Voice Biometrics Lock

ECE 445 Project Proposal - Spring 2021

Team 34 - Bella Chen(aotingc2) Lixin Guo(lixing2) Zaki Khan (zakik2)

TA: Anand Sunderrajan

1. Introduction

1.1 Objective

Losing your keys is not a pleasant experience. In addition, key locks don't do a good job of protecting homes because all of them can be picked, unless you have a keyless lock [1]. Because of this, electronic locks like the Nest x Yale [2] are becoming more prevalent for modern homes. They even work with voice recognition like Google Home, and you can lock the door from the inside with one command. Yet when you enter from the outside, a passcode is still needed because home devices would not recognize who should not be allowed into the door, and passcodes can be compromised. Our project will solve this security issue and improve home safety by using biometric traits, such as your voice and fingerprints, that are unique and can be used as a more secure way to verify your identity.

In order to solve this issue, we propose to design a biometrics voice lock. This lock would work with voice recognition and a fingerprint sensor and would be connected to an application that users would be able to download on their phones. This lock would use real-time voice recognition to distinguish the voice of the authorized user(s). It would do so by generating a random command for the user to read aloud. The app would verify that the command said was correct and also that the voice was that of any authorized user. This would prevent someone from getting a recording of someone and trying to pose as the authorized user. In addition, in the case that the user is unable to use his/her voice, we would also implement a fingerprint scanner on the lock to prevent someone from being locked out. In other words, the fingerprint scanner would help prevent false negatives and the randomized command would help prevent false positives. The mobile application would be connected to a receiver circuit through Bluetooth. Overall, our solution would target the everyday individual that is hoping to improve the security of his/her home.

1.2 Background

According to the US Department of Justice, there are 2.5 million burglaries annually in the United States, with 66% of these being home invasions. In addition, 34% of burglars use the front door when breaking into a home, according to the Bureau of Justice [3]. Our solution would add an additional level of security to the user's front door. We would remove the keyhole which would prevent the lock from being picked by the burglar. This would reduce the method of entry for the burglar. Reducing a method of entry would discourage some home burglars who look for easy and not obvious methods of entrance and would in result lower the number of burglaries that occur.

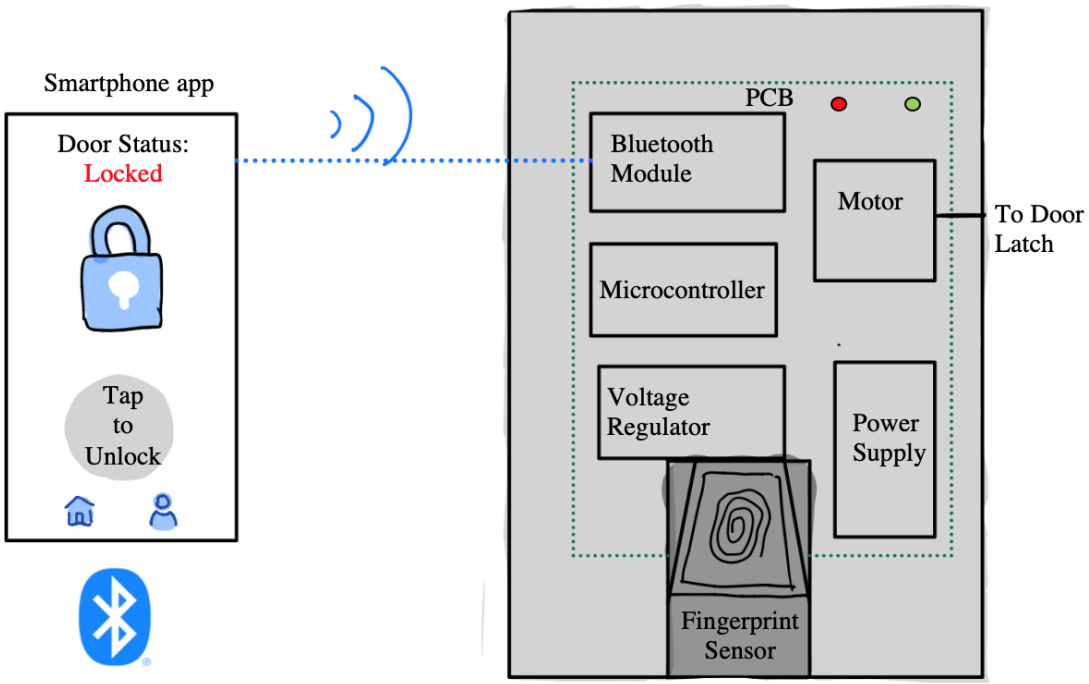
Recently, there has been an increase in mobile keys. For example, Hyundai and Mercedes have both implemented applications that let you unlock your car with your phone [4]. In addition, some hotels such as Marriott now allow you to unlock your room with your phone using a mobile room key [5]. However, there are not any commercially available door locks with voice recognition and fingerprint scanners. As time is passing, users are beginning to prefer mobile solutions to everyday problems, home security being one of them. Our solution would satisfy this

