Singapore Polytechnic

REPORT ON Secured End-to-End IoT for Door Entry System

Prepared and submitted by:

Class:	DCPE/FT/3A/25
Team Members	Student Id
Joseph Luther Tabaluyan	2033204
Brandon Chong Jun Wei	2032779
Ling Yi Hao Craigus	1908828

In partial fulfilment of the requirements for the module
ET0731: Internet of Things Security

Lecturer: Chee Wai Chan
Submission Date: 5th February 2023

Overview

Based on the topic given, we are planning to implement a door entry system for a house owner. The features used would ensure high security in the physical layer as it would be very difficult for threat actors to break and enter into the household.

First of all, residents would have to log into a web server with their username and password and request for an otp based password. Subsequently, the user will then input the otp based password into the web server to unlock the door. Additionally, there will be a camera on the door which is activated by the microcontrollers to automatically capture a picture when the otp based password input is wrong. This can also act as a physical deterrence. The photo will be sent to the home owner's phone via telegram bot.

Lastly, when the user decides to leave, he would have to press a button inside the booth. That will give him 15 seconds to exit before the door will be locked.

Why we decide to implement this project

1. To provide home owners a secure and safe solution to control access into their household
2. Remove the use of keys

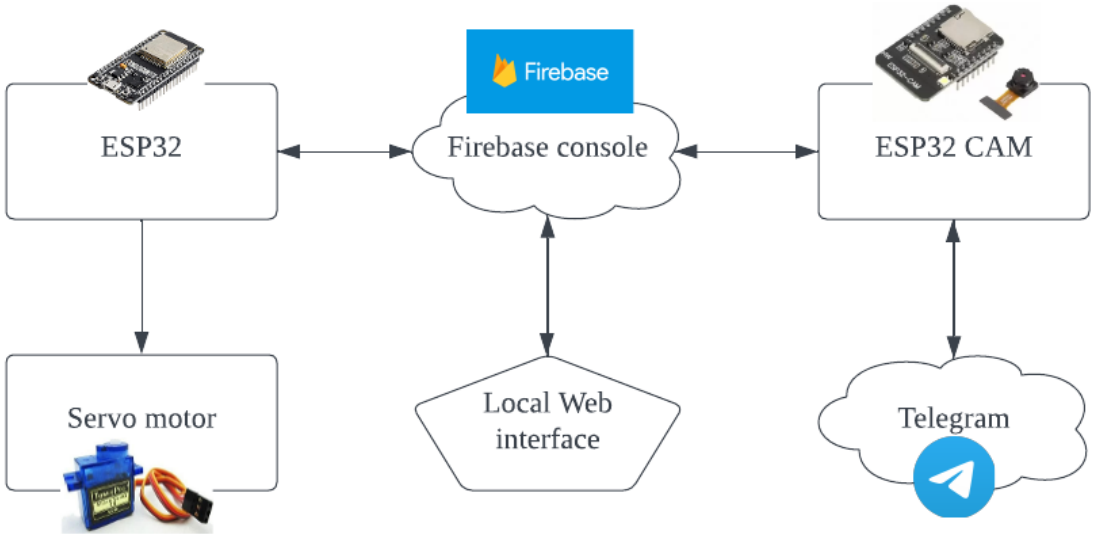
Goals

- Collect data and send user details to Firebase (database) through ESP 32
- OTP Based Password using random number generator]
- Complete the camera function using the ESP32 Cam
- Simulate a door lock using a servo motor
- Create a secured end-to-end IoT for door entry system

