NIPES

Advances in Engineering Design Technology

Journal homepage: www.nipesjournals.org.ng

Self-Reporting Electronic Voting System for Use in Nigeria

[a]S. Akinbohun, S.T. Apeh[b]

[a,b] Computer Engineering Department, University of Benin, Benin City, PMB 1154, Ugbowo, Nigeria

ARTICLE INFORMATION

Article history:
Received 03 March 2019
Revised 14 March 2019
Accepted 25 March 2019
Available online 29 February 2019

Keywords:
Electronic voting, Paper ballot, Biometric Encryption (BE), Framework, Direct recording electronics

ABSTRACT

Voting is an electoral system act in which an organization, community or party use for selecting their executives or representatives. This paper focuses on sysrecording, casting and/or counting of votes by use of electronic metem that supports the ans. The self-reporting e - voting system is modeled using the e-voting architecture. This system makes use of fingerprint reader and keybinding cryptosystem template. MATLAB R2015a v8.5.0.19761, SimEvent was used for the system simulation and MySQL Server for the database. This model of self-reporting e-voting solution gave results that are more accurate compared to traditional paper balloting, which is prone to written and reading errors. This system has shown to have maximum accuracy and higher security defense against election malpractice compared to paper balloting and previous e-voting systems.

1. Introduction

Election is the process in which people choose their representatives and express their preferences for how they will be governed by the chosen seeker. Naturally, the entire process of an election is central to the integrity of democracy itself. The election system must be sufficiently robust to resist a variety of fraudulent behaviors and must be sufficiently transparent and comprehensible so that voters and candidates can have the outcomes of an election [1]. Unsurprisingly, history is beset with cases of elections being manipulated in order to influence the outcome to their favorite's party and candidate. Be it electronic or using traditional paper ballots or mechanical devices, the purpose of a “good” voting system must be efficient [1, 2]. The anonymity of a voter's ballot must be preserve, both to guarantee the voter's safety when voting against a malevolent candidate, and to guarantee that voters have no evidence that proves which candidates received their votes [3]. The existence of such evidence would allow the purchasing of votes. The voting system must also be tamper-resistant to prevent a wide range of attacks, including ballot stuffing by voters and incorrect tallying by insiders [4]. On the other hand, some systems use punch cards where voters punch holes in computer readable ballot cards, these systems are not reliable because of problems in reading cards, but this was later changed to optical scan device systems, which allow voters to record choices by filling in areas on the ballots. The scanned ballots, using a computer scanner and then the votes automatically tallies using a computer program [5].

Human aspect is another important factor in a voting system, because the voting system must be understandable and usable by the entire voting population, regardless of age, literacy, infirmity, or disability.

Providing access to such a diverse population is an important engineering problem and one where, if another security is done well, electronic voting could be a great improvement over current paper systems [6]. Flaws in any of these aspects of a voting system, however, can lead to uncertain or incorrect election results, though there have been several studies using computer technologies to improve elections [7]. The need to control access to certain information and resources in electoral practice has seriously been focused on, due to electoral fraud, such as multiple thumb printing, impersonation, carting away of ballot boxes and other threats to current security systems of election.

The use of a fingerprint as an ID in electronic voting system is a brilliant strategy, considering that just about every person on earth is born with unique fingerprint even twins born with very different fingerprints. The fingerprint is naturally unchangeable throughout life. The illustration scheme of the fingerprints either based on global or local information such as ridge ends and minutiae (ridges branches). The matching algorithm combines both extracting of local and global information. This matching algorithm is required in two different stages of the electoral, the first is voter's registration to identify the right to vote and later on at voting time, to allow voters to cast their vote by confirming if the man or woman meets all the requirements required for the voting, which known as authentication [8]. Hence, a multiple fingerprint security is needed to provide the level of protection against electoral fraud and other threats to an election.

Technology has moved forward in several aspects of our lives, in addition to overcoming commonly encountered election pitfalls [9], electoral vote counts is done in a real-time by the end of the exercise and the result is automatically out. The increase in the use of mechanics and electronics has also emerged.

Although, Nigeria is a country with a diverse ethnic group which corrugates different political motive ranging from the individual perspective of the political to geo-political zones. What is wrong with the Nigeria electioneering process is the will to be in power at all cost and not minding the interest of the people [10]. Every political party wants power for their selfish interest, while doing this; they map out strategies that will enable them rig the election by all means. These things are not mostly peculiar to the Nigeria system alone but also common to some other countries.

Electioneering process have been improved since 2015 general election in Nigeria, with the embedded biometric technology, this system was also used for voters authentication of voters during voting. This system has been able to reduce voters duplication during registration by making use of their fingerprints and by so doing, it reduce the level of multiple voting during election [10]. This proposed framework for self-reporting electronic voting system use, Biometric Encryption (BE) for authentication scheme in order to reduce false rejection rate (FRR) and false acceptance rate of the system while the TV White Space Spectrum proposed for the internet networking for its wider range services.

