International Refereed Journal of Engineering and Science (IRJES)
ISSN (Online) 2319-183X, (Print) 2319-1821
Volume 8, Issue 1 Ser I (Jan 2019), PP. 48-57

Design and Development of an Arduino Based Electronic Voting System.

Abdulkadir H. Alkali[1], Emmanuel G. Dada[1], Dauda E. Mshelia[1], Sadiq O. Onundi[1]

[1]Department of Computer Engineering, University of Maiduguri, Maiduguri, Borno State, Nigeria.
Corresponding Author: Abdulkadir H. Alkali

ABSTRACT: *- Election is a key issue when it comes to deciding who the next leader(s) or representative(s) are going to be through democratic means. The existing prevalent processes of voting in these elections are slow and strenuous and the outcome is often inaccurate. Thus, people lose faith in the electoral process and consequently in their leaders as well. This work developed an electronic voting system that aids the process of choosing such leaders in a manner that is fast, free and fair. The device was developed by interfacing fingerprint sensor, a keypad, GSM module, real time clock, an LCD and a personal computer to an Arduino Mega. Algorithm was developed and coded using the Arduino IDE. The unit stores voter data, which includes biometric information, during registration and randomly assign voting pins to registered voters to their given mobile numbers. Prior to voting, it checks for a match with the stored data during the authentication by comparing biometric and then pin of a voter to that in the database. Upon successful authentication, the voter is allowed to cast their vote, either in open ballot or closed ballot mode. The device collates result of voting including time of each vote and can deduce the winner based on majority votes. The device was deployed and evaluated against a mock election using the secret ballot system and was found to not only produce expected results but was also found to eliminate possible irregularities such as vote inflation while also reducing both voting and collation times.*

KEYWORDS: -Arduino, Election, Finger-print.

Date of Submission: 29-03-2019 Date of acceptance: 09-04-2019

I. INTRODUCTION

Voting could be by open ballot where the voters queue up according to their preference or by way of secret ballot in which voters choose a preferred candidate by casting a vote normally on paper in favor of their candidate. The major difference to note between the two types is that in open ballot, results are a bit difficult to manipulate since each voters intent is known to everyone at the venue while the secret ballot can easily be manipulated. Although the secret ballot gives the voter more confidence to align to their choices rather than possibly aligning to another due to coercion in open ballot. Perhaps secret ballot is mostly used for its privacy and the fact that less time is required by a voter to conclude and leave the venue.

Secret ballot has a tendency to be manipulated during collation and thus people have confidence issues with its outcome. Another factor affecting this mode is time spent in accrediting voters which takes up a good percentage of the total election time, while counting if considered as part of the election, takes up to 40% of the time [1].

To forestall the confidence issues as well as improve on the accreditation to ensure that only eligible and registered voters vote and also to reduce (almost eliminate) the collation (counting) time, electronic voting (e-voting) was introduced.

Elections date back to ancient times, most notably to the Greek city-states and republican Rome. Athens in the fifth and fourth centuries BC is often considered to be the first direct democracy – a system in which citizens vote on public policies and laws directly [2]. Elections in Nigeria dates as far to the first republic, in the general election of 1959 to determine which parties would rule in the immediate postcolonial period [3].

E-voting system (EVS) is voting using electronic means to either aid or take care of the chores of casting and counting votes. Due to most elections being marred with doubts such as voter impersonation, result rigging and issues of ballot box snatching, most elections are now being suggested to turn to electronic voting as a way to fix these shortcomings of the conventional paper/ballot voting system. Additionally, the cost of EVS is considered less since technology procurement is considered an investment that is re-usable.

Electronic voting technology can include the use of punched cards, Radio Frequency Identification (RFID) tags, pass codes, optical scan voting systems, finger print sensors and specialized voting kiosks (including self-contained direct-recording electronic voting systems, DRE). It can also involve transmission of ballots and votes via telephones, private computer networks, or the Internet.

According to (Ashok, 2014), E-Voting can either be one that is physically supervised by representatives of constituted authorities (e.g. electronic voting machines located at polling stations) or remote voting via the internet (also called I-voting) where the voter votes at home or without going to a polling station.

Electronic voting technology can speed the counting of ballots, reduce the cost of paying staff to count votes manually and can provide improved accessibility for disabled voters.

In [4], a Raspberry Pi based system was developed in which four buttons were used to vote for four candidates or parties. A voting count emanates when a voter presses a button assigned to his/her candidate or party. For each button press, the count was incremented by one and an LED blinks while a buzzer beeps for one second, to indicate that Vote has been given. After the Voting completes, a “Result” button, shows the results of the Voting on the LCD screen, indicating the name of the winner with the number of votes accumulated by each party. The limitations of this system included a total absence of any form of voter registration and authentication system, lack of portability and alternative forms of power supply, absence of separate user and administrator interfaces, absence of an algorithm that picks up voting times. It also limited the number of candidates to four.

