



Design and Simulation of a Smart Card-Based Electronic Voting Machine

¹Iyidobi, Jonathan C., ²Onuigbo, Chika M., ³Eze, Marcel N.

^{1,2,3}Department of Electrical and Electronic Engineering, Enugu State University of Science and Technology, Nigeria

Accepted: September 21st, 2022

Published: September 30th, 2022

Citations - APA

Iyidobi, J. C., Onuigbo, C. M., Eze, M. N. (2022). Design and Simulation of a Smart Card-Based Electronic Voting Machine. *International Journal of Information Sciences and Engineering*, 6(2), 34-45.

This project focuses on the design of a secured, reliable and efficient smart card-based electronic voting machine. The system utilizes RFID technology for automatic identification and data capturing of voters. More so, the system consists of a microcontroller, an RFID scanner, push buttons, and an LCD display. This project is aimed at providing a homegrown electronic voting system in Nigeria owing to the recent enactment of a law powering the Nigerian electoral umpire to adopt electronic voting in conducting elections in Nigeria. Elections in Nigeria have been adjudged the most violent in Africa. This is perhaps owing to the large population and plurality of the Nigerian states that have compounded electioneering processes for the country. This system will, therefore, eliminate the challenges that have been associated with manual voting in Nigeria. With this system in place, all that is required of a voter is to present his or her voter's identity card, the card will be swiped before the RFID scanner; the RFID senses the information of the voter and sends it to the ATMEGA 328P microcontroller. Having received the voter's information, the microcontroller will check whether such a voter is eligible to vote in the particular polling unit. If the voter belongs to the polling unit, the system checks whether the voter has already voted, of and if the voter has not voted before, the system will be activated to receive the vote.

↑
ABSTRACT

Keywords: Smart Card-Based Electronic Voting Machine; Design and Simulation; Microcontroller

Introduction

Over the years, elections at national, state and local government levels in Nigeria and indeed many West African countries have been characterized by diverse forms of irregularities and violence (Labinjo, 2007). This situation has impacted negatively on the credibility of the country's democratic processes. Some of these irregularities include: ballot box snatching/stuffing, multiple voting, under age voting, over voting, impersonation, etc. More so, it is pertinent to note that Nigeria is the most populous black nation on earth with over hundred million voters, thus it takes the electoral umpire-the independent electoral commission (INEC) undue time to conduct elections and announce the results, especially during national elections. The population of Nigeria especially the surge in the number of registered voters has posed a serious challenge to the traditional method of voting in Nigeria, it is crystal clear that these aforementioned irregularities cannot be resolved in view of the growing population if the traditional voting system is not jettisoned. These electoral irregularities have been facilitated by the continued use of a manual (paper) system of voting. This system is devoid of any form of electronic authentication and transfer of voting data from voting points to collating centers.

Recent innovations in information and telecommunications technologies are facilitating a fully automated electronic based election process. Added to preventing common election malpractices, electoral vote counts are done and transmitted in real time such that election results automatically come out shortly after voting on election day (Radeep *et al.*, 2019). According to Keerthana (2015) electronic voting was first introduced in the United States in the year 2000 and was perceived as somewhat controversial by political analyst and some scientist, just like any new innovation has always been received with suspicion. However, several years down the line, the American democracy has continued to wax stronger and elections in American has been adjudged credible, free and fair. Thus, the initial fear and suspicion over the efficiency, security, dependability, and reliability of electronic voting has been allayed.

Efforts made to amend the electoral act in support of electronic voting in Nigeria have recently produced good result as the 2022 amended electoral act empowered the Independent Electoral Commission (INEC) to employ electronic transfer of result from pooling centres to INEC servers. The newly introduced Bimodal Verification Accreditation System (BVAS) machine has also made electronic voter authentication more credible. These new changes are fast bringing Nigeria closer to an era of full-blown electronic voting system.

This paper seeks to develop a locally made smart card based electronic voting machine that will accommodate at least 1000 users. The system will be designed to have effective protection against any external manipulation. Being a Nigerian made system, the fear of possible manipulation by countries where the machine was produced will entirely be dispelled. The proposed machine will be secure, portable, interactive and user friendly.

Voting machines are the overall combination of, electronic equipment, electromechanical, or mechanical (including firmware, software and documentation required to support equipment and program control), that is used to define ballots; to report or display election results; to cast and count votes; and to maintain and produce any audit trace the information (Praful *et al.*, 2015). Thus, voting machine is more of a generic description of a process and not just hardware. A voting machine takes cognizance of the system components and versions of such components which includes the practices and the documentation associated with it; to ensure proper records of system errors, to assess the system at the point of development and maintenance, to give feedback to the voter such as issuing paper notice; and to evaluate certain alteration implemented after initial clarification (Pandey and Aghwariya, 2015). There are different levels of efficiency, accuracy, usability and security. Some of systems might be more or less accessible to those who are casting the vote (Praful *et al.*, 2015). An electronic democratic framework requires a more significant level of security than an Internet business framework, the stage over which electronic casting a ballot is done goes far in deciding the security necessities they can accomplish and its practicability in genuine decisions (Arif, Mohammad, and Rocky, 2019).

