Office Access Control System

By

Shariar Alamgir (alamgir2)

Thomas Ng (thomasn3)

Vincent Nguyen (vn4)

Design Document for ECE 445, Senior Design, Spring 2021

TA: Anand Sunderrajan

March 4, 2021

Project No. 27

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 a rate of 95% of the time at least, 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. [3].
- The response time is less than 2 seconds from authentication to door unlocking. 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.

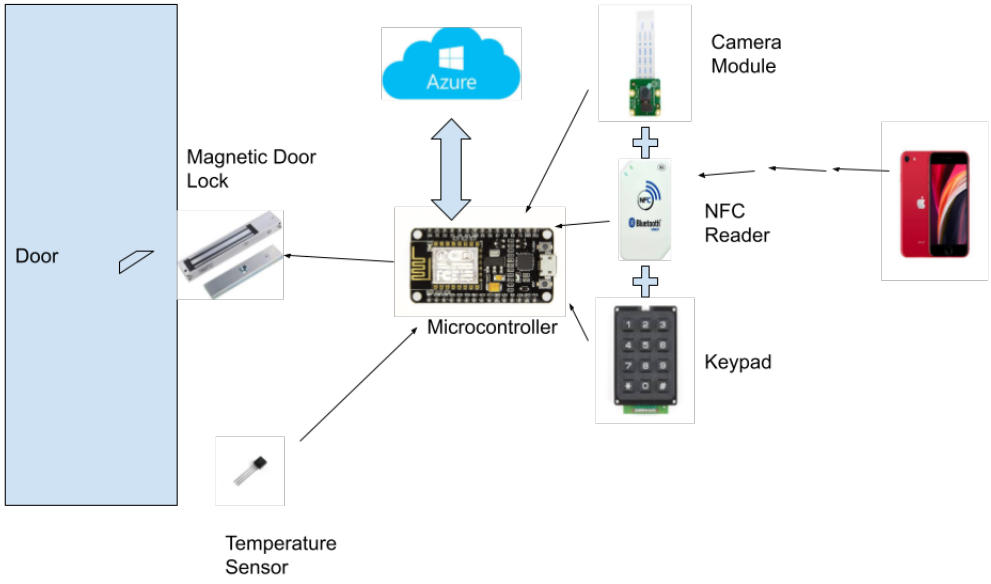

Figure 1: Physical design for Office Access Control System.

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.

