

# **Design and Construction of Online Biometric Electronic Voting System**

**Boma-George Esther Daisy and Akinmuyisitan T.M**

Department of Electrical/Electronic Engineering

Benson Idahosa University

## **ABSTRACT**

This journal aims to describe the design and construction of an online biometric electronic voting system using locally available components. It uses a fingerprint biometric sensor, integrated via microcontroller to verify users of the system. The inclusion of biometrics improves the security features of the system. The software was developed with a C++ programming language that is user friendly and modification could be made from time to time and when necessary. The device is designed to enable the electoral body to use an electronic device to capture the voter's information and carry the voting process effectively. The design covers some security issues such as authenticating the voters through integrating biometric fingerprints during the voter registration process, capturing the fingerprint of the voter for validation during the election, and ensuring voters can only vote once. The design worked as designed and was able to successfully conduct a test run election. It can withstand a 220/240V, 50 Hz power supply. The overall design of the device serves better than the existing system, secures, enhances authentication and improves effectiveness, efficiency, and better voting security. Hence proffers remedies to multiple votes in electoral systems.

## **INTRODUCTION**

Democracy is a system of governance of the people, by the people and for the people. The backbone of this governance system is the existence of elections, the right of governing citizens to choose their leaders. Voting is the process through which elections are carried out. The outcome of voting is the expression of the electorate, opinion, and decision that is accepted by everybody. It means that the integrity of elections is the most important factor in the success of the democratic process. The conduct of elections in a democratic system is important not only because through it a change of government is put in place but also because voting is the main form of political participation for most people. Accuracy should be enhanced to avoid malpractice. Past centuries, most societies were primitive and had not evolved a system of voting to elect the leaders that will govern then and promote societal tranquility. This means that people have to devise a system where the leader or a set of leaders are elected from the ranks of the people. At that point, the idea of voting and being voted for became important and necessary. But before an individual can cast his or her vote, there are certain conditions to be met, one of which is to be registered as a voter. (Alhasnawi and Alkhalid, 2017).

The Federal Republic of Nigeria comprises of 36 states, the Federal Capital Territory (FCT), and 774 local government areas (LGAs). The country is located in West Africa and shares land borders with the Republic of Benin in the west, Chad and Cameroon in the east and Niger in the

north. The three largest ethnic groups in Nigeria are the Ibo, Hausa, and Yoruba ethnic groups. Nigeria as a focus for this research, general elections are conducted every four years, where a head of state the president and the national assembly representatives are elected. They are elected by the people. The national assembly has about 360 members representing various constituencies. (Ajayi, 2013).

Nigeria has been operating paper-based electoral systems for all her elections. This system involves printing ballot paper on which votes will be cast and distributing this paper to polling booths before the days of the election. After all, votes have been cast on election day, sealed boxes containing votes are opened before all legitimate members of the booth and counted. This information of counted votes is then submitted to a centralized station along with the paper evidence in the boxes. It is the duty of the central station to comply and publish the names of the winners and losers through television, radio, or another official channel. This entire system, as with any other electoral system is only useful if the system is transparent (Najam et al., 2018).

However, this has not been the case in Nigeria. Most citizens are of the opinion that elections held in Nigeria today are neither free nor fair. Ahmad et. al., (2015) put forward that “elections as an essential component of the democratization process remain weak and undeveloped in the country with the biggest challenge of transparency of the voting system”. Consequently, they argue, this leads to a loss of confidence and trust in the electoral process. Other challenges associated with the paper-based electoral system currently employed by the Independent National Electoral Commission (INEC) include and are not limited to, missing names of some registered voters, intimidation and disfranchisement of voters, multiple and underage voting, snatching or destruction of ballot boxes, miscomputation, and falsification of results. These challenges stimulate post-election related violence with the far-reaching consequence of eroding peoples’ trust and confidence in the democratic process (Ahmad et. al., 2015).

With this in view, it is necessary to adopt a better method of the electoral process. There is evidence pointing to electronic voting systems as the only means of achieving credible, fraud-free, and fair elections in Nigeria (Salimonu et al., 2013).

## **APPLICATION**

The online biometric electronic voting system discussed in this paper is an electronic voting machine when deployed will not only be power-efficient, secure, and easy to use for the electorate but characterizes elections with credibility, integrity, and vote authenticity.

