# Voice Coded Lock

ECE 445 Team #62 Project Proposal

Aman Thombre
Logan Greuel

TA: Zicheng Ma
03/03/2023

# 1 Introduction

## 1.1 Problem

Currently, accessing secure areas usually requires some type of access card or keys. These can easily be misplaced or left at home, leading to being locked out of your area of work Additionally, solutions such as access cards have been known to have security vulnerabilities, exposing government buildings, schools, factories, and companies [1]. These security flaws are a big risk, as according to the FBI, there were over 340,000 burglaries of nonresidence properties in 2019, with an average value of $8781 being stolen [2].

Using access cards or key locks can also be hard to operate with your hands full; trying to get an iCard out while accessing a lab in the ECEB while holding a laptop and FPGA can be quite difficult. Other keyless options requiring physical contact, such as a keypad, may also pose a health concern for some users, especially during cold/flu seasons or a pandemic. These issues show a need for a new form of keyless, contactless entry to secure areas.

## 1.2 Solution

Our proposed solution is to implement an audio-based locking system for a door. We plan to create an attachment on or near a door which will listen for a user's voice, and upon hearing a user saying some keyphrase, the device will automatically unlock the door. This system will use keyphrase recognition to identify an audio password, allowing for hands free operation of a lock. Keyphrase recognition will be used to verify that the user has access, as only verified users should know the password for the locking system.

This solution eliminates the need for any physical component used to gain access, as only the spoken password is required. The key will only be used as a backup in the event of power failure (so entry would still be possible). This will allow for hands-free operation of the lock, and help reduce the risk of stolen, misplaced, or copied access cards and keys. This solution is intended more for access points with many authorized users rather than for private homes; our solution allows for multiple users to gain access to an area using a single, shared audio password.

