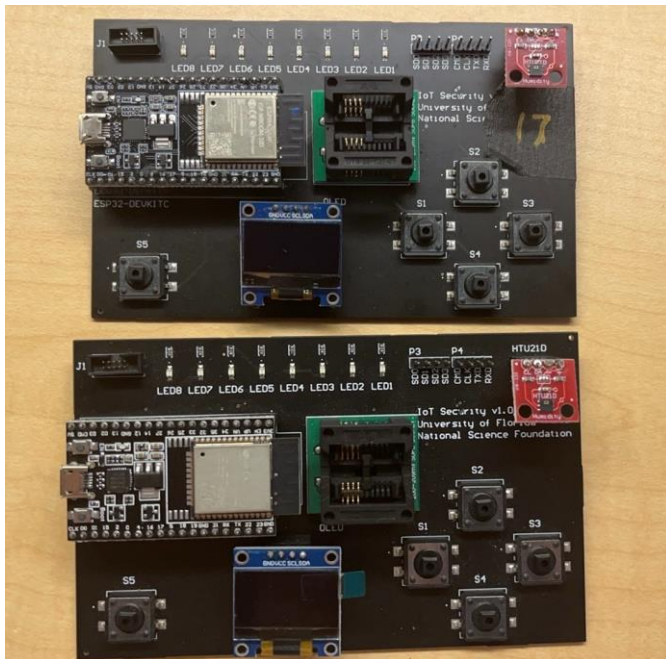


# Cloud-based dual inspection system for factory environment

# 1

Description

# System Overview



- Our project is a temperature and humidity alarm system designed for sensitive environments, especially factories where production is critical. Two ESPs act as temperature and humidity detectors, connected to a WIFI connection that sends a constant stream of temperature and humidity data to the AWS.

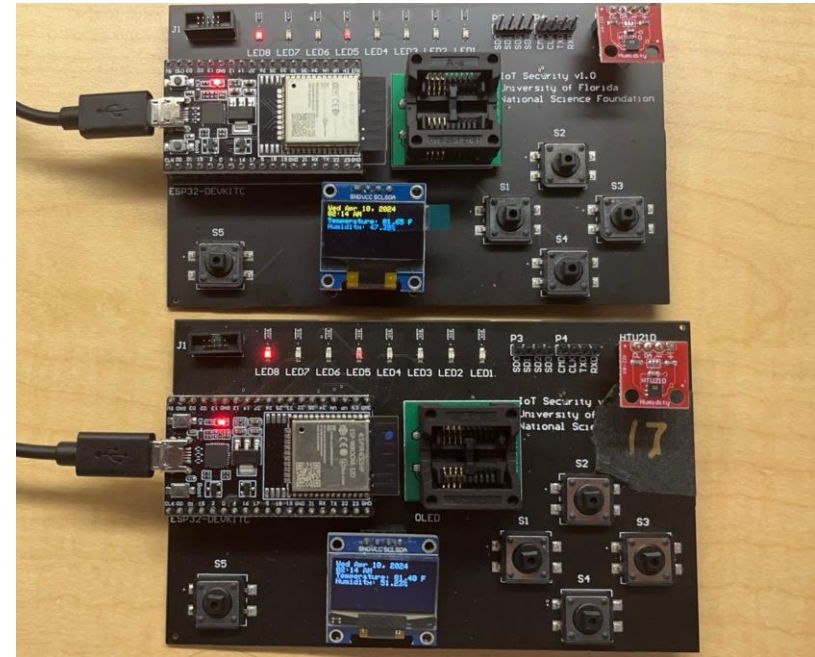
Sensors used: Temperature and humidity sensors

