

# IOTS Secured Doorly

The Presentation





# Mobile App



Used for unlocking of the door.



# Mobile App: Front End

IOTS Main App

IOTS Main App

IOTS Main App

MAX 4 ATTEMPTS BEFORE 2 MINS LOCKOUT

Group 3

Email:

Password:

ENTER

Group 3

Email:

merely[REDACTED]@gmai[REDACTED]

Password:

[REDACTED]

ENTER

- Button pressed.

Group 3

Email:

merely[REDACTED]@gmai[REDACTED]

Password:

[REDACTED]

ENTER

C

- 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 Database

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



AWS SES Cloud



ThingSpeak MQTT Broker

# Mobile App: Front End

The diagram illustrates the mobile application's front-end flow for two-step authentication. It consists of three main sections: a left panel for generating the OTP, a central panel showing the OTP in an email inbox, and a right panel for entering the OTP.

**Left Panel:** Shows the interface for generating the OTP. It includes a text input field labeled "Enter OTP sent to email:" containing the placeholder ".YwytTy6", a note to check spam/junk mail, and a green "SUBMIT" button.

**Central Panel:** Shows a screenshot of a smartphone displaying the home screen with a notification bar at the top. Below the bar is a red rounded rectangle containing the text "MAX 3 ATTEMPTS BEFORE 2 MINS KICK OUT". The main screen shows an email inbox with one message highlighted. The message is from "BKTR IOTP" with the subject "Secured Doorly OTP" and the body ".YwytTy6". A red circle and arrow point to this message, indicating it is the OTP to be entered. The message has a pink circular badge with the letter "B" on it. Other messages in the inbox include "Android Setup" and "Quick device connect".

**Right Panel:** Shows the interface for entering the received OTP. It has a text input field with ".YwytTy6" entered, a note to check spam/junk mail, and a green "SUBMIT" button.

**Bottom Summary:** A bulleted list summarizes the process:

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

# Mobile App: Back End



# Mobile App: Front End



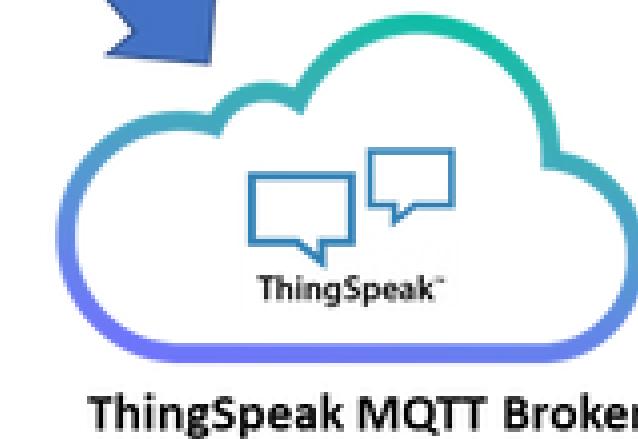
## UNLOCK PRESSED:

