N. Virginia | ISSAM

S3 | IoT Core | DynamoDB | AWS Glue | IAM

DynamoDB

- Dashboard
- Tables
  - Update settings
  - **Explore items**
- PartiQL editor New
- Backups
- Exports to S3
- Imports from S3 New
- Reserved capacity
- Settings New

▼ DAX

- Clusters
- Subnet groups
- Parameter groups

Items returned (50)

Actions ▼ | Create item

1 ...

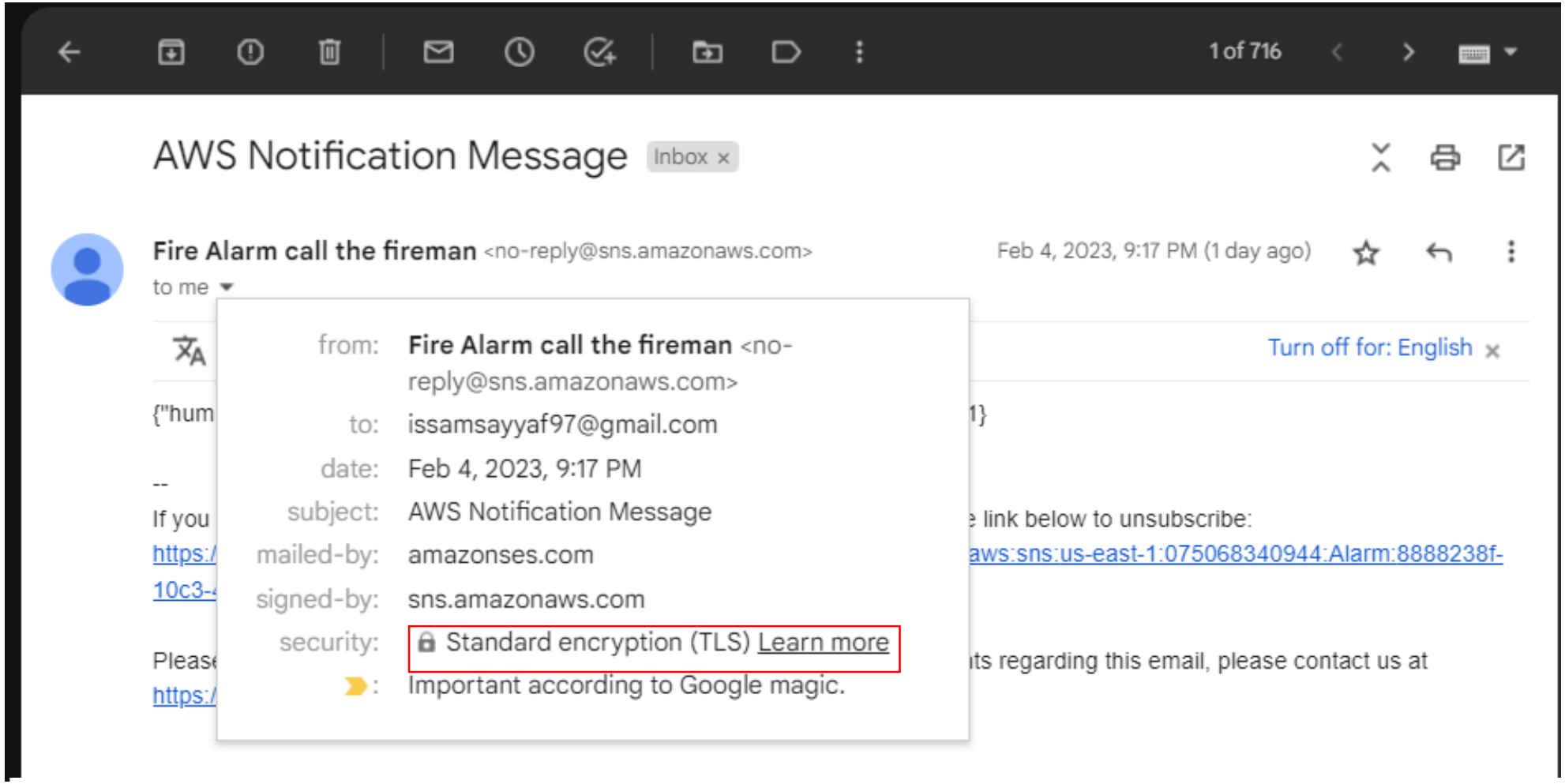
Device ID	timestamp	MyMessage
ESP32_001	1671400653317	{ "temperature" : { "N" : "22.79999924" }, "humidity" : { ...
ESP32_001	1671400658347	{ "temperature" : { "N" : "22.79999924" }, "humidity" : { ...
ESP32_001	1671400663378	{ "temperature" : { "N" : "22.79999924" }, "humidity" : { ...
ESP32_001	1671400668385	{ "temperature" : { "N" : "22.79999924" }, "humidity" : { ...
ESP32_001	1671400673404	{ "temperature" : { "N" : "22.79999924" }, "humidity" : { ...
ESP32_001	1671400678374	{ "temperature" : { "N" : "22.79999924" }, "humidity" : { ...
ESP32_001	1671400683448	{ "temperature" : { "N" : "22.79999924" }, "humidity" : { ...