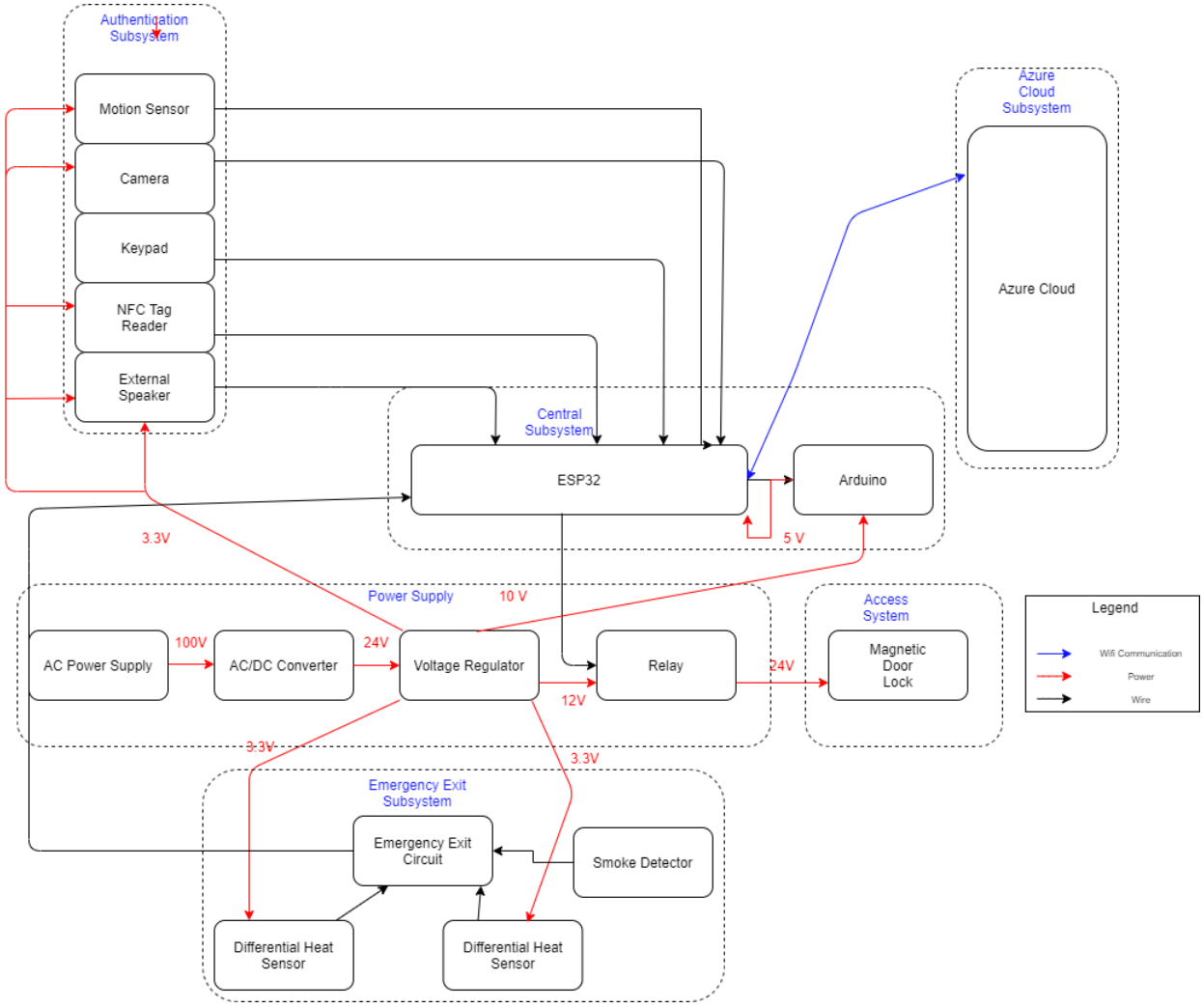

Figure 2: Block diagram for Office Access Control System. Components are divided into their subcategories based on their operation.

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 and Arduino software module.

2.1.1 ESP32 Microcontroller

The ESP32 Microcontroller is integral to the authentication and access steps of the system, as well as maintaining communication with the Azure cloud database. 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. To keep the user data secured, ESP32 will perform a hash operation on the inputted data, and use this data to confirm that the information is valid for a single user in the Azure Cloud 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

Requirements	Verification
1. Must output software results to relay in under 2 seconds	1. Begin with locked door 2. Perform Authentication check once microcontroller receives two factors of authentication. Begin a timer 3. On success, send a low signal to relay, stop timer. Ensure it is under 2 seconds
2. Must send packets with Azure IoT Hub at 7 Mbps	1. Create a 7 Mb packet 2. Perform a POST request to Azure Hub, begin timer 3. Perform a GET request for the same packet, ensure packet matches, end timer. Confirm that the operation finished in 1 second or less.
3. Must operate between 2.5-3.6V with an average of 80 mA	1.Connect microcontroller with resistor in series 2. Measure voltage drop across microcontroller and current through multimeter.

2.1.2 Arduino Uno

The Arduino Uno will program the software logic needed for the ESP32 to communicate with the components of the project.

Requirements	Verification
1. Must operate at 5 Volt given 7-12 V input	1. Apply power from voltage regulator to Arduino. 2. Use 5 Volt output pin and pass through a resistor. 3. Use a multimeter to check voltage drop for 5 voltage approximation.

2.2 Authentication Subsystem

The authentication subsystem is built by components necessary for our three factors of authentication: the NFC Tag Reader for cell phone proximity, the 9-digit Keypad for PIN access, and the Facial Recognition subsystem. All of these subsystems have a similar requirement, along with unique ones for their specific operation and design. 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 both factors of authentication at once if they wish to, or do them one at a time.

2.2.1 Keypad

Built directly on the PCB, the keypad is used for PIN access authentication. The pin is used for unlocking the door from both the inside and outside. The entered PIN is sent to the ESP32 that will validate the PIN in the database.

Requirements	Verification
1. Must be able to debounce each keypress in 100ms	1. Press and release '1' key and take in input. 2. In Arduino Loop, begin a timer. 3. Initialize counter to 0. This will count how many times the button was "pressed". 4. Begin checking debounce condition, by determining if signal has changed from low to high after a time larger than the debounce delay. If so, increment counter. 5. Once signal is low again for a given amount of time (debouncing time), stop the timer. Check that the counter value is equal to 1. If counter is 1 and timer is under 100ms, debouncing was handled in under 100 ms properly.