With electronic voting machine in place, many forms of electoral irregularities like impersonation, over voting, ballot snatching and reckless vote allocation will be a thing of the past. The system will have the capacity to collate and display result in real time there by giving no room for manipulation.

To strengthen democracy and enthrone quality leaders that will transform our Nigeria from a developing country to a developed country, a transparent and secure electoral system must be put in place. This can be achieved by the use of an electronic voting system in place of manual/ paper voting method. The smart card-based e-voting machine will use a digital authentication system to avoid impersonation. The use of a database system in the e-voting system and the absence of ballot boxes will also prevent ballot snatching while electronic transmission of result will prevent writing of fictitious results outside polling stations.

Review of Related Literature

The conventional voting equipment which includes paper-based voting, lever voting machine, direct recording electronic voting machine, punch card, optical voting machine, etc. have continued to phase out in recent years owing to their flaws; it takes unduly long time to count the votes, it is highly complex, and the accuracy is often in doubt. Thus, many countries have embraced electronic voting to address these issues; such countries include America, Japan, Belgium, Brazil, Kenya etc.

Against this backdrop, electronic voting has attracted the interest of many researchers. Arif, Mohammad, and Rocky (2019) proposed an electronic voting machine for Bangladesh. The system was mainly based on finger print, which is a unique security system to eradicate vote manipulation. The system hardware consists of Microcontroller (Arduino MEGA2560), Fingerprint Sensor (GT-511C3), LCD Display, Power Supply, Piezo Buzzer, Keypad. Although this system was successfully implemented; it is not suitable for presidential elections in Nigeria owing to the limitations inherent with the hardware components such as small memory capacity of the Arduino MEGA2560). Similarly, Praful *et al.* (2015) developed an electronic voting machine based on RFID technology. The researchers used a microcontroller, a RFID reader and LCD display. A voter is meant to swipe his or her identity card on a RFID reader. When RFID reader senses the voter ID then it sends this information to the microcontroller 89c52. After receiving the voter ID information, the microcontroller checks whether the received voter ID belongs to the particular polling booth or not. If the voter ID belongs to the particular booth, the microcontroller finds if the voter has voted or not. If not, then it makes the voting machine ready for voting. That process continues for each and every voter.

Keerthana *et al.* (2015) designed an electronic voting machine in India taking cognizance of unavailability of electric power supply in many remote areas in India. Thus, the machine is powered by ordinary 6volts alkaline battery. The system consists of two units— a Control Unit and a Balloting Unit – joined by a five-meter cable. The balloting unit enables the voters to provide their votes. Each balloting unit can accommodate more than 10 candidates. Such units can be connected to a single control unit. The system can record a maximum of 4000 votes. The hardware consists of EEPROM, Finger Print Module, Keyboard, Buzzer, LCD Display, and RFID Module with RFID card, PIC Microcontroller (16f877a). Radeep, *et al.* (2019) sought to eliminate over-voting in India elections, thus the researchers carried out a modular designed of electronic voting machine. The system hardware consists of Arduino, NI Lab output, GSM module and fingerprint module. In order to ensure integrity of the system, security features that are hack proof with the enchain security were added to the system.