Computing platform used: AWS

Software used: VsCode - PlatformIO

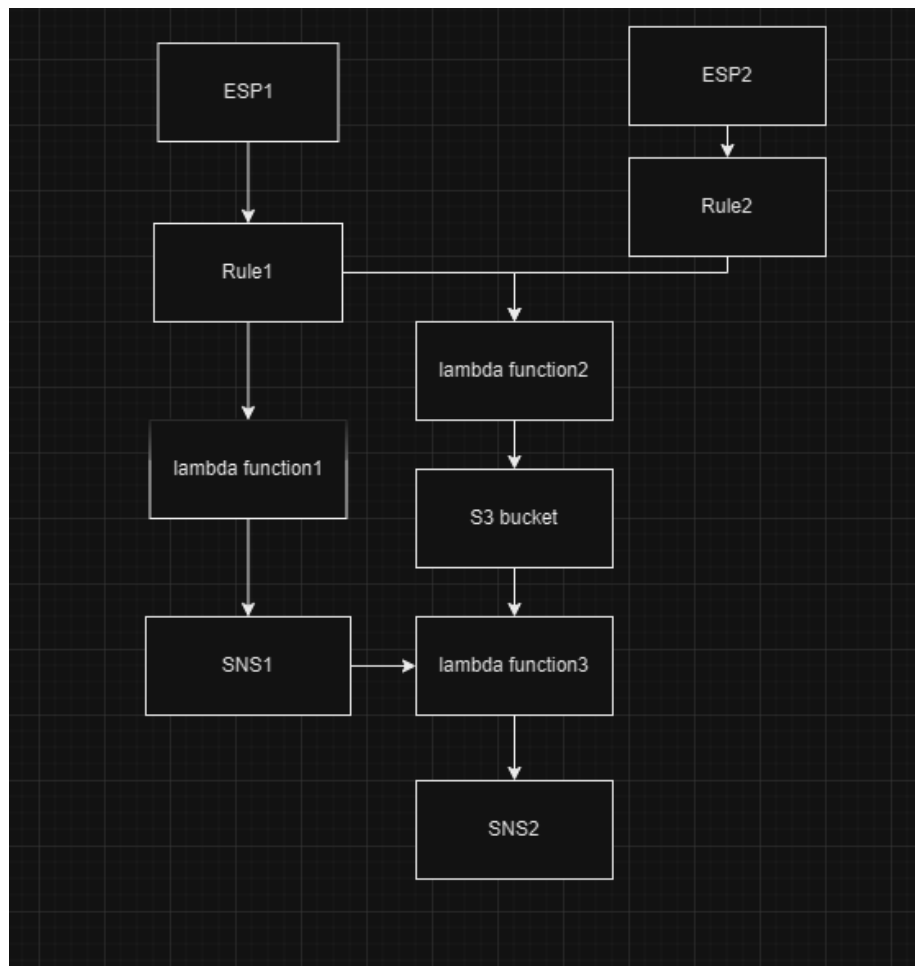
# System Function

- When AWS receives a temperature above 70 degrees and a humidity below 30%, it sends an email warning to the manager to report the anomaly. After AWS sends out an alert, it compares the data collected by another ESP within a minute. If the difference in temperature and humidity is less than 10, It will continue to send emails alerting the factory to abnormal conditions. Judgment is made by secondary detection, thus avoiding false alarms due to certain malfunctions.



## Network Structure

Solution



## AWS Setup—Things

**AWS IoT** X

Monitor

Connect

- Connect one device
- ▶ Connect many devices

Test

- MQTT test client

Manage

- ▼ All devices
  - Things
  - Thing groups
  - Thing types
  - Fleet metrics
- ▶ Greengrass devices
- Software packages [New](#)
- ▶ Remote actions
- ▶ Message routing
- Retained messages
- ▶ Security

**Things (4)** Info [Refresh](#) [Advanced search](#) [Run aggregations](#) [Edit](#) [Delete](#) [Create things](#)

An IoT thing is a representation and record of your physical device in the cloud. A physical device needs a thing record in order to work with AWS IoT.


| <input type="checkbox"/> | Name                             | Thing type |
|--------------------------|----------------------------------|------------|
| <input type="checkbox"/> | <a href="#">scd_mosquitto_id</a> | -          |
| <input type="checkbox"/> | <a href="#">scd_esp</a>          | -          |
| <input type="checkbox"/> | <a href="#">17_mosquitto</a>     | -          |
| <input type="checkbox"/> | <a href="#">17_ESP</a>           | -          |

0 things selected

## AWS Setup——Policy

**mosquitto\_id** [Info](#) [Edit active version](#) [Delete](#)

**Details**

|   |                                  |   |  |
|---|----------------------------------|---|--|
| Policy ARN<br> <code>arn:aws:iot:us-east-2:767397760104:policy/mosquitto_id</code> | Active version<br><code>9</code> | Created<br>March 25, 2024, 12:59:14 (UTC-04:00) | Last updated<br>March 25, 2024, 12:59:14 (UTC-04:00) |
|---|----------------------------------|---|--|

[Versions](#) | [Targets](#) | [Noncompliance](#) | [Tags](#)


**Active version: 9** [Info](#) [Builder](#) [JSON](#)

| Policy effect | Policy action | Policy resource  |
|---------------|---------------|--|
| Allow         | iot:Subscribe | arn:aws:iot:us-east-2:767397760104:topicfilter/lab5    |
| Allow         | iot:Receive   | arn:aws:iot:us-east-2:767397760104:topic/lab5          |
| Allow         | iot:Connect   | arn:aws:iot:us-east-2:767397760104:client/mosquitto_id |