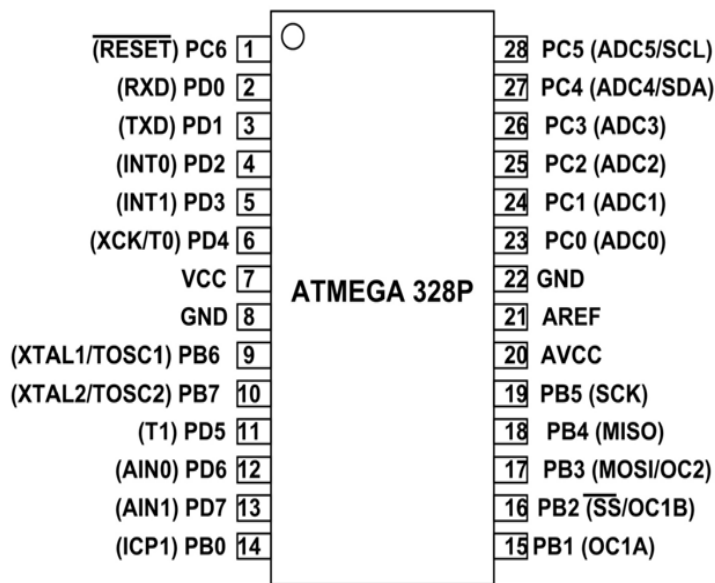
## **MATERIAL AND METHOD**

Electronic voting is simply the use of some electronic means or machinery that is more or less computer supported in voting, where election data is recorded, stored, and processed primarily as digital information. The main objective of the system is to take advantage on fingerprint

biometrics for voter verification and encryption of the template of each enrolled fingerprint for security. This is achieved by using a fingerprint biometric sensor, integrated via microcontroller to verify users of the system. The inclusion of biometrics improves the security features of the system. The brain behind this design is the microcontroller.

### **ATMEGA328P MICROCONTROLLER**

ATMEGA328P is a high performance, low power controller from Microchip. ATMEGA328P is an 8-bit microcontroller based on AVR RISC architecture. It is the most popular of all AVR controllers as it is used in ARDUINO boards. ATMEGA328 is used similarly to any other controller. All there to do is programming. The controller simply executes the program provided the programmer us at any instant. Without programming controller simply stays put without doing anything. ATMEGA328P is a 28-pin chip



**Fig 1: The ATMEGA328P chip (components101, 2020)**

Many pins of the chip here have more than one function. We will describe the functions of each pin in Table 1 below.

**Table 1. Pin Description of ATMEGA328P chip**

Pin No.	Pin name	Description	Secondary Function
1	PC6 (RESET)	Pin6 of PORTC	Pin by default is used as RESET pin. PC6 can only be used as I/O pin when RSTDISBL Fuse is programmed.
2	PD0 (RXD)	Pin0 of PORTD	RXD (Data Input Pin for USART) USART Serial Communication Interface [Can be used for programming]
3	PD1 (TXD)	Pin1 of PORTD	TXD (Data Output Pin for USART) USART Serial Communication Interface [Can be used for programming] INT2(External Interrupt 2 Input)
4	PD2 (INT0)	Pin2 of PORTD	External Interrupt source 0
5	PD3 (INT1/OC2B)	Pin3 of PORTD	External Interrupt source1 OC2B (PWM - Timer/Counter2 Output Compare Match B Output)
6	PD4 (XCK/T0)	Pin4 of PORTD	T0 (Timer0 External Counter Input) XCK (USART External Clock I/O)
7	VCC		Connected to positive voltage
8	GND		Connected to ground
9	PB6 (XTAL1/TOSC1)	Pin6 of PORTB	XTAL1 (Chip Clock Oscillator pin 1 or External clock input) TOSC1 (Timer Oscillator pin 1)
10	PB7 (XTAL2/TOSC2)	Pin7 of PORTB	XTAL2 (Chip Clock Oscillator pin 2) TOSC2 (Timer Oscillator pin 2)
11	PD5 (T1/OC0B)	Pin5 of PORTD	T1(Timer1 External Counter Input) OC0B (PWM - Timer/Counter0 Output Compare Match B Output)
12	PD6	Pin6 of PORTD	AIN0(Analog Comparator Positive I/P)

	(AIN0/OC0A)		OC0A (PWM - Timer/Counter0 Output Compare Match an Output)
13	PD7 (AIN1)	Pin7 of PORTD	AIN1(Analog Comparator Negative I/P)
14	PB0 (ICP1/CLKO)	Pin0 of PORTB	ICP1(Timer/Counter1 Input Capture Pin) CLKO (Divided System Clock. The divided system clock can be output on the PB0 pin)
15	PB1 (OC1A)	Pin1 of PORTB	OC1A (Timer/Counter1 Output Compare Match an Output)
16	PB2 (SS/OC1B)	Pin2 of PORTB	SS (SPI Slave Select Input). This pin is low when controller acts as slave. [Serial Peripheral Interface (SPI) for programming] OC1B (Timer/Counter1 Output Compare Match B Output)
17	PB3 (MOSI/OC2A)	Pin3 of PORTB	MOSI (Master Output Slave Input). When controller acts as slave, the data is received by this pin. [Serial Peripheral Interface (SPI) for programming] OC2 (Timer/Counter2 Output Compare Match Output)
18	PB4 (MISO)	Pin4 of PORTB	MISO (Master Input Slave Output). When controller acts as slave, the data is sent to master by this controller through this pin. [Serial Peripheral Interface (SPI) for programming]
19	PB5 (SCK)	Pin5 of PORTB	SCK (SPI Bus Serial Clock). This is the clock shared between this controller and other system for accurate data transfer. [Serial Peripheral Interface (SPI) for programming]
20	AVCC		Power for Internal ADC Converter
21	AREF		Analog Reference Pin for ADC
22	GND		GROUND
23	PC0 (ADC0)	Pin0 of PORTC	ADC0 (ADC Input Channel 0)