Methodology

Block Diagram and Key Components Used

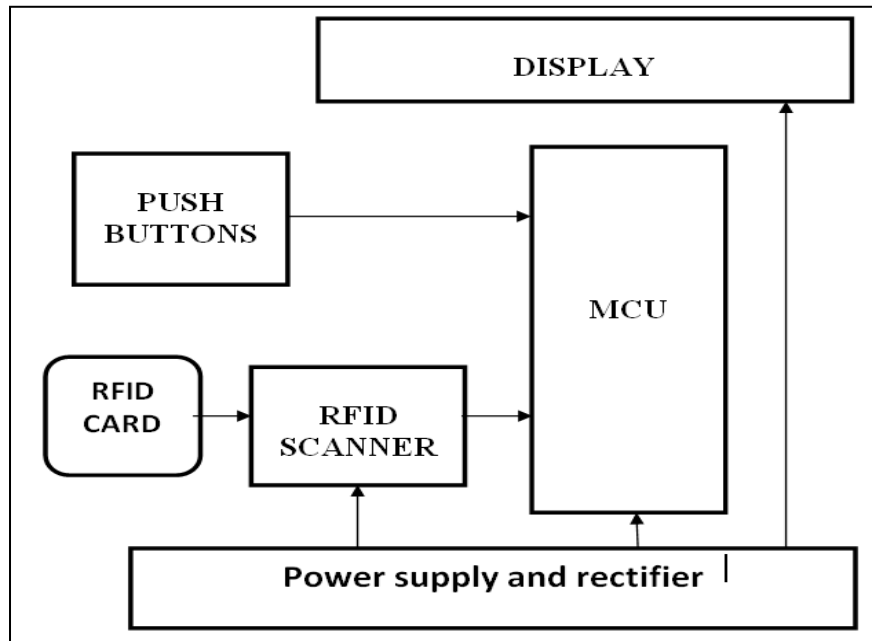


Figure 1: Block diagram of the electronic voting machine

This project has effectively demonstrated how a Smart card-based electronic voting machine can be designed to eliminate the possibility of rigging, reduce time wasted in accrediting and sorting votes manually. The machine so designed is relatively cost effective. The system is simple and convenient to use. A voter simply needs to present his or her permanent voter's card (PVC) and swipe at in front of the Radio Frequency Identification (RFID) scanner to gain access to vote. The voter then votes by pressing one of the keys which corresponds to the political party of his or her choice, and the system will accept and record the vote against the political party as shown in figure 4.3.

The power supply is a 12V AC power supply rectified to DC and further regulated to 800mA/8V DC for charging the 7.4V lithium battery and 500mA /5V DC for powering the various components in the system. The Microcontroller Unit (MCU) is an ATMEGA328 microcontroller. The RFID reader/card is the RC552 RFID module. While the Liquid Crystal Display (LCD) is a 16X2 screen capable of displaying 2 lines of 16 characters.

The MCU triggers the RFID scanner to check for available RFID signal once the card is about 10cm close. The RFID scanner sends a digital signal to the MCU. The MCU in turn converts the digital signal to characters. The characters are used to match the existing packets of data present in the memory location of the MCU. Here Boolean logic is performed where true represents match and false represents mismatch. If a mismatch results, the program sends an error code to the LCD and returns to scan mode. If a match results, the program moves to the next loop which is the voting loop. Here the MCU monitors the three buttons labeled A, B, and C to increment the memory locations assigned to each party to be voted for. Once any of the button is pressed the program returns to the Scan loop.

At the poling unit is the voting machine which validates the voter and gives access to the voters to vote for the candidate of their choice. The voters' card is an RFID card which bears the bio-data of the voter and most importantly the tag number which is a unique identification number of every voter-card. Once a voter places his/her voter's card on the card scanner integrated to the voting machine; the scanner fetches the tag number and sends to the MCU (ATMEGA328). The microcontroller using the firmware programs embedded in it sends a query to its database to check if the tag number of the voters' card is in its database while the status is displayed on the LCD (16X2). Here a Boolean condition True/false would determine the next action of the machine whereby if the Boolean is false the machine returns an error message "invalid PVC you are not eligible to vote". If true the machine will return a congratulatory

message "Congratulations! PVC valid Choose your candidate accordingly by pressing A, B or C for Party X, Party Y and Party Z respectively. On pressing the corresponding button, the microcontroller increments the vote count of the corresponding party.

The microcontroller Unit (CMU)

The microcontroller board consists of the microcontroller, crystal oscillator circuit, the reset resistors, also attached to the microcontroller is the RFID reader and the LCD. This microcontroller was used because it bears the whole features needed for the project which include: Serial port, digital I/O, up to 2234B of RAM, 32KB of ROM, 1B of EEPROM and Speed of up to 16MHZ. The above listed features made the microcontroller worthy of the design.



Figure 2: ATMEGA 328 microcontroller board

Clock Circuit

The clock signal is a periodic sequence of pulses. The ATMEGA328P can generate its own internal clock signal. In order to generate clock for the microcontroller, the output of the clock circuit must be connected to the XTAL and EXTAL on pin. A crystal and 2 capacitors 30pF are required for the connection. The internal clock frequency is one-fourth of that supplied to the crystal pins. A 16 MHz crystal oscillator was used in this study to design the clock frequency. Hence, the clock speed (frequency) is 4 MHz and often referred as E clock. The E clock can be measured on ATMEGA328P by using an oscilloscope or any frequency measuring devices.

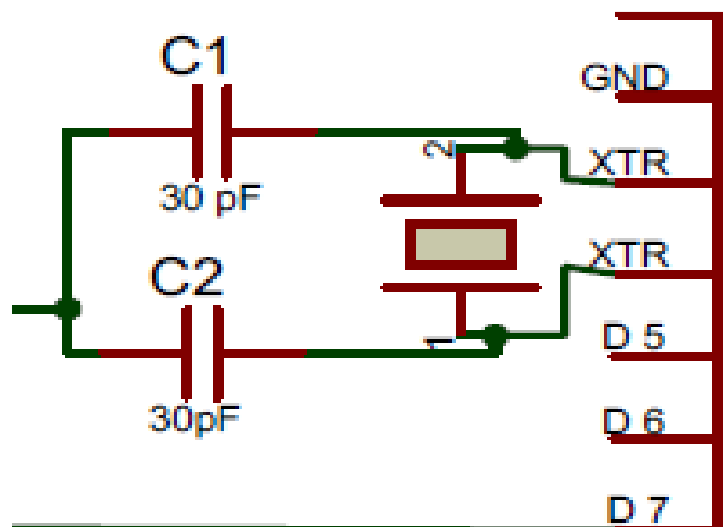


Figure 3: Clock Circuit

Liquid Crystal Display (LCD)