## AWS Setup——Policy

**scd\_mosquitto\_id** [Info](#) [Edit active version](#) [Delete](#)

**Details**

|   |                                  |   |  |
|---|----------------------------------|---|--|
| Policy ARN<br> <code>arn:aws:iot:us-east-2:767397760104:policy/scd_mosquitto_id</code> | Active version<br><code>4</code> | Created<br>April 05, 2024, 16:49:11 (UTC-04:00) | Last updated<br>April 05, 2024, 16:49:11 (UTC-04:00) |
|---|----------------------------------|---|--|

[Versions](#) [Targets](#) [Noncompliance](#) [Tags](#)

**Active version: 4** [Info](#) [Builder](#) [JSON](#)

| Policy effect | Policy action | Policy resource   |
|---------------|---------------|---|
| Allow         | iot:Connect   | <code>arn:aws:iot:us-east-2:767397760104:client/scd_mosquitto_id</code> |
| Allow         | iot:Subscribe | <code>arn:aws:iot:us-east-2:767397760104:topicfilter/lab4</code>        |
| Allow         | iot:Receive   | <code>arn:aws:iot:us-east-2:767397760104:topic/lab4</code>              |







## AWS Setup—Rules

[AWS IoT](#) > [Message routing](#) > [Rules](#) > email\_final7

### email\_final7 Info

[Activate](#) [Deactivate](#) [Edit](#) [Delete](#)

#### Details

|  |  |                                      |
|--|--|--------------------------------------|
| Description  |  |                                      |
| securite   |  |                                      |
| ARN  | Topic  | Created date                         |
|  arn:aws:iot:us-east-2:767397760104:rule/email_final7 |  lab5                     | April 05, 2024, 23:48:31 (UTC-04:00) |
| Status   | Basic ingest topic   |                                      |
|  Active   |  \$aws/rules/email_final7 |                                      |

#### SQL statement

|   |             |
|---|-------------|
| SQL statement   | SQL version |
| SELECT * FROM 'lab5' WHERE temperature > 70 AND humidity < 30 | 2016-03-23  |

[Actions](#) | [Error action](#) | [Tags](#)

#### Actions (1)

[View details](#)

Actions occur when an event is triggered. Actions are executed from top to bottom, until all actions are completed or an error occurs. To add or remove actions, you will need to edit the rule.

## AWS Setup—Rules

AWS IoT > Message routing > Rules > senddatalab5

**senddatalab5** Info Activate Deactivate Edit Delete

**Details**

Description  
send\_data

ARN  
arn:aws:iot:us-east-2:767397760104:rule/senddatalab5

Topic  
lab5

Created date  
April 07, 2024, 21:29:51 (UTC-04:00)

Status  
Active

Basic ingest topic  
\$aws/rules/senddatalab5

**SQL statement**

SQL statement  
SELECT \* FROM 'lab5' WHERE temperature > 70 AND humidity < 30

SQL version  
2016-03-23

**Actions** | Error action | Tags

**Actions (1)** View details

## AWS Setup——Rules

### scd\_final7 [Info](#)

[Activate](#) [Deactivate](#) [Edit](#) [Delete](#)

#### Details

Description

send\_dataiab4

ARN

arm:aws:iot:us-east-2:767397760104:rule/scd\_final7

Status

Active

Topic

lab4

Basic ingest topic

\$aws/rules/scd\_final7

Created date

April 07, 2024, 21:29:43 (UTC-04:00)

#### SQL statement

SQL statement

SELECT \* FROM 'lab4' WHERE temperature > 70 AND humidity < 30

SQL version

2016-03-23

[Actions](#) [Error action](#) [Tags](#)

#### Actions (1)

[View details](#)

# 2

## Risk Assessment

## Initial Risk Assessment --- Methodology of scoring

| Vulnerability Rating (1-5) | Description  |
|----------------------------|--|
| 1 - Very Low               | The vulnerability is unlikely to be exploited within the next year.              |
| 2 - Low                    | The possibility exists that the vulnerability could be exploited at some point.  |
| 3 - Medium                 | There is a balanced chance of the vulnerability being exploited within the year. |
| 4 - High                   | It is likely that the vulnerability will be exploited within the next year.      |
| 5 - Very High              | The vulnerability is almost certain to be exploited within the next year.        |

| Impact Rating (1-5) | Description  |
|---------------------|--|
| 1 - Low             | Minimal impact, slight inconvenience or minor costs.   |
| 2 - Low-Medium      | Minor impact, causing noticeable but manageable effects.   |
| 3 - Medium          | Moderate impact, measurable damage that is not severe.   |
| 4 - Medium-High     | Significant impact, serious consequences that may require substantial resources.                 |
| 5 - High            | Major impact, causing major financial loss, legal repercussions, or severe damage to reputation. |

### Risk Score Calculation:

The Risk Score is calculated by multiplying the Likelihood(Vulnerability) Rating by the Impact Rating. The resulting score helps prioritize risks.

