Design of Secure Electronic Voting System Using Multifactor Authentication and Cryptographic Hash Functions

Olayemi Mikail Olaniyi

Department of Computer Engineering
Federal University of Technology Minna, Nigeria
E-mail: mikail.olaniyi {at} futminna.edu.ng,

Oladiran Tayo Arulogun and Elijah Olusayo Omidiora

Department of Computer Science and Engineering
Ladoke Akintola University of Technology, Ogbomoso, Nigeria.

Adeoye Oludotun
Department of Computer Science and Technology
Bells University of Technology, Ota, Nigeria

Abstract **—The primary goal of every voting system is to ensure that electorate vote counts therefore, electronic democratic governance that provides a transparent and trusted election is needed. The traditional method of voting involves the use of physical paper ballot to casts vote. This is susceptible to time wasting procedures, ballot snatching, lacks voter privacy and question the integrity of fair electoral process. This paper describes our attempt to improve the authentication and integrity of evoting system using multifactor authentication and cryptographic hash function methods. Our system meets two of the key security issues in secured e-voting system: The threat of erring voter's authentication and integrity of vote transmitted over insecure wireless medium. The results obtained from the test and evaluation of secured electronic voting system based on this model so far shows an avenue to ensure the integrity of the electoral process and as such, encourages the populace to have trust in the election, through the detection of altered votes in wireless medium and voter authentication through One time Short Message Service (OTSMS) and Grid Card multifactor authentication**.

Keyword: E-voting System, Cryptography, Authentication, Integrity, Grid Card

I. INTRODUCTION

Democratic governance is based on elections which allow the populace to choose their representatives and express their preferences for tenure based leadership. Naturally, the integrity of the election process is fundamental to the integrity of democracy [10]. The election system must be sufficiently robust to withstand a variety of fraudulent behaviors and must be sufficiently transparent such that voters and candidates can accept the results of an election [1].

In traditional voting system, the primary means of voting embraces physical balloting of voters' intent. The paper ballots are read and interpreted. The results of each candidate are individually tabulated and displayed. The physical presence of the voter is required where by the thumbprint of individual registered voter is used to vote. Although, the design of a voting system whether electronic, paper ballots or mechanical devices must satisfy a number of competing criteria [7, 1]. These criteria are the anonymity and tamper resistance of a voter's ballot, both to guarantee the voters' 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 [1]. The voting system must also be tamper-resistant to avoid a wide range of attacks, including ballot stuffing by voters and incorrect tallying by insiders [1].

The conventional system of voting is characterized with high rate of fraudulent practices ranging from stolen of ballots, falsification of vote counts or rigging, improper voting and votes lost through invalid ballot marks due to ignorance and inadequate prior awareness and negligence [10]. This voting system is insecure and has been characterized with suits of election malpractices. The most fundamental problem is that the entire election hinges on the correctness, robustness, and security of the software within the voting terminal. With this, due to the high rate of election malpractices, secure electronic voting system is proposed based on multifactor authentication of voters and cryptographic hashed electronic vote.

The current single factor authentication technique embraced in electoral process of most developing countries is not very secure to protect users from identity theft. Single factor authentication increases risks posed by phishing, identify theft, online fraud and loss of confidence on democratic decision making process. So, voting systems need to implement an effective multifactor authentication system to reduce fraud and make elections fair, free and credible.

E-voting refers to an election or referendum that involves the use of electronic means in at least the casting of the vote [7]. Once recorded, the elector's vote is dispatched in real time to a secure electronic vote store, where it is held prior to counting. The presence of electronic voting system to voting

brings a lot of security measures into the voting system, thus, eradicating issues such as stolen of ballots, falsification of vote counts or rigging, improper voting and vote lost through invalid ballot marks due to ignorance and inadequate prior awareness and negligence, allocation of vote counts and other theft activities related to the traditional voting system [9, 10, 13]. Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. In an attempt to achieve security measures in e-voting system, major security features to fulfill are Confidentiality, Integrity, Non-repudiation and Authentication [2, 11].

Voting is a vital part of the democratic process. As such, the efficiency, reliability, and security of the technologies involved are critical. In this paper, we present the design and development of a multifaceted cryptographic model for a secured electronic voting system in e-democratic engendered countries where emphasis is placed on conducting transparent, fair and trusted elections. The designed system is practically aimed at securing electronic voting system by ensuring authentication and integrity in transmission of data flows in the network.