## 1.3 Visual Aid

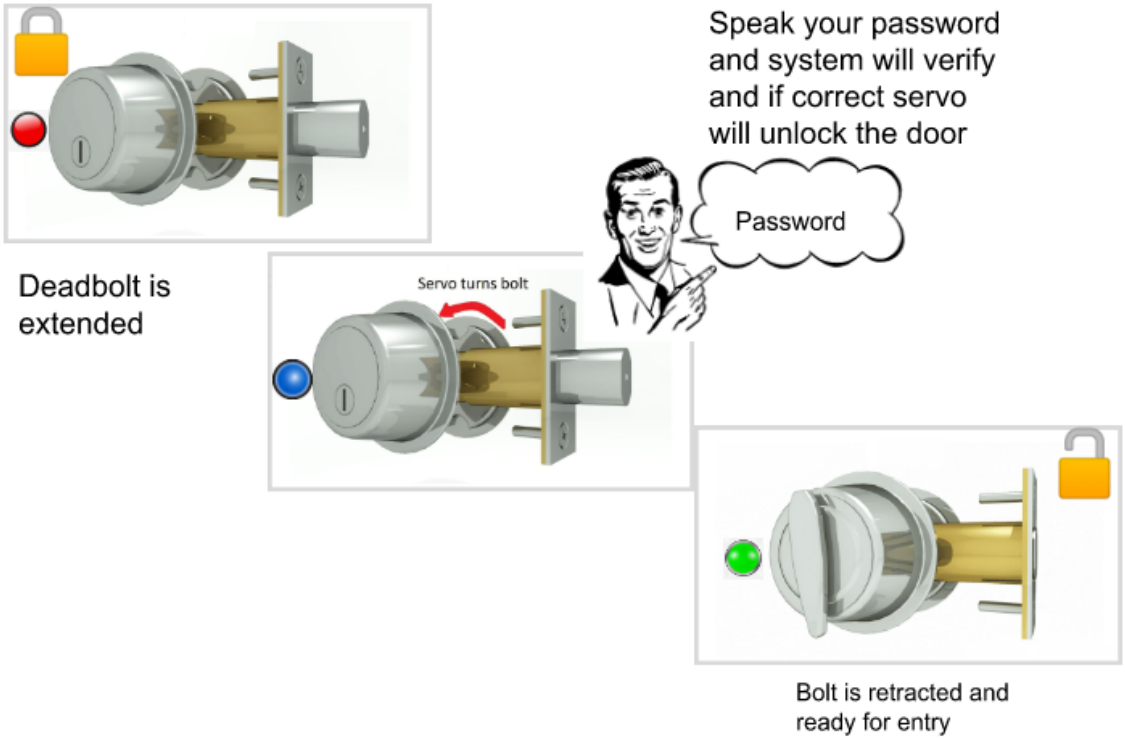


Figure 1: Visual Aid

## 1.4 High Level Requirements

1. Keyphrase recognition should be able to consistently correctly classify audio password as correct/incorrect.
2. Operation of the locking system, from time of saying password to unlocking should be performed in reasonable time (<8 sec).
3. System should be able to operate a door lock automatically.

# 2 Design

## 2.1 Block Diagram

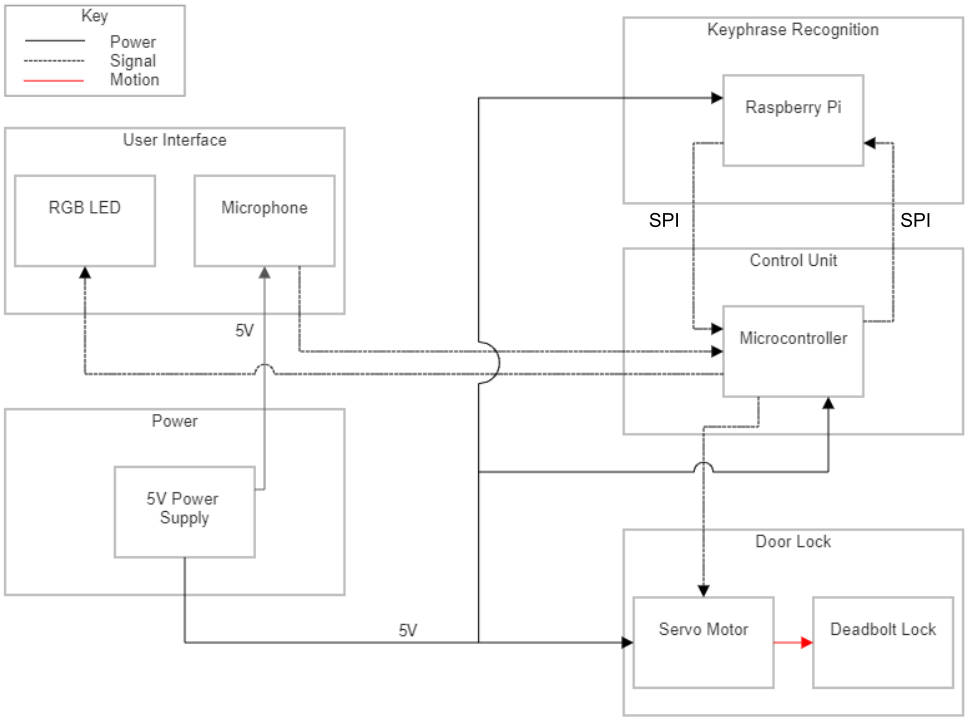


Figure 2: Block Diagram

## 2.2 Block Descriptions

### 2.2.1 User Interface

Includes microphone for user input and LED for system status. The user will interact with our locking system through a microphone and LEDs. Keyphrases will be listened for using a microphone, which will send the audio signal it records in real time to our raspberry pi. An RGB LED will be used to signal to the user the state of the locking system - we plan to use different colors to indicate locked, unlocked, and listening.

Microphone

- The microphone will record user input, and send data to the raspberry pi.
- *Requirements:* The microphone must accurately record users speaking at a reasonable volume into the microphone and transfer that signal to the keyphrase recognition subsystem.