Feedback | Looking for language selection? Find it in the new Unified Settings | © 2023, Amazon Web Services, Inc. or its affiliates. | Privacy | Terms | Cookie preferences

IoT Stack

Cloud Platform

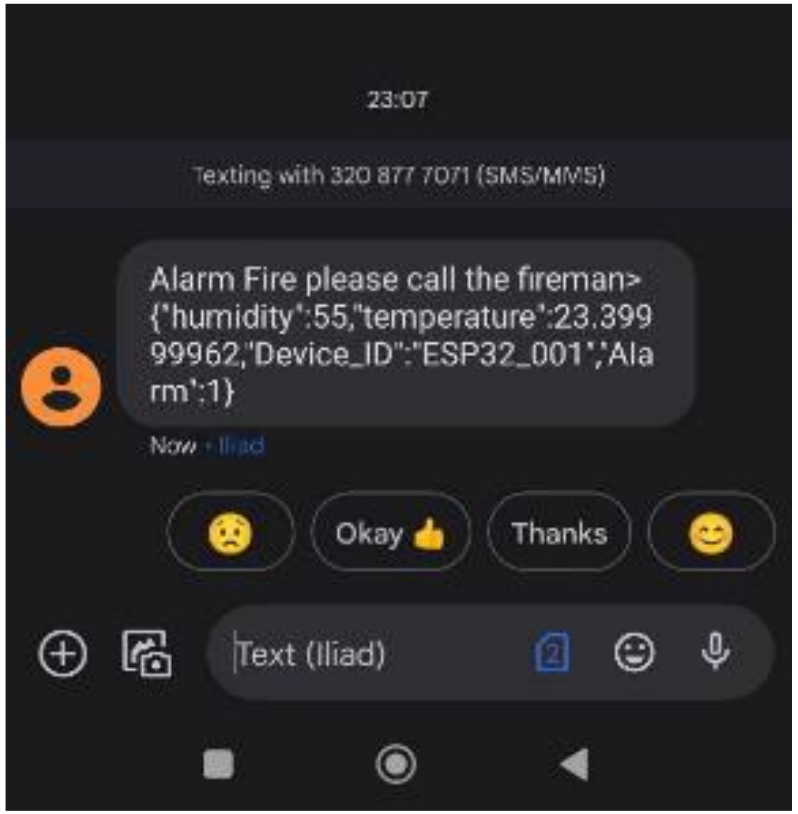
SNS



IoT Stack

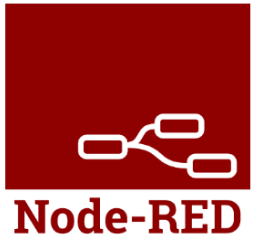
Cloud Platform

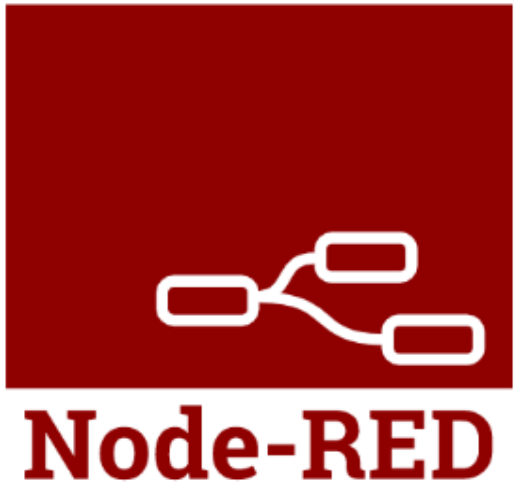
SNS



IoT Stack

Application





Username:

Password:

Login

Device

ID ESP32_001

Alarm State

Temperature

23

-10 50

slider 51

humidity

60

units

Device

ID ESP32_001

Alarm State

Temperature

24

-10 50

slider 100

humidity

76

units

Security Aspects

- First level of security: The esp32 connects with Wi-Fi using WPA2 protocol, So the connection between the node and Access point is encrypted and secure.
- Second level of security: The connection between the node and AWS server is secure by using SSL/TLS with MQTT for this reason the node uses 3 certificates to make authentication and encryption.
- Third level of security: The policies of the certificate are restricted in, Amazon. So these certificates do not have the right to access to different services.
- Fourth level of security: The monitor data is done by Node-red, also the access to node-red is secured by username and password.

References

[1]. https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/

[2]. Jurcut, Anca & Ranaweera, Pasika & Xu, Lina. (2019). Introduction to IoT Security. 10.1002/9781119471509.w5GRef260.

[3]. https://aws.amazon.com/iot/

[4]. https://mqtt.org/

[5]. https://www.appviewx.com/education-center/what-is-tls-ssl-protocol/

[6]. https://nodered.org/

[7]. https://www.arduino.cc/

[8]. https://www.espressif.com/en