II RELATED WORK

Various works in literatures exist in the area of secure electronic voting system for democratic governance. In [3], the author specified mainly on securing the voting system, by comparing the insecurities that exist in the manual voting system to that of the electronic voting system. Authors in [4] suggested the use of Remote Internet Voting, with a view to enhance voter convenience, increase voter confidence and voter turnout. In the survey, authors suggested remote poll-site electronic voting as the best step forward as it provides better voter convenience, but at the same time, does not compromise security. In [5], the author review the security measures needed for remote online voting system by focusing on two cases where voters cast their ballots over the Internet – the 2000 Arizona Democratic Primary and the University of Virginia Student Council Elections. The author claims that a secure voting system must thoroughly satisfy four major requirements: authentication, availability, confidentiality and integrity. In [6], the author reviewed e-voting procedure by describing its advantages and disadvantages. His work majored were on the security measures such as firewalls or SSL communications which are necessary but not sufficient to guarantee the specific security requirements of e-voting. Also, the author describes the additional layer of specialized security technology to address the specific risks posed by electronic voting and guarantee critical security requirements such as voters' privacy, vote integrity and voter-verifiability. The author equally suggested the use of Biometrics and smartcard for authenticating users.

One major issue the author stressed out is the difference between biometric authentications compared to "classic" authentication like smart cards. The e-voting system proposed in [6] does not interact in any way with the biometric characteristics of the actual users, but still authenticates the user with the help of the user's authentication certificate on the smart card.

In [7], authors lay emphasis on the rapid advancement in Information and communications technologies which has given rise to new applications that were impossible just few years ago. This paper details the requirements, design and implementation of a generic and secure electronic voting system where voters can cast their votes anytime, anywhere and using a number of electronic devices including private computer networks, web and mobile phones. Authors in [7] also compared both the manual voting system with electronic voting system and evaluate the flaws of manual voting system in relation to how the electronic voting system can improve the flaws. Further work was reviewed by the author in a bid to make and electronic voting system work on various platforms.

In [8], the author specified on the authentication methodology in securing transaction, through the use of multilayered encryption algorithms. The author laid emphasis on the use of multifactor authentication method, which includes both the mobile station authentication and the financial institution authentication.

In [1], the author describes the security features of the electronic voting system and e-voting system is better than manual voting system. Also, the author shows that voters, without any insider privileges, voter can cast unlimited votes without being detected by any mechanisms within the voting terminal software. Also in [13], authors presented the design and development of real time of an electronic-voting system with emphasis on security and result veracity for increase in the efficiency in electoral process and compensate for challenges in manual voting in a multi-ethnic and diverse climate like Nigeria. In this paper we present the design and development of a multifaceted cryptographic model for a secured electronic voting system in e-democratic engendered countries where emphasis is placed on conducting transparent, fair and trusted elections.

III SYSTEM DESIGN

The purpose of system design is to create a technical solution that satisfies the functional requirements for the system. The functional specification produced during system requirements analysis is transformed into a physical architecture through system modeling and database design.

A. Requirements Definition for the Secure E-voting System

According to the literature, the design of any voting system must satisfy a number of competing criteria [3, 6, 7, and 12]. These requirements give an avenue for a free, fair, credible and confidential election. These requirements by [7] are

grouped into generic and system specific; by [12] as functional and non-functional requirements. Considering e-voting from functional and non-functional point of view, the following requirements are necessary:

i. ***Confidentiality***: Ensuring that no one can read the message except the intended receiver.
ii. ***Non-repudiation***: A mechanism to prove that the sender really sent this message.
iii. ***Authentication***: Only the eligible and authorized voters can vote through the system.
iv. ***Accuracy***: Every voted ballot should be correctly counted into the final tally within the tolerable extent of error.
v. ***Integrity***: Votes should not be able to be modified, forged or deleted without detection
vi. ***Secrecy and Non-Coercion***: Only voters know what they vote for. Voters must not be able to prove what they vote for in order to reduce the risk of coercion and vote-buying activity.
vii. ***Audit trail***: The system should provide the mechanism for audit trail. Audit trail can help to verify that the votes are accounted correctly in the tally and maintain the security for the system.
viii. ***Uniqueness***: Every voter has the same number of the votes. No one can vote more times than others.
ix. ***Transparency***: The election process should be transparent to the voters. Voters can clearly understand the mechanism of the electronic voting system and know whether their votes have been correctly counted.
x. ***Simplicity***: The system should be designed user friendly. It should also meet the need of the disabled and illiterate.
xi. ***Democracy:*** Permits only eligible voters to vote only once.
xii. ***Privacy***: All votes remain secret while voting takes place and each individual vote cannot be linked by any individual to the voter who casts it. The privacy issue is paramount.
xiii. ***Accuracy***: The voting result accurately reflects voters' choices. In this case, no vote can be altered, duplicated or eliminated without being detected.
xiv. ***Fairness***: No partial result is available before the final result comes out.
xv. ***Security***: Votes should not be manipulated during the whole process of voting.
xvi. ***Verifiability:*** Voting systems should be verified so as to have confidence that they meet necessary criteria.