Since its discovery in 1888, liquid crystal display (LCD) has been used extensively in display system; this is especially because of its low power consumption, ability to be used in battery-powered electronic equipment which is more efficient than CRTs. A liquid crystal display (LCD) is a flat-panel display tool or simply an electronic visual display. LCD does not emit light directly; rather it utilizes the light-modulating properties of liquid crystals. A typical LCD is made up of several segments controlling a layer of liquid crystals. The reflector can produce image in different types of colors.

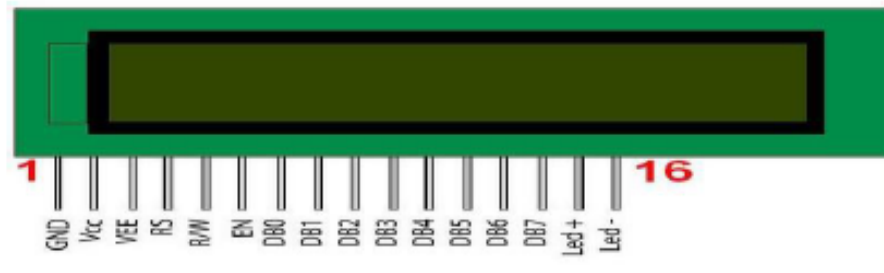


Figure 3: 16x2 LCD display

RFID

Radio frequency identification (RFID) is used for recognition and tracking of tags attached to objects by virtue of electromagnetic fields. Information is electronically typed and stored in the tag. The tag is of two types; passive and active tags. The passive tag gathers information about the radio waves around the RFID, while the active tag must have a power source such as a dry battery and can operate several meters away from the RFID (Ranjan, Tomar, and Gowri, 2016). For an object to be tracked, it must be situated in the line of sight of the reader which is barcode. In essence, the RFID is a means of providing automatic identification and data capture (AIDC).



Figure 4: EM-18 Reader Module

Power Supply and Rectifier circuit

The rectifier block comprises of the transformer, diodes, capacitors and voltage regulator.

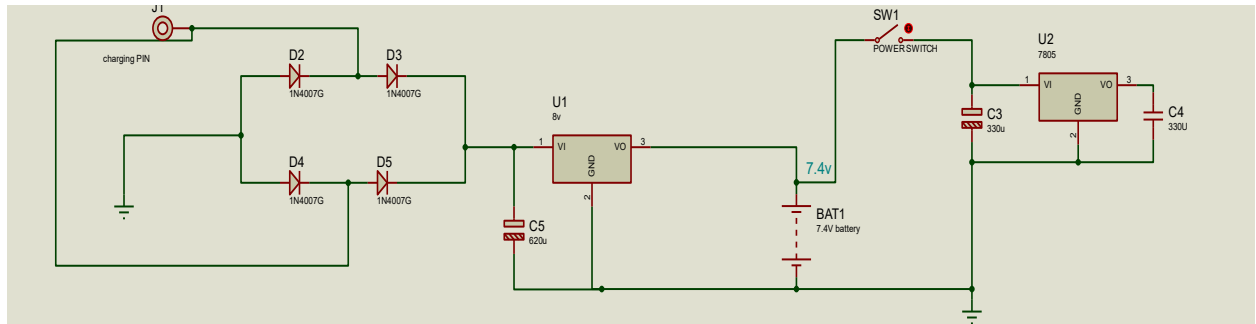


Figure 5: Rectification Circuit

To select the transformer for the rectification circuit, the power consumed by each of the components is tabulated below;

Table 1: Total power demand from the rectification circuit

DEVICE	VOLTAGE	CURRENT	POWER
Battery charger	8V	0.2A	1.6W
RFID READER	5V	0.03 A	0.15W
LCD	5V	0.03A	0.15W
2 LEDs	2V	0.04 A	0.08W
ATMEGA 328P	5V	0.2 A	1W
Total		0.207 A	2.98W

Putting into consideration the net value of power demand of the components which make up the e voting machine it simply implies that the power supply must not be less than 2.98W and 5V respectively.

Current consumption = power/voltage
 $2.98/5 = 0.372 = 0.4A$

The maximum DC voltage required by the system is 12 volts; this led to selecting a transformer of 12V /0.5A (closest available value in the market).

Ripple Factor of bridge rectifier

The output voltage from the transformer is 12V at 50Hz while the current output is 0.4A therefore 1N4007 is suitable for the design since it meets the specifications.

According to datasheet, 1N4007 has the following features:

Max frequency = 60HZ

Max current = 1A

Max Voltage = 100V

The pulsating output of a rectifier can be considered to contain a dc component and ac component called the ripples.