In[5], a simple, low cost fingerprint based electronic voting machine using ARM9 microcontroller was developed. The hardware was implemented with ARM9 microcontroller along with KY-M6 finger-print module. During the enrolment stage, the finger-print of a candidate alongside their details such as name and photo were captured and stored in a remote server via the internet. To vote, a voter’s finger-print was authenticated against existing records on the server. It detects attempted double voting and non-registered voters. The main short coming of this design was the single authentication method employed which was not sufficient to completely eliminate the issues of voter fraud. The downside of the work is the use of dedicated push buttons for each candidate/party. This makes it static in that new candidates/party cannot be incorporated without modifying the hardware.

An RFID (Radio Frequency Identification) based voting machine that authenticates and accredits voters based on their RFID tags was developed and constructed in [6]. An ATmega32 microcontroller for system control, a Liquid crystal display to guide users through voting process, RFID cards and tags to authenticate voters and four push buttons were made available to vote for one of four candidates. The limitations of this design were the fixed number of candidates. It also operated on mains power only in addition to the single method of authentication (by RFID cards). Assembly language was used for programming the device making any future improvements to the system very tedious.

[7], in their publication designed an electronic device that could be used to perform elections. Their design incorporated the use of an Arduino board, a liquid crystal display, a keypad, a printer and four push buttons used to input vote for each party. The authentication was linked via the internet to India citizen identification data base that gives a unique identification number for every citizen. The method, although more secured than the previous listed, has limitations such as access to voter pins by officer-in-charge during printing, the number of parties (or candidates) is limited to four and the use of the same interface for both administrator and user which displays personal details to all to see during registration.

In [8], a fingerprint sensor was used to authenticate the voter based on a computer serving as the database. What was not mentioned is the way the voter is first registered and how the GSM module functions in the system.

A voting system whose authentication is also linked to the India citizen identification data base just as reported in [7] was reported in[9]. The main difference is that the authentication was via a zigbee which has a short communication range. In [10] the finger print sensor was activated by the microcontroller once a finger was placed on it. The finger print pattern was scanned and compared on the database already stored on a PC.
Major improvements were made in the method being proposed against existing ones. These improvements include:

- Addition of real time clock to get actual voting time of each voter.
- Generation of random pins, unknown to any, and sent to the registered voter phone number.
- Ability to register higher candidates or parties.
- Separate user and administrative interfaces to improve on data integrity.
- Using both mains and battery power.
- Double authentication (biometric and pin)
- Flexibility to allow for easy improvements

II. METHODOLOGY

The proposed system block diagram is shown in Figure 1 and consists of an Arduino Mega as the main unit of the system. The sub-units interfaced to the Arduino include the keypad, fingerprint sensor, real time clock, personal computer, liquid crystal display and a GSM module. The software aspect was programmed using the Arduino sketch on a personal computer and uploaded to the Arduino board Via USB port. External power supply was thereafter used to power the system.

.

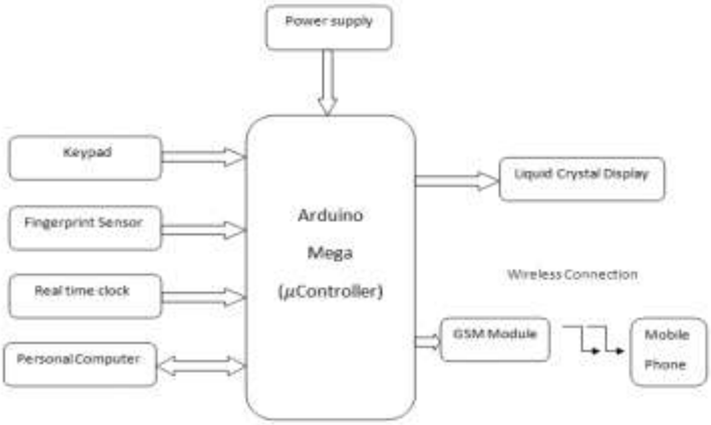


Figure 1: Proposed block Diagram

The flow chart of the system is shown in Figure 2. The following sections briefly discuss each of the sub-units of the block diagram alongside the flow chart.

