Office Access Control System

By

Shariar Alamgir (alamgir2)

Thomas Ng (thomasn3)

Vincent Nguyen (vn4)

Final Report for ECE 445, Senior Design, Spring 2021

TA: Anand Sunderrajan

May 4, 2021

Project No. 27

Abstract

The Office Access Control System is a multi-factor authentication system to allow for secure access into an office without the need of a physical key. The factors of authentication include a PIN entry, an NFC Tag Verification, and a Facial Recognition system using Microsoft's Face API to allow for three different combinations of access. The methods of authentication can be performed in parallel for quick access into the office. The Office Access Control System also has emergency exit capabilities for emergency situations such as a fire. The system is able to accurate authenticate users within the system using all three methods of authentication, as well as rejecting individuals who are not in the system and fail to provide two factors of authentication. The system also detects fires with high accuracy and does not trigger an emergency situation in scenarios where a fire is spoofed.

Contents

1 Introduction

1.1 Objective

British Petroleum (BP) is in need of a more secure way to give office access to employees. The current BP Spark office is only accessible by one or two people with the key. If one of these employees is not in the office, the door is inaccessible. Due to this, the main entrance is typically left unlocked once one of these employees is in the office posing a security threat.

To solve this problem, we will integrate a two-factor authentication system for access into a room, attached to the entry point of the room. The door will require people to validate themselves via two out of three forms of identification: Cell Phone Proximity, Facial Recognition, and Pin Access. This will ensure more secure entry to the office as it will validate a person using something he or she has, knows, and a bio-metric quality. Along with making access to the office more secure, we will enhance the overall security of the system by protecting against data leaks and other malicious attacks.

1.2 Background

The necessity of a more secure way of accessing the office is not isolated to BP. Many companies and organizations over the past couple of decades have been working to create more secure offices as security breaches have sparked. Security risk is assessed in two different categories: physical and information security [1]. Cyber-physical systems try to protect against these two risks.

The current BP Spark office only has two keys. This makes access to the office only available if one of these two people are in the office. If someone loses the key, it poses a security risk because anyone can access the office. BP is looking for a way to make the office more secure and accessible to their employees while protecting employee privacy. This project serves as a proof of concept for further use at other office locations such as their Houston office which has many turnstiles that this system can replace.

1.3 High Level Requirements

- Facial recognition is accurate at least 95% of the time, and the false non-match rate is less than .75%. According to the NIST Patriot Act bio metric standards, the best commercial facial recognition systems reached 90% accuracy with 1% false acceptance rate [2]. We will try to improve on these numbers because they are relatively old.
- The rate of successfully identifying a fire is 95%. A research paper was able to achieve 93.1% using only computer vision, so by combining computer vision with differential temperature sensors, it is possible to achieve an even higher rate of identification. [5].
- The response time from authentication to door unlocking is less than 2 seconds. We chose less than two seconds because the main bottleneck is the facial recognition component and its communication to the Azure database.

1.4 Physical Design

In the BP office, the NFC tag reader, microcontroller, and camera module will be located behind a glass wall that is adjacent to the door. The keypad will be in front of the glass wall, right next to the door handle. The microcontroller will communicate with a laptop that is elsewhere in the BP office, out of sight.

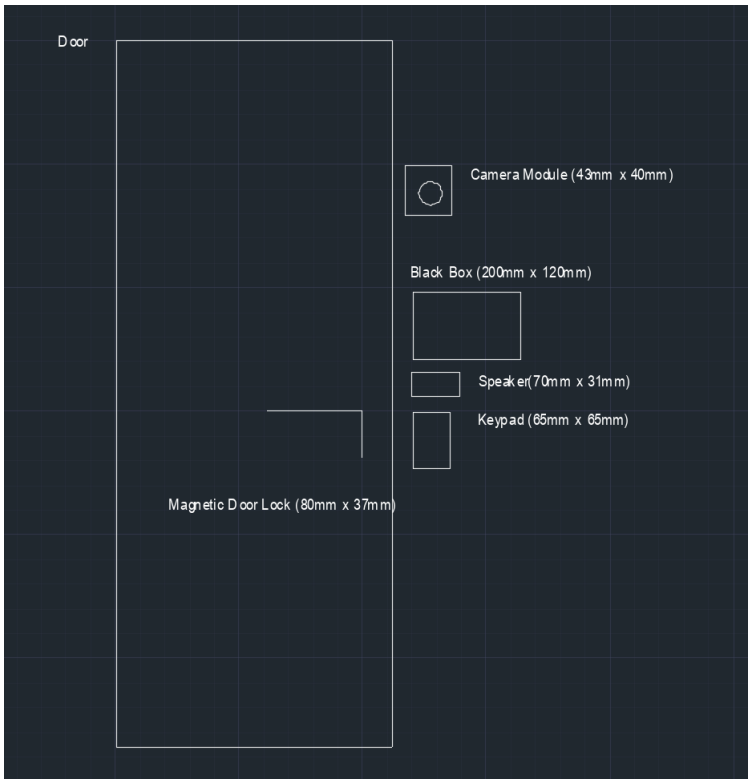

Figure 1: Physical design for Office Access Control System.

