Mobile, Secure E - Voting Architecture for the Nigerian Electoral System

Nwogu Emeka Reginald

Directorate of Information and Communication Technology, Michael Okpara University of Agriculture, Umudike, Umuahia, Abia state, Nigeria.

Abstract: *This work discusses electronic voting for the Nigerian electoral system, modeling a two-level hierarchical architecture that includes the national and state level infrastructure. This solves most of the electoral challenge in the country. The system proposed is a form of Public Network Direct Recording Electronic Voting System (PNDRE Voting System) that run on a Virtual Private Network (VPN) implemented on the existing General System for Mobile (GSM) communication network infrastructure. It makes use of asymmetric cryptography, with the preferred protocol being RSA algorithm running on a Public Key Infrastructure (PKI) that enables the various communicating units of the system to be authenticated for information exchange; making it impossible for attackers to break into the system. Smartcards are used as voter accreditation tokens, with every prospective voter having to first register by supplying their biological and voting information to the Voter Information Database. This allows very good mobility and flexibility on the system, as voters can register and cast their votes at different polling stations other than where they were registered. The system is proposed with the good ergonomics, allowing even non ICT compliant persons to use it efficiently.*

Keywords: *E – Voting, Public Key Infrastructure, Electronic Voting System, Electronic Voter Register, Voter Information Database, Smartcard.*

I. Introduction

In all the world's established democracies, elections are a national and very serious civic business. This is because a country's leadership is produced through this process. Governments in these democracies have continued to invest huge sums of money in search of better ways of managing and administering electoral processes in order to make it easier, less tedious and less controversial. Despite the investments on elections and electoral processes, it has seemed most countries – especially developing countries like Nigeria may have to wait longer than necessary to achieve near electoral efficiency.

So many challenges are associated with elections and electoral processes; these have made it even more difficult for countries that run manual electoral system to effectively organize free and fair elections. Some of these challenges have been identified to include ballot box snatching and stuffing, difficulty in timely delivery and distribution of electoral materials, biased electoral umpires and officials, result manipulation, inconclusive elections, low voter turnout, disenfranchisement of eligible voters, child voter registration, poorly managed voter registration process and week electoral policies and laws. Nigeria as a country has got her unfair share of the challenges listed above, which has made it increasingly difficult to organize complaint free elections.

Some pro-technology pundits have argued strongly and unequivocally that the introduction of verifiable, accountable, auditable and reliable technology in the electoral process in Nigeria can go a long a way in addressing the challenges listed in the foregoing. This stand has not been without strong opposition from some schools of thought; as the opponents of e - election have continually argued that the introduction of technology, especially information technology can lead to widespread and uncontrolled hi-tech electoral manipulation from desperate politicians. This topic has been debated severally on the floors of the two chambers of the National Assembly of Nigeria, with the outcome being the dropping of such bills seeking to introduce e - election in the country.

Nigerians on the other hand have continued to voice out their frustrations over the electoral system and consequently, there have been loud outcries from most Nigerians for the development of a system that minimizes the intricacy in this process. Such system, they say will encourage voter participation in the electoral process by reducing the stress associated with it.

This work presents a secure architecture for a mobile voting system specifically for Nigeria. It describes a system that will not only enable voters to cast their votes electronically and securely, but also allows them cast their votes from any polling station in any part or state of the country other than where they were registered or are resident.

1.1 Scope Of The Work

This work did not analyze the current electronic voting technologies with a view to designing a more robust system. It only modeled an electronic voting architecture for the Nigerian electoral system.

II. Current Voting System In Nigeria

Currently, Nigeria operates an open secret ballot system. This system is open because elections are done in the open where prospective voters queue up in wait for their turn; the ballot paper is dropped after marking, in a transparent ballot box located in an open place. The secret nature of this system is that voters mark and fold their ballot papers in a cubicle where nobody is able to see what they have marked or who they have voted for. Elections in Nigeria are administered by the Independent National Electoral Commission (INEC).

As of 2011 elections, Nigeria had about 120,000 polling units. Voter registration was done at any of the 8800 registration centres nationwide.

The election process in Nigeria starts with voter registration, where eligible voters (people from eighteen and above) supply their information including biometric data at any registration centre to be stored in the INEC database. According to Institute Policy (2000), INEC began modernizing her information technology infrastructure by migrating from an outdated legacy voting system heavily dependent on inaccurate paper records and polling cards to the newer Electronic Voting System (EVS). Kuye et al (2013) write that the EVS includes in it, the Electronic Voter Register (EVR), which, by capturing the names of all eligible voters, eliminates duplication of voters and minimizes discrepancies in the electoral process. After the voter registration process, a plastic voter’s card is produced for every registered voter and subsequently issued to the voters before Election Day.