by allowing them to control their front door with their phone and would reduce the need for people to carry around bulky house keys.

During the COVID pandemic, a lot of businesses are considering incorporating voice-based features into their product, as there is an increase in demand for contactless solutions to contain the spread of the virus. By primarily relying on speech recognition and using a fingerprint sensor only as a backup, we create a door lock that minimizes physical contact with its surface.

1.3 Physical Design

Our solution would require the user to install the physical lock on his/her door and download a smartphone app that communicates with the Bluetooth module inside the lock. The door status will be shown at the top-center of the screen, and the below smartphone screen shows a locked status. A gray button will prompt the user to tap and speak a one-time, random passcode. If the app's voice recognition system deems that it is the rightful owner, a wireless signal will be sent from the smartphone to trigger the lock. The fingerprint sensor would be activated after three failed attempts of voice recognition.



`

Figure 1. Physical Design Diagram

1.4 High-level requirements list

1. The smartphone app should be able to verify a spoken string of at least 6 characters long with a mix of letters and numbers [6] with a minimum of 95% percent accuracy, the highest rate that is achieved by Google in 2017 [7].
2. The processing time of speech recognition should be real-time, taking no longer than 3 seconds for a 5-second audio clip, for example [8].
3. Verification with the fingerprint sensor should have an extremely low error rate of lower than 1% [9].

2. Design/Block Diagram

In our block diagram below, we have shown that the smartphone application will carry out the voice-recognition feature and store any voice or account data. The lock itself will require a control unit to lock or unlock the door by a series of connections that can receive external signals that trigger the rotation of the servomotor. The microcontroller is the central processor of all information and will be able to communicate back with the phone to report back the lock status. The sensor data will be processed by the microcontroller when fingerprint verification is activated. A power supply unit must be able to supply at least 12 V. A voltage regulator will provide the required voltage to all subcomponents inside the lock. Detailed requirements and sources will be explained and cited in the functional overview section.

