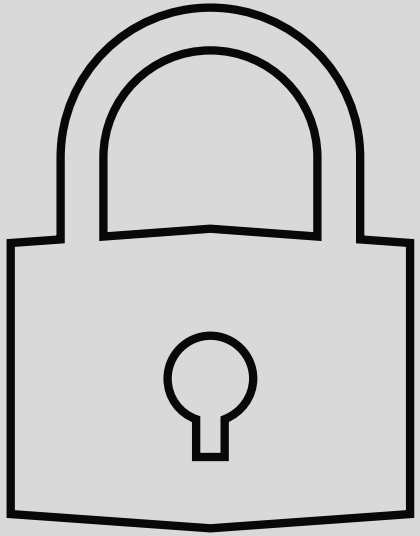
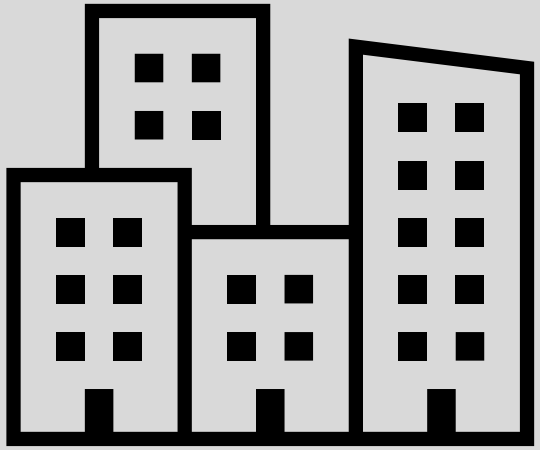