2.2.2 NFC Tag Reader

The NFC Tag reader is responsible for the cell phone proximity method of authentication. An NFC Reader is preferred over RFID since it requires the cell phone to be placed much closer to the door, so as to avoid false reading from nearby cell phones. The Tag Reader will read the NFC Tag from a phone, and send it to the ESP32, which will use it to validate the cell phone being linked to a user in the database.

Requirements	Verification
1. Must operate between 3-5 mA and consume 3.3V	1. Place phone within range of NFC tag reader to begin reading results and sending to microcontroller. 2. Measure voltage using voltmeter, confirm 3.3V drop. 3. Measure current using ammeter, confirm 3-5mA current passing through element.

2.2.3 ESP32 Camera Module

The camera module will be used for two key functions of our access system. The first function is to gather the images required to perform facial recognition. This will include a regular image of the persons face, which will be used for texture analysis, and will also record the challenge response given to the user. This information will be then sent directly to the ESP32 microcontroller for validating the facial recognition. The camera must also be used to count the number of individuals that will be entering the room.

Requirements	Verification
1. Continuously capture images and send to microcontroller at 4 frames per second	1. Begin a timer. 2. Initialize packet counter to 0. 3. Receive frame packets on microcontrller from camera and increment counter. 4. Once timer reaches 10 seconds, stop incrementing counter on frame arrival. 5. Check that the counter value is greater than or equal to 10, indicating 4 frames per second sending rate.
2. Must operate between 3.3-5V and 20-70 mA	1. Connect with Arduino power supply or DC power supply 2. Connect with resistor connected to ground, and pass voltage through camera 3. Measure voltage and current with multimeter.

2.2.4 External Speakers

The output speaker is used for the second portion of authentication during facial recognition. This will be used to inform the user to perform a challenge response to ensure that an actual human being is presented in front of the camera, not an image. This speaker will output text generated in the Arduino Interface, which can be many different variations of face poses.

Requirements	Verification
1. Must output 3 Watts of Power.	1. Connect with Arduino power supply or DC power supply 2. Supply with at least 5 volts from power 3. Measure voltage with multimeter. Internal resistance is 8 ohms, so a drop of 5 volts will give at least 3 ohms of power.

2.2.5 Motion Sensor

To keep the privacy of employees, the camera will only be active when the motion sensor detects an individual walking near the door and standing in front of it.

Requirements	Verification
1. Must run on at least 3 volts of power.	1. Connect with DC power supply 2. Pass through 3 volts of power 3. Check for operation of motion sensor by walking in front of it. System must be able to detect motion on Arduino.

2.3 Azure Cloud Subsystem

The BP Spark user information is held in a Microsoft Azure Cloud database. The information held must not reveal any personal information about the user, other than a given username. This database will also hold images for facial recognition, hashed PIN values, as well as hashed NFC Tag values.

2.3.1 Azure IoT Hub

While not a part of our development, the Azure IoT hub is the communication endpoint for receiving and sending data from our central control system. It is responsible for being able to rapidly send and receive data securely to minimize the wait time between authentication and the door unlocking. The IoT Hub communicates with the NodeMCU ESP32 to receive information from the camera module for facial recognition and to receive data about authentication values and access logs. It also sends data about valid authentication.

Requirements	Verification
1. Must send HTTP Response in under 1 second.	1. Begin a timer 2. Perform a GET request from the microcontroller for a log of the most recent entry. 3. Once response is received, end timer. Ensure the time is under 1 second.

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.

2.4.1 Differential Temperature Sensor

Two sensors will be used to compute the differential temperature inside and outside the room. This will be used to determine if a fire occurred within the room. This is crucial for emergency exit capabilities so that our door does not lock individuals inside the room. The sensors will be sent to an Analog-to-Digital converter that the microcontroller can interpret for emergency situations.

Requirements	Verification
1. Must detect temperature difference of 150 degrees Fahrenheit and inform microcontroller.	1. Check current temperature readings in Arduino 2. Hold a lighter or match around the temperature sensor. 3. Read temperature differences from the sensors. 4. Once temperature difference is at 150 degrees, the microcontroller will send an active LOW to the relay, unlocking the door.
2. Must operate at 3.2-5.25 volts of DC power and 2 mA of current.	1. Connect with Arduino power supply or DC power supply. 2. Supply with 3.2-5.25 volts from power 3. Measure voltage with multimeter. Check for proper operation by receiving temperature difference.

