

A Framework for Electronic Voting in Nigeria

Oladotun Olusola Okediran
Ladoke Akintola University of Technology,
P. M. B. 4000, Ogbomoso,
Nigeria

Rafiu Adesina Ganiyu,
Ladoke Akintola University of Technology,
P. M. B. 4000, Ogbomoso,
Nigeria

ABSTRACT

It is generally considered that a key component of electronic government in the future will be electronic voting, as a means of facilitating the participation of citizens in elections and public debates. The Nigerian 2015 general elections witnessed the use of electronic voters' register, permanent voters' card (PVC) and smart card readers for authentication of voters but actual ballot casting was still by manual means under a scheme called Re-Modified Open-Secret Ballot System (REMOBS). This paper proposed a framework for an electronic voting system that can be adopted for voting in Nigeria. The framework is capable of handling electronic ballots with multiple scopes at the same time, for example presidential, gubernatorial, legislative and so on. The framework caters for integrity of an election process through essential requirements of privacy, authenticity, accuracy, security, democracy and verifiability. The functional requirement in the design of the proposed framework requires well-secured identification and authentication processes for voters through the use of biometrics. Actual ballot casting is through direct recording electronics (DRE) voting machines connected together and with a central server over a private network.

Keywords

Electronic voting, Paper ballot, Framework, Direct recording electronics

1. INTRODUCTION

Elections and voting are fundamental to any consensus-based society. They are one of the most critical functions of democracy. Elections allow the populace to choose their representatives and express their preferences for how they will be governed while voting is a method by which a group of people express their opinion over who will lead them for a specific period of time through electoral processes. Naturally, the integrity of the election process is fundamental to the integrity of democracy itself. Usually correctness, robustness to fraudulent behaviors, coherence, consistency, security, and transparency of voting are all key requirements for the integrity of an election process [7]. Election system must be sufficiently robust to withstand a variety of fraudulent behaviors and must be sufficiently transparent and comprehensible that voters and candidates can accept the results of an election [6].

There are a number of voting systems adopted all over the world with each of them having its peculiar problems. The manual voting system (paper ballot) still appears prominent among the developing nations. In traditional paper ballots, voters choose or mark their favourite choices on ballots and place them in boxes, which are sealed and officially opened under special conditions to warrant transparency [12]. The ballots are then counted manually, which is a tedious process that is subject to human error. In Nigeria, most elections in

times past were conducted using this method with various balloting methods that includes; open balloting, open-secret balloting, option-A4, modified open-secret balloting and so on. This method of voting has littered history with examples of elections being manipulated in order to influence their outcome. Allegations of violence, intimidation, ballot stuffing, under-age and multiple voting, counting error, complicity of the security agencies and the absence or late arrival of election materials and so on often trail elections conducted using this method [7, 9, 10, 13].

Furthermore, the cost and process of manual voting are both increasing geometrically and tedious to execute [3] and there has been a declining participation rate due to: inconvenience of manual system of voting like: inaccuracy in ballot counting and delayed announcement of election results [5]; loss of significant time during ballot counting [1]; unacceptable percentages of lost, stolen and miscounted ballot papers, votes loss through unclear or invalid ballot marks and limited accommodations for people with disabilities [2, 8].

For the first time in the history of electioneering process in Nigeria, the 2015 general elections saw the emergence of the use of a combined technology of electronic voters' register, permanent voters' card and smart card readers for authentication of voters. These technologies to a large extent eliminated duplication of voters' registration and hence multiple voting. However, ballot casting was still by manual means. Some of the aforementioned inherent problems associated with paper ballot were still significant during the said electioneering process.

This paper proposed a framework for an electronic voting system that utilizes the authentication scheme of the REMOBS. The requirements definition for the system is described in Section 2. The architecture framework of the e-voting system that satisfies the stated requirements in Section 2 is presented and described explicitly in Section 3 while, Section 4 presents some concluding remarks.

