ECE445 Design Document
Fingerprint Protected Voting Machine

Team 68

Ashwin Dandapani (ashwind2), Brennan Hartigan (bah4), Jeremiah Kennedy (jck5)

Spring 2021

TA: Dean Biskup

Table of Contents

1. Introduction

1.1 Objective

As the 2020 election brought upon many questions with regards to voter fraud [9], we felt our project would be best served to attempt to help or fix this problem. One effective tool to uniquely identify voters and prevent voters from revoting is to use each voter's fingerprint. Since each fingerprint is unique to a person, there will not be the ability to fake your eligibility or your name when voting.

Our plan is to utilize fingerprint identification to confirm that a voter has not voted previously to keep the voting fair. We will design and create a scrolling device that allows the voter to scroll through the options and select the candidate they decide on. After this, they will receive a receipt to confirm that they had voted and the receipt will be placed in the ballot box to cast their vote.

1.2 Background

The 2020 presidential election was littered with claims about potential voter fraud. This is something we feel can be completely fixed with voter identification through fingerprints. According to the BBC, Donald Trump's campaign mentioned "voter turnout in some areas was higher than 100%, an outcome known as an 'overvote'" [9].

There has been plenty of dispute over these claims, with many claiming that voter fraud is, in fact, very rare and unlikely, but it has been documented in the past in smaller scale elections [12]. Whether the Trump Campaign's claims are accurate or not, by having this more robust and accessible voter identification through fingerprints would prevent any further questions on the topic of voter fraud and thus would help eliminate much of the controversy that has developed around election time.

Along with voter fraud, this new method for voting can help reduce voter suppression, as eligibility of voters is scanned with the fingerprint. By utilizing the fingerprint as a method of identification, this eliminates any further voter identification needed in order to officially register and vote. Currently the strict laws with respect to voter registration have made it disproportionately difficult for racial and ethnic minorities to vote [11].

An overvote would not be possible if after a uniquely identified fingerprint has a boolean true saying that the person has in fact voted. It is understood that this election was

unique because mail-in votes were more prominent due to COVID-19, but we feel this would be a safe alternative to the current system for voting.

A current concern is that without stricter voting ID requirements, which have been shown to cause voter suppression, we could be compromising prevention of voter fraud [11]. This alternative would not only be able to prevent voter fraud but also prevent voter suppression, without having to compromise on one or the other. Preventing both of these potential outcomes will allow for a smoother, less controversial election.

1.3 High-Level Requirements

- Voter can scan their fingerprint and successfully make a vote. In order to identify that the voter is allowed to vote, we will look for an accuracy of 95%.
- If the fingerprint of a voter did not have a match after three tries, then the voter is rejected. This will be done three times to prevent a potential error by the system the first time it scans the voter's fingerprint.
- Voter will be able to receive feedback through the LEDs, speaker, and thermal receipt printer after voting is completed. Specifically will light up the LED red when a voter is denied and green when a voter is accepted. When a voter is rejected the buzzer will sound on the speaker. Also, after a voter completes casting their vote, a receipt with the chosen votes will be printed.

2. Design

Block Diagram

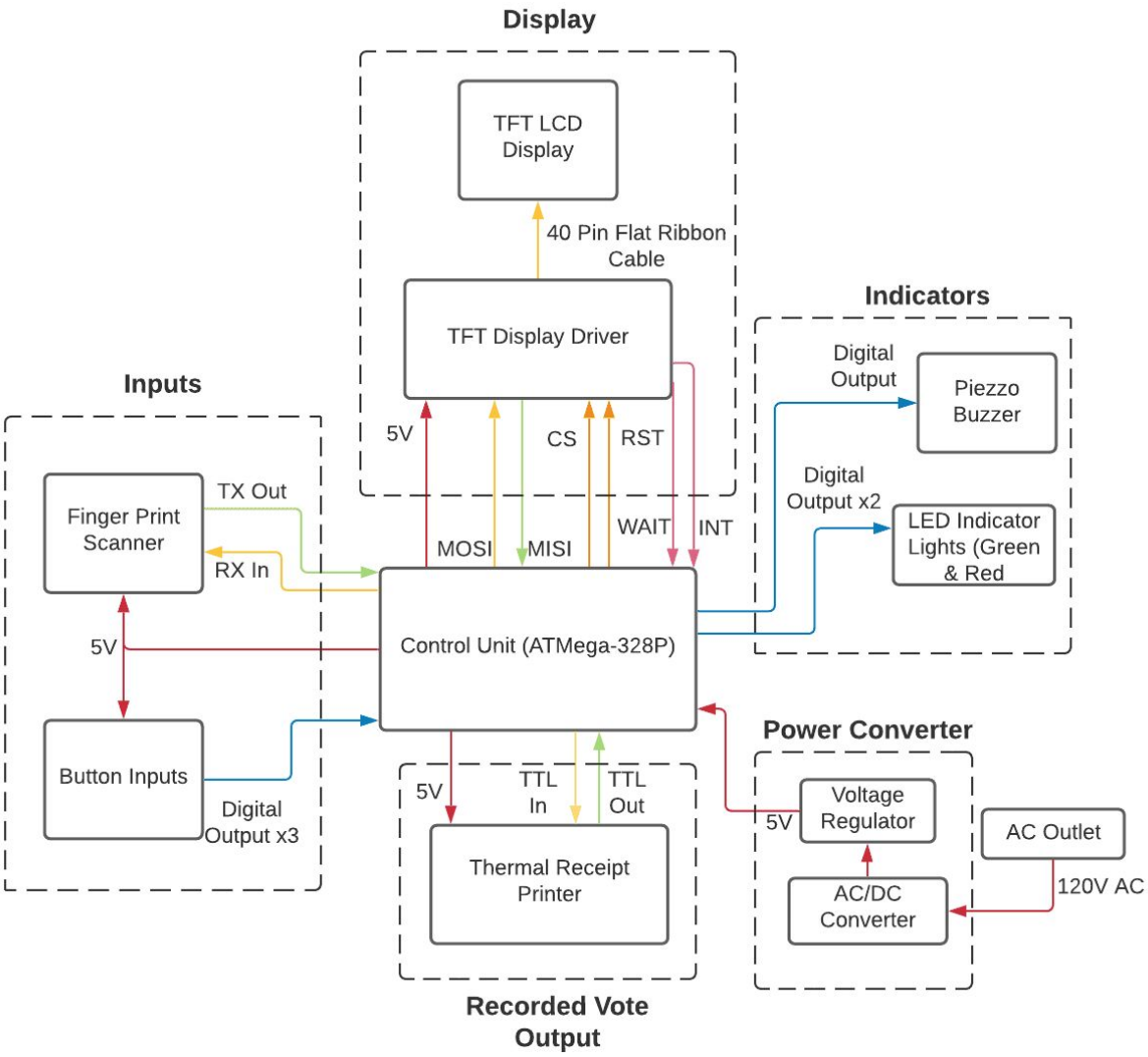

Fig. 1: Block Diagram

Physical Design

Our project will have a fingerprint scanner that is attached to a control panel that allows for scrolling up, down, and a select button to choose the vote. This will connect to a monitor screen to allow for the voter to see who they can select from and then click on the option. The monitor will also tell them if they are eligible to vote after scanning their fingerprint. Above the monitors will be holes for two LEDs, to indicate whether the voter has gained access to the system by verifying their fingerprint.