1.1. Electronics Voting System Requirement

There are different forms of electronic voting (e-voting) known so far, some of which includes, internet, remote electronic and kiosk voting [11]. Although, there are some form of electronic voting system which do not require identification electronically. Example, with DRE voting systems or kiosk voting this is the form of e-voting that take place in a polling station or other supervised area by electoral officials, while the voter’s identification process may remain the same as with traditional voting (paper balloting), this system is only used to cast and/or count the ballots. However, e-voting systems may include an electronic identification process which is known as remote internet voting. Nevertheless, with remote Internet voting, voters can authenticate themselves with the biometric even without a token; although, voter self-authentication may be less reliable [12]. A necessary precondition for the electronic identification is an electronic voter registration. In the case of electronic voter identification, additional arrangements need to be in place in order to make sure that the voters' identity may not link to the

content of his/her vote. Specific technical and procedural security measures needed in order to guarantee that these two sets of information could not linked at any time and under any circumstances.

There are many security reasons to encourage electronic voting system model in order to draw up voting systems to digital era [13]. The use of the electronic voting system has the potential to reduce or remove unwanted human errors in addition to its reliability; it can also handle multiple modalities, and provide better scalability for large elections.

By the proposed design requirements, definition for electronic voting systems documented in the design requirements proposed in this self-reporting electronic voting system framework are into two areas, general and system standard. In the general area, the system is to take care of the following:

i. Reliability: No vote should be lost, even when faced with electoral failures
ii. Flexibility: Election equipment should be accessible to all voters.
iii. Accessibility: Voters should be enable as far as possible to participate directly in the election process.
iv. Verifiability: Verify that all the votes have accounted for, in the final tally and those reliable and authentic records exist to that effect.
v. Eligibility: Only authorized and eligible voters should allow for casting ballots.
vi. Accuracy: Voter's intent should recorded and counted correctly, to ensure that the will of the people is standing in.
vii. Uniqueness: Voters should allow casting only one vote.
viii. Integrity: Forged, modified should be rejected and detected.
ix. Convenience: Voters should be able to cast their ballot without undue delay.
x. Cost-effectiveness: Voting systems should be affordable while still being efficient and effective
xi. Transparency: Voters should possess a general understanding of the voting process and should not be deceived into voting a certain way
xii. Fairness: Result not to announce until the end of the exercise.

The system standard framework will allow:

i. Multiple fingerprint, only one will be necessary for voting
ii. Automatic collation of election result
iii. Simultaneously voting for different electoral positions
iv. Concurrent election
v. Easy and friendly user interface
vi. Wider range of internet network connectivity

1.2. Biometric Encryption Operational Models

At enrollment, a filter function, H(u), derived from $f_0(x)$, which is a two dimensional image array "0" indicates the first measurement. Subsequently, a correlation function c(x) between $f_0(x)$ and any other biometric input $f_1(x)$ obtained during verification is defined by:

$$c(x) = FT^{-1}\{F_1(u)F*_0(u)\} \quad (1)$$

This is the inverse Fourier transform of the product of the Fourier transform of a biometric input, denoted by $F_1(u)$, and $F*_0(u)$, where $F*_0(u)$ is represented by H(u). The output c(x) is an array of scalar values describing the degree of similarity. To provide distortion tolerance, the filter function is calculated using a set of T training images $\{f_0^1(x), f_0^2(x) \ldots, f_0^T(x)\}$.

The output pattern of $f_0^T(x)$ is denoted by $c_0^T(x)$ with its Fourier transform $F_0^T(u)H(u)$. The complex conjugate of the phase component of the $H(u)$, $e^{i\phi}(H(u)$, is multiplied with a random phase-only array of the same size to create a secure filter, $H_{stored}(u)$, which is stored as part of the

template, while the magnitude of $H(u)$ is discarded. The output pattern $c_0(x)$ is then linked with an N-bit cryptographic key k_0 using a linking Algorithm I.

Algorithm I: Linking k_0 with $c_0(x)$

If (the n-th bit of $k_0 = 0$) then L locations of the selected part of $c_0(x)$ which are 0 are chosen and the indices of the locations are written in the *nth* column of a look-up table which is stored as part of the template, termed Bios-crypt. Standard hashing algorithms was used to compute a hash of k_0, termed id_0 which is stored as part of the template. During authentication, a set of biometric images is combined with $H_{stored}(u)$ to produce an output pattern $c_1(x)$. With the use of the look-up table, an appropriate retrieval algorithm calculates an N-bit key k_1 extracting the constituent bits of the binarized output pattern. Finally, a hash id_1 is calculated and tested against id_0 to check the validity of k_1.

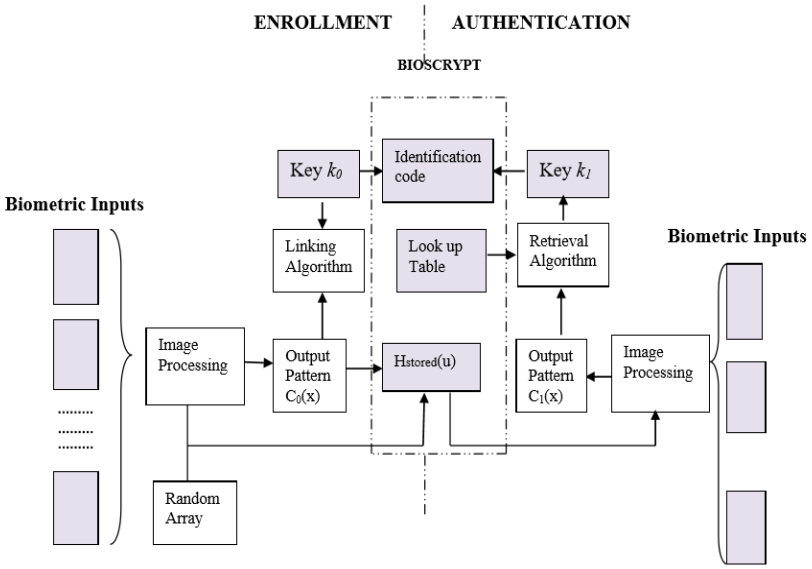


Figure 1: Composite Process Model for Enrollment and Verification in Biometric Encryption System