- Sends MQTT message to ThingSpeak

# Mobile App: Back End



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



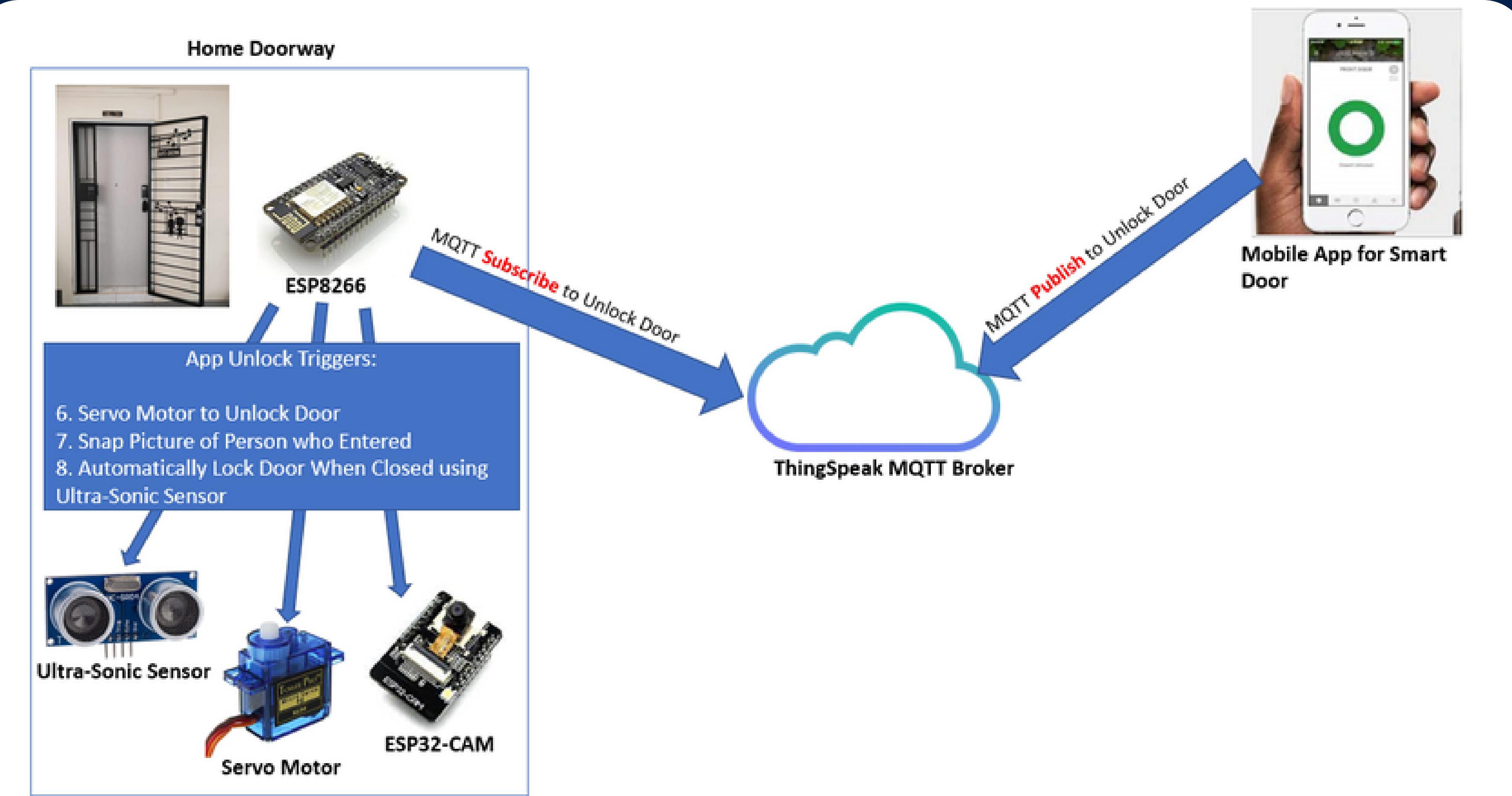


# Smart Lock

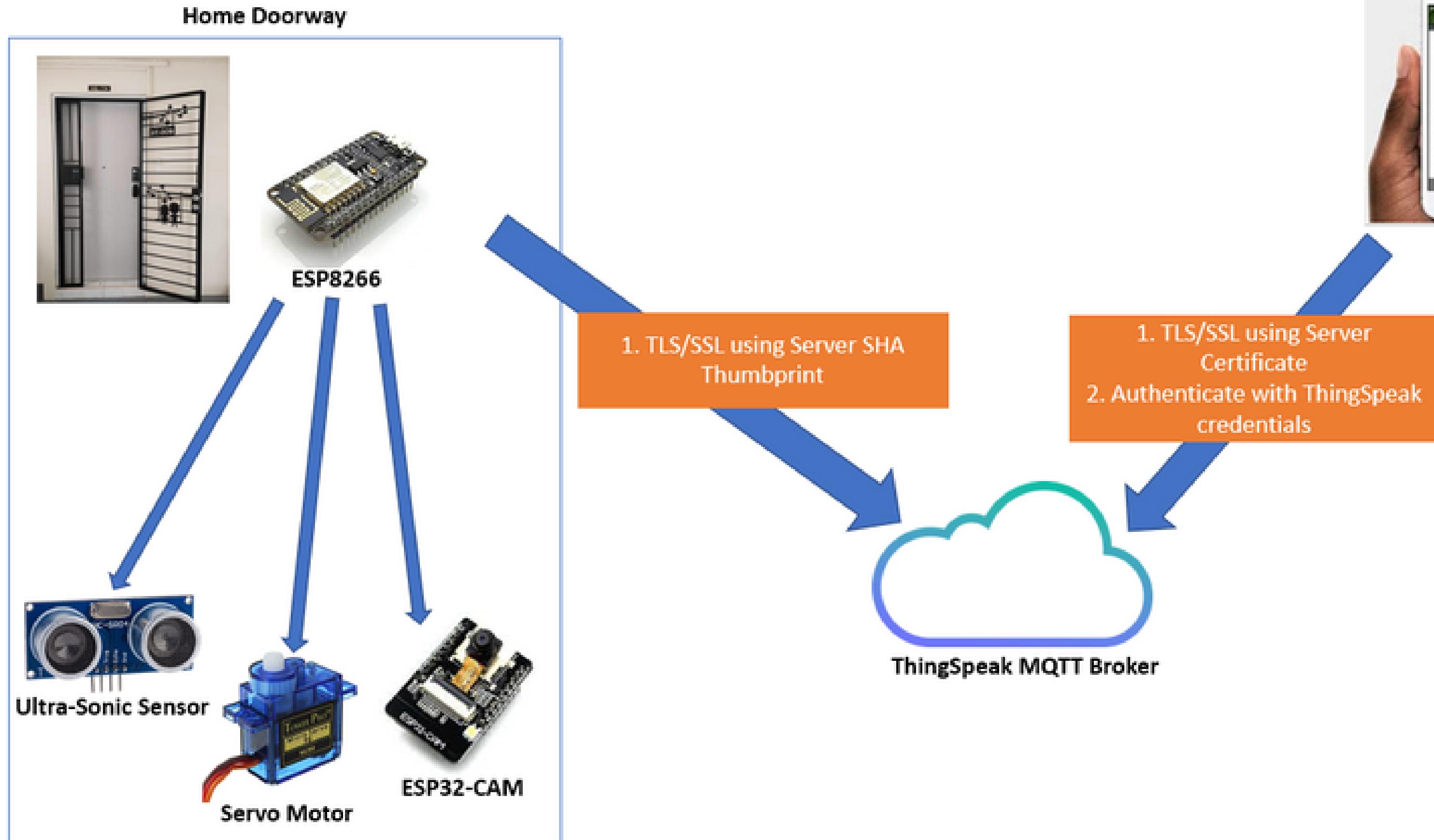
Our Smart Door System.