The physical envisioning of this system will look like a flat box, constructed out of wood. The buttons and fingerprint scanner will be mounted to a piece of wood parallel to a table, with the screen mounted directly above these hardware devices, as the centerpiece of the design. All electronics will be housed on the interior side of the wooden panels, out of sight from the user. Pictured below is a conceptual drawing of what the physical design of this project will look like:

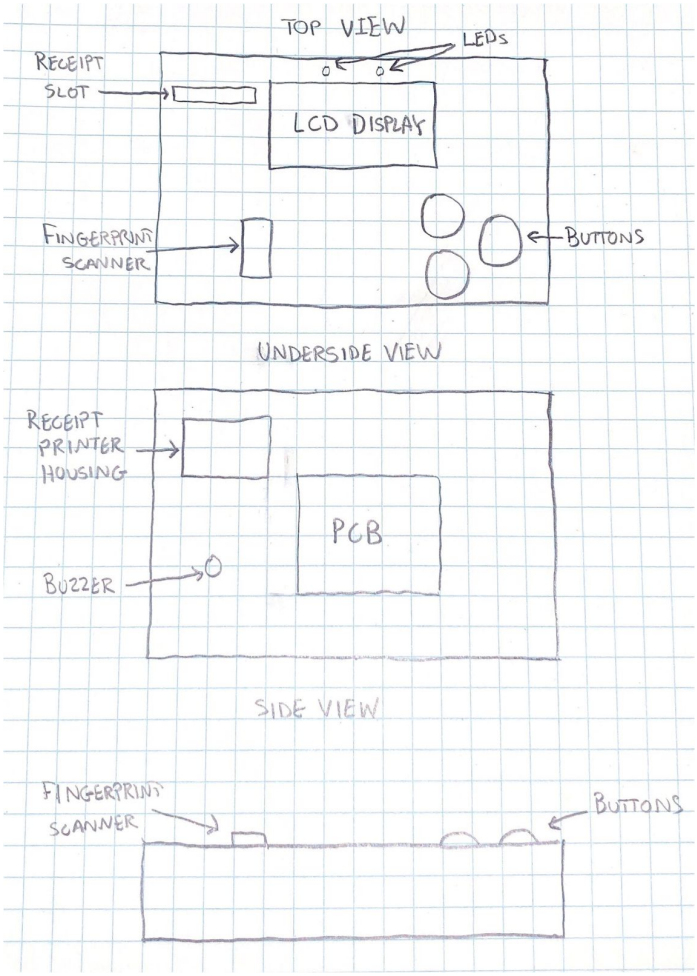

Fig. 2: Physical Design of Solution

Requirements and Verification

2.1 Power Supply

A power supply is required to keep the voting machine and all hardware peripherals running during use.

2.1.1 AC to DC converter

An AC to DC power supply converter is needed in order to allow the system to be plugged into a 120V AC standard wall plug, and convert the power to DC voltage so the hardware in this project can be powered correctly. The AC to DC converter will also need to step down the voltage to 12V so it can be handled by the voltage regulators.

Requirement	Verification
Must be able to convert AC wall voltage to DC voltage, and step down the voltage to 12V +/- 5% so it can be processed by voltage regulator ICs.	Use a voltmeter to ensure that the DC output is steady at within 5% of 12V, which we will monitor for 15 seconds to confirm.

2.1.2 Voltage Regulator

These ICs will supply the necessary 5V to the hardware in this project. These ICs will need to be able to handle incoming DC voltage from the AC to DC converter [2].

Requirement	Verification
1. The voltage regulator ICs must be able to handle incoming 12V DC voltage from the wall. 2. Provides 5V +/- 5% from the 12V source 3. Can operate at currents within 0-1.5A	1. A. The voltage regulator specifications indicate that it may receive a 12V DC input 2. A. Using a multimeter, measure the output voltage(s) and ensure that they are within 5% of the required 5V. 3. A. Use resistors to scale down the current from 1.5A to lower currents to match peripheral hardware's specifications. Use an ammeter to measure and verify this range of currents.

2.2 Control Unit

A control unit will handle all inputs from people (selection buttons), sensors (fingerprint reader), and process the voter identification and voter selection data to be displayed on a screen, with feedback given to the user through LEDs, a buzzer, and a receipt printer in this system.

2.2.1 Microcontroller

The microcontroller, chosen to be an Atmega328p [1] will handle all user input and output for the voting machine. These input and output signals sent to the various other devices in the system will be a variety of UART, digital, and SPI signals.

Requirement	Verification
1. The microcontroller must be able to communicate over UART in order to process and transmit the input data from the fingerprint reader. 2. The microcontroller must be able to receive and send digital signals 3. The microcontroller must be able to communicate over SPI in order to echo movements on the screen.	1. A. Using an LED and the fingerprint scanner, test the microcontroller's ability to process UART signals from the fingerprint scanner in fingerprint matching. The LED turning on will indicate a matched fingerprint. B. Using example text specified in the software, send UART signals to the receipt printer to print out the example text. 2. A. The LED lights will receive digital signals and light up if a user is granted access or denied B. The buzzer will buzz if a user is denied 3. A. The screen will respond to digital input signals from the buttons

2.2.2 Input Controller Device

An input controller device will be made up of three buttons: two for scrolling up and down, and one to advance the display/enter a selection. These buttons will communicate with the microcontroller via digital signals.