The ripple current is undesirable and its value should be the smallest possible in order to make the rectifier effective.

The ripple voltage or current is measured in turn of the ripple factor which is defined as the ratio of the effective value of the ac components of voltage (or current) present in the output from the rectifier to the direct or average value of the output voltage (or current). At this point, a capacitor is need to eliminate the ripple in the power supply.

Calculation for filtering capacitor (C2);

$$Q = C \times V$$

where C = capacitance in farads, Q = charge in coulombs, V = voltage potential

but $Q = I \times T$

where I = current flow in amps,
T = time in seconds

Recall, $T = 1 / F$

Where F = frequency in Hz,

$$\Rightarrow I \times T = C \times V, \Rightarrow C = (I \times T) / V \equiv C = I \times \Delta T / \Delta V$$

$$\Rightarrow C = I / (\Delta V \times F)$$

Now including the 10% ripple factor, the final relationship holds thus;

$$C = 0.1 \times I / (\Delta V \times F) \equiv I \times \text{rms} \frac{dt}{dv}$$

Where, ΔV and dv = peak-to-peak ripple voltage, F and dt = ripple freq in Hz. Note that ripple frequency in a full-wave rectifier is double line frequency. For half-wave rectification, the ripple frequency is the line frequency.

Where Rms = 0.1 (ripple factor)

$Dt = (1/100) = 0.01$ (which is time period in full bridge rectification)

$dV = 17$ (peak to peak voltage of stepped down AC supply = $12 \times \sqrt{2}$)

$$C = 0.4 \times \frac{0.01}{17}, C = 0.000235F = 235\mu F.$$

Therefore, $C1 = C2 = 330\mu F$ nearest available value.

Solving for the voltage regulator capacitor (C3)

For voltage regulator

$$C = \frac{I \times t}{\Delta V}$$

Where $t = 1/50 = 0.02S$ and $\Delta V = 12 - 5 = 7Vdc$

$$C = \frac{0.207 \times 0.02}{7}$$

$$C = 0.000591 \text{ Farad}$$

$$= 591\mu F \approx 620\mu F \text{ (nearest available value).}$$

Having realized the value and specifications of all the components, they are connected as shown in figure 4.1 to produce the proposed smart card based voting machine.

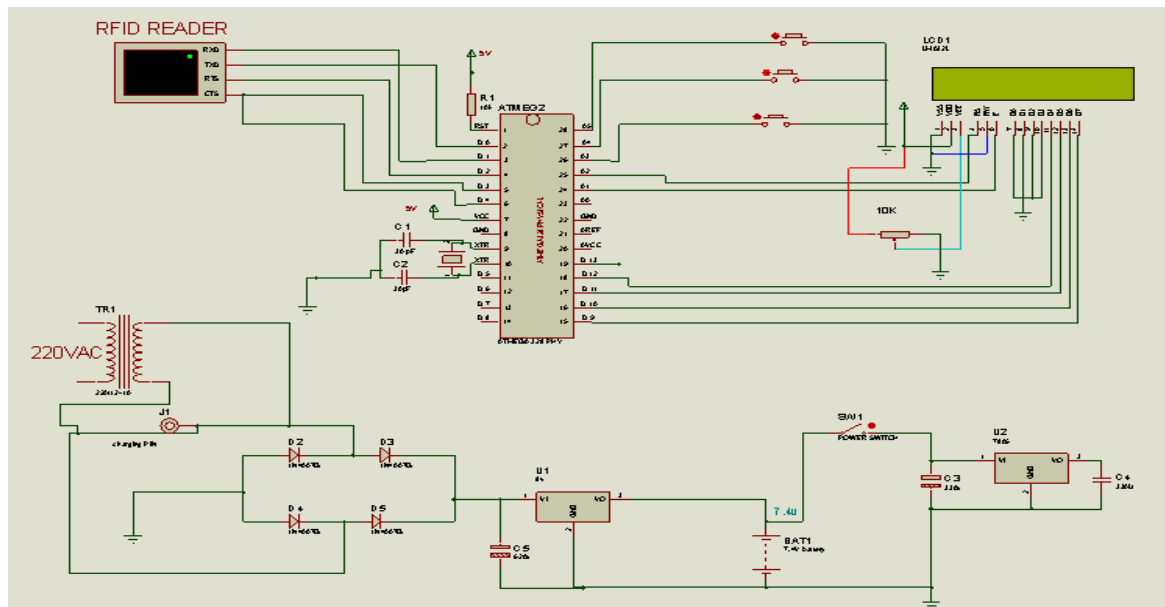


Figure 6: Circuit diagram of the smart card based electronic voting machine implemented in Proteus software

