A BIOMETRIC BASED STAND-ALONE ELECTRONIC VOTING UNIT FOR E-VOTING IN NIGERIA

By

G. O. Uzedhe, and J. E. Okhaifoh
Electrical & Electronic Engr. Dept.,
Federal University of Petroleum Resources,
Effurun, Delta State, Nigeria
E-mail: osmenawin22@yahoo.com & jokhaifoh@yahoo.com

ABSTRACT

This paper presents the design of an electronic voting machine suitable for the implementation of transparent e-voting frameworks and cut the cost of running elections using the otherwise traditional means. The system presented here, makes it possible to handle the elections processes in a more effective way through biometric authentication. This biometric based small scale electronic voting machine is designed to handle a limited number of candidates with options for upgrades to meet future demands. A user can be registered and verified through a biometric finger reader and an alphanumeric keypad. The voting procedure and final result can be seen on an LCD interface. The system's operational algorithm and interface management procedures are embedded into an ATMEGA2560 microcontroller which serves as the central processing unit (CPU). The CPU also connects to a GSM radio device that sends election results to the central collation office for further actions through SMS. The result obtained shows that the machine is able to do two major functions separately and independent of each other; register voters prior to Election Day and carry out the voting process by allowing only eligible voters earlier registered to vote after verification. The results also show that voter registration and elections can be carried out at a reduced time with an average registration time of 22.67sec and an average voting time of 32.93sec per voter.

Keywords: Biometric, voting, GSM, Election, SMS

INTRODUCTION

Democracy is becoming more acceptable internationally as a better form of government. One key factor for this international acceptance of democratic governance is the degree of power given to the citizenry in deciding the affairs of the state such as electing their leader, through referendum and public polls.

Recently in this present era, countries and states globally are exploring new technology frontiers to connect with their citizens more closely. In relation to technological progress, exploring methods of increasing involvement in democracy and sovereign institutions has become more important, as electronic participation media presents a seamless communication process between the electorates and their elected representatives. Currently, emerging information policies and instruments have made electronic governance globally encompassing. Since their initial introduction (Barlow, 2003), electronic government services have been continuously growing and evolving in sophistication. Information and Communication Technologies (ICT) are continuously being introduced into various aspects of the electoral process. Back-end computers are now an integral part of almost all elections held internationally (Douglas, 2001). Even in countries not officially exploring electronic voting implementations, back-end computer systems are most used at some stage of the electoral process, either for ballot counting or for voter list

generation. Voter registration databases are now automated, ballots are cast into computer based equipment in an ever-increasing number, and results are often computed and transmitted electronically to necessary locations. These back-end computers could be more dreadful (Jacobs and Pieters, 2009) than an efficiently designed and protected electronic voting system (Al-Ameen and Talab, 2013). It will be difficult to stop electronic voting in our technically oriented society (Ananda et al), where more number of processes link the electronic world and the mobility of voters is increasing. It is apparent, in this present time that the basic questions no longer focus on whether information technology should be accepted in the electoral process, but rather on what kind of technology to be implemented and to what extent.

In recent years, official pilots and trials have been held internationally, by a number of countries, aiming to evaluate the benefits and drawbacks of electronic voting Uzedhe and Okhaifoh (2016), but evidence does not seem to be conclusive; mostly due to the diversity of the systems implemented, which are meant to support a mixed range of contexts and requirements. Although the benefits of introducing electronic voting systems are often stated, concerns which are most often voiced are not just based on the security risks, but also sociological and political implications, that may be raised from the introduction of this technology. Using digital technologies between governments and the "people" is a process necessary to be viewed within a wider framework. Electronic voting is a social and political project not just a technical project and must be handed with a verifiable structure.

Electronic voting technology can speed up the entire electoral process as was demonstrated in the Brazilian general election in which after the winners were determine in few minutes after the close of election (Filho et al, 2003). E-voting technology can also reduce both the short and long-term cost of elections. In the short term, it can reduce the manpower required in the conduct of election by a very large per cent, eliminate the cost of producing specialized Identity Cards for voters and most interestingly remove the cost of printing ballot papers and result sheets totally. In the long term, there will be significant savings from the reduction in numerous post-election litigations that usually characterized the traditional voting system.
E-voting can also improve accessibility for disabled voters, and eliminate multiple voting completely. All these will positively affect the outcome of election and reshape the present political ideologies for better elections.

In this paper, an automated standalone e-voting machine was designed and constructed. It allows a voter to walk into the polling unit for which he has been registered prior to the election, insert his fingerprint on the machine-humane interface which verifies the voter using automated fingerprint identification system (AFIS). If the voter is verified, the kiosk automatically grants access to the voter through it access control unit. Once the voter is authenticated he gains access to vote. At the close of voting the results of the election are automatically tallied and winners for the polling unit displayed outside the voting booth and a true electronic copy of the result is automatically transmitted to the central database for a final collation. A back up copy of the result is also stored in a tamperproof non-removable memory for the purpose of auditability.