2. Methodology

2.1. Framework Communication Network Architecture

In the characterization of the framework, the polling booths at the various wards is characterized as the remote sites collation center while INEC offices in LGA is characterized as the corporate office. A tunneling process was used in transporting the encrypted data over the internet using white space technology. Tunneling is a mechanism for encapsulating one protocol in another protocol. In the context of the internet, tunneling allows protocol such as AppleTalk, encrypted IP that is encapsulated in IP envelop then transmitted safely over the internet. On the receiving side, the IP envelope removes the decrypted data delivered to the appropriate device. The white space spectrum architecture consists of the IEEE 802.22 backbone links and IEEE802.11af access links, operating in the UHF frequency band, and geolocation spectrum databases for automatic assignment of available TVWS channels. TVWS Wi-Fi can cover 4 times the radius of a normal Wi-Fi AP at the same power level and can reach several kilometers with higher power. Data is encrypted before it is tunneled and transmitted, while at the receiver's side the scrambled data is decrypted. This data is effectively sent through a tunnel that cannot be entered by data that is not properly encrypted and part of the communications process involves placing a packet within another packet and sending it over a network.

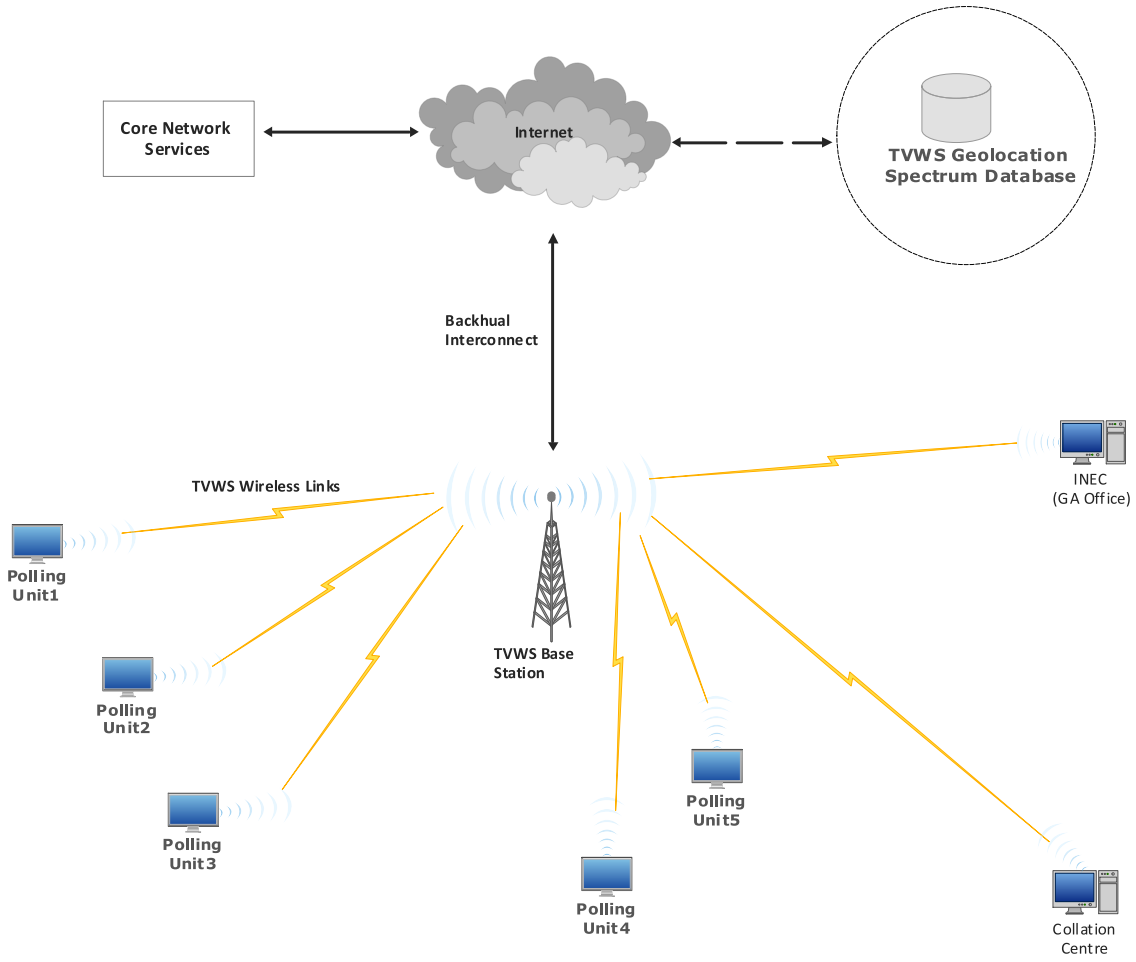


Figure 2: Tvws Network Architecture Evolution

2.2. Framework of E-Solution System Architecture

The necessary requirement for the framework architecture is given as follows:

a) These modules are present in the all-polling booth:

Touch Screen Visual Display Unit: This used for helping the voter input and have a clear-cut picture of his transactions as it takes place. It also gives the voter a notification that his vote has been accepted by the system, i.e if he is a genuine voter. If a non-registered voter or a voter who has earlier cast his vote should try voting, it would display an invalid vote.
The Bios-crypt fingerprint module: The Bios-crypt fingerprint module does both the acquisition of fingerprints and the biometric key binding operation of voters and protects their privacy. This operation releases the N-bit digital key that allows voters to cast their vote.
Secure Crypto-processor: This is located within a secure enclosure, the details of its processing and functions are kept hidden to prevent intruders from manipulating scores.
Virtual Network Interface: This is used for capturing the incoming traffic before encryption. The packets of votes is sent through the VNI and delivered to any programs attached to the VNI.

b) Collation center comprises have the following:

Control keyboard: This is used to co-ordinate the various operations at the collation centers.

The Bios-crypt finger print module: Bios-crypt fingerprint module does both the acquisition of fingerprints and the biometric key binding operation. It releases the N-bit digital key that allows the administrator to have access to the tallied election results and prevents unauthorized persons from having access to election results.
Secure Crypto-processor: This is located within a secure enclosure, the details of its processing and functions kept hidden to prevent intruders from manipulating scores.
Virtual Network Interface: This is used for sending the outgoing traffic after decryption of data. The packets of votes sent via the VNI and delivered to programs is attached to the VNI.
This system is based on cloud, cluster and distributed computing architectures for proper data transmission.