SECURE IOT SOLUTION FOR OFFICE BUILDING MONITORING

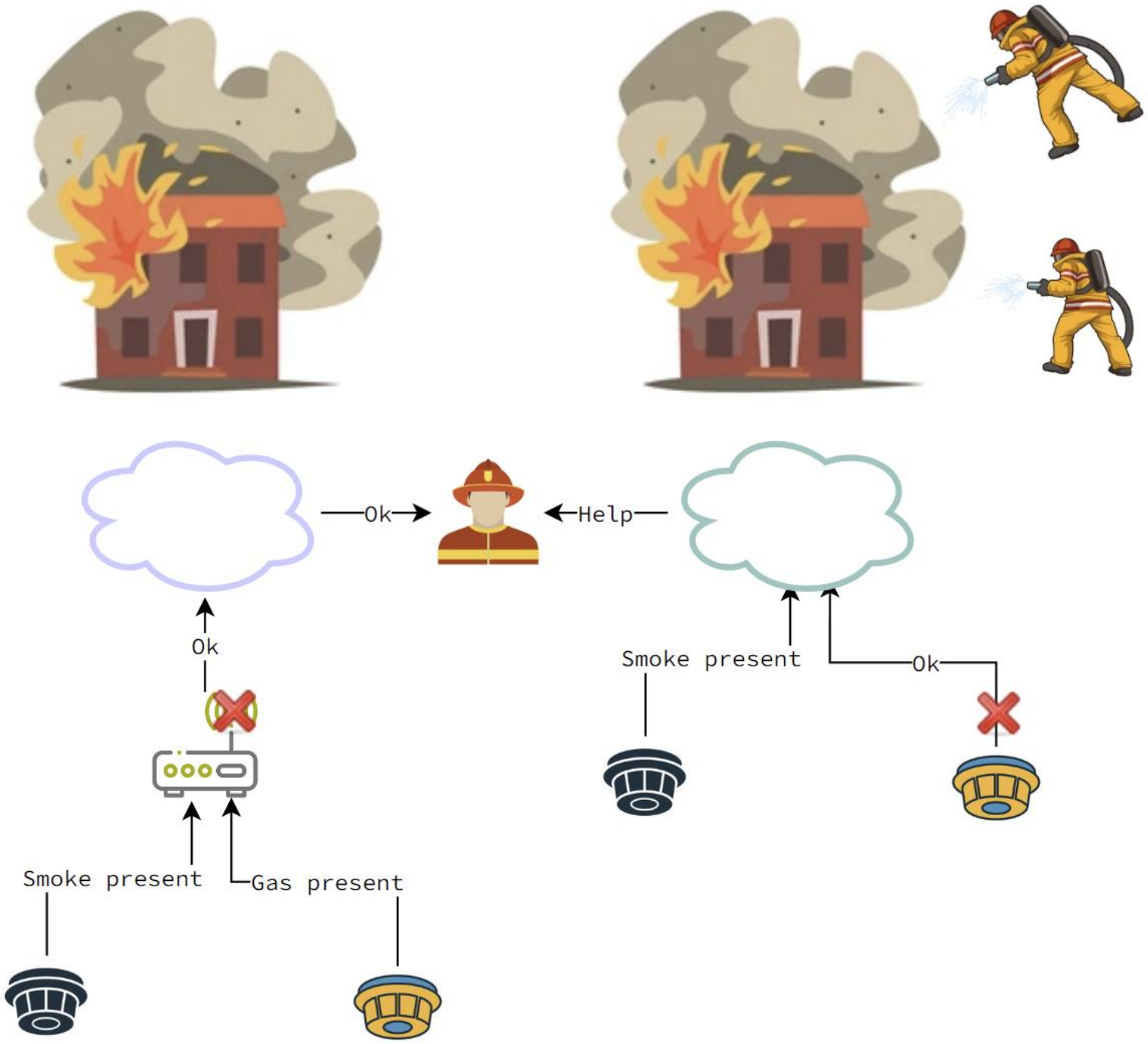
PURPOSE OF THE THESIS

Designing a low-powered IoT solution which enforces entity attestation and securely transmits data into the cloud, performing edge Machine Learning and issuing blockchain transactions.