Hardware & Software required

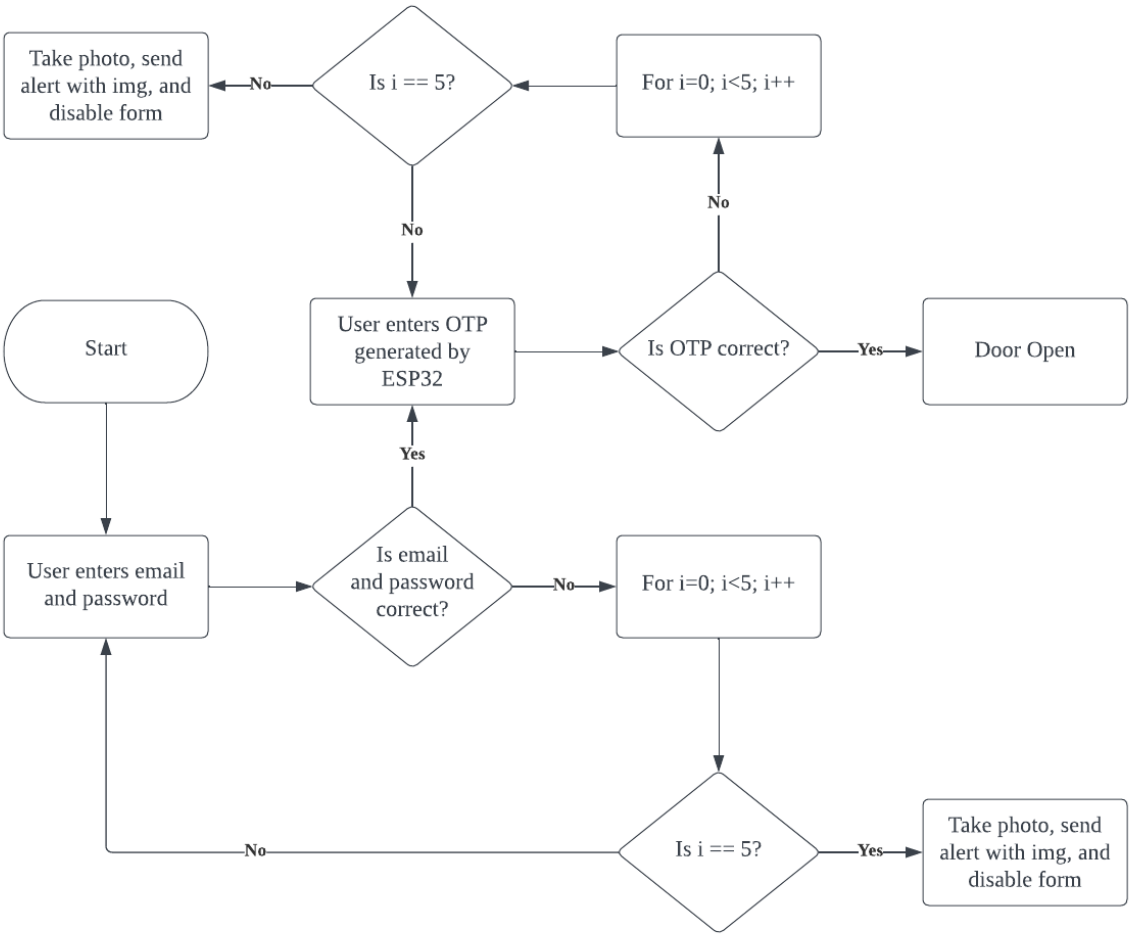
1. ESP32 Camera
2. Micro Servo Motor SG90
3. Firebase
4. Telegram bot
5. Arduino Software

Flow charts and component connections



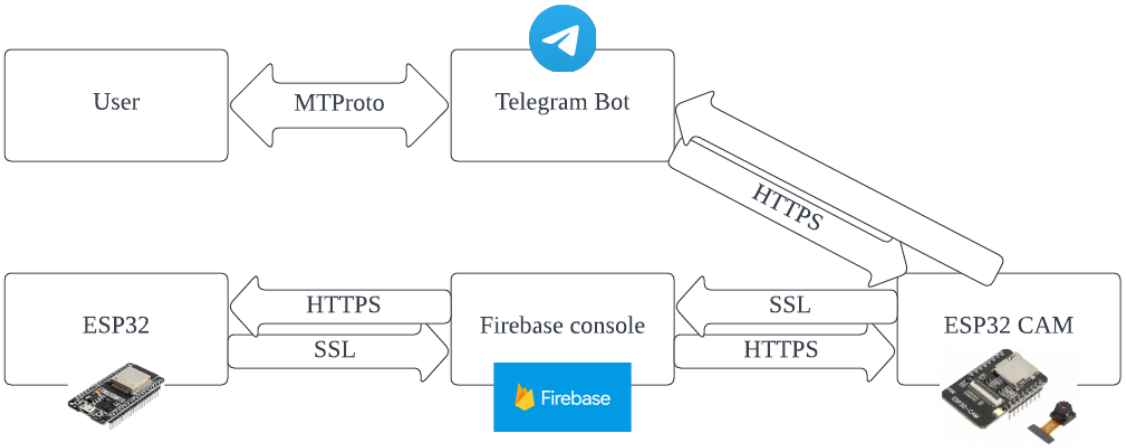
We will be using 2 microcontrollers in this system, ESP8266 acts as the middleman and will handle the motor, the camera, telegram integration, and communication with Firebase which also hosts the webserver. The data will be sent through and uploaded onto Firebase Console. Not only will we be storing our data in Firebase, but also using it as an OTP generator. Firebase has embedded encryption available making it a reliable and relatively safe option.