2.4.2 MQ2 Gas Sensor

To improve the accuracy of our fire detection system, a gas sensor will be installed within the office will also be connected to the emergency subsystem to ensure the microcontroller makes a proper decision on

unlocking the door automatically.

Requirements	Verification
1. Must operate at 4.9-5.1 volts of DC power	1. Connect with DC power supply from regulator. 2. Supply with approximately 5 volts of power 3. Check that gas can be detected by creating gas via a lit piece of paper.

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 via the microcontroller.

2.5.1 AC Power Supply

Our AC Power supply is passed through a voltage regulator to provide the subcomponents of our system with the proper amount of power. Notably, the system must be able to ensure the temperature sensors and the magnetic door lock is always being powered since those are used at all points of time, whereas the pieces of the access control system that are not always used such as the NFC Tag Reader only need power when triggered for a new entry.

Requirements	Verification
1. Must be able to source between 100-240 V before going into DC Converter.	1. Connect power supply to wall port 2. Pass through DC Converter 3. Confirm that DC Converter can output 24 Volts by checking voltage drop through resistor connected with DC Converter and Ground.

2.5.2 AC/DC Converter

To utilize the power from the power supply, an AC/DC converter is used to get digital voltage to our other components.

Requirements	Verification
1. Must convert AC input into 24V DC output.	1. Plug AC Supply into DC converter. AC supply must be 100-240V. 2. Take DC output and pass through resistor and into ground. 3. Measure voltage drop. Confirm it is 24 Volts.

2.5.3 Voltage Regulator

The voltage regulator is critical to maintain the proper voltage requirements of our system. Different components will require a different voltage value, but all are powered via the same AC Power supply, and the voltage regulator must ensure that voltage is applied properly.

Requirements	Verification
1. Must be able to properly output voltages of 3.3-12V for respective components.	1. Connect DC output to voltage regulator for various voltage readings. 2. Take regulator output and pass through resistor and into ground. 3. Measure voltage drop. Confirm it is equivalent to voltage regulator pin used. Must satisfy range of 3.3 and 12 volts.

2.5.4 Relay

Since the ESP32 microcontroller is not strong enough to provide power to lock the door, an intermediate relay is placed to generate high enough voltages so the door can remained locked. The relay will switch to low once authentication is successful.

Requirements	Verification
1. Must be able to source 12V to magnetic door lock.	1. Send HIGH signal to Relay from microcontroller. 2. Connect 12V voltage regulator output to relay. 3. Connect relay output to magnetic door lock. 4. Check that door is locked.

2.6 Access Subsystem

2.6.1 Magnetic Door Lock

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.

Requirements	**Verification**
1. Must be able to resist 100 lbs of force applied to door when locked.	1. Send HIGH signal to Relay from microcontroller and power on magnetic door lock. 2. Attach a spring to the side of the lock that separates from the plate. Attach a force sensor/reader to spring 3. Apply up to 100 lbs of force to spring. Lock must be attached together.

3 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. We will use a scheduling algorithm to split up CPU time spent on the camera stream, NFC verification, and keypad verification. We can measure the performance of our scheduler through criteria such as CPU utilization, throughput, waiting time, and response time.

A form of scheduling is round robin, where the CPU will cycle through each process and divert an equal amount of time and resources to each process. In essence, the ESP32 will spend a third of the time running the video streaming code, a third of the time running the NFC reader code and a third processing the keypad input. One downside to this approach is that it will increase the latency of the camera streaming video to our Azure server, as well as lower the framerate of the video. The NFC reader is not always active and neither is the keypad, so there are wasted CPU cycles. The benefits of round-robin scheduling are that it is the easiest to implement and that it is the most fair.

Another form of scheduling is priority scheduling, where all processes are given a priority, and the scheduler runs the highest priority task until it stops or blocks. This form of scheduling will benefit the task that handles the video streaming, the CPU will not have to switch tasks as often, but the other two tasks are subject to starvation. The upside to this is that we can choose which task to prioritize, so for the video streaming task, the latency would decrease and the frame rate would increase in comparison to its performance with round robin scheduling.

