IOTS

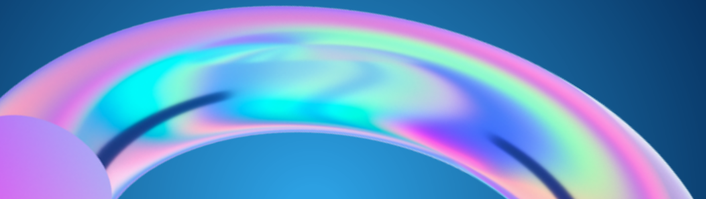
Secured Doorly

The Presentation

By: Soh Tai Rong (2032766) | Brian Lim Beng Xian (1908873) | Keegan Lim Beng Yang (1908857)

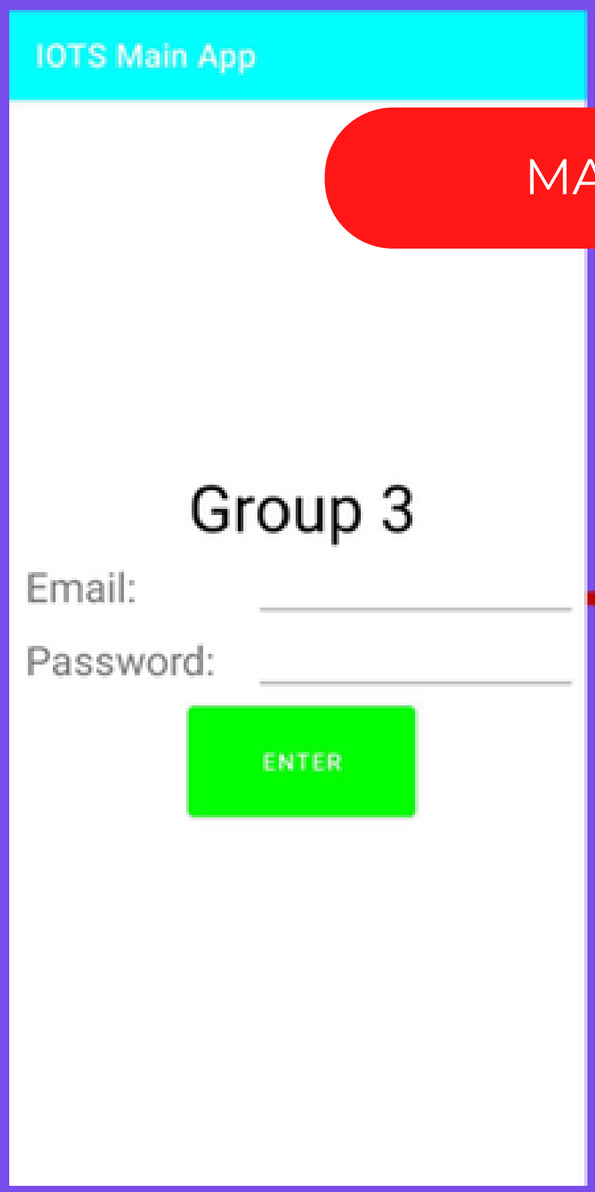
Mobile App

Used for unlocking of the door.



Mobile App: Front End

MAX 4 ATTEMPTS BEFORE 2 MINS LOCKOUT



- Button pressed.