RGB LED

- The RGB LED will display a different color for each status of the lock (locked, unlocked, listening).
- *Requirements:* The LED must be able to display at least three colors, depending on inputs given and have forward voltage of 2-4.5V [4] .

### 2.2.2 Keyphrase Recognition

Consists of Raspberry Pi Zero, which will perform keyphrase recognition software. We plan to code this software in Python, and use some machine learning model (determined by which models give us best results in testing) to determine whether a given keyphrase is correct or incorrect. Current plans for models include hidden Markov Models and convolutional neural nets. Signals will be fed from the Raspberry Pi to the microcontroller, signaling whether the keyphrase heard was correct or incorrect.

Raspberry Pi Zero

- Will perform keyphrase recognition based on inputs given from microcontroller.
- Will send a signal to the microcontroller if the audio password was recognized.
- *Requirements*: Software must be able to consistently distinguish correct/incorrect keyphrases from one another with >80% accuracy, which is around what is achieved using probabilistic models [5]. Must be able to provide 3.3V at GPIO pins [6].

### 2.2.3 Door Lock

Consist of a servo motor mounted on a deadbolt style door lock. Lock should still be accessible with a key in the event of power failure (to make entry possible still).

Servo Motor

- A servo motor will be used to operate the deadbolt.
- *Requirements:* Servo motor must be able to operate the deadbolt, and requires 4.8-6.0V (will be run at 5V) [7].

### 2.2.4 Microcontroller on a PCB

The microcontroller will be used to control outputs for the mechanical parts of the design. It will send signals to/from our user interface and to our door locking subsystem. When the audio signal is verified, the microcontroller will send a signal to the locking system to disengage the lock, and also the signal to re-engage the lock. The microcontroller will also send signals to our RGB LED, displaying whether the door is locked, unlocked, or whether a phrase is being processed.

Microcontroller

- Will be used to take signals from Raspberry Pi and operate door lock and LED.

- *Requirements:* Must be able to sink/source 5V +/- 5% at GPIO pins to send/receive inputs, must be able to send PWM signal for servo motor.

### 2.3.5 Power Supply

We will use an AC voltage adaptor to power our components. Every component in our design requires power, so we will need a consistent supply. Since our design will be mounted on a door, a wall adapter in a nearby outlet will work sufficiently.

AC Adaptor

- Convert the AC wall power to 5V DC for our system to use.
- *Requirements:* Convert AC 120-240V power from wall into DC 5V +/- 5% for our circuit to use.

## 2.3 Risk and Tolerance Analysis

The riskiest block of our design is the keyphrase recognition; the main feature of the system is that this lock will be able to recognize a keyphrase, and then operate a lock based on this recognition. In order to implement this, we plan on implementing a keyphrase recognition algorithm in Python on a Raspberry Pi board; many possible methods for this exist, and our final implementation will determine what method we end up using.

Algorithms that currently exist for keyword recognition include using probabilistic models, such as hidden Markov models, or using some machine learning models. Currently, we plan to implement a few models, including a probabilistic model based on HMMs and a convolutional neural net model. These have been shown to work for the problem of keyword spotting [8], and we intend to implement multiple models and test for which one gives best performance. These methods have been shown to be able to achieve accuracies of around 80% [8], so we believe that we will be able to achieve similar results. Testing models will be done by providing example cases and noting results in a confusion matrix, as described in table 2. If these methods do not work, we could use existing speech recognition packages to implement our design as a last resort.

Another risk with this module is the availability of the Raspberry Pi; they are currently out of stock due to chip shortages. However, Raspberry Pi has said that they plan to make more devices available early this year [9]. If this does not work out, we can use an Arduino UNO Rev3 for this module as a replacement, as this board also allows us to program in Python.