2. REQUIREMENTS DEFINITION FOR THE E-VOTING SYSTEM

The design of any voting system, whether electronic or manual, must satisfy a number of sometimes competing criteria including a high degree of security and accuracy, eligibility and authentication, integrity, verifiability and auditability, reliability, flexibility, performance and scalability

[13]. The anonymity of a voter's ballot must be preserved, 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. The existence of such evidence would allow votes to be purchased by a candidate. The voting system must also be tamper-resistant to thwart a wide range of attacks, including ballot stuffing by voters and incorrect tallying by insiders. Another factor, of immense importance is the "human

factors". A voting system must be comprehensible to and usable by the entire voting population, regardless of age, infirmity, or disability. Providing accessibility to such a diverse population is an important engineering problem and one where, if other security is done well, electronic voting could be a great improvement over current paper systems. Flaws in any of these aspects of a voting system, however, can lead to indecisive or incorrect election results.

Guided by the design requirements' definition for electronic voting systems documented in [13], the design requirements of the electronic voting system's framework proposed in this work are divided into two groups, namely, generic and system-specific. The system is to cater for the following generic requirements:

- a) *Privacy*: After casting a vote, no one should be able to link the voter to this vote and no voter can prove that he or she voted in a particular way;
- b) *Authenticity*: Only eligible voters can cast their votes;
- c) *Accuracy*: Once a voter cast a vote, no alternation to this vote is permitted. Moreover, All valid votes must be counted, whereas all invalid votes must not be discarded;
- d) *Security*: Throughout the voting process, a vote can't be tampered with;
- e) *Democracy*: All eligible voters must be able to vote, one person - one vote and no one can vote more than once or vote for others.
- f) *Verifiability*: Voters can independently verify that their votes have been counted correctly and are included in the final tally.

The system-specific requirements of the framework allow:

- a) *Multi-user*: A number of voters can vote simultaneously;
- b) *Multi-campaign*: A number of elections can be running simultaneously;
- c) *Availability*: The system must have high-availability during an election campaign.

3. ARCHITECTURAL FRAMEWORK FOR THE E-VOTING SYSTEM

The architectural framework for the electronic voting system is presented in Figure 1. The framework is a client/server

web-enabled architecture. The framework follows the conceptual perspective of e-voting as defined by the Organisation for the Advancement of Structured Information

Standard (OASIS). The OASIS consortium is a standard for the structured interchange among hardware, software, and service providers who engage in providing election or voter services to public or private organizations. OASIS in 2003 conceptualized e-voting to be made of three phases [11]:

- *Pre-voting phase* which involves election declaration, candidate nomination, referendum options and voters' registration.
- *Voting phase* which involves ballot information, voter authentication, vote casting and confirmation.
- *Post-voting phase* which involves election counts, results and audit.

Considering e-voting systems this way follows the high level models of election systems given by the OASIS. The OASIS consortium specifies Election Markup Language (EML) especially for the exchange of data within e-voting processes. Therefore, OASIS drafts a high level overview and a high level model dealing with the human view and a high level model dealing with the technical view. In this paper, mainly the human view is taken as a basis for talking about e-voting systems from the conceptional point of view. These models should be the initial point of creating e-voting concepts. EML is in particular useful for interoperability reasons. Separating the process into these phases gives a good abstraction of an election process. Moreover, these models provide a common terminology and a conceptional perspective

3.1 Pre-voting Phase of the Architecture

In the pre-voting phase, the clients are direct data capture machines equipped with biometric fingerprint readers and web cams as it is in the Nigerian voting system. Voter's data captured during registration includes biographical data, voter's passport size photograph, thumbprints (both left and right thumbprints) and delimitation details (state of origin, local government area, registration area and polling unit/registration centre). In order to reduce the traffic rate on the network links, a local database at the client side is required to host the data which pertains to the local registration/voting centre. The size of the local database at any registration/voting center is only a small fraction of the central database at the server side. The use of a local database enhances the performance of the registration process. The two major outputs of pre-voting phase of the Nigerian voting system are:

Electronic voters' register which contains the details of all eligible voters including a biometric feature (fingerprints) of voters which eliminates duplication of registration of voters thereby minimizes discrepancies in the electoral process.

