Fingerprint Protected Voting Machine

By

Ashwin Dandapani

Brennan Hartigan

Jeremiah Kennedy

Final Report for ECE 445, Senior Design, Spring 2021

TA: Dean Biskup

5 May 2021

Project No. 68

Abstract

Our project is a Fingerprint Protected Voting Machine. The features of our machine are a fingerprint scanner, LEDs, a buzzer, an LCD display, buttons to navigate the user interface, and a thermal receipt printer. Together, these hardware devices, along with the software work together to create a near seamless voting experience, with less human interaction and more ease of use during the voting process. The device will not let a voter vote twice as it keeps track of who has voted based on their fingerprint. In addition, the system will ”lock out” any voter who tries to access the machine and is denied three consecutive tries. At the conclusion of this project, we found that voting using a biometric ID is an extremely efficient way of voting, and could help to dispel claims of voter fraud and give more access to voting to those who cannot afford a government ID.

Contents

1 Introduction . . . 1
1.1 Objective . . . 1
1.2 Background . . . 1
1.3 Project Summary . . . 2
1.4 High-Level Requirements . . . 2
2 Design . . . 3
2.1 Power Supply . . . 5
2.1.1 AC to DC Converter . . . 5
2.1.2 Voltage Regulators . . . 5
2.2 Control Unit . . . 5
2.3 Input Devices . . . 6
2.3.1 Fingerprint Scanner . . . 6
2.3.2 Input Controller . . . 7
2.4 Display . . . 7
2.4.1 5.0” 40-pin TFT Display . . . 7
2.4.2 RA8875 TFT Display Driver Board . . . 7
2.5 System Indicators . . . 7
2.5.1 LEDs . . . 8
2.5.2 Piezo Buzzer . . . 8
2.6 Recorded Vote Output . . . 8
2.7 PCB . . . 8
2.8 Software . . . 9
3 Design Verification . . . 10
3.1 Functional Tests . . . 10
3.1.1 Access Granted . . . 10
3.1.2 Button Usage . . . 10
3.1.3 Ballot Printing . . . 10
3.1.4 Security Features . . . 10
3.2 Fingerprint Scanner Reliability Tests . . . 11
3.3 PCB Testing Procedures . . . 11
3.3.1 LEDs . . . 11

3.3.2 Buttons . . . 11
3.3.3 Thermal Receipt Printer, Fingerprint Scanner and Display . . . 12
3.3.4 PCB Conclusions . . . 12
4 Cost . . . 13
4.1 Parts . . . 13
4.2 Labor . . . 13
4.3 Total Costs . . . 13
5 Conclusion . . . 15
5.1 Accomplishments . . . 15
5.2 Uncertainties . . . 15
5.3 Ethical considerations . . . 15
5.4 Future work . . . 16
Appendix A Requirement and Verification Table . . . 19

1 Introduction

1.1 Objective

The 2020 Presidential Election, one of the most contentious in American history brought voter fraud and questioning the integrity and security of our elections to the forefront of the news cycle [1]. This project aims to attempt to help or fix this problem, and guarantee complete security in elections, whether related to concerns about people voting more than once, or committing voter fraud by voting under the identity of someone other than themselves. One effective tool to uniquely identify voters and prevent voters from re-voting is to use each voter's fingerprint as a form of biometric identification. Since each fingerprint is unique to a person, there will not be an opportunity to fake your eligibility or your name when voting.

The team's plan is to utilize fingerprint identification to confirm that a voter has not voted previously to keep the voting fair. Our product works by scanning in a voter's fingerprint, determining eligibility from their biometric ID, and either granting or restricting access to voting on the device. Once a registered voter has been given access, they can select the candidate of their choice using buttons mounted on the machine, and receive a printed ballot that will be deposited in a ballot box for later counting. This way, the vote is still private, but the process is secure.

1.2 Background

The 2020 presidential election was littered with claims about potential voter fraud. This is something the team felt that could 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'" [1]. While this has been widely disproved, this project aims to silence any such claims from arising, due to the security of our product and its ability to uphold integrity in elections.

While there has been plenty of dispute over these claims, voter fraud is, in fact, very rare and unlikely, but it has been documented in the past in smaller scale elections [2]. Whether the Trump Campaign's claims are accurate or not, by having this more robust and accessible voter identification through fingerprints, the machine 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 using a fingerprint, and not a government-issued voter identification card. 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 [3], with this unequal opportunity to vote being labeled a "modern day poll tax."

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 [3]. 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 that is fair for all who participate.

1.3 Project Summary

In this report we are going to discuss our voting machine project that we worked on throughout this semester. Throughout this project we came across many challenges that we had to work through along with new ideas that we utilized to make the project as useful as possible. We feel that our final product that we have completed is ultimately a very useful device to replace the current voting process and prevent questions that might arise about voter fraud. With this device, it make the process of voting simple and user friendly, but also makes note of when a registered voter has already voted through their fingerprint's unique identification. It only allows the voter to vote, if their fingerprint has been registered and the voter has not already voted.