B. Architecture of Secured Model for E-Voting System

The electronic voting system was designed to enable the overall populace to vote over wireless medium, and the system is opened to the voter and the administrator. The primary aim of the design is to provide a secured system over wired and wireless connection. The design architecture follows conceptual perspective of the three layered Organization for the advancement of Structured Information Standards (OASIS): the pre-election phase, election phase and the post-election phase shown in Figure 1.

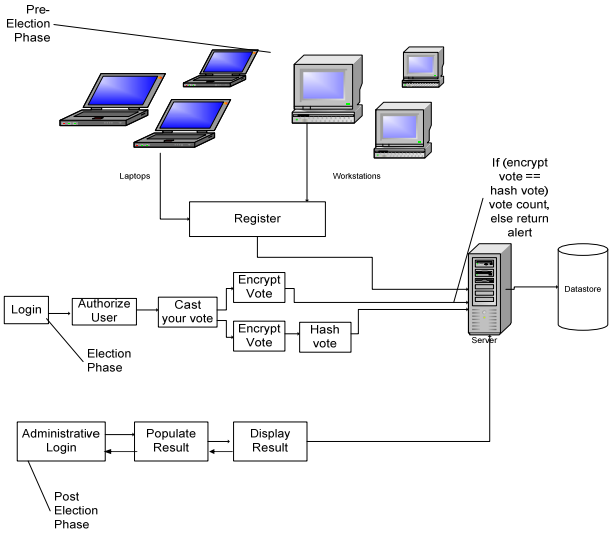

Figure 1: System Architecture of the Secured Voting System

The pre-election phase provides an aspiring voter a phase to register his/her identity into the system. The process involved includes providing input access for qualified voter, and thereafter, the system automatically generates a unique id, unique grid card that matched directly with the unique id generated by the system, and then a unique short message service (SMS) one time pin is also generated by the system. This generated on time random array of pin is then automatically sent to the aspiring voter in a form of Short Message Service (SMS) to the user if he/she meets the requirement to vote. The pre-election has several operations involved in it. The first operation involves the registration phase, whereby each aspiring client registers his/her profile. During registration, some fields such as phone number and email address would be made mandatory for clients to fill data in. After registration, a soft random grid card code is generated by the system for each user. Also, an SMS containing random array of America Standard Code for Information Interchange (ASCII) would be sent to the registered clients' phone number. All details pertaining to registration is stored in the database.
The election phase involves voting, the voter uses the randomly generated SMS pin, and then the grid card code, to vote, coupled with his/her registered number (unique id). The vote when casted is encoded with a private key. The encoded result is divided into two parts. One part of the encoded result is further hashed using the SHA256 (secured hash function) and a 256 bit of random number is generated. The first encoded result and the hashed function is then sent to the database to be processed at the post-election phase. Figure 2 and Figure 3 shows the diagrammatic flow of these vote integrity check of the election phase.