Figure 2: Front Display of Black Box for Office Access Control System

2 Design

The door requires many small subcomponents for operation to allow for multiple options of authentication. The authentication subsystem holds the blocks required for facial recognition, PIN access, and cell phone proximity to allow a user to enter the office. All of the components in the authentication subsystem must communicate the data to the central subsystem, which holds the ESP32 microcontroller and the Arduino interface. User information for who can and has accessed the office is sent and stored within an Azure cloud database. The emergency exit subsystem is responsible for quick and accurate communication with the microcontroller during an emergency situation that requires unlocking the door immediately. Incorporating a power supply that can output between 3.3V and 12V during open office hours is required to keep the door locked and allow for authentication when prompted.

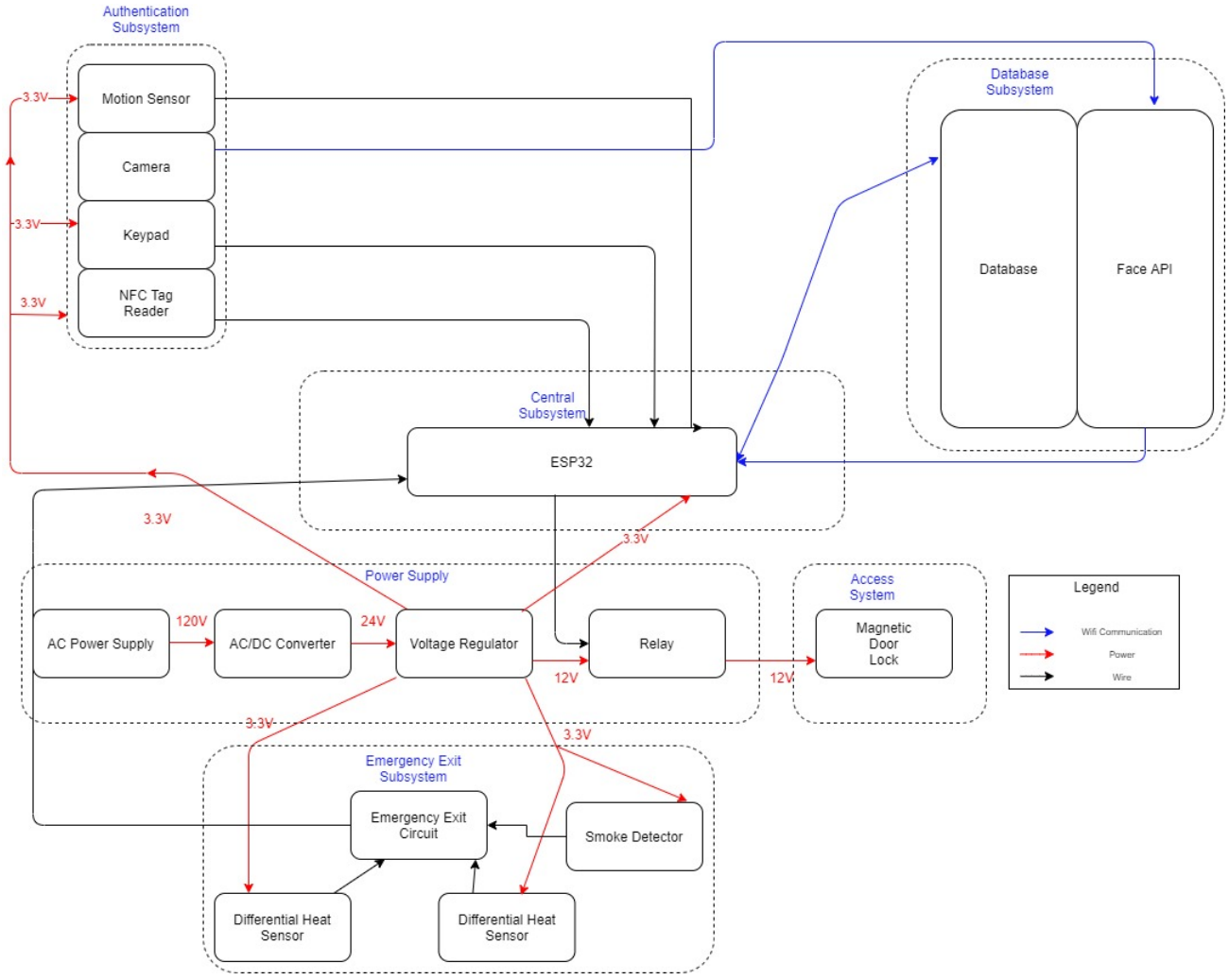

Figure 3: Block diagram for Office Access Control System. Components are divided into their subcategories based on their operation.

2.1 Design Alternatives

After our initial Design Review, we ran into some obstacles that required us to either modify or change our design implementations. Two changes occurred within our Authentication and Database subsystems that helped us integrate our project as well as provide for more secure data storage

1. Switching to Microsoft's Face API:
2. Removing Face Data from Database:
3. Utilizing an NFC white card: This was to combat the technical aspects of mobile devices, specifically Apple devices, that did not provide a simple solution to reading NFC values from the device. With the commonality of Apple devices, we decided to use Mifare blank cards to give each user their own card with a NFC value that we can write on user creation. This card can be kept/integrated into an ID card for all employees when scaled out to BP.

2.2 Subsystems

2.2.1 Central Subsystem

The central subsystem is responsible for validating the factors of authentication, unlocking the door, and communicating with the cloud database through the ESP32 Microcontroller. The ESP32 must validate whether the two different factors of authentication match a single username in the system, and allow for the magnetic lock to unlock and log the access into the database.If valid, the software will allow the microcontroller to unlock the door, and the database will log the authenticated individual entering the room. All parts of the authentication system will communicate with the ESP32 and the microcontroller is programmed using the Arduino IDE for software operations.

