Development of a Semi-Automated Electoral System

Case Study: Nigeria Electoral System

Ayeni Joshua[1] and Odion Andrew[2]
Department of Mathematics and Computer Science,
Benson Idahosa University, Benin City, Edo State, Nigeria
[1]ayoayeni@yahoo.com [2] odionand@yahoo.com

Abstract - **In developing democracies of the world, the electoral process is often enmeshed in distrust, fraud, unprecedented level of rigging and in most cases ends up in courts of law where millions of hard earned funds (public and private) are wasted. Nigeria, despite her democratic experience, has remained 'exemplary' in such profligacy. The reason has always been the absence of a reliable electoral process capable of ensuring a fraud-free general election with the use of the available technology. In this paper, a Semi-Automated Electoral System (SAES) that uses biometric technology is proposed to enhance the electoral system and minimize fraud often associated with the process. The system is based on research into the past electoral processes in the years 2003, 2007 and 2011 in Nigeria and the attempted but unsuccessful introduction of said technology. Biometric technology is the most patronized identity enhancement technique used today in the ICT industry and has been successfully implemented where the identity of a user, customer, citizen, traveler, student etc. is of prime importance. For the development of the proposed system, the fingerprint biometric technology was used because of its reliability, correctness and accessibility. In the proposed system, the electoral process is categorized into three sub-processes viz; the constitution, validation of the voter register and the elections proper.**

Keywords – validation; accreditation; voter register; polling station; wards; constituency

I. INTRODUCTION

In all world democracies, there exists an electoral process designed based on the ideals, demands, requirements and the type of democracy in practice. The Nigerian electoral process is categorized into three sub-processes in the following order; the constitution of the voter register, validation of the register and the elections. A fully automated electoral system would have been the ideal choice in Nigeria but for the level of computer literacy among the old and the young, and the inadequacy or absence of infrastructure (good roads, electricity and Internet access); a *semi-automated system* is therefore proposed. This involves using biometric technology for the process of voter registration (voters' national database) – fingerprints – and voter authentication (voter accreditation) before voting. Nigeria has a population of about 120 million inhabitants, located in West Africa, comprising of 36 states and the federal capital City – Abuja, 774 local government areas and six geopolitical zones [1]. For the purpose of national elections, the Independent National Electoral Commission (INEC) is the statutorily constituted body that organizes and conducts national elections in Nigeria [2]. They are Presidential, National Assembly, Governorship and Houses of Assembly elections. The states are delineated into 8,810 wards and 120,000 polling stations [3].

For the April 2011 general elections, INEC procured 120,000 Direct Data Capture (DDC) machines (including notebook computers, high resolution cameras, printers and fingerprint scanners). It is alarming that despite the huge investments regularly committed to the electoral process the results have always been that of fraud, violence, ballot snatching, multiple voting, ballot box stuffing and brazen falsification of results. The Semi-Automated Electoral System was proposed to address the various issues associated with the electoral process.

II. SYSTEM ANALYSIS

A. Analysis of the Present Electoral System

For the purposes of the 2003, 2007 and 2011 general elections, Electronic Voter Register (EVR) was constituted by INEC. The EVR contained the bio-data of the voters such as voter personal identification number (PIN), name, home address, date of birth, age, profession, photograph, and fingerprint data. The voter registration exercise took place throughout the country and at each polling station with the DDC machine and voter cards issued after successful registration of voters. Upon completion of the exercise, a printed copy of the EVR was pasted at the venue of registration (registration centre) for voters to validate and make corrections. On the day of election, the voter gets accredited after the verification of the voter card on the voter register (in hard copy), and waits until the end of the accreditation period (12 noon). Thereafter the accredited voters queue and are given ballot papers consecutively to cast their votes in secret. At the close of the voting period (5 PM), the ballot papers are counted and the winners announced.

B. Analysis of Related Work

Okonigene and Ojieabu [4] developed an automated electoral system algorithm using biometric data to eliminate electoral irregularities in Nigeria. The system was designed to use a central database server at the INEC's national headquarters in Abuja and stand-alone servers in each state headquarters and geopolitical zones. The client computer system has no database installed but the Web-based application was linked to the central database server for information query and request during voting. The system was based on the

false assumption of a high level of infrastructure, literacy and computer awareness of the electorates.