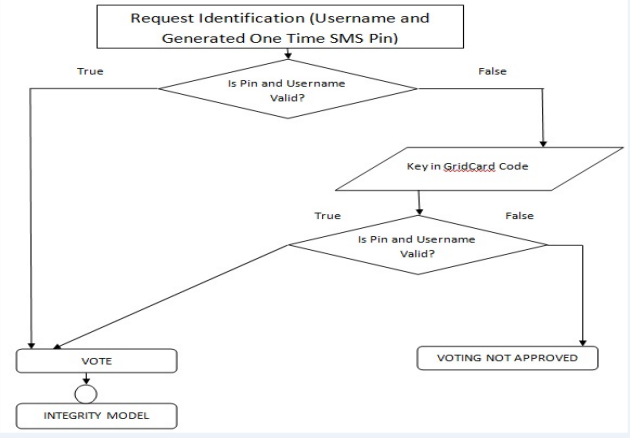

Figure 2: Secure E-voting Election Phase for voter's authentication Check

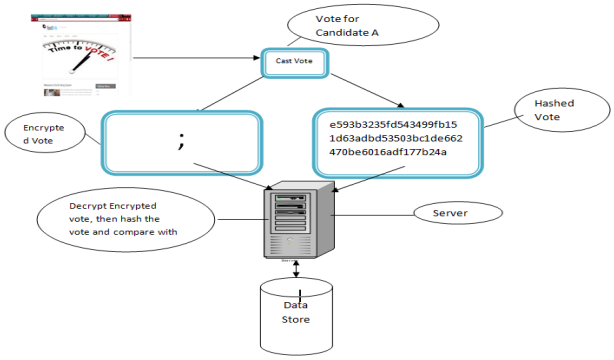

Figure 3: Secure E-voting Election Phase for voter's Integrity Check

The post-election phase verifies each voter's vote to ensure vote is not altered while in transit. The process involves comparing the result of each unique identity by comparing the encrypted vote to the hashed vote. The encrypted vote is decrypted and then hashed using sha256. If the hashed result matches with the hashed function sent during voting phase, the system would automatically update the user's vote by one, else, the vote would be regarded as to have been hacked while in transit, hence, vote would not be counted for the voter. Figure 4 shows the system flowchart of the integrity check mechanism from overall system architecture shown in Figure 1

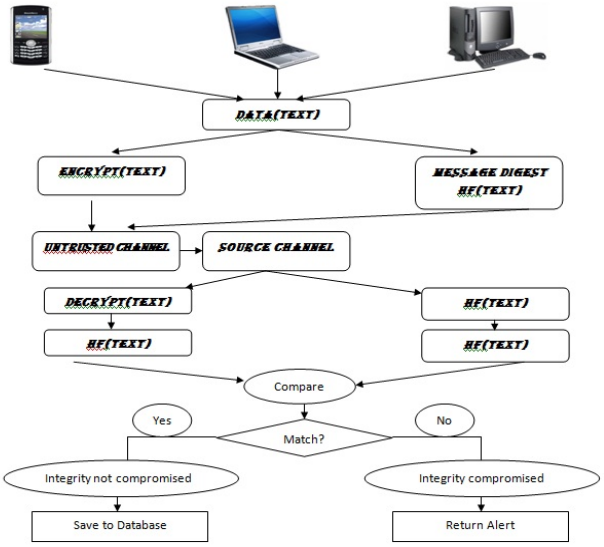

Figure 4: Flowchart of System architecture

C. *Model Definition*

By definition, cryptographic hash functions provides assurance of data integrity with notion of implantation on fingerprint of source data, an alteration in transit of which the integrity of data cannot longer be guaranteed. Let h be a hash function of x data, then the corresponding fingerprint or message digest is defined as:

$$y = h\,(x) \qquad (1)$$

If y is stored in secure place (e.g. image or video media) then

$$k = y \qquad (2)$$

If the source data, x, is change in transit to x', then the corresponding message digest or fingerprint from equation 3.1 change from y= y' as:

$$y' = h(x') \qquad (3)$$

If data in transit has been altered by comparing equation 3.1 and 3.3, then it can be inferred that

$$y \neq y' \qquad (4)$$

verifying that integrity of data has been compromised. The algorithm for verifying vote integrity was designed around SHA (256) as follows:

Start:
Vote1 = sha256 (vote)
Vote2 = encrypt (vote)
Vote3 = sha256 (decrypt (vote2))
Compare vote1 with vote3
If vote1 equals vote3, populate database
Else return alert
Stop

Based on enhanced secure hash algorithm, message encoding and decoding algorithm below:

```
Start
AdvancedSha (String hash)
Let j, sum = 0
Let cc = empty character
While i <hash.length
 cc = hash.character(i)
 j = (AsciiFunctionOf(cc))
 sum = sum + j
        i = i + 1
end while loop
Output:
New hash = sha256function (sum)
```

```
Start
Let len = 100, key = 8
Encmsg ,decmsg = emptyString
Processes:
 getEncode(String msg)
 let i = 0;
          while i <msg.length
encmsg = encmsg + msg.charactAt(i) ^ key
          i = i + 1
          end while
 getDecode(String msg)
end
```

D. System Modeling

Using Unified Modeling Language (UML) standard, the secured e-voting system was visualized along the following use case, class, sequence, and activity diagrams. The functionality anticipated by the secured e-voting system in terms of actors, their goals represented as use cases and available dependencies is shown in Figure 5.