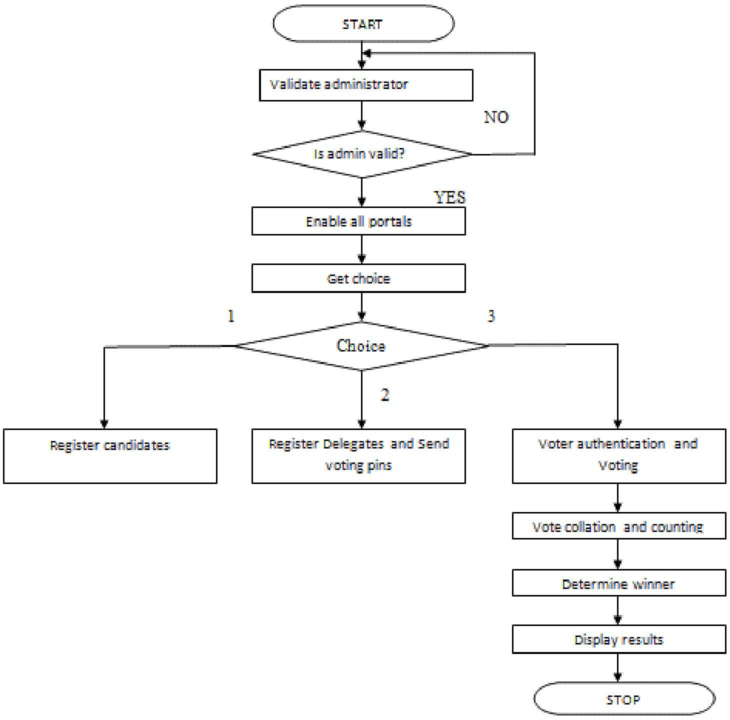


Figure 2: Flow chart of the system

1.1 Fingerprint Sensor

The FPM10A fingerprint sensor was used and shown in Figure 3. It is a biometric fingerprint recognition device used for storing and comparing fingerprint patterns. It was used as a means of authentication where during registration; a voter's fingerprint was captured and stored in the database alongside his/her other details such as name, age, phone number and gender. It was interfaced with the Arduino in order to control the working of the whole device by merging the individual components and making decisions on when to use each. The fingerprint sensor also reads a voter's fingerprint pattern during election in order to authenticate them. During this stage, the fingerprint captured was compared to those in the database. It should be noted that depending on the number of voters, the match search may take different time, i.e. the more the longer. The match search was carried out by the main unit (Arduino) after receiving the pattern read. It (Arduino) then makes the decision as to whether there was a match or not. If there was a match, then the next authentication was initiated, else, the voter was denied voting. This approach was a valid authentication method as each human being possess a unique fingerprint pattern that is not replicable.

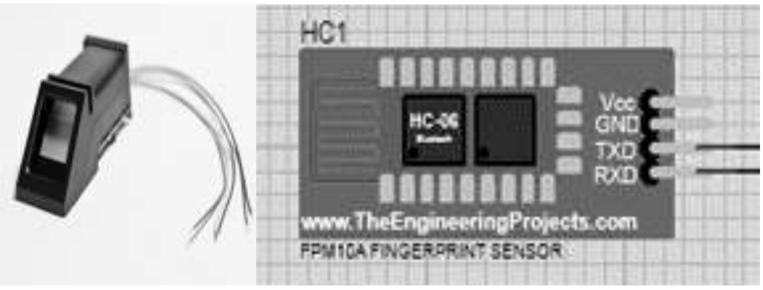


Figure 3: FPM10A fingerprint sensor and its pin outs.

1.2 GSM Module

The Simcom sim900 shield is a type of GSM module that can be used to send and receive information from mobile devices. Here, after being interfaced with the board and programmed accordingly, it was used to send the randomly generated unique voting pins of each voter to their respective mobile phones via their phone number provided during registration. During registration, as details of the voter was taken, a randomly assigned pin was generated and sent to the voters provided mobile number. This pin can only be known by the owner of the phone number to which it was sent. Even the administrator cannot have access to the pin. Although this is strict measure, it may affect voters who may have lost their pins or the phone entirely. Others may be disenfranchised due to non-delivery of pins due to phone network failure. A way to address this was the window for re-registration where voter data can be pulled up using the fingerprint of the voter as provided during registration. The connection of the shield to the Arduino is shown in Figure 4.

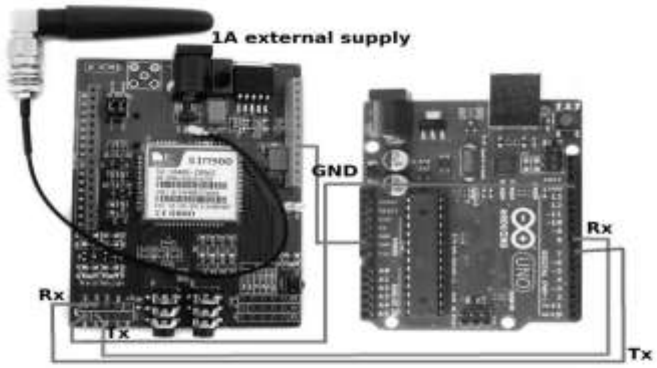


Figure 4: Simcom sim900 shield and its pin outs connection to Arduino.