An alternative approach to the scheduler is to just let the video streaming task run all the time and to use interrupts for when the NFC reader or keypad are used. This allows for maximum frame rate and for lowest latency. The upside is that there are little to no wasted CPU cycles and that our video streaming task will be very smooth. A potential downside is that configuring the interrupt handlers for the NFC reader and keypad may be a bit difficult.

To maximize CPU utilization however, we can run different tasks on each core of the CPU. The first core can always run the video streaming task, while the second can constantly switch between waiting for input for either the NFC tag reader or the keypad. There will be 100 percent CPU utilization with very little waiting time for the tag reader and keypad tasks.

4 Cost and Schedule

4.1 Cost Analysis

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 5v Regulator Module	$12.99
Fuzadel Electromagnetic Lock 12v	$24.98
Zulkit Project Box	$11.99
DZS Elec 2pcs LM386 Audio Amplifier Module	$6.99
GAOHOU 2 PCS DS18B20 Waterproof Digital Temperature Sensor	$15.99
10 Pcs Black Cap SPST Momentary Mini Push Button Switch	$7.99
CQRobot Speaker 3 Watt 8 Ohm	$7.99
FTCBlock NFC/RFID Reader PN532 kit	$27.99
Grove I2C 4 Ch / 16 Bit Analog to Digital Converter	$16.95
Espressif Systems ESP32-S2-WROVER	$2.20
Youngneer 5v Relay Board	$2.20
Assorted Resistors, capacitors, and IC chips	$10.00
Arducam Mini Module Camera Shield with OV2640 2 Megapixels Lens	$25.99
DFRobot SEN0127 Analog Gas Sensor MQ2	$6.90
Total Cost	**205.83**

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 $84425.46. 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.

4.2 Schedule

Week	Shariar Alamgir	Thomas Ng	Vincent Nguyen
3/8/21	Create PCB design	Work on testing camera with ESP32	Work on testing camera with ESP32
3/15/21	Get NFC Tag reader connected, review PCB design	Set up database to store user data and help with facial recognition	Work on getting first facial recognition algorithm working
3/22/21	Version 2 of PCB	Integrate motion sensor with facial recognition system	Work on eye blink integration with facial recognition algorithm
3/29/21	Make 10 digit keypad and final version of PCB	Test stream of data and sending/receiving of data to/from database	Work on challenge response
4/5/21	Stress test NFC tag reader and keypad	Work on challenge response	Work on challenge response
4/12/21	Integrate keypad and NFC tag reader with rest of system	Test accuracy and speed of facial recognition system	Test accuracy and speed of facial recognition system
4/19/21	Integrate heat sensor and smoke detector	Make connection with database secure	Schedule processes on ESP32
4/26/21	Make emergency protocol for heat sensor and smoke detector	Test parallelism of all factors of authentication running at same time	Test parallelism of all factors of authentication running at same time
5/3/21	Prepare final presentation and write final report	Prepare final presentation and write final report	Prepare final presentation and write final report

5 Safety and Ethics

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 [4]. In order to achieve this we are designing our database of access logs as simple as possible. We will store only information that is necessary to gain access to the BP Spark office but not any incriminating or private information. We are also designing our database such that only trusted individuals will have access to it. The usage of facial recognition gives companies unprecedented access to personal information. Techniques to overcome misuse of facial recognition technology include signal processing techniques such as fuzzy hash, fuzzy vault, and secure sketch [5]. In our use of facial recognition, we will employ a one-way hash, meaning that when our system scans the face of a person, our system will hash the input data in a way such that it is impossible to generate the original input data from the hashed data. This will ensure that any malignant actors will be unable to retrieve personal information from the database that contains our access logs.

As for state regulations in Illinois, our project must be compliant with the Biometric Information Privacy Act (BIPA). It essentially states that entities which use facial recognition technology must ensure that they obtain consent from individuals subject to the facial recognition technology, that the biometric identifiers destroyed in a timely manner, and that these biometric identifiers are safely stored [6]. The first part of the requirements is out of our control, but our technique of one-way hashing will ensure that the biometric identifiers are not even stored into our database, but rather a hash of them.

Another potential safety concern is that of the BP Spark office itself. Our project will not be able to improve the physical security of the doors themselves, since they can be broken and are not bulletproof. We aim to fix this issue by having our Azure IoT hub check for OK flags from our microcontroller when the camera has logged an entry. If no OK flag has been sent, then our microcontroller can contact BP security.

6 References

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

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

[5] 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.

[6] Biometric Information Privacy Act. 2008.