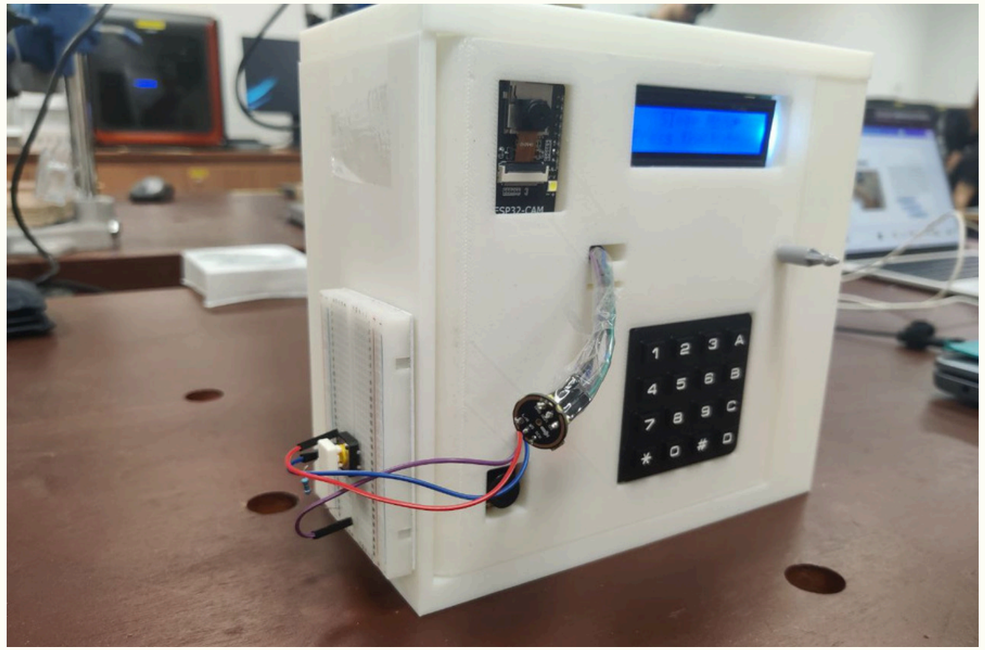
SMART LOCK

Ennouri Hsan
Rahman Satya
Yang Congxu
Zhao Zijie

START PRESENTATION

Problem Statement

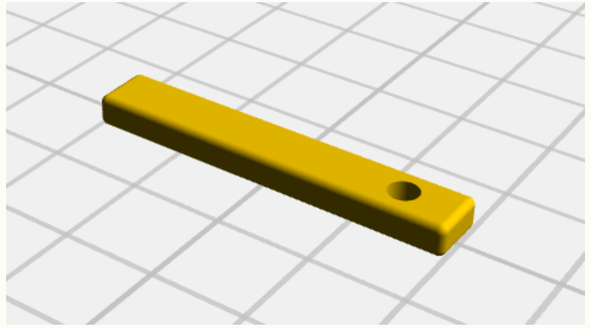
Traditional lock lacks multilayer verification to deal with the arising security challenges. A solution that provides more ***powerful protection*** and yet ***convenient*** to use is needed



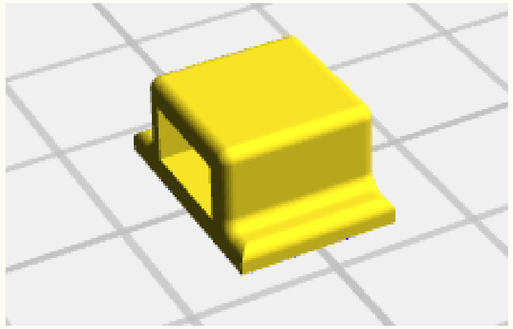
3D printed parts

Our project consists of a secured volt. In order to simulate the vault structure, we chose to design it using Computer Aided Design (CAD) and 3d print the parts in the lab 3d printers. Because of time constraints and not to use a huge amount of materials, we decided to reduce the size of our vault making it harder to fit all the hardware inside for the live demo. For a more secure version, all the parts should be made using a more secure material such as steel, and the size should be slightly increased (increasing the width to make the vault a cube could be sufficient).
Here, we present the 3d designed parts.