Requirements	Verification
1. The buttons must be pressable and work on first attempt. 2. The buttons should be prominently displayed and easily accessible. They will be the main forefront of the physical design.	1. A. Press the buttons and ensure that it can be done without multiple presses. 2. A. The buttons will be mounted on the front of the physical design. The housing will be placed at a variety of heights, and ensure that a wide variety of users can easily access them.

2.3 Fingerprint Scanner

The fingerprint scanner [6] will have the ability to read in a user's fingerprint, and send data to the microcontroller via UART to compare with existing fingerprint data.

Requirements	Verification
1. The scanner will have a less than 1 second fingerprint image acquisition time 2. The scanner accurately produces a fingerprint image within 3 user attempts. If there is an unsuccessful attempt, the screen will display a message asking the user to wipe or clean their finger, as dirt or sweat may be impeding the scanner from reading the fingerprint.	1. A. If the scanner is able to administer the fingerprint and decide a response in a second. The delay will be set in the software. 2. A. If the scanner is able see a match in the system or if not it makes the user re scan. B. If the scanner is able to mention if the user needs to re-scan their finger after checking for a match.

2.4 LCD Display

An LCD display will be the main user interface of the machine. It will provide instructions, show messages granting or denying access to the system, and show candidate choices for a voter to make their selection.

2.4.1 5.0” 40-Pin TFT Display

This is the LCD display that has been chosen for use in this project [3]. It will communicate data on the machine’s with the user, and will be the main output source for the overall UI.

Requirement	Verification
Each display must have a brightness of no lower than 350 lumens in order for best visibility to voters [26].	Confirming that the screen measures to have a brightness that is 350 lumens or greater.

2.4.2 TFT Display Driver Board

A RA8875 driver board for 40-pin TFT touch displays [4] will be used as the driver for the LCD display. This will allow the display to be refreshed at 60hz, and adjust the power to the display, as the display requires a 5-9V and 125-150mA input. The driver board will maintain the input power to the screen, and handle the screen RAM and timing requirements in the background.

Requirement	Verification
1. The display will need 5-9V and 125-150mA input to maintain its backlight, so it is easy for users to read. 2. This driver will communicate with the microcontroller via SPI.	1. A. Using the voltage regulator, ensure that this steady voltage can be maintained, while using resistors to adjust the current. B. Place the screen mounted in the physical design at a range of distances, and ensure that the screen can still be read.

	2. Connect to the microcontroller and send example images to the screen, ensuring that the data displayed matches the data sent.

2.5 Output Hardware

Output hardware devices will help to improve the overall user experience, as well as enhance the project with audio and visual output.

2.5.1 Buzzer

A Piezo buzzer, model PS1240 [7] will be used to communicate to the user that their access has been denied. This will be communicated from the microcontroller via a digital signal.

Requirement	Verification
Output frequency should be at a minimum 2KHz, and maximum 4KHz	A. Use a frequency spectrum analysis application to measure the frequency produced by the buzzer. B. Ensure that the buzzer's frequency matches the frequency specified by the software.

2.5.2 LEDs

LEDs will communicate “access granted” with a green LED illuminating, and “access denied” with a red LED illuminating.

Requirements	Verification
1. Turn on within 10ms of access denied/granted 2. Remain RED until access is granted, remain GREEN once access has been granted until the user is finished voting. The user is finished voting when their vote has been cast and the receipt printer prints out a record of their vote. 3. Operate on a drive current of 10mA, 1.8-2V	1. A. Use the fingerprint sensor in conjunction with the LEDs; write sample code with 10ms delay between fingerprint analysis and LED indication. 2. A. In conjunction with the fingerprint scanner, simulate this process by using a matched fingerprint to turn on the GREEN LED, and using a non-matched fingerprint to turn on the RED LED. This will be done using the microcontroller. 3. A. Adjust resistances from a voltage regulator to deliver 10mA to the load. B. Use a multimeter to verify the input voltage and current.

2.6 Mini Thermal Receipt Printer

A mini thermal receipt printer [5] will print the voter’s selection on thermal paper, to be placed in a secure ballot box and counted and tallied at the end of the voting process. It will receive data from the microcontroller via digital signal.

Requirement	Verification
Accurately print a voter’s selection onto thermal paper with a resolution of 8 dots per millimeter, 384 dots per line.	Using the microcontroller, send a variety of example texts in different fonts and sizes to be printed from the receipt printer, and ensure that it can be read clearly

