April 17,2024

IoT Based: Gas-Leakage detection system for chemical labs

<removed for privacy concerns>, <removed for privacy concerns>, gcad-ee, <removed for privacy concerns>

Group-12

INTRODUCTION

- Gas leaks are dangerous and hard to notice incidences that can cause serious damage and poses significant health and safety concerns

- Gases are invisible to the eye and depending on the type, can be very hard to detect, especially since a lab can contain many types of gas.

- Our proposal is an IoT device that will use the humidity and temperature sensors on the board to make a IoT system that will detect a gas leak by sensing the difference temperature and humidity between the norm conditions of the control environment and the current conditions.
- Our system will monitor environmental parameters continuously, identifying potential gas leakages through real-time data analysis

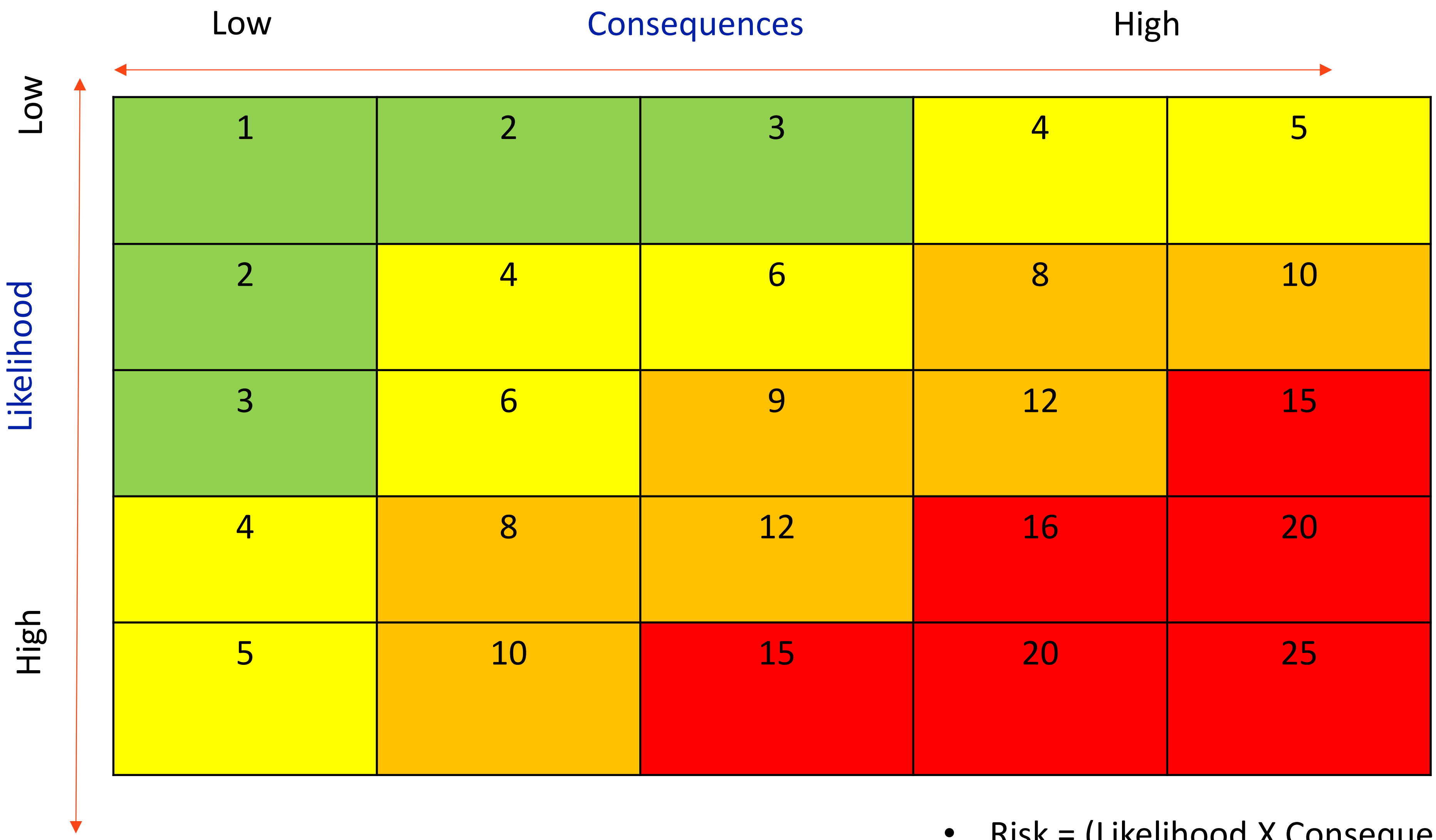
PROJECT OUTLINE

- As a secure monitor broker utilizing the MQTT console within AWS, our focus is dedicated to gas leak detection and temperature regulation in laboratory settings.

- We tackle the challenge of providing swift and precise surveillance to safeguard chemical laboratory from gas leakage.

    - Sensors used:Humidity sensor,Temperature Sensor
    - Platform used: ESP 32
    - Software used: PlatformIO
    - Network Structure: Two MQTT's publish data to AWS ,TLS/SSL protocol