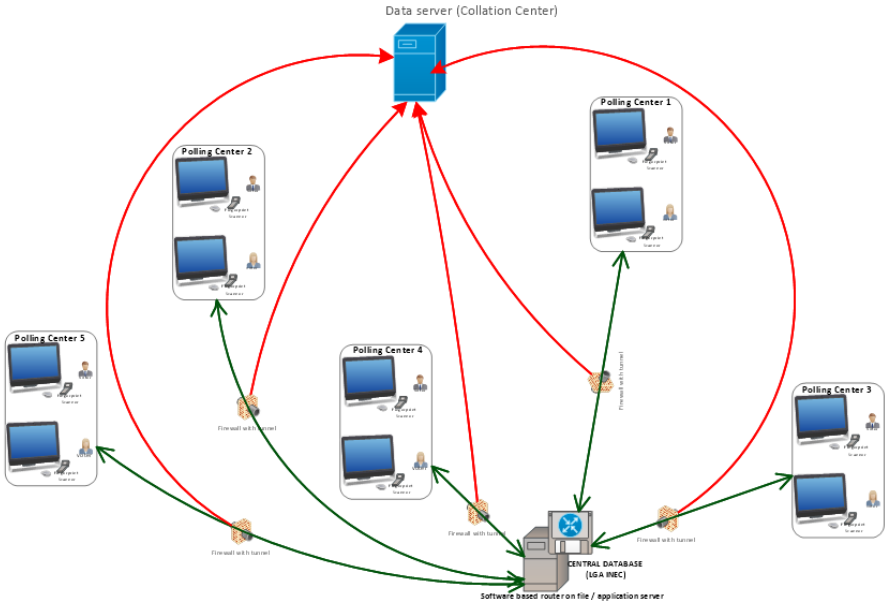


Figure 3: General View of System Framework Architecture

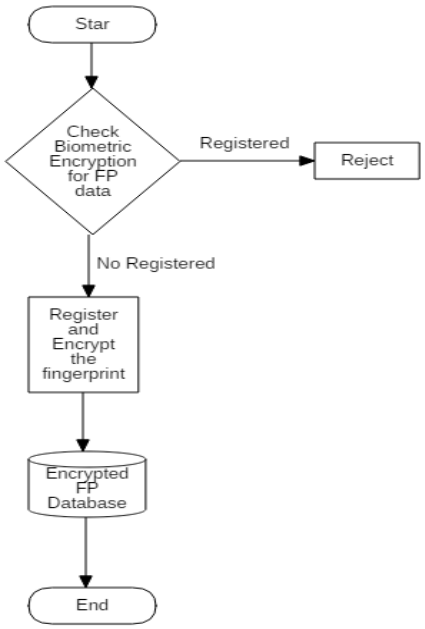


Figure 4: Flowchart For Voter's Registration Process

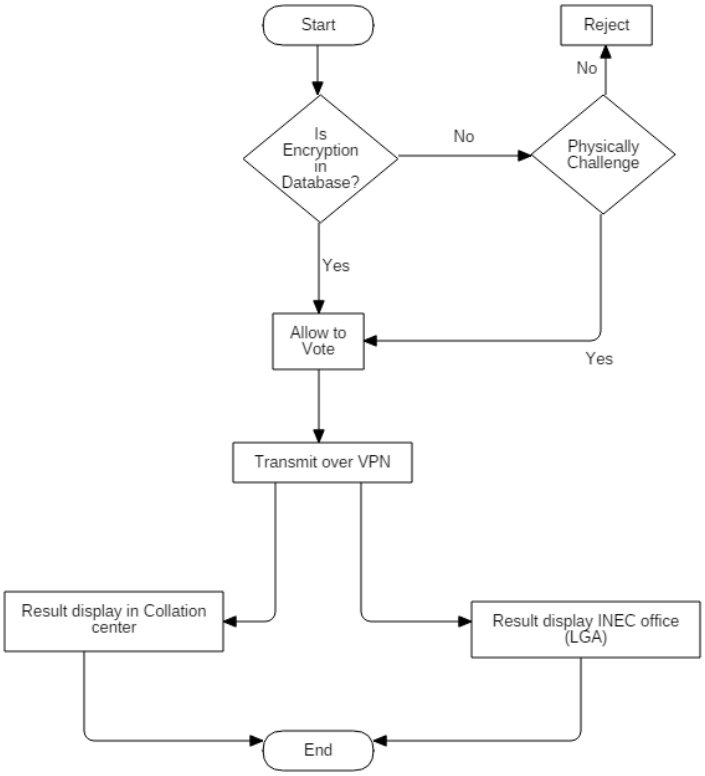


Figure 5: Flowchart For e-Voting Process

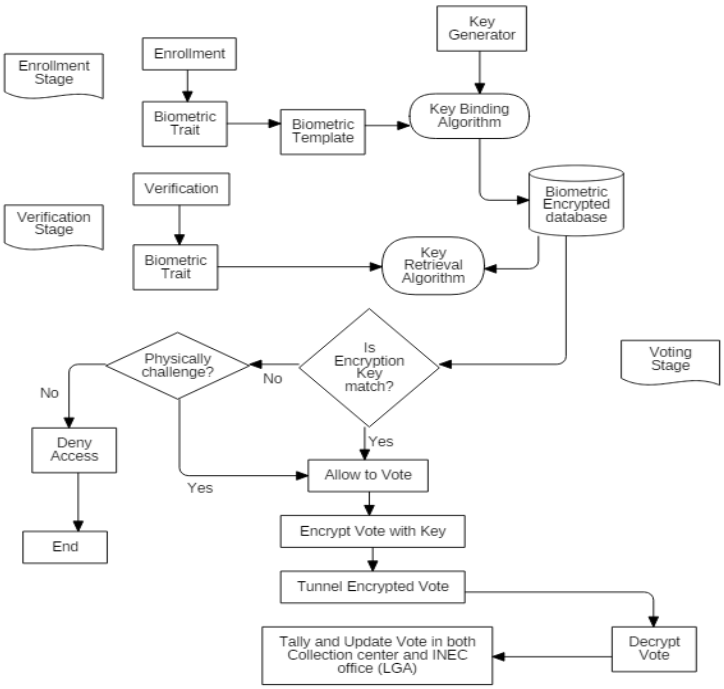


Figure 6: E-Voting System Logical Interfaces for the Biometric

We obtained tolerability data scores from (University of Benin, Benin City) as primary data sources for this research and various flowcharts that capture the framework of a biometric key scheme was also developed using UML as shown in Figure 4 and Figure 6. We used MATLAB version R2015a version 8.5.0.19761 to develop a real life simulation that illustrates the voting situation using Simulink (SimEvent). The implementation was characterized with various components to realize the expected simulation behavior.

2.3. The e-Voting Simulation Model

Figure 7 shows the state diagram of the voting process. Average simulations were over five voting runs. This is particularly important because the model entails several random factors. The simulator, also, includes modules, which emulate the arrival of voters at voting centers and the voting process itself. The simulator allows a voter to cast a vote at any voting center, irrespective of his actual voting location (locality). This is one of the main advantages of an online e-Voting system. We conducted a small number of simulations of the proposed voting system, although we realize that the number of voters in a given locality will surely be very much larger than the numbers we used in the simulator. However, the simulation results are scalable as the simulation model is capable of modelling a large number of voters. We fixed the number of voters at a given voting center in the simulator.