1.3 Keypad

A 4*4 matrix keypad was interfaced via its output pins and was used as an input for the user interface. The 4*4 matrix keypad makes it easier to input the four digit voting pins as there won't be a need to design additional circuitry to achieve that. The six (6) non numeric keys were also used to add functionality like "SUBMIT", "ERASE", and "UNDO" to provide flexibility to the user such as during an error in inputting the pin before submitting. The pin referred to here was the pin that was sent to the user's mobile phone after registration. This also serves as an authentication method after scaling the fingerprint evaluation. Thus, the functionality of this stage was only enabled by the Arduino after successful evaluation of the user by the fingerprint sensor. This stage was the second authentication method. The PIN layout and connection of the 4*4 matrix keypad is shown in Figure 5.

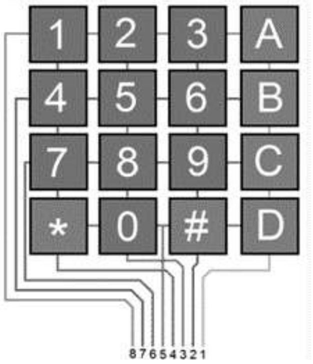


Figure 5: 4*4 matrix keypad and its pin outs.

1.4 Real Time Clock

The real time clock was used to pick up the voting time of each voter, so as to be able to ascertain the instance voting was conducted. The DS 1302 real time clock was used in this work and it uses a 3.3V coin cell battery to keep track of time. The connection of the real time clock is shown in Figure 6.

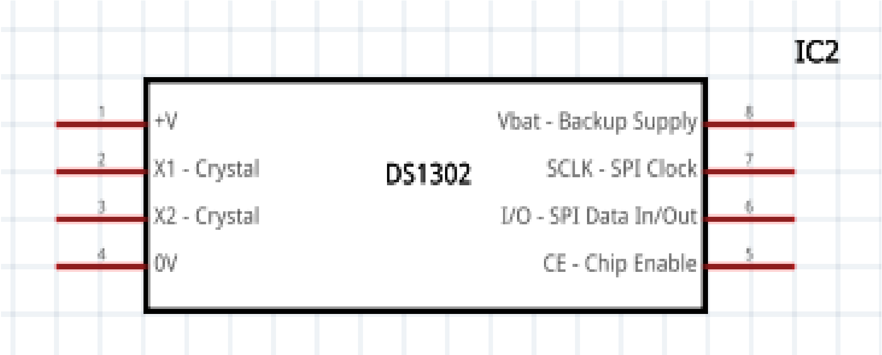


Figure 6: DS 1302 Real time clock and its pin outs.

1.5 Liquid Crystal Display

The liquid crystal display (LCD) was used as an interactive screen that helps guide voters through the voting process. It serves as the display unit for the user interface. The 20 * 4 display was used in this work and shown in Figure 7.

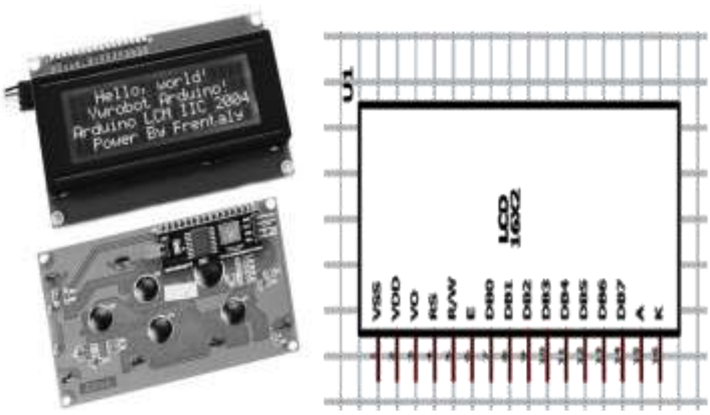


Figure 7: FPM10A Liquid crystal display and its pin outs.

The PIN configuration and connection of the 4*4 keypad and the complete circuit diagram is shown in Figure 8.

