Office Access Control System

By

Shariar Alamgir

Thomas Ng

Vincent Nguyen

Project Proposal for ECE 445, Senior Design, Spring 2021

TA: Anand Sunderrajan

February 15, 2021

Project No. 27

Contents

1 Introduction

1.1 Objective

BP is in need of a more secure way to give office access to employees. The current BP Spark office can only be accessed by one of two people with the key. If one of these employees is not in the office, it cannot be accessed. Due to this, the main entrance is typically left unlocked once one of these employees are in the office posing a security threat.

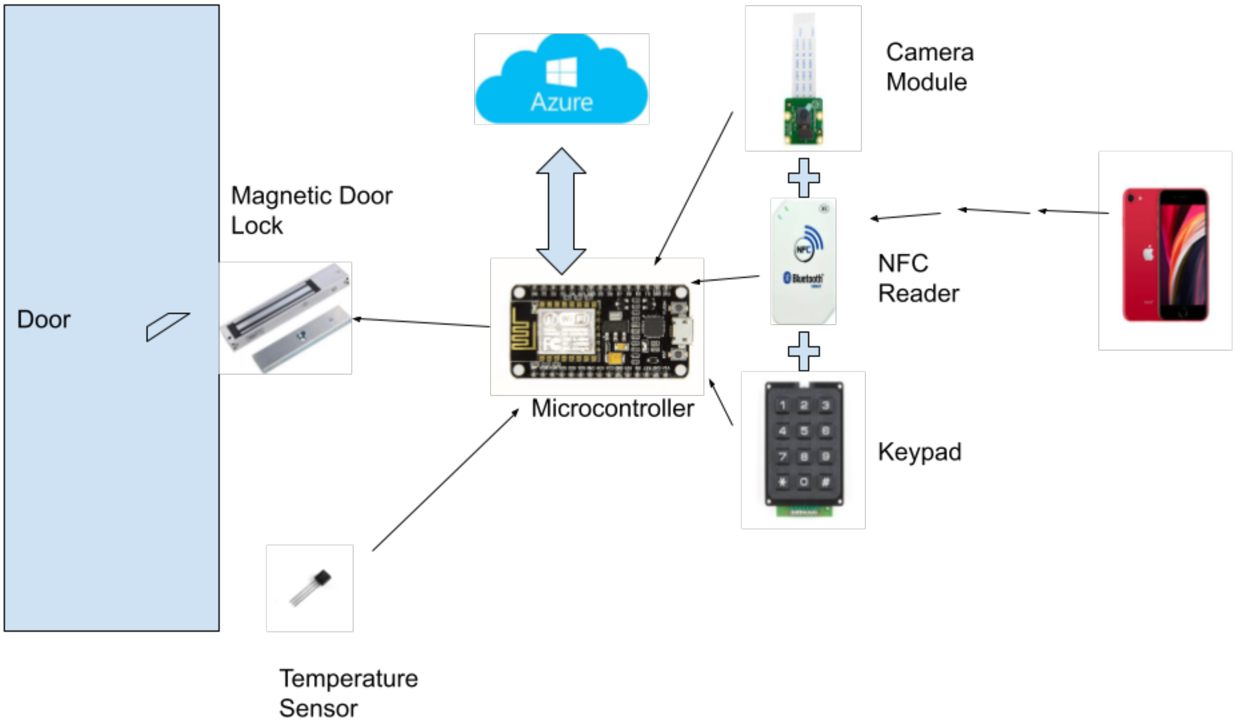
To solve this problem, we will integrate a two-factor authentication system for access into a room, attached to the entry point of the room. The door will require people to validate themselves via two out of three forms of identification: Cell Phone Proximity, Facial Recognition, and Pin Access. This will ensure more secure entry to the office as it will validate a person using something they have, something they know, 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 trying to create more secure offices as security breaches have sparked. Security risk can be 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. It poses a security risk if someone loses the key because someone else 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 could be replaced with this system.