- App hashes user input
- Hashed input compared with hashed credentials in DB

Mobile App: Back End

1. TLS/SSL using Server connection string
2. White-listed IP only
3. Authenticate with AWS credentials

Azure SQL

Azure SQL Database

1. Credentials at rest are hashed
2. Database auto-encrypted by Azure

aws

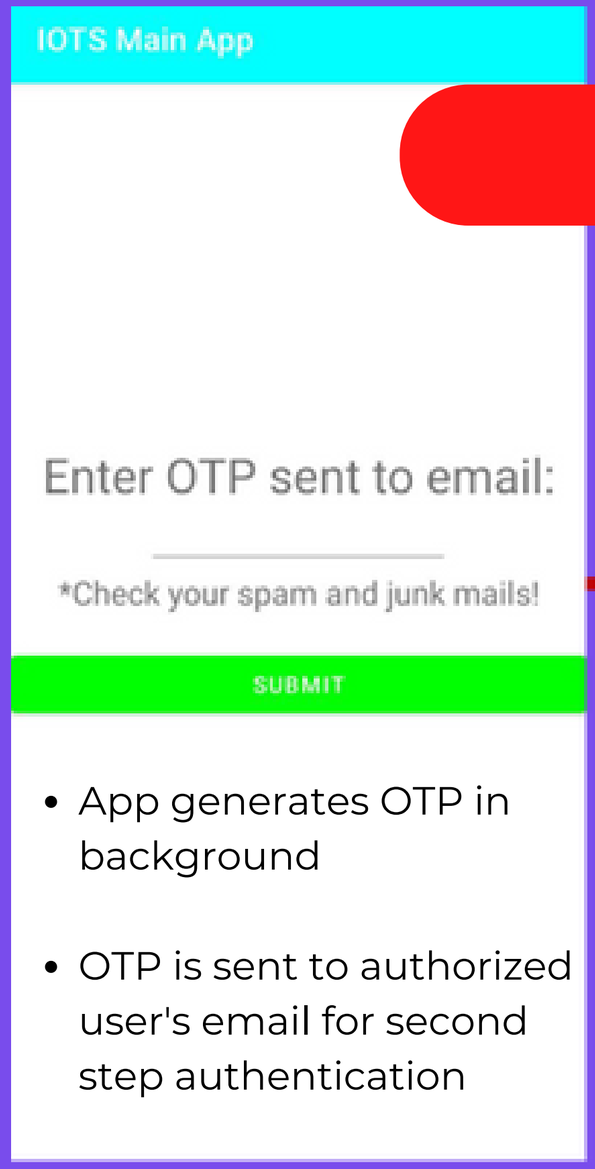
AWS SES Cloud

ThingSpeak

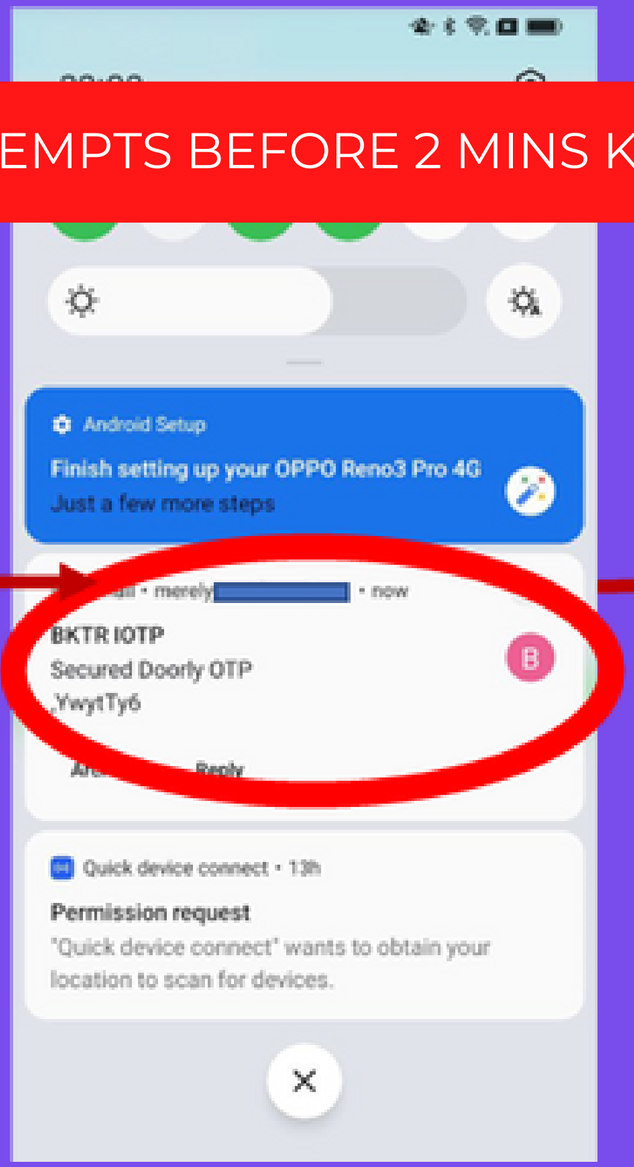
ThingSpeak MQTT Broker

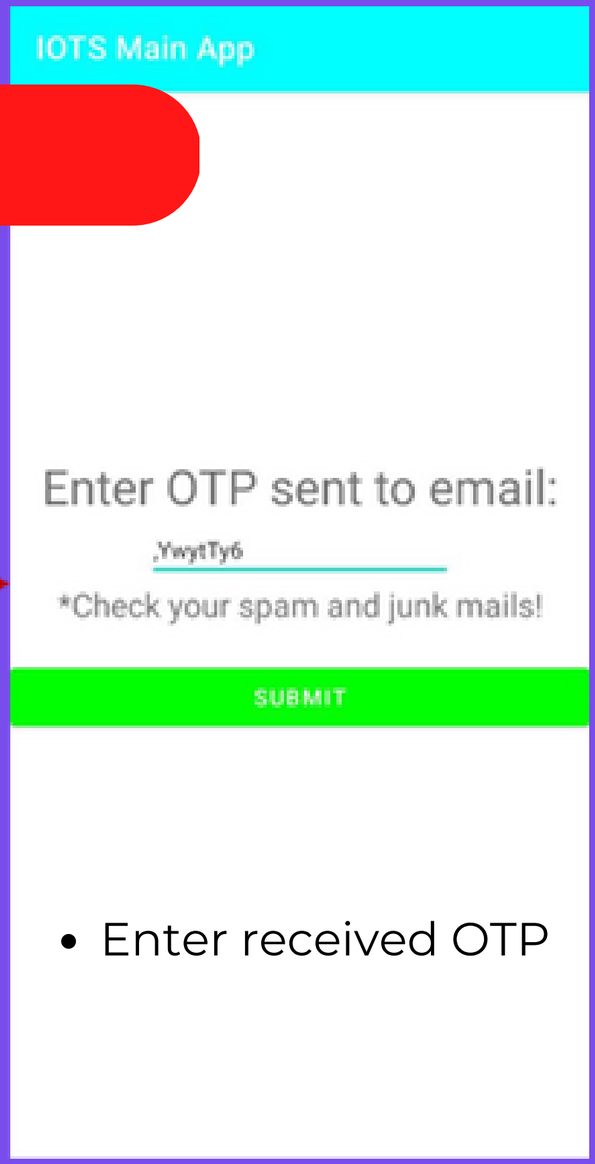
Mobile App: Front End

MAX 3 ATTEMPTS BEFORE 2 MINS KICK OUT



- App generates OTP in background