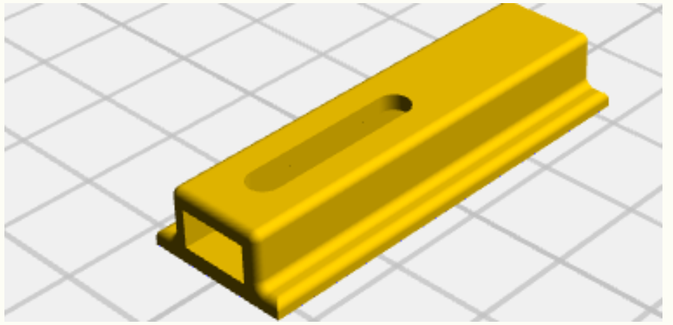
Locking mechanism :



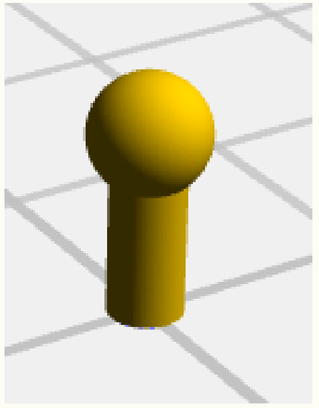
Sliding Bolt



Lock Bolt Receiver



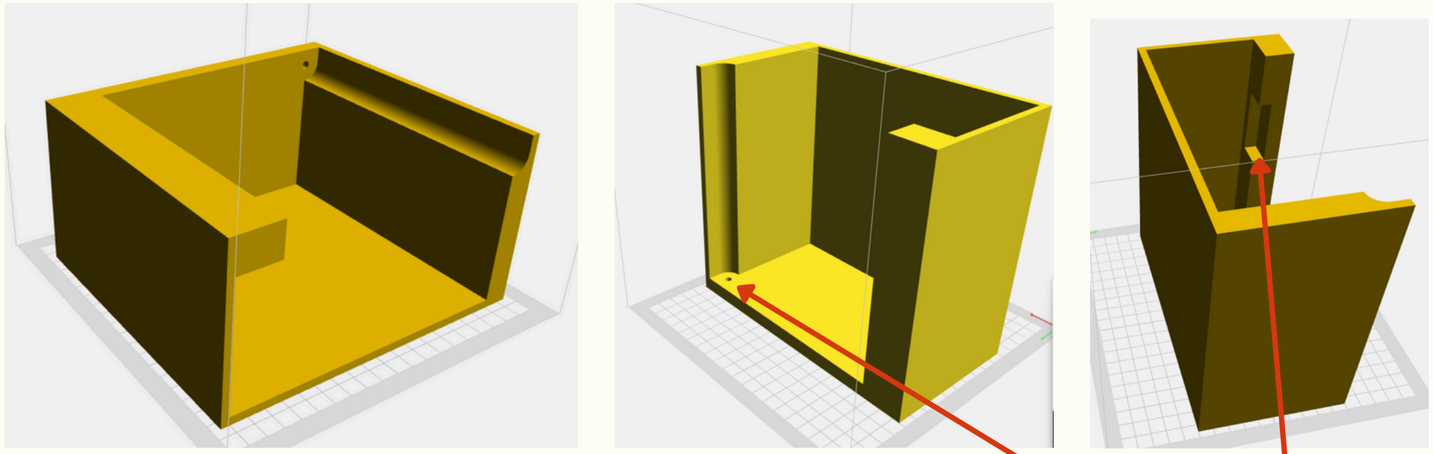
Lock Main Body



Lock pin

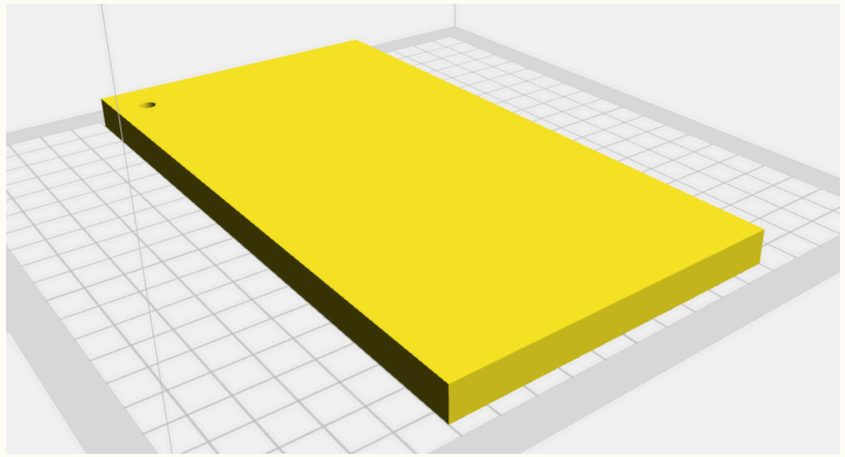
Remark : The locking mechanism CAD design have been taken from the internet due to lack of time

Vault Main Body



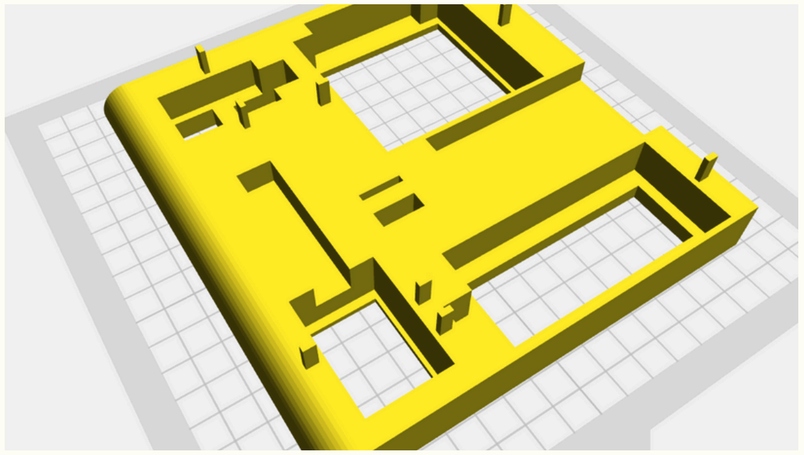