## Risk categorization

|              |               | Impact →   |         |          |             |        |
|--------------|---------------|------------|---------|----------|-------------|--------|
|              |               | Negligible | Minor   | Moderate | Significant | Severe |
| Likelihood ↑ | Very Likely   | Low Med    | Medium  | Med Hi   | High        | High   |
|              | Likely        | Low        | Low Med | Medium   | Med Hi      | High   |
|              | Possible      | Low        | Low Med | Medium   | Med Hi      | Med Hi |
|              | Unlikely      | Low        | Low Med | Low Med  | Medium      | Med Hi |
|              | Very Unlikely | Low        | Low     | Low Med  | Medium      | Medium |

- **Physical Risks:** Risks that involve physical damage to, or theft of, the IoT devices.
- **Communication Risks:** Risks associated with the transfer of data between devices and servers.
- **Cybersecurity Risks:** Risks related to unauthorized digital access to systems, such as hacking or malware.
- **Operational Risks:** Risks that impact the continued operation of the IoT system, including service disruption and data loss due to system malfunctions or configuration errors.

## Risk Matrix

| Risk ID | Risk Description  | Likelihood (1-5) | Impact (1-5) | Risk Score<br>(Likelihood x Impact) | Risk Type     |
|---------|---|------------------|--------------|-------------------------------------|---------------|
| R1      | The factory experienced a power outage or power failure | 2                | 5            | 10                                  | Physical Risk |
| R2      | Sensors aging leads to damage                           | 2                | 5            | 10                                  |               |
| R3      | Physical theft or tampering with esp32 boards           | 1                | 5            | 5                                   |               |

## Risk Matrix

| Risk ID | Risk Description   | Likelihood (1-5) | Impact (1-5) | Risk Score<br>(Likelihood x Impact) | Risk Type          |
|---------|--|------------------|--------------|-------------------------------------|--------------------|
| R4      | Man-in-the-middle attacks during transmission to AWS             | 2                | 4            | 8                                   | Communication risk |
| R5      | SNS message spoofing   | 2                | 3            | 6                                   |                    |
| R6      | Data corruption in transit due to unreliable communication links | 3                | 3            | 9                                   |                    |
| R7      | Wifi been attacked   | 3                | 4            | 12                                  |                    |



## Risk Matrix

| Risk ID | Risk Description   | Likelihood (1-5) | Impact (1-5) | Risk Score<br>(Likelihood x Impact) | Risk Type           |
|---------|--|------------------|--------------|-------------------------------------|---------------------|
| R8      | Protocols encryption leading to data leaks                       | 3                | 4            | 12                                  | Cybersecurity Risks |
| R9      | Unencrypted Lambda invocations causing data breaches             | 2                | 5            | 10                                  |                     |
| R10     | Unauthorized access to AWS IoT rules leading to data mishandling | 3                | 4            | 12                                  |                     |
| R11     | S3 bucket data hacked  | 3                | 5            | 15                                  |                     |
| R12     | Been DDoS attacked   | 3                | 4            | 12                                  |                     |

## Risk Matrix

| Risk ID | Risk Description  | Likelihood (1-5) | Impact (1-5) | Risk Score<br>(Likelihood x Impact) | Risk Type         |
|---------|---|------------------|--------------|-------------------------------------|-------------------|
| R13     | Lambda function errors leading to data loss             | 2                | 3            | 6                                   | Operational Risks |
| R14     | Lack of S3 bucket backup processes leading to data loss | 1                | 4            | 4                                   |                   |
| R15     | AWS service disruption from overloading with messages   | 2                | 3            | 6                                   |                   |

# 3



Risk  
management



## Risk mitigation

Risk mitigation refers to measures taken to reduce the likelihood of a potential risk occurring or to mitigate its impact on the organization. This strategy is aimed at identifying sources of risk and implementing preventive measures to reduce the likelihood of a risk or minimize its potential impact

## Risk transference

Risk transference is the transfer of the financial impact of a potential risk from one organization to another. This is usually accomplished by purchasing insurance or transferring the risk to a third party through a contractual clause.