RISK MATRIX



	Low		Consequences		High
Low	1	2	3	4	5
	2	4	6	8	10
Likelihood	3	6	9	12	15
	4	8	12	16	20
High	5	10	15	20	25

- Risk = (Likelihood X Consequences)

METHODOLOGY OF SCORING

- If the chances of risk happening is high the consequence is rated from (1-5) appropriately.
- 1:Wont affect the normal working of the system
- 2:Some functions in the system have error and might not work
- 3:Device will stop working but it can be repaired
- 4:Device stopped working completely/Sensitive data leakage
- 5:System Control Lost,lead to potential property damage

CLASSIFICATION OF RISKS

RISK ID	Risks	Likelihood	Consequences	Risk level
1	Gas Leak not detected	2	5	10 (high)
2	False alarm	3	2	4(moderate)
3	Cyber Security Breach	3	4	12 (high)
4	Hardware Failure	2	5	10(high)
5	Dependence on External Networks	1	3	3(low)
6	SCA	3	5	15(high)
7	MITM	3	5	15(high)

HOW TO MANAGE THE IDENTIFIED RISK??

RISK MANAGEMENT

Mitigation of Risks

- Better algorithm and calibration of sensors and higher quality control to minimize false positives and false negatives,
- To mitigate cyber security, use encryptions to make it harder for third parties to breach
- Hardware Failures can be mitigated by higher quality control
- To mitigate the risk of external network going out, we must find a reliable external network services like amazon AWS
- For Data Sniffing,Encryption will ensure data cannot be read by unauthorized entiti