Main body of the vault. The Lock bolt receiver will be fixed here. The vault door will be supported by a small rod on the hole at the left bottom of the vault, this will allow the door to slide open.

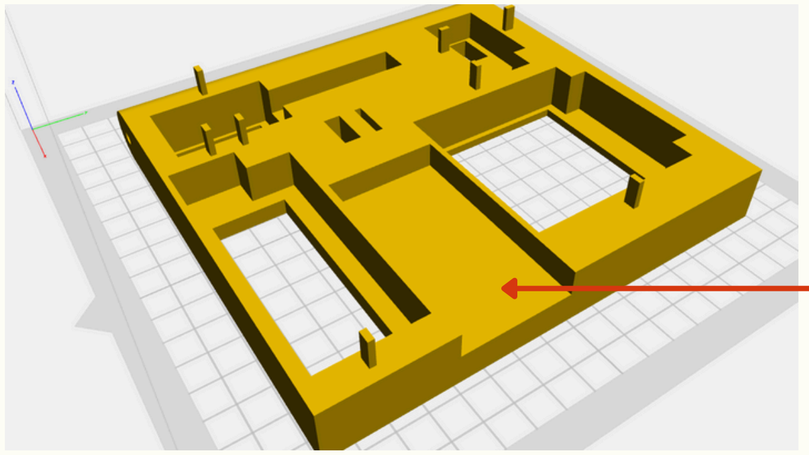
Vault ceiling



Ceiling that will be glued on top of the main body after securing all the parts inside. It has a hole on the side to allow the door to slide when we decide to open it.