The client system depends on the central server for the voting process and N-to-N[4] matching of ten fingerprint, iris and facial characteristics; duplicate entries in the central database of about 80 million eligible voters online with the above templates might be technically and logically unjustifiable. In addition, the security of the e-votes could be compromised due to hacker attacks. The N-to-N matching technique involved the comparison of the templates with the scanned fingerprints, iris and facial characteristics for authentication purposes. Another aspect of the biometric infrastructure is its high demand on security. It has to maintain the two requirements of a secure e-voting system: personalization and privacy. Each and every vote has to be linked to a person while preserving the person's anonymity and concealing their vote. [5]. Again, the online e-voting technique would fail as its requirement of internet connectivity with high bandwidth and with no provision for other options would be catastrophic to a time-dependent electoral system.

Ofori-Dwumfuo and Paatey [6] developed an online voting system (OVIS) as a result of the findings of a study of the electoral process of the Electoral Commission of Ghana. It is meant to phase out the outdated paper ballot, punch cards and other mechanical voting systems with a paperless electronic or online voting system. OVIS's infrastructural requirements made it most inappropriate for the Electoral Commission of Ghana. The low level of internet accessibility and Ghana's literacy level are similar to Nigeria. Some of the existing related work include Joaquim[7], Amankona et al.[8] and Sergei et al.[9].

C. *Analysis of the Proposed System*

The SAES was designed to respond to the shortcomings of the present system and block the loopholes in the electoral process that often go exploited. The registration of voters is the same as currently in use with the present system and it is in conformity with the present e-voter register. However, the voter PIN now carries some identification features. There are three tables for the SAES; the *Voter*, *Voter History* and *Election Tables*. The tools for the development of the **SAES** application are MySQL for the database end and the Visual Studio (C#) for the front end.

D. *The Voter Table*

The various data components of the voter table are as follows:

- The PIN of the voter (State code / LGA code / WARD code / Polling-Registration centre code / voter serial no) e.g. INEC/052/23/10/05/255 (Max. 25 Chars)
- Surname of voter (Max. 40 Chars)
- Other Names (50 Chars)
- State of Origin (15 Chars)
- Local Government Area (30 Chars)
- Date of birth (12 Chars)
- Age (SMALLINT(2))
- Sex (7 Chars)
- Marital Status (10 Chars)
- LThumb (MEDIUMBLOB)*
- RThumb (MEDIUMBLOB)
- LSThumb (MEDIUMBLOB)
- RSThumb (MEDIUMBLOB)
- VoterPhoto (MEDIUMBLOB)

** MEDIUMBLOB is a data type in MySQL for storing binary objects/images.*

E. *The Voter History Table*

The voter history table consists of the following:

- PIN of voter (as in voter table)
- Election year (5 Chars)
- Election date (11 Chars)
- Type of Election (25 Chars – Presidential, Senate, House of Representatives, Governorship, House of Assembly)
- Sub Type of election (1 Char – 1 – General Election, 2 – Bye-Election 3 – Others)
- Status (1 Char)

F. *The Election Table (Client)*

- Election year (5 Chars)
- Election date (11 Chars)
- Type of Election (25 Chars – Presidential, Senate, House of Representatives, governorship, House of Assembly)
- Sub Type of election (1 Char – 1 – General Election, 2 – Bye-Election 3 - Others)
- Total number of accredited voters (Integer)
- Total number of ballots cast (Integer)

G. *The Voter Registration Process*

The voter registration process is identical to the current system; the voter goes to the nearest registration centre (polling station), waits for their turn and gets registered by supplying all the mandatory information pertaining to identity (indicated in the voter table above). However, unlike the present process of voter validation (centralized), the process is done using a 'bottom-top' technique.

This involves the validation (eliminating multiple registrations) at the point of registration, ward level (all registration centers), local government level (all wards at the LGA), state level (all LGAs), national headquarters (all states and the FCT); see Figure 1. Multiple voter registration and other forms of fraudulent practices would be expunged from the voter database (EVR) of the central server.