On Election Day, voters are required to first be accredited by presenting their voter’s card to an electoral official who in-turn, checks that the voter’s name is on the register for the polling station where they have presented themselves for casting of vote. Once this is confirmed, the voter is accredited and issued with a ballot paper. They in-turn go to the voting cubicle where they mark there ballot paper by thumb printing on the space for the candidate and party of their choice. The marked ballot paper is then folded and dropped in the transparent ballot box. This completes the voting process.

III. Electronic Voting

According to Oostveen .A.M. and Bessdaar P.V. (2009), electronic voting system (also known as e – voting) is an electronic system which uses electronic ballot that would allow voters to transmit their secure and secret voted ballot to election officials over the computer. Also VoteHere Inc (2002) defined an electronic voting (e-voting) system as one in which the election data is recorded, stored and processed primarily as digital information. Lastly, Qadah, G.Z. and Taha R. (2007) defined e-voting systems as systems that allow the eligible voter to cast their vote via a computer normally connected to internet or intranet from anywhere like home or office. The basic feature of electronic voting and an electronic voting system is that electorates are able to cast their votes electronically with the use of computers in such a way that the ballots can be transmitted electronically through a secure channel to a central collation centre where the votes can be counted in real-time with ease, thereby eliminating the usual delays and challenges associated with handling manual voting and collation. There have also been distinctions between electronic voting (E-voting), which is voting on a machine in a fixed location and internet voting (I-voting), which is voting on the internet without people having to converge at a the polling station to be able to cast their votes. The later requires more security.

According to Dimitrios Zissis (2011), supervised e-voting machines are used by voters in all elections in Brazil and India, and also on a large scale in Venezuela and the United States. He further writes that they have been used on a large scale in the Netherlands but recently have been decommissioned, due to public concern. Remote e-voting otherwise known as Internet Voting has gained popularity and has been used for government elections and referendums in the United Kingdom, Canada, Switzerland and Estonia.

The first countries to adopt widespread deployment of electronic voting in their general and state elections were Brazil in 1998 and India in 1999. The Indian electronic voting system was not networked and lacked the capacity to transmit results to a central collation centre; it still solved a need by allowing quick counting of the votes which previously took the government days to achieve. On the other hand, Brazil’s E-voting system transmitted votes to the electoral center immediately.

Dimitrios Zissis (2011)**,** reports that since 1998, the Swiss government has actively pursued the implementation of electronic voting (e-voting), as Switzerland has a large number of elections performed on a yearly basis.

In France, the first e-voting project was in the constituency of Brest, during the 2004 local elections, on the 21 and 28 March of that year (Norwegian Working Committee, 2006). Consequently, during the country’s presidential elections of 2007, e-voting systems were used in 82 localities as a pilot test.

The US on the hand has continued to run experiments with different forms of electronic voting for some years now; and currently, numerous voting technologies have been implemented across the country. Also, during the 2004 presidential election, around 40 million votes were cast electronically in polling sites in the US.

In 2005, Estonia became the first country to deploy I-voting in her general elections which allowed voters to cast their votes using a computer with internet facility.

3.1 Electronic Voting Security Requirements

According to Internet Policy Institute (2001), electronic voting systems should satisfy the following security requirements;

1. **Authentication**: Only authorized voters should be able to vote.
2. **Uniqueness**: No voter should be able to vote more than once.
3. **Accuracy**: Voting systems should record the votes correctly.
4. **Integrity**: Votes should not be modified without detection.
5. **Verifiability**: It should be possible to verify that votes were correctly counted in the final tally.
6. **Auditability**: There should be reliable and demonstrably authentic election records.
7. **Reliability**: Systems should work robustly, even in the face of numerous failures.
8. **Secrecy**: No one should be able to determine how any individual voted.
9. **Flexibility**: Equipment should allow for a variety of ballot question formats.
10. **Convenience**: Voters should be able to cast their votes with minimal equipment and skills.
11. **Certifiability**: Systems should be testable against essential criteria.
12. **Transparency**: Voters should have a general understanding of the whole process.
13. **Cost-effectiveness**: Systems should be affordable and efficient.

3.2 Advantages Of Electronic Voting

Council of Europe-Commitee of Ministers (2004) lists the advantages of electronic voting to include the following;

1. Facilitating participation in elections and referendums for all those who are entitled to vote, and particularly of citizens residing or staying abroad
2. widening access to the voting process for voters with disabilities, or those having other difficulties in being physically present at a polling station and using the devices available there
3. Increasing voter turnout by providing additional voting channels
4. Bringing voting in line with new developments in society and the increasing use of new technologies as a medium for communication and civic engagement in pursuit of democracy
5. Reducing, over time, the overall cost to the electoral authorities conducting an election or referendum
6. Delivering voting results reliably and more quickly
7. Providing the electorate with a better service, by offering a variety of voting channels.