Review of Existing System

Electronic voting system has brought revolutionary change in the traditional manual voting system. It makes the voting process simple and people friendly (Alaguvel, Gnanavel, and Jagadhambal, 2013). The main purpose of an e-voting machine is to record votes and provide result very fast. The term "electronic voting" is potentially broad, and refers to several distinct possible stages of electronic usage during the course of an election.

The electronic voting system is emerging as one of most preferred system in the 21st century. It may be adopted in the entire voting process or just a part of

the process. The use of electronic-voting machines has been faced with so many challenges over the years. Scientists who have done work in, or are interested in electronic-voting all seem to agree on two things:

i. Internet voting does not meet the requirement for public elections.
ii. The widely developed voting systems need improvement.

Voting on the internet using everyday computers offer only weak security, but its main disadvantages are in the areas of anonymity and protection against coercion and/or vote selling (Bungale and Sridhar). A review of electronic voting machines (Kumar and Begum, 2012) reveals that there is a strong need for biometric based e-voting devices to mitigate the security of electronic voting. Iloanusi and Osuagwu (2008) in an overview of biometric recognition processes and a comparison of their performance indicates that iris and fingerprint biometric recognitions are much more suitable for electronic voting devices. Sudhakar and Sai (2015) in their work developed a biometric based e-voting system with a Arm9 microcontroller which connects to a central server through its Ethernet interface. In a similar work, Anandaraj et al (2015) and Anjum et al (2014) presented secured biometric based voting machines with databases held in a connected PC. The work of Syed et al (2015) provided a better secured biometric based e-voting device as a standalone system that is not connected to external devices. It however implements a removable SD card as its database. Though the authors claimed a non-evasive security of the system, the use of such removable data card could impose a strong security threat. Biometric security alone cannot however be guaranteed if a process information can be accessed from a centre server or any external device. It is therefore necessary to draft out operational criteria to enhance the development of biometric based e-voting machines.

Ncumann (1993) gives a list of suggestions for "generic voting criteria" which suggests that a voting system should be so hard to tamper with and so resistant to failure that no commercial system is likely to ever meet the requirements and developing a suitable custom system would be extremely difficult and prohibitively expensive.

The NSF Voting Report (2001) addresses the feasibility of different forms of internet voting from both the technical and social science perspectives, and defines a research agenda to pursue if internet voting is to be viable in the future. It groups internet voting systems into three general categories as follows:

i. Poll-site internet voting: It offers the promise of greater convenience and efficiency in that voters could cast their ballots from any poll-site, and tallying process would be both fast and certain more importantly, since election officials would control both the voting platform and physically managing the security risks of such systems is feasible.
ii. Kiosk voting: Voting machines would be located away from traditional polling places in such convenient locations as malls, libraries, or schools. The voting platforms would still be under the control of election officials, and physical environment could be modified as needed and monitored. (E.g. by election officials' volunteers or even cameras) to address security and privacy concerns, and prevent coercion or other forms of intervention.
iii. Remote internet voting: It seeks to maximize the convenience and access of the voters by enabling them to cast ballots from virtually any location that is internet accessible. While this concept is attractive and offers significant benefits, it also poses substantial security risks and other concerns relative to civic culture. Current and near-term technologies are inadequate to address these risks.

METHODOLOGY AND SYSTEM DESIGN

Polling administration is a very important aspect of any electoral process and devices used must be acceptable to voters and concern bodies. Electronic

voting devices must then be tailored towards voter's satisfaction while still ensuring accuracy, transparency, and trust. As pointed out by Uzedhe and Okhaifoh (2016), problems could arise if the representation of these devices are not open enough — both in hardware and software development.

Standalone polling units can be complex to develop if all measures must be considered in terms of human behaviour. The units must however be made simple enough to reduce polling time and encourage voter participation. Of course, the polling unit must be compact enough but not complex to setup, and should be provided with a simple access. The voter should easily understand the voting process; therefore, the system must have a very simple interface for text and graphics information. The units should be made to be adaptable to different weather conditions and tamper proof against physical security.

To handle this complexity with simplicity, the work presents a modularized micro-processing method in which simple modular units are interfaced through a control software algorithm. By this method, the control algorithm is embedded in a microcontroller and interacts with modular agent algorithms that coordinate the activities of each modular interface. The two most notable modular agent algorithms handle voter registration and voter verification. These modular agents are individually enabled to take control of the physical modular devices with the flexibility to switch from one function to another. This software agent device sharing method makes it possible to provide a very simple user interface that can help speeds up electoral processes. Unexpected human behaviour is handled through error notations and switch-back modes. These modes include access denial and process cancellation that helps to avoid vote invalidation and swing voting.