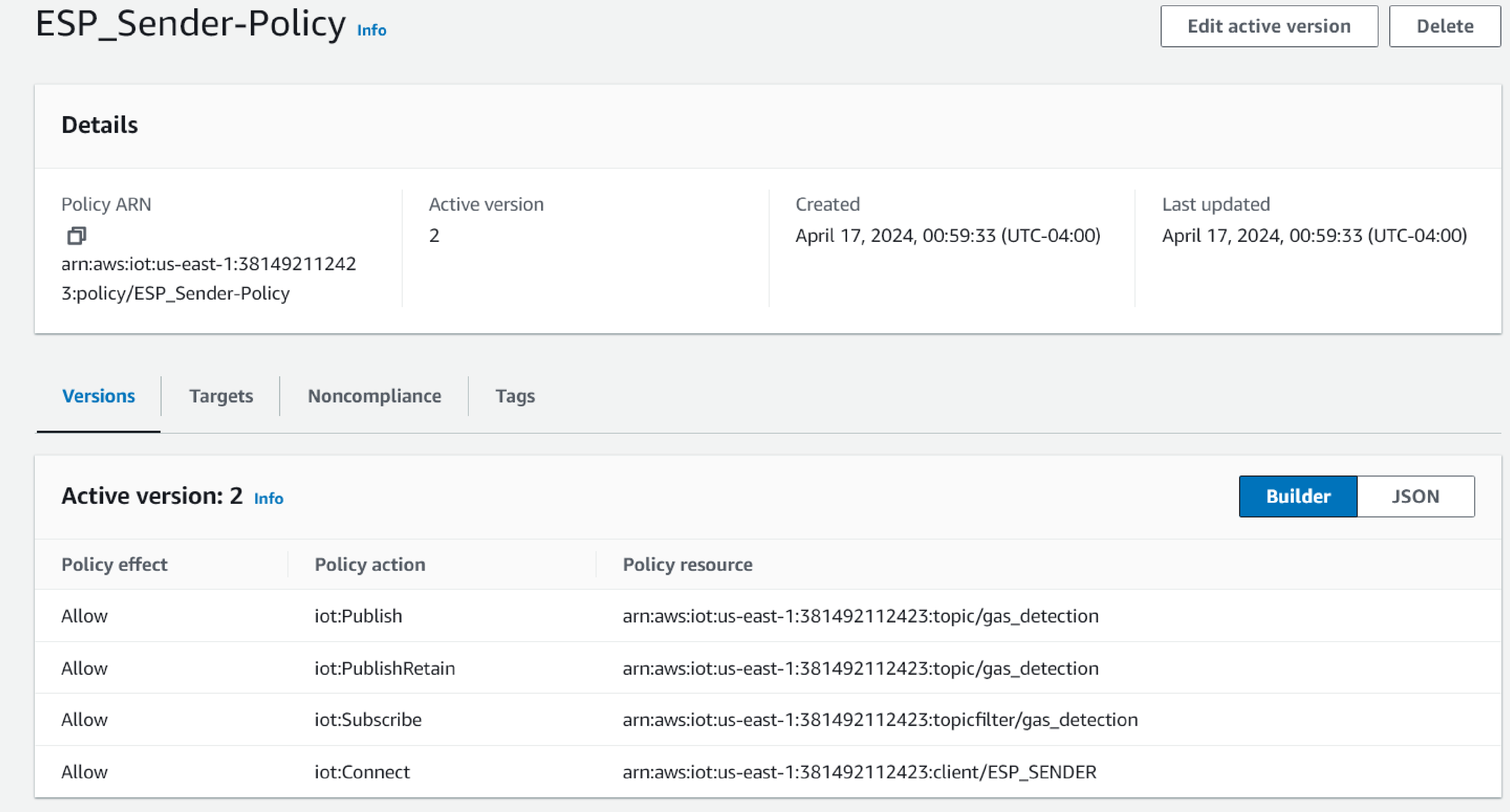
Risk Transfer

- It might be possible to hire a third party to deal with any complex cybersecurity problems and to help prevent any unwanted parties from hacking into your network

RISK MANAGEMENT

- <u>Risk Acceptance</u>
- False Positives and False negatives can't be fully mitigated and there will always be some form of error in the detection.
- If there is a tradeoff between false positives and negatives, then we prioritize mitigating the false negatives even at the expense of higher false positives. This is because a false negative has far higher risks and consequences than that of a false positive.
- Some things like network outages are usually beyond the controls of the user and should be accepted as an occasional occurrence that will happen sometimes even with the best of external services