2.7 Schematics

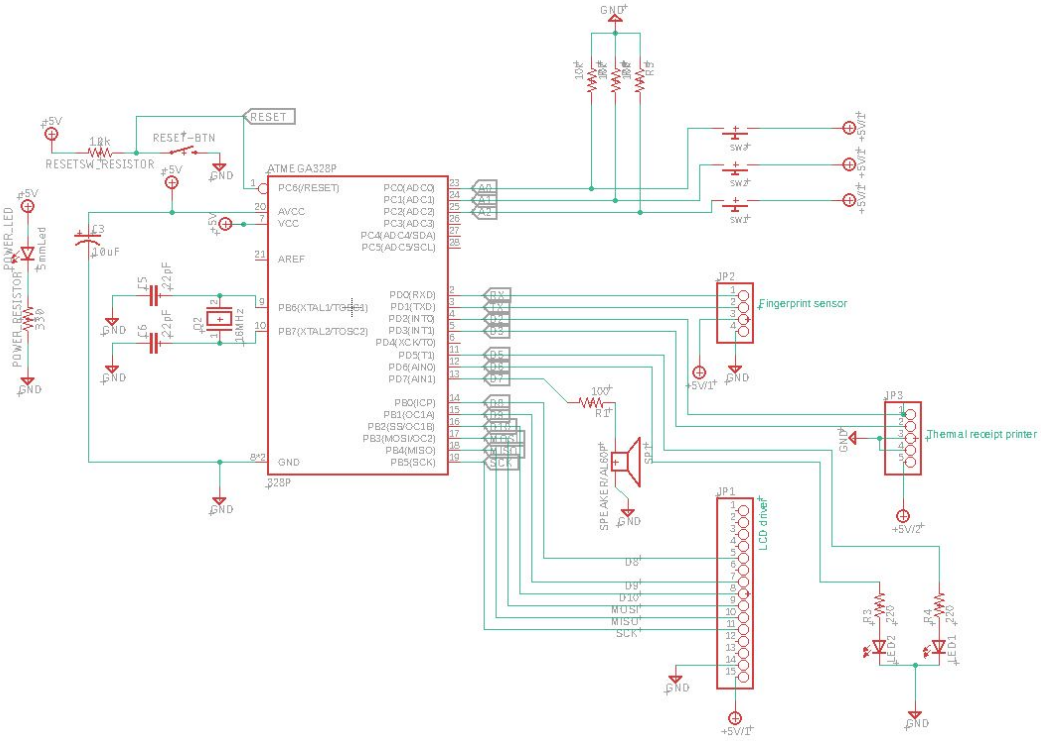

Fig. 3: Microcontroller and Hardware Peripherals

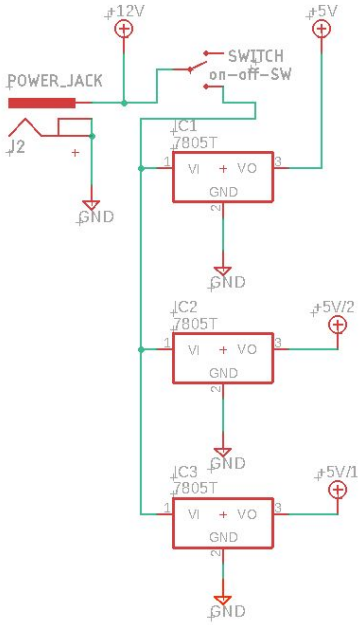

Fig. 4: Power supply

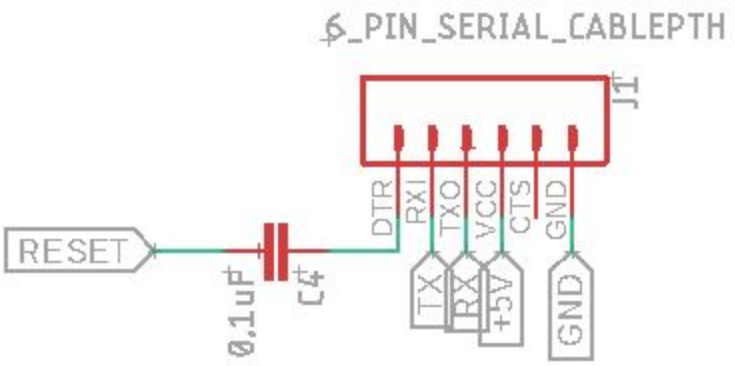

Fig. 5: Programming interface

2.8 Software Algorithm

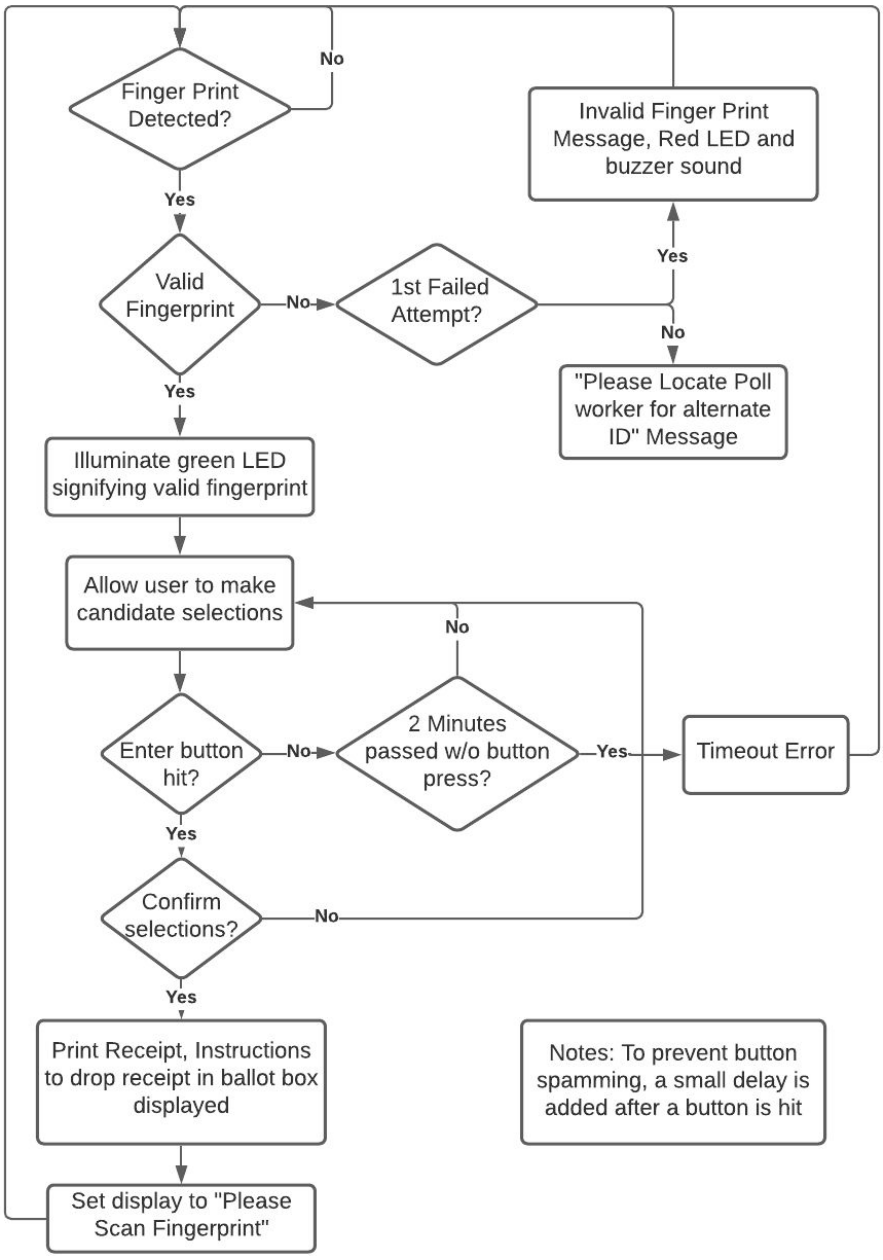

Fig. 6: Software Algorithm

2.9 Tolerance Analysis

An important tolerance this project must adhere to deals with the fingerprint sensor. This sensor is the backbone of the project, and will not allow the project to be considered a success unless the fingerprint scanner has high accuracy and low error when it comes to fingerprint matching and granting access to the voting machine. We are setting our accuracy tolerance at 95%. The fingerprint scanner hardware chosen for the design is rated with a <0.001% false acceptance rate, and a <1.0% false rejection rate [6]. Overall, computerized systems that automatically match fingerprints have become so sophisticated, they are accurate more than 99% of the time, according to an NIST study on fingerprint scanning systems [16]. Given these specifications, we believe that as this is the first version of this product, a 95% tolerance rate is acceptable for the scope of this project.