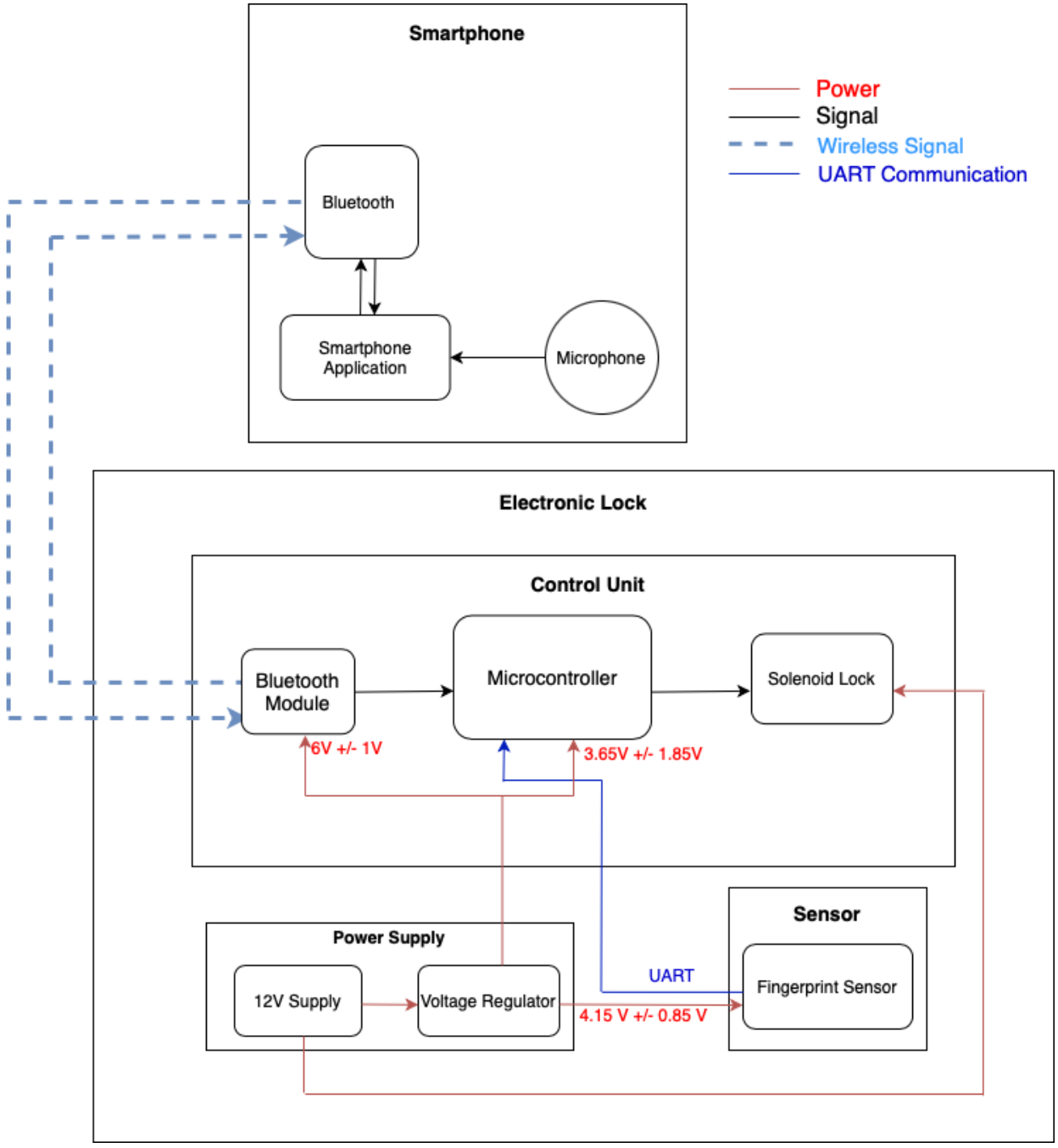


Figure 2. Design Block Diagram

Functional Overview

2.1 Smartphone

The smartphone would serve as one way for the user to interact with the lock. Our project would use three main components on the phone: an application that we would develop, a microphone, and a Bluetooth receiver/transmitter. The user would use the microphone to communicate with the application and say the command needed to unlock the lock. The microphone would also be used to help the application learn the voice of the user. Whenever a successful unlock is made, the application would use the Bluetooth sensor to send the lock a signal to unlock. This signal would be sent to the Bluetooth module on the control unit of the electronic lock module. In addition, it also receives a signal whenever the fingerprint scanner was used to unlock the lock. This is so that the lock status can be updated on the application. In addition, the application would let the user lock the lock by tapping a button. Overall, this block would add the features of allowing the user to unlock the lock using a passphrase, allowing the user to lock the door with one tap in the app, and having the correct status of the lock displayed.