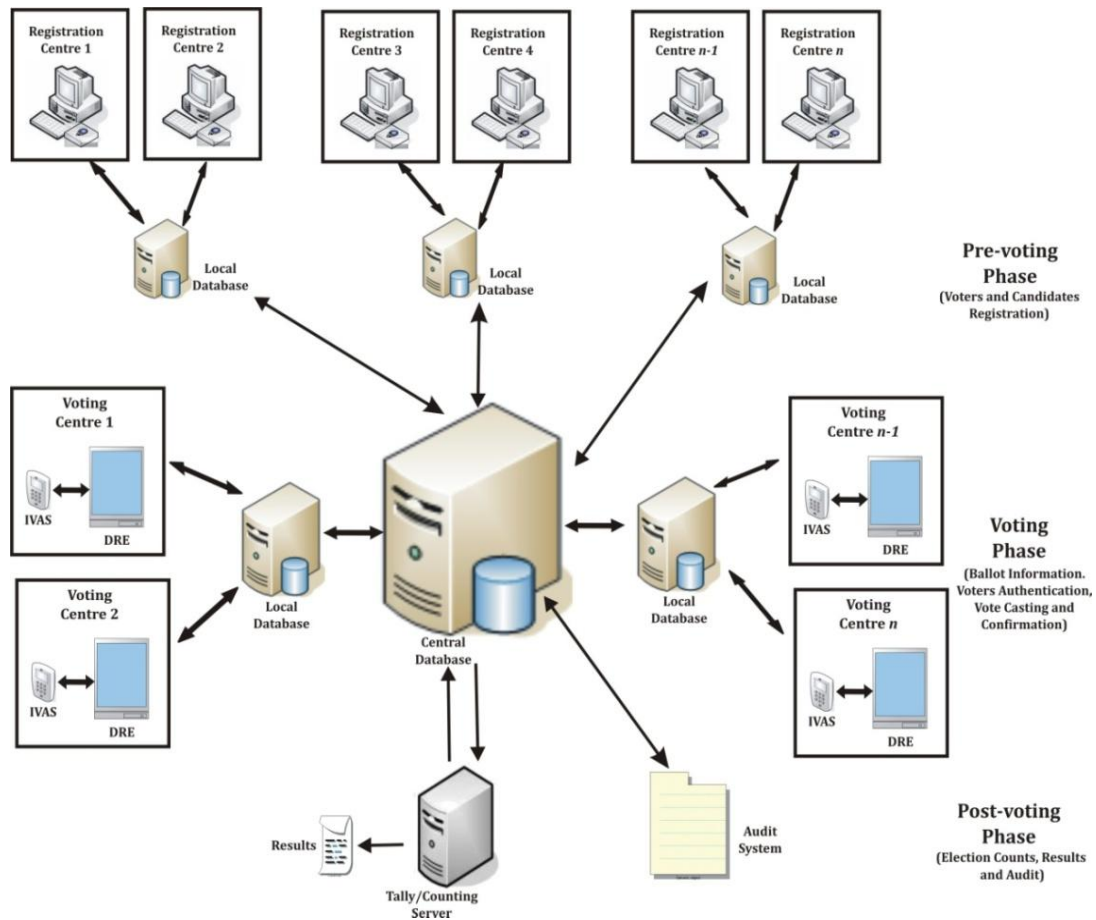


Fig 1: Architectural Framework of the Proposed E-voting System

- Permanent voters' card (PVC) is considered as a receipt for all successful voter's registration process and contains voters information such voter's name, voter's photograph, name of the state the voter is registered in, the name of the local government area, the registration area/centre and code and the voter's identification number.

Communication between clients and the central server is by a private network over public infrastructure (virtual private network) while a RSA encryption algorithm is proposed to secure end to end messaging between clients and the server.

3.2 Voting Phase of the Architecture

The client side of the voting phase of the architecture represents voting centres, where voters cast their votes. A local database at the client side is also required to host the data which pertains to the local voting centre. Similar to its function in the pre-voting phase, the local database is also necessary in the voting phase in order to reduce the traffic rate on the network. The local database should be a dynamic one, in the sense that the data stored in its tables may vary over the election time period. The hardware on the client side includes:

- Smart card readers for voters' verification and authentication. The smart card reader which is referred to as IVAS (INEC Voters Authentication System) in the Nigerian voting system (REMOBS) is a device which is specially designed for the electronic authentication of voters on polling day. It adopts a dual core cortex – A7 CPU with ARM ultra-low power consumption. It has a single core frequency of 1.2GHz and an Android 4.2.2 operating system. It supports both touch and keyboard input. It is configured to read contactless card and output same on the LCD screen. It protects data by supporting the SAM (Secure Access Module) card [4].
- Direct Recording Electronics (DRE) voting machine for balloting. Upon authentication, voters mark their choice electronically (perhaps on touch sensitive screen or pushing buttons) rather than on paper ballot. The votes are counted on individual machines and the votes casted are transferred to the central tallying point by unspecified means.