Fingerprint scanners of all types and systems operate and verify under the same common manner. The sensor is used to produce an image sample (fingerprint). An algorithm in the sensor's on-board AS608 chip extracts the sample's most characteristic features, and saves this information as a binary template in its storage. Below are some characteristic features of fingerprints that scanners, such as the one being used in this project look for:

Fig. 7: Fingerprint Characteristics[17]

Once the fingerprint enrollment is complete, the binary template of this image is saved in the system's secure storage. When it is time for verification, the system again produces an image sample of the fingerprint, and this fresh image is compared against the enrolled fingerprints by an algorithm. A similarity score is calculated, and the hardware can then decide whether the scanned fingerprint is a match or a non-match [18]. Pictured below is a plot illustrating the distribution of similarity scores calculated by the scanner, with the "imposter" being a fingerprint not enrolled in the system, and a "genuine attempt" being a user already enrolled in the system:

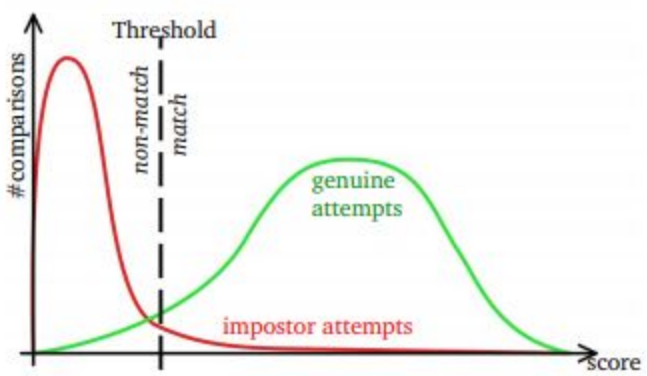

Fig. 8: Distribution of Scored by Attempt Type [18]

In this process, the hardware is bound to encounter errors and variation in the verification process. The most common type of error is a “false rejection,” in which the recognition system fails to verify a user, despite their registration in the system. This can happen for a myriad of reasons such as dirty, wet, or dry fingers, or a dirty or scratched sensor surface. Systems usually mitigate this error by rejecting the acquired image, and asking the user to rescan[19]. This is similar to what the design of this project intends to do, as each user will be given three attempts to access the machine. The metric used for the fingerprint error rate of false rejections is called FRR (false rejection rate). The hardware being used has an FRR of less than 1%, which falls within our tolerance threshold.

The other most common error is a “false acceptance,” in which the system falsely accepts an unregistered fingerprint scan, and grants the user access. This is a much more concerning error, as it allows an unauthorized user to gain access to the system. This occurs due to erroneous matching of a sample acquired for performing authentication with a stored template, which belongs to an authorized user [19]. The metric used for the fingerprint error rate of false acceptances is called FAR (false acceptance rate). The hardware being used has an FAR of less than 0.001%, which falls well within our tolerance threshold.

Errors caused in the matching process can be attributed to some common user disparities when using the hardware [20]:

- Finger rotation: Part of the fingerprint falls outside the sensor’s field of view, resulting in a smaller overlap between the stored template and the input fingerprint. For example, a finger displacement of 2mm results in a translation of about 40 pixels in the scanned fingerprint image.
- Non-linear distortion: The sensing process maps the 3-D image of the finger onto the 2-D surface of the sensor, which results in a non-linear distortion of the finger image.

- Differing pressure and skin condition: The finger being imaged is not always uniformly contacted with the sensor surface, and finger pressure, skin dryness, sweat, dirt, and grease confound the image acquisition.
- Feature extraction errors: The feature extraction algorithms are not foolproof, and can introduce measurement errors.

Luckily, the device hardware has algorithms aimed at mitigating these errors, and can be classified into three types of correction.

The first type of error correction is correlation-based matching, in which two fingerprint images are superimposed, and the correlation between corresponding pixels is computed for different displacements and rotations of the finger [20]. Mathematically, this is what the algorithm does:

Let $\mathbf{I}^{(\Delta x,\ \Delta y, \theta)}$ represent a rotation of the input image $\mathbf{I}$ by an angle θ around the origin (usually the image center) and shifted by Δx, Δy pixels in directions x and y, respectively; then the similarity between the two fingerprint images $\mathbf{T}$ and $\mathbf{I}$ can be measured as

$$S(\mathbf{T},\mathbf{I}) = \max_{\Delta x,\Delta y,\theta} CC\left(\mathbf{T},\mathbf{I}^{(\Delta x,\Delta y,\theta)}\right)$$

Eqn. 1: Correlation-based matching algorithm calculation [20]

Where $CC(T,I) = T^T I$ is the cross-correlation between T and I. [20]
However, the direction application of this method rarely leads to accurate results, due to computation size and external factors not considered by the algorithm, such as image brightness, contrast, and ridge thickness. For these reasons, another approach to fingerprint matching is used.

The most popular and widely used algorithm in fingerprint matching is the minutiae-based method, which is based off of fingerprint examination by professional fingerprint examiners. Minutiae are the major features of a fingerprint image, and are used in the matching process. A common fingerprint image can have 25 to 80 minutiae, defined as the points where fingerprint ridge lines end or fork [21]. Pictured below are common minutiae patterns that the algorithm searches for:

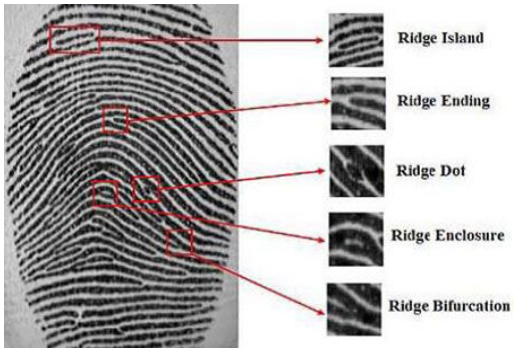

Fig. 9: Common Minutiae Patterns [21]