This report will highlight the design and hardware choices the team made to ultimately produce our product. The verification of the design through testing will be detailed, as well as the total costs and labor needed to produce a prototype, as well as a mass-produced version of the machine. The report will conclude with our accomplishments, some ethical considerations, and future work that can be done to improve the device.

1.4 High-Level Requirements

Listed below are the high-level requirements for this product, as this report will explore how these requirements were met throughout the design process.

1. 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 acceptance accuracy of 95%.

2. 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.

3. 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

The design of this project is meant to make the voting process as easy as possible for the voter, with audio and visual feedback given during the voting process, and the overall flow made nearly seamless. The added security features in the software make our prototype a very secure voting machine that is easy to navigate by all voters.

Figure 1 shows the front view of the physical design, with individual hardware labeled. When the device is given power, the screen will illuminate showing the "welcome" message as seen in Figure 2. The fingerprint scanner will begin scanning for a fingerprint image, and will remain doing so until a voter places their fingerprint on the scanner. Figure 3 shows the rear view of the physical design. Unfortunately, the PCB for this project did not end up working, as the team faced a slew of shipping delays and back-orders on parts. The physical design of this project is something very close to what we would want to use in a final, mass-production design. The team considered using a larger display or more powerful fingerprint scanner; however, costs were cut for the purposes of this project.

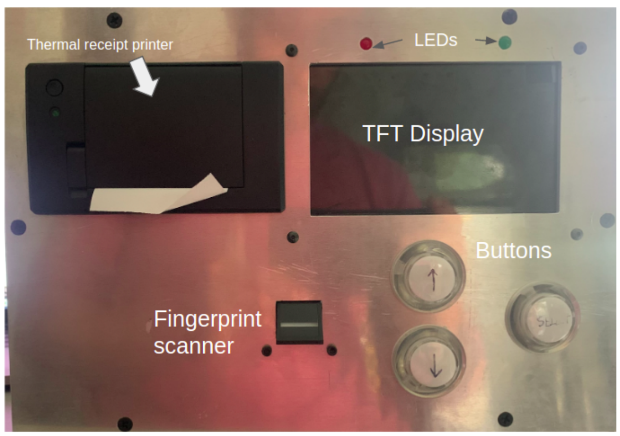

Figure 1: Front view of the physical design

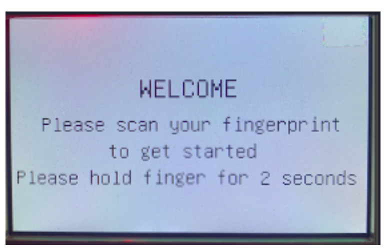

Figure 2: Welcome screen at the start of the voting process

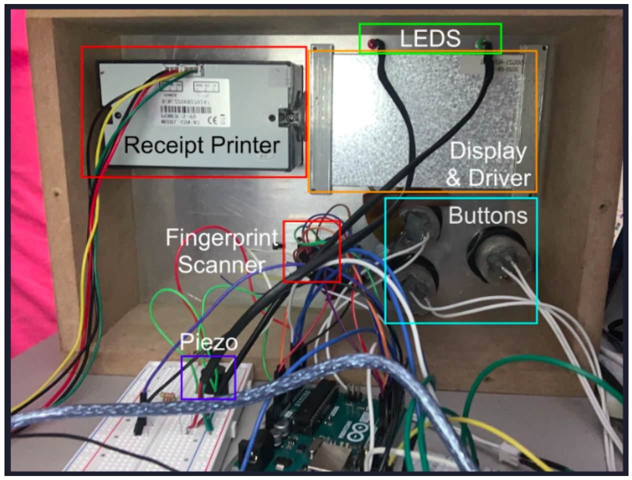

Figure 3: Back/interior view of the physical design

Figure 4 shows the block diagram for the design of the overall system. As seen on the block diagram, there are six major subsystems, each containing their own subcomponents that work together to accomplish voting securely on the machine. Each block was tested and verified to the standards set in Table 2, which will be discussed more in detail. The block diagram shows that the main modes of communication between the devices are digital signals, TTL Serial, and SPI.

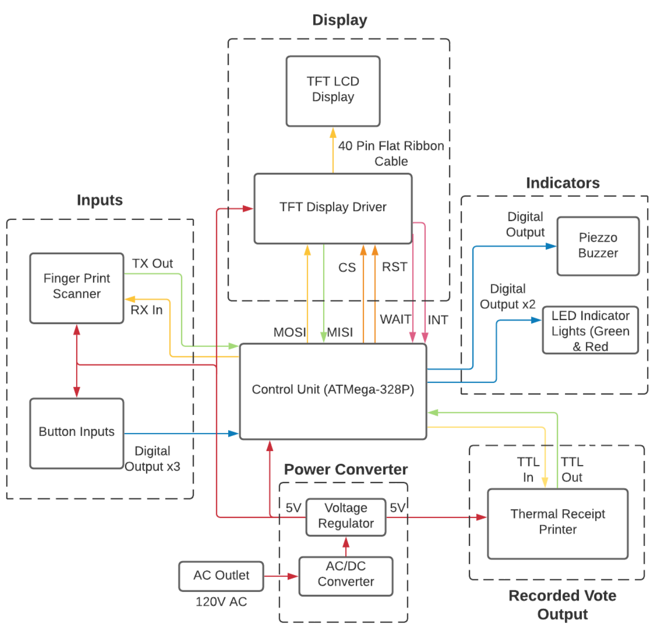

Figure 4: Block diagram

The individual subsystems and their components in this design will now be explored:

2.1 Power Supply

A power supply is required to keep the voting machine and all hardware peripherals running and operating as normal during the use of the machine. We challenged ourselves to use a power supply that would be able to plug into a wall outlet (rather than a lab power supply) to demonstrate the versatility of our design, and that it could be used in any setting that has access to a wall outlet.

Figure 5 shows the schematics of the power supply, with a power jack input and voltage regulators to power the system.

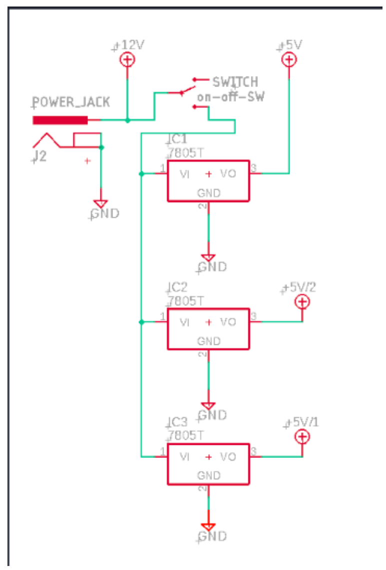

Figure 5: Power supply schematics

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 120 V AC standard wall outlet, and convert the power to DC voltage so the hardware in the project can be powered correctly. The AC to DC converter steps down the 120 V AC power to 12 V 5 A power, which can be handled by the system voltage regulators. The requirements for this component, as well as the verification steps can be found in table 2.

2.1.2 Voltage Regulators

Three 5 V, 1.5 A voltage regulators are used to distribute power among the hardware devices used in the system. Texas Instruments' UA7805CKCT linear voltage regulators were chosen for this project. The team chose to use these ICs as they are LDO regulators, which are more stable, highly accurate, and low-noise than other types of voltage regulators [4]. The requirements for this component, as well as the verification steps can be found in Table 2.

2.2 Control Unit

The control unit is the main processing unit for all inputs and outputs of the machine. The control unit, made up of an ATmega328P-PU microcontroller [5] handles all inputs from people (selection buttons), sensors (fingerprint scanner), and display feedback to the voter on the LCD display. The control unit will also process outputs to the voter, such as the LED indicators, buzzer, and thermal receipt printer. Figure 6 shows the schematics of the control unit. To the left of the microcontroller are circuits to keep the microcontroller powered, as well as a 16 MHz clocking circuit that allows the microcontroller to be run at twice its internal clock speed of 8 MHz. To the right of the microcontroller are the hardware peripherals used in this project, and their connections to the microcontroller.