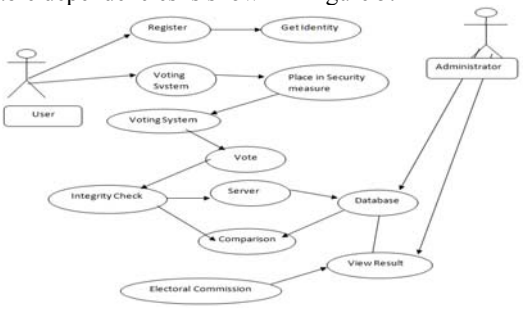

Figure 5: Secure E-voting System Use-case Diagram

The type of objects used in the system and their static relationships is shown in the class diagram shown in Figure 6. Figure 6 represents how each function of an object interact, type of relationship that exist between various actors and their functions, and the operation each actor can perform.

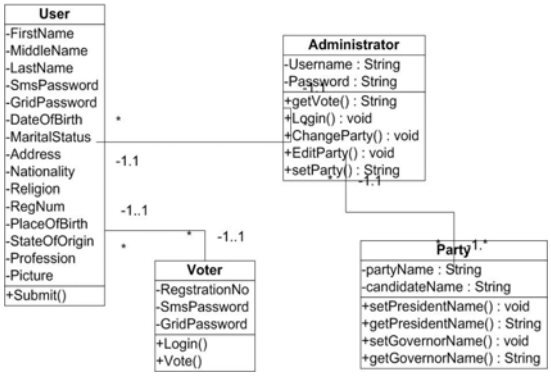

Figure 6: Secure E-voting System Class Diagram

IV SYSTEM IMPLEMENTATION

The hypertext processor embedded in HTML was used for the preliminary implementation of electronic web and mobile platform. The secured E-Voting system consists of two main users: the user of the system, and the administration. The administrator is the person that oversees the overall operation that takes place in the voting system. The administrative user has the right to view votes in the records, check for registered candidates, edit registered user's information, resend user's one time SMS (short message service) password, set candidates to be voted for, both in the gubernatorial and presidential election. Furthermore, the administrator has the right to disqualify a user from voting, if the registered user is not eligible to vote.

A. Homepage

This is the first page on the E-Voting system, which welcomes each user to the page. It consists of links that link each user to all other pages in the system. The home page consists of information about electronic voting system as well. Figure 7 shows a designed system on personal computer.

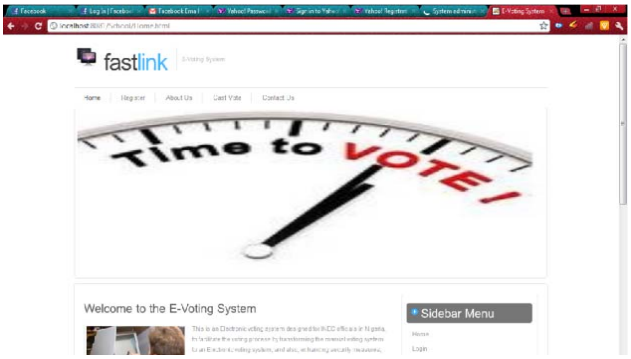

Figure 7: Home page on PC (Personal Computer)

The implementation of the homepage designed on mobile platform is shown in figure 8.

Figure 8: Home Page (on mobile phone)

B. Registration Page

The registration page shows the page where prospective voter can register into the system. The system is designed to accept input from the user, and some texts are made mandatory for user to fill in details. It basically contains First name, Middle name, Last Name, Address, Email, Zip Code, Phone number, Postal Address, Email, Date of Birth, Religion, Gender and Marital Status. Figure 9 provides a pictorial representation of the design.