# Smart Door Functionality



# Security Feature (Transit)





# TR64

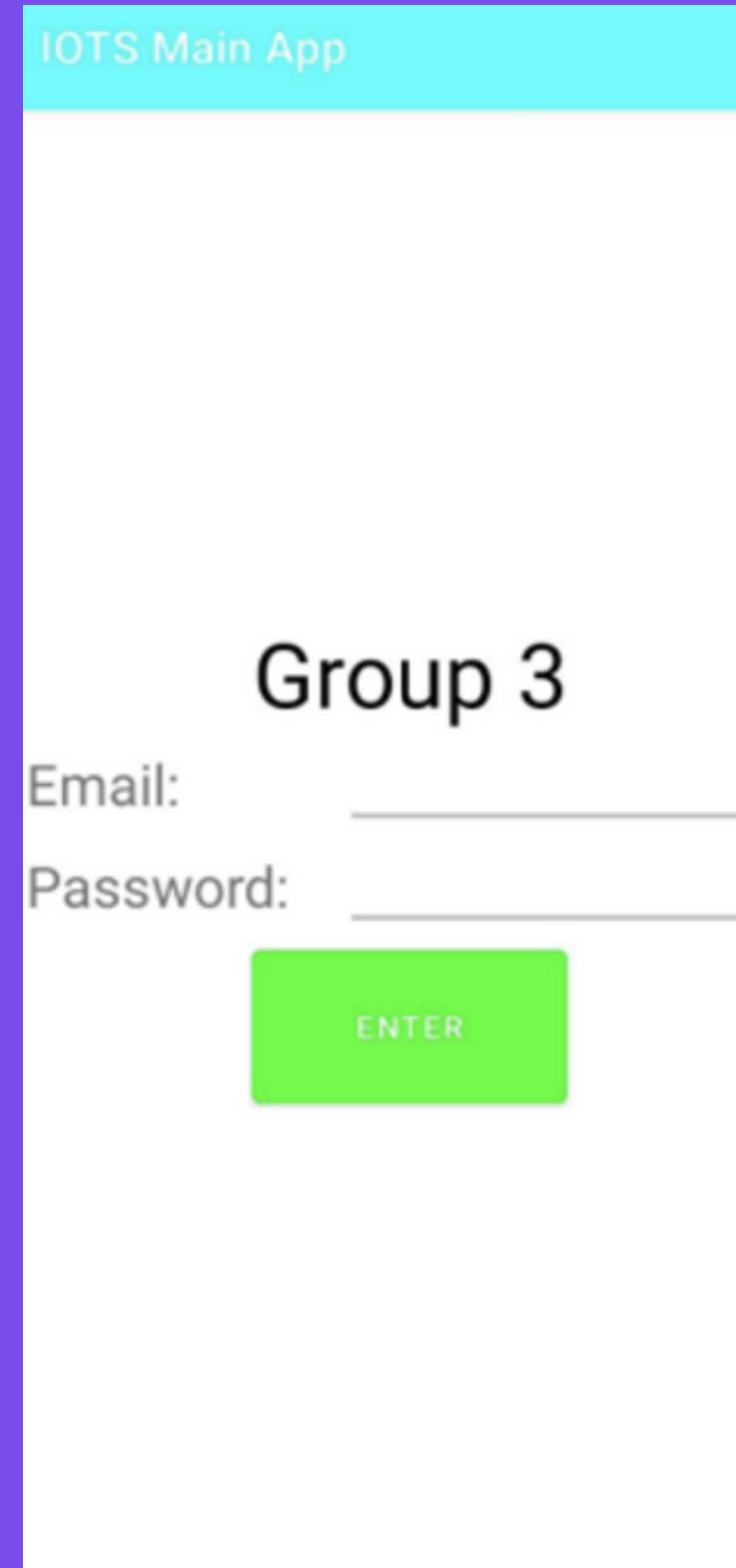
TR64 Compliance Checklist



# 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

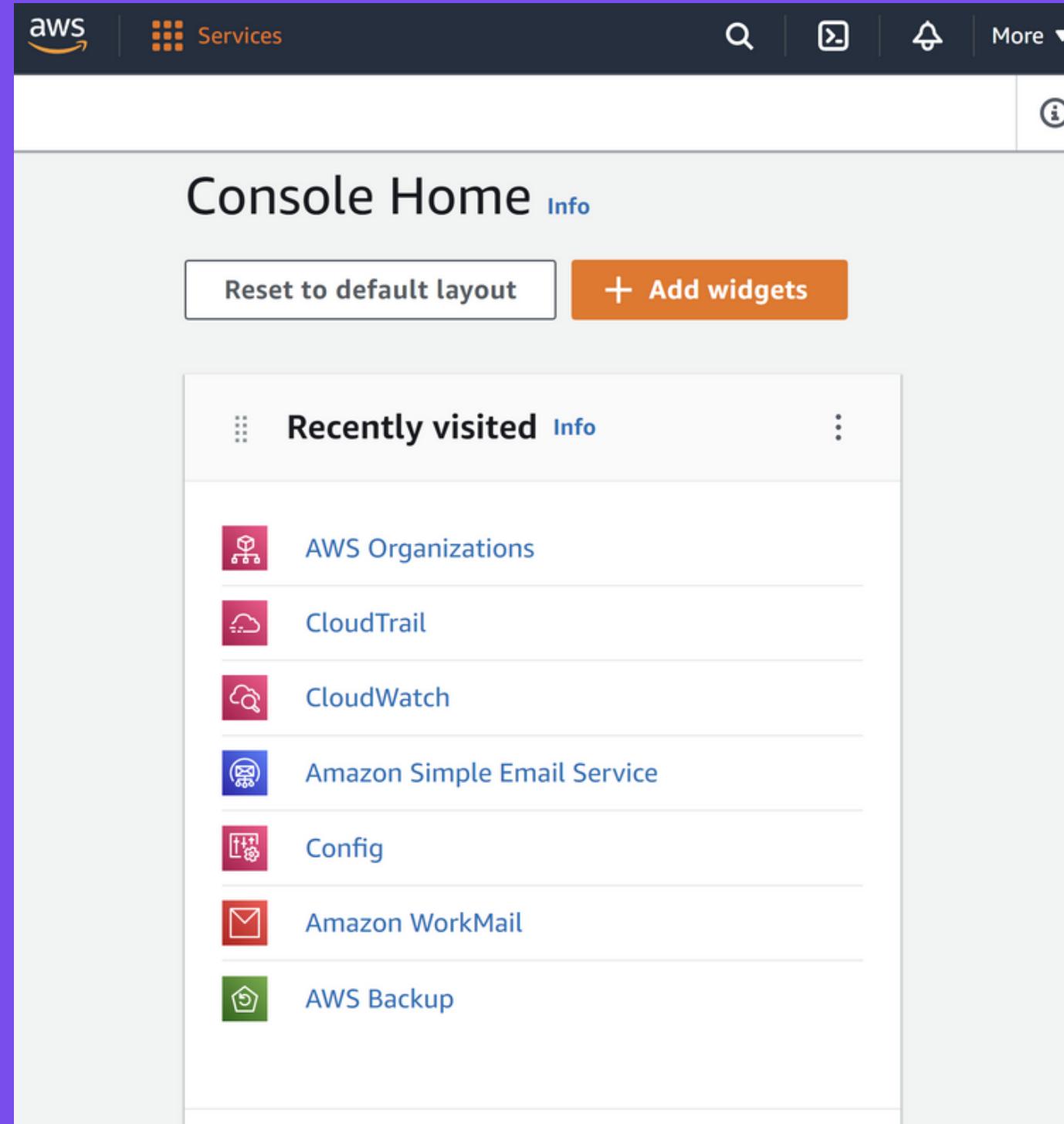
**AP-01**

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)

The screenshot shows the Microsoft Azure portal interface. In the top left, it says "Microsoft Azure". Below that, "Home > iotp-bkt". The main title is "iotp-bkt | Networking". On the left, there's a sidebar with various options: "Data management", "Backups", "Deleted databases", "Failover groups", "Import/Export history", "Security" (which has "Networking" highlighted with a red oval and a red arrow pointing to the main content), "Microsoft Defender for Cloud", "Transparent data encryption", "Identity", and "Auditing". The main content area is titled "Firewall rules" with the sub-instruction "Allow certain public internet IP addresses to access your resource. Learn more". It includes buttons for "+ Add your client IPv4 address" and "+ Add a firewall rule". There are two rows of rules listed:

Rule name	Start IPv4 address	End IPv4 address
Other white listed public IPs	EEE-IOT Wi-Fi	Public IP
Other white listed public IPs	ET0731-IOTS Wi-Fi	Public IP

