International Conference on Information and Communication Technology and Its Applications (ICTA) 2016
Federal University of Technology, Minna, Nigeria
November 28 – 30, 2016

A framework for Pre and Post Vote Cast Audit to Enhanced Electronic Voting Systems' Credibility (PsVCF)

Enesi Femi Aminu[1], Aliyu Abdulmalik[2], Hussaini Abubakar Zubairu[3]
[1,2]Department of Computer Science, [3]Department of Information & Media Technology
[1,2,3]Federal University of Technology, Minna
Minna, Nigeria
{[1]enesifa, [3]abu.zubairu} @futminna.edu.ng, [2]aliyuabdulmalik57@yahoo.com,

***Abstract*— A citizen of any democratically practiced nation under the permitted age reserves the legitimate right to vote and be voted for. This right is so powerful which needs to be guided diligently. Because the functions of this right when carefully used can yield national developments and growths in all sense of live. In order to guide this right from all possible human interference and manipulations thus; the introduction of electronic voting machines (eVotingMachines). However, it is ascertain that this has not yet yield the expected results. Because Information Technology (IT) experts, particularly software designers and engineers are alleged to manipulate the system (program) to favor their prefer candidate(s). It is in the light of this that this paper proposes a pre and post vote cast audit framework for electronic voting machines such that every voter can audit the system before and after voting. This will ensure real free and fair vote cast, authentication of vote casted and true results of vote casted. Ultimately, reduces to zero any acts of suspicious and malpractices.**

***Keywords- eVotingMachines; pre-vote cast; post-vote cast; audit; credibility; benefitted contestant; party; system*.**

I. INTRODUCTION

It is a known fact that the words "democracy and election" are intervolving. Democracy, a type of government in which the utmost power is confined to the people which can be directly applied by them or by their designated representatives under a free electoral system. While, election on the other hand is a process in which voters select their representatives and express their preferences for the way that they will be governed [1]. Poor electoral system is a major cause of unhealthy political competition among power contenders and consequently leads to electoral violence. It is ascertain that one of the prime causes of political struggle amid power contestants and eventually leads to electoral hostility is poor electoral system [2].

In any democratic settings; qualified citizens or registered voters are expected to guide and respect their voting right because it is their desire for such right to be given to their intended party or candidate. It is important to note that if the platform designed or adopted to cast and count vote lacks credibility, unarguably; that will call for so many questions and presumptions [3]. It is assumed that there individuals who are unscrupulous that can compromise the system for some gains. Most a time; these set of people are highly proficient in Information Technology (IT) knowledge.

Election conducts in Nigeria for instance, is attributed with a huge number of issues and challenges [4]; common among the problems include prolonged legal tussle, missing names of some registered voters, intimidation and disfranchisement of voters, multiple and under aged voting, snatching or destruction of ballot boxes, miscomputation and falsification of results [2]. As a result of poor electoral system in most developing nations, the sizes of electoral mayhem is seriously on the increase, and the political elites have taken the advantages of this worrisome situation to engage uninformed and poverty ridden youths to indulge in various electoral violence [5]. In addition, it is also asserted that in [6] the syndrome of godfatherism and godson also forms a factor to electoral violence exploiting the weaknesses of the traditional voting system. The collective effect of the electoral abnormalities are but not limited to misuse of incumbency power, lack of lucidity and stern flawed voter lists; actual or perceived bias of election officials resulting to real or perceived fraud stimulate election related violence with far reaching consequence of eroding peoples' faith and confidence in democratic process [7]. Therefore, it is also the view of [8] that if the voting mechanism and systems are well managed (just as proposed in this paper); it will guarantee good governance based on rule of law, transparency, and accountability. The remaining sections of this paper are thus organized as follow. Section II captures the account of some related literatures (studies) of the proposed work; Section III depicts the architectural framework of the proposed pre and post vote cast audit which form the pivot of this paper; Section IV implores some data modeling approaches to further gives a pictorial details of the proposed framework and Section V concluded the work and it recommendations.