Vault Door

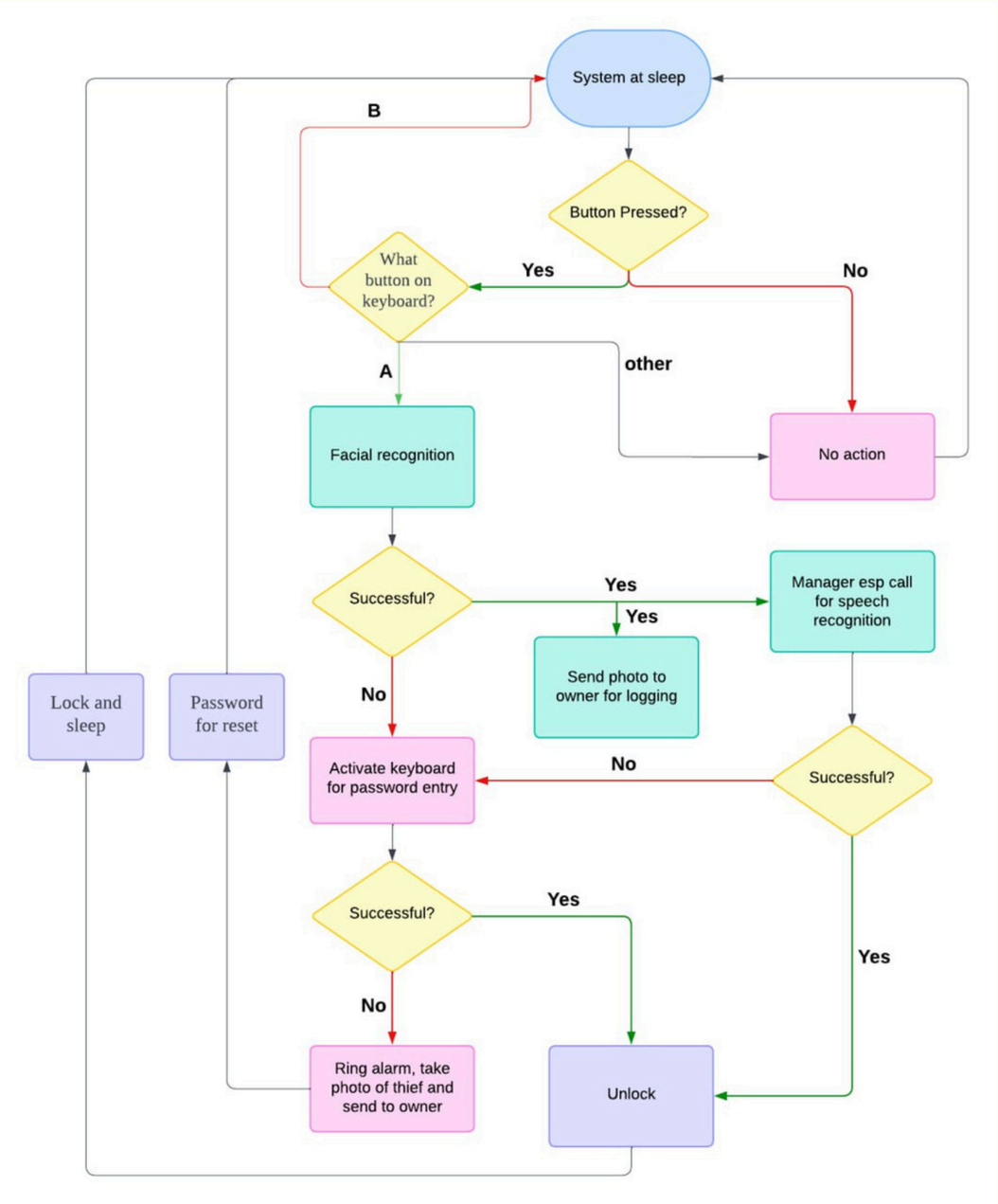




The door was design specifically so that all the components can fit in a specific spot resulting in a very esthetic door seen from the outside. Each component will be fixed to its designated slot using hot glue.