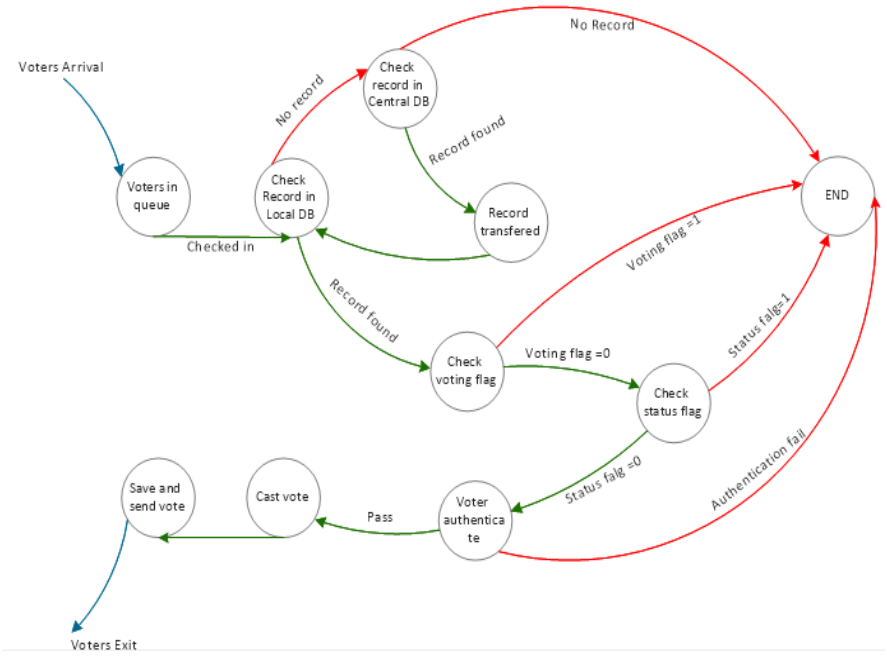


Figure 7: State Flow Diagram of the Proposed Simulation Model

3. Results and Discussion

3.1. SimEvent Modelling

The obtained results are from the simulation model test using MATLAB and Simulink presented in Figure 8. This is the screen shot of the Electronic Voting System self-report architecture captured using MATLBA 2015. The final tallied results were tabulated using mySql database as display in Figure 9.

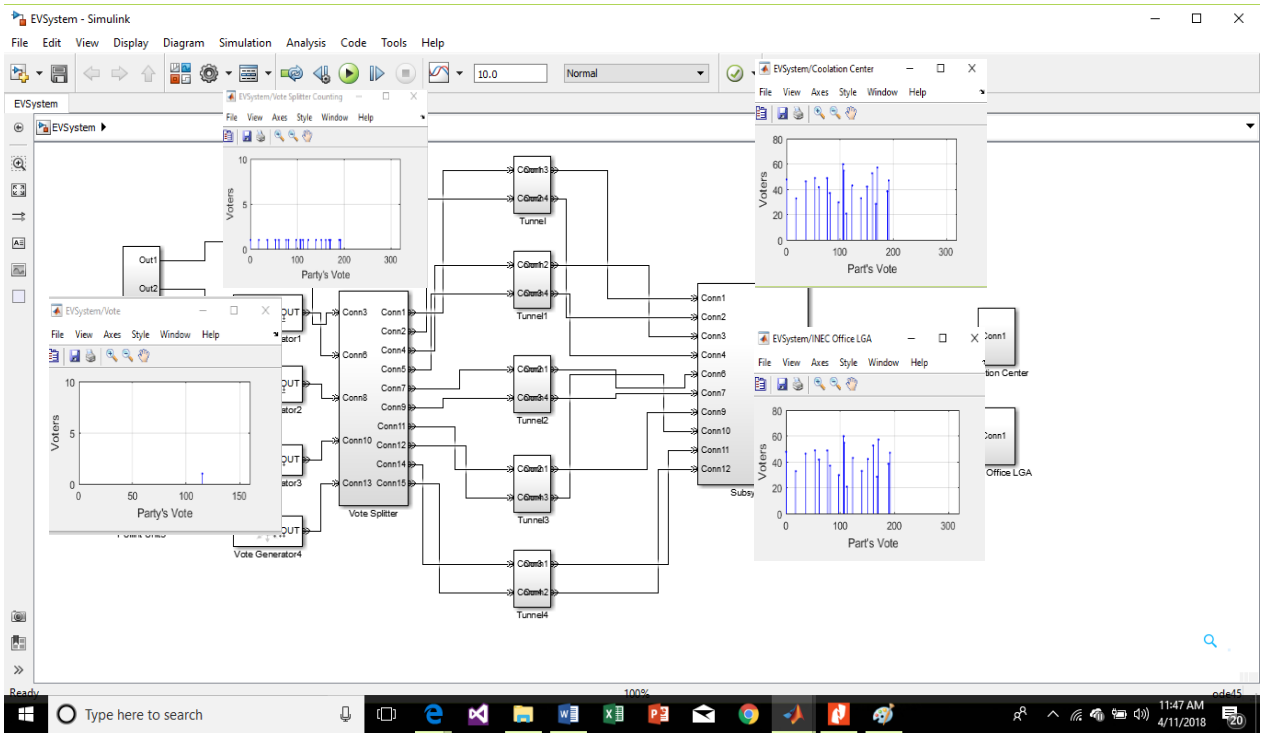
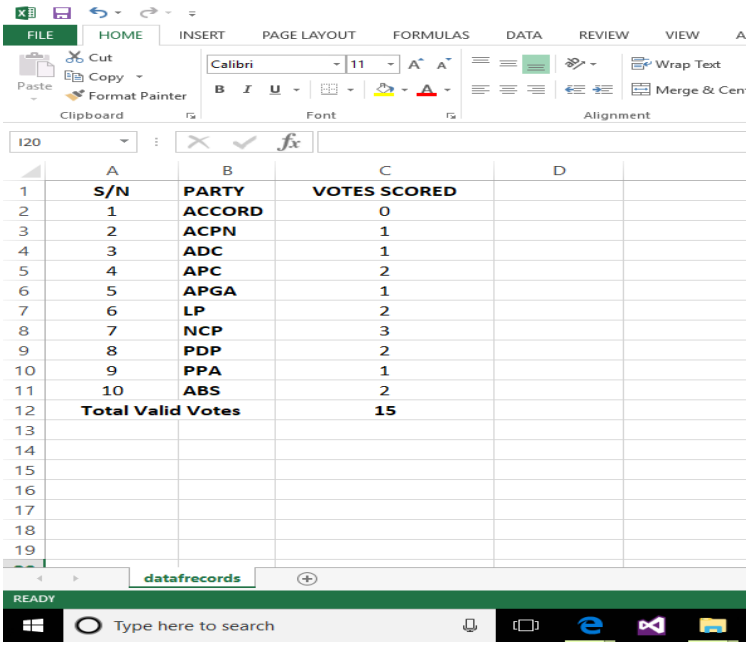