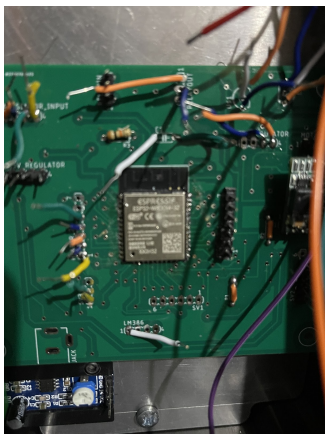

Figure 4: ESP32 on the main PCB

2.2.2 Authentication Subsystem

The authentication subsystem is built by components necessary for our three factors of authentication. The first factor is the NFC Tag reader. The NFC Tag reader is responsible for the cell phone proximity method of authentication. The Tag Reader will read the NFC Tag from a phone or card and validated with the

databases hashed-stored entry for the user. The second factor is the 10-digit Keypad. Built directly on its own PCB, the keypad is used for PIN access authentication using a shared PIN with all BP employees. The final factor is the Facial Recognition Module. This module is triggered from a motion sensor which detects an individual approaching the door. Once triggered, the ESP32 CAM captures images of the user and requests a challenge response by the user (via smiling) before sending this data to Microsoft's Face API. An important feature is that all 3 of these components are capable of working in parallel with each other, allowing for a more optimized way of authentication. This way, a user can complete multiple factors of authentication at once if they wish to, or do them one at a time.

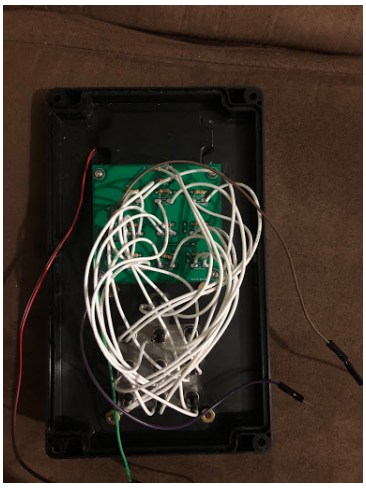

Figure 5: Inside display of Front of Black Box, with PCB and Wires for Keypad

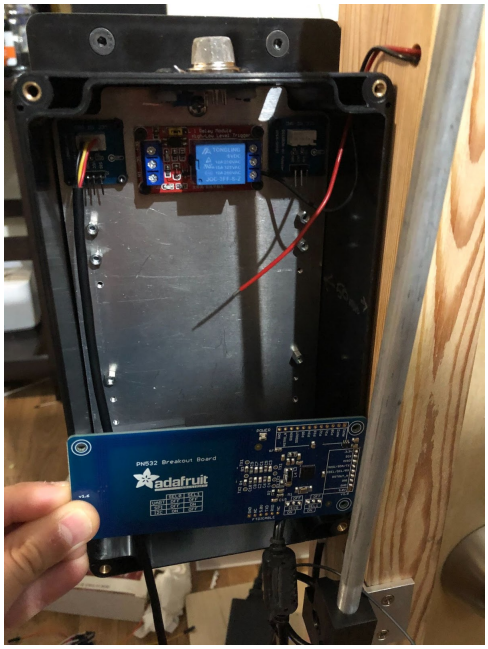

Figure 6: Adafruit NFC/RFID Breakout Board

Figure 7: ESP32 Camera and Motion Sensor

2.2.3 Database/Server Subsystem

The BP Spark NFC Tag information is held in an Azure Cloud database, and the facial recognition processing is performed on Microsoft's Face API. The information held must not reveal any personal information about the user, other than a given username. Microsoft's Face API solves this challenge as well since none of the images are saved on the server or database side, following ethical guidelines.

2.2.4 Emergency Exit Subsystem

To ensure secure exit from the office in case of an emergency, the Emergency Exit Subsystem is required to monitor the environment and inform the ESP32 if issues arise. This subsystem is built using two DS18B20 Differential temperature sensors and one MQ2 Gas Sensor to accurately detect fires. The combined signals sent by this system will automatically override the authentication necessity to unlock the door.

2.2.5 Power Subsystem

Power must be maintained during the hours of building operation so that all employees who wish to enter the office are able to authenticate themselves properly. Likewise, power must be provided to the magnetic door lock at all times to ensure the door remains locked, unless unlocked by authentication or emergency. A 24-Volt power source is used with three voltage regulators to distribute the proper voltage to all components, ranging between 3.3 and 12 volts. A relay switch is also used to handle communication with the microcontroller and the magnetic door lock for locking mechanism.

Figure 8: One temperature sensor, shown being pointed on the inside of the office.

Figure 9: MQ2 Gas Sensor mounted above the black box.

2.2.6 Access Subsystem

The door at BP Spark operates via a 12V magnetic door lock. This lock will remain powered on until a user has been authenticated, at which the voltage provided to the door will go to 0. This lock is powered after 5 seconds of being opened, locking the door once it is closed. The lock must be able to provide enough resistance force so that the door cannot be opened with ease while locked.

Figure 10: One of the voltage regulators on our PCB, used to distribute 12 Volts to the magnetic door lock.