Design Analysis

In the design for this project, the most important requirements were characterized as:

i. Voters are only eligible to vote if their biometrics are found in the database.
ii. Eligible voters are verified and authenticated by their unique characteristics.
iii. Eligible voters are not allowed to cast more than one vote.
iv. Result of election should be secret until the end of an election.
v. Voter privacy must be ensured
vi. While voting is on, there should not be a method of knowing intermediate result that can affect the remaining voters' decisions
vii. All valid votes must be counted correctly and the system outputs the final tally.

With these requirements in mind, the standalone voting unit must include a dynamic database in an in-built memory device form which can be updated at all times but with the capacity to retain its content. There must be an algorithm to control the flow of data with necessary data protection through encryption or other data protection techniques. The data protection process is a necessary step to voter verification, authentication, security and privacy. Therefore, the voting unit should include such device that can help identify unique treat of voters and as well contain modular agent algorithms for proper identification. Such algorithm must be able to authenticate the uniqueness of a voter's treat. It must also verify whether the voter have been registered or not, or that he/she has voted or not. Of course, the use of such an algorithm ensures that multiple registrations are not allowed to a single voter and that a voter cannot cast more than one vote in a single election.

Voter privacy is a very important tool that can affect participation and swing voting. Therefore, the design of the standalone unit must be done to avoid the possibility of other voters or the official predicting which candidate or party a particular voter cast for. Such secrecy occasioned by voter privacy will secure the electoral process and greatly improves voter participation and reduce swing voting.

The final result of an election from a voting unit is very important aspect of the process. Here, trust must be guaranteed by a way of using a trustworthy algorithm that tallies the votes correctly. This part of the algorithm must be open for people of all interest and verifiable that the results are skewed in favour of any candidate or party.

In order to meet with the requirement of the electronic voting machine, the hardware system was sectioned into units as shown in Figure 1. These units which include the balloting unit, the identification unit, the communication unit, display unit, and alarm unit, interfaced the processing unit with respect to their individual component specifications and data and/or control protocol.

Hardware Design

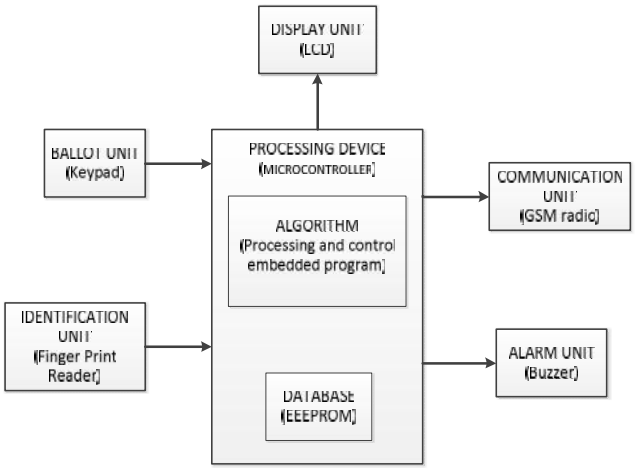

Figure 1: System block diagram

Ballot Unit

The ballot unit is implemented using an alphanumeric keypad connected to the digital pins of the Arduino mega 2560. Different function keys are used to represent the candidates for each category of election during a voting session. The functions can be adjusted depending on the type of election. For each category of election, the number of candidates determines the number of function keys configured for selection to prevent the possibility of invalid votes. Only one key can be pressed for each category. This condition was also set to prevent multiple voting. The microcontroller reads the output state of the buttons of the keypad in real time, once a high state is detected on any of the buttons, the vote for that candidate is incremented by one provided all necessary voting conditions have been met.

Identification unit:

One of the key requirements of the system is that only eligible voters are allowed to vote. Therefore, authentication and verification must be done through identification of voter specific treats. In this work, an automated fingerprint identification unit was used to achieve this requirement. The biometric finger print reader (R305) applied here is a small embedded module that consists of an optical sensor mounted on a small circuit board. The optical sensor scans a fingerprint and the microcontroller and software codes provides the modules functionality which automatically processes the scanned fingerprint. The module is responsible for the reading and identification of the fingerprints with an on-board optical sensor and a 32-bit CPU. This device was selected based on its specification as shown in Table 1.1 and its compact nature that allow easy mounting.