- OTP is sent to authorized user's email for second step authentication





- Enter received OTP

Mobile App: Back End

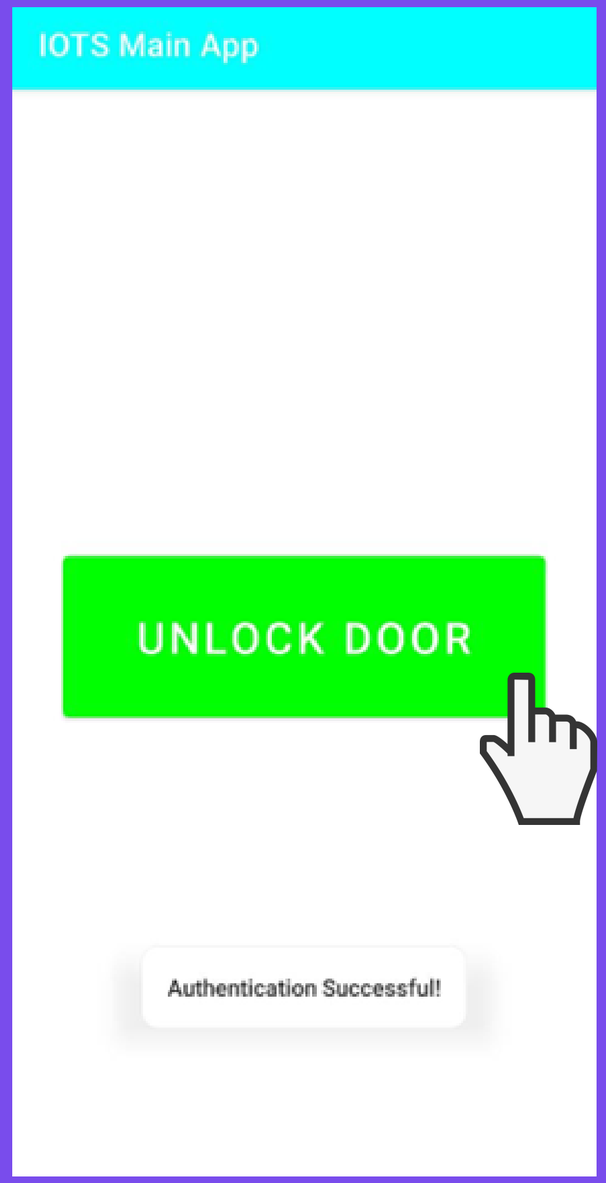
1. AWS SES SMTP protocol
2. Client authentication with SMTP credentials

Azure SQL Database

AWS SES Cloud

ThingSpeak MQTT Broker

Mobile App: Front End



UNLOCK PRESSED:

- Sends MQTT message to ThingSpeak

Mobile App: Back End

1. TLS/SSL using Server Certificate
2. Client authenticate with ThingSpeak credentials

Azure SQL Database

AWS SES Cloud

ThingSpeak MQTT Broker

Smart Lock

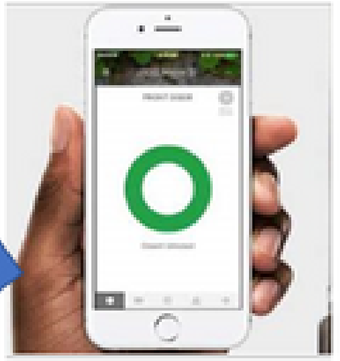
Our Smart Door System.