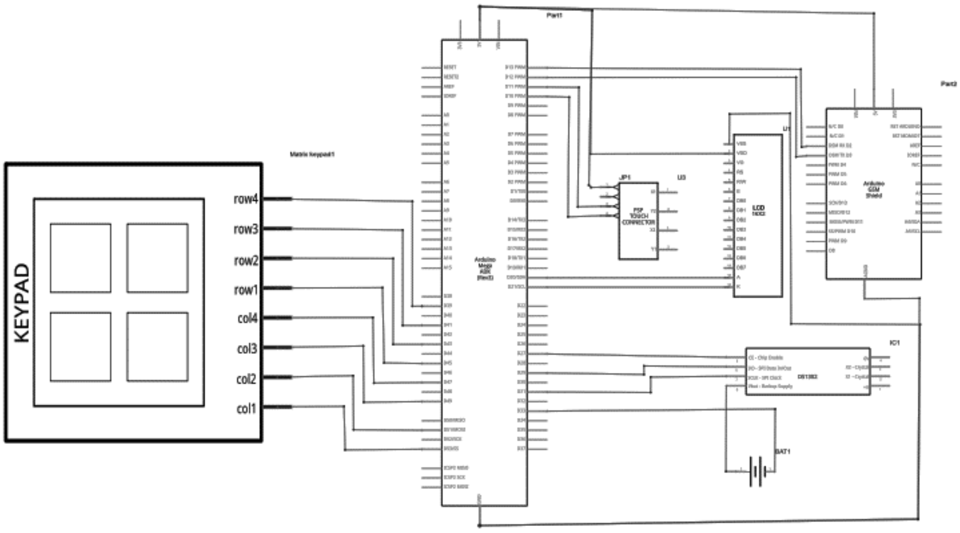


Figure 8: Circuit diagram of the complete Electronic voting system

1.6 Description of System

Figure 8 shows the flowchart of algorithm. The actions that can be performed with the device can be divided into three sub categories namely:

1. Candidate Registration Portal
2. Delegate registration portal and
3. The voting portal.

1.7 Packaging

The electronic voting system components was packaged and housed in a 40cm * 20cm rectangular transparent box as shown in Figure 9.

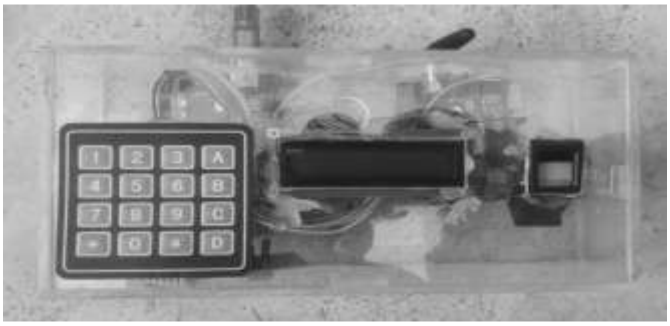


Figure 9:Casing of the device

1.7.1 Candidate registration portal:

This is a portal where each candidate participating in the election is registered by the administrator. This is done by inputting the data of each candidate such as name, age, gender, and mobile phone number via the personal computer (PC) keyboard connected to the Arduino board. The PC is only accessible to the administrator.

1.7.2 Delegate registration portal:

This is a portal where each prospective voter is registered by the administrator. This is done by inputting the data of each voter such as name, age, gender, ethnicity and phone number via the personal computer keyboard connected to the Arduino board. During this process, the fingerprint pattern of the delegate being registered is captured and stored in the fingerprint sensor database for reference during voting. After all delegates might have been registered, the device automatically generates unique voting pins for each registered voter and forwards these voting pins to the phone numbers provided by respective voters during registration.

1.7.3 Voting portal

At the voting portal, the administrator can either decide to use an open ballot or a secret ballot system. The administrator then proceeds to enter the required password to BEGIN VOTING.

Once voting has begun, the name of each candidate in the election is displayed on the screen (LCD) and each voter is in turn prompted to place their fingers on the fingerprint sensor for biometric verification. If the fingerprint pattern read at this time tallies with any of the finger prints saved in the database during registration, access is granted and the device now prompts the voter to input his or her voting pin. Else, if the finger print provided does not match any saved in the database during registration, access is denied, indicating that such a person is probably not eligible to vote.

If access is granted, the voter then proceeds to input the voting pin sent to their phone using the 4*4 matrix keypad. This is the second stage of voter authentication.

If the correct pin combination is entered by the voter, he or she can now vote for their desired candidate by simply inputting the digit that corresponds to their candidate and pressing the submit button “#”. For incorrectly entered PIN, the voter is prompted to enter the correct PIN for up to 3 times before being denied the chance to vote. The chance to enter the correct PIN can be changed, although, we felt 3 is sufficient in order to save time.

If an open ballot system was used, the screen displays the name of each candidate and the number of votes amassed by that candidate so far, also the vote count of each candidate will be updated in real time as each delegate votes.