Table 1: R305 Module Specification (Source: www.rhydolabz.com)

Power	DC 3.6V-6.0V	**Interface**	UART(TTL logical level)/ USB 1.1
Working current	150mA (max)	**Matching Mode**	1:1 and 1:N
Baud rate	(9600*N)bps, N=1—12	**Character file size**	256 bytes
Image acquiring time	<0.5s	**Template size**	512 bytes
Storage capacity	256	**Security level**	5 (1, 2, 3, 4, 5(highest))
False Acceptance Rate	<0.001%	**False Rejection Rate**	<0.1%
Average searching time	< 1s (1:1000)	**Window dimension**	18mm*22mm
Working environment	Temp: -10°C- +40°C RH: 40%-85%	**Storage environment**	Temp: -40°C- +85°C RH: <85%

Communication unit

The communication unit consists of a GSM radio modular device that sends that enables connection to the central administration office. The radio implements two different interface protocols that enable connection to either a microcontroller or a PC. With its TTL output protocol, a range of microcontrollers can easily be linked to the GSM network for communication with available devices. The radio device also provides access to a Personal Computer (PC) through an RS232 protocol. The radio device module also has provisions to attach microphone and speaker, to take out +5V or other values of power and ground connections. These types of provisions vary with different modules. SIM900A GSM Module was used in this project, since it supports communication in 900MHz band. This is the band in which most mobile network providers in Nigeria operate. The SIM900 GSM module includes features such as: Dual-Band 900/ 1800 MHz, GPRS multi-slot class 10/8, GPRS mobile station class B, Compliant to GSM phase 2/2+, Class 4 (2 W @900 MHz), Class 1 (1 W @ 1800MHz), Control via AT commands (GSM 07.07, 07.05 and SIMCOM enhanced AT Commands), Supply voltage range: 3.1- 4.8V, Low power consumption: 1.5mA(sleep mode) and Operation temperature of -40°C to +85°C

Display unit

The display unit is a Liquid Crystal Display (LCD) and provides a dynamic human-machine interface for the voting unit. With the LCD all operations, during voter registration and voting processes, are made interactive to the user. The LCD used in this project work, is a 20-character by 4-line LCD module that is readily available. This was considered for the design to meet with required system non-complexity and the fact that it offers enough character blocks needed certain configuration commands.

Alarm unit

The alarm unit is a buzzer that is enabled by the processing unit to trigger an alarm sound whenever there is an error indication. The power requirement of the buzzer is +5v dc supply and can be controlled from a single pin of the microcontroller.

Database

The system's database is implemented in the microcontroller internal EEPROM memory (which stores the votes accumulated) and the fingerprint module internal memory that provides a database for storing the biometrics of all voters registered prior to the voting process.

Processing unit

As shown in Figure 2, the processing unit contains mainly a microcontroller (ATmega2560) which

served as the system's CPU. It houses the main processing and control algorithm that enables connection to other peripheral devices. The processing unit handles all process manipulations, protocol management and peripheral device control. The selection of ATmega2560 is mainly due to its numerable features that made it a good choice for the voting machine. It has internal EEPROM memory of 4Kbyte with data retention of up to 20years at 85°C which makes it possible to store enough information in the unit with little or no cost for a long period of time. With its 8Kbyte internal RAM, data and I/O manipulation is flexible and adaptable. The ATmega2560 implements the necessary interface protocols (I^2C, SPI, USART) that provides robust interface with other external devices. The device runs an Advanced RISC Architecture that enables the use of few number of program code to implement complex functions.

Software Design

Modern electronic systems are made of two dependent components that create flexibility, controllability at reduce complexity and physical size. The software component design needs a proper consideration to ensure system requirements are met. It implements the systems algorithms as control sequences for necessary operations. The algorithms are the formal definition of the system functions and must be properly considered in order to present the right operation to the user. The function definitions of the standalone electronic voting machine are extraction of the system's requirement and are listed here as follows:

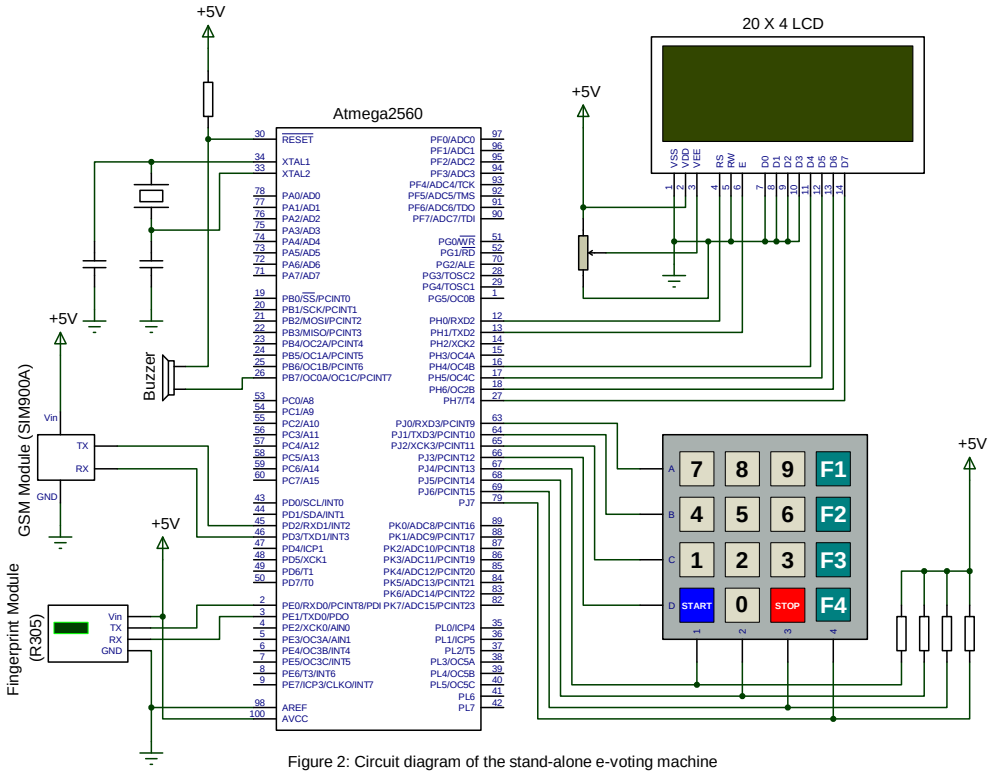

Figure 2: Circuit diagram of the stand-alone e-voting machine

i. System initializes at power-up—LCD turned on, finger print sensor activated and with a beep from the buzzer.

ii. Administrative access information—LCD displays instruction to grant access to its two main features: enrolment of voters and voting respectively.

iii. Password—to access any of the two features, a unique administrative password is required.

iv. Starting and Stopping a section—the use of the 'START' and 'STOP' buttons begins and ends each section of the enrolment and voting processes.

v. User interaction—the machine must be interactive all through a process, providing a simple step by step guideline to the user.

vi. Multiple registration—during registration, an individual who has been registered before cannot be registered again.

vii. Voter access permit—before voting, every voter must be identify and only permitted to vote, if his/her identity is found on the database.

viii. Multiple vote casting—a registered voter is only permitted to vote once after which access must be denied.

ix. Closing the voting process—to end a voting process, an administrative password is required to prevent illegal process termination.

x. Result publications—at the close of electoral process, results are displayed on the LCD and copies sent through SMS to the central administrative office.

3.3.1 Agent Algorithms

As mentioned in section 3.0, a number of modular agent algorithms are needed to handle different aspects of the standalone electronic voting system. Figure 3 shows the main control algorithm that provide link to the two major modular algorithms for registration process (Figure 4) and the voting process (Figure 5).