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

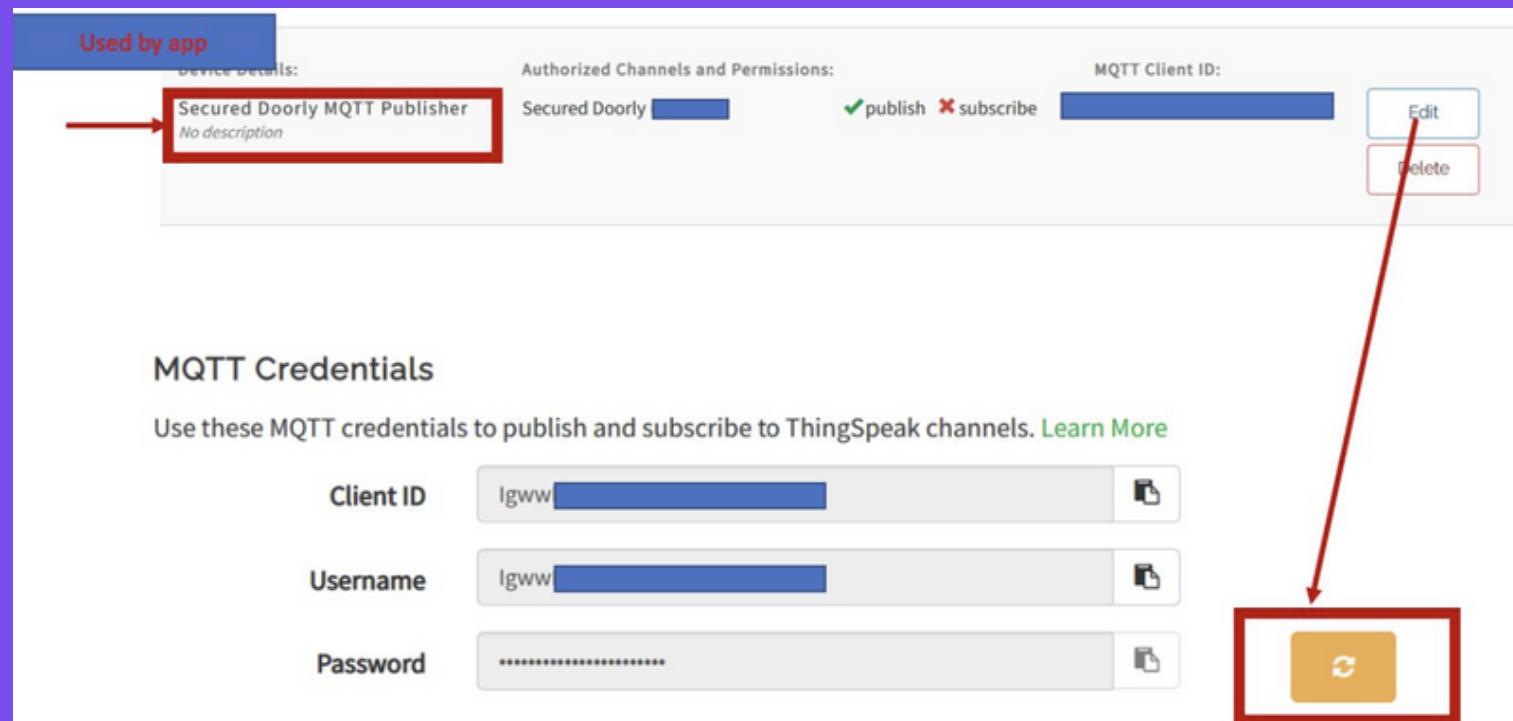
RS-04

Regular backup of system data

AU-01

Significant events recorded