24	PC1 (ADC1)	Pin1 of PORTC	ADC1 (ADC Input Channel 1)
25	PC2 (ADC2)	Pin2 of PORTC	ADC2 (ADC Input Channel 2)
26	PC3 (ADC3)	Pin3 of PORTC	ADC3 (ADC Input Channel 3)
			ADC4 (ADC Input Channel 4)
27	PC4 (ADC4/SDA)	Pin4 of PORTC	SDA (Two-wire Serial Bus Data Input/output Line)
			ADC5 (ADC Input Channel 5)
28	PC5 (ADC5/SCL)	Pin5 of PORTC	SCL (Two-wire Serial Bus Clock Line)

### **R305 BIOMETRIC FINGERPRINT MODULE**

This is an optical biometric fingerprint reader/sensor (R305) module with TTL (Transistor-Transistor Logic) UART (Universal Asynchronous Receiver/Transmitter) interface for direct connections to a microcontroller UART. The user can store the fingerprint data in the module and can configure it in 1:1 or 1: N mode for identifying the person. This module can directly interface with any 3.3V or 5V microcontrollers, but a suitable level converter/serial adapter is required for interfacing with the serial port of a PC. (Hareendran, 2019).

Fingerprint processing includes two parts, fingerprint enrollment and fingerprint matching (the matching can be 1:1 or 1:N). When enrolling, the user needs to enter the finger two times. The system will process the two-time finger images, generate a template of the finger based on processing results, and store the template. When matching, the user enters the finger through an optical sensor, and the system will generate a template of the finger and compare it with templates of the finger library. (Hareendran, 2019).

For 1:1 matching, the system will compare the live finger with a specific template designated in the Module; for 1: N matching, or searching, the system will search the whole finger library for the matching finger. In both circumstances, the system will return the matching result, success, or failure.

The module itself does all complex tasks behind reading and identifying the fingerprints with an on-board optical sensor and fingerprint algorithm. All the programmer needs to do is send it

simple commands, and the fingerprint scanner can store different fingerprints. (Hareendran, 2019).

The database of prints can even be downloaded from the unit and distributed to other modules. As well as the fingerprint template, the analyzed version of the print, the programmer can also retrieve the image of a fingerprint and even pull raw images from the optical sensor. (Hareendran, 2019).

Although several fingerprint reader/sensor modules with slight variations are available, most have a 4-pin external connection interface. The R305 Biometric fingerprint module can communicate with a microcontroller (uC) runs on of 3.3V or 5V power supply. TX/TD pin of the module connects with RDX (RX-IN pin of the uC), and RX/RD pin connects with TXD (TX-OUT pin of the uC).

### **ACTIVATING THINGSPEAK ACCOUNT**

There are many open-source cloud platforms available today for IoT project integrations. Each platform has its specialty, for this application I was looking for something good in data logging and visualization and found Thingspeak.com to suit that purpose. I created an account with thingspeak.com to get started.

### **ACTIVATING THE ESP8266 MODULE**

The ESP8266 should be operated both in AT command mode and Programming mode for this project. The author used LM317 to regulate 3.3V for powering the ESP8266 module and connect the Tx Rx pins to FTDI (Future Technology Devices International) board The toggle switch can be used to toggle the ESP8266 between AT command mode and Programming mode and the push button can be pressed to reset the module. It was noted that the ESP8266 has to be reset every time before code is being uploaded to it.

The Circuit in figure 3 was only used to upload the program to ESP826. I replaced the FTDI board with Arduino UNO in the final set-up.

## **PROGRAMMING ALGORITHM**

- Step 1: Start the methodology.
- Step 2: Voter places his/her finger
- Step 3: Data sent to Arduino
- Step 4: Data sent to Server
- Step 5: Server data verification
- Step 6: If No, Display No Authorized user/voter
- Step 7: Go to step 2 and repeat the process
- Step 8: If Yes, Display Authorized used information
- Step 9: Go to voting machine
- Step 10: Vote for your preferred candidate
- Step 11: Press reset button for next voter
- Step 12: End process.