Smart Door Functionality

Home Doorway

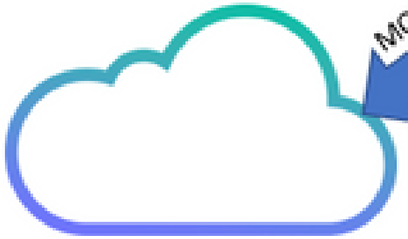
ESP8266

MQTT **Subscribe** to Unlock Door



Mobile App for Smart Door

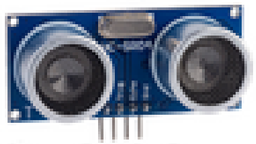
MQTT **Publish** to Unlock Door



ThingSpeak MQTT Broker

App Unlock Triggers:

6. Servo Motor to Unlock Door
7. Snap Picture of Person who Entered
8. Automatically Lock Door When Closed using Ultra-Sonic Sensor

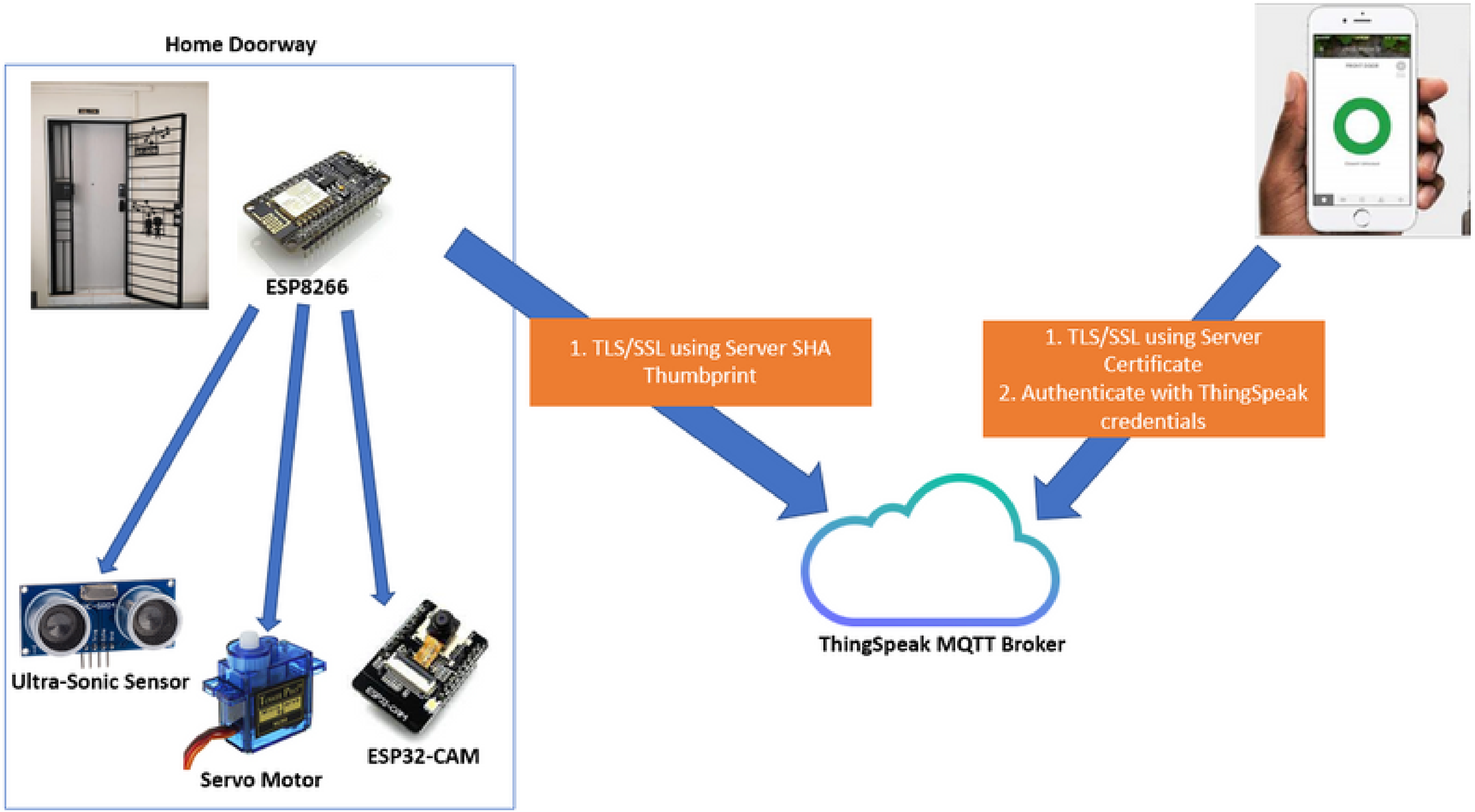


Ultra-Sonic Sensor

Servo Motor

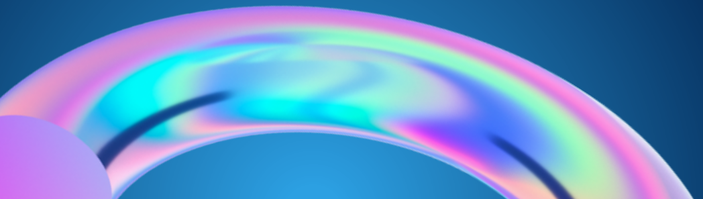
ESP32-CAM

Security Feature (Transit)



TR64

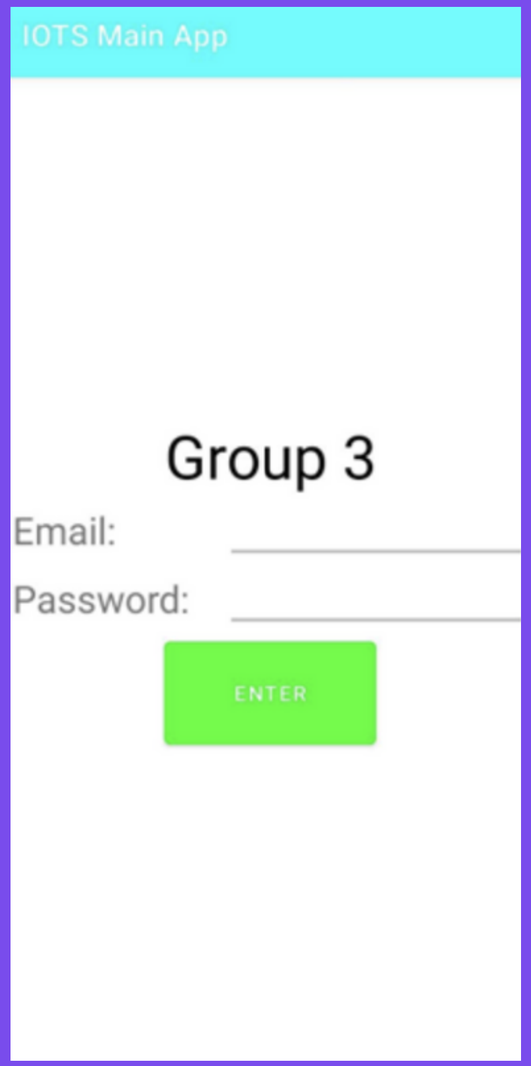
TR64 Comliance Checklist



TR64 Assessment

Attack Surface	TR64 Reference
Phone app	MT-01, CS-01, IA-01, AP-01, AP-02
Amazon Web Service	NP-03, DP-04, AP-02, MT-01, RS-03, UA-01
Azure SQL Database	MT-01, CS-03, IA-01, NP-03, NP-04, RS-04, AU-01
Thingspeak MQTT	MT-01, NP-04
Hardware	AP-04
Entire system	LP-01, LP-02, LP-07

TR64 Assessment(App)