3.3 Issues With Electronic Voting

The main issue with electronic voting has been securing the device from the activities of hackers and fraudsters. According to Adida (2006), electronic voting requires a level of security higher than e-commerce. He further states that e-commerce grade of security will not be good enough for e-voting systems. There have been such issues as tampering with system’s configuration in order to manipulate the election results and threats posed by insiders (electoral officials). Kohno et al (2004) raised such issues as privacy and double voting problems etc. Another problem with electronic voting has been the preserving of the anonymity of voters.

Also Tadayoshi et al (2004) discussed the ergonomics of such a system. They posit that voting systems must be comprehensible to and usable by the entire voting population, regardless of age, infirmity, or disability. This view is also shared by kohno et al (2004), where they posit that e-voting systems must not be too complex so voters can understand how to use these systems and also have confidence in the system that their votes are counted.

IV. Research Design

Nigeria is a republic of 36 federating states, a federal capital and 774 local government areas. There are three tiers of government in Nigeria, namely; the federal, state and local governments. The country is further politically divided into 6 geo political zones representing the six geographical areas of the country. Elections are conducted usually four-yearly at the federal and state levels and three-yearly at the local government levels or sometimes when needed, to fill up the executive and legislative positions in the three tiers of government.

Each Nigerian belongs to a ward at the local government level. This is the lowest level of democratic representation in the constitution of the federal republic of Nigeria. Consequently, every Nigeria is expected to operate from their ward.

4.1 New System Design

The proposed electronic voting system is a form of a Direct Recording Electronic (DRE) machine but with advanced features. According to Marco Ramilli (2008), an electronic machine is able to collect ballots using a large display (typically a touch screen) to visualize the ballot, a touch screen monitor or buttons set to collect the votes and a smart software to record them. The system proposed here differs with the conventional DRE in the sense that ballots are transmitted straight to a central office. G.O. Ofori-Dwumfuo and E. Paatey (2011) called this system a Public network DRE voting systems (PNDRE).

Our system will comprise the electronic voting terminal (client), the electronic voting tallying server, the voter information database, the card authentication system, the public key infrastructure, the vote-escrow system and the electronic voter's card. The proposed media is a Virtual Private Network (VPN), run on the existing General System for Mobile (GSM) communication's Radio Frequency (RF) network across the country.

These various components of the proposed system are arranged in a two-level hierarchical physical architecture. This makes the management of elections and election data a lot easier.

4.1.1 Electronic Voting Terminal (CLIENT)

This is a standalone machine with two terminals (accreditation terminal and vote casting terminal) that enables the voter accredit and cast their vote by inserting their electronic voter's card into the card reader slot just like the ATM card. The screen is touch-screen with good ergonomic features that make it extremely easy for the voter to cast their vote with ease even without being Information Technology compliant or computer literate.

The accreditation terminal is placed before the election official who inserts the voter's card into the slot for accreditation. The terminal has a display screen and some control buttons that help cancel or reset the machine when error occurs. This terminal also notifies the election official of successful or unsuccessful casting of votes.

The vote casting terminal is placed in a cubicle where the voter is expected to enter and cast their vote without being observed by anybody. Less knowledgeable voters may request assistance from the official.

The machine is designed with features that enable it dial and connect with the necessary servers and databases for voting to commence. It is also designed with encryption and authentication features.

The only confirmation of successful voting for the voter is a vote casting receipt. This machine is placed in all polling booths.

4.1.2 Electronic Voting Tallying Server

According to Abu-Shanab et al (2010), the tallying authorities collect the cast votes and tally the results of the election. The tallying server receives the ballots from the voting terminal, processes and collates the votes. This machine is located at the central office. We have adopted a two-level central office model where each state has a central office called the level two central offices that connect and synchronizes with the national central office called the level one central office.

The level one central office processes all local elections in the state like state and local government legislative elections, state and local government executive elections and federal legislative elections. Each level two central office has two back-up central offices that synchronize with the active central office. Also the level one central office has two back-up central offices in different parts of the country.

This server is equipped with server software and ballot processing application with a data warehouse for information storage.

4.1.3 Voter Information Database

The voter information database contains the record of all registered voters in the country. Whenever a voting request and query are sent to this database by the voting terminal, it calls up the prospective voter's election and voting area information irrespective of where it is queried from or the particular voting terminal that sent the request. This is the mobile nature of this system, since voters can vote even in ward councilor elections from just any part of Nigeria. This database is designed in a two hierarchical structure, namely the executive and the legislative hierarchies. Every record on this database belongs to a particular ward which is simply the smallest grouping of voters in the Nigeria electoral system. Each ward belongs to the two hierarchies listed above.