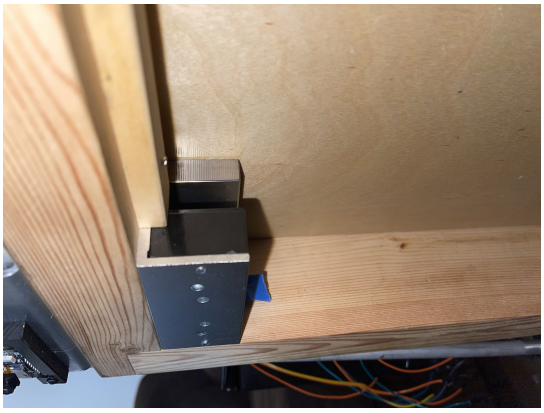

Figure 11: The magnetic door lock on the top of our door frame.

2.3 Authentication Control Flow

The authentication is handled by the ESP32 and a remote server that runs a Python script. The remote server communicates with the ESP32 to handle authentication inputs for the facial recognition and NFC Tag verification. The communication happens on one core of the ESP32, while the other core is always registering keypad inputs so that there is no delay in how any inputs are handled.

Once a form of authentication has passed, the ESP32 will set a flag for it, and the ESP32 always checks the flags to determine if the door should be unlocked.

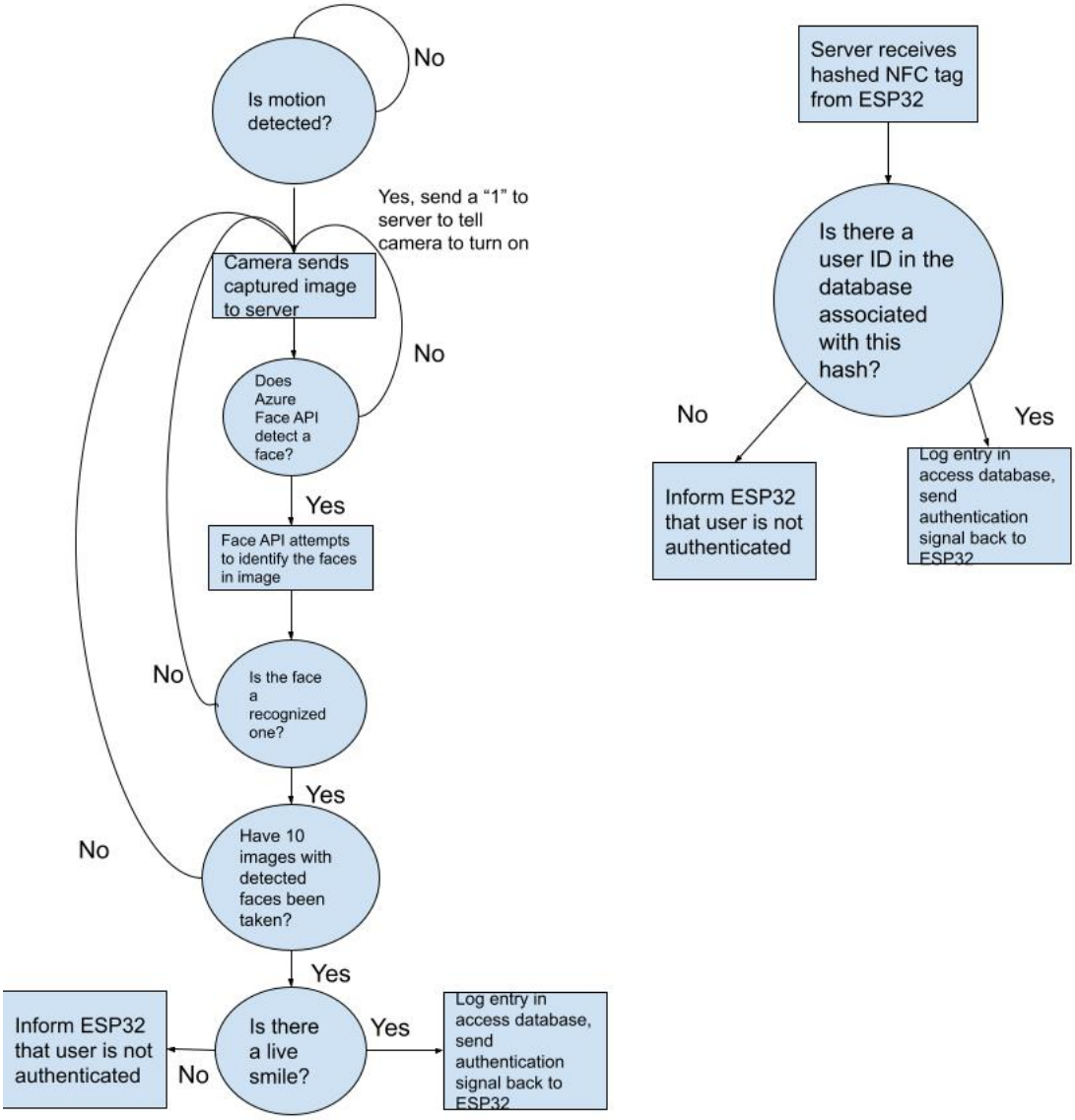

Figure 12: Flow diagram for face authentication (left) and NFC tag authentication (right).