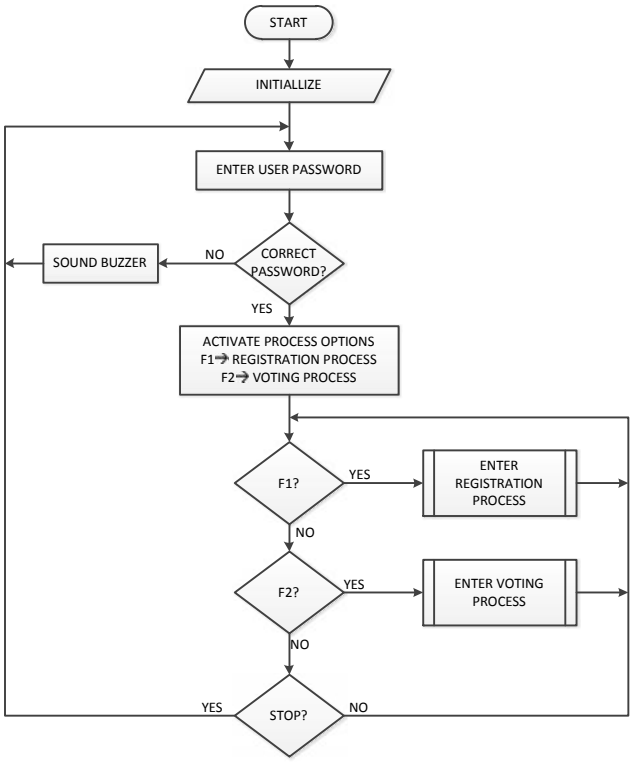

Figure 3: Main Device Control Algorithm

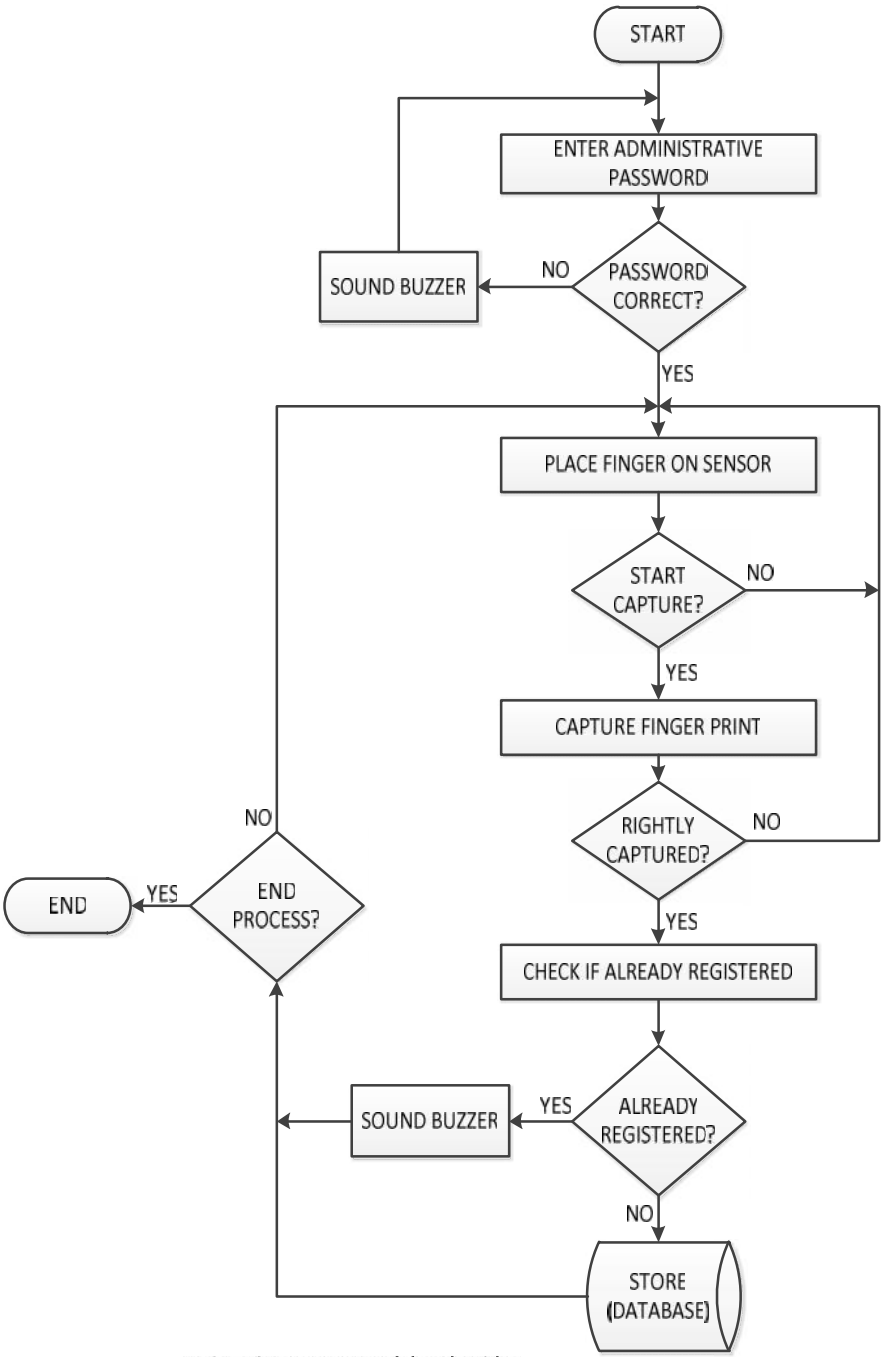

Figure 4: Registration Process Modular Algorithm

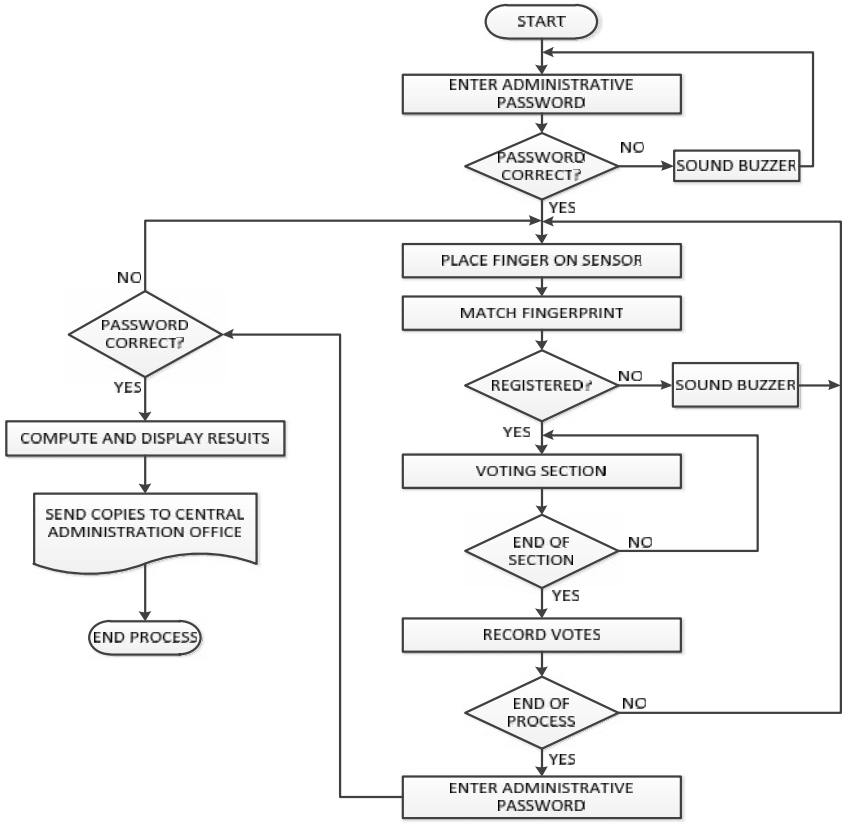

Figure 5: Voting Process Modular Algorithm

RESULTS

To test the operation of the standalone voting machine shown in Figure 6, a sample of fifteen students were asked to register secretly with either the right or left thumb. After registration, they were asked to vote cast vote for three choices with a YES or NO option by pressing F1 for YES and F2 for NO on the keypad. The results of these experiments are as tabulated in tables 2 and 3.

Figure 6: Finished standalone biometric e-voting

Table 2: Process timing and Choice Selection

SN	REGISTRATION TIME (in seconds)	VOTING TIME (in seconds)	VOTING CHOICE			REMARK
			PRESIDENT	SENATE	HOUSE OF REP	
1	27	35	NO	YES	YES	Successful
2	25	34	NO	YES	NO	Successful
3	23	31	YES	NO	YES	Successful
4	24	33	YES	YES	NO	Successful
5	24	33	NO	YES	YES	Successful
6	22	32	NO	YES	NO	Successful
7	26	30	NO	YES	YES	Successful
8	27	31	YES	NO	YES	Successful
9	29	33	YES	NO	NO	Successful
10	21	37	YES	YES	NO	Successful
11	20	34	YES	NO	NO	Successful
12	23	34	NO	YES	NO	Successful
13	28	35	YES	NO	YES	Successful
14	22	31	NO	YES	NO	Successful
15	23	31	YES	NO	NO	Successful
	Total: 340s = 5.67min Average: 22.67s	Total: 494s = 8.23min Average: 32.93s				

Table 3: Voter Authentication and Verification

