SIMULATION OF BIOMETRIC E-VOTERS REGISTRATION USING SMART CARD TOKEN AS AUTHENTICATION FOR DISTRIBUTED SYSYEM

OGUNLOLA Okunola O[1], FALUYI Bamidele I[2]

[1,2]*Department of Computer Science, The Federal Polytechnic, Ado Ekiti*

Abstract: Elections in Nigeria had been marred with irregularities like multiple registrations, false registration and under aged registration. It is desirable to design and develop a secured e-voters registration model based on smart card biometric token and Rivest Shamir Adleman (RSA) Public-key Encryption Algorithm that enhances transparent and accountable voting.

The system model was designed to specify voters' registration model and smartcard based on Rivest Shamir Adleman (RSA) Algorithm. The Independent National Electoral Commission (INEC) officials verify the voters' eligibility by matching the minutiae template with the voters' minutiae before issuing the secured smart cards. The front-end application was designed using Java as programming language for the e-voter registration system while MySQL version 2.26 was used as back-end for the database running on Microsoft Window 8 Ultimate platform. DigitalPerson fingerprint scanner was used to capture the minutiae of the fingerprint of voter and U20 Digital Camera to take the photograph of the voter.

Voters card based on paper-ID cards and plastic ID cards could be torn or destroyed or lost but voters ID cards embedded with cryptographic smart cards is durable, user friendly and convenient for physical access control with high-rate of security.

A secure voter registration system combining both smart card and biometric technology can provide a very high level of confidence in the confirmation of sustainable voter register, while also improving overall security and protecting the voter's privacy. The use of smart card reduces counterfeiting attempts due to enrollment process that verifies identity of the voters and captures their biometrics.

Keywords: Voter's Registration, Authentication, Biometric, Distribution SystemSmart Card, INEC

1. INTRODUCTION

The ability to exercise the democratic voting forms an important part of democracy. In any country, for democracy to be sustainable, the voter's participation is a key consideration. Apart from voters being encouraged to exercise this democratic right, the election that facilitates the function must be credible, watertight and free of bias (Masuku, 2006). Election is a fundamental instrument of democracy that provides an official mechanism for people to express their views to the government. Voting and elections are very essential in making communities modern. Unlike any other transactional events, the result of elections determines the fate of these communities and their wellbeing either positively and/or negatively.

Voter's registration is the process of recognizing citizens' eligibility to vote in an election and collecting their personal details in a register called a Voter Register. A comprehensive voter registration is very important to a successful election. Voter's registration is highly complex and is the single most expensive activity within the framework of elections. Voter's registration is not just the procedural implementation of an activity; it is administrative and practical process. The place of voter's registration is highly important when it comes to evolving democracies: it can make or mar an election. The quality of the process of registration and its subsequent product, that is the Voters Register, can determine the conclusion of an election and consequently the strength of the democratic institutions of a country. (Astrid, 2010)

Authentication is the process of showing that someone (in this case, an intending voter) is whom he /she is claimed to be. Typically, a person could be identified based on (i) a person's possession ("something that you possess), for example, permission is given to individual person have access into a building by providing an acceptable key to the building; (ii) person's knowledge of a piece of information ("something that you know"), for example, permission granted to a system based on the knowledge user-id and a password associated with it. Another approach to positive identification is based on identifying physical characteristics of the person. The characteristics could be either a person's physiological traits, e.g. fingerprints, hand geometry, etc. or her behavioural characteristics, e.g. voice and signature. The method of identification of a

person based on his/her physiological/behavioural characteristics is called Biometrics, since the biological characteristics cannot be forgotten (like Passwords) and cannot be simply shared or misplaced (like keys), they are generally considered to be a more reliable method to solving the personal identification problem (Prabhakar, 2001). Biometric characteristics are distinctive that cannot be forgotten or lost, and the person to be authenticated need to be physically present at the point of identification. Biometric is inherently more reliable and more capable than traditional knowledge-based and token-based techniques.

Biometric technology is recognition of human based on one or more intrinsic physical trait, which has become usable for voters registration purposes and many countries have successfully incorporated this technology. Fingerprints are one of the most mature biometric technologies and are considered legitimate proofs of evidence in courts of law all over the world. Fingerprints are, therefore, used in forensic divisions worldwide for criminal investigations. More recently, an increasing number of civilian and commercial applications are either using or actively considering using fingerprint-based identification because of a better understanding of fingerprints as well as demonstrated matching performance than any other existing biometric technology (Jain *et al*, 1999). In this paper fingerprint was used for biometric due to its distinctive, uniqueness and collectability.