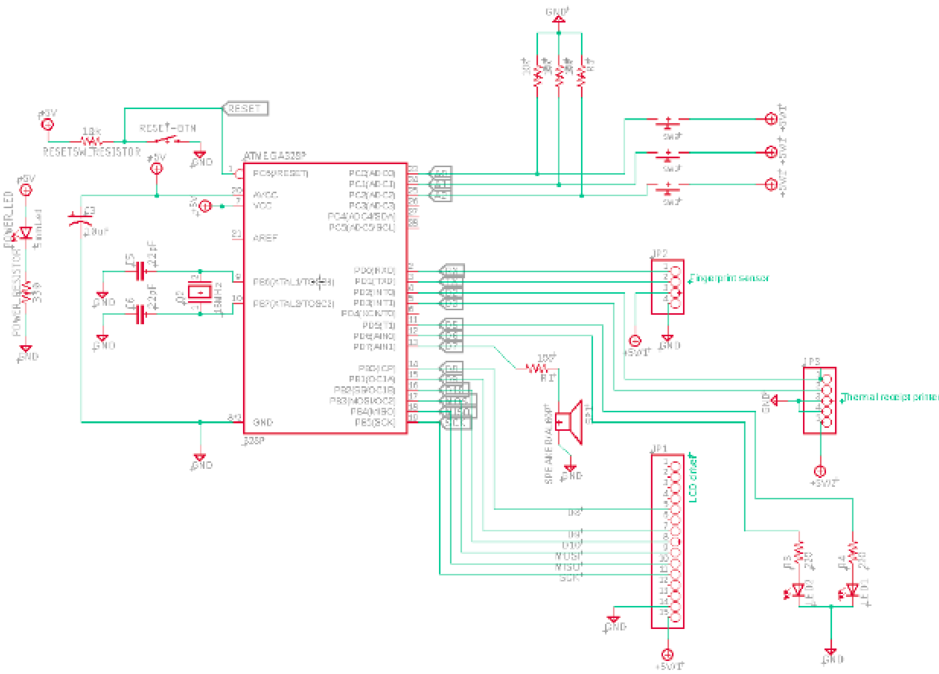

Figure 6: Control Unit schematics

The team chose the ATmega328P-PU microcontroller for this project because it is a very low-cost, multi-purpose microcontroller that can be used in a variety of settings. The most important characteristic of this microcontroller is that it can be bootloaded for use with the Arduino IDE, which makes writing software and uploading software to the microcontroller very easy. In addition, there is a myriad of resources online for the ATmega328P-PU, which was especially useful in troubleshooting and debugging our project. Being able to use Arduino and the Arduino IDE proved to be very useful in prototyping and testing the project, and ultimately demonstrating the project, as the PCB failed to come to completion.

The requirements for this component, as well as the verification steps can be found in Table 2.

2.3 Input Devices

2.3.1 Fingerprint Scanner

The team chose to use a generic project fingerprint scanner that could communicate with the microcontroller over UART, for the purposes of the scope of this project [6]. The AS608 chip on the device, which does all the major calculations and operations in fingerprint scanning, matching, and feature detection can hold up to 128 fingerprints in its internal memory. For a large-scale operation, a fingerprint scanner with a much larger memory, or a separate system would be needed for a larger population's biometric data. However, in terms of cost and functionality, this device worked perfectly, and exceeded our goal of 95% accuracy (see Section 3.2). In addition, an important advantage of this device is that it is compatible with the Arduino IDE, as Adafruit has a fingerprint sensor library [7] that makes interacting software with the hardware quite simple. The requirements for this component, as well as the verification steps can be found in Table 2.

2.3.2 Input Controller

The input controller for the machine is made up of three large, arcade-style push buttons [8] that allow the user to navigate the candidate selection process: two buttons for scrolling up and down, and a third to make a candidate selection. In the design process, the team chose these types of buttons because they are much sturdier than normal PCB pushbuttons, and are reliable in terms of debouncing and indicating to the microcontroller a ”press” and ”release.” In addition, these buttons mounted very nicely to our physical design, and should be very usable for all voters. The requirements for this component, as well as the verification steps can be found in Table 2.

2.4 Display

2.4.1 5.0” 40-pin TFT Display

The display in this design is a 5-inch LCD display, with a bright backlight and high resolution (800x400) that can be visible in a variety of settings, no matter what venue the voting is taking place at [9]. The display communicates each step of the voting process to the user, and is the main output source for the overall user interface. The requirements for this component, as well as the verification steps can be found in Table 2.

2.4.2 RA8875 TFT Display Driver Board

This driver board, which connects to the display via a 40-pin ribbon cable is necessary for the correct operation and programming of the main display, as well as interacting the display with the microcontroller [10]. The driver board is needed to refresh the display at our desired 60 Hz, as well as maintain a constant 5-9 V 125-150 mA input to the display, so it can maintain its bright backlight. In addition, the RA8875 chip on the driver board handles all RAM for the display, as well as the timing requirements for changing the display throughout the program. The RA8875 handles these functions in the background, so they do not have to be directly implemented in the software.

This combination of driver board and display was chosen especially due to the hardware’s compatibility with the Arduino IDE, as there is are Arduino libraries for use with the RA8875 board and displaying graphics on the display [11] [12]. This made working with the display and creating images for the display not terribly challenging.

The requirements for this component, as well as the verification steps can be found in Table 2.

2.5 System Indicators

The system indicators give audio and visual feedback to the user as they work their way through the voting process.

2.5.1 LEDs

LEDs are used to signal "access granted" and "access denied" to the user. The GREEN LED will illuminate for the entire duration of the voting process once a verified user has accessed the candidate selection. The RED LED remains on whenever the machine has not been accessed, and remains on until a registered voter has been granted access. The requirements for this component, as well as the verification steps can be found in Table 2.

2.5.2 Piezo Buzzer

The team chose to use a Piezo buzzer, model PS1240 [13] that will buzz whenever a user is denied access to the machine. This adds the extra element of audio feedback when a user is denied access, whether they are not registered in the system, or they need to re-try their fingerprint scan due to their finger or the scanner plate being dirty. The requirements for this component, as well as the verification steps can be found in Table 2.

2.6 Recorded Vote Output

To produce a record of a voter's vote, the team decided to use a mini thermal receipt printer [14]. After a voter has selected a candidate, the display prompts them to wait until their ballot is printed, which is then intended to be dropped in a ballot box for counting later. This way, the vote remains completely anonymous, as the voter's name or identification is not associated with the vote. Figure 7 shows an example of a ballot receipt that would print after a vote has been cast:

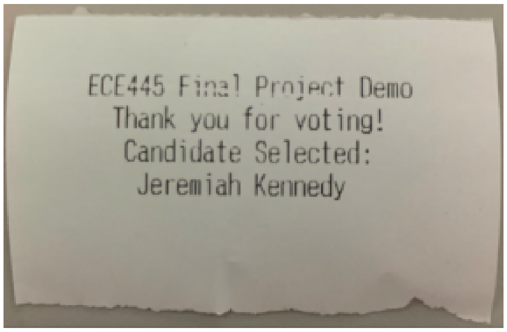

Figure 7: Example ballot receipt

One advantage of this piece of hardware is that it is intended for use with the Arduino IDE for programming, and has its own library in the IDE [15]. This allowed the team to interact with the printer and try many different fonts, styles, and outputs before deciding on the final ballot look. The requirements for this component, as well as the verification steps can be found in Table 2.