CONTENTS

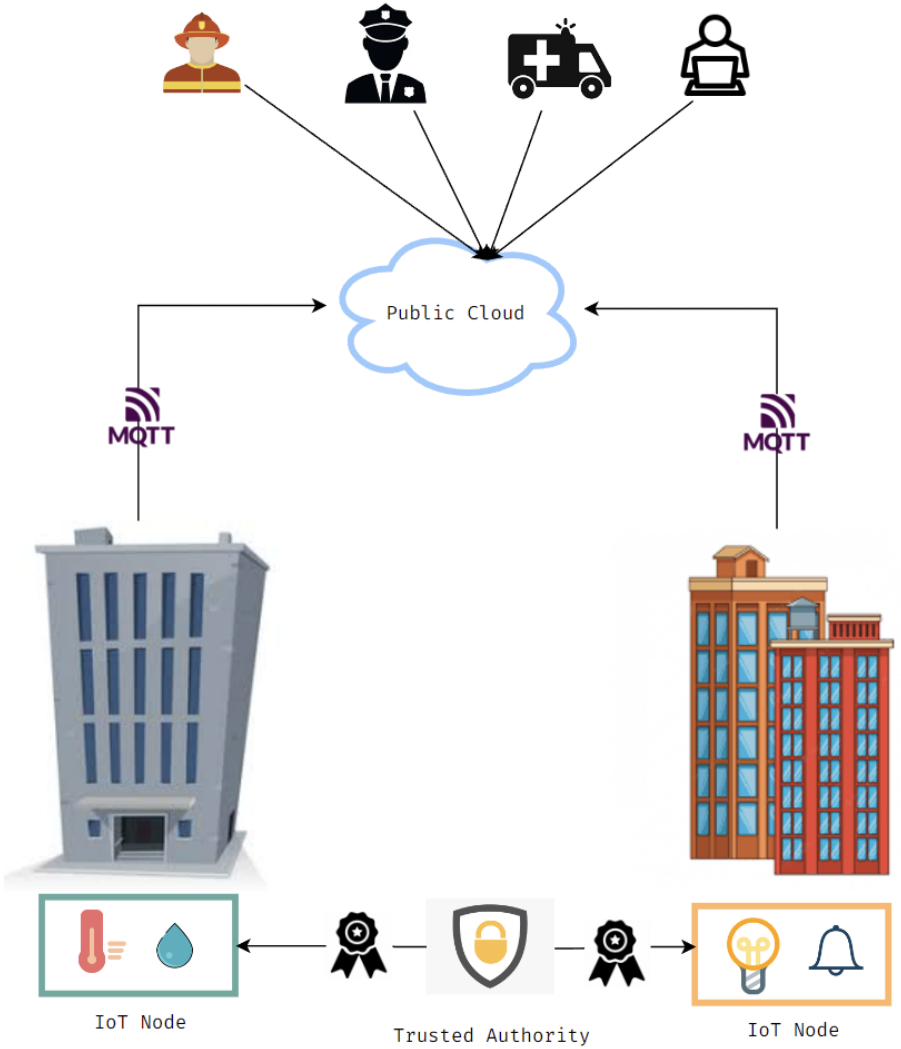
INTRODUCTION

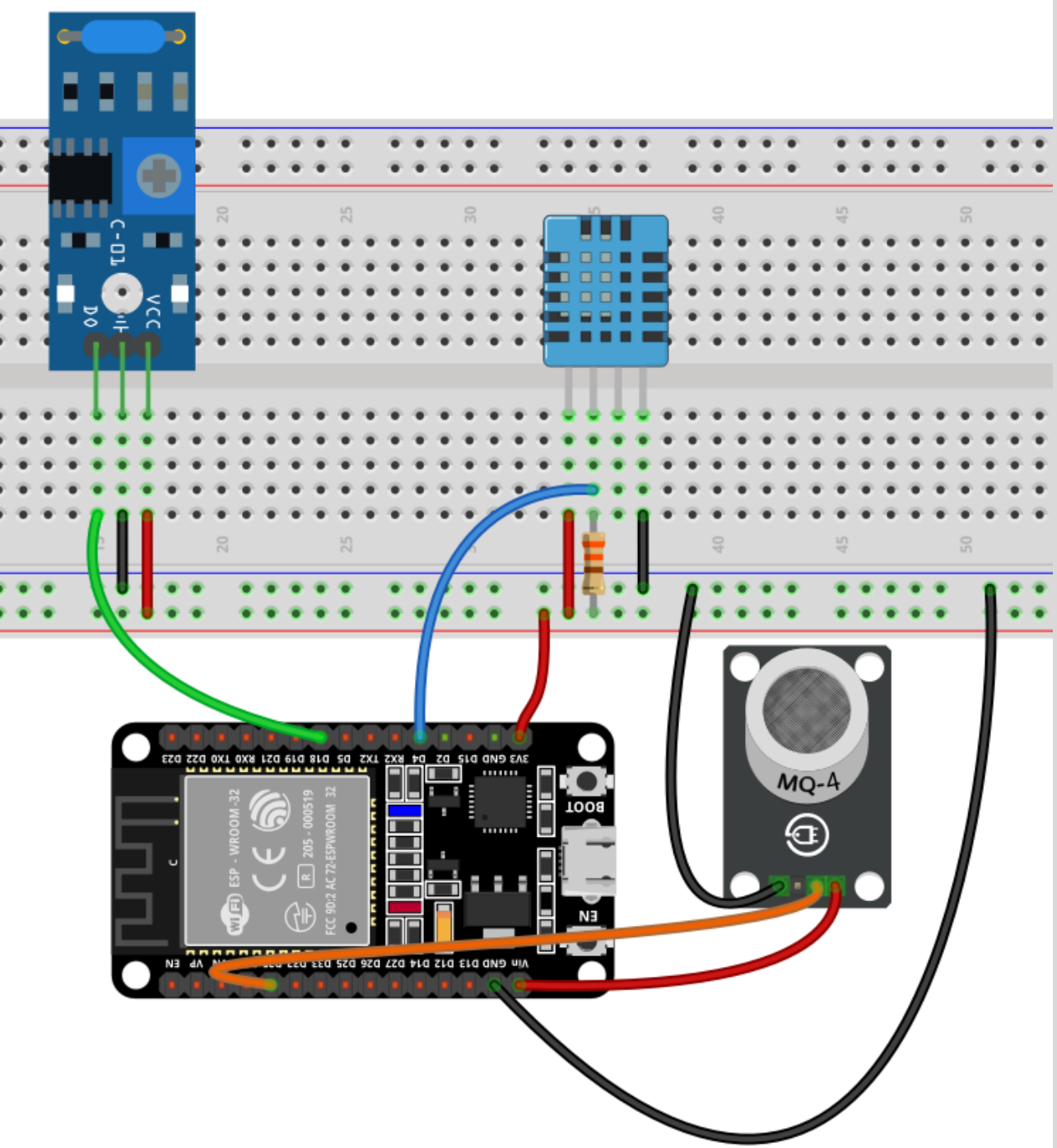
- Current IoT fog computing solutions pose a severe security risk by introducing single points of failure
- Creating an architecture that is more resilient is imperative in mission-critical applications