H. *The Election Process*

The DDC machines (client systems) used for the voter registration will be provided for the elections

Figure 1: The voter registration process

proper. However, in the event of the DDC machine being damaged, lost or faulty, a new machine will be provided and configured for the affected polling station. All that is required is uploading the corresponding EVR from the central server and installing the client software (SAES), taking into account the identity of the affected polling/registration centre.

Election starts from 8 A.M. and the voter is digitally accredited by placing the fingertip on the fingerprint scanner, validated and the corresponding ballot paper is stamp-printed with the information (i.e., voter and polling station identification, date, time and the voter's serial number) and thereafter the voter is handed the ballot paper to cast his/her vote; see Figure 2.

III. HARDWARE & SOFTWARE REQUIREMENTS

The hardware (HW) requirement for the SAES is categorized into three; the *client, intermediate server* and *central server* at the polling/registration centers, state and national headquarters of INEC. The software (SW) requirements are as in (iv) and (v).

(i) **HW:** Client System - Integrated notebook system, 4GB DRAM, 2*200 GB HDD, high resolution webcam, high resolution fingerprint scanner, solar powered backup battery, integrated dot-matrix stamp printer, integrated backup flash disk, detachable DeskJet color printer.
(ii) **HW:** Intermediate Server – Dedicated blade server with dual processors, 10 – 20 terabyte SATA HDDs, 5-10 GB of memory, heavy duty dot-matrix printer and laser color printer. VSAT internet connectivity equipment is also required.
(iii) **HW:** Central Server – Dedicated server with dual processors, 100 terabytes SATA HDDs, 10 GB of memory, two heavy duty dot-matrix printers and two heavy duty laser color printers. VSAT internet connectivity equipment and a backup server of similar capacity are also required.
(iv) **SW:** Client System - Microsoft Windows operating system XP/VISTA/7 with MySQL 5.X for the database management.
(v) **SW:** Servers – All the servers will run Linux operating system with MySql server installed.

IV. THE SAES METHODOLOGY

A biometric system can provide two functions. One of which is verification and the other one is authentication [10]. The verification method is referred to as "One to One" (1:1). This method consist of stating a first identification token (User ID, smart card etc.) and verifying if the person is who he claims to be. The authentication method is known as "One to Many" (1:N). This technique consists in comparing the biometric template against a set of stored templates and finds the identical match [11].

The client systems have the choice of being implemented using either of the two methods; using the voter identification number (identification token) or the fingerprint template. Using the former implies a higher level of error (typing the voter identification number) and a longer time compared with the latter, notwithstanding being faster in accessing the record entry directly (identification).

The server end employs the 1:N identification technique because of the size of the database and the need to purge the system of potential multiple entries during the pre-election process.

V. THE SAES DEVELOPMENT

The SAES software is divided into two distinct modules – the registration (create, update, data validation) and the election (manage elections and collates).

a. The registration module (client) – this captures voter data (see II.D above). The photograph is captured, the size verified (max. 10 KB) and then stored in the database (client) in JPEG format. The fingerprint images are captured, converted to their corresponding templates and then stored in the database (client).

b. The verification module (client) – the fingerprint(s) of the voter is captured and used to extract the voter information from the database.

VI. THE ADVANTAGES OF SAES

(a) Elimination of over-voting by ensuring that unregistered voters are not allowed to vote.
(b) Prevention of double registration of voters.
(c) Assurance of easy detection of ballot box stuffing (a significant feature of previous elections)
(d) Elimination of a set period of accreditation – there is a single process (immediate accreditation and voting)
(e) Reduction in the number of polling units (possible).
(f) Elimination of non-dependent on ballot paper numbers
(g) Removal of data irrelevant to the polling station