II. RELATED STUDIES

The research work carried out by [9], pointed out verifiability, fairness, eligibility, privacy, among others as salient characteristics of electronic voting systems. The authors aimed to develop an electronic voting system that suite these characteristics of electronic voting process. The system included voting, counting, result announcement among others. However, at

the counting stage; the voter has no idea if the vote cast is actually benefited by the targeted contestant or party. The final results would only be announced by the counter when the election period of time is over at the result announcement stage. We argued that suspected system's manipulations could still be carried out by unethical IT experts.

In the course of this research, a good number of works have been carried out on enhancing electronic voting systems; particularly on security - mainly introduction of biometric for voter's authentication. This fact was buttress in the work of [10]. However, little or no attention is given to intended vote cast credibility.

Bringing security and authentication like biometric based computer network into electronic voting machines was the survey work carried by [11]. The researchers emphasis the significance of Biometric techniques in electronic voting machines. In their work, they finally propose a biometric-based design that protects transparency, secrecy, and anonymity as well as other important services. Three different types of authentications in security related were discussed in their work. They are as follows: "something we know"; this simply mean some sort of personal information. For example, Personal Identification Number (PIN), password (short or long), the second type is "something we have"; the researchers described this type in form of physical objects for example, token and smart cards and lastly, "something we are", a typical example is biometric. This third type of authentication brings us to the security measure we adopted in the research work. The term biometric (fingerprint, iris, face and other passive traits); describe the science of measurement of creatures [12].

In the research work of [13], they provided security to electronic voting system through the means of visual cryptography and homomorphic encryption that protect user authentication by adopting shared construction algorithm. Thus, in summary of their work; a voter is authenticated before voting take place. The adoption of biometric system of security in this proposed research is further strengthen by the authors as stated in their work under review that the likelihood of two or more users not possessing the same identification features in the biometric system is clearly not daisy. However, auditing process and technique as propose in this paper was not included in their work.

In the proposed system of [14] the work depicts how mobile phones that are android based are proficient in voting system. The system supported concurrent voting as a result of distributed nature of the database. In summary, the researchers claimed that the proposed new e-voting system ensures voter privacy and voting correctness, hence providing a key mechanism that based on distinctive identification number. However, economy and illiteracy factors among others in developing nations were not taken into consideration. Besides, android – an open source platform can easily be manipulated by software engineers to satisfy their negative motives; thereby poses credibility issue to electronic voting system.

Furthermore, [15] developed a real-time e-voting system in Nigeria with emphasis on security and result veracity. Considering the methodology in which the system is implemented which were divided into five main modules for instance; in the voting module, a voter is expected to register and a password is thereby sent to his mail. By implication, such voter is expected to have an existing mail account and cost of accessing his mail before a vote is casted must be incurred. Considering the low level of literacy and the negative outlook of economy in this part of the world, such system would by extension discourage and disfranchise so many eligible voters. However, in the proposed framework; fingerprint biometric as a means of security is required for voter to register and proceed to execute the vote cast activities. Thereby eliminates the cost of signing-in and accessing email account. Besides, avoid any form of account hijack by third party. Also, the issue of disenfranchisement of eligible voters who are illiterates is completely avoided using the proposed method of security.

A paper titled "A Simplified Electronic Voting Machine System" by [16] proposed a transparent operation on the system by using unique information and produces the results of aggregate casted votes for the contestants.

The greatest danger to e-voting system is that interference on program of the systems can go undetected affecting the results of the voting, then an independent and extensive security monitoring, auditing, cross checking and reporting needs to be a critical part of e-voting system [17].

The work of [18] equally stated that as a result of lack of transparency, the use of electronic voting system in some nations who have adopted its usage had equally generated a lot of controversies. The researchers further pointed out that few years ago; there was an argument that the trustworthiness of the system may be achieved by the use of backup paper trails. And in contrast; they argued that the paper trails would not provide the adequate measures but the transparency of the machine could be restore by adopting sufficient security measures. They concluded that when technology is inaccurately and hastily applied to election, it can inadvertently give room to so many electoral challenges and thereby lowering the electorate confidence in the exercise. Therefore, the issue is not just adopting electronic voting system in countries like Nigeria but enhancing the system for electoral confidentiality and credibility is the utmost concern; which is what this proposed work is sought to address.