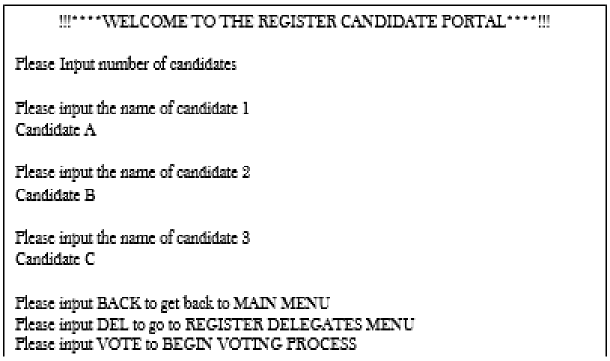
After all delegates have voted, the device automatically detects this and ends the voting process.
It then rapidly collates and counts all the votes and determines the winner which can either be displayed for all to see or just on the administrator interface.

III. RESULTS AND DISCUSSION

The results highlights how the components, methods and interconnections described in methodology are geared towards solving the issues of voter fraud, voter impersonation and result rigging as stated earlier.
The results generated by the electronic voting system can be grouped into following phases:

1.8 Registration

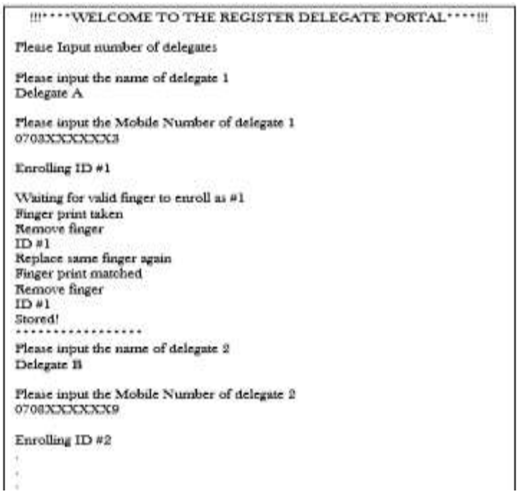
Below are screenshots of the administrator interface which serves as portal for candidate and delegate registration and described accordingly.



```
!!!****WELCOME TO THE REGISTER CANDIDATE PORTAL****!!!

Please Input number of candidates

Please input the name of candidate 1
Candidate A

Please input the name of candidate 2
Candidate B

Please input the name of candidate 3
Candidate C

Please input BACK to get back to MAIN MENU
Please input DEL to go to REGISTER DELEGATES MENU
Please input VOTE to BEGIN VOTING PROCESS
```

Figure 10: Portal for candidate registration

From Figure 10, the names of the candidates were provided by the administrator. The first prompt was to input the number of candidates. Three candidates were chosen and therefore registered, although more could have been chosen from the initial stage. Three “prompts” were provided by the system at the lower bottom of the interface to: go back to “MAIN MENU”, “REGISTER DELEGATES MENU” or “BEGIN VOTING PROCESS”. Although at this stage, voting cannot commence as there is no registered delegate (voter). If there were registered delegates, then, voting could begin by proceeding to the voting process after inputting VOTE. At the conclusion of candidates’ registration, Delegate Registration Menu was chosen by inputting DEL.



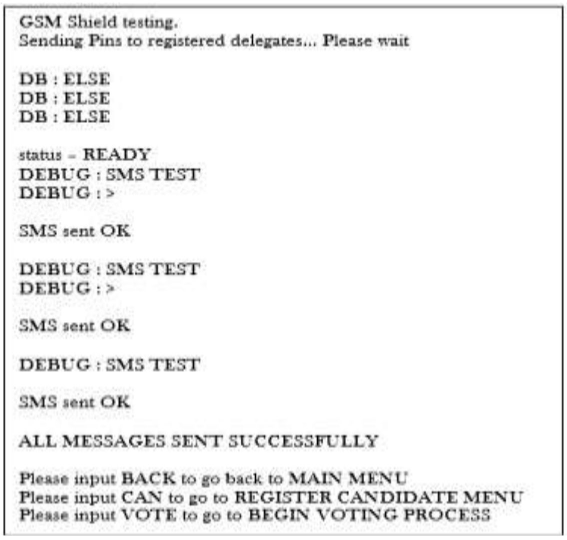
```
  !!!****WELCOME TO THE REGISTER DELEGATE PORTAL****!!!

Please Input number of delegates

Please input the name of delegate 1
Delegate A

Please input the Mobile Number of delegate 1
0703XXXXXX3

Enrolling ID #1

Waiting for valid finger to enroll as #1
Finger print taken
Remove finger
ID #1
Replace same finger again
Finger print matched
Remove finger
ID #1
Stored!
****************
Please input the name of delegate 2
Delegate B

Please input the Mobile Number of delegate 2
0708XXXXXX9

Enrolling ID #2
.
.
.
```