Smart Cards, incorporating magnetic strips or data chips to store electronic data about the person who is the subject of the card. This data may include bio-identification data. The smart cards can be used with smart card readers and bio-identification readers such as fingerprint scanners to automatically verify a person's identity. Smart cards can be 'read only' cards that simply contain information about the subject or can be 'read-write' cards, which have the information contained on the card updated as the cards are used (Olabode, 2011). The smart card is now known for its high level of security and is used as a tool for authentication and authorization in today's different information systems (Bushager, 2011).

Relevant technology has developed rapidly in recent years and Independent National Electoral Commission (INEC) has begun using new equipment and programmes for managerial and operational purposes. Technological solutions have also become available for voter registration purposes, for example, voters' information is stored in electronic databases. Where capacity exists within INECs to use modern technology effectively, these developments have improved the capacity of INECs to plan and conduct elections more professionally. Just like the recent voter registration which was conducted in year 2010.

2. MOTIVATION

All elections since Nigeria's return to democratic governance in 1999 had been marred with irregularities like low turnout, multiple voting, ballot boxes stuffing among others. Reducing these electoral problems has been difficult. Voters' registration is one of the stages at which there are opportunities to manipulate election results, anomalies of the voting started from the voters registration such as double registration, false registration, ghost registration and the underage registration.

It is desirable to design and simulate a secured e-voters registration system to gear towards promoting transparent and accountable voting. For voting to be foolproof and credible, the voter's registration must be put into consideration. Voter's registration is understood as the process of registering eligible voters, while voters' register is the result of this process. Both the process and the result of voter's registration need to be accurate, sustainable and politically accepted and have tendency of reducing voting time to probably increase turnouts during the election day. Hence, the need for a procedure that supports these practice right from the registration stage of voters.

Distributed system is a collection of independent computers that appears to its users as a single coherent system or as a single system. This system is network system where data stored at different location are accessed in respective of the location and all update made to the data are reflected as if made at the original location. Saving the voters registers on the distributed system make the voters data available at any location covered by the system irrespective of change of location of the voters over a period of time. This make the voters' vote to count at his/her original registration even if (s)he is miles away.

3 RESEARCH OBJECTIVES

This work designed a secured and distributed e-voters registration model based on smart card biometric token and Rivest Shamir Adleman (RSA) Public-key Encryption Algorithm; simulate the designed model and determine the efficacy of the system using sample demographic data from the selected staff and students of Federal Polytechnic, Ado-Ekiti, Nigeria.

4 RESEARCH METHODOLOGY

The electoral system of Nigeria was studied through interviews, reading of literatures and observations of recent governorship election in Ekiti State. Successful election start with credible voters registration. Registration system that will disallow multiple registration, under age and "ghost" voters was designed using Unified Modeling Language (UML).

During the registration, the Independent National Electoral Commission (INEC) officials will request the bio-identification details of the intending voters and (s)he will provide the detail after which the system will check the eligibility of the voter whether (s)he is eligible to register by connecting with the National Identity Management Database to first authenticate the claims of the intending voter.

Thereafter, the biometric (fingerprints) will be captured and the photograph also taken and stored in the database. The fingerprint has been identified to be most unique to each person. Minutiae points are used for determining uniqueness of a fingerprint. An enrollment procedure is used to extract minutae from the fingerprint and store the minutiae into a template.

minutia features: $\{(P_1,\Theta_1,T_1), (P_2,\Theta_2,T_2),....(P_{ME},\Theta_{ME},T_{ME})\}$

where ME minutia enrolled, P is the position, Θ is the orientation, and T is the type. Minutia are the basic features, it is possible to use a subset of the full feature set to represent the fingerprint. Authentication is then reduced to a comparison of two sets of points in space and deciding if they match well enough:

enrolled featured: $\{f_{0,e}, f_{1,e},..., f_{NC,e}\}$,

comparison featured: $\{f_{0,c}, f_{1,c},...,f_{NE,c}\}$,

where NE is the number of enrolled features (minutiae) and NC is the number of live-scan or comparison features (minutiae). Generally, the number of features detected in the two different prints (i.e. the enrolled featured and comparison featured), NE and NC will be different. Therefore, the matching routine must compare two sets with a different number of elements. For example, a minutiae match score S_m can be defined as:

$$S_m = \frac{2n_m - n_n}{N_T} \quad 1.1$$

Where

N_T = (NE + NC) = total number of minutiae in both segment

n_m = number of minutiae that match

n_n = number of minutiae that do not match

and using

$n_n = N_T - 2n_{m'}$

The minutiae matching score, S_m can be rewritten as:

$$S_m = \frac{4n_m - N_T}{N_T} = \frac{4n_m}{N_T} - 1 \quad 1.2$$

A match occurs when a minutiae is detected in the comparison image at an enrolled minutiae location. A mismatch occurs when a detected minutiae from either image does not correspond to one from the other image. Based on S_m a decision is made to accept or reject the claimed identity of the user. Fingerprints extraction was done using digitalPersona Fingerprint Scanner model.