## Risk acceptance

Risk acceptance is the decision, after assessing a risk, not to take any particular action to avoid, mitigate or transfer the risk. This is usually because the likelihood of the risk is low, the impact is limited, or because the cost of taking action outweighs the potential loss. In this case, the organization decides to accept the risk and prepare for possible negative impacts.

## Risk management strategies

| Risk ID | Risk Mitigation Strategy  | Risk Transference Strategy   | Risk Acceptance Decision   |
|---------|---|--|--|
| R1      | Implement an Uninterruptible Power Supply (UPS) and backup generators. Regularly test backup power systems. | Purchase insurance for business interruption.                              | Accept the residual risk of power outage impacts after mitigation and transference strategies are applied. |
| R2      | Regular maintenance and scheduled replacements based on sensors' expected lifespan.                         | Outsource sensor maintenance to vendors with liability clauses for faults. | Accept the residual risk that comes with the natural wear and tear of sensors.                             |
| R3      | Install security cameras and alarms. Implement device tracking and remote disabling features.               | Purchase insurance for theft and damages.                                  | Accept the low likelihood of physical theft after physical security enhancements.                          |
| R4      | Use end-to-end encryption for data in transit. Conduct regular security audits.                             | Utilize cloud services that offer shared security responsibility.          | Accept a minimal risk of MITM attacks due to strong encryption protocols in place.                         |

## Risk management strategies

| Risk ID | Risk Mitigation Strategy  | Risk Transference Strategy  | Risk Acceptance Decision   |
|---------|---|---|--|
| R5      | Implement message authentication codes and verification processes for message integrity.          | Employ third-party messaging services with indemnification clauses for spoofing incidents.        | Accept the low-impact risk after implementing strong verification processes.       |
| R6      | Implement redundancy in communication channels and data validation protocols.                     | Contract with reliable service providers and consider service level agreements (SLAs) for uptime. | Accept minor communication inconsistencies that can be quickly resolved.           |
| R7      | Secure the WiFi network with strong encryption, regular password changes, and network monitoring. | Work with ISPs that offer DDoS protection and mitigation services.                                | Accept the risk of WiFi attacks as low probability due to strong network defenses. |



## Risk management strategies

| Risk ID | Risk Mitigation Strategy  | Risk Transference Strategy  | Risk Acceptance Decision  |
|---------|---|---|---|
| R8      | Ensure protocols and services have the latest encryption standards implemented.                 | Contract with third-party cybersecurity firms for additional protection layers. | Accept the risk after employing advanced encryption and regular security reviews. |
| R9      | Enable encryption for all Lambda invocations and use AWS KMS for managing keys.                 | Obtain cyber liability insurance to cover potential data breach costs.          | Accept the risk for non-sensitive data after encryption measures are in place.    |
| R10     | Apply the principle of least privilege for access to AWS IoT rules and enable detailed logging. | Use cloud services that provide breach responsibility and response services.    | Accept minimal risk post-implementation of access controls and monitoring.        |
| R11     | Employ strict access controls, enable versioning, and use MFA for sensitive operations.         | Utilize cloud-based security services with robust data protection guarantees.   | Accept low residual risk given strong data protection and monitoring measures.    |

## Risk management strategies

| Risk ID | Risk Mitigation Strategy  | Risk Transference Strategy  | Risk Acceptance Decision   |
|---------|---|---|--|
| R12     | Plan and implement a DDoS response strategy, including rate limiting and traffic filtering.       | Invest in a Content Delivery Network (CDN) with DDoS mitigation capabilities.             | Accept the risk due to proactive monitoring and a response plan to minimize downtime.                |
| R13     | Enforce strict error handling, logging, and automated rollback procedures in Lambda functions.    | Engage with cloud service management firms for high reliability and error management.     | Accept the risk when mitigation measures are in place to quickly rectify any issues.                 |
| R14     | Introduce regular data backups, cross-region replication, and robust disaster recovery protocols. | Use third-party backup solutions and cloud storage with high durability guarantees.       | Accept the risk for non-critical data and ensure critical data is regularly backed up.               |
| R15     | Implement API throttling, load balancing, and autoscaling for AWS services.                       | Choose cloud services with operational resilience and financial compensation for outages. | Accept some level of risk for message overloading, contingent on alerting and auto-scaling measures. |

# 4

demonstration  
of  
project



Herbert Wertheim  
College of Engineering  
UNIVERSITY of FLORIDA

# Thank You!

POWERING THE NEW ENGINEER TO TRANSFORM THE FUTURE