Figure 11: Portal for delegate (voter) registration

In Figure 11, the number of delegates was indicated. The name and then mobile number of the first delegate was requested by the system. Upon successful entry, an enrolling identification number (ID #) was serially assigned by the system starting from the lowest available and in this case 1. The next stage was the system waiting till a finger of the candidate was placed on the scanner. Upon successful reading of the print, the system request removal of the finger from the scanner and again its re-placement in order to re-validate. Once re-validation was successful, the delegate was asked to remove their finger and the matched finger-print was stored. This process for each of the delegates to be registered.

1.9 Generating and Sending Voting Pins

Once all candidates are successfully registered, the system generate a random 4-digit PIN for each delegate. The PINs are sent to their respective registered mobile numbers and encoded and saved alongside their details on the database for authentication use during election. Encoding provides secrecy that even the administrator cannot have access to a candidate's PIN. During authentication, the delegate will be asked to provide the PIN sent to him/her which will be compared to the one in the database. The process indicating successful PIN generation and sending is shown in Figure 12.



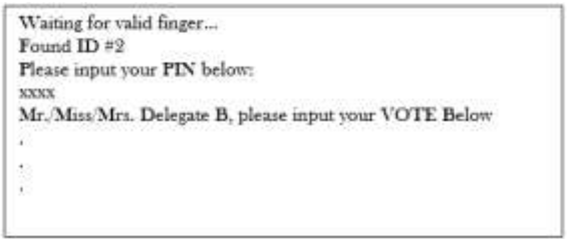
```
GSM Shield testing.
Sending Pins to registered delegates... Please wait

DB : ELSE
DB : ELSE
DB : ELSE

status = READY
DEBUG : SMS TEST
DEBUG : >

SMS sent OK

DEBUG : SMS TEST
DEBUG : >

SMS sent OK

DEBUG : SMS TEST

SMS sent OK

ALL MESSAGES SENT SUCCESSFULLY

Please input BACK to go back to MAIN MENU
Please input CAN to go to REGISTER CANDIDATE MENU
Please input VOTE to go to BEGIN VOTING PROCESS
```

Figure 12: GSM unit showing delegate voting pins being sent

1.10Authentication and Accreditation

Once registration is concluded or when voting process commences, the first process was to authenticate the delegates.

The process began by waiting for a valid finger as shown in Figure 13. Upon scanning the finger, it matches the finger-print to those in the database. If a match returns, a PIN sent to the delegate during registration is requested. Once a match is obtained from the provided PIN, the delegate will be allowed to proceed with vote casting. Should the finger-print not exist in the database, the system would request for a replacement of a valid finger. After three trials, it will call for the next delegate. At this stage, a human intervention would be required. Should the finger-print be valid and a wrong PIN provided, the system will allow for three entries after which the delegate will be disqualified from voting.

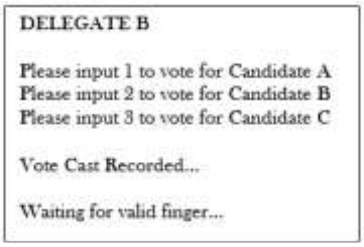


```
Waiting for valid finger...
Found ID #2
Please input your PIN below:
xxxx
Mr./Miss/Mrs. Delegate B, please input your VOTE Below
.
.
.
```

Figure 13: Delegate authentication unit

1.11Vote Casting

Figure 14 shows the dialogue during vote casting. The authenticated delegate is presented with the candidates and the voting option for each. One the delegate casts his/her vote, the “vote cast recorded” is returned and the next delegate is called upon.



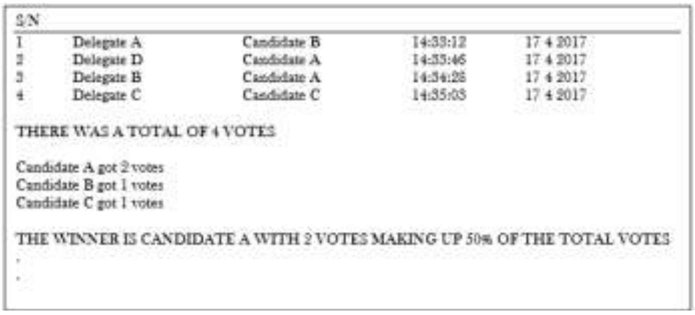
```
DELEGATE B

Please input 1 to vote for Candidate A
Please input 2 to vote for Candidate B
Please input 3 to vote for Candidate C

Vote Cast Recorded...

Waiting for valid finger...
```

Figure 14: Vote casting

The recorded vote can be displayed if the election is open ballot, if it is a closed ballot election, the result is hidden from the delegates. It may be visible to the administrator and to the voters at the end of the voting process.