Additional level of security was added by encrypting the voter's data (both bio-data and biometric feature) using RSA algorithm before being stored in the database, and the smart card before being issued to voter. In the RSA public-key encryption, is when one key is known to the public (reveicer's public key) and is used to encrypt the information by the sender. The other key is known as a private key, and it is used to decrypt the encrypted data received by the receiver (receiver's private key). The voter encrpt an integer m, $0 \leq m < n$, which should be compute by INEC official, $c = m^e \bmod n$. In the decrypt is recover in the plaintext m from the ciphertext c as $m = c^d \bmod n$. Once the voter's card has been validated for a particular election, it cannot be used for such election elsewhere until the time lag set for the election lapses and validation for another election can be done.

5. REVIEWS OF THE RELATED LITERATURES

Olabode (2012) provides a robust, efficient and effective information technology system that will ensure proper registration of eligible voters in Nigeria. It also provides models for database architecture and structure for electronic registration of eligible voters in Nigeria by presenting the mathematical modeling of distributed database system for voters registration system. Alese and Adetunmbi (2011) highlight policy statement of the electoral regulatory body that e-voting system would be used for all elections in Nigeria from 2007 vis-à-vis the level of literacy in Nigeria. This work also gave highlights of possible problems e-voting would encounter in Nigeria if eventually implemented. Kalaichelvi and Chandrasekaran (2011) adopts biometric with smart token was used and the iris pattern as a template, to verify the voter in the election. In Sebastien and Herve (2005), the cryptographic components encountered in this voting system are Signature scheme, encryption scheme and anonymous signature scheme.

6.1 Models

6.2 Voter Registration Model Using Use Case Diagram

In Figure 1, the stakeholders are the INEC official and the voter, while the system goal is capturing of prospective voters' biometric features and store same into smart cards. The voter provides personal details to the system through the INEC official which check the eligibility of the voter before capturing the fingerprint and then issue a biometric smart card to the voter.

6.2 Voter Registration Model

Sequence diagram (as shown in Figure 2) is used primarily to show interactions between objects that are represented as lifelines in a sequential order. It is more important that lifeline show all their interaction points with other objects in events. The design of a secured smart card system