2.7 PCB

The PCB was designed around the bare minimum components needed for the microcontroller to function as it does on an Arduino board [16] [17] [18] to make the device easy to program and debug, as all prototyping and testing was done with an Arduino UNO. Figure 8 shows the finalized PCB:

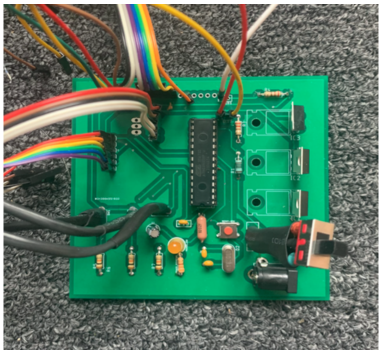

Figure 8: PCB

2.8 Software

The software for this project was written in C++ language, and compiled and uploaded using the Arduino IDE. Figure 9 shows the flowchart for the software implemented on the voting machine:

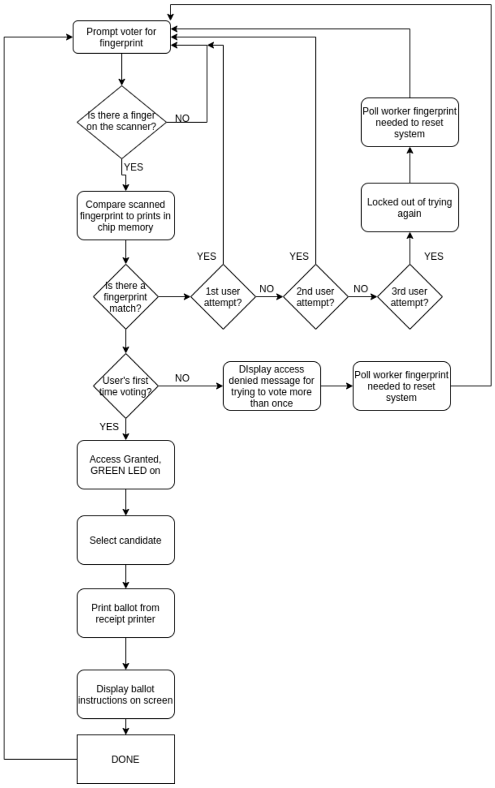

Figure 9: Software flowchart

3 Design Verification

The first set of tests performed were functional tests on the system. These were predominantly qualitative tests to ensure the code uploaded to the ATmega was working as expected. The team performed these tests multiple times and made tweaks to the code to achieve the desired outcome. The second set of tests were reliability tests for the fingerprint sensor. The team performed these tests to learn more about the fingerprint scanners consistency and accuracy. The last set of tests the team performed was to verify the functionality of the PCB. In the event that the PCB was not fully functional, an Arduino was used in its place.

3.1 Functional Tests

3.1.1 Access Granted

The first functional test performed was to ensure that the fingerprint scanner was granting access to voters with a matching fingerprint. If there was no match, a screen prompting the user to scan their fingerprint a second time would pop up. The team observed the display and since the correct messages were displayed, the system met the specified requirements and passed the test.

3.1.2 Button Usage

The team performed another functional test to verify the buttons worked correctly. The up and down arrows were clicked multiple times and the screen was observed to see if the system was responding correctly. The display switched between the candidates and the select button picked the currently highlighted candidate so this test was deemed a success.

3.1.3 Ballot Printing

The next functional test was printing the ballot from the thermal receipt printer and visually verifying all of the correct information was printed. The test also included visually verifying the system returned to the beginning of the voting process by displaying the initial welcome screen and the green LED turning off and the red LED turning on. The result of this test was a success on the breadboard and Arduino but did not function correctly on the PCB. The ATmega328P was not able to recognize the thermal receipt printer, or the display driver. The pins on the ATmega328P used for communication with these devices was potentially damaged during initial PCB testing.

3.1.4 Security Features

The last three functional tests all were used to verify some of the different security measures. The first test was related to having three incorrect fingerprint scans in a row. In the event of this, the screen displays a message instructing the voter to find a poll worker and locks the system until a poll worker provides an override fingerprint. To verify this functionality, three invalid fingerprints were scanned and the display was observed to make sure the system remained in the locked out state. Since this was observed, the test was deemed a success. The last functional test was to make sure the double voting preventative measures worked. For this test, a valid fingerprint was scanned and the voting process was completed. Then, the same fingerprint was used a second time to try and vote and the screen was observed to see if the ”You cannot vote more than once” message was displayed. Since the message was observed on the display, the voting machine passed this test as well.