On the Executive hierarchy, every ward is associated to a particular Local Government Area, which belongs to a particular State of the country and then the country at large. On the legislative hierarchy, every ward belongs to a particular state constituency; each state constituency belongs to a particular federal constituency, while each federal constituency belongs to a particular senatorial zone of a state.

Table 1 Sample voting information table in the Voter Information Database

	Voting information
🔑	**National Identification Number**
	Ward
	Local Government Area
	State

Table 2 Sample Biological information table in the Voter Information Database

	Bio-information
🔑	**National Identification Number**
	Surname
	First name
	Last name
	Maiden Name
	Date of birth
	Place of birth
	Sex
	Marital Status
	Photo
	Fingerprint
	State of origin
	Local Government Area
	Home town
	Education
	Office address
	Residential address

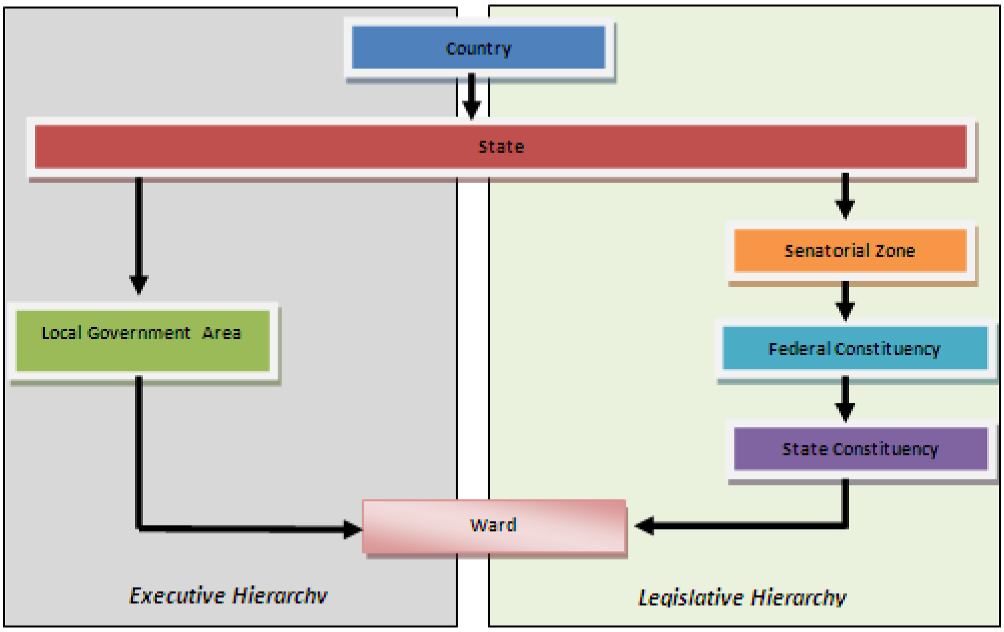


Fig. 1 Macro model of executive and legislative hierarchies

4.1.4 Card Authentication System

This system comprises the authentication server and election database. The authentication system receives an election request for a particular card from the voting terminal. Using the card ID, the authentication server queries the election database to find out if the requested election is available for the card. On the database, there is a list of available elections (elections the card can participate in) and that of unavailable election (elections the card has participated in). All elections are identified using their IDs. Once the election is confirmed available for the card, the card authentication system authenticates the card by adding a logic one value on the election availability field of the response. With this field turned on for the card, a similar voting available field is sent to the tallying server, informing it of an election availability state for the card with the card number. The voting terminal can now use this authentication message to connect to the tallying server for voting to begin. Once a request is sent to the tallying server, the server confirms that the message on the card authentication information is the same as the earlier received message from the card authentication server, then it can register the cast ballot.

If an election has been confirmed unavailable for the card ID, the card authentication server turns the election availability field to a logic zero. Once the voting terminal gets this message, it automatically informs the voter and the election official of an election unavailability status for the card.

4.1.5 The Public Key Infrastructure

PKI enables users of a basically unsecure public network such as the Internet, to securely and privately exchange data and money through the use of a public and a private cryptographic key pair that is obtained and shared through a trusted authority (Ane Divine Jinor, 2011).

The public key infrastructure authenticates the voting terminal to the voter information database, the card authentication system and the tallying server. Keys are distributed between the voting terminal and the other servers. These keys will be used to encrypt and decrypt information during communication between the voting terminal and any of the other systems.

4.1.6 The Vote-Escrow System

The vote escrow system is a third party vote storage information system. This will be used only for result verification and authentication. All the cast ballots can be printed and counted manually or automatically as it is done at the tallying server. A second agency different from INEC will be responsible for this system. When a voter casts their vote, the cast ballot is sent to both the tallying server and the vote-escrow system. The strong encryption and authentication system ensures no tampering of the information sent to either system.