MT-01
Strong Password enforced

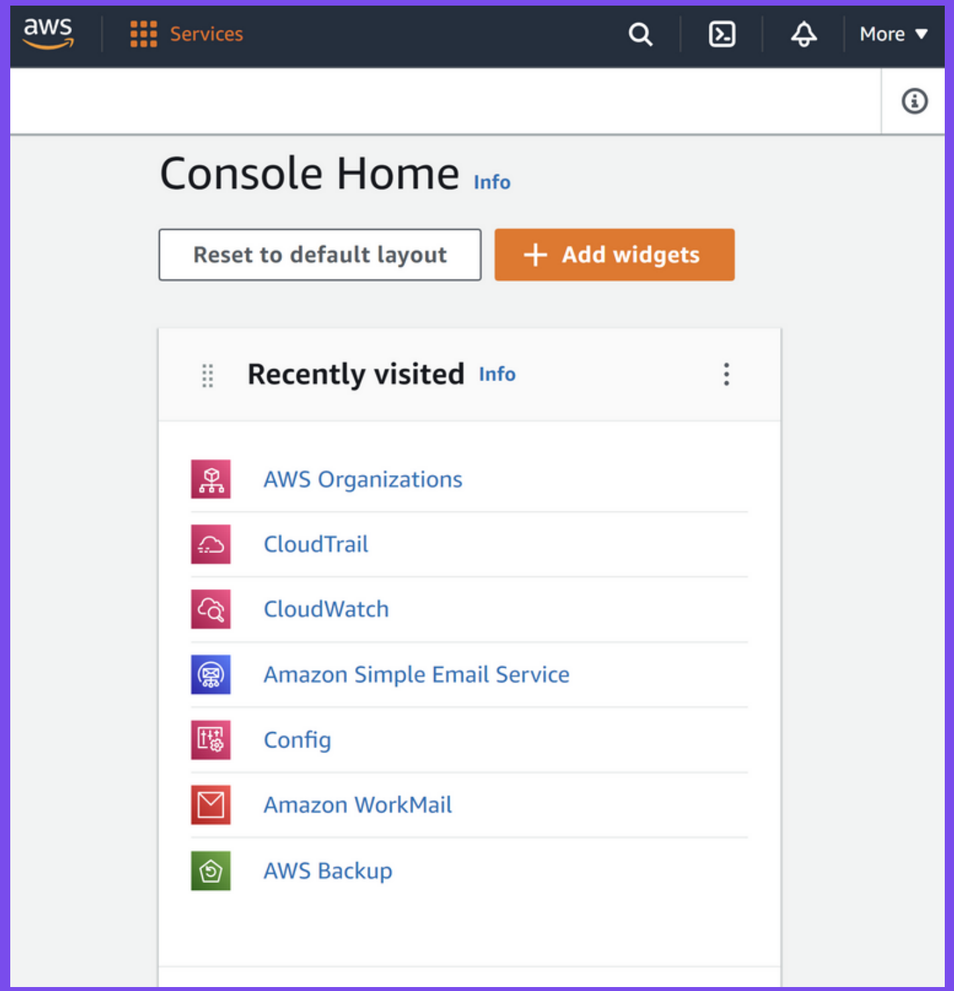
CS-01
Employment of random number generator

IA-01
Secure storage of user credentials, Input validation to guard against vulnerabilities

AP-01
Protection against repeated attempts

AP-02
Multi factor Authentication

TR64 Assessment(AWS)



NP-03
Secured connectivity is enforced

DP-04
Access control mechanism

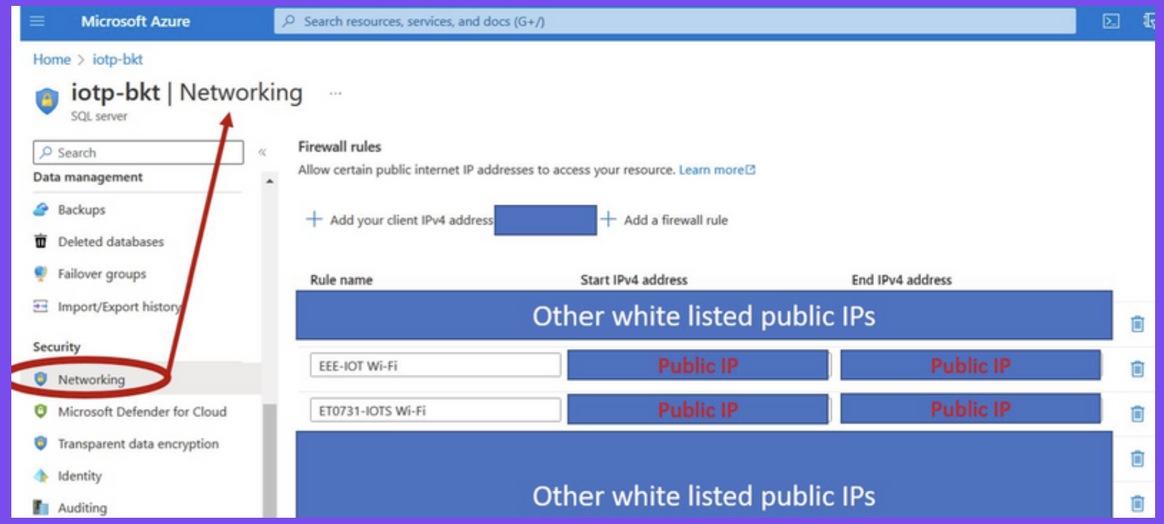
AP-02
Multi-Factor Authentication

MT-01
Strong password policies

RS-03
able to withstand malicious attacks

UA-01
significant events recorded

TR64 Assessment(Azure)