Figure 8: MATLAB SimEvent



	A	B	C	D
1	S/N	PARTY	VOTES SCORED	
2	1	ACCORD	0	
3	2	ACPN	1	
4	3	ADC	1	
5	4	APC	2	
6	5	APGA	1	
7	6	LP	2	
8	7	NCP	3	
9	8	PDP	2	
10	9	PPA	1	
11	10	ABS	2	
12	Total Valid Votes		15	
13				
14				
15				
16				
17				
18				
19				

Figure 9. Electronic Voting System Self-Report Collated Results of Different Parties

One of the main objectives of this paper is to design a system with low error rate. For analyzing proposed system from differentiating with other existing one, the following analysis is carried out.

i. FRR (False Rejection Rate)

False Rejection rate is defined as the ratio of the number of times the genuine user is rejected to the total number of verifications. Given by:

$$\text{FRR} = \frac{\text{No.of times the genuine user rejected}}{\text{Total No.of Verification}} \quad (2)$$

ii. FAR (False Acceptance Rate)

False Acceptance rate is defined as the ratio of the number of times an unauthorized user is accepted to the total number of verifications.
Given by:

$$\text{FAR} = \frac{\text{No.of times an unauthorized user gets accepted}}{\text{Total No.of Verification}} \quad (3)$$

The above parameters in Equations 2 and 3 are tested in the proposed system and it was found that the first parameter i.e. FRR (False Rejection Rate) was very low i.e. Only one time the system has rejected the authorized user because of defect in the fingerprint. The second parameter, i.e. FAR (False Acceptance Rate) was found to be zero i.e. there is no such acceptance of any unauthorized user in the system. The system was tested by enrolling more users.

4.3. Validation of Model

OPNET modeler was used to validate the traffic engineering in the system and evaluate the end to end latency between the polling modules and the collection centers and its throughputs. It is seen from the graphs in Figure 10a, 10b, 10c, 10d that the communication backbone for the framework of this Model of Self-Reporting Electronic Voting System had a low end to end latency, high throughput, high stability margin and efficient resource utilization considering the design layout for deployment of the Electronic Voting System.

Figure 10a shows that the metric of the resources deployed for the network simulation was well utilized. This indicates that no resource is over or under utilized in the simulation
Resource utilization = Busy time / Available time
This value, expressed in percent, shows how much of resources time is spent working.

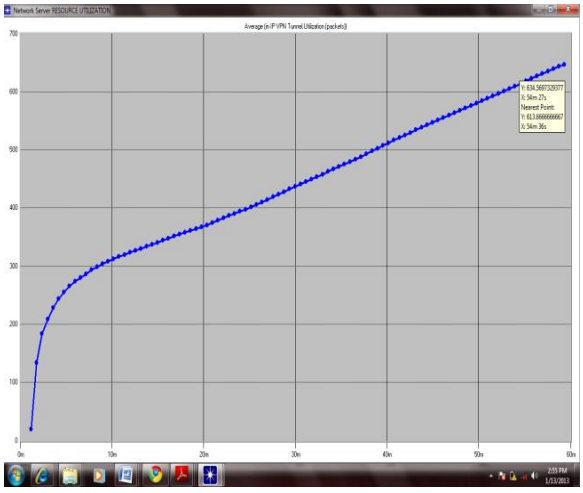


Figure 10 (a): Avg. Resource Utilization

Figure 10b, shows the short length of time it takes a signal to be sent and the length of time it takes for an acknowledgement of that signal to be received with high frequency. In addition, Figure 10c shows how stable the network response to the resource is. Figure 10d, i.e the network throughput shows the average rate of successful message delivery over a communication channel, delivered over or logical link. Throughput is measured in bits per second (bit/s or bps).