3.2 Fingerprint Scanner Reliability Tests

The first reliability test verified that no non-registered fingerprints were granted access. A series of 100 non-registered fingerprints were scanned and out of the 100, 0 of those fingerprints were granted access. Additionally, throughout the testing process there was no event where an unregistered fingerprint was reported as a match to a registered one. The second reliability test determined the probability of different fingers failing the first scan try. For this test, 50 registered fingerprints were placed on the scanner individually. Figure 10 shows that out of all the fingerprints that failed on the first scan, the thumb tended to fail more often than other fingers.

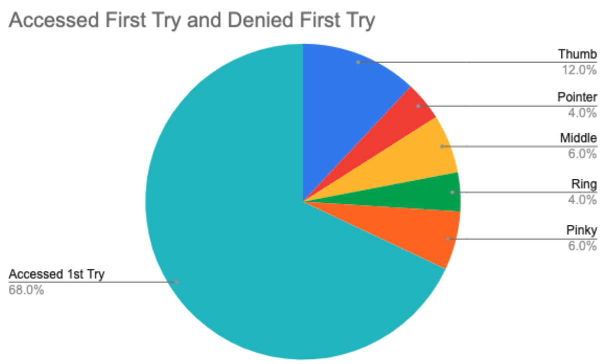

Figure 10: Valid Fingerprints Denied First Try

It should be noted that for this test, before each scan the finger was not cleaned or dried off in any way unless given an invalid scan. From a sample size of 50 trials, somewhat sweaty (a subjective metric) registered fingers were still able to scan successfully on the first try 68% of the time. The pointer and ring fingers failed on the first try roughly 4% of the time while middle and pinky fingers were approximately 6%. A potential reason for the thumb failing more often is because it is the largest finger, key fingerprint details might be off the scanner which results in an invalid scan. Out of all the attempts, a 3rd scan was only required 1-2% of time.

3.3 PCB Testing Procedures

3.3.1 LEDs

There were a series of tests performed on the PCB to check if it would work as a replacement for the Arduino. The first test consisted of uploading a program to the PCB which would flash the onboard LED. This was done to verify the serial connection to the board from the computer. After uploading the program the onboard LED would flash on and off indicating the test was a success. The LED testing also extended to the green and red LEDs used in the voting machine. Similar to the onboard LED test, the green and red LED test would turn each LED on and off alternating from each other. This test was a success because the PCB and code were successfully able to achieve the alternating flashing LEDs.

3.3.2 Buttons

This test verified the button functionality when connected to the PCB. When a button was pushed (closed position) the serial monitor would print out the number 1. Each button was working correctly since when pressed, "1" was printed.

3.3.3 Thermal Receipt Printer, Fingerprint Scanner and Display

When the team tried to test each of these components on the PCB, the serial monitor said it could not find any of the devices. There was some issue with the TX and RX ports on the ATmega328P so that the microcontroller could not communicate with each of the devices. Unfortunately, the team ran out of time trying to debug the issues with these devices before the demo and had to perform the demo using an Arduino instead of the PCB.

3.3.4 PCB Conclusions

While the LEDs and buttons worked as expected on the PCB, further investigation is required for the thermal receipt printer, fingerprint scanner and display. The devices worked properly with the Arduino so there is some disconnect between the hardware the team created on the PCB and the hardware on the Arduino. A bit more time in between PCB orders might have given more time to solve this issue.

4 Cost

4.1 Parts

Table 1: Parts Costs

Part	Manufacture	Retail Cost ($)	Bulk Purchase Cost ($)	Actual Cost ($)
Optical Fingerprint Reader	Geekstory	18.88	7.23	18.88
Mini Thermal Receipt Printer	Adafruit Industries	49.95	39.96	49.95
5.0” 40-pin 800x400 TFT Display	Adafruit Industries	29.95	23.96	29.95
RA8875 Driver Board	Adafruit Industries	34.95	27.96	34.95
PS1240 Piezo Buzzer	Adafriut Industries	0.95	0.76	0.95
Mini LED Arcade Button	Adafruit Industries	2.50 * 3 = 7.50	2.00 * 3 = 6.00	7.50
ATmega328P-PU Microcontroller	Microchip Technology	2.52	2.09	2.52
PCB	PCBWay	5.00	1.00 (estimate)	5.00
PCB Parts	Digi-key	11.78	3.92	11.78
Power Supply	JOVNO	4.99	0.99	4.99
Wood & metal	ECEB Machine Shop	20.00	5.00	20.00
Total	——	186.47	118.87	186.47

4.2 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 fingerprint information from voters. Our costs will account for 80% of the final design neglecting the extra costs:

$$3 \text{ people} * \$40/\text{hr} * 8 \text{ hr/week} * 16 \text{ weeks}/0.8 * 2.5 = \boxed{\$48,000}$$

We must also include the machine shop labor, as they did the design and build for the physical component of our project design:

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

4.3 Total Costs

Our total costs with labor and parts combined amounts to:

$$\$186.47 \text{ (parts)} + \$48{,}000 \text{ (engineering labor)} + \$300 \text{ (machine shop labor)} = \boxed{\$48,486.47}$$

If this product was to go into mass production, the total costs with the reduced bulk parts pricing amounts to:

$$\$118.87 \text{ (parts)} + \$48{,}000 \text{ (engineering labor)} + \$300 \text{ (machine shop labor)} = \boxed{\$48.418.87}$$

For comparison, brand new electronic voting machines cost within the $2,500-$3,000 range, with the optical scanning machines pricing at $5,000. With our design, we aim to reduce the overall cost of the voting hardware significantly, from up to $8,000 down to $118.87 (assuming bulk purchasing of the devices).