## 3 Ethics and Safety

Our project should not have any major ethical or safety concerns. The main ethical concern that could be relevant would be due to recording audio for the lock. If this were being used to record conversations this would be a violation of people's privacy which would break the IEEE Code of Ethics section I part 1 [10] and also the ACM code part 1.6- Respect Privacy [11]. However, our design will only record short inputs which prevents it from recording entire conversations and will contain any audio recordings internally. Audio recordings will not be shared with any other device and will not be stored, so we do not pose the risk of violating user's privacy or sharing sensitive information.

Safety hazards for the project will also be very minimal. The highest voltage used will be due to using the wall adaptor but everything else in the design will be very low voltage. The mechanical portion of the design is the servo which will only be used when the door is actively locking or unlocking, so there will be very few moving parts. Therefore, the design poses no significant safety hazards or ethical concerns.

# 4 References


[1] Cameron, Dell. “Critical Flaws Leave Some Government Access Cards Vulnerable to Attack.” *Gizmodo*, Gizmodo, 15 Jan. 2019, https://gizmodo.com/critical-flaws-leave-some-government-access-cards-vulne-1831785262.

[2] “2019 Crime in the United States.” *FBI UCR*, Federal Bureau of Investigation, https://ucr.fbi.gov/crime-in-the-u.s/2019/crime-in-the-u.s.-2019/topic-pages/tables/table-23 . Accessed 9 Feb. 2023.

[3] “Electret Microphone Amplifier - MAX4466 with Adjustable Gain : ID 1063 : $6.95 : Adafruit Industries, Unique & Fun DIY Electronics and Kits.” *Adafruit Industries*, Adafruit Industries, https://www.adafruit.com/product/1063#technical-details. Accessed 9 Feb. 2023.

[4] “Diffused RGB (Tri-Color) LED [Common Anode] : ID 159 : $2.00 : Adafruit Industries, Unique & Fun DIY Electronics and Kits.” *Adafruit Industries, Unique & Fun DIY Electronics and Kits*, Adafruit Industries, https://www.adafruit.com/product/159?gclid=CjwKCAiA0JKfBhBIEiwAPhZXD3SFC1-uvJZXTvw7qj_EFlj4a_3rZqow17SQUkMDHsOSb_Yb-Od5ZhoC6g0QAvD_BwE. Accessed 9 Feb. 2023.

[5] Rose, R. C., and D. B. Paul. “A Hidden Markov Model Based Keyword Recognition System.” *International Conference on Acoustics, Speech, and Signal Processing*, IEEE. *Crossref*, doi:10.1109/icassp.1990.115555. Accessed 9 Feb. 2023.

[6]“Raspberry Pi Documentation - Raspberry Pi Hardware.” *Raspberry Pi*, https://www.raspberrypi.com/documentation/computers/raspberry-pi.html. Accessed 9 Feb. 2023.

[7] “Continuous Rotation Servo.” *Adafruit Industries*, Adafruit Industries, https://www.adafruit.com/product/154?gclid=CjwKCAiA0JKfBhBIEiwAPhZXDyM_2kg296y0_3YSy4qWPKv9_87anO0Qg7oYSY_LauXVC0iskXSNUhoCwEQQAvD_BwE. Accessed 9 Feb. 2023.

[8] Silaghi, Marius. “Spotting Subsequences Matching a HMM Using the Average Observation Probability Criteria with Application to Keyword Spotting.” *American Association for Artificial Intelligence* , American Association for Artificial Intelligence , 2005. https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=d94ba6d52cfe095dce25a3563a4dd47f754ee495

[9] Upton, Eben. “Supply Chain Update - It’s Good News! - Raspberry Pi.” *Raspberry Pi*, https://www.raspberrypi.com/news/supply-chain-update-its-good-news/.

[10] “IEEE - IEEE Code of Ethics.” *IEEE*, IEEE, https://www.ieee.org/about/corporate/governance/p7-8.html. Accessed 9 Feb. 2023.

[11] “Code of Ethics.” *Association for Computing Machinery*, Association for Computing Machinery, https://www.acm.org/code-of-ethics. Accessed 9 Feb. 2023.