Requirement: The smartphone should be able to send a Bluetooth signal to the lock within 150ms from when the audio signal was spoken. This is average for Bluetooth and Android and would ensure that the lock gets unlocked within a reasonable time [10].

2.2 Control Unit

The control unit works as the central processor unit for the electronic lock, it controls the actions on the lock based on verification result signals. There are four parts connected here including the Bluetooth module for wireless signals, the microcontroller for data operation, and the motor with a relay to physically lock or unlock the door. This unit will be implemented with the lock and communicate with the smartphone and fingerprint sensor to simultaneously update lock status and take actions by instructions.

2.2.1 Bluetooth Module

The Bluetooth receiver unit uses a Bluetooth audio receiver gadget to build a wireless connection with the smartphone to transmit the signals forward or backward accordingly. We plan to use Adafruit Bluefruit LE UART Friend for Bluetooth Low Energy and this will be the interconnection between the phone and the microcontroller. Once the phone finishes operation on voice data, it will send the signal to the receiver which will be passed to the microcontroller to determine the instruction. The information of the lock identified in the microcontroller will also be sent back to the phone through this block for the user to check.

Requirement: The bluetooth module must complete the data transition between the phone and microcontroller with minimum possible delay below 46ms [11] referring to the optimal performance. It is expected to work with a standard frequency of around 2.4GHz.

2.2.2 Microcontroller

The microcontroller processes the ignition verification to control the motor. It communicates with the phone to read the Bluetooth data through the oscillator and send commands through the relay to trigger the motor. The condition of the motor will be simultaneously sent back to the Bluetooth module and then delivered to the phone displayed for users. If the voice recognition fails as accidents, the processor will receive data from the fingerprint system and operate for the commend passed to the motor that if the data matches the motor will be triggered and this status update will be sent back to the smartphone at the same time. We plan to use the ATmega328 since it is compatible with the sensor and all other subcomponents inside the control unit.

Requirement: The microcontroller must be compatible with both the Bluetooth module and the fingerprint sensor. It is expected to work with 1.8-5.5 volts [12] and achieve the standard throughputs of close to one MIPS per MHz to minimize power consumption while processing the data.

2.2.3 Solenoid Lock

The motor receives a signal from the microcontroller through the relay that tells it which direction to rotate, realizing the electrical part of locking and unlocking the door.

Requirement: The lock must be compact enough to fit onto the door. A typical bolted lock has dimensions 6.1 in x5.8 in x 3.9 in [13], and our solenoid lock must be similar in size or smaller. It must be able to rotate at least 90 degrees to the left and 90 degrees to the right to lock or unlock.

2.3 Power Supply

All sub-components inside the electronic lock need a power supply for operation. Due to different needs in the voltage source, we would need a central power supply that can provide sufficient power to all subsystems and a voltage regulator that allocates the correct amount of voltage according to the specifications of each unit.

2.3.1 12 V Supply

A DC power supply needs to provide a constant 12 V because the required voltage for the solenoid lock is 10.5 ± 1.5 V. Supplying it at the maximum voltage allows less current to be drawn from the solenoid lock, and more current to drive the rest of the components.

Requirement: A DC power supply needs to provide a constant 12 V because the component that requires the most amount of power is the solenoid lock, whose required voltage is 10.5 ± 1.5 V[14]. It is ideal to supply the solenoid lock at 12 V because it draws a large current of 500 mA and thus might not be powered by voltages near 9 V[14].

2.3.2 Voltage Regulator

Because the lock subcomponents require different voltages that are lower than the microcontroller's minimum voltage requirement, we need a voltage regulator to deliver different amounts of voltages to the subcomponents without losing too much power.

Requirement: The voltage regulator must have a minimum input voltage of 7V and must handle at least 350 mA peak current draw. It must supply 6 ± 1 V to the bluetooth module[15], 4.15 ± 0.85 V to the fingerprint sensor[9], and 3.65 ± 1.85 V to the microcontroller[12].