## **WORKING OPERATION OF THE ELECTONIC VOTING SYSTEM**

The finger print voting device is driven by a central Arduino Mega development board which has an onboard +5v regulator. Therefore, we have used an external +9volts and the onboard regulator regulates this external voltage to +5volts required by all the attached peripherals.

The attached peripherals are outlined as follows:

- M1 – Arduino Mega module
- sW1 – sW6-Push button switches
- LCD1 – Graphical LCD
- M4 – ESP8266 WIFI module
- M2 – Finger Print Module

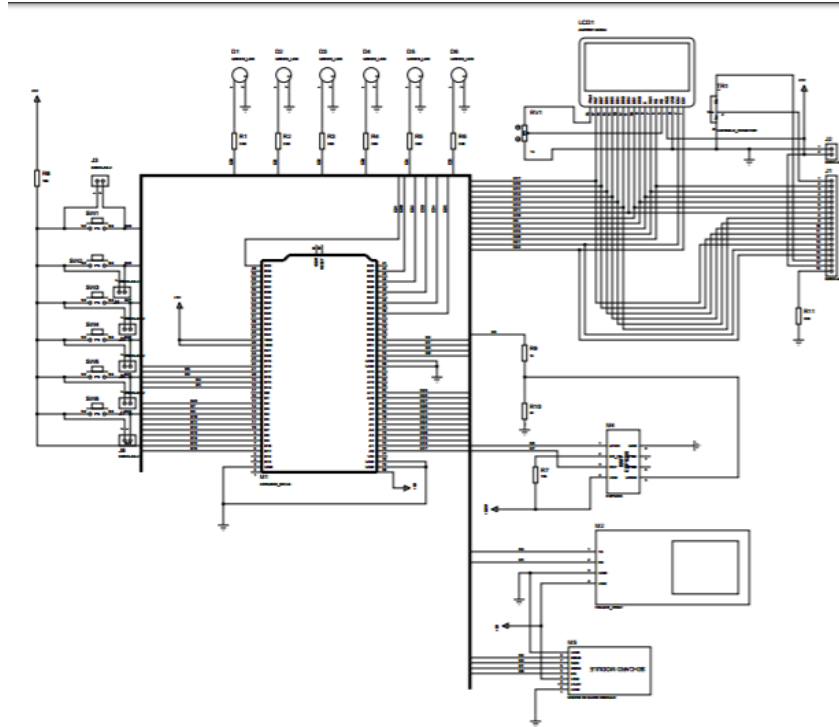




**Fig 2: Internet of Things (IoT) Biometric voting system**

**Source: Benson Idahosa University Lab, Nigeria**

As shown in the circuit diagram below, when the device is turned on, +5V is instantly supplied to all the attached peripherals. Instantly M4 begins to search for an available WIFI connection. This connection takes about 30 seconds to establish provided the available WIFI has the same preprogrammed SSID and password. Once this connection has been established, the screen defaults to a mode that allows a new voter to register or for an existing registered voter to vote. When the user depresses the left button, it indicates an intention to register. The finger print device then flashes a red light as an indication to accept the user finger print. When the user places his finger, the finger print is captured. The user is then prompted to remove the finger and place it again. This second placement confirms the finger-print and stores the template if the first and second finger placements match. Only registered finger-prints are eligible to vote. To vote, the user depresses the right button as an indication to vote. The device now prompts the user to place his finger on the finger print device and checks to see if the finger-print is registered. If it has been registered, the screen displays the political party logos. The user can then scroll to the preferred party and push the vote button. Once a vote has been successfully made, the device automatically increments the vote count of the said party and transfers the result to a cloud service at thingspeak.com. This result can be integrated into a web or mobile application which can allow viewing from anywhere in the world.



**Fig 3: Circuit diagram of online biometric electronic voting system**

### **DESIGN OF THE POWER SUPPLY UNIT**

The power supply unit performs the function of converting an AC source to a DC power which is needed to power the load section of the circuit. The power supply unit design involves the use of a step-down transformer, a rectifier circuit, a capacitor filter, and a voltage regulator.

### **DC PARAMETERS OF THE CIRCUIT**

For the design of the circuit, the following dc parameters were required

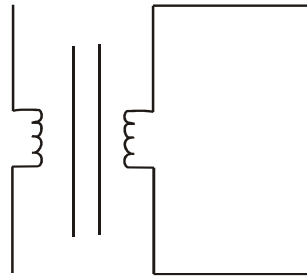
1. D.C current rating of the circuit = 300mA
2. D.C voltage rating of the circuit = 5V

### **TRANSFORMER DESIGN**

This is a step-down transformer having a rating of 240V, 300mA. The transformer converts the mains 220-240V to a voltage of 12V. The step-down transformer steps down the AC supply voltage to suit the requirement of the circuits.