ARCHITECTURE OVERVIEW

- Wi-Fi enabled IoT nodes are pushing sensitive data into the cloud
- Fast dispatch and reaction is achieved through encoding of the payload to reduce size
- Complete confidentiality is achieved through End-to-End encryption
- Each entity is attested



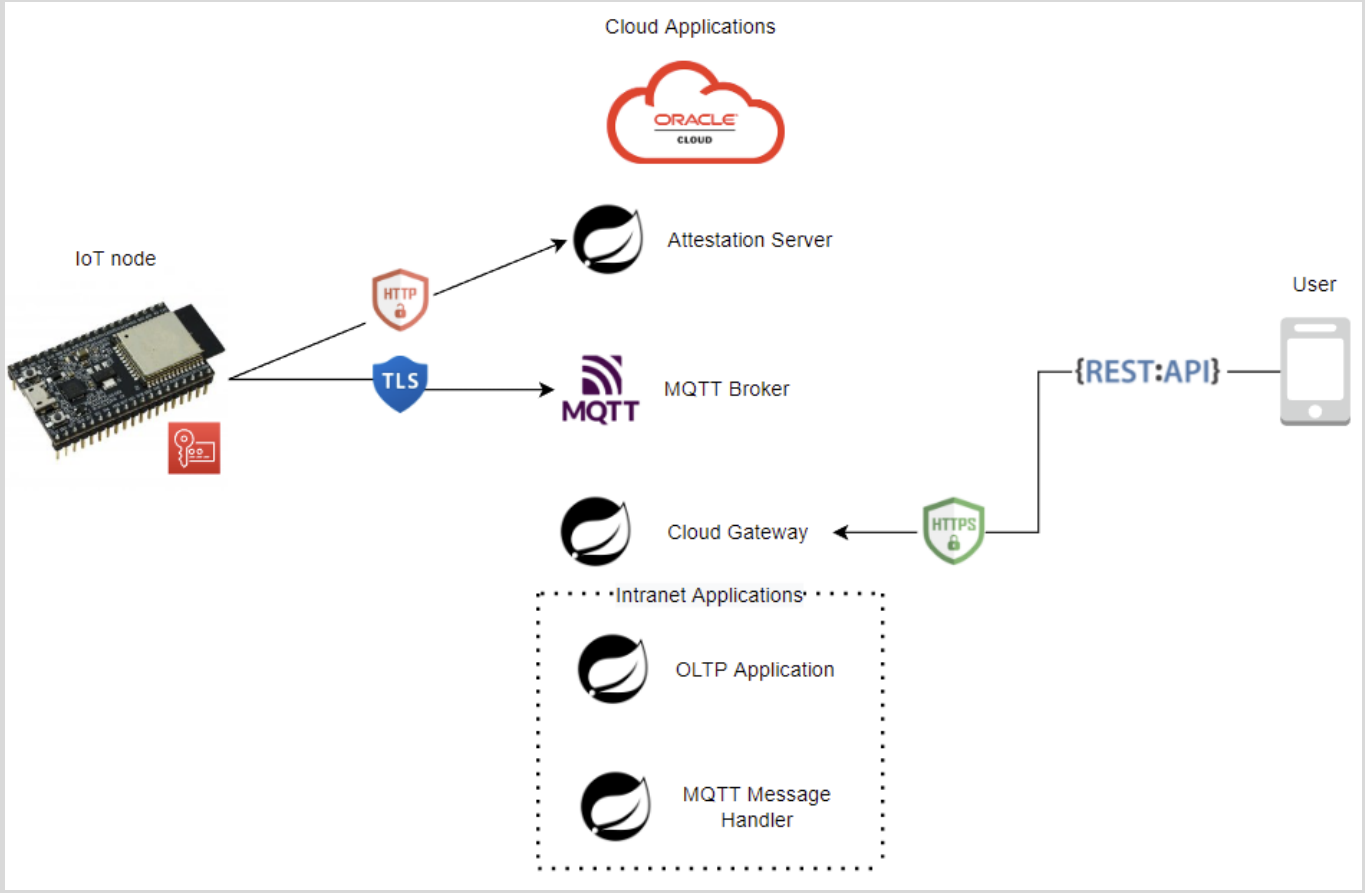


DESIGN OF THE IOT NODE

- Built using off the shelf components:
  - Espressif ESP32
  - DHT11 Temperature and Humidity Sensor
  - SW-420 Vibration Sensor
  - MQ-2 Gas Sensor
- Performs Edge Machine Learning
- Issues blockchain transactions
- Runs ESP-IDF and uses a CMake derived build system
- Has two Xtensa LX6 CPU cores and supports FreeRTOS
- Baked-in support for mbedTLS, which offers a plethora of cryptographic operations
- Sensor data is sent CBOR encoded and formatted according to the IPSO guidelines

CLOUD-HOSTED MICROSERVICES

- Hosted on an Oracle Cloud Instance with 4 ARM cores and 24 GB of RAM
- Developed in Spring Boot
- Conforms to the microservice architecture: exposes all available endpoints through a web-facing gateway
- Runtime serving of configuration files using Spring Cloud Configuration Server
- Service Discovery through Netflix Eureka Server
- Transport layer security through HTTPS
- All requests are authenticated using JWT
- Deployed using Docker Compose



SECURING THE SOLUTION ATTESTATION SERVICE

01 Mutual Authentication

Through signed X.509 certificates

02 Session Key Establishment

Through EC Ephemeral Diffie-Hellman

03 Instance ID allocation

By calling the DB microservice

04 MQTT Connection

Using the established key for TLS-PSK

SECURING THE SOLUTION PROTECTING SECRETS

Credentials and other sensitive information are served to the microservices using HashiCorp Vault over HTTPS

The chosen strategy to prevent the secret zero problem is cubbyhole response wrapping

The flash storage of the IoT node is encrypted, saving the key in eFUSE

CONCLUSION

Resilient and secure solution

- End-to-End encryption
- Resiliency is improved by removing gateways
- Entity attestation is enforced

CONCLUSION

Feature rich and easily expandable

- Handles sensor data transparently which allows facile extensions
- Performs edge Machine Learning supporting a large number of models
- Able to issue blockchain transaction
    - Persisting records into Ethereum Smart Contracts

CONCLUSION

Interoperable

- Industry standards such as IPSO formatting guide and CBOR have been used
- Transport over IP

THANK YOU!