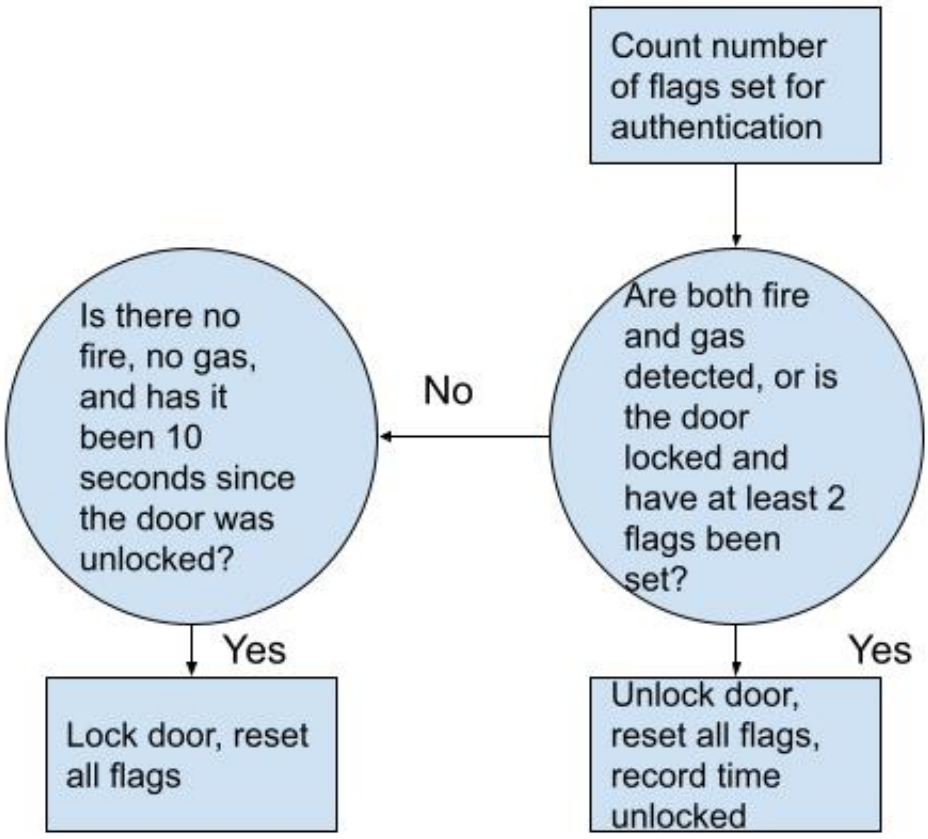

Figure 13: Flow diagram for locking and unlocking the door.

3 Design Verifications

3.1 Facial Recognition Module

To test the accuracy of our facial recognition system, 300 images were taken of 3 different people; 2 of these people are registered users in the database system and have had Azure's facial recognition system trained on their personal images, and the third person is anonymous to Azure. For each person, we measure the classification accuracy and the false non-match rate across 300 images. False non-match rate refers to the rate at which a biometric matcher miscategorizes two captures from the same individual as being from different individuals. We have a target classification accuracy of greater than 95 percent, and a target false non-match rate of less than 0.75 percent. The results of our tests were a classification accuracy of 97.7 percent, and a false non-match rate of 2.3 percent. We accepted these results because we prioritize classifying the correct individual.

We also verified the latency of the real time streaming protocol server that our ESP 32 Camera used. We calculated a latency of about 6.4 frames per second measured as the time from the camera taking an image to the server receiving it. This was calculated by calculating the average of every ten images sent about 50 times.

3.2 Emergency Exit Subsystem

To test the effectiveness and accuracy of our emergency exit Subsystem, 400 trials were conducted with different situations to trigger the emergency exit subsystem components. The trials were done to ensure that our high level requirement for fire detection accuracy was met while also checking the anti-spoofing defense of the signal handling on the ESP32 side. Each trial lasted 10 seconds.

1. The first 100 trials consisted of simulating an actual fire. This included a temperature increase that triggered the temperature sensor, as well as a smoke concentration build up that triggered the gas sensor. From the 100 trials, 97 of the fires were accurately detected, exceeding our high level requirement. The 3 fires that were not detected could have been due to trial duration or distance of the fire from the sensors. Regardless, our specifications were met in a large set of trials.
2. The next 100 trials only had a temperature increase with no smoke build up. This was simulated with using a lighter next to the temperature sensor. In these 100 trials, a fire signal was never sent, properly rejected the fake fire.
3. The next 100 trials only had a smoke build up with no temperature sensor. This was simulated with using incense sticks next to the gas sensor. In these 100 trials, a fire signal was never sent, properly rejected the fake fire.
4. The last 100 trials were controlled experiments with no temperature increase or gas build up. This was done to ensure our system operated normally and did not have glitches or random incorrect readings. A fire signal was never sent, ensuring the quality of the system.

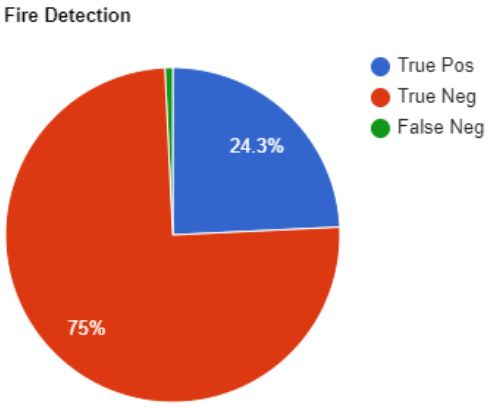

Figure 14: Pie chart depicting the fire detection accuracy as True Positives, and fire-spoofing rejections as True Negatives. Fire misses are false negatives.

4 Tolerance Analysis

One important part of our project is the ability of the microcontroller to multitask and process inputs in parallel. This is important because the microcontroller should be able to verify two or more authentication factors at the same time to ensure fast access to unlocking the door. The ESP32 has a dual core processor, so it is capable of multitasking. Instead of implementing a scheduling algorithm, we instead make use of both of the ESP32's cores. By doing this, we can make full use of the ESP32's processing capabilities while increasing the speed of unlocking the door.