220/ 240V, 50Hz.

12 V AC



**Fig 4: Schematic diagram of 12 volts, 300mA step down transformer (Akinmuyisitan T. M. and Dr. K. Obahiagbon, 2017)**

### RECTIFIER CIRCUIT

A bridge rectifier is a type of full-wave rectifier that uses four or more diodes in a bridge circuit configuration to efficiently convert the Alternating Current (AC) into Direct Current (DC). During the Positive half cycle of the input AC waveform diodes, D1 and D2 are forward biased and D3 and D4 are reverse biased. During the negative half cycle of the input AC waveform, the diodes D3 and D4 are forward biased, and D1 and D2 are reverse biased.

The peak voltage of the A.C rectified voltage is given as

$$\begin{aligned} \text{DC (out)} &= V_{\text{rms}} \sqrt{2} \\ &= 12 \sqrt{2} \\ &= 12 * 1.414 \\ V_p &= 16.9\text{V} \end{aligned}$$

### PEAK INVERSE VOLTAGE (PIV) OF THE DIODE

The peak inverse voltage (PIV) of the diode should be about 1.5 times the peak voltage of the A.C rectified voltage

$$\begin{aligned} \text{PIV} &= 1.5 * V_{\text{rms}} \sqrt{2} \\ &= 1.5 * 12 \sqrt{2} \\ &= 1.5 * 16.9\text{V} \\ &= 25.455 \text{ Volts} \sim 25\text{V} \end{aligned}$$

## **FILTER CIRCUIT**

The function of this circuit element is to remove the fluctuation present in the output voltage ( $V_{out}$ ) supplied by the rectifier. A capacitor filter was used.

## **CHOICE OF FILTER CAPACITOR**

Since the supply voltage is 12V, the minimum voltage of the capacitor will be as follows

## **CAPACITANCE RATING**

From the approximate ripple voltage formula,

$$V_r = \left( \frac{I_o}{2FC} \right)$$

$$C = \left( \frac{I_o}{2FV_r} \right)$$

Where

F = main frequency = 300mA

C= capacitance

$V_r$  = Ripple factor = 45% of  $V_{de}$  where 45% is the ripple factor

$$V_r = 45\% * 12 = 5.4$$

$$C = \left( \frac{I_o}{2FV_r} \right)$$

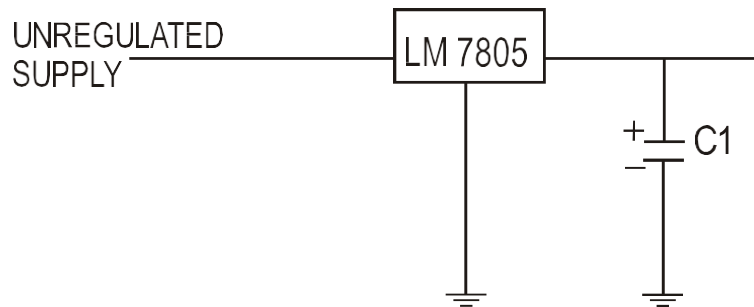
$$C = \left( \frac{0.3}{2*50*5.4} \right)$$

$$C = 5.55 \times 10^{-4}$$

Hence 1000microFarads was used

## **VOLTAGE REGULATOR**

Minimum input voltage is 7V, the maximum input voltage is 25V, operating current is 5mA, Internal thermal overload and short circuit limiting protection is available and Junction temperature maximum 125 degree Celsius.



**Fig 5: Constant 07 Volts circuit using LM 7805 (Akinmuyisitan T. M. and Dr.K.Obahiagbon, 2017)**

## RESISTORS

- Resistance values and limiting values
- Dissipation
- Current carrying capacity
- Tolerance or precision
- Temperature coefficient and 'initiation
- Maximum voltage limits
- Noise
- Voltage coefficient
- Frequency effect

To get the resistance of the circuit, we will use the power formula  $R = P / (I^2)$

Since  $V = 5v$  and  $I = 2$  amps, therefore  $P = 2.5$  watts

To find the resistance  $P = (I^2) * R$

$$R = P / (I^2)$$

$$R = 2.5 / (2^2)$$

$$R = 0.625 \text{ ohms}$$

## **Graphical LCD**

- 128×64 resolution
- Display monochrome images, custom texts in different fonts etc.
- Two ports, J41 and J42. By default, it can be connected to J43 (Port D) and J44 (Port A).

## **DISPLAY CALCULATION**

Since we know the value of the desired current and voltage, we can get the value of the voltage of the resistor.