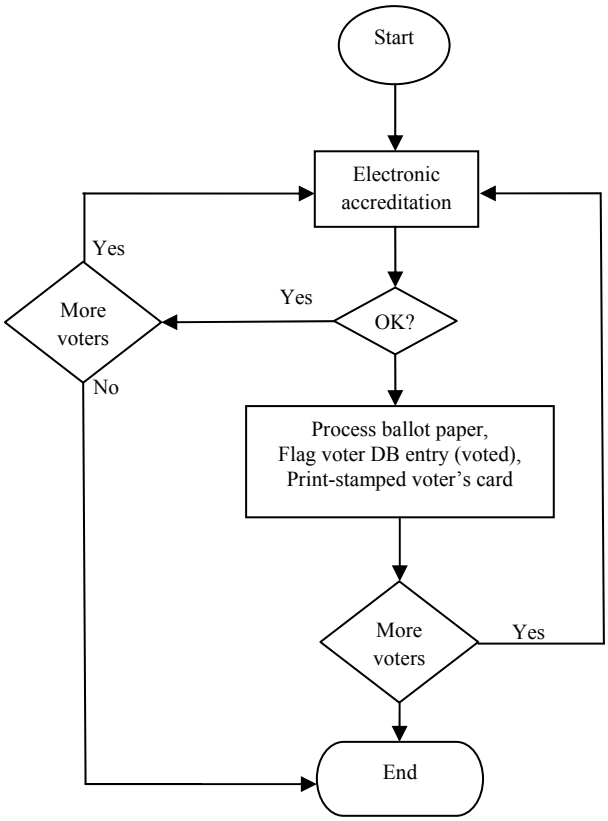

Figure 2: Schematic representation of the voting process

VII. CONCLUSION

A Semi Automated Electoral System was developed to eliminate the various electoral frauds often associated with the process in Nigeria. The system took into account the level of infrastructure, literacy and size of the population of registered voters (77 Million – 2011 general election) and the various problems that confronted the Independent National Electoral Commission during the past elections. The total number of accredited voters was electronically computed while votes for each of the contestants were manually counted and an election record sheet generated electronically and manually. When implemented, the SAES would reduce the problems of Nigeria's electoral process to the barest minimum and offer a free and fair election to Nigerians.

REFERENCES

[1] E. Onwudiwe "Communal Violence and the future of Nigeria" GLOBAL DIALOGUE Volume 6, Number 3–4, Summer/Autumn 2004—Africa in Crisis. Available at http://www.worlddialogue.org/content.php?id=321

[2] A. Guobadia "How to improve Nigeria's Electoral System", 2005, available at http://dawodu.com/guobadia1.htm.

[3] A. Mobolaji, "Securing the future of our electoral democracy in Nigeria", available at http://www.nigeriavillagesquare.com/articles/mobolaji-aluko/securing-the-future-of-our-electoral-democracy-in-nigeria.html - 2007

[4] R. Okonigene and C.E Ojieabu, "Developed Automated Electoral System Algorithm using Biometric Data to Eliminate Electoral Irregularities in Nigeria". International Journal of Computer Applications (0975 – 8887) Volume 14– No.6, February 2011.

[5] S. Hof, "E-Voting and Biometric Systems?" Electronic Voting in Europe - Technology, Law, Politics and Society, Workshop of the ESF TED Programme together with GI and OCG, July, 7th-9th, 2004, in Schloß Hofen / Bregenz, Lake of Constance P-47, 63-72 (2004). Available at http://subs.emis.de/LNI/Proceedings/Proceedings47/Proceeding.GI.47-7.pdf

[6] G. Ofori-Dwumfuo and E. Paatey , "The Design of an Electronic Voting System" Research Journal of Information Technology 3(2): 91-98, 2011, ISSN: 2041-3114 Maxwell Scientific Organization.

[7] R. Joaquim, "A fault tolerant voting system for the internet. M.S. Thesis, IST/UTL, Lisboa, 2005.

[8] E. Amankona and E. Paatey, "Online Voting Systems". Graduation Project, Wisconsin International University College, Ghana, 2009.

[9] A. Sergei, L. Nikolai, and L.Vitaly, The Guarantor: A web-centric system for organization and remote monitoring of election events, Transforming Government: People, Process Policy,5(1): 56-67. 2011.

[10] D. Bhattacharyya, R. Ranjan, F. Alisherov A., and M. Choi, "Biometric Authentication: A Review", International Journal of u-and e-Service, Science and Technology Vol. 2, No. 3, September,2009.

[11] Biometric Authenticator Lite Edtion Manual available at http://www.biometricsdirect.com