The rest of the lock will be fixed in this small designated space allowing a perfect alignment with the bolt receiver

System Overview



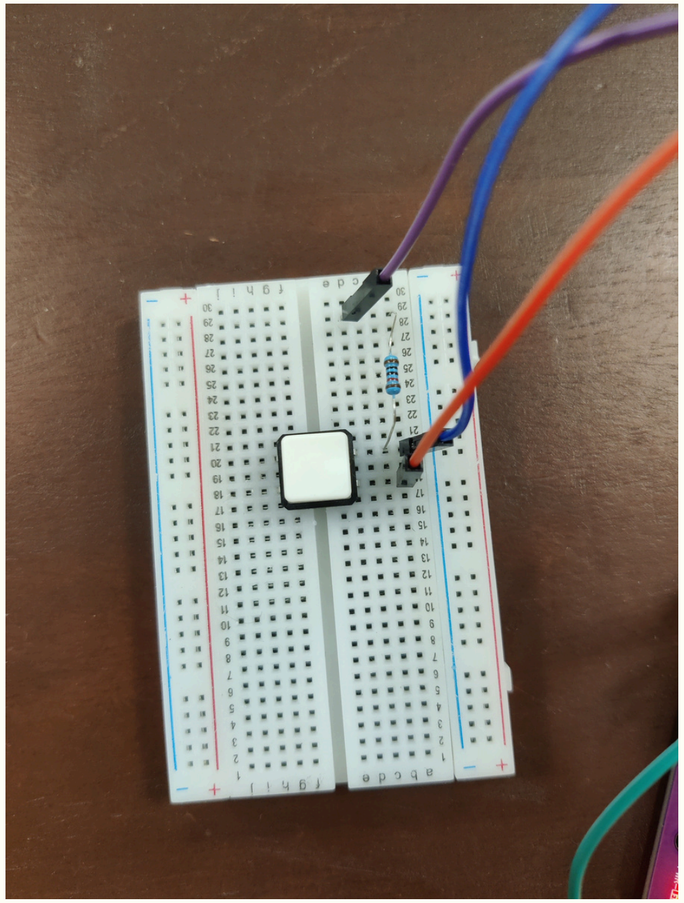
ESP Pin Arrangement

Component	ESP32 Pin	Notes
4x4 Keypad		
- R1	GPIO 26	Row 1 of the keypad
- R2	GPIO 27	Row 2 of the keypad
- R3	GPIO 12	Row 3 of the keypad
- R4	GPIO 13	Row 4 of the keypad
- C1	GPIO 19	Column 1 of the keypad
- C2	GPIO 18	Column 2 of the keypad
- C3	GPIO 4	Column 3 of the keypad
- C4	GPIO 25	Column 4 of the keypad
LCD Screen (I2C)		
- SDA	GPIO 21	Dedicated for I2C communication
- SCL	GPIO 22	Dedicated for I2C communication
INMP441 Microphone		I2S mic – works with I2S protocol
- VCC	3.3V	Power
- GND	GND	Ground
- SCK	GPIO 14	I2S Serial Clock
- WS	GPIO 15	I2S Word Select
- SD	GPIO 32	I2S Data Output
Servo Motor	GPIO 33	Control pin for servo
Active Buzzer	GPIO 16	To generate sound/alarm
Wake-up Button	GPIO 35	Button to wake up ESP32 from deep sleep

System Activation

After every unlocking, the entire system will be locked and put to sleep after specific buttons pressed to wait for the next useage. We add a button to the manager ESP so that it can be the trigger to wake up the system.

- Lower power consumption
- Easy & reliable activation



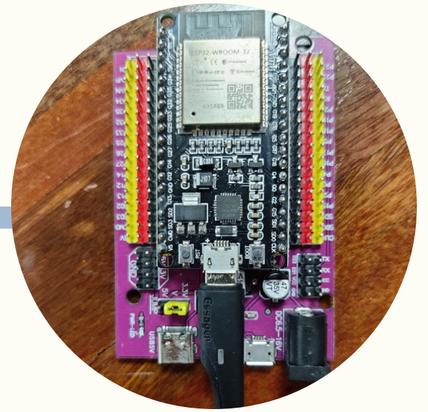
Facial Recognition

This facial recognition uses an ESP32-CAM to capture image and then send it to a server over Wi-Fi for processing using HTTP request. The photo taken will be sent to the owner for logging purpose. The server compares the image against a set of known faces using a trained neural network model. The server verifies the identity and returns a recognition result with regards to a set threshold. The server then returns the result to ESP32-CAM. The camera will publish these results to the manager ESP via MQTT for other actions to be taken.