5 Cost

For our group of three people, we are estimating our development cost to be $35/hour, working 20 hours/wk. The labor cost comes out to:

$$3 * \frac{\$35}{hr} * \frac{20hr}{wk} * 16wk * 2.5 = \mathbf{\$84,000} \tag{1}$$

Part	**Cost**
ALITOVE 24V DC Power Supply	$12.99
Weewooday Regulator Module	$12.99
Fuzadel Electromagnetic Lock 12v	$24.98
Zulkit Project Box	$11.99
GAOHOU 2 PCS DS18B20 Waterproof Digital Temperature Sensor	$15.99
10 Pcs Black Cap SPST Momentary Mini Push Button Switch	$7.99
Adafruit NFC/RFID PN532 Breakout Board	$39.95
Breadboard-friendly 2.1mm DC barrel jack	$0.95
Arcade Button Quick-Connect Wire Pairs	$4.95
FTDI Friend	$14.95
ESP32-CAM	$9.50
Espressif Systems ESP32-WROOM-32D	$5.40
Youngneer 5v Relay Board	$2.20
Assorted Resistors, capacitors, Jumper Wires	$25.00
DFRobot SEN0127 Analog Gas Sensor MQ2	$6.90
Total Cost	**196.73**

BP requires the system to be applied to both their front and back door, which requires us to double the parts of our system, bringing the net total cost including labor costs to be **$84393.46**. The price may change depending on the strength of the lock we wish to use, building our own voltage regulator, and other specific hardware changes. The cost does not include any costs for Azure database hosting.

6 Conclusion

6.1 Accomplishments

We were able to successful meet all of our requirements that we had set for our project (see Appendix A for breakdown and verifications). All three methods of authentications were able to be checked and provide a signal when properly authenticated. The door was able to send the relay a signal if two factors were met and the relay was able to unlock the door. The emergency exit subsystem is able to accurately detect fires, accurately reject fake fires, and override the authentication subsystem.

6.2 Uncertainties

Some uncertainties that we would face if we were to continue development of our project include how well the system will be integrated if the power supply functions correctly. If we can deliver enough current to the ESP32 at 3.3V, then it may be possible to fully integrate the system. Another uncertainty is the ease of getting multiple access points to function correctly. Something that may be difficult is processing multiple camera inputs and making sure we send the authentication signal to the correct ESP32.

6.3 Ethical Considerations

One of the main concerns inherent in this project is the use of facial recognition. In regards to the ACM Code of Ethics, we are seeking to respect privacy and honor confidentiality [6]. Our design met these specifications by removing the need to retain user face data in our system with the switch to Microsoft's Face API. This also makes our project compliant with the Biometric Information Privacy Act (BIPA), since biometric identifiers are no longer stored [10]. Our database securely stores only NFC Tag Reader data by hashing the NFC Tag of each user before storing it inside of the database, preventing attacks on the NFC module.

6.4 Future Work

Some future work involves being able to get the complete integration of our system all together. This requires three processing units for absolute parallel processing and three different power supplies for the correct power necessities. As mentioned earlier, BP wishes to expand this system to offices that have multiple doors, which would require multiple copies of the system as well as changes to logging methods to ensure that the proper door is tracked. To increase the security capabilities of the Facial Recognition Module, the challenge response could include multiple different challenges, indicating to the user which challenge to perform through a speaker output. This would further advance the security aspects of the door

References

[1] S. Yoneda, S. Tanimoto, T. Konosu, H. Sato and A. Kanai, "Risk Assessment in Cyber-Physical System in Office Environment," 2015 18th International Conference on Network-Based Information Systems, Taipei, Taiwan, 2015, pp. 412-417, doi: 10.1109/NBiS.2015.63.

[2] C. Wilson, "Biometric Accuracy Standards," Information Security and Privacy Advisory Board 2003

[3] "Creating a Resistor Based Keypad & Interface With Arduino!" [Online]. Available: https://www.instructables.com/Creating-A-Resistor-Based-Keypad-Interface-With-Ar/ [Accessed: 29-Mar-2021].

[4] "Arduino - Electromagnetic Lock" [Online]. Available: https://arduinogetstarted.com/tutorials/arduino-electromagnetic-lock/ [Accessed: 29-Mar-2021].

[5] P Gomes, P Santana and J Barata, "A Vision-based Approach to Fire Detection" International Journal of Advanced Robotic Systems Portugal 2014

[6] "ACM Code of Ethics and Professional Conduct," Code of Ethics. [Online]. Available: https://www.acm.org/code-of-ethics. [Accessed: 19-Feb-2021].

[7] "ESP32 DS18B20 Temperature Sensor with Arduino IDE (Single, Multiple, Web Server)" [Online]. Available: https://randomnerdtutorials.com/esp32-ds18b20-temperature-arduino-ide/ [Accessed: 19-Feb-2021].

[8] J. Riyaz, "How to Connect MQ2 Gas Sensor to Arduino" [Online]. Available https://create.arduino.cc/projecthub/Junezriyaz/how-to-connect-mq2-gas-sensor-to-arduino-f6a456

[9] N. Memon, "How Biometric Authentication Poses New Challenges to Our Security and Privacy [In the Spotlight]," in IEEE Signal Processing Magazine, vol. 34, no. 4, pp. 196-194, July 2017, doi: 10.1109/MSP.2017.2697179.