1.12Vote Collation and Result Generation

Once voting is concluded, the result is displayed as seen in Figure 15. For each vote cast, the delegate name appears alongside the candidate voted for as well as the time the vote was recorded. The system also displayed the collated votes for each candidate and returns the percentage of the total votes amassed by the winner.



```
S/N
1      Delegate A      Candidate B      14:33:12      17 4 2017
2      Delegate D      Candidate A      14:33:46      17 4 2017
3      Delegate B      Candidate A      14:34:26      17 4 2017
4      Delegate C      Candidate C      14:35:03      17 4 2017

THERE WAS A TOTAL OF 4 VOTES

Candidate A got 2 votes
Candidate B got 1 votes
Candidate C got 1 votes

THE WINNER IS CANDIDATE A WITH 2 VOTES MAKING UP 50% OF THE TOTAL VOTES
.
.
```

Figure 15: Breakdown of election results

IV. CONCLUSION

An Electronic voting system was developed. It employed a dual authentication technique using both voter biometrics (finger print) and unique voting pins sent to the voter at the point of registration. This restores confidence in the electoral process. With this system data collation as regards demographics breakdown becomes way easier. It also provides a cheap, locally assembled, easily reproducible and highly sort after but presently unavailable or costly automated voting system.However, this electronic voting system is more suitable for small scale elections such as during political party primaries to select their flag bearer in a general election.

It was discovered that the device experienced problems when the numbers of voters became extremely large due to the limited memory of the AtMega32 microcontroller used in developing the device. This shortcoming of the system necessitated the limitation of the number of voters prior to registration. This however is acceptable in delegates voting since their number is known prior to election. It is also valid if the polling unit population is predetermined.

During the mock election conducted to verify the systems' efficacy, participants in the elections expressed satisfaction with the results of such elections as it was said to encompass the attributes of a credible voting system which are democracy, accuracy, efficiency and verifiability.

REFERENCES

[1]. Bobson, "stackexchange," 2016. [Online]. Available: https://politics.stackexchange.com/questions/13673/why-does-it-take-so-long-time-to-count-votes-in-us-elections. [Accessed 25 December 2016].

[2]. D. Allen and E. Chenoweth, "Democracy Web," 2016. [Online]. Available: http://democracyweb.org/node/24. [Accessed 2 December 2017].

[3]. I. Akinwalere, "brief-history-of-elections-in-nigeria," March 2013. [Online]. Available: https:// newsnowmagazines.blogspot.com/ 2013/09/brief-history-of-elections-in-nigeria.html. [Accessed January 2017].

[4]. Saddam, "circuitdigest," 2017. [Online]. Available: https://circuitdigest.com/microcontroller-projects/raspberry-pi-electronic-voting-machine/. [Accessed 15 March 2017].

[5]. M. Sudhakar and B. D. S. Sai, "Biometric System Based Electronic Voting Machine Using Arm9 Microcontroller," IOSR Journal of

[6]. D. Raja , "circuitdigest.com," 30 June 2015. [Online]. Available: www://circuitdigest.com/microcontroller-projects/rfid-based-voting-machine-project. [Accessed 15 March 2017].

[7]. M. R. Prasad, P. Bojja and M. Nakirekanti, "AADHAR based Electronic Voting Machine using Arduino," International Journal of Computer Applications, vol. 145, no. 12, pp. 39 - 42, 2016.

[8]. M. Venkateswarlu and Y. V. V. Kumar, "Biometric System Based Electronic Voting Machine with security algorithm and password protection on ARM Microcontroller and GSM," International Journal of Science Engineering and Advance Technology, vol. 2, no. 7, pp. 197 - 200, 2014.

[9]. M. D. Kumar, A. Santhosh, N. S. Aranganadhan and D. Praveenkumar, "Embedded System based Voting Machine System using Wireless Technology," International Journal of Innovative Research in Electrical, Electronics, Instrumentation And Control Engineering, vol. 4, no. 2, pp. 127 - 130, 2016.

[10]. R. Prabha, X. Trini, V. Deepika and C. Iswarya, "A Survey on E-Voting System Using Arduino Software," International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, vol. 5, no. 2, pp. 687 - 690, 2016.

Abdulkadir H. Alkali" Design and Development of an Arduino Based Electronic Voting System." International Refereed Journal of Engineering and Science (IRJES), vol. 08, no. 01, 2019, pp 48-57