Parties who are not satisfied with the election result can with the authorization of an election tribunal request a recount of the votes at the vote-escrow system.

4.1.7 The Electronic Voters’ Card.

This card is similar to a smartcard, with a unique card identification number hard-coded into a chip on the card. This number is used to identify the voter together with their palm-print information. The card number is used to create a voter profile at the voter information database that contains voter bio-information and voting information.

4.2 New System’s Operation

A prospective voter inserts their card in the accreditation terminal before the election official. Once inserted, the terminal connects to the Public Key Infrastructure to acquire a ticket. With the help of this ticket, the terminal is authenticated to the voter information database and subsequently connects to this database to verify the validity of the voter. Once it is verified that the card information exists in the voter information database, the machine prompts the user to supply their palm print information and if accepted, the machine connects to the card authentication server to confirm the availability of that particular election for the card. If there has been a vote cast on that particular election, ineligible voter information is returned on the screen, and the session is subsequently closed with the voter’s card being ejected from the card slot. And if no vote has been cast on that particular election, the machine returns eligible voter information and uses the card ID to query the database to generate the voter’s ward information which will be used to call up the ward’s candidates’ data. The voter is subsequently asked to go to the vote casting terminal; this completes the accreditation phase. A session is now opened at the vote casting terminal in the voting cubicle with the ballot window and voter’s information on each half of the screen. The voter will only need to scroll to the logo of the party of their choice and press any finger on the voting box on the ballot window to supply fingerprint information which indicates successful voting by showing a green indicator or returns a red indicator if an error occurs.

Once a vote has been cast, the electronic voting client sends the ballot to two machines at a time, the electronic vote tallying server and the vote-escrow database. The tallying server collates the result while the vote-escrow database keeps a record of the votes which can be subsequently printed and verified if need arises. A voting receipt is generated and printed for the voter before the session for that particular card is closed with the ticket expiring. The receipt contains the polling booth information, the voter information and the time of the vote.