Within the algorithm, minutiae are extracted from the scanned image and stored image, and stored as sets of points in the 2-D plane. Each minutia is stored as a triplet:

$$m = \{x, y, \theta\}$$

Which indicates the x, y minuita location coordinates and the minuita angle θ. Then, using the same image **I** and **T** notations as in correlation, based matching, the following sets are formed:

$$\mathbf{T} = \{\mathbf{m}_1, \mathbf{m}_2, ..., \mathbf{m}_m\}, \quad \mathbf{m}_i = \{x_i, y_i, \theta_i\}, \quad i = 1..m$$
$$\mathbf{I} = \{\mathbf{m}'_1, \mathbf{m}'_2, ..., \mathbf{m}'_n\}, \quad \mathbf{m}'_j = \{x'_j, y'_j, \theta'_j\}, \quad j = 1..n,$$

Eqn 2a, 2b: Sets of minutiae for two images Defining the coordinate system used to identify minutiae [20]

From this, the spatial difference (sd) and direction difference (dd) are calculated. The sd must be below a given tolerance r_0, and the dd must be below a given tolerance θ_0.

$$sd(\mathbf{m}'_j, \mathbf{m}_i) = \sqrt{(x'_j - x_i)^2 + (y'_j - y_i)^2} \leq r_0,$$
$$dd(\mathbf{m}'_j, \mathbf{m}_i) = \min(|\theta'_j - \theta_i|, 360° - |\theta'_j - \theta_i|) \leq \theta_0$$

Eqn 3a, 3b: Calculating the spatial difference and direction difference [20]

A minutia $\mathbf{m}'_j$ in **I** and a minutia $\mathbf{m}_i$ in **T** are considered "matching," if the *spatial distance* (*sd*) between them is smaller than a given tolerance r_0 and the *direction difference* (*dd*) between them is smaller than an angular tolerance θ_0:

If the scanned fingerprint is rotated compared to the stored image, the two images need to be aligned to be properly compared.

Let map(.) be the function that maps a minutia m_j' (from **I**) into m_j'' according to a given geometrical transformation; for example, by considering a displacement of [Δx, Δy] and a counterclockwise rotation θ around the origin:

$$map_{\Delta x,\Delta y,\theta}\left(\mathbf{m}'_j = \{x'_j, y'_j, \theta'_j\}\right) = \mathbf{m}''_j = \{x''_j, y''_j, \theta'_j + \theta\},$$

$$\begin{bmatrix} x''_j \\ y''_j \end{bmatrix} = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} \begin{bmatrix} x'_j \\ y'_j \end{bmatrix} + \begin{bmatrix} \Delta x \\ \Delta y \end{bmatrix}.$$

Eqn. 4: Mapping minuita from the original image to the aligned image [20]
Eqn. 5: Coordinate transformation to align minuita [20]

Let mm(.) be an indicator function that returns 1 in the case where the minutiae m_j'' and m_i match:

$$mm\left(\mathbf{m}''_j, \mathbf{m}_i\right) = \begin{cases} 1 & sd\left(\mathbf{m}''_j, \mathbf{m}_i\right) \le r_0 \quad \text{and} \quad dd\left(\mathbf{m}''_j, \mathbf{m}_i\right) \le \theta_0 \\ 0 & \text{otherwise.} \end{cases}$$

Eqn 6: Indicator function to determine if minutiae from two fingerprint images are a match [20]

Lastly, the matching can be finalized and formulated as:

$$\underset{\Delta x,\Delta y,\theta,P}{\text{maximize}} \sum_{i=1}^{m} mm\left(map_{\Delta x,\Delta y,\theta}\left(\mathbf{m}'_{P(i)}\right), \mathbf{m}_i\right)$$

Eqn. 7: Finalized matching formula [20]

Where P(i) is an unknown function that determines the pairing between **I** and **T** minutiae. Each minuita has either exactly one mate in the other fingerprint, or no mate at all [20].

Visually, this is what this looks like:

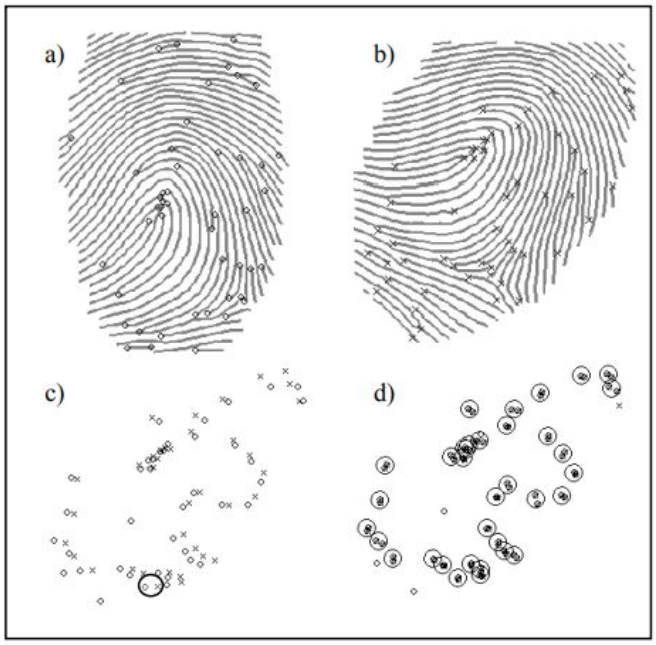

Fig. 10: Minutiae Matching [20]

A. Minutiae extracted from the stored fingerprint
B. Minutiae identified on the input fingerprint
C. Minutiae superimposed
D. Each circle denotes a pair of minutiae as mated by the algorithm

We are relying on this algorithm implemented on our hardware's AS608 chip to correctly match fingerprints, reject imposters, and accept verified users. Because of this sophisticated and high accuracy algorithm, our project's tolerance of 95% success in the fingerprint scanner's ability to overcome FAR and FRR is acceptable, and will allow the project to be considered a success.