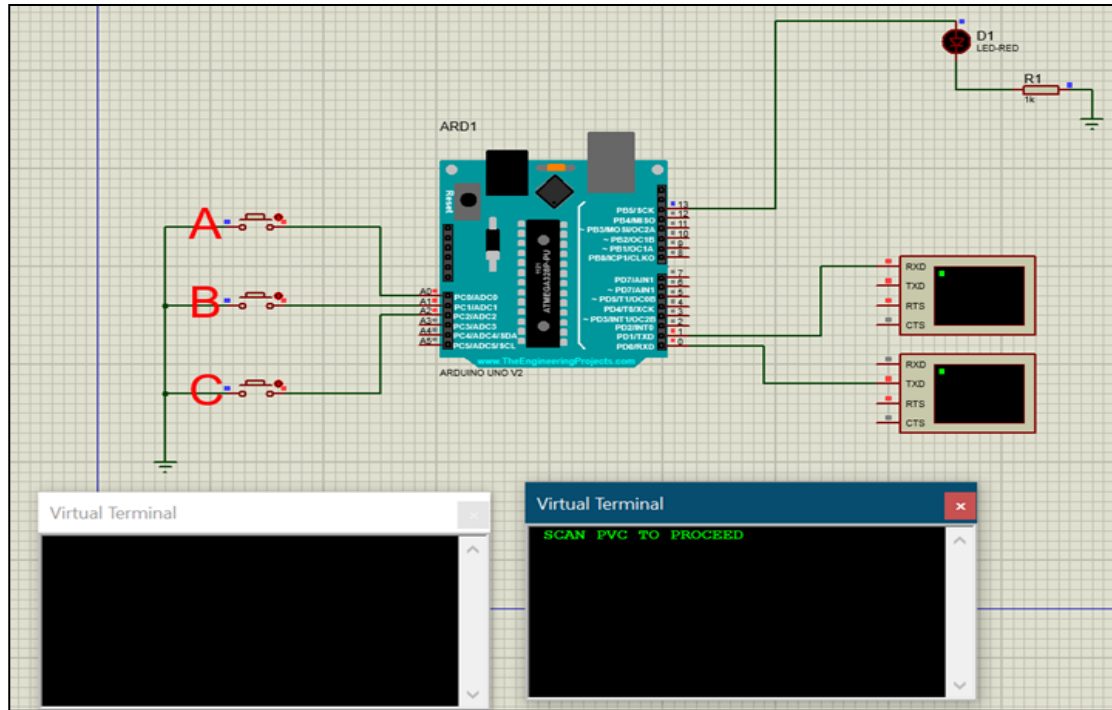


Figure 7: Proteus based model of the smart card based electronic voting machine prompting the voter to scan his/her PVC to vote