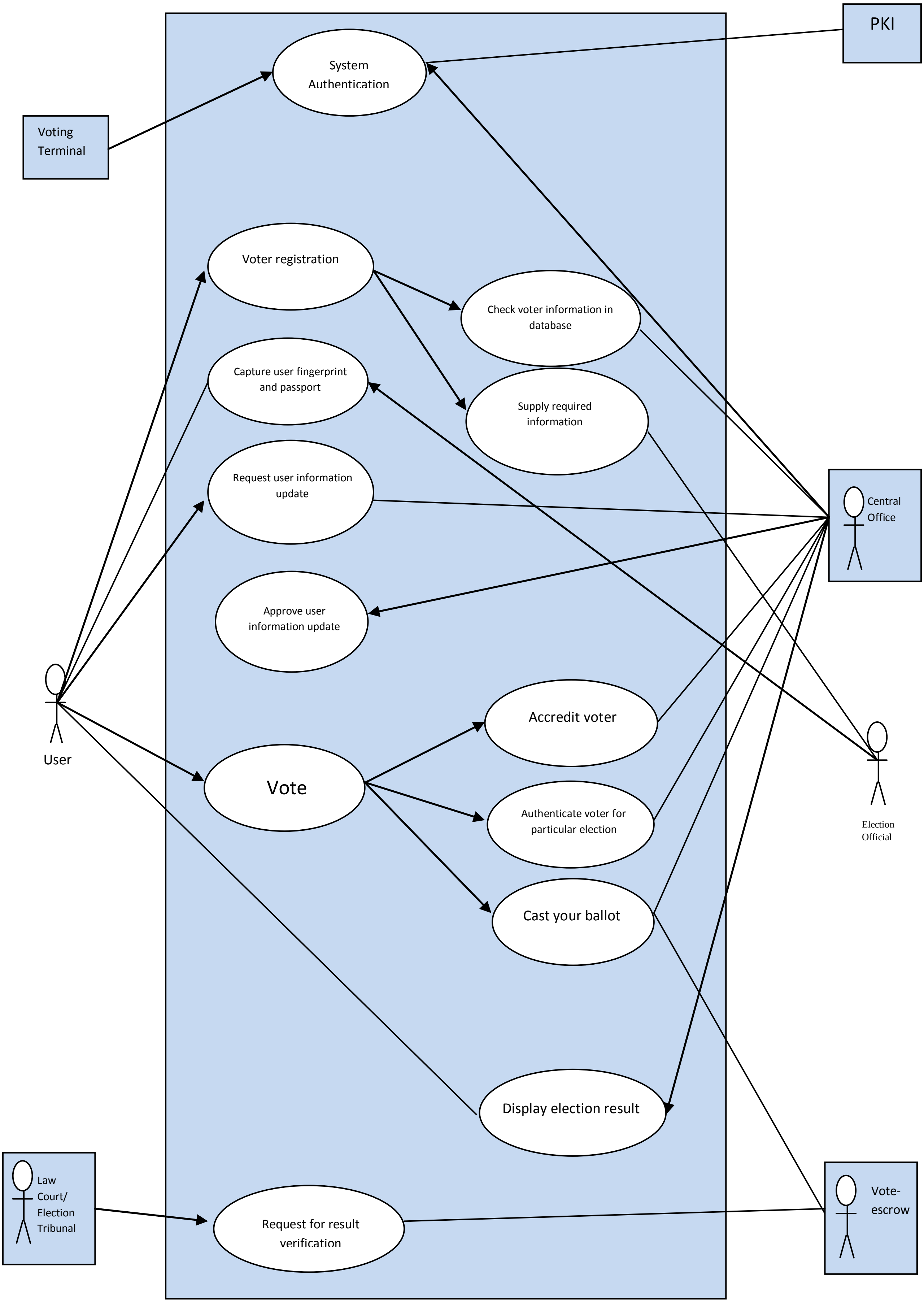

PKI
System Authentication
Voting Terminal
Voter registration
Check voter information in database
Capture user fingerprint and passport
Supply required information
Request user information update
Central Office
Approve user information update
User
Accredit voter
Vote
Authenticate voter for particular election
Election Official
Cast your ballot
Display election result
Law Court/ Election Tribunal
Request for result verification
Vote-escrow

Fig. 2 Use Case diagram for the system operation

4.3 New System's Physical Architecture

The system proposed here is arranged in a two –level hierarchical structure. The level two of this hierarchy is the state owned tallying centre (collation centre). The state owned tallying centres process, tally and announce results of local state election. The level one of this hierarchy is the national tallying centre. This centre processes, tallies and announces results of national elections such as the presidential elections. There is also communication and synchronization between the state owned central office infrastructure and the national central office infrastructure.