SN	VOTER REGISTRATION SIGNATURE FINGER	1st VOTER VOTING SIGNATURE FINGER	REMARK	2nd VOTER VOTING SIGNATURE FINGER	REMARK
1	Left thumb	Right thumb	NR	Left thumb	R
2	Left thumb	Left thumb	R	Left thumb	AV
3	Right thumb	Right thumb	R	Right thumb	AV
4	Left thumb	Left thumb	R	Left thumb	AV
5	Left thumb	Left thumb	R	Right thumb	NR
6	Right thumb	Right thumb	R	Left thumb	AV
7	Right thumb	Left thumb	NR	Right thumb	R
8	Left thumb	Right thumb	NR	Right thumb	NR
9	Right thumb	Left thumb	NR	Right thumb	R
10	Left thumb	Right thumb	NR	Left thumb	R
11	Right thumb	Left thumb	NR	Right thumb	R
12	Right thumb	Right thumb	R	Right thumb	AV
13	Right thumb	Right thumb	R	Left thumb	NR
14	Right thumb	Left thumb	NR	Right thumb	R
15	Left thumb	Right thumb	NR	Left thumb	R

AV→Already Voted, R→Registered, NR→Not Registered

As seen from table 1, the fifteen students registered for the exercise in a total of 5.67min with an average registration time of 22.67s. The total voting time for these fifteen students as shown is 8.23min with an average voting time of 32.93s. Table 3 shows that eight students try at first to vote with the wrong finger and the machine responded that they are not registered. On a second-round voting, three students voted with the wrong finger and the machine responded with Not Registered (NR). The machine equally responded Already Voted (AV) for five students who attempted to vote again with the correct finger.