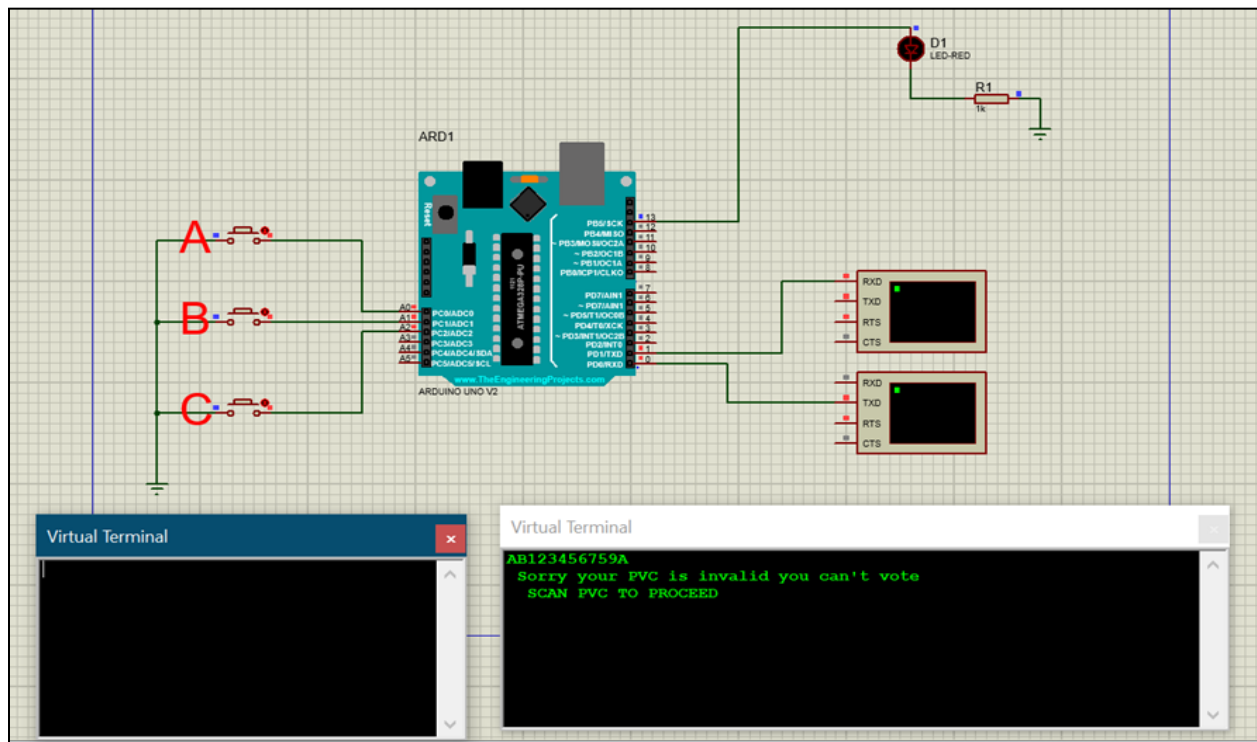


Figure 8: Proteus based model of the smart card based electronic voting machine denying an unregistered voter access to the system

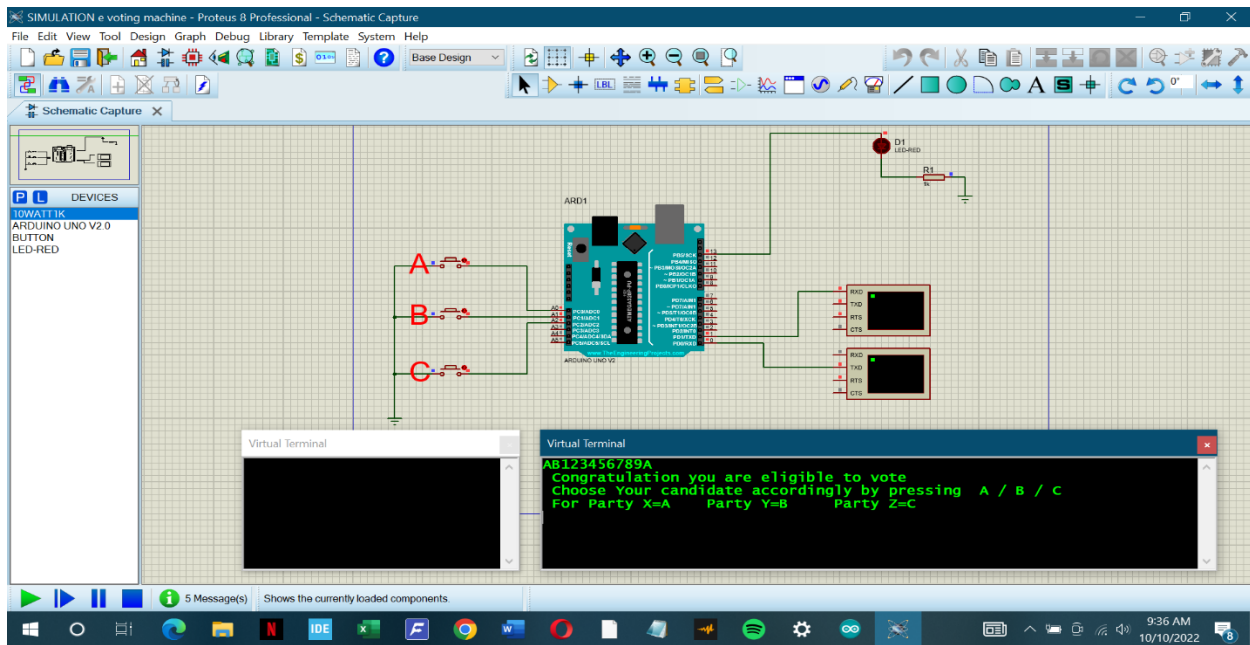


Figure 9: Proteus based model of the smart card based electronic voting machine authenticating a registered voter and granting him/her access to vote