3. Costs

Labor

Our fixed development costs are estimated to be $40 per hour, 8 hours per week for three people, for a 16-week semester. This neglects the eventual cooperation and partnerships with local governments to implement the system, and gathering biometric information from voters. Our costs will account for 80% of the final design neglecting the extra costs.

$$3\ people * \$40/hr * 8hr\ /week * 16wk/0.8 * 2.5 = \$48,000$$

We also must include machine shop labor, as they will be building the physical component of our design:

$$1\ person * \$30/hr * 10hrs\ total\ (design\ and\ manufacturing) = \$300$$

Parts

Part	Manufacturer	Part #	Quantity	Cost (prototype)	Cost (bulk)
Optical fingerprint reader	Geekstory via Amazon	N/A	1	$18.88	$7.23
Mini thermal receipt printer	Adafruit Industries LLC via Digi-Key	597	1	$49.95 (not accounted for in personal costs, covered by ECE senior lab)	$39.96
5.0” 40-pin 800x400 TFT Display	Adafuit Industries LLC	1680	1	$29.95	$23.96
RA8875 Driver Board for 40-pin TFT Display	Adafruit Industries LLC	1590	1	$34.95	$27.96

Buzzer	Adafruit Industries LLC via Mouser	1536	1	$0.95	$0.76
Arcade Push Button	Easyget via Amazon	N/A	3	$7.50	$6.00
ATMEGA328P-PU microcontroller	Microchip Technology via Digi-Key	ATMEGA328P-PU	1	$2.52	$2.09
PCBs	PCBWay	N/A	1	$5.00 (estimate)	$1.00 (estimate)
Associated resistors, capacitors, ICs, crystals, diodes	Via Digi-Key	N/A		$10.00	$0.50
Power supply	JOVNO via Amazon	N/A	1	$4.99	$0.99
Wood (physical build)	ECE Machine Shop	N/A	N/A	$20.00 (estimate)	$2.00 (estimate)
TOTAL				**$184.69**	**$112.45**

Labor and parts included, the development of the prototype of this project comes out to a total sum of $48,484.69.

4. Schedule

Week	Ashwin	Brennan	Jeremiah
2/28	- Design document	- Order parts - Schematics version 1 - Design document	- Design document - Start board layout
3/7	- Testing code for parts that have delivered so far	- Order rest of parts - Breadboard unit testing for delivered parts - Schematics version 2	
3/14	- Program functionality to take care of fingerprint inputs and how the buzzer and LEDs relatively	- Improve schematics (if needed) - Help Jeremiah with board layout	- Finalize board layout
3/21	- Program functionality to take care of buttons and screen - Program receipt printer functionality to print out voter selections	- Finalize physical design with machine shop - Test power supply equipment, ensure power requirements met	- Order PCB, ensure passes Audit - Order components for PCB
3/28	- Debug any edge cases and issues that arise - Finish up any handling of buttons, LEDs, buzzer, fingerprint scanner, receipt printer, or any miscellaneous items.	- Install hardware into physical design - Version 2 PCB design (if needed)	- Solder components to PCB - Check connections
4/4	- Debug any	- Order version 2	- Integrate all

	edge cases and issues that arise - Finish up any handling of buttons, LEDs, buzzer, fingerprint scanner, receipt printer, or any miscellaneous items.	PCB (if needed) - Integrate all hardware into physical design with PCB	hardware into physical design with PCB - Debug
4/11	- Finalize all testing, make sure system is “hack-proof”		
4/18	- Mock demo - Make changes to demo where feedback is given		
4/25	- Finalize demo - Write final paper		
5/02	- Perfect Presentation - Finish final paper		

5. Ethics and Safety

One of the biggest ethical issues facing this project is the possibility of a person's name being linked to their ballot submission. In person ballots cast in the US have to follow a style of ballot called the "Australian Ballot." The qualifications of an "Australian Ballot" means they must be printed by the government, contain all candidates, distributed at a polling place and marked in secret [10]. Therefore, our system must protect the privacy of voters to abide by state laws in the US. The machine protects against this by not storing the persons votes locally on the machine and only printing out the results on the receipt printer. This is done in order to abide by article 1, section 1 of the IEEE code of ethics which states members of IEEE are to uphold and "protect the privacy of others" and abide by state laws [8]. Once someone has voted, we will not store who they have voted for since this is a privacy concern, but simply print out a receipt with the voting results to be dropped in the "ballot box." People who don't have their fingerprints registered with the government would have the option to register them for free when they register to vote. If they would prefer to use traditional forms of ID (drivers license, state ID, passport, etc) they can choose to do so.

There are also potential ethical concerns about the security and data protection of the fingerprint information. In quite a few states, voter information is public or can be purchased from the state government at a specified cost. However, in all states, sensitive information like a person's social security number is redacted [22]. Similarly, a person's fingerprint information would be hidden and not available.

A common stigma surrounding fingerprints is that they are thought to be only used when crimes are committed or as some level of security clearance. Because of this, fingerprinting individuals has some negative connotations surrounding it. A commonplace example of fingerprints being collected is by the Department of Homeland Security from international visitors to verify identity [23]. Also, states like Texas, California, Utah, Colorado, Hawaii and Georgia all require fingerprinting in order to get or renew their driver's license [24]. Despite this being a common practice in these states, there is still some question on the constitutionality of requiring fingerprints for drivers license. According to one lawyer, there could be an argument that this requirement is in violation of "due process" rights guaranteed by the Fifth and Fourteenth Amendments [24]. In order to not risk potential constitutional conflicts, this system would be used in addition to traditional registration and voting methods. That way, people are not forced to register their fingerprints.However, if they would like to use this free method of registering to vote and voting, then they would have to submit their fingerprints upon registration.

A current voting system in the US is a line of voting machines and ballot counting machines built and designed by Dominion. Before they can be used, voting systems need to be certified by the U.S. government and not rely on the internet for use [25]. The software and hardware components are submitted to test labs to ensure their security. After being approved federally, voting machines need to be certified on a state and county level [25]. If put into common practice, our system would also have to be certified in a similar manner before being used in elections.

References

[1] "ATMEGA328P-PU", *digikey.com*, 2021. [Online]. Available: https://www.digikey.com/en/products/detail/microchip-technology/ATMEGA328P-PU/1914589?s=N4IgTCBcDaIIYBcC2BTA5nAzGAHABwFo8BXEAXQF8g. [Accessed: 04- Mar- 2021]

[2] "UA7805CKCT", *mouser.com*, 2021. [Online]. Available: https://www.mouser.com/ProductDetail/Texas-Instruments/UA7805CKCT?qs=l6ZoeTYLMwMYqlaPjFFaBg%3D%3D&mgh=1&gclid=Cj0KCQiA4feBBhC9ARIsABp_nbXT4PEnPq_BgtRVFp0JFS0EaHrkPhpWebB9vgJVZW58qjE279cOfAkaAksNEALw_wcB. [Accessed: 04- Mar- 2021]

[3] "5.0 40-PIN 800X480 TFT DISPLAY", *digikey.com*, 2021. [Online]. Available: https://www.digikey.com/en/products/detail/adafruit-industries-llc/1680/10670023. [Accessed: 04- Mar- 2021]

[4]"RA8875 Driver Board for 40-pin TFT Touch Displays - 800x480 Max", *Adafruit.com*, 2021. [Online]. Available: https://www.adafruit.com/product/1590. [Accessed: 18- Feb- 2021].