Supply voltage  $V_{sc} = 5V$

Voltage desired = 2V

Therefore

$$V_r = 5V - 2V$$

$$V_r = 3V$$

## **SYSTEM IMPLEMENTATION AND MAINTENANCE**

This chapter discusses the step by step procedures undertaken to accomplish this work. It also briefs on the various tests conducted to ascertain the effective and satisfactory performance of each section of the project. The chapter also discusses how the materials used for the work were selected as well as the basic measures to be adopted for the maintenance of the system.

## **CIRCUIT CONNECTION**

Basically, all components/circuits were tested to ensure their satisfactory operation before they were finally mounted. The circuit that involved chips and their surrounding electronic components was first constructed and connected using the breadboard. When satisfactory results were achieved these components were now transferred to a Vero-board where they were permanently soldered. For the voting machine circuit, a PCB (i.e. printed circuit board) was used instead. Other units that are placed alongside others were connected separately and tested before being transferred to their respective positions in the construction.

For this design, the following module/component was connected together according to the circuit diagram shown in Figure 3:

- M1 – Arduino Mega module
- SW1 – SW6 Push button switches
- LCD1 – Graphical LCD
- M4 – ESP8266 WIFI module
- M2 – Finger Print Module
- 12V Adapter

The circuit of the IoT biometric fingerprint voting system is simple which contains the above components. The Arduino controls whole the process of the project.

The circuit was then arranged into the casing.

### **CASING AND ASSEMBLING**

This is an important aspect of the design work; it is the appearance given to the final work. After soldering on the Vero board, we do not leave it like that it has to be arranged in a case in such a way that looks attractive to the eye.

### **SOFTWARE DEVELOPMENT**

This is the computer programming, documenting, and testing involved in creating and maintaining applications and frameworks involved in the production of software.

### **PROGRAMMING LANGUAGE**

The software was developed with a C++ programming language that is user friendly and modification could be made from time to time and when necessary.

C++ is a powerful general-purpose programming language. It can be used to develop operating systems and software

### **HARDWARE TESTING**

After the construction of the circuit on bread board, testing was carried out to determine if the result obtained met the parameters used. Testing was carried out in various stages as the entire circuit was built on models. The first model consists of power supply unit then to the Arduino Uno and finally to the entire circuitry.

## SOFTWARE TESTING AND RESULTS

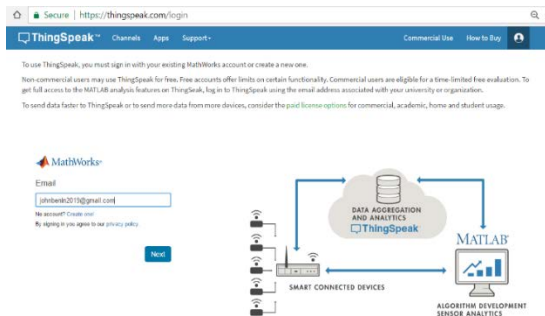
This is the result obtained after testing the system with the test plan and test data. During the testing, the actual and expected results were compared to ensure they produced same result or if there is a difference, it should be slight and negligible. Hence the result;

**Table 2.0 Comparison between expected and actual results**

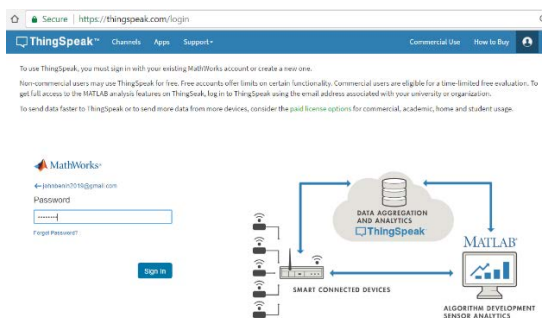
TEST CONDUCTED	EXPECTED RESULT	ACTUAL RESULT
Admin enters username and password	Admin should be able to access the main menu if the correct user name and password is entered properly.	Admin that enters the correct username and password was granted access to the main menu
Admin click on voter’s information	Admin enters a new voter Information to get his or her user details.	Admin was able to login to the system and view voters’ details
Voter login to cast vote	Voter login to view candidate and vote the candidate of choice	The voter was able to login and cast vote successfully.