MT-01
Strong Password enforced

CS-03
AES encryption

IA-01
Client credential's stored securely

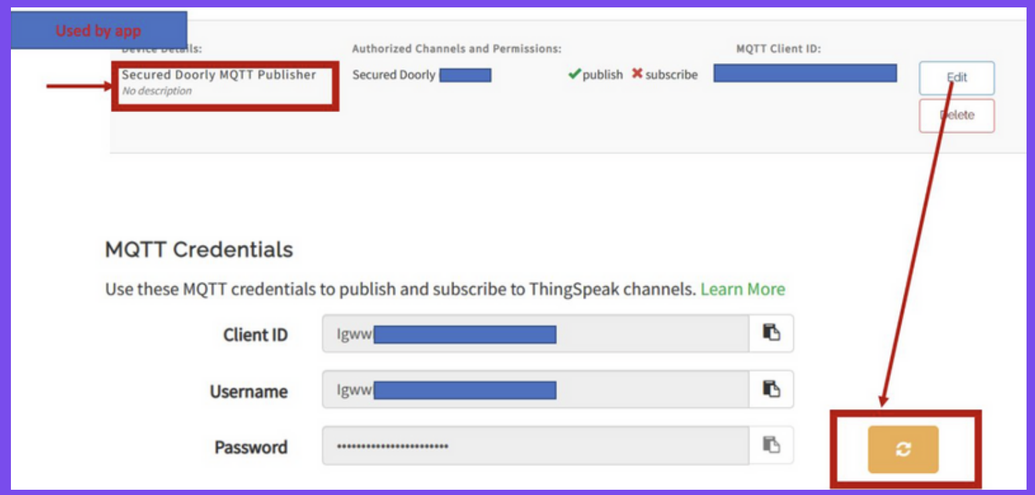
NP-03
Transport layer security employed

NP-04
Secured connectivity is enforced

RS-04
Regular backup of system data

AU-01
Significant events recorded

TR64 Assessment(MQTT)