CONCLUSION

E-voting is an important process that must be considered if transparency and trust must be built with increase participation. Such voting system are undoubtedly better than the orthodox ballot voting system which is quite expensive to conduct, and faced with a lot of irregularities. The results from this work have shown that elections can be conducted faster and at reduced cost since the e-voting machines are adaptive and re-usable over a long period of time. The security layers and technology featured in the gadget would surely serve as a basis for conducting secured elections. Voting process with this system overcomes most of the problems faced during the election period and its adoption for use in any electoral process will build confidence on our national elections.

REFERENCES

1. Lelia Barlow (2003), "An Introduction to Electronic Voting", https://pdfs.semanticscholar.org/87e0/50a900fce2fbc373fa3e5f33ac7f80ed4032.pdf , [17/05/17].
2. Douglas W. Jones (2001), "Counting Votes with Computers", presented for the League of Woman Voters of Johnson County, Iowa City, Iowa May, http://www.cs.uiowa.edu/~jones/voting/
3. Bart Jacobs and Wolter Pieters (2009), "Electronic Voting in the Netherlands: from early Adoption to early Abolishment", Published in: Foundations of Security Analysis and Design V: FOSAD 2007/2008/2009 Tutorial Lectures. Springer LNCS 5705, p. 121-144.
4. Abdalla Al-Ameen and Samani Talab (2013), "The Technical Feasibility and Security of E-Voting", *The International Arab Journal of Information Technology, Vol. 10, No. 4, pp397—404.*
5. Dev Ananda, Amanda Bui, Janet Gonzalez and Martha Prempeh, "The Future of E-Voting", Information Technology and Public Policy, https://courses.cs.washington.edu/courses/csep590/04au/clearedprojects/Ananda.pdf , [17/05/17]. Ppl—27.
6. G. O. Uzedhe and J. E. Okhaifoh (2016) "A Technological Framework For Transparent E-Voting Solution In Nigeria Electoral System", Nigerian Journal of Technology (NIJOTECH), Vol. 35 No. 3, pp. 627—636. www.nijotech.com
7. R.N. Costa Filho, M.P. Almeida, J.E. Moreira, J.S. Andrade Jr, (2003) "Brazilian elections: voting for a scaling democracy", Science Direct, Physica A 322, pp. 698 – 700.
8. Alaguvel R., Gnanavel G., and Jagadhambal K. (2013), "Biometrics using Electronic Voting System with Embedded Security", *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2, Issue 3, pp1065—1072.*
9. Prashanth P. Bungale and Swaroop Sridhar, "Requirements for an Electronic Voting System", Department of Computer Science The Johns Hopkins University, http://www.cs.jhu.edu/~rubin/courses/sp03/group-reports/group4/group4_requirements.pdf , [17/05/17]
10. D. Ashok Kumar and T. Ummal Sariba Begum (2012), "Electronic Voting Machine – A Review",

Proceedings of the International Conference on Pattern Recognition, Informatics and Medical Engineering, https://www.researchgate.net/profile/Ashok_Kumar_D/publication/261394443_Electronic_voting_machine_-_A_review/links/5569639608aeab777220fce6.pdf , [17/05/2017]

11. Iloanusi, O. N and Osuagwu C. C, (2008) "Biometric Recognition: Overview and Applications", NIGERIAN JOURNAL OF TECHNOLOGY, VOL. 27 NO.2, pp36—45.
12. M.Sudhakar, B.Divya Soundarya Sai (2015), "Biometric System Based Electronic Voting Machine Using Arm9 Microcontroller", *IOSR Journal of Electronics and Communication Engineering (IOSR-JECE), Volume 10, Issue 1, Ver. II, PP 57-65.*
13. Anandaraj S, Anish R and Devakumar P.V. (2015) "Secured Electronic Voting Machine using Biometric", IEEE Sponsored 2nd International Conference on Innovations in Information,Embedded and Communication systems (ICIIECS), http://wineyard.in/Abstract/mtech/Embedded/2015/bp/15EM32.pdf , [17/05/17].
14. B.Farhath Anjum M.Deepa Mrs.C.N. Kalaivani, (2014) "Advanced Microcontroller Based Bio-Metric Authentication Voting Machine", IOSR Journal of Engineering (IOSRJEN), Vol. 04, Issue 05, ||VI|| PP 29-40.
15. Syed Razwanul Haque, Miah Md. Asaduzzaman, Prasanta Bhattacharjee, Akhlak Uzzaman Ashik, Robi Kormokar (2015), "Finger Print Enabled Electronic Voting Machine with Enhanced Security", International Journal of Engineering and Technology Volume 5 No. 6, pp368—374.
16. Neumann, P. (1993) "Security Criteria for Electronic Voting", *Proceedings of the 16th National Computer Security Conference*, Baltimore, MD. http://www.csl.sri.com/users/neumann/ncs93.html , [17/05/17]
17. National Science Foundation (US), https://www.nsf.gov/od/lpa/news/press/01/pr0118.htm , [17/05/2017]