## TEST PROCEDURES

### 1. Input email address (Thingspeak.com)

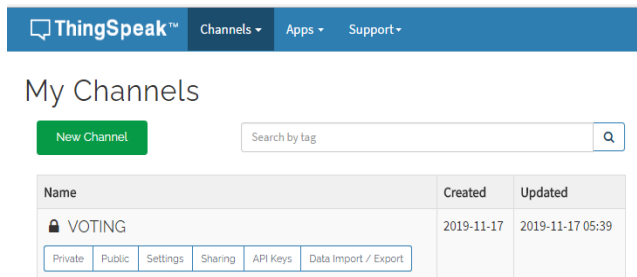


### 2. Input password (Thingspeak.com)



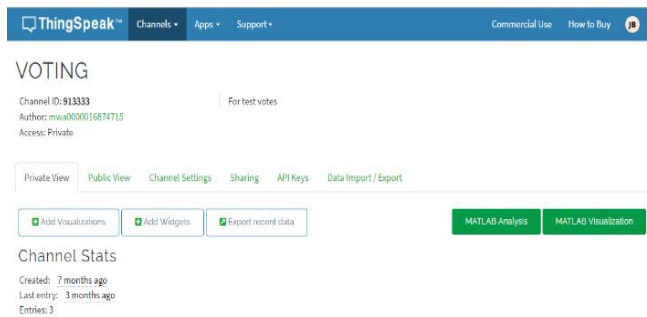


### 3. Channel page (Thingspeak.com)



Name	Created	Updated
VOTING	2019-11-17	2019-11-17 05:39

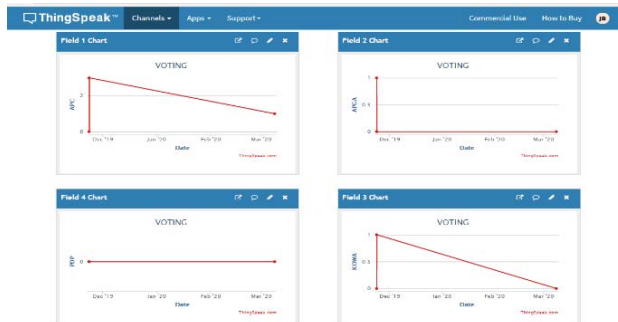
### 4. Channel statistics (Thingspeak.com)



Channel ID: 913333  
 Author: mwa000016874715  
 Access: Private

Channel Stats  
 Created: 7 months ago  
 Last entry: 3 months ago  
 Entries: 3

### 5. Graph (Thingspeak.com)



## MAINTENANCE

The maintenance of biometric equipment is vital to its effective use. Its maintenance includes;

1. Setup and clean up: Successful setup of a biometrics system hinges first and foremost on accurate registration of unique identifiers.
2. Regular cleaning of once every three months if not used.
3. Use the right cleaning tools

## **CONCLUSION**

A fingerprint-based voting machine using an embedded system is implemented. Design is done to meet all the requirements and specifications. The performance of the system is more efficient. Reading the Data and verifying the information with the already stored data and perform the specified task is the main job of the microcontroller. The mechanism is controlled by the microcontroller. The performance has been verified both in software and hardware design. The design implemented in the present work provides portability, flexibility, and data transmission are also done with low power consumption. Once the result is on the server it could be relayed on the network to various offices of the election conducting authority. Thus, the journal makes the result available any corner of the world in a matter of seconds IOT module is used to check the result in the website online. This journal has contributed to knowledge by reducing the stress and risks during elections. It has also reduced fraudulent activities such as the rigging of the ballot box. It is efficient and reliable.

## **REFERENCES**

- Ahmad A., Mohammed A and Diamond, L. (2015). The state of democracy in Africa. In National Intelligence Council (ed), *Democratization in Africa: what progress toward institutionalization?* Conference Report.
- Ajayi G. (2013). *The military and the Nigerian state, 1966-1993: a study of the strategies of political power control Africa* World Press, Trenton New Jersey.
- Alaguvel G. and Jagadhambal K. (2013) “Biometrics using Electronic Voting System with Embedded Security,” *International Journal of Advanced Research in Computer Engineering & Technology*, Vol. 2, No. 3, Pp. 2278 – 1323.
- Alausa D. and Akingbade, L. (2017) *Electronic Voting: Challenges and Prospects in Nigeria’s Democracy*,” *The International Journal of Engineering and Science*, Vol. 6, No. 5, Pp. 67-76.
- Alhasnawi M. and Alkhalid, A. (2017) “Secure Online Voting using Steganography and Biometrics,” *International Journal of Current Engineering and Technology*, Vol. 7, No. 3, Pp. 1097.
- Bañez N., Estrebou, C., Pasini, A., Chichizola, F., Rodríguez, I. and Pesado, P. M. (2013), “Biometric identification in electronic voting systems,” *In Ciencias de la Computación*, Pp. 1295.