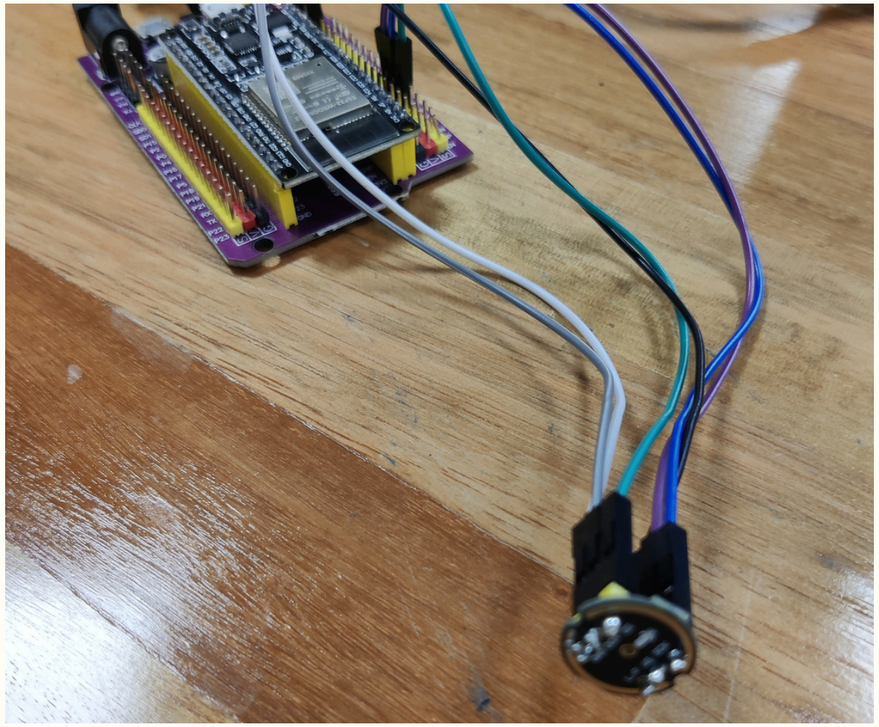
Photo taking

Image analysis in server

Result publish via MQTT



Speech Recognition



When a successful result of facial recognition is detected, the manager ESP will signal the start of speech recognition. We use the I2S interface to collect audio data from the microphone and then convert sound into digital data. When the server receives an audio file, it stores it locally in the .wav format and utilizes the speech_recognition library to transcribe the audio from spoken words to text for. The transcribed text will be compared with a preset password to determine the result of the recognition.