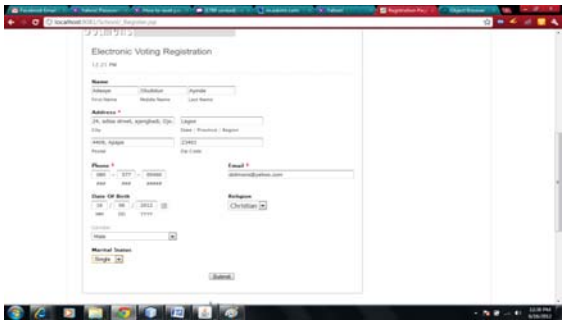

Figure 9: Registration Phase on PC

The implementation of the design on other cross platform is shown in figure 10:

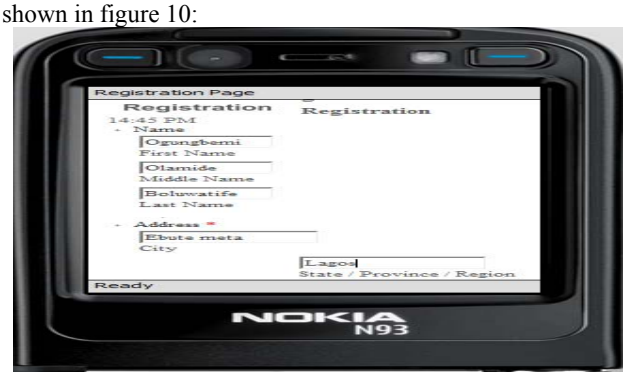

Figure 10: Registration Phase on mobile phone

C. Registered Voter's Page

The next phase shows the registered voter's page, the page that provides the registered user with a unique grid card number. Also, the user is requested to print the page for safety, and an SMS is sent from the server end to the registered candidate. Figure 11 and Figure 12 show the description of a registered voter both on PC and mobile platform while Figure 13 shows SMS sent to a registered client which contains random sets of character that is uniquely associated to the registered clients' registration ID.

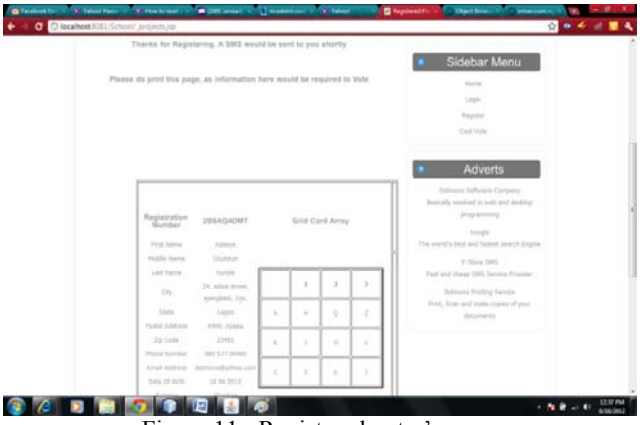

Figure 11: Registered voter's page

The implementation of the design on other cross platform is shown in figure 12

Figure 12: Registered voters page on mobile phone

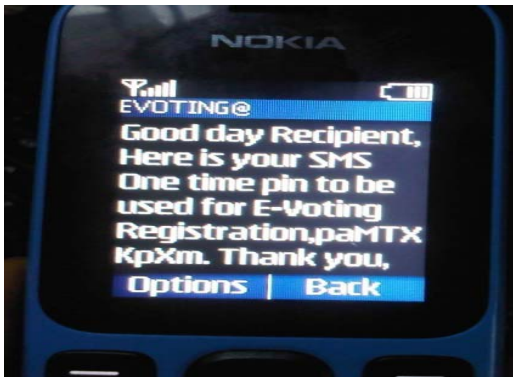

Figure 13: Registered voters SMS One Time Pin

D. Login Page

The login page provides registered user with the option of logging in to the secured e-voting system, by supplying a unique registration number of a user, the SMS password that was sent to a user, and a grid card pass code. The grid card pass code consists of random array of values, i.e., the requirement needed at every instance of a new page alters automatically.

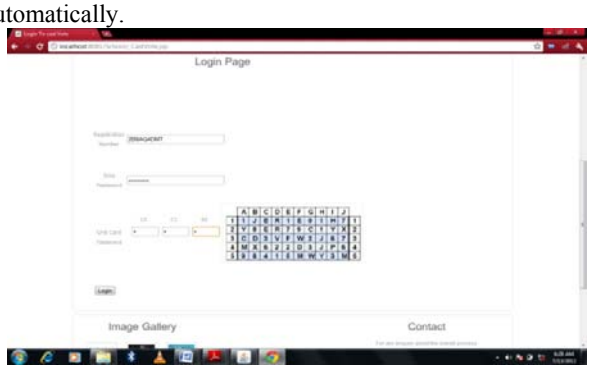

Figure 14: Login Page

The implementation of the design on other cross mobile platform is shown in figure 15

Figure 15: Login Page (On mobile phone)

E. Presidential Page

Presidential page provides users with the option of selecting just a candidate to be voted for. In this, it consists of the presidential logo, the picture of the candidates and the name of the candidates. In figure 16 just a candidate can be voted for.