[10] Biometric Information Privacy Act. 2008.

Appendix A Requirement and Verification Table

Table 1: System Requirements and Verifications

Requirement	Verification	Verification status (Y or N)
Power Supply Requirements 1. Capable of outputting voltage between 3.3 and 12 Volts to components after receiving 24 volts from power supply.	**Verification** 1. While the power source is plugged in, measure all of the voltage values in the system with a voltmeter to ensure that the voltage regulators are providing each component with the correct amount of voltage to operate.	Y
Central Module Requirements 1. Must be able to receive data from all components of the authentication module to generate a signal to unlock the door. 2. This module should receive signals from the emergency exit module to generate a signal to unlock the door. 3. The central module should be able to send and receive data to the Database for authentication checks to be able to accurately unlock the door.	**Verification** 1. Central Module and Authentication Verification (a) Receive keypad presses to store the entry pin, and compare this with the authenticated pin. On success, one of the factors should be authenticated. (b) Receive image data from the ESP32-CAM and transport this to the Microsoft Face API. Receive the proper authentication signal. On success, one of the factors should be authenticated. (c) Receive NFC Tag Reader data from the users NFC tag. Send this data to the database subsystem to compare to the users stored NFC value. On success, one of the factors should be authenticated. 2. In case of an emergency, receive simulated data from the emergency exit circuit components and unlock the door. 3. Central Module and Database/Locking Verification (a) Once two factors are authenticated, generate a signal to unlock the door. (b) If two factors are not met, generate a signal to lock the door.	1. Y 2. Y 3. Y
Continued on next page		

Table 1 – continued from previous page

Requirement	Verification	Verification status (Y or N)
Authentication Module 1. This module should allow for all 3 methods of authentication to be accessible simultaneously and should be able to individually provide data for any combination of authentication.	**Verification** 1. Attempt to authenticate with keypad. Enter the 6 digit pin and send to the central module. 2. Attempt to authenticate with NFC Tag Reader. Hold your phone/blank white card to the tag reader. Send this value to the central module to authenticate 3. Attempt to unlock the door with facial recognition. On motion sensor detection, the camera should wait for a face to appear. Look at camera, and also perform the challenge response. Send these images to central module/database module. Confirm it recognizes you. 4. Check if door unlocks when any two authentication methods are provided properly, and otherwise remains closed	1. Y 2. Y 3. Y
Database Subsystem 1. This module should securely hold information for each user's NFC Tag in the database, compare this data to received data from the microcontroller, and send back a success or failed signal to the microcontroller.	**Verification** 1. Attempt an access with an individual in the system. Provide correct data for this individual, and confirm database can find you and authenticates you. 2. Attempt an access with an individual not in the system. Door should remain locked no matter which two authentication methods are provided, since user won't be found.	Y
Access Subsystem 1. This module should be able to withstand force applied to the door when the door is locked. 2. This module should be able to open properly once the central subsystem sends a signal to unlock the door. 3. This module should also use temperature and gas sensors signals sent by the ESP32 to unlock the door in case of an emergency.	**Verification** 1. Try to open the door before authentication. The door should remain locked. 2. Try to open the door after authentication. The door should open. 3. Using simulated data, simulate a fire and gas concentration change. Have the ESP32 automatically send the unlock signal and the door should open.	1. Y 2. Y 3. Y

Appendix B Final Schematics

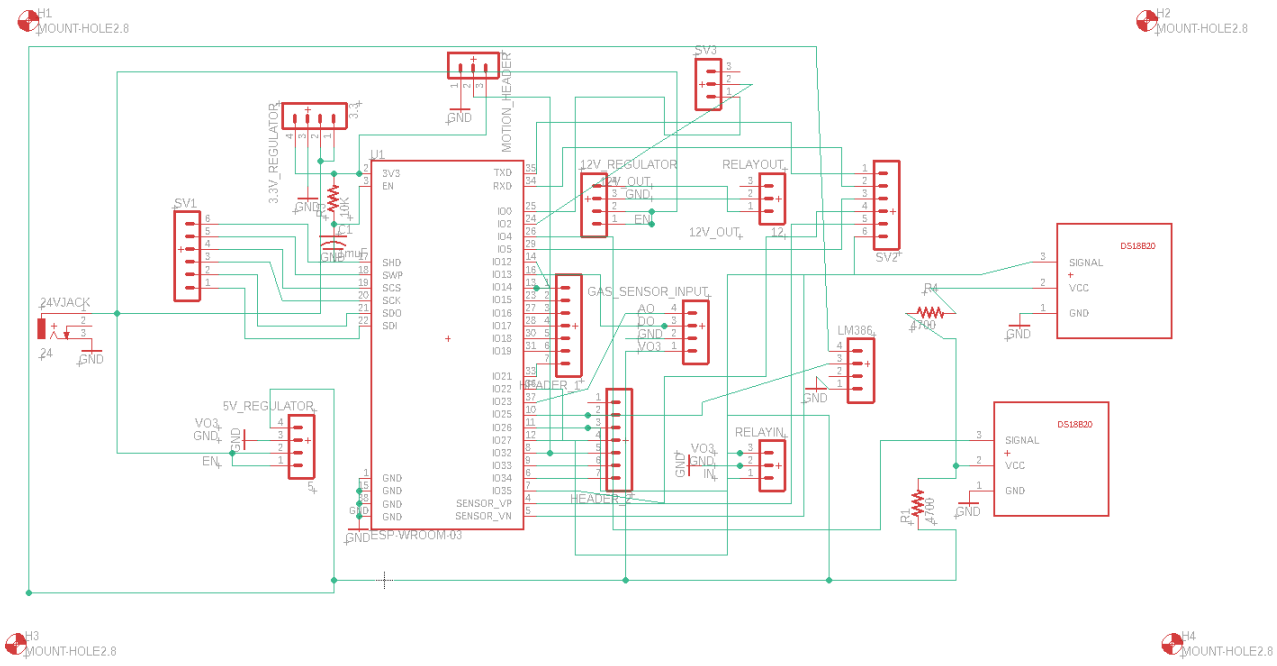

Figure 15: The final schematic design of the main PCB.