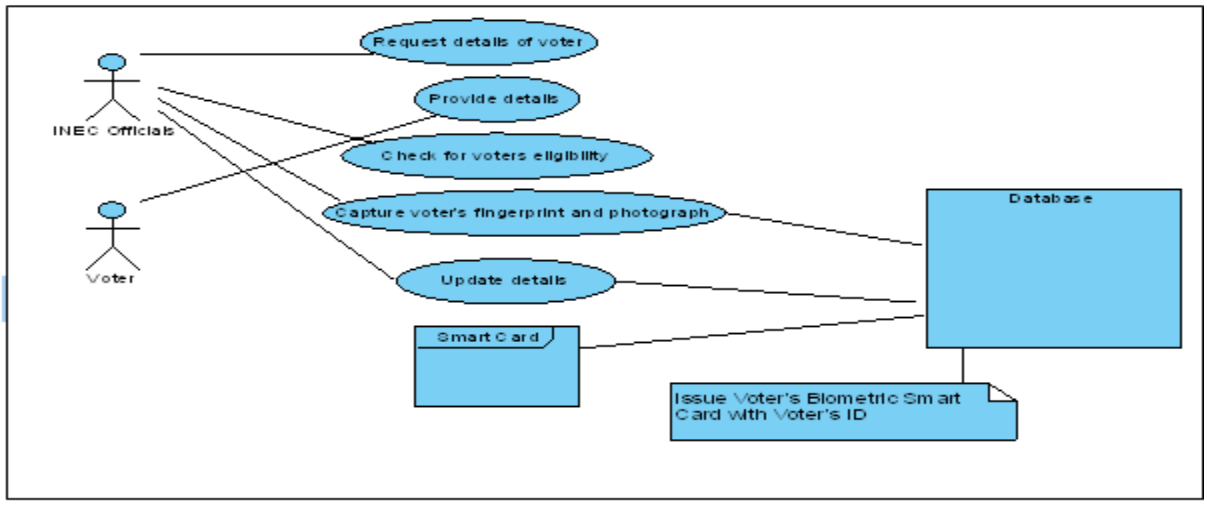

Figure 1: **Voter Registration Model Use Case Diagram**

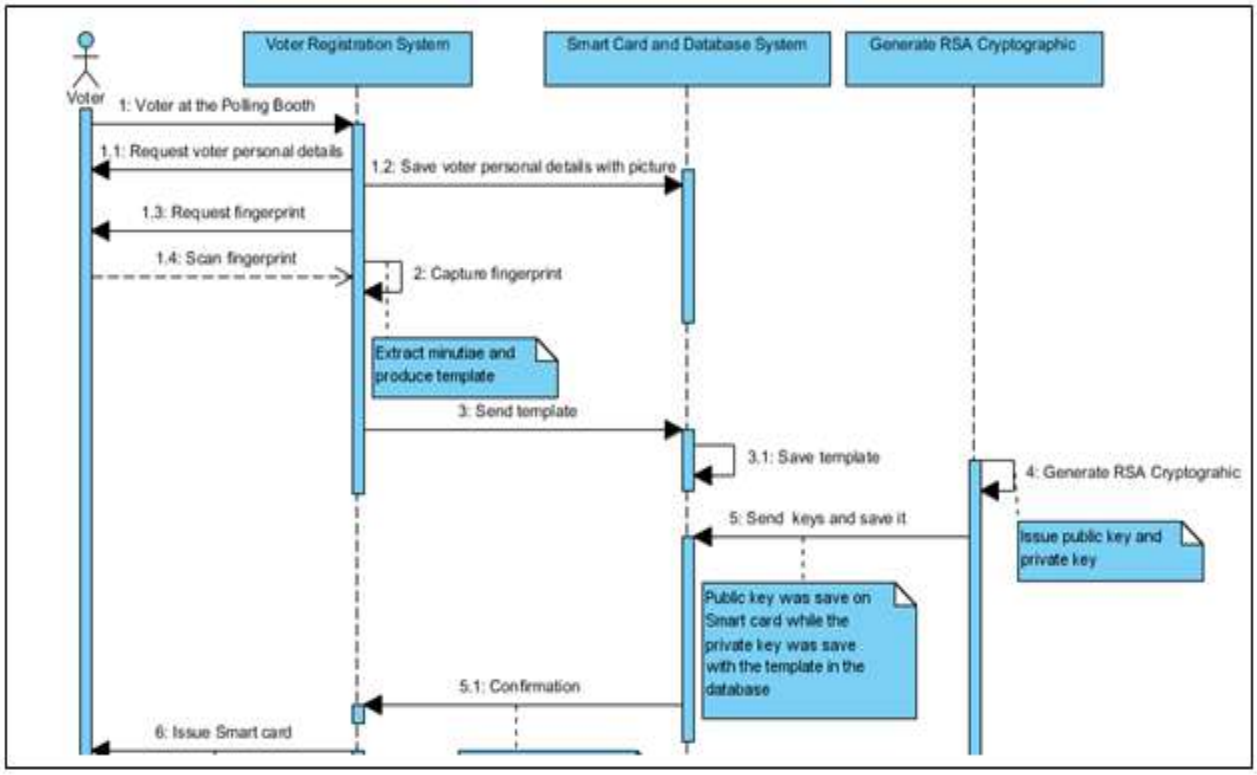

Figure 2: **Sequence Diagram for Voter Registration System with RSA Biometric Smart Card**

Must have a secure enrollment process and a secure verification and authentication process. The enrollment process is part of the registration system that is responsible for collection of voter's information, ensuring that the voter is eligible to vote and issuing of smart card. The INEC official verify the voter by authenticating the voter's claim on the national database and also matching the minutiae template with the voter minutiae before issuing the smart card and the information will be secured by using RSA algorithm. RSA is currently one of the favourite public key encryption methods. It was the first algorithm known to be suitable for encryption, as well as decryption. The key length for RSA is variable. The long key provides more security, and the short key provides less security but makes the algorithm more efficient (Pachghare, 2010, Dhiren, 2010). RSA is still widely used in electronic commerce protocols and digital signature algorithms. It is believed to be secured given sufficiently long keys. The numbers of transaction in Figure 2 shows the voter registration system with RSA Biometric Smart Card.

Transaction (1 and 2): The voter applies for the voter card and therefore provides the required information and details to the Voter Registration System. The Voter Registration System must make sure that the information provided is of high quality and accuracy. After making sure that all data are accurate, the Voter Registration System saves the voter information and captures the fingerprint, takes voter photograph and produces the template of it.