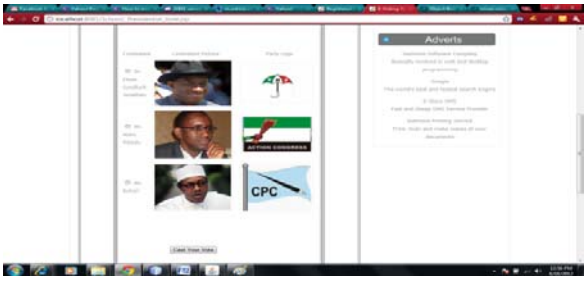

Figure 16: Presidential Voting Page

F. Governorship Page

Governorship page provides a voter with the option of voting for just one out of the available contestants. This consists of the Governorship logo, the picture of the candidates and the name of the candidates in Figure 17.

Figure 17: Governorship Voting Page

V SYSTEM EVALUATION

The system was evaluated through comparison of hashed vote (message digest) with encrypted vote. Figure 18 displays table that represent presidential vote, having column named as Reg_Id, Encrypt_Vote, Sha_Vote, Sms_Onetime and ID. Reg_Id denotes each unique registration number of every user, whereas the Encrypt_Vote represents the casted vote in an encrypted format. The Sha_Vote represents the hashed function of encrypted vote, sms-one-time denotes that vote has not populated by the server. Figure 18 also shows the general table of a presidential vote, and the values that are sent to the database in the server whenever a vote is made.

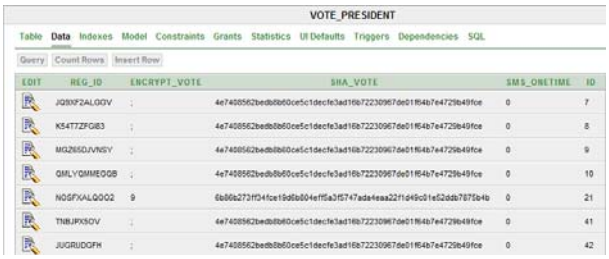

Figure 18: Database for Presidential vote

In Figure 18, it shows that the character ';' is equal to '4e7408562bedb8b60ce5c1decfe3ad16b72230967de01f64b7e4729b49fce', therefore, to evaluate this system, the server compares the value of encrypted_vote to sha_Vote. If the character in encrypted ***Vote does not correspond to*** sha_vote, such registration_id is populated into the hackedvote, based on the definition in equation 4 i.e., then such vote has been hacked during transmission, thus such vote is added to vote in the ignored, However, if the character ***in encrypted Vote does correspond to sha_vote***, such registration_id is populated into the database, Figure 19 shows a table representing hacked vote and figure 20 shows the total result of presidential vote.

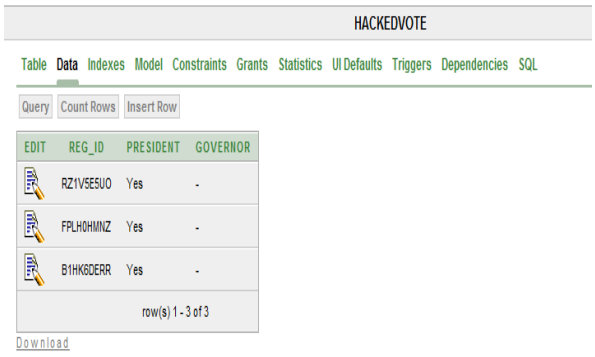

Figure 19: Database for Hacked Votes

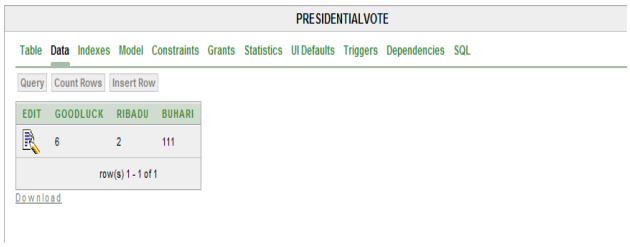

Figure 20: Database for Presidential Votes

VI CONCLUSION AND RECOMMENDATION FOR FUTURE WORK

The developed secured electronic voting system has been tested and implemented on different electronic platforms which include personal computer, tablets and mobile phones. The electronic voting system automates the manual voting system by providing a platform in which users can vote using devices that are connected together in a network environment. Also, the issue of security was implemented by enforcing both integrity measure and authentication measure of the electronic voting system. The result of voted candidates and how integrity check is achieved on each user's vote has been presented in this work.