The sequence diagram of the proposed e-voting system is depicted in Figure 2. During authentication of voters, the IVAS which will be operated by a designated polling official

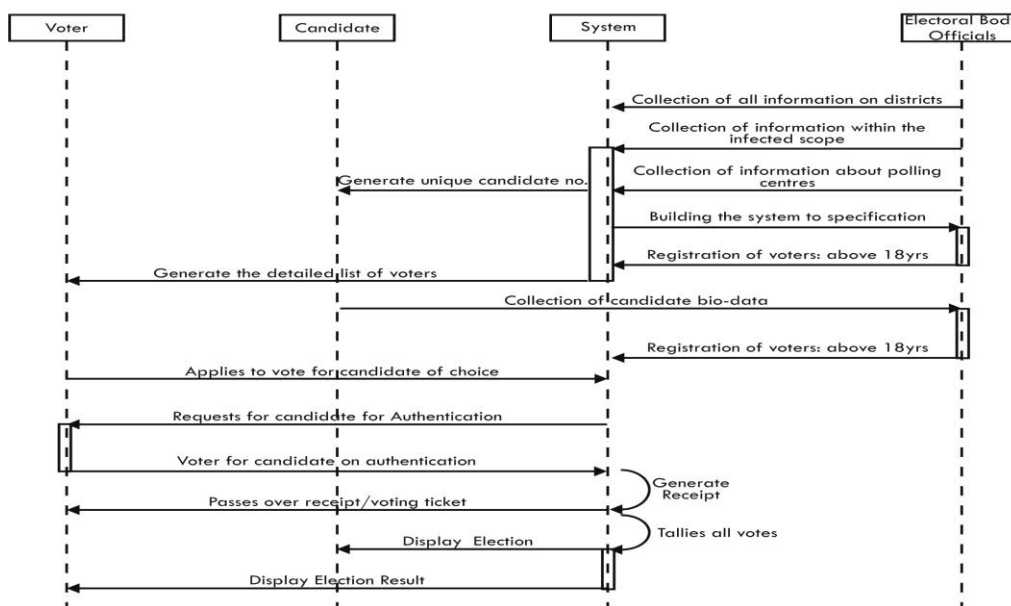


Fig. 2: Sequence Diagram of the Proposed E-voting System

scans the PVC and the voter's fingerprint for a match; if there is a match, this indicates that the bearer of the PVC owns the card and otherwise if there is no match. The IVAS thereafter stores the VIN on the scanned PVC and the authentication status of the voter. The IVAS should be interfaced with DRE. Upon authentication of an eligible voter, at the IVAS terminal of the electronic voting system, the voter proceeds to the voting point whereby the DRE presents a ballot to the voter on the DRE voting terminal screen. At this point, the voter interacts with the voting terminal, touching the appropriate boxes on the screen for his or her desired candidate(s). Upon submission of the ballot, the vote is recorded on the voting terminal and the terminal is ready for another voter to use. Communication between clients and the central server is by a private network over public infrastructure (virtual private network) while a RSA encryption algorithm is proposed to secure end to end messaging between clients and the server.

3.3 Post-voting Phase of the Architecture

Activities of voting saving, maintaining and counting for a final tally is accommodated by this component of the framework. Close to the counting mechanisms, an analysis system is needed. Such a system provides the auditing team and the election officials with various reports. One of the most important reports is of course the final result of the counting. The form and the precise schema of such reports is although out of scope of the model provided by EML. The audit system checks that eligible voters were capable to vote and their votes participate in the computation of final tally. Additionally, there are some other e-voting specific rules verified in this phase.

Beside the phases and roles given above, there are some other important actors and elements in the model. Very important are the audit mechanisms needed along all phases of an election. On the one hand, it is important to have possibilities to prove the correctness of the process as such. On the other hand, it is crucial not to violate the main principles and security requirements, keeping a vote an inviolable secret in particular. However, audit is necessary to prove the authenticity of the result of the election. Thus, a special set of persons, for example election officials and candidate's representatives, should be allowed to gain access to auditing information. System administration is critical as well, since

administrators are allowed to access the system. Nevertheless, administration is necessary and therefore the security concept of the e-voting system has to protect critical data and components, the secrecy of the ballots especially. This affects the organizational aspects of the security concept either. Not only technical security mechanisms can guarantee this. The administrative staff has to be elected in respect to reliability as well.