Transaction (3 - 4): The Voter Registration System send the template and save it in the smart card and database.

Transaction (5 and 6.1): Generate the RSA cryptographic and issue the keys; public keys to be on smart card while the private key will be with template in the database.

Some Screenshots of the simulated voter's registration application are shown at the Appendix of this paper.

6. CONCLUSION

Voter registration is understood as the process of registering eligible voters, while the voters' register is the result of this process. Both the process and the result of voter registration need to be accurate, sustainable and politically accepted. A secure voter registration system combining both smart card and biometric technology can provide a very high level of confidence in the confirmation of sustainable voter register, while also improving overall security and protecting the voter's privacy.

The use of smart card will reduce the counterfeiting attempts due to enrollment process that verifies identity of the voter and captures biometric. Extremely high security and excellent user-to-card authentication will be sustained and also smart cards have sufficient memory to store growing amounts of data including programs, one or more biometric templates, and multiple cryptographic keys to restrict data access and ensure that data is not modified, deleted or appended.

In this work, the voter registration system is to be more secured by incorporating smart card cryptographic keys which will serve as security measure during voting. The fraudulent acts during the election will be minimized because when the biometric on the smart card match the live biometric of the voter, this will authenticate the voter to vote. It will be trusted that the carrier of the smart card is the rightful owner of the biometric on it.

Voter card that was formerly issue by INEC was based on paper-ID card and plastic-ID card which can be torn or destroyed or lost but voters ID card embedded with cryptographic smart card will be durable, more user friendly, convenient for physical access control, support more application on it and have high-rate of security.

7. FUTURE WORK

In the future, multi-biometric can be studied and implemented for a more robust secured e-voter registration.

8. APPENDIX

Screenshot of the Simulated Application for the Secured Distributed Registration System