5 Conclusion

Ultimately, the team felt our project was very successful. The team was satisfied with what we produced to demonstrate what we had worked on throughout the semester. We feel that this system could be very beneficial if used in the future by the government.

5.1 Accomplishments

As for the accomplishments of the project, the team was able to get a complete project working. Unfortunately, due to memory constraints on the microcontroller, our receipt printer would not work during the demo, despite it working when we were testing previously. The team was able to properly showcase that the system can successfully recognize if a voter has already voted, and denies them access to the machine. The team was also able to show that the machine denies access if a fingerprint was not found for 3 attempts in a row. We were able to grant access and allow the voter to use the up and down buttons along with the select button to cast a vote for a candidate. The team also had the opportunity to add a ”poll worker override” on the machine, which was a design feature that we did not initially propose, but felt that it added security to the product.

5.2 Uncertainties

While the team is very happy with the design and low cost of our overall project, we are uncertain if the costs for employing and training poll workers for this new system will ultimately be feasible. Another concern that we have is the potential difficulties with getting voters to register their fingerprints well prior to voting.

5.3 Ethical considerations

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 [19]. 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 [20]. Once someone has voted, they system will not store who the voter has 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 [21]. 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 [22]. Also, states like Texas, California, Utah, Colorado, Hawaii and Georgia all require fingerprinting in order to get or renew their driver's license [23]. 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 [23]. 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 [24]. 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 [24]. Different states have different voting machine verification procedures. For example, Illinois requires all voting machines are tested to federal standards and must be tested by a federally accredited laboratory [26]. The first step in the process is the State Board of Elections accepts applications for new voting systems and conducts tests. After reviewing the system and the results, it writes to the Board and a hearing is conducted to discuss the new system [26]. If the board decides that this could be a efficient, safe and accurate system, the voting system is used but has a probationary period of two years [26]. The people advocating for the voting system could then apply for continued use and the Board has the power to make the decision based on past performance and current information [26]. This process is solely for the state of Illinois so to implement it elsewhere would require similar processes being executed in different states. For our system to be used in common practice it would also have to be certified in a similar manner before being used in elections.

5.4 Future work

We believe that completely altering the voting process would not be possible immediately, which is why we chose to use the receipt and still use a ballot box to count the votes. However, we do want to ultimately move the casting of votes to a secure database to prevent lost receipts and any other issues that can arise with paper ballots. In order to improve this, a plan we have is using a data storing service like Firebase to hold voters' information, whether they are registered, and if they have voted yet, given in a real election there will need to be many more fingerprints enrolled. We will be able to also use a database then to total the votes, but not keep record of who the voters voted for, but simply whether they have voted or not. Another future addition we would like to make is using a more accurate fingerprint scanner to prevent any potential mistakes and also expedite the voting process. With a more accurate scanner, there would be less need for multiple attempts or a poll worker override and this would make voting more efficient and allow votes to be cast faster.

References

[1] "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].

[2] "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].

[3] "Are Voter ID Laws The New Poll Tax?", Truth Be Told, 2018. [Online]. Available: and . [Accessed: 01- March- 2021].

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

[5] "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]

[6] "Optical Fingerprint Reader Sensor", Amazon.com, 2021. [Online]. Available: https://www.amazon.com/gp/product/B07BQ9VNWR/ref=vp_c_AISVZPAOFZQXX?ie=UTF8m=A1GUQD3SRXOFFI. [Accessed: 04- Mar- 2021]

[7] L. Fried, "adafruit/Adafruit-Fingerprint-Sensor-Library", GitHub, 2020. [Online]. Available: https://github.com/adafruit/Adafruit-Fingerprint-Sensor-Library. [Accessed: 13- Apr- 2021].

[8] A. Industries, "Mini LED Arcade Button - 24mm Translucent Clear", Adafruit.com, 2021. [Online]. Available: https://www.adafruit.com/product/3429?fbclid=IwAR2sASattClwhp46-8ujvciEGNss1B5_1_Eq6xBOTcsXaj4qSyjfnA_qUn8. [Accessed: 06- Apr- 2021].

[9] "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]

[10] "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].

[11] "adafruit/Adafruit_RA8875", GitHub, 2021. [Online]. Available: https://github.com/adafruit/Adafruit_RA8875. [Accessed: 13- Apr- 2021].