AWS Policies – Sender



Details

Policy ARN
arn:aws:iot:us-east-1:381492112423:policy/ESP_Sender-Policy

Active version
2

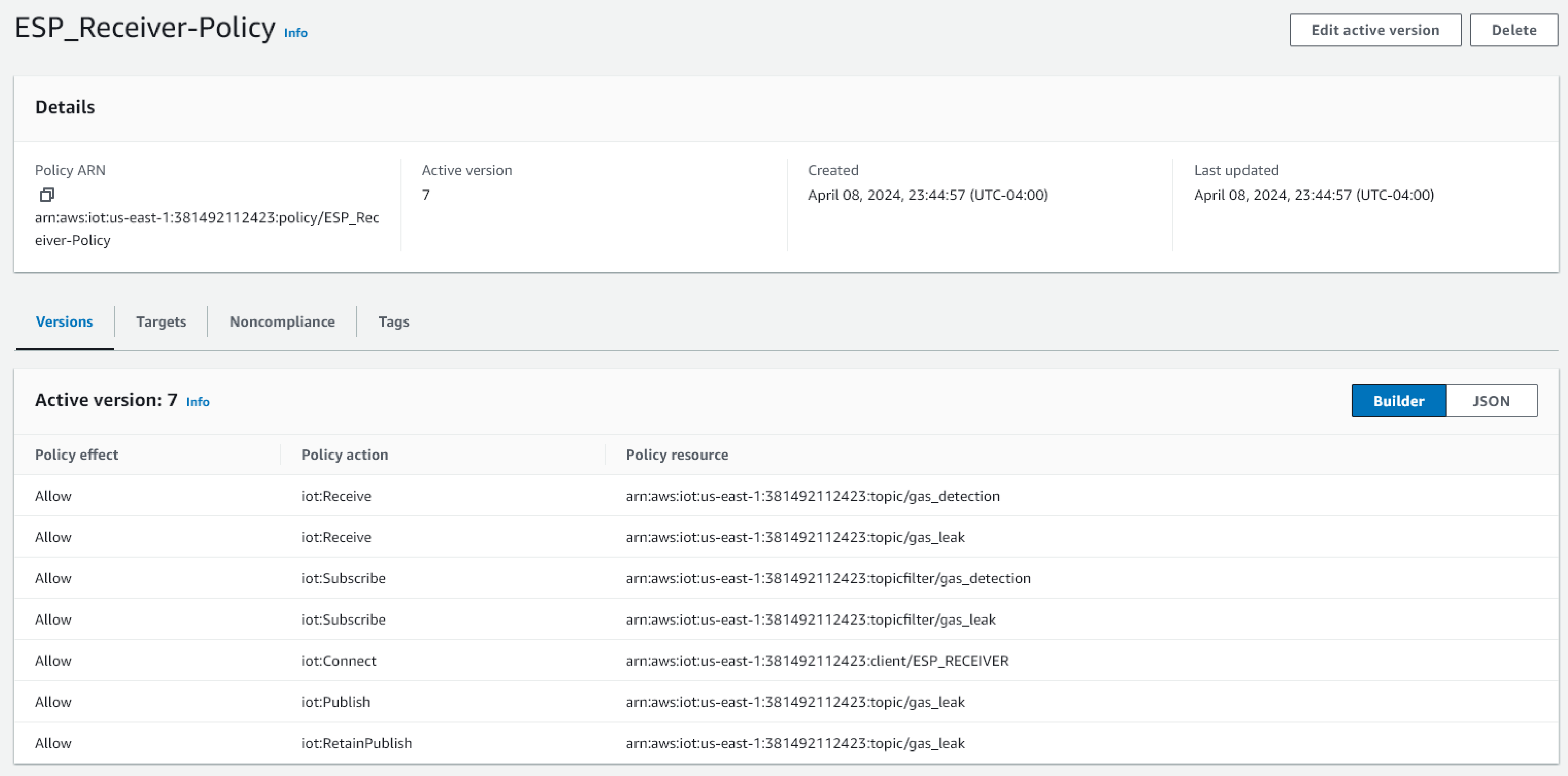
Created
April 17, 2024, 00:59:33 (UTC-04:00)

Last updated
April 17, 2024, 00:59:33 (UTC-04:00)

Active version: 2

Policy effect	Policy action	Policy resource
Allow	iot:Publish	arn:aws:iot:us-east-1:381492112423:topic/gas_detection
Allow	iot:PublishRetain	arn:aws:iot:us-east-1:381492112423:topic/gas_detection
Allow	iot:Subscribe	arn:aws:iot:us-east-1:381492112423:topicfilter/gas_detection
Allow	iot:Connect	arn:aws:iot:us-east-1:381492112423:client/ESP_SENDER