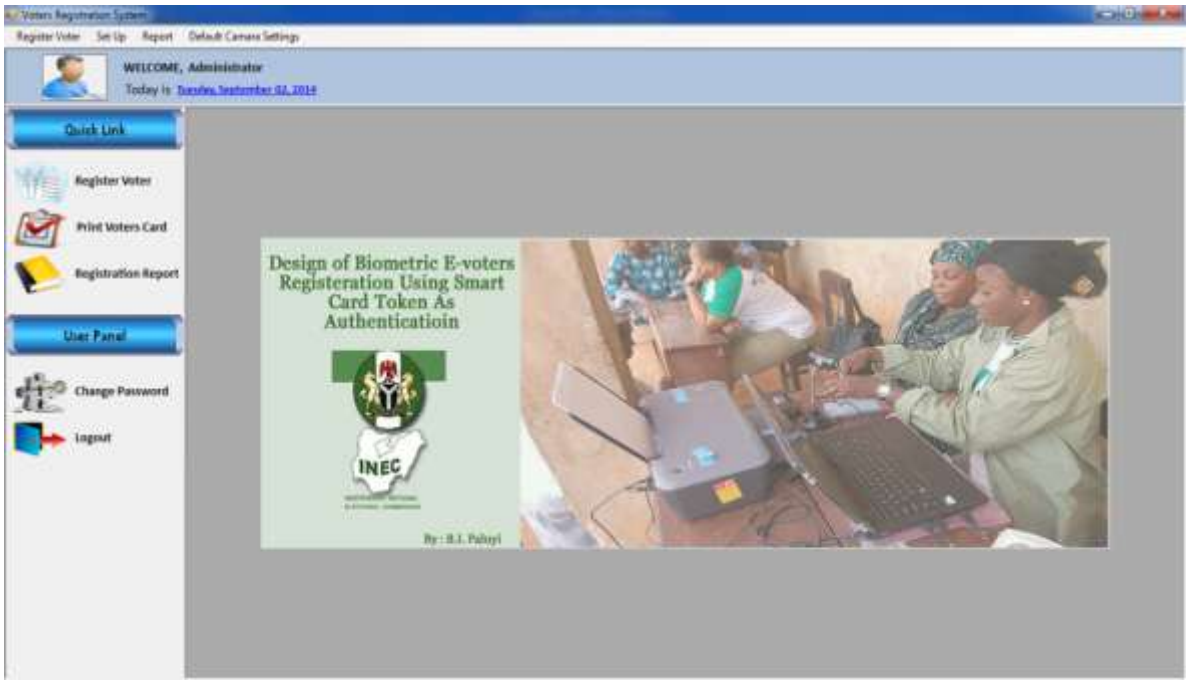

Figure 3: Main Screen for e-voter Registration System

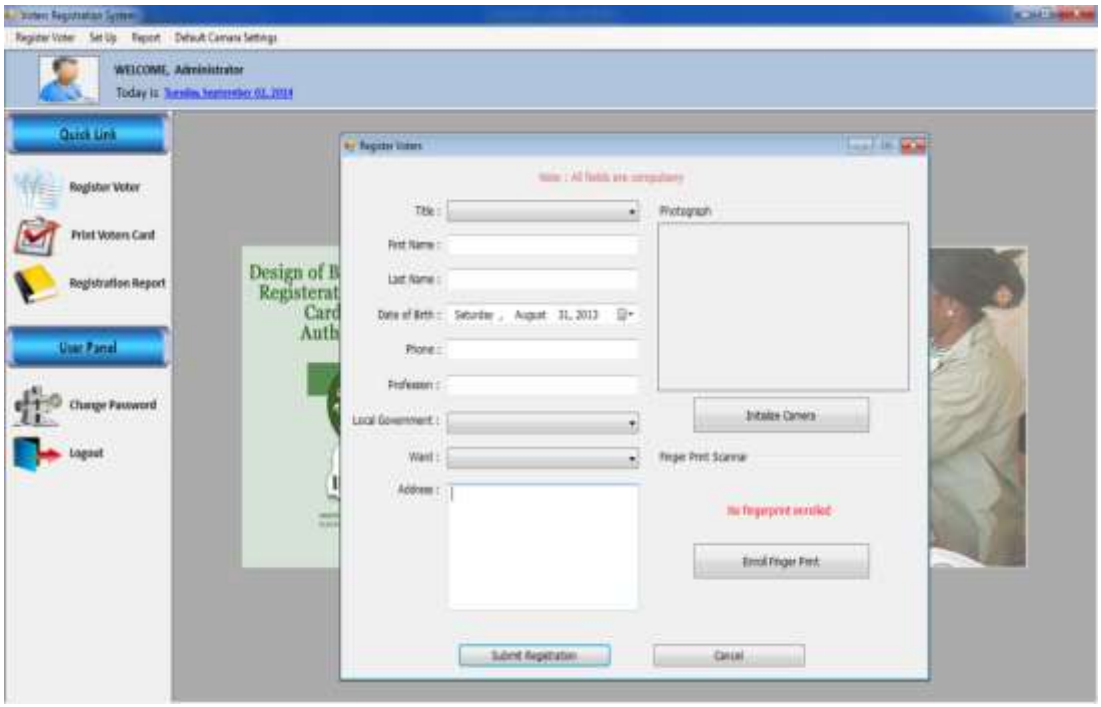

Figure 4: Voter's Registration Screen

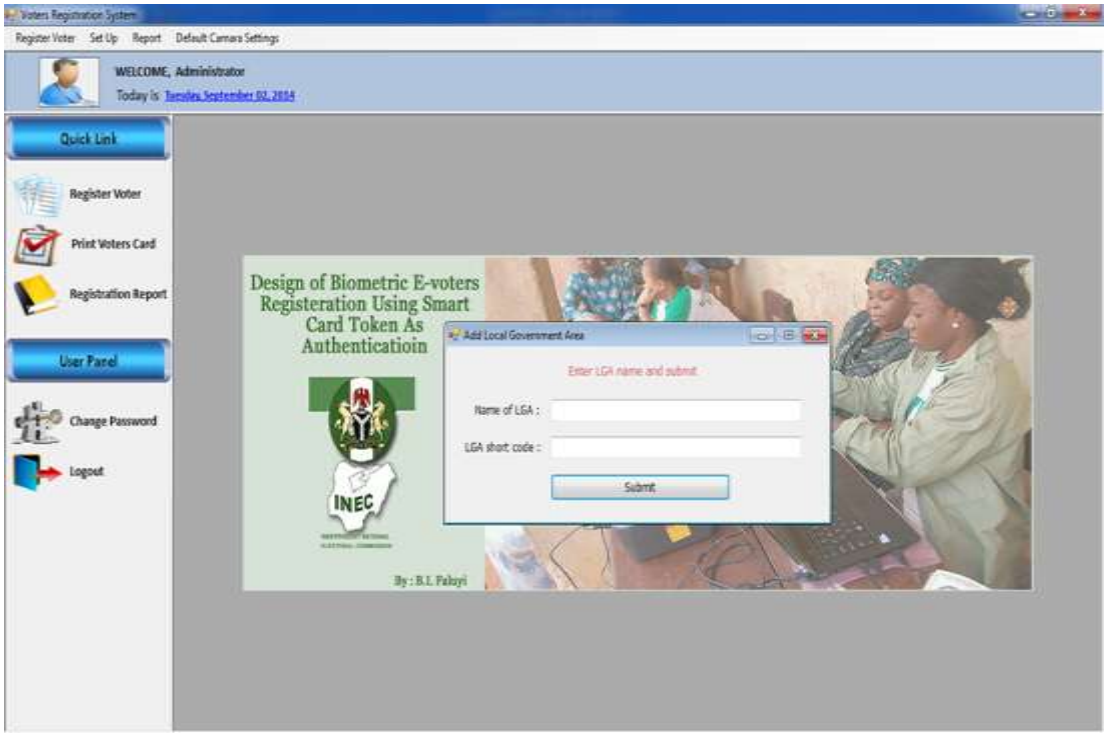

Figure 5: Local Government Setup Screen

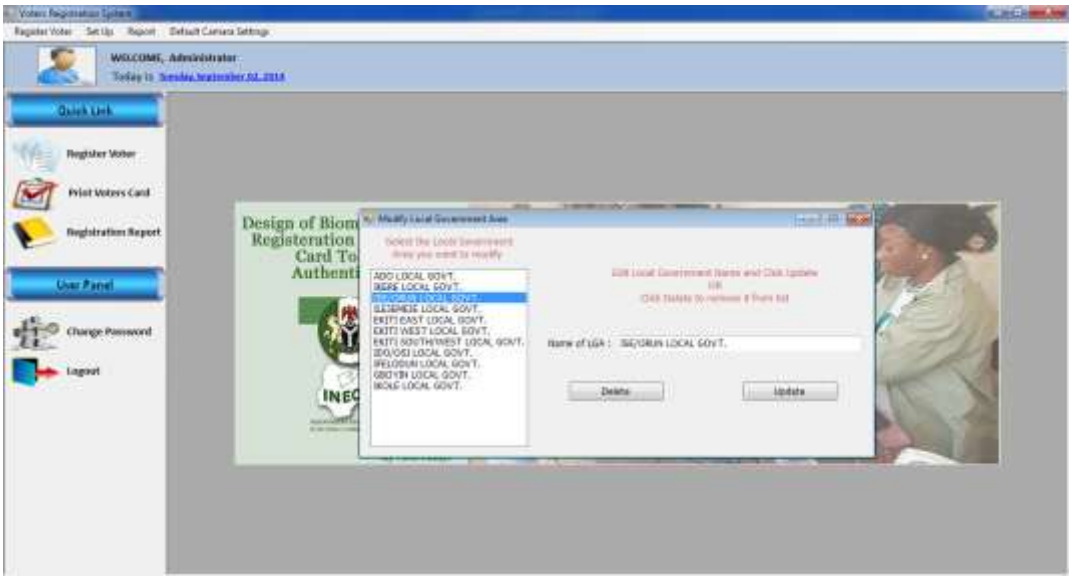