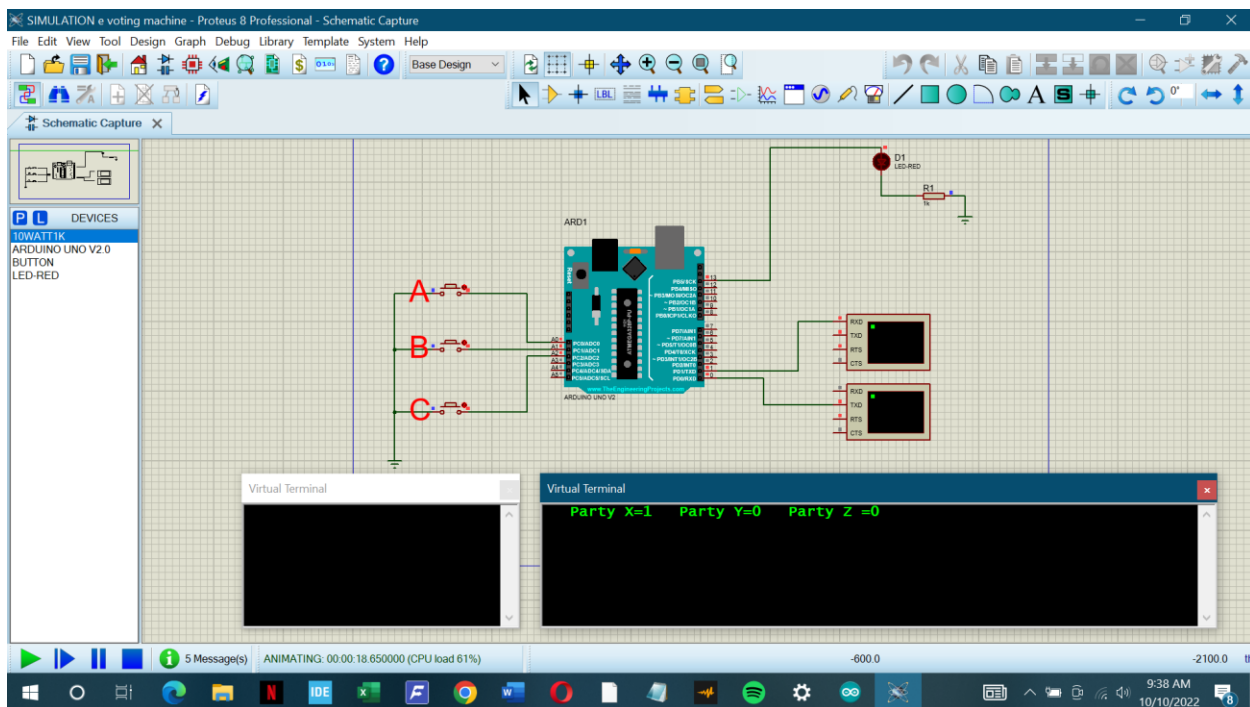


Figure 9: Proteus based model of the smart card based electronic voting machine updating the vote of a voter

Result, Analysis and Conclusion

For every voter the voters' card must be scanned for validation thus the first interface of the voting machine as seen in figure 4.2 is the "scan PVC to proceed" message. By placing the voters' card on top of the scanner the tag number is automatically fetched by the RFID scanner. If the voter's PVC number is not found in the database the machine returns an error message "Sorry your PVC is not valid you cannot vote" as displayed in figure 4.3. However, if voter's

PVC number exists in the database the machine returns a message for the voter to proceed with the voting process by voting the candidate of their choice. This can be observed in figure 4.4 where the system congratulates the voter for being qualified to vote and asking him/her to go ahead and vote for the candidate of his choice. Once the voter makes his choice by pressing the corresponding button the machine increases the vote count of the corresponding party. This is clearly shown in figure 4.5 where the party that benefited from the candidate's vote, XXX now has a score of 1 as against the other party that are test to get any vote.

From the result and analysis, it can be concluded that with key components like: microcontroller, crystal oscillator circuit, the RFID reader and the LCD; a smart card based electronic voting machine can be designed and simulated successfully in Proteus software.

References

- Arif A., Mohammad S. H., Rocky C., M., and Mahfujur R. (2019). Design and Fabrication of Electronic Voting Machine. *Journal of Control System and Control Instrumentation*, 5(3)
- Keerthana, G., Priyanka, P., Alise J. K., Rajadharashini, R., Aruna D.P. (2015) Impressive Smart Card Based Electronic Voting System. *International Journal of Research in Engineering and Technology*, 4(3)
- Labinjo, J. (2007). The national question issue: A contractile and dilative phenomenon in Nigeria. In: Osaghae, E. E. and Onwudiwe, E. eds. *The Management of the National Question in Nigeria*. Okada: Igbinedion University Press, 163–181.
- Pandey, P. S., Ranjan, P. and Aghwariya, M. K. (2016). The Real-Time Hardware Design and Simulation of Thermoelectric Refrigerator System Based on Peltier Effect. *ICICCD*, DOI 10.1007/978-981-10-1708-7_66. 7, 581-589.
- Praful R., Abhishek A. B., Saatwik B., Neha S. (2015). Design of RFID based electronic machine. *International Journal on Human and Smart Device Interaction*, 2(1), 1- 6.
- Rani, G., Pandey, P. S. Aghwariya, M. K. Ranjan, P. (2016). LASER as a Medium for Data Transmission Proceeding of International conference on ICARE MIT-2016, Organized by Department of Mechanical Engineering, M.J.P. Rohilkhand University, Bareilly-. ISBN No.: 978-93-82972-19-8, 9-11, December (2016).
- Radeep, K. R., Lakshmipriya, A., S.kalaiselvi, and Hilalkhan, A. (2019).Modular Design of Electronic Voting Machine for Future Elections. *International Journal of Digital Communication and Networks (IJDCN)*, 11(6).
- Ranjan, P., Tomar, G. S. Gowri, R. (2016). Metamaterial Loaded Shorted Post Circular Patch Antenna. *International Journal of Signal Processing Image Processing and Pattern Recognition (IJSIP) SERSC Publication*, 9(10), 217-226.