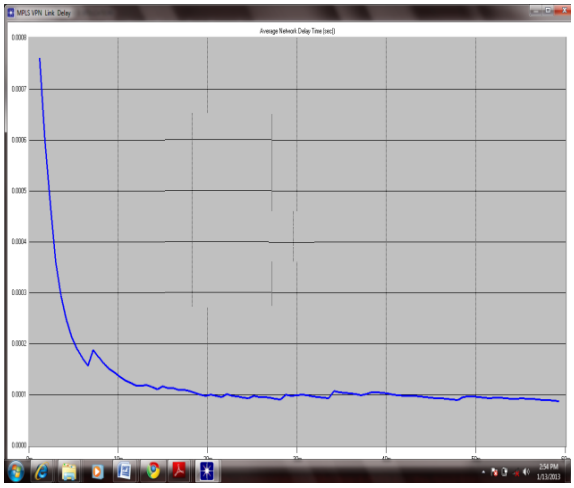


Figure 10 (b): Avg. Network Delay Response

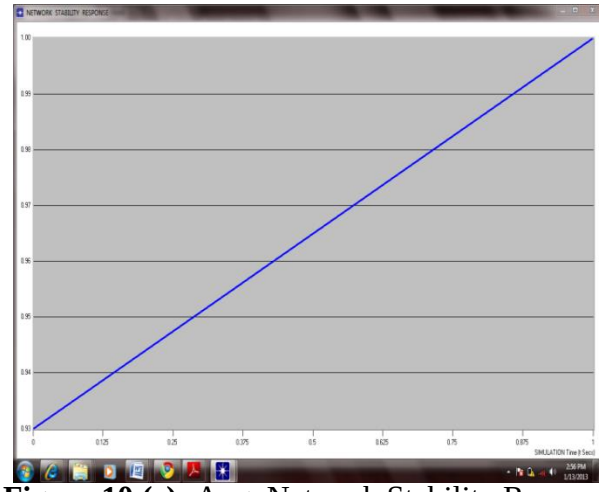


Figure 10 (c): Avg. Network Stability Response

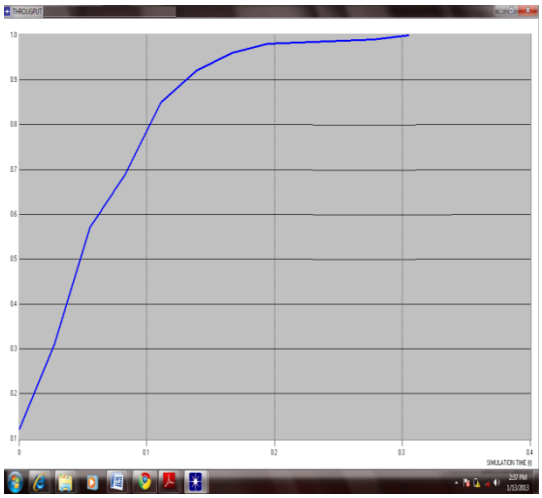


Figure 10 (d): Avg. Network Throughput Response

4. Conclusion

In this research, simulation model of an e-voting system leveraging on biometric encryption was conducted. The self-reporting electronic voting system gave accuracy of data reading and

flexibility in usage. It was able to eliminate errors of read and write of the results and issues of invalides votes which may occure in the traditional voting method. Results also showed that the electronic voting system is faster in ballot collation compared to the manual process of collation. Communication was successfully characterized and validated using metrics like end-to-end latency, throughput, network stability and tunnel resource utilization in OPNET modular.

5. Acknowledgement

I would like to express my deepest gratitude to God for His blessings, strength and grace that has enabled me to complete this investigation. My sincere gratitude goes to my supervisor Engr. Prof. S.T. Apeh, Engr. Prof. Ariavie G.O. and the Head of Department Engr. Dr. Omoifo for their constant guidance, positive criticism and above all their viable suggestions and priceless advice, which tremendously contributed to my success within the shortest time possible.

6. Conflict of Interest

There is no conflict of interest associated with this work.

References

[1] Anil Pandit and R. C. Gangwar, 2015 “Issues and Challenges in Electronic Voting and Direct Recording Electronic Voting Systems” International Journal of Advanced Research in Computer Science and Software Engineering Volume 5, Issue 1.pp22-33

[2] T. Kohno, A. Stubblefield, D. S. Wallach and A. D. Rubin, 2004 “Analysis of an Electronic Voting System” IEEE Symposium on Security and Privacy February.

[3] Ibrahim Inuwa and N.D. Oye, 2015 “The Impact of E-Voting in Developing Countries: Focus on Nigeria” International Journal of Pure and Applied Sciences and Technology 1(1)pp24-34

[4] Maria Rigou, Spiros Sirmakessis and Athanasios Tsakalidis 2003“Is it Secure to Vote Electronically? Security Considerations in the e-Election Process”

[5] Denise Demirel, Richard Frankland, Darko Popovic and Melanie Volkamer, 2011 “Voting software to support election preparation, counting, and tallying” Conference for E-Democracy and Open Government, CeDEM11.

[6] Oladotun Okediran and Ganiyu Rafiu Adesina, 2015 “A Framework for Electronic Voting in Nigeria” International Journal of Computer Applications 24(1)pp14-24

[7] Martin Russell and Ionel Zamfir, 2018 “Digital technology in elections efficiency versus credibility” European Parliamentary Research Service11(1)pp24-34

[8] Haydar Imad Mohammed, 2013 “FingerPrint Base Electronic Voting System” Asia PacificUniversity of Technology & Innovation Faculty of Computing, Engineering & Technology School of Engineering. Thesis

[9] James Iraya Njogu, 2014 “e-Voting System: A Simulation Case Study of Kenya” University of Nairobi, School of Computing and Informatics. Thesis

[10] Uwhejevwe-Togbolo Samuel, “Problems Of Election In Nigeria” Movement for Youth Actualisation International (MYAI) a Non-Governmental Organization (NGO)

[11] V.C. Ossai , K.C. Okafor, H.C. Inyama and A.O. Agbonghae, 2013 “An Improved Model of E-Voting System Based on Biometric Key Binding” International Journal Of Engineering And Computer Science Volume 2 Issue 6 June, 2013 Page No. 1704-1726.

[12] Hari K.P., J.A. Halderman, R. Gonggrijp, Scott Wolchok, E. Wustrow, A. Kankipati, 2010 "Security Analysis of India's Electronic Voting Systems" Proc. 17th ACM Conference on Computer and Communications Security (CCS '10).

[13] Abdul Aziz, 2011"Online Election System a proposed system for Pakistan" Institutional for information technology, Department of Information Technology. Thesis report