- Barry C., Paul D., Tim. P. and Byrne (2005). Electronic Voting and Electronic Counting of Votes: A Status Report.
- Brian F. (2006) Government Accountability Office “Electronic Voting Offers Opportunities and Presents Challenges.
- Cho, D. Rem and Rein, L. (2006). "Fairfax to Probe Voting Machines Washingtonpost.com. <http://www.washingtonpost.com/wp-dyn/articles/A54432-2003Nov17.html>
- Dakota N. (2010). "Voter Registration in North Dakota" critical success factors of executive information systems.
- Di Franco, A., Petro, A., Shear, E., and Vladimirov, V. (2004). Small vote manipulations can swing elections.
- Ezeani, O. E. (2005). Electoral malpractices in Nigeria: The case of 2003 general elections. In G. Onu & A.
- Gelb, A. & Clark, J. (2013). Identification for development: The biometrics revolution. Working Paper 315. Centre for Global Development, Washington, D.C.
- Gelb, A. & Decker, C. (2012). Cash at your fingertips: Biometric technology for transfers in developing countries. *Review of Policy Research*, 29(1), 91–117.
- Golden, M., Kramon, E. & Ofosu, G. (2014). Electoral fraud and biometric identification machine failure in a competitive democracy. Available online at <http://golden.polisci.ucla.edu/workinprogress/golden-kramon-ofosu.pdf>.  
<http://golden.polisci.ucla.edu/workinprogress/golden-kramon-ofosu.pdf>.
- Itinfo (2018) software development methodologies available at [www.itinfo.am/eng/software-](http://www.itinfo.am/eng/software-)
- Kashif, H.M., Dileep K. and Syed M. U. (2011) “Next Generation A Secure E-Voting System Based on Biometric Fingerprint Method” 2011 International Conference on Information and Intelligent Computing IPCSIT vol.18 pp .26-27
- Kim, Z. (2008). "E-Vote Snafu in California County". *Wired*. <http://www.wired.com/politics/security/news/2004/03/62721>
- Krimmer, R., Triessnig, S. and Volkamer, M. (2010) “The Development of Remote E-Voting around the World: A Review of Roads and Directions”. *Springer Lecture Notes in Computer Science*, Volume 4896/2007, pp. 1-15, 2007
- Lawal, K. (2008, May 12). 2007 Elections: Courts receive 6, 180 cases. *The Herald*, pp. 1 & 23.
- Martin E. (2009), Voter Registration: An International Perspective. Fair Vote Research Report

- Momoh (Eds.), Elections and democratic consolidation in Nigeria (pp. 413431). A Publication of Nigerian Political Science Association.
- Najam S, Shaikh, A and Naqvi, S.2018) “A Novel Hybrid Biometric Electronic Voting System: Integrating Finger Print and Face Recognition,” Mehran University Research Journal of Engineering and Technology, Vol. 37, No. 1, Pp. 59–68
- Odeh, J. O. (2003). This madness called election 2003. Enugu: SNAAP Press Limited.
- Okolie, A. M. (2005). Electoral fraud and the future of elections in Nigeria: 1999–2003. In G. Onu & A. Momoh (Eds.), Elections and democratic consolidation in Nigeria (pp. 432447). A Publication of Nigerian Political Science Association.
- Oladimeji, A. D., Olatunji, A. E. & Nwogwugwu, N. N. (2013). A critical appraisal of the management of 2011 General Elections and implications for Nigeria’s future democratic development. Kuwait Chapter of Arabian Journal of Business and Management Review, 2(5), 109-121.
- Olaniyi, O. Taliha, F. Ahmed, A., and Joseph, O. (2016) “Design of Secure Electronic Voting System Using Fingerprint Biometrics and Crypto Watermarking Approach,” International Journal of Information Engineering and Electronic Business, Vol. 8, No. 5, Pp. 9 – 17.
- Olaniyi O., Taliha, F., Abdullahi, I. and Abdusalam, A. (2015) Design and Development of Secure Electronic Voting System Using Radio Frequency Identification and Enhanced Least Significant Bit Audio Steganographic Technique.,” Journal of Computer Engineering, Vol. 17, No. 6, Pp. 2278 - 2661,
- Omotola, J. S. (2010). Elections and democratic transition in Nigeria under the Fourth Republic. African Affairs, 109(437), 535–553. Doi:10.1093/afraf/adq040.
- Patni, G. and Sharma S. (2017) Biometric System Introduction with its various Identification Techniques,” International Journal of Scientific Research in Computer Science, Engineering and Technology, Vol. 2, No. 3, Pp. 866 – 871.
- Salimonu, E., Ruth A. and Robert E. (2013), Voter Registration: An International Perspective. Fair Vote Research Report.
- Saxena P., Prakash S. and Pandey P. (2017) “Design of Biometric Electronic Voting Machine.,” International Journal of Advanced Research, Ideas and Innovations in Technology, Vol. 3, No. 6, Pp. 211 - 214
- Sudhakar M., Divya, B., and Sai, S., (2015) Biometric System Based Electronic Voting Machine Using Arm9 Microcontroller.,” IOSR Journal of Electronics and Communication Engineering Vol. 10, No. 1, Pp. 2278 – 2834.