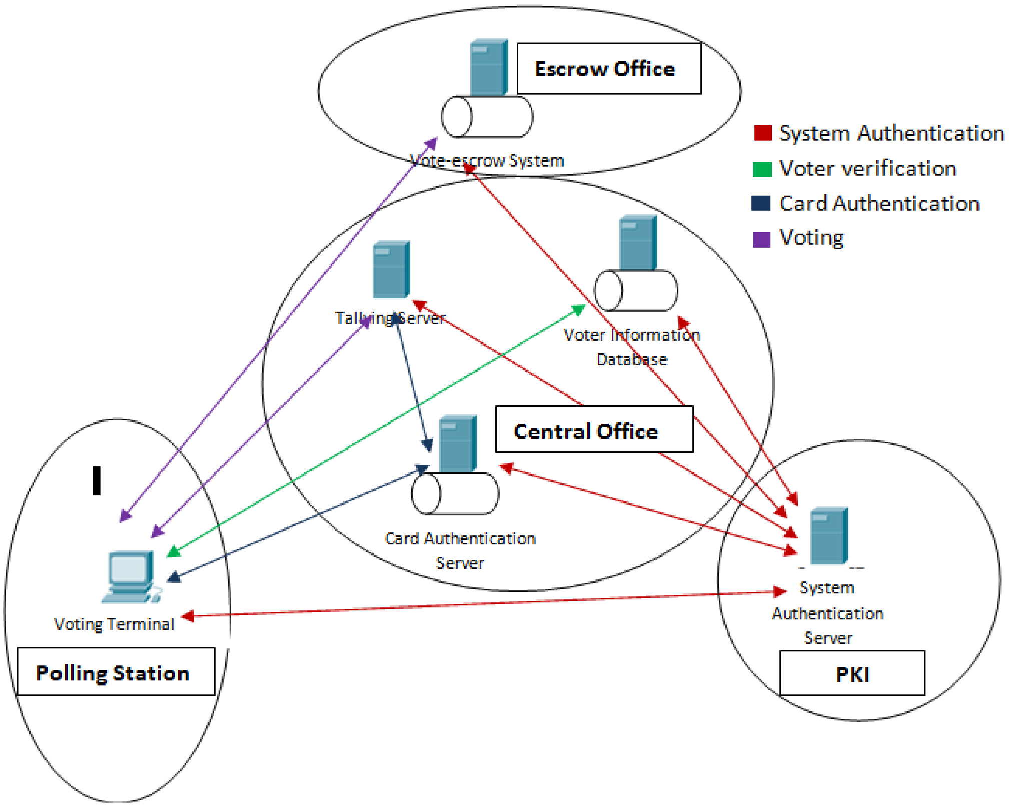


Fig. 3 New system unit architecture

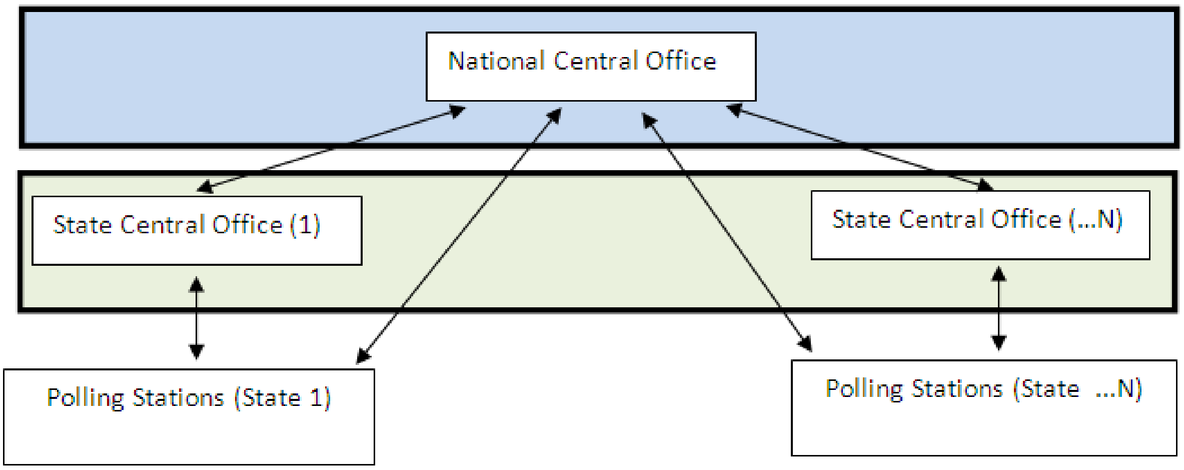
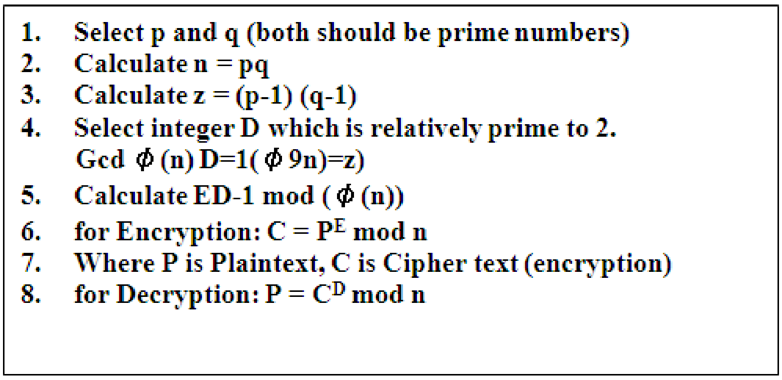

National Central Office
State Central Office (1)
State Central Office (...N)
Polling Stations (State 1)
Polling Stations (State ...N)

Fig. 4 Two-level hierarchical architecture of the proposed system

4.4 New System Security Protocols

The system proposed here makes use of good security protocols. We have adopted asymmetric cryptography; this is because the proposed system will run on the existing GSM network infrastructure. Asymmetric cryptography is also known as public key cryptography. According to A.V.N. krishna (2009), Public-key encryption (also called asymmetric encryption) involves a pair of keys a public key and a private key, used for security & authentication of data. Each public key is published, and the corresponding private key is kept secret. One other reason for the adoption of public key cryptography is because of the flaw associated with private keys. Once private keys are intercepted by an attacker, the information can be decrypted easily. The most widely used and known form of public key cryptography is the RSA algorithm. According to Cormen et al (2001), the RSA cipher was described in 1997 and the name was taken after the inventors Ron Rivest, Adi Shamir and Leonard Adleman.

The process of the RSA algorithm is described in the figure below;



1. Select p and q (both should be prime numbers)
2. Calculate n = pq
3. Calculate z = (p-1) (q-1)
4. Select integer D which is relatively prime to 2.
Gcd ϕ (n) D=1(ϕ 9n)=z)
5. Calculate ED-1 mod (ϕ (n))
6. for Encryption: C = P^E mod n
7. Where P is Plaintext, C is Cipher text (encryption)
8. for Decryption: P = C^D mod n

Fig. 5 RSA algorithm process

4.5 New System Mobility

The current arrangement in the Nigeria electoral system is that one must vote at the same polling station where they were registered, thereby disenfranchising those who may not be in the same place where they were registered during elections. This has caused a lot of problems in the country. The system proposed here makes voter’s card highly mobile, making it possible for one to register and cast their vote at separate polling stations.