[5]"Mini Thermal Receipt Printer", *Adafruit.com*, 2021. [Online]. Available: https://www.adafruit.com/product/597. [Accessed: 18- Feb- 2021].

[6]"Optical Fingerprint Reader Sensor", *Amazon.com*, 2021. [Online]. Available: https://www.amazon.com/gp/product/B07BQ9VNWR/ref=vp_c_AISVZPAOFZQXX?ie=UTF8&m=A1GUQD3SRXOFFI. [Accessed: 04- Mar- 2021]

[7]"Adafruit Accessories Buzzer 5V", *mouser.com*, 2021. [Online]. Available: https://www.mouser.com/ProductDetail/Adafruit/1536?qs=GURawfaeGuBH8sXw8BXHwg%3D%3D&mgh=1&gclid=CjwKCAiAmrOBBhA0EiwArn3mfC5ZCV1S6u5sI_nAF_xvolSuCzrGVrj3Ezg4_ssEF6eUC5zKGi9L8xoCJQgQAvD_BwE. [Accessed: 18- Feb- 2021].

[8]"IEEE Code of Ethics", *ieee.org*, 2016. [Online]. Available: http://www.ieee.org/about/corporate/governance/p7-8.html. [Accessed: 17- Feb- 2021].

[9]"US election 2020: Fact-checking Trump team's main fraud claims", *BBC News*, 2021. [Online]. Available: https://www.bbc.com/news/election-us-2020-55016029. [Accessed: 18- Feb- 2021].

[10]"Australian ballot | politics", *Encyclopedia Britannica*, 2021. [Online]. Available: https://www.britannica.com/topic/Australian-ballot. [Accessed: 18- Feb- 2021].

[11]"Are Voter ID Laws The New Poll Tax?", *Truth Be Told*, 2018. [Online]. Available: https://truthbetold.news/2018/11/are-voter-id-laws-the-new-poll-tax/. [Accessed: 01- March- 2021].

[12]"Voter fraud is real, just not on the scale claimed by Trump", *the CT Mirror*, 2020. [Online]. Available: https://ctmirror.org/2020/11/13/voter-fraud-is-real-just-not-on-the-scale-claimed-by-trump/. [Accessed: 01- March- 2021].

[13]"ATMEGA328P Pinout, Programming, Features, and Applications", *Microcontrollers Lab*, 2021. [Online]. Available: https://microcontrollerslab.com/atmega328p-microcontroller-pinout-prograammi ng-features-datasheet/. [Accessed: 04- Mar- 2021]

[14]"Cairoduino-PCB", *GitHub*, 2021. [Online]. Available: https://github.com/ahmedibrrahim/Cairoduino-PCB/tree/master/Ahmeduino/Ah meduino%20Board. [Accessed: 04- Mar- 2021]

[15]"ATmega328P Standalone Board", *Arduino Project Hub*, 2021. [Online]. Available: https://create.arduino.cc/projecthub/ahmedibrrahim/atmega328p-standalone-bo ard-77044d. [Accessed: 04- Mar- 2021]

[16]"NIST Study Shows Computerized Fingerprint Matching Is Highly Accurate", *NIST*, 2021. [Online]. Available: https://www.nist.gov/news-events/news/2004/07/nist-study-shows-computerize d-fingerprint-matching-highly-accurate. [Accessed: 04- Mar- 2021]

[17]"Fingerprint Biometric Systems and their Accuracy", *Bayometric*, 2021. [Online]. Available: https://www.bayometric.com/fingerprint-biometric-systems-and-their-accuracy/. [Accessed: 04- Mar- 2021]

[18]"Understanding Biometric Performance", *Precisebiometrics.com*, 2021. [Online]. Available: https://precisebiometrics.com/wp-content/uploads/2014/11/White-Paper-Unders tanding-Biometric-Performance-Evaluation.pdf. [Accessed: 04- Mar- 2021]

[19]"How Accurate are today’s Fingerprint Scanners?", *Bayometric*, 2021. [Online]. Available:

https://www.bayometric.com/how-accurate-are-todays-fingerprint-scanners/. [Accessed: 04- Mar- 2021]

[20]"A Tutorial on Fingerprint Recognition", *Cedar.buffalo.edu*, 2021. [Online]. Available: https://cedar.buffalo.edu/~govind/CSE666/fall2007/FP_Tutorial.pdf. [Accessed: 04- Mar- 2021]

[21]"Minutiae Based Extraction in Fingerprint Recognition", *Bayometric*, 2021. [Online]. Available: https://www.bayometric.com/minutiae-based-extraction-fingerprint-recognition/#:~:text=Minutiae%20points%20are%20the%20major,uniqueness%20of%20a%20fingerprint%20image.&text=matching%20of%20fingerprints.-,These%20minutiae%20points%20are%20used%20to,uniqueness%20of%20a%20fingerprint%20image. [Accessed: 04- Mar- 2021]

[22]H. McDonnell, "Closing in on the US election with voter privacy and election security", *Iapp.org*, 2020. [Online]. Available: https://iapp.org/news/a/closing-in-on-the-u-s-election-with-voter-privacy-and-election-security/. [Accessed: 03- Mar- 2021]

[23]Department of Homeland Security, "New Biometric Technology Improves Security and Facilitates U.S. Entry Process for International Travelers", Department of Homeland Security, 2008.

[24]T. Dodrill, "States Now Demanding Fingerprints From (Pretty Much) Every Adult - Off The Grid News", *Off The Grid News*. [Online]. Available: https://www.offthegridnews.com/privacy/states-now-demanding-fingerprints-from-pretty-much-every-adult/#:~:text=Other%20states%20which%20mandate%20the,Colorado%2C%20Hawaii%2C%20and%20Georgia. [Accessed: 03- Mar- 2021]

[25]"Elections 101: About Dominion Voting Systems - Dominion Voting Systems", *Dominion Voting Systems*. [Online]. Available: https://www.dominionvoting.com/elections-101-about-dominion-voting-systems/. [Accessed: 03- Mar- 2021]

[26]"High definition 40 pin 800x480 5 inch LCD display module", *Alibaba*. [Online]. Available:

https://weshare.en.alibaba.com/product/60760120417-804174267/High_definition_40_pin_800x480_5_inch_LCD_display_module.html[Accessed: 08- Mar- 2021]