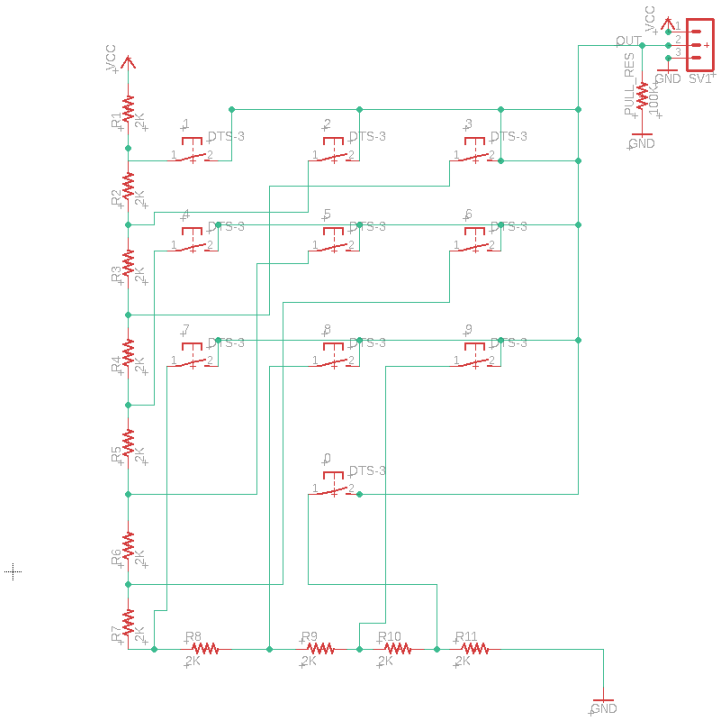

Figure 16: The final schematic design of the keypad PCB.

Appendix C Final PCB Layout

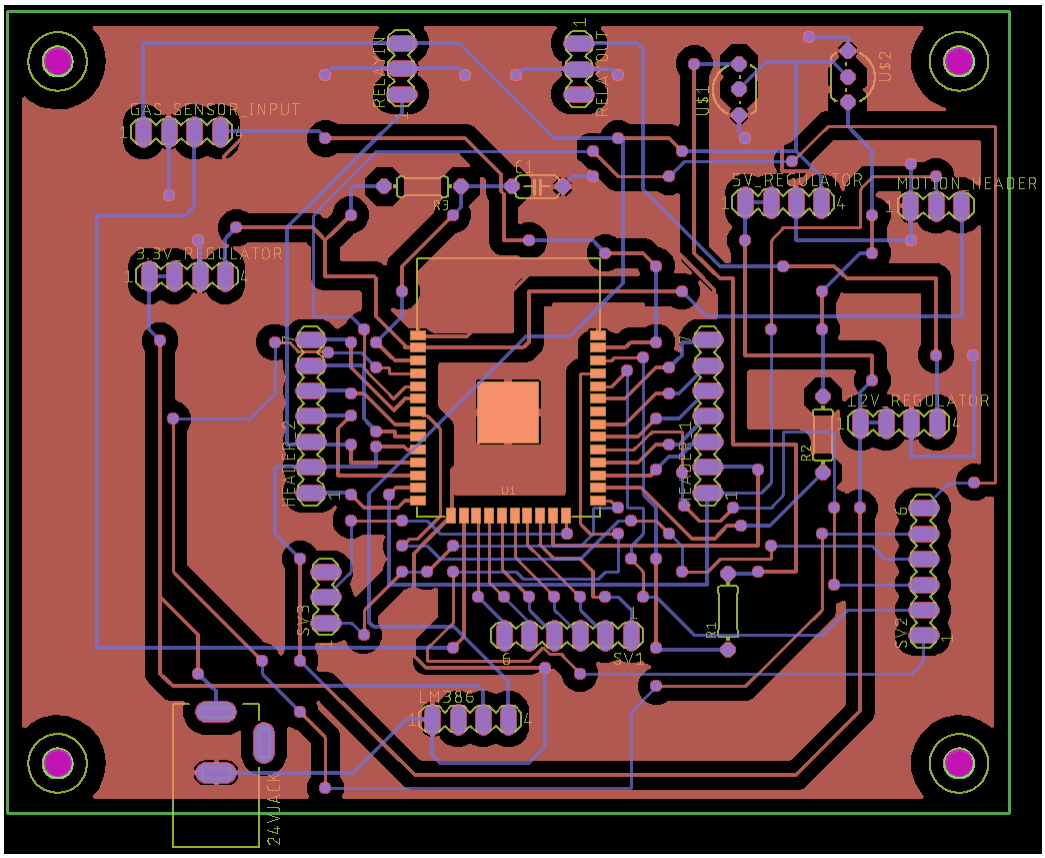

Figure 17: The final PCB design