System Flow Chart



The user will have to log in with their username and password on a web browser. The user has 3 attempts before he is logged out and his picture will be taken by the ESP32 CAM. Upon a successful log in an OTP will be generated and sent to the user and he has to input it into the web browser. Once the right OTP is inputted the door will open.

Dataflow



Users access the Firebase console as an interface to unlock the door lock. Firebase will contain all the residents usernames and passwords along with their email address for verification. Besides acting as a database, Firebase will host a web server as well as communicate with the ESP8266 via HTTPS. ESP8266 is connected physically to the ESP32 CAM and will send an output to the chip for the camera to be activated whenever password is detected incorrect 3 times. The ESP32 CAM then sends the image to telegram via MQTT. Additionally, the homeowner can request for an image capture anytime he wants by slash commands in the bot's chat.

Attack Surface	TR64 ID	Description
Website	CS-01	One-time password
	AP-02	User will need to enter a OTP
Firebase	CS-02	Uses TLS 1.3 to encrypt data in transit
	CS-03	Data encrypted at rest using AES-256
	IA-01	Users password will be hashed
	IA-02	User will need to enter a OTP
	NP-01	Firebase will double check user credentials in order to read and write to and from database
	DP-04	Implement role-based access control
	RS-02	Supports ephemeral elliptic curve Diffie-Hellman cryptographic key exchange signed with RSA and ECDSA which help protect traffic and minimise the impact of a compromised key, or a cryptographic breakthrough
System	LP-01	Conduct threat modelling to identify and analyse threats
Network	MT-01	Used a strong password for Wi-Fi network

Threat Type	Mitigation
Spoofing	TLS is protected against replay attacks using the Message Authentication Code(MAC)
Tampering	Data at rest is encrypted using AES-256 and data in transit is encrypted using TLS 1.3
Repudiation	One-time password shows the email of the user who requested it
Information Disclosure	Role-based access control prevent unauthorised access to information
Denial of Service	Strong WiFi password, MAC address filtering, turn off ports that are not used, Firewall
Escalation of Privilege	Access to the physical system is needed

Gantt Chart

GANTT CHART

PROJECT TITLE	IOTS Mini Project End-toEnd Door System	**Group 4**	Joseph Luther, Brandon Chong, Craigus Ling
Project start date:	3-1-2023	**Project end date:**	

WBS NUMBER	TASK TITLE	TASK OWNER	START DATE	PCT OF TASK COMPLETE
1	**Project Conception**			
1.1	Project Propoal	Joseph L	3/1/23	100
1.2	TR64 Guidelines	Craigus L	3/1/23	100
1.3	Research on Web server	Brandon C	3/1/23	90
2	**Project Initiation**			
2.1	Firebase console	Joseph L		75
2.2	ESP32 Cam code	Joseph L		100
2.3	VS Web server	Brandon C		30
2.4	Prototype	Craigus L		0
2.5	Telegram Bot Integration	Joseph L		100
2.6	Chart Updates	Craigus L		70
2.7	Website documentation	Craigus L		10
2.8	Testing and troubleshooting	Brandon C		0
2.9	Presentation preperation	Brandon C		0

PHASE ONE	PHASE TWO					
WEEK 1	WEEK 2	WEEK 3	WEEK 4	WEEK 5	WEEK 6	WEEK 7
M T W R F	M T W R F	M T W R F	M T W R F	M T W R F	M T W R F	M T W R F