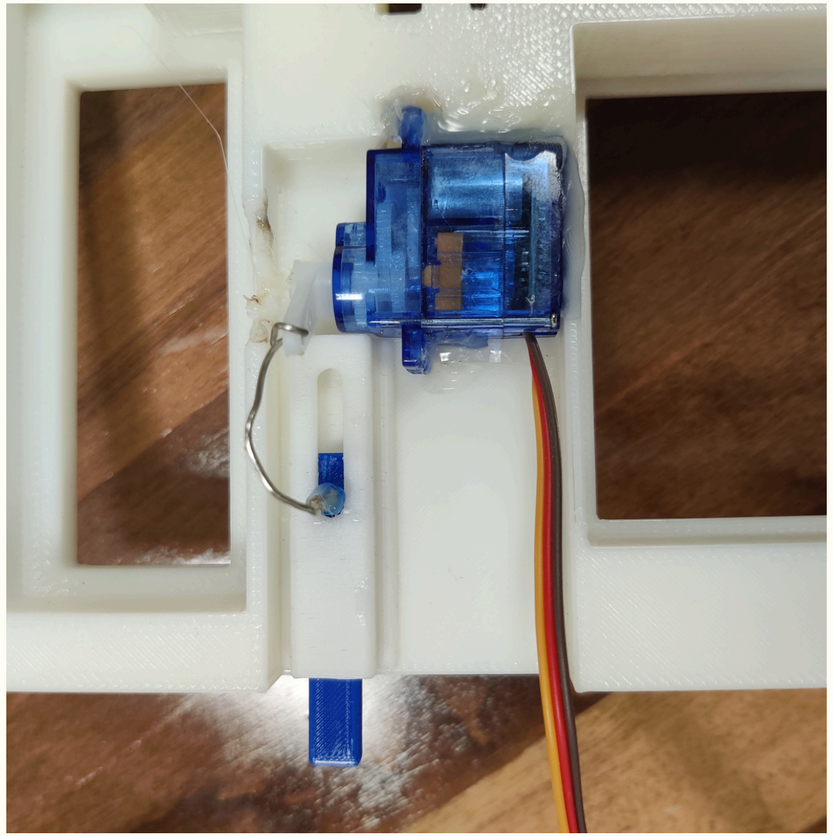
- HTTP requests
- Flask
- Threading

Passsword Entry

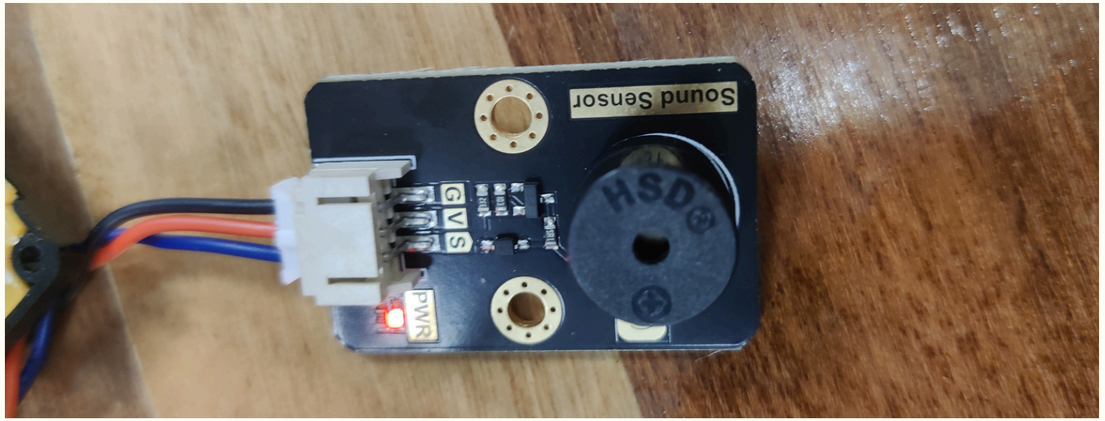
When either of the previous 2 steps fails, the keyboard will be activated for password input. The user will be given 3 chances to enter the correct password. The password is composed of 4 digits and the system compares the entered password to the correct one when 4 digits have been entered. Erasing function for the alarm is assigned to “*” button for possible missed click.

If all 3 attempts have failed, the manager ESP will signal the alarm to ring.

Unlocking & Alarming



Upon successful Two-Step authentication or correct keyword entry, the manager ESP will signal the servo to unlock the gate. When all measures fail, the alarm will ring to alert nearby personel for the breach attempt.



Alert Message

Telegram bot linked to ESP32-CAM

Automatic photo taking and sending

When the keypad authentication fails, it marks the failure of the whole authentication process, access is prohibited and the photo taking process is also activated, the picture will be sent to user’s phone through telegram for further information.

Lock, Sleep & Reset

After successfully unlocking, the door can be locked and the system can go to sleep with a “C” input on the key board.

An input of “B” will put the system to sleep . This feature is only possible immediately after the system have been awakened from sleep, for security reasons.

If unlocking fails, a secret password can be entered to reset the system to sleep mode.

Conclusion

The smart lock system is a powerful integration of advanced security technologies, combining facial recognition, voice authentication, and keyword entry for multi-layered protection. By leveraging ESP-CAM, a Python server, Telegram bot and MQTT communication, the system provides a seamless and responsive user experience. In addition to security, the system offers immediate alerts and fallback options, ensuring robust access control in any situation.