Figure 6: Modify Local Government Area Screen

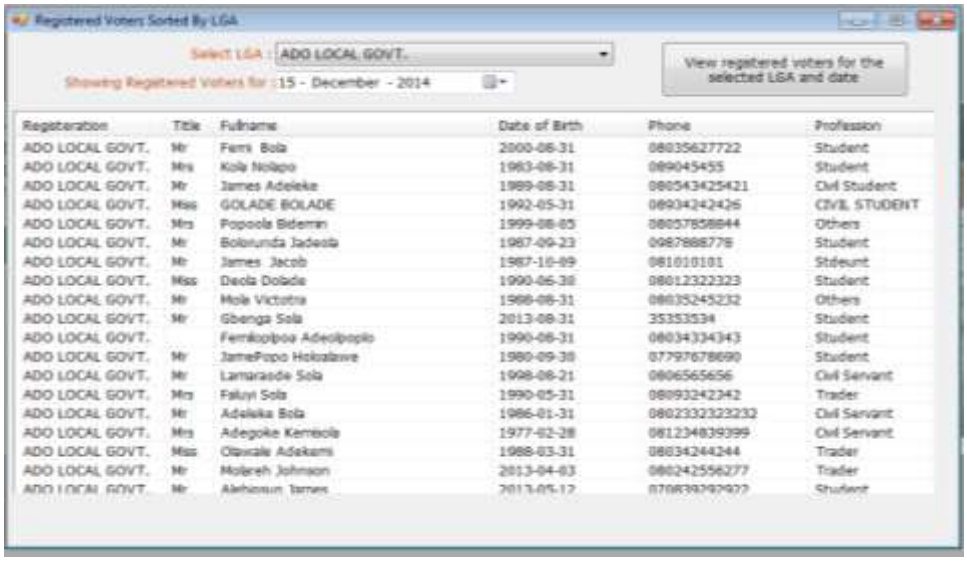

Figure 4.8: Report Generating for Voter Register

9 REFERENCES

- Alese, B.K. and Adetunmbi, A.O. (2011), Nigerian Electronic Voting (e-voting) System: Prospects and Challenges. Proceeding of the Nigeria Computer Society. Pp. 197-208.