2.4 Sensor

The sensor module would contain the fingerprint sensor. The fingerprint sensor would be used to prevent false negatives. The power supply module would be used to provide power to the fingerprint sensor and to regulate the voltage that it receives. It would communicate with the microcontroller in the control unit through UART. When a person places his fingerprint on the sensor, the fingerprint sensor would communicate with the microcontroller and if the verification of print is successful, will send a signal to the application to unlock the lock. This module would add the feature of allowing the user to unlock the lock using a fingerprint scanner to our overall project.

Requirement: To ensure the security of the lock, we would need to source a sensor that identifies living things only, so that artificial replicas of the user's fingerprint would not work. It should have an extremely low false acceptance rate of less than 0.005% and a false rejection rate of less than 1% [9].

2.5 Risk Analysis

The block that poses the greatest risk to the successful completion of our project is the smartphone app. This is because, for the smartphone application, we would need to implement the voice recognition and speaker identification functions simultaneously, which traditionally would utilize some machine learning algorithms that are complicated to implement. If we were to pursue this path, we would need to learn how to utilize pre-built machine learning pipelines, such as AWS. We would also need to approach the least time-consuming algorithm to ensure real-time processing.

Another solution would be utilizing a cognitive service from well-known AI companies, like Microsoft or Google. Since we would only perform speech recognition on audio data with brief durations not exceeding 10 seconds, we would be able to use them for free. However, this approach would require an initial learning phase for us to integrate their services with our app. It is vital that we are capable of using those tools during app development because speech recognition is the core of our project idea.

Another issue that we could run into is the difficulty of overcoming the permission issues for accessing the microphone and enabling Bluetooth in React Native for the Android application. Since we would need to use the phone's microphone and Bluetooth, we would need permission from the user before using it, and it might vary based on the version of Android. If we are not able to figure out how to get permissions on the mobile platform, we would then switch to a web app service for the application development. For example, Chrome has built-in features that would ask the user to allow access to both the microphone and Bluetooth LE.

3. Ethics and Safety

During the development of our project, we will follow the instruction from ACM Code 2.9 to make design and implement "robustly and usably secure"[16]. We as a team will use our own information during the testing process of the voice and fingerprint systems. We will ensure agreements reached with conditions on no third-party usage of all testing data to avoid the potential issues of data breaches in this phase. We will erase the data permanently after the development phase or any closed beta tests. For the accidental misuses which may arise in this case, we will keep track of the recording of data accesses to protect every team member.

Typically, fingerprint sensors are not as secure as our proposed voice recognition scheme because fingerprint data can be easily stolen, and sensors can be cheated with a master fingerprint. A Forbes article discussed that researchers from the X-Lab have demonstrated that any fingerprint lock from Android or iPhones can be hacked in 20 minutes [17]. However, the total cost of hacking fingerprints costs more than $142, and the research methodologies on how to replicate fingerprints are not publicly accessible [17]. For the everyday person, we can

increase the security of fingerprint encryption by choosing a capacitive fingerprint sensor that requires detection of electrical properties, and one that can achieve high accuracy, such as one with a false positive rate of < 0.005%[9]. This eliminates the possibility of hacking the sensor with a printed photograph of the fingerprint pattern and increases the cost of breaking in. Fabricating a fingerprint on conductive material would require access to expensive equipment, such as 3D printers with precision on the micrometer scale, and is not commonly accessible.

For training the voice recognition model, our project would require the collection of the user's voice, which is a form of biometric information and is under severe regulation by local and international laws. When accessing the user's voice, we must proceed with caution and follow all legal compliances to ensure the user's privacy and security are protected. In May 2018, the EU passed the General Data Protection Regulation (GDPR) that tightened the regulation of a class of data called "personal information" [18], any form of data that can be used to identify an individual. It requires businesses to own personal information to give their subjects the "right to access" and "delete" those data [18]. In addition, state laws require businesses that possess personal information to destroy the data when they are no longer needed and to send a notice to the subjects in a data breach, such as when their voice data is exposed to hackers trying to access their accounts [18]. Regarding IEEE and ACM Codes of Ethics, the development and employment of voice recognition and fingerprint systems are restricted by ACM Code 1.6 of "respect privacy" and 1.7 of "honor confidentiality"[16]. This part reflects also on the aim of protecting others' privacy and informs potential dangers stated in IEEE[19].