In future, it is recommended that further works should consider the following factors in order to ensure full secured electronic voting system, and which would serve as a basis for an implementation of trusted e-governance through secured e-voting system.

i. Include biometric system to capture the real identity of voter.
ii. Extend to other security requirements of electronic voting system such as non-repudiation, privacy and confidentiality.

REFERENCES

[1] Kohno T., Stubblefield A., Rubin A. and Wallach D. S, (2004), "Analysis of an Electronic Voting System", In Proceedings of IEEE Symposium on Security and Privacy 2004, pp. 1-23.

[2] Abo-Rizka M and Ghounam H.R (2007), "A Novel E-voting in Egypt", International Journal of Computer Science and Network Security" ,Vol.7,No.11,pp 226-234.

[3] Manish K, Suresh K.T, Hanumanthappa. M, Evangelin G.D (2005), "Secure Mobile Based Voting System", Retrieved online at http:// www.iceg.net/2008/books/2/35_324_350.pdf on November 17th 2012.

[4] Rossler T.G (2011),"E-voting: A survey and Introduction ", Available at http://wiki.agoraciudadana.org/images/5/56/An%2BIntroduction%2Bto%2BElectronic%2BVoting%2BSchemes.pdf Retrieved on 15th June 2012.

[5] Avi Rubin (2001),"Security Considerations for Remote Electronic Voting over the Internet", AT&T Labs – Research Florham Park, NJ. Available at http://avirubin.com/e-voting.security.html, (date accessed 7th July, 2012).

[6] Ciprian Stănică-Ezeanu (2008), "e-Voting Security", Buletinul Universităţii Petrol – Gaze din Ploieşti, Vol. LX (2), pp 93-97

[7] Okediran O. O., Omidiora E. O. Olabiyisi S. O., Ganiyu R. A. and Alo O. O. (2011)," A Framework for a Multifaceted Electronic Voting System" , International Journal of Applied Science and Technology Vol. 1(4), pp 135 – 142.

[8] Akinmosin D., Egbedokun G.G.O. and Ibitowa F.O (2011),"An Extended Multifactor Authentication in Mobile Financial Transaction Using User Authentication Module with Multilayered Encryption Algorithms", African Journal of Computer and

Information Communication Technology, ICT (Journal of IEEE Nigeria Computer Section),Vol. 4 (2), pp 17-24.

[9] Olaniyi, O.M, Adewumi D.O, Oluwatosin E.A, Arulogun, O. T and Bashorun M.A(2011), "Framework for Multilingual Mobile E-Voting Service Infrastructure for Democratic Governance ", African Journal of Computing and ICT (Journal of IEEE Nigeria Computer Section),Vol 4, (3), pp 23 – 32.

[10] Olaniyi, O.M, O.T Arulogun, E.O, Omidiora, A Omotoso, Ogungbemi O.B. **(**2012), " Design of A Secured Model For Electronic Voting System Using Stegano-Cryptographic Approach ", Proceedings of the 7th International Conference on ICT Applications, Application of ICT to Teaching, Research, and Administration (AICTTRA 2012), National Defense College Abuja, pp 84-89.

[11] Ibrahim S, Kamat M, Salleh M, and Abdul Aziz S (2003), "Secure voting using blind signature *".Available at URL http://eprints.utm.my/3262/1/IEEE02-EVS_full_paper_ver14Nov.pdf* Retrieved on November17th 2012

[12]NSF (2001)," Report on the National Workshop on Internet Voting: Issues and Research Agenda" , National Science Foundation, Retrieved at http://news.findlaw.com/cnn/docs/voting/nsfe-voterprt.pdf.

[13] Abdulhamid S M , O.S. Adebayo, D. O,Ugiomoh,M.D AbdulMalik (2013),"The Design and Development of Real Time E-Voting System In Nigeria with Emphasis on Security and Result Veracity ", International Journal of Computer Network and Information Security",Vol.5,pp 9-18,Retrieved Online at http://www.mecs-press.org/ijcnis/ijcnis-v5-n5/IJCNIS-V5-N5-2.pdf on 7th August 2013.