- Anderson, R and Kuhn, M. (1996), Tamper Resistance a Cautionary Note. Presented at the Proceedings of the 2nd Conference on Proceedings of the Second USENIX Workshops on Electronic Commerce, Oakland, California, Vol. 2.

- Astrid E. (2010), Voter Registration in Africa: A Comparative Analysis, EISA, South Africa.Pp. 1-2. Brarral, C. (2010), Biometric and Security: Combining Fingerprints Smart Cards and Cryptography. Ph.D Thesis, Swiss Federal Institute of Technology, Switzerland. Pp. 11-14. Available at www.linkedin.com, Accessed on 14th August, 2012.

- Bushager, A.F. (2011), Smart Card Systems: Managing Risks and Modeling Security Protocols Using System C and Transaction Level Modeling., Ph.D Thesis of University of Southampton. Pp. 128-133. Available on www.google.com Accessed on 14th August, 2012.

- Chander, K. (2009), "Efficiency and Security Optimization for Fingerprint Biometric System". Ph.D Thesis, Kurukshetra University, kurukshetra. Pp. 11-22.

- Dhiren, R.P. (2010), Information Security: Theory and Practice, PHI Learning Private Limited, New Delhi, India, pp. 91 -92 Jain, A.K., Bolle, R. and Pankanti, S.(1999), Biometrics: Personal Identification in Networked Society. Kluwer Academic Publishers.

- Kai Xi, Tohari Ahmad, Fenhling Han and Jiankun Hu (20100, A Fingerprint Based Bio-Cryptographic Security Protocol Designed for Client/Server Authentication in Mobile Computing Environment. Security and Communication Networks, Published Online in Wiley Online Library. Wileyonlinelibrary.com

- Kalaichelvi, V. and Chandrasekaran, R.M. (2011), Secured Single Transaction E-voting Protocol: Design and Implementation. European Journal of Scientific Research, Europe, Vol. 51, No. 2, pp. 276-284. Available on www.eurojournals.com

- Masuku, W. K. (2006), An exploratory Study on the planning and design of a future e-voting system for South Africa. M.Admin. Thesis, University of the Western Cape, South Africa. Pp. 14-30.

- Nor, F. B. (2006), Implementation of Fingerprint Biometric Template System in Embedded Software Design. M.Engineering Thesis, University of Technology, Malaysia. Pp. 1-36

- Olabode, O. (2011), Smart Card Identification Management over a Distributed Database Model, Journal of Computer Science, Science Publication, pp. 1770 – 1777.

- Pachghare, V.K. (2010), Cryptography and Information Security. PHI Learning Private Limited, New Delhi, India. Pp. 58 -60.

- Prabhakar, S. (2001), Fingerprint Classification and Matching Using a Filterbank. Ph.D Thesis. Michigan State University. Pp. 33-36. Available on www.google.com

- Ramya, J. (2004), Voter Registration Systems, Project Report of University of Law, Hyderabad. Available on www.google.com

- Sebastien, C. and Herve, S. (2001).How to fit Cryptographic e-voting into Smart Cards. Fundamenta Informaticae, France. Vol. XXI, pp. 1003-1009.'

- Sebastian, F. (2006), Towards Secure Electronic Workflows Example of Applied PKI, Diploma Thesis, Darmstadt University of Technology.

- Sergey T., Faisal F., Praveer M. and Venu G. (2007), Symmetric Hash Functions for Secure Fingerprint Biometric Systems, ScienceDirect of Pattern Recognition Letters 28, New York, pp. 2427 – 2436. Available on www.sciencedirect.com

- Shelfer, K.M. and Procaccino, J.D. (2002), Smart Card Evolution, Communications of the AGM, Vol. 45, pp. 83 – 88. Smart Card Alliance (2002), Smart Cards and Biometric in Privacy-Sensitive Secure Personal Identification System. A Smart Card White Paper, NJ. Pp.1-21. Available on www.smartcardalliance.org