To adhere to those laws, we must provide the users of our product full transparency regarding the use of voice data. During the product development, we would use public databases and mostly our own voice data to test the product's functionality. If this were made into a product, we would need to explain what personal information would be collected, the purpose of collecting those data, and how they will be used. The user will only proceed with registration by checking a box indicating they have reviewed and agreed to those terms. The user's voice will be the only personal data that we would access for training the voice recognition model, and it will be stored online or on the device. Once the training phase is completed, the data will be automatically removed. We will use subsequent recordings of the user's voice to update the model, but they will be permanently erased from the device afterward. The fingerprints of the user will need to be stored for recognition. We will never distribute any biometric information to any third party. Users will always hold the right to end the program and amend or delete their information and if they decide to close the account, we will destroy all pertinent information of the user. If we ever notice a data breach, we will be responsible for notifying the affected users in a timely manner. With our promises on the respect of data collection and declaration of responsibility, the potential safety concern over unexpected hacker intrusion to steal user's data still exists. For this type of issue, we will follow the regulation process to help customers track the criminal's legal liability, and we will inform them of this possibility at the beginning.

Our product utilizes Bluetooth technology for wireless communication between the smartphone and the microcontroller. The FCC poses regulations on all RF devices, including the Bluetooth modules. For devices operating below 6 GHz, the allowed energy exposure is 1.6 W/kg [20]. Since we will be using a Bluetooth LE module that has low power requirements and maximum transmission power of 0.7 mW [21], exposure to the radiation for an extended amount of time would have no adverse effect on health.

We agree to comply with the ethical codes and safety regulations to protect and respect user privacy and develop prevention rules to follow throughout the development and employment to minimize client concerns. We guarantee to take our professional responsibilities to pursue high standards on our project and we expect the wide usage of this system to contribute to the society with advanced security.

References

[1] “Pick Proof Locks – Are They Worth It?,” *NGCL*, 13-Aug-2019. [Online]. Available: https://www.thengcl.co.uk/pick-proof-locks/. [Accessed: 19-Feb-2021].

[2] “Learn about the Nest × Yale Lock before you buy,” *Google Nest Help*. [Online]. Available: https://support.google.com/googlenest/answer/9251009?hl=en#zippy=,does-it-support-voice-commands. [Accessed: 19-Feb-2021].

[3] “Burglary Statistics & Research from the BSJ and FBI: The Zebra,” Burglary Statistics & Research from the BSJ and FBI | The Zebra. [Online]. Available: https://www.thezebra.com/resources/research/burglary-statistics/. [Accessed: 18-Feb-2021].

[4] B. C. Corum, “NFC vehicle keys let Mercedes drivers go keyless,” SecureIDNews, 16-May-1970. [Online]. Available: https://www.secureidnews.com/news-item/nfc-vehicle-keys-let-mercedes-drivers-go-keyless/. [Accessed: 18-Feb-2021].

[5] “Marriott expands mobile requests as keyless room entry takes flight,” *Latest News*. [Online].Available:https://www.marketingdive.com/ex/mobilemarketer/cms/news/strategy/21718.html. [Accessed: 18-Feb-2021].

[6] “Password strength,” *VoiceThread*. [Online]. Available: https://voicethread.com/howto/password-strength/. [Accessed: 18-Feb-2021].

[7] “The Complete Guide to Speech Recognition Technology,” *Globalme*, 05-Jan-2021. [Online]. Available: https://www.globalme.net/blog/the-present-future-of-speech-recognition/. [Accessed: 18-Feb-2021].