Demo Scenario

Authorised User

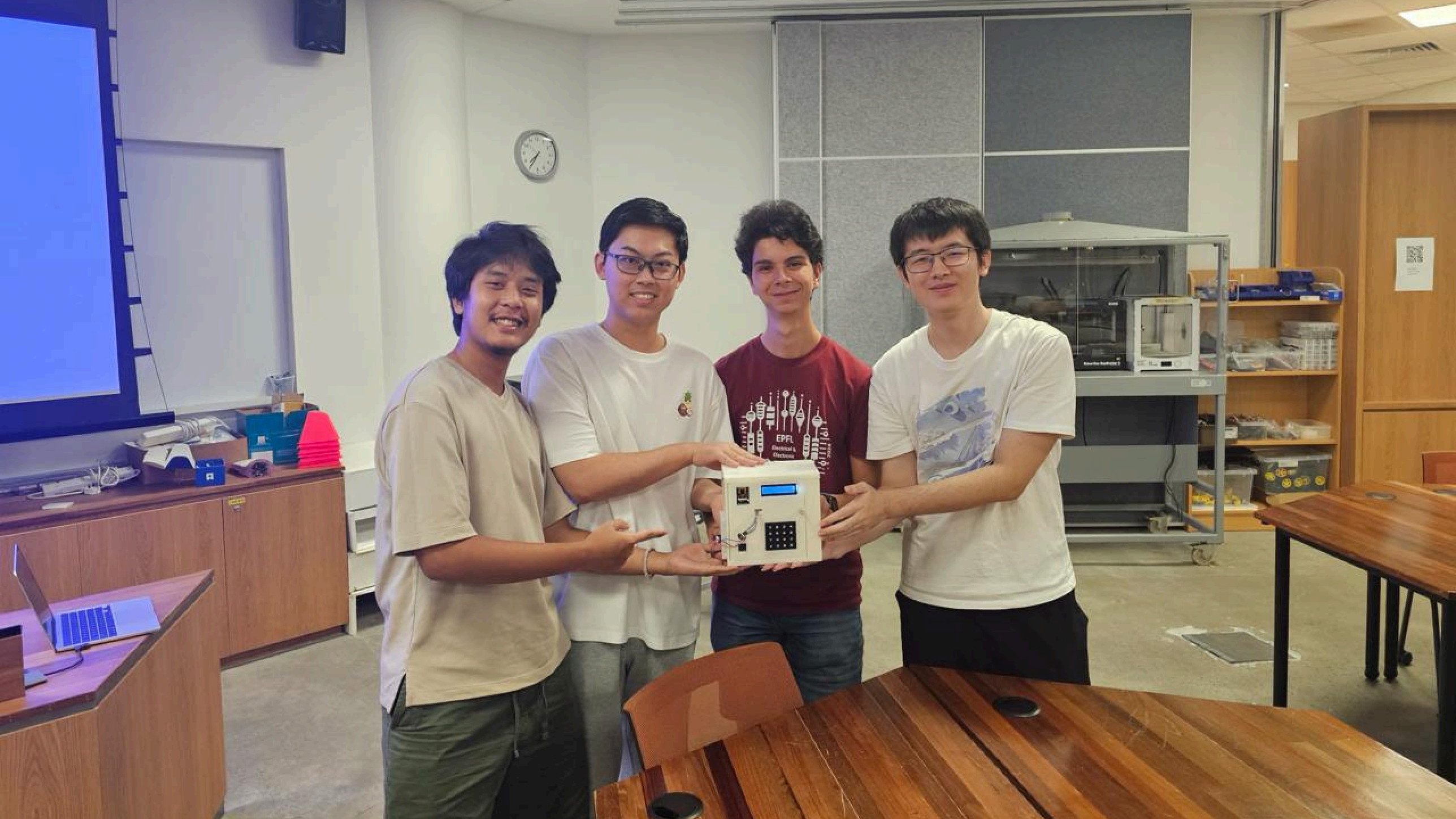
Demo Scenario

Stranger with Password

Demo Scenario

Thief!

THANK YOU!


EPFL