[12] "adafruit/Adafruit-GFX-Library", GitHub, 2021. [Online]. Available: https://github.com/adafruit/Adafruit-GFX-Library. [Accessed: 13- Apr- 2021].

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

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

[15] "adafruit/Adafruit-Thermal-Printer-Library", GitHub, 2021. [Online]. Available: https://github.com/adafruit/Adafruit-Thermal-Printer-Library. [Accessed: 06- Apr- 2021].

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

[17] "Cairoduino-PCB", GitHub, 2021. [Online]. Available: https://github.com/ahmedibrrahim/Cairoduino-PCB/tree/master/Ahmeduino/Ahmeduino

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

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

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

[21] 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]

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

[23] 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

[24] "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]

[25] S. Breitenback, "Aging Voting Machines Cost Local, State Governments", Pewtrusts.org, 2016. [Online]. Available: https://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2016/03/02/aging-voting-machines-cost-local-state-governments. [Accessed: 01- May- 2021].

[26] The U.S. Election Assistance Commission, "State Requirements and the U.S. Election Assistance Commission Voting System Testing and Certification Program", 2021.

Appendix A Requirement and Verification Table

Table 2: System Requirements and Verifications

Requirement	Verification	Verification status (Y or N)
1. AC to DC Converter (a) must be able to convert AC wall voltage to DC voltage, and step down the voltage to 12 V +/- 5% so it can be processed by voltage regulator ICs	1. AC to DC Converter (a) Use a voltmeter to ensure that the DC output is steady at within 5% of 12 V, which we will monitor for 15 seconds to confirm.	(a) Y
2. Voltage Regulator (a) The voltage regulator ICs must be able to handle incoming 12 V DC voltage from the wall. (b) Provides 5 V, 1.5 A +/- 5% from the 12V source	2. Voltage Regulator (a) The voltage regulator specifications indicate that it may receive a 12 V DC input (b) Using a multimeter, measure the output voltage and current and ensure that they are within 5% of the required 5 V, 1.5 A.	(a) Y (b) Y
3. Microcontroller (a) The microcontroller must be able to communicate over UART in order to process and transmit the input data from the fingerprint reader. (b) The microcontroller must be able to receive and send digital signals. (c) The microcontroller must be able to communicate over SPI in order to echo movements on the screen.	3. Microcontroller (a) i. 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. ii. Using example text specified in the software, send UART signals to the receipt printer to print out the example text. (b) i. The LED lights will receive digital signals and light up if a user is granted access or denied. ii. The buzzer will buzz if a user is denied. (c) The screen will respond to digital input signals from the buttons.	(a) Y (b) Y (c) Y

Continued on next page

Table 2 – continued from previous page

Requirement	Verification	Verification status (Y or N)
4. Input Controller Buttons (a) The buttons must be pressable and work on first attempt.	4. Input Controller Buttons (a) Use pushbutton example code on Arduino IDE to monitor button presses and ensure buttons can be pressed with each press and release accurately recorded.	(a) Y
5. Fingerprint Scanner (a) The scanner will have a less than 1 second fingerprint image acquisition time. (b) 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.	5. Fingerprint Scanner (a) The scanner is able to administer the fingerprint and decide a response in a second. The delay will be set in the software. (b) i. The scanner is able see a match in the system or if not it makes the user re scan. ii. The scanner is able to mention if the user needs to re-scan their finger after checking for a match.	(a) Y (b) Y
6. 5.0" 40-pin TFT Display & RA8875 Driver Board (a) The display will need 5-9V and 125-150mA input to maintain its backlight, so it is easy for users to read. (b) This driver will communicate with the microcontroller via SPI.	6. 5.0" 40-pin TFT Display & RA8875 Driver Board (a) Using the voltage regulator, ensure that this steady voltage can be maintained, while using resistors to adjust the current. (b) Connect to the microcontroller and send example images to the screen, ensuring that the data displayed matches the data sent.	(a) Y (b) Y

Continued on next page

Table 2 – continued from previous page

Requirement	Verification	Verification status (Y or N)
7. Piezo Buzzer (a) Output frequency should be at a minimum 1KHz, and maximum 4KHz	7. Piezo Buzzer (a) i. Use a frequency spectrum analysis application to measure the frequency produced by the buzzer. ii. Ensure that the buzzer's frequency matches the frequency specified by the software.	(a) Y (b) Y
8. LEDs (a) Turn on within 10 ms of access denied/granted. (b) 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. (c) Operate on a drive current of 10 mA, 1.8-2 V.	8. LEDs (a) Use the fingerprint sensor in conjunction with the LEDs; write sample code with 10ms delay between fingerprint analysis and LED indication. (b) 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. (c) i. Adjust resistances from a voltage regulator to deliver 10mA to the load. ii. Use a multimeter to verify the input voltage and current.	(a) Y (b) Y (c) Y
9. Mini Thermal Receipt Printer (a) Accurately print a voter's selection onto thermal paper with a resolution of 8 dots per millimeter, 384 dots per line.	9. Mini Thermal Receipt Printer (a) 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.	(a) Y