[8] “Speech-to-Text basics | Cloud Speech-to-Text Documentation,” *Google*. [Online]. Available: https://cloud.google.com/speech-to-text/docs/basics. [Accessed: 18-Feb-2021].

[9] B. Zuo, “Grove - Capacitive Fingerprint Scanner/Sensor,” seeedstudio. [Online]. Available: https://wiki.seeedstudio.com/Grove-Capacitive-Fingerprint-Sensor/. [Accessed: 17-Feb-2021].

[10] “Android's Bluetooth latency needs a serious overhaul,” *SoundGuys*, 12-Apr-2019. [Online]. Available: https://www.soundguys.com/android-bluetooth-latency-22732/. [Accessed: 18-Feb-2021].

[11] “Evaluating Bluetooth Low Energy Suitability for Time-Critical Industrial IoT Applications,” *International Journal of Wireless Information Networks.* [Online]. Available: https://link.springer.com/article/10.1007/s10776-017-0357-0

[12] “ATmega328P Automotive - Complete Datasheet,” *Microchip*. [Online]. Available: https://ww1.microchip.com/downloads/en/DeviceDoc/Atmel-7810-Automotive-Microcontrollers-ATmega328P_Datasheet.pdf [Accessed: 17-Feb-2021].

[13] “834 Barrel Bolts,” N151-654 | National Hardware. [Online]. Available: https://www.national-hardware.com/detail/834-barrel-bolts-n151-654. [Accessed: 17-Feb-2021].

[14] A. Industries, “Lock-style Solenoid - 12VDC,” adafruit industries blog RSS. [Online]. Available: https://www.adafruit.com/product/1512. [Accessed: 17-Feb-2021].

[15] A. Industries, “Adafruit Bluefruit LE UART Friend - Bluetooth Low Energy (BLE),” adafruit industries blog RSS. [Online]. Available: https://www.adafruit.com/product/2479?gclid=Cj0KCQiA962BBhCzARIsAIpWEL2hKXYKYeMwCB3aJRV6bTdp0kTPdfmKgCdLwMSnp5xlyeVECqWaxdYaApboEALw_wcB. [Accessed: 17-Feb-2021].

[16] ACM (Association for computing machinery) Code of Ethics and Professional Conduct, 2016. Available: https://www.acm.org/code-of-ethics

[17] D. Winder, “Hackers Claim 'Any' Smartphone Fingerprint Lock Can Be Broken In 20 Minutes,” Forbes, 02-Nov-2019. [Online]. Available: https://www.forbes.com/sites/daveywinder/2019/11/02/smartphone-security-alert-as-hackers-claim-any-fingerprint-lock-broken-in-20-minutes/?sh=4d37a44d6853. [Accessed: 17-Feb-2021].

[18] J. J. Lazzarotti and M. Atrakchi, “As Voice Recognition Technology Market Surges, Organizations Face Privacy and Cybersecurity Concerns,” *Voice Recognition Tech Privacy and Cybersecurity Concerns*, 10-Dec-2020. [Online]. Available: https://www.natlawreview.com/article/voice-recognition-technology-market-surges-organizations-face-privacy-and. [Accessed: 12-Feb-2021].

[19] IEEE (Institute of Electrical and Electronics Engineers) Code of Ethics, 2015. Section 7 - Professional Activities, Available: https://www.ieee.org/about/corporate/governance/p7-8.html

[20] “Wireless Devices and Health Concerns,” *Federal Communications Commission*, 04-Nov-2020. [Online].Available:https://www.fcc.gov/consumers/guides/wireless-devices-and-health-concerns. [Accessed: 19-Feb-2021].

[21] “Adafruit Industries Bluetooth Module BLUEFRUIT FCC ID S6OBLUEFRUIT,” *FCC ID*, 08-Apr-2013. [Online]. Available: https://fccid.io/S6OBLUEFRUIT.