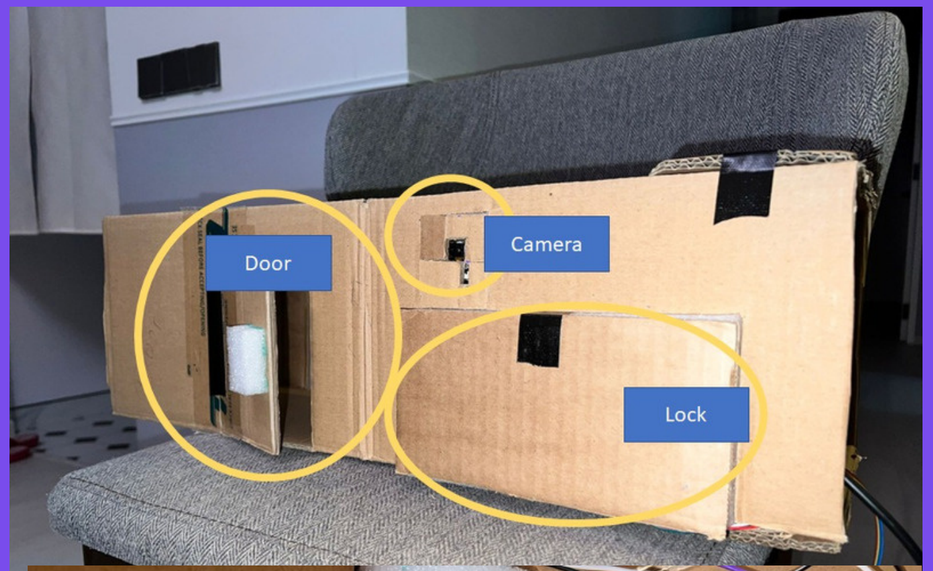
MT-01

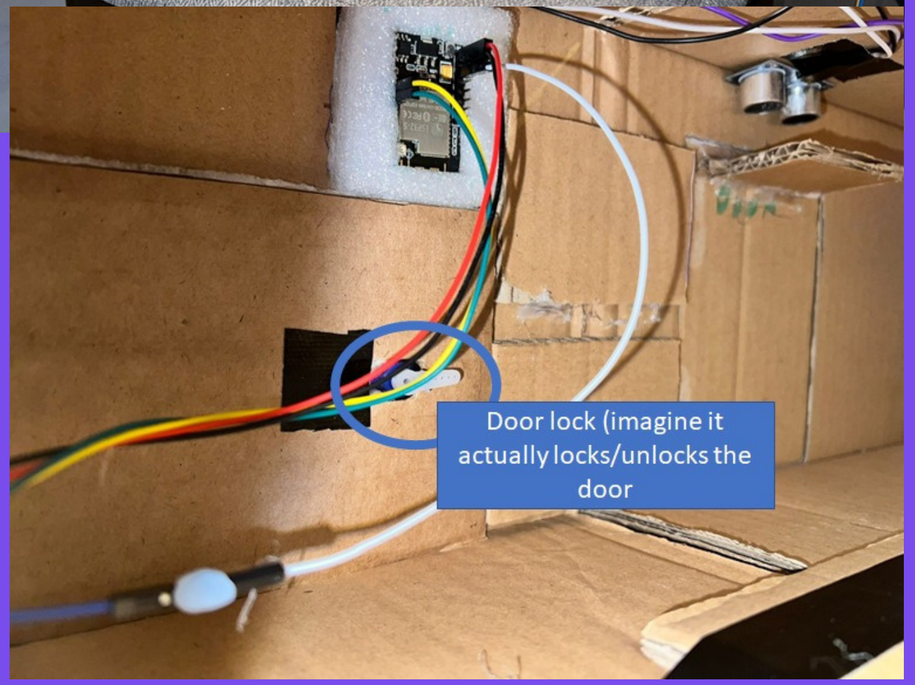
Strong password policies

NP-04

Secure connectivity based on industry best practices

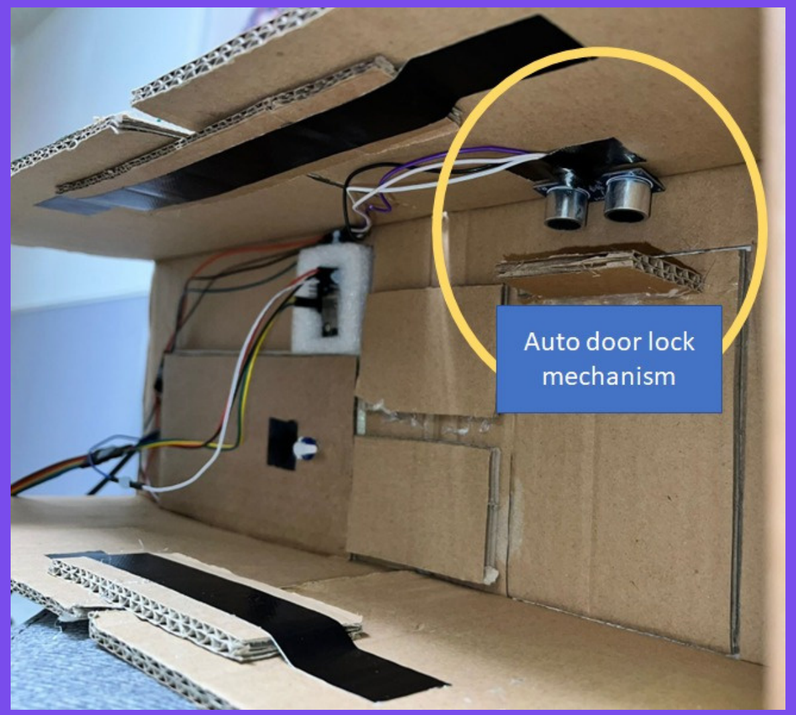
TR64 Assessment(Hardware)



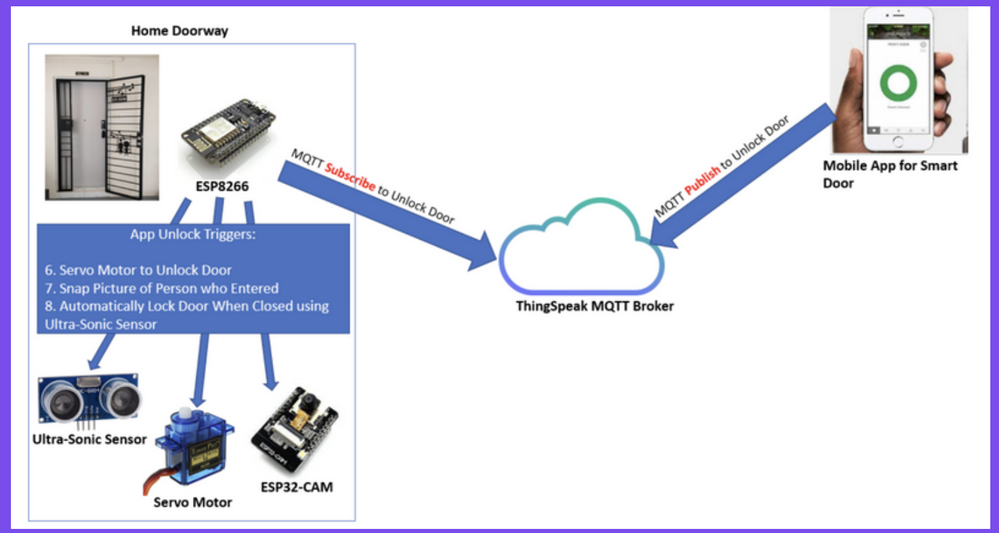


AP-04

Tamper resistant hardware



TR64 Assessment(System)



LP-01

Conducted threat modeling to identify threats

LP-02

System is designed and developed using secure systems engineering approach and best practices

LP-07

Penetration-testing and vulnerability assessment

Vulnerability Assessment

1. Identifying of security Objectives
2. Documentation of IoT System Architecture
3. Decomposing of IoT System
4. Identifying and Rating Threats
5. Recommending Mitigations

Found in Report