AWS Policies – Receiver



ESP_Receiver-Policy Info

Details

Policy ARN
arn:aws:iot:us-east-1:381492112423:policy/ESP_Receiver-Policy

Active version
7

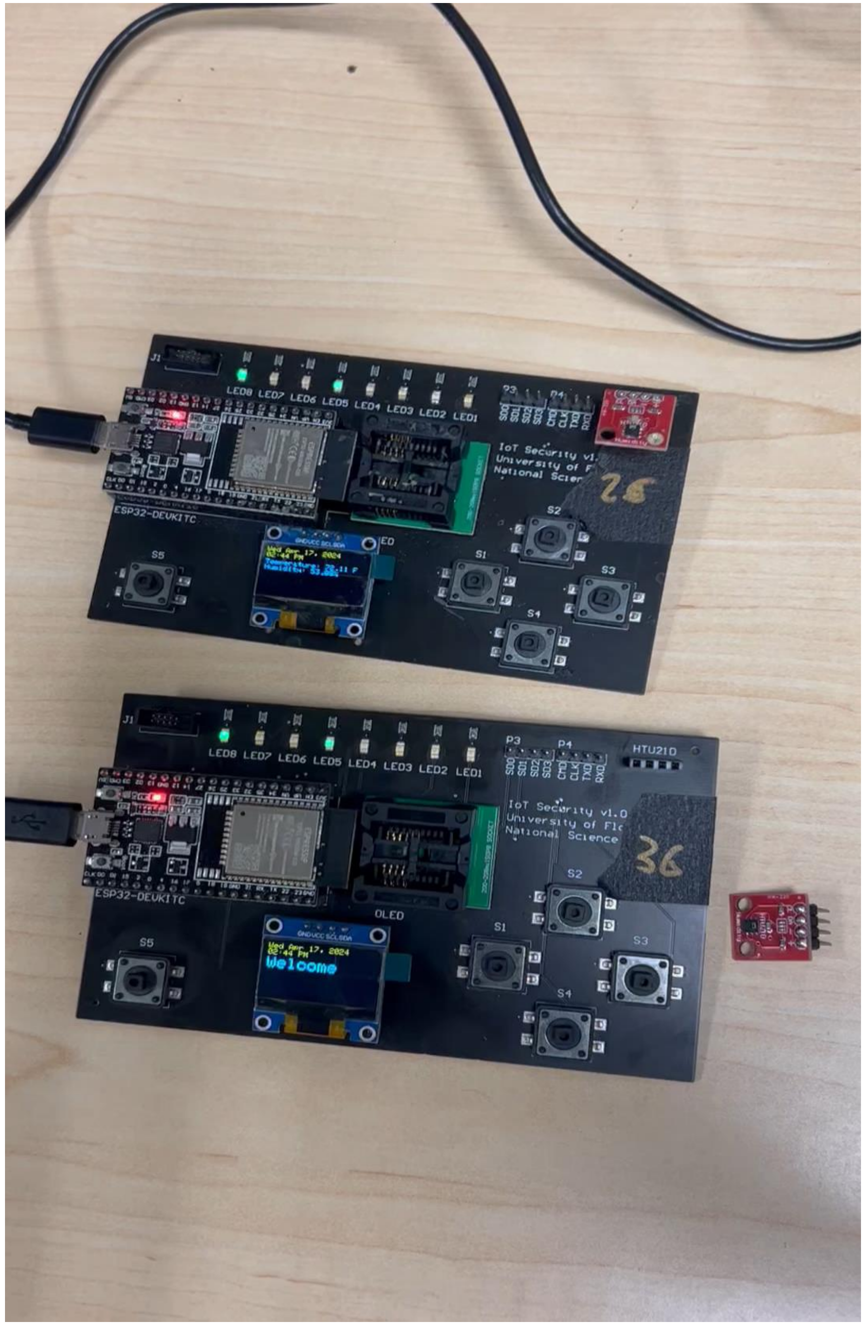
Created
April 08, 2024, 23:44:57 (UTC-04:00)

Last updated
April 08, 2024, 23:44:57 (UTC-04:00)

Active version: 7 Info

Policy effect	Policy action	Policy resource
Allow	iot:Receive	arn:aws:iot:us-east-1:381492112423:topic/gas_detection
Allow	iot:Receive	arn:aws:iot:us-east-1:381492112423:topic/gas_leak
Allow	iot:Subscribe	arn:aws:iot:us-east-1:381492112423:topicfilter/gas_detection
Allow	iot:Subscribe	arn:aws:iot:us-east-1:381492112423:topicfilter/gas_leak
Allow	iot:Connect	arn:aws:iot:us-east-1:381492112423:client/ESP_RECEIVER
Allow	iot:Publish	arn:aws:iot:us-east-1:381492112423:topic/gas_leak
Allow	iot:RetainPublish	arn:aws:iot:us-east-1:381492112423:topic/gas_leak

DEMONSTRATION OF PROJECT



Thank You!