During voter registration, one only needs to be associated with a particular ward in a particular Local Government Area and in a particular state of the country. One will be able to vote in election regarding their ward and state just from any location. This is made possible by the synchronization of the state central offices with the national central office; thus having uniform voter information database across the state central offices and the national central office.

V. Conclusion

Electronic voting offers good ergonomics especially to the voter, election managers and organizers. The system proposed here will go a long way in minimizing most of the electoral issues that have been predominant in the Nigeria electoral system. One such issue is that of trust and confidence in the ability of INEC as a body to conduct a fair election, free of most of the common electoral malpractices seen at the moment. Another issue is the problem of voter mobility. The system makes it possible for voters to vote in places order than their place of registration.

Perhaps, the biggest advantage offered by this system, is the prospects of automation and easy management of the whole electoral process; from voter registration to voter information update and even to Election Day activities that include voter accreditation, casting of ballots, tallying and collation of the ballots and results.

This architecture is affordable, maintainable, scalable and can be implemented easily.

References

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

[2]. Marco Ramilli (2008) Designing A New Electronic Voting System. M.Sc Thesis Alma Mater Studiorum - University of Bologna

[3]. Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest and Clifford Stein (2001), Introduction to Algorithms, second edition.MIT press and MC Graw Hill

[4]. A.V.N.Krishna (2009), Performance Evaluation of New Encryption Algorithms with Emphasis on Probabilistic Encryption & Time Stamp in Network Security. Department of Computer Science and Engineering, Acharya Nagarjuna University, Nagarjuna Nagar – 522 510 Andhra Pradesh, India

[5]. Ane Divine Jinor (2011), Pro-active Architecture and Implementation of a Secure Online Banking System that Uses Fingerprint Data as Part of Client Side Digital Signatures. M.Sc Thesis, Information Technology University of Copenhagen, ftware Development Technology Department

[6]. Abu-Shanab E., Knight M. and Refai H. (2010) E-Voting Systems: a Tool for E-Democracy, Management Research and Practice Vol. 2 Issue 3, pp: 264-274

[7]. Kuye C.O, Coker J.O, Ogundeinde I.A and Coker C.A. (2013), Design and Analysis of Electronic Voting System in Nigeria, International Archive of Applied Sciences and Technology IAAST; Vol 4 [2]: 15-20

[8]. Institute Policy (2000): “Report of the National Workshop on Internet Voting: Issues and Research Agenda, Proceedings of 2000 Annual National Conference on Digital Government Research, 1-5

[9]. Internet Policy Institute (March 2001), Report of the National Workshop on Internet Voting, USA

[10]. Kohno T., Stubblefield A., Rubin A.D., and Wallach D.S. (2004) Analysis of an Electronic Voting System," Security and Privacy. Proceedings. 2004 IEEE Symposium on , vol., no., pp. 27-40, 9-12 May 2004 doi: 10.1109/SECPRI.2004.1301313. retrieved December 12, 2015 from http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1301313&isnumber=28916

[11]. Voke Augoye (2013), Electronic Voting: An Electronic Voting Scheme using the Secure Payment card System, Information Security Group Royal Holloway, University of London Egham, Surrey TW20 0EX, United Kingdom

[12]. Tadayoshi Kohno, Adam Stubblefield, Aviel D. Rubin and Dan S. Wallach (2004), Analysis of an Electronic Voting System, IEEE Symposium on Security and Privacy

[13]. Oostveen .A.M. and Bessdaar P.V. (2009), Users Experiences with E-voting: A Comparative Case Study, J of Electronic Governance, vol.2, No 4, pp 38-46

[14]. VoteHere Inc. (2002), Network Voting Systems Standards, Public Draft 2, USA

[15]. Adida, B. (2006), Advances in Cryptographic Voting Systems. Electrical Engineering, Massachusetts Institute of Technology

[16]. Qadah, G.Z. and Taha, R. (2007), Electronic Voting Systems: Requirements, Design, and Implementation. Comput. Stand. Interf. 29(3), 376–386 (2007)

[17]. Council of Europe. (2004). Recommendation Rec (2004)11 of the Committee of Ministers to member states on legal, operational and technical standards for e-voting. BMJ (Clinical research ed.), 340, c3033. Retrieved from http://www.pubmedcentral.nih.gov/articlerender.fcgi?artid=2933870&tool=pmcentrez&rendertype=abstract.

[18]. Dimitrios Zissis (2011) Secure Electronic Voting Information Systems**,** PHD dissertation, Department of Product and Systems Design Engineering, University of The Aegean

[19]. Norwegian Working Committee (2006), Electronic Voting – Challenges and Opportunities. Retrieved December 12, 2014 from http://www.umic.pt/images/stories/publicacoes1/evalg_rapport_engelsk.pdf