1.3 Physical Design

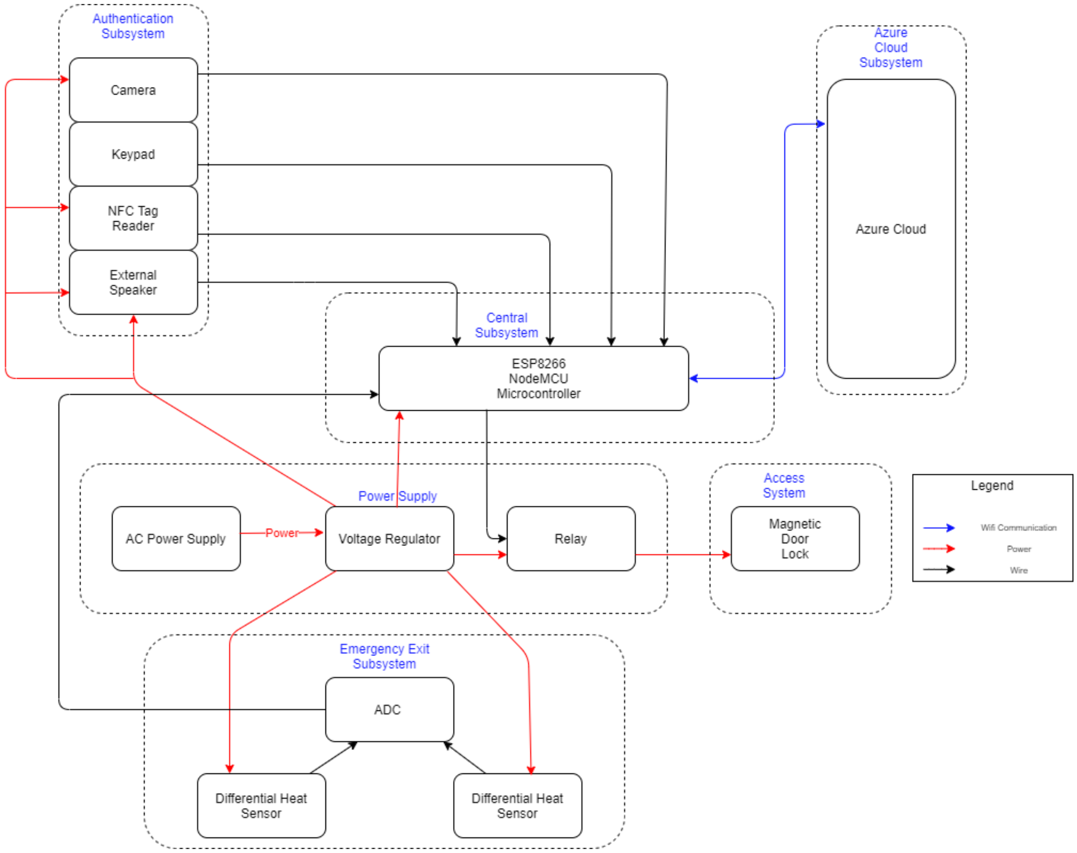


1.4 High Level Requirements

- Authentication is accurate at a rate of 95% of the time at least. False non-match rate of 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.
- 95% rate of successfully identifying a fire. A research paper was able to achieve 93.1% using only computer vision, so by combining computer vision with differential temperature sensors [3].
- Response time of less than 2 seconds from authentication to door unlocking. We chose less than two seconds because the main bottleneck will be the facial recognition component and its communication to the azure database.

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 NodeMCU ESP8266 development board and the Arduino interface. User information for who can and has accessed the office will be 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 the door to be unlocked immediately. A power supply that can output between 3.3V and 12V during open office hours must be incorporated to keep the door locked and allow for authentication when prompted.



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 ESP8266 Microcontroller and Arduino software module.

2.1.1 NodeMCU ESP8266 Development Board

The NodeMCU ESP8266 Development Board is integral to the authentication and access steps of the system, as well as maintaining communication with the Azure cloud database. The NodeMCU ESP8266 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, NodeMCU ESP8266 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 NodeMCU ESP8266 and the development board will be programmed using the Arduino IDE for software operations

Requirement 1: Must output software results to relay in under 2 second
Requirement 2: Must be able to perform GET and POST HTTP requests with Azure IoT Hub at 7 Mbps

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.

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 will be sent to the ESP8266 that will validate the PIN in the database.

Requirement 1: Must be easy to press
Requirement 2: Must work in parallel with NFC Tag Reader and Facial Recognition camera

2.2.2 NFC Tag Reader

The NFC Tag reader will be 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 ESP8266, which will use it to validate the cell phone being linked to a user in the database.

Requirement 1: Must work in parallel with Keypad and Facial Recognition camera
Requirement 2: Must operate at 3-5 mA and 3.3V

2.2.3 ESP8266 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 ESP8266 microcontroller for validating the facial recognition. The camera must also be used to count the number of individuals that will be entering the room.

Requirement 1: Must work in parallel with NFC Tag Reader and Facial Recognition camera
Requirement 2: Must continuously capture clear images and capture face changes for challenge response

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.

Requirement: Must be able to output speech from written text for challenge response

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 apart 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 ESP8266 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.

Requirement: Must send HTTP Response in under 1 sec

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 ESP8266 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.

Requirement: Must be able to detect temperature rise of 200 degrees in the office

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 will be 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 aren't always used such as the NFC Tag Reader only need power when triggered for a new entry.

Requirement: Must be able to source at least 12 V for largest components

2.5.2 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 will all be powered via the same AC Power supply, and the voltage regulator must ensure that voltage is applied properly.

Requirement: Must be able to properly output voltages of 3.3-12V for respective components

2.5.3 Relay

Since the NodeMCU 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

Requirement: Must be able to source 12V to magnetic door lock

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 remained power on until a user has been authenticated, at which the voltage provided to the door will go to 0. This lock will be powered after 5 seconds of being opened, locking the door once it is closed.

Requirement: Must be able to source 12V from relay to stay locked

3 Safety and Ethics

One of the main concerns regarding 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 to be as simple as possible. We will store only information that is needed 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 a person's face is scanned, 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.

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.