4. CONCLUSION

Elections and referenda are the essential vehicles for citizens to participate in democratic processes. With the raise of e-governmental applications, e-voting initiatives are gaining more and more interest. It is emerging as significant alternative to these conventional systems in the delivery of reliable and trusted elections. Thus, many countries are piloting with various e-voting models and systems in order to enable voting using diverse electronic channels. The emergence of e-voting will undoubtedly enabled voters to cast their vote from a place other than the poll site in their voting district, facilitate the casting of the vote by the voter, facilitate more participation in elections by those who are entitled to vote, widen access to the voting process for voters with disabilities or those having other difficulties in being physically present at a poll site, increased voters turnout by providing additional voting channels, reduced overall cost to the electoral authorities of conducting an election, deliver voting results reliably and more quickly amongst many other benefits. In this paper, a detailed requirements definition and framework of an e-voting system was proposed and developed where ballot casting is by electronic means that can be adopted for voting in Nigeria.

5. REFERENCES

- [1] Akinyede R.O. (2010), "Nigerian Voting System: Present and Future States", Proceedings of 23rd National Conference of Nigeria Computer Society July 26th -30th, Volume 21, pp. 77-81.
- [2] Ayannuga O. O. and Folorunso O. (2010), " Electronic Voter's Authentication Management System (eVams)", Proceedings of 23rd National Conference of Nigeria Computer Society July 26th -30th 2010, Vol. 21, pp. 105-110.

- [3] Ibrahim S., Kamat, M., Salleh M., and Abdul-Aziz, S. (2003), "Secure Voting Using Blind Signature" accessed at http://eprints.utm.my/3262/1/IEEE02VS_full_paper_ver14Nov.pdf
- [4] INEC, (2015), "Manuals for Election Officials-Updated Version" accessed at www.inecnigeria.org/uploads/2015/02
- [5] Kalaichevi V. and Chandrasekaran R. M. (2011), "Secured Single Transaction of E-Voting Protocol: Design and Implementation", *European Journal of Scientific Research*, Vol. 51 No.2, pp. 276-284.
- [6] Kohno T., Stubblefield A., Rubin A. Wallach D. S., (2003): "Analysis of an Electronic Voting System" Johns Hopkins University Information Security Institute Technical Report TR-2003-19.
- [7] Malkawi M., Khasawneh M., Al-Jarrah O., (2009): "Modeling and Simulation of a Robust E-voting System", *Communications of the IBIMA*, Volume 8, 2009. ISSN: 1943-7765.
- [8] Manish K, Suresh K. T, Hanumanthappa M. and Evangelin G. D. (2005), "Secure Mobile Based Voting System", accessed at http://www.iceg.net/2008/books/2/35_324_350.pdf.
- [9] Muir H. Laville S. and Gillan A., (2005): "New Fears over Postal Vote Fraud", accessed at <http://politics.guardian.co.uk/election/story/0,15803,1458341,00.html>.
- [10] NSF, (2001), "Report on the National Workshop on Internet Voting: Issues and Research Agenda, National Science Foundation, accessed at <http://news.findlaw.com/cnn/docs/voting/nsfe-voterprt.pdf>.
- [11] OASIS, (2003), "Election Markup Language (EML) 4.0a, Organization for the Advancement of Structured Information Standards.
- [12] Okediran O. O., Omidiora E. O., Olabiyisi S. O., Ganiyu R. A. and Sijuade A. A., (2011a): "Towards Remote Electronic Voting Systems", *Journal of Computer Engineering and Intelligent Systems*, International Institute of Science, Technology and Education, New York, USA, vol. 2, no. 4, pp. 72-81.
- [13] Okediran O. O., Omidiora E. O., Olabiyisi S. O., Ganiyu R. A. and Alo O. O., (2011b): "A Framework for a Multifaceted Electronic Voting System", *International Journal of Applied Science and Technology*, Philadelphia, USA, vol. 1, no. 4, pp. 135-142.