# TR64 Assessment(MQTT)



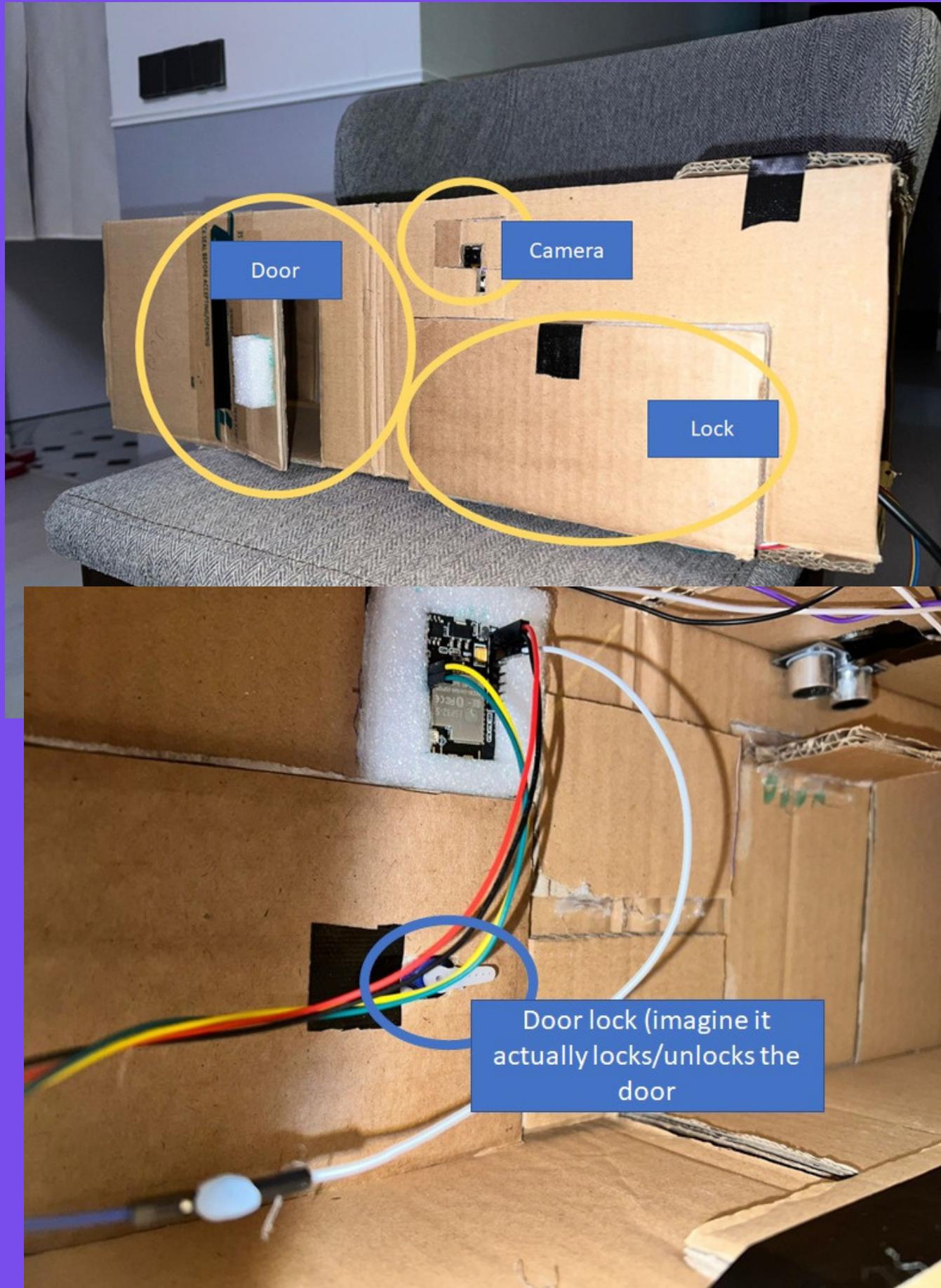
MT-01

Strong password policies

NP-04

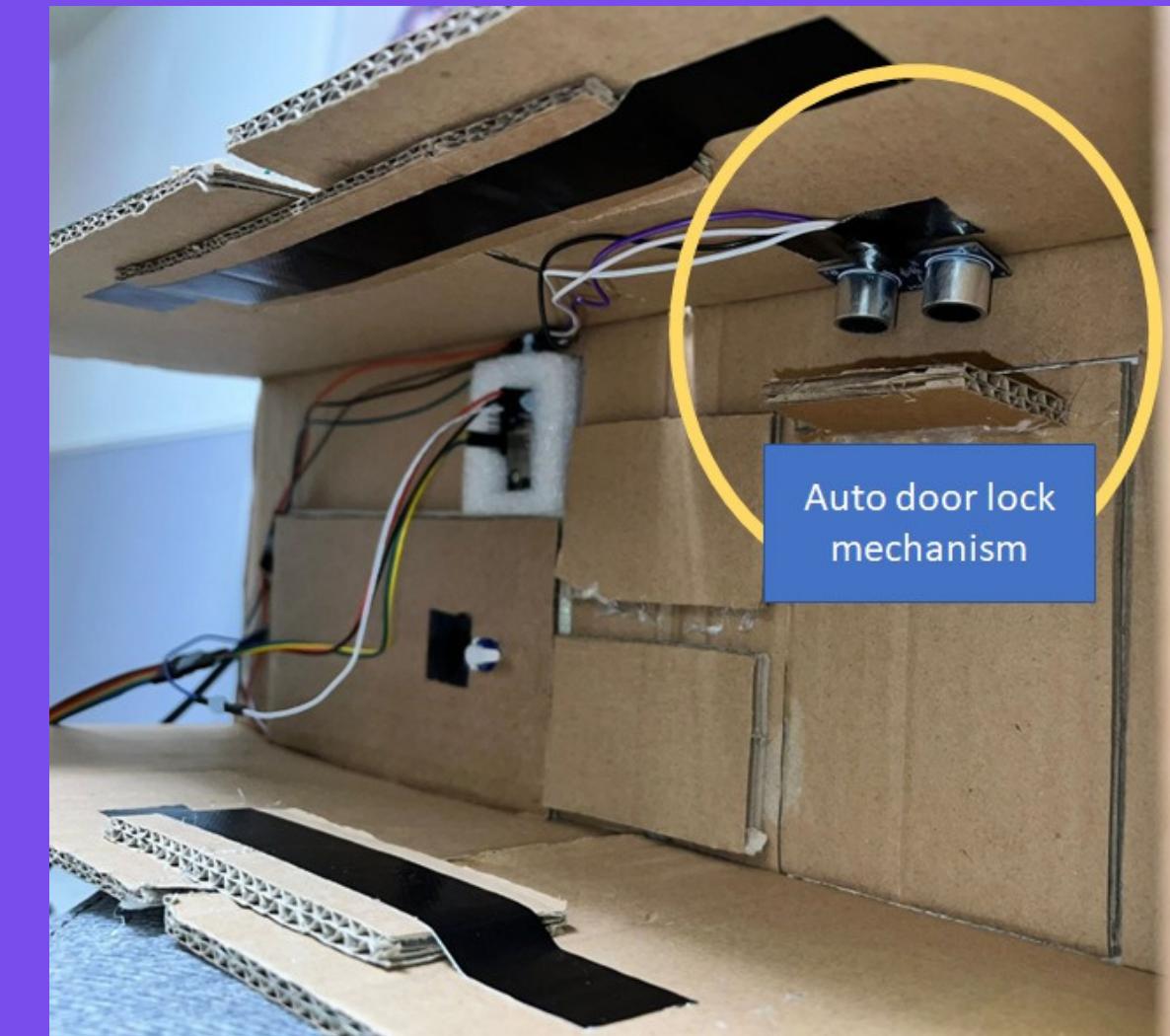
Secure connectivity based on industry best practices

# TR64 Assessment(Hardware)

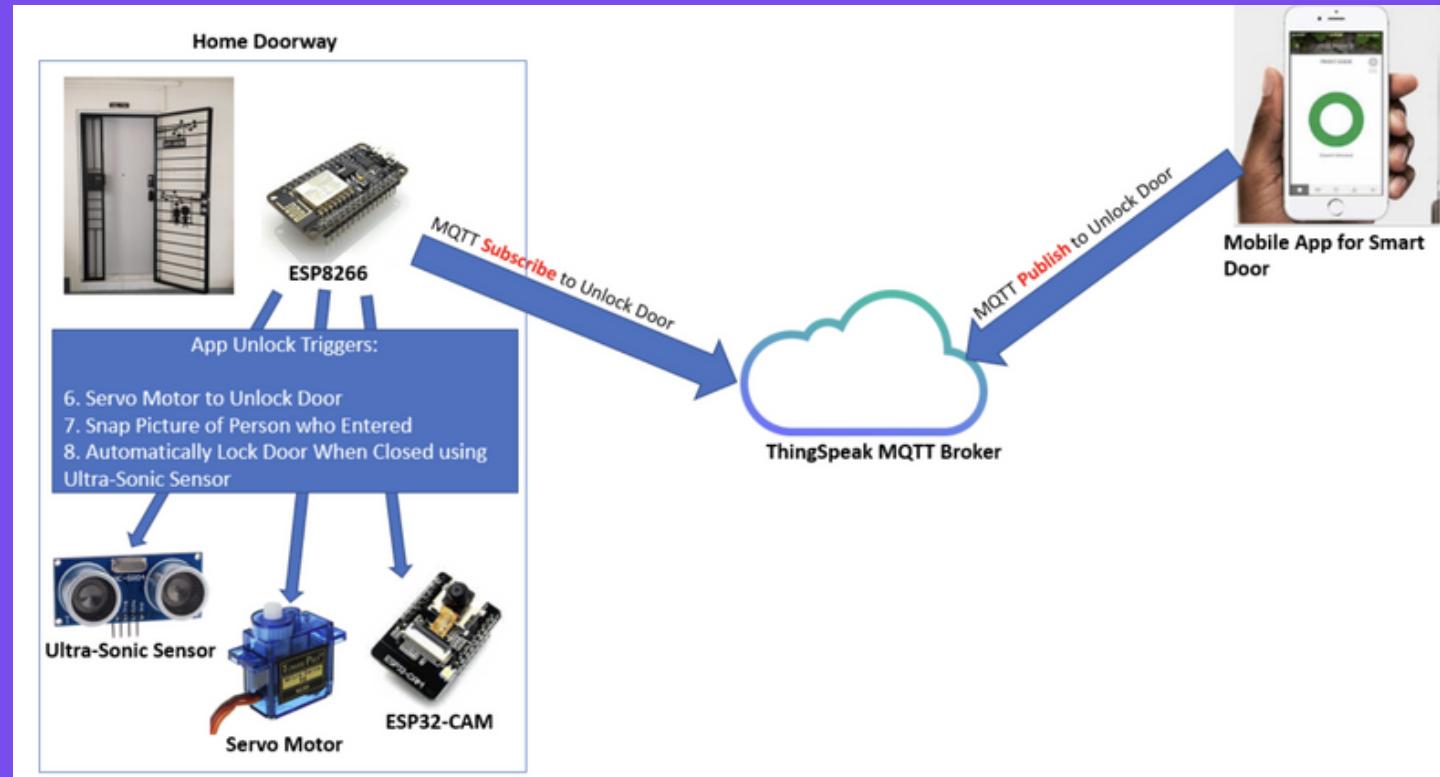


AP-04

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