The need for the proposed framework is justified reviewing the work of [19]; where some nefarious actions that could be carried out by different categories of people. Among these is where votes could be illegitimately created, deleted or modified by voting device or operating system developers, internet provider or poll worker (with access to network traffic or storage media). Table 1 shown the summarized list of these nefarious actions (attacks) by researchers who done the analysis of Diebold voting system.

TABLE I. ATTACKS ON THE SYSTEM [19]

	Voter (with forged smartcard)	Poll Worker (with access to storage media)	Poll Worker (with access to network traffic)	Internet Provider (with access to network traffic)	OS Developer	Voting Device Developer
Vote multiple times using forged smartcard	•	•	•			
Access administrative functions or close polling station	•	•			•	•
Modify system configuration		•			•	•
Modify ballot definition (e.g., party affiliation)		•	•	•	•	•
Cause votes to be miscounted by tampering with configuration		•	•	•	•	•
Impersonate legitimate voting machine to tallying authority		•	•	•	•	•
Create, delete, and modify votes		•	•	•	•	•
Link voters with their votes		•	•	•	•	•
Tamper with audit logs		•			•	•
Delay the start of an election		•	•	•	•	•
Insert backdoors into code					•	•

Other types of attacks discussed were insertion of backdoors into operating systems, compiler or loader; insertion of backdoors into codes attacks; attacks on network capabilities of the systems;

attacks on the capabilities of harddisks; and attacks on smart cards.

III. THE PROPOSED FRAMEWORK FOR PRE AND POST VOTE CAST AUDIT

The framework has the administrator (admin.) and the voter as shown in Figure1. The Administrator refers to a key staff that is completely saddled with the responsibility of monitoring and managing the e-voting system. While the voter category demands voter to first log-in using a biometric finger printing device. If the finger print input is confirmed to be valid by the system, the voter's details will be displayed.

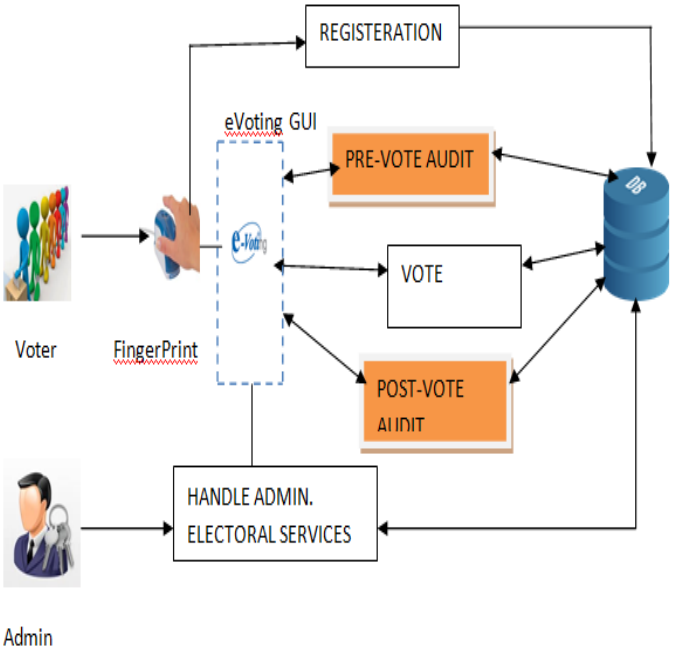

Figure 1. The Proposed Framework

The blue dotted rectangle represents the graphical user interface (GUI) of the proposed framework for the e-Voting system. Eligible voter is expected to fully register. The biometric device for fingerprint forms core details of the registration and the details information will automatically keep in the database (DB). The Administrator (Admin) is expected to perform some administration tasks such as registering contestants/parties, voters, responsible to display parties or contestants details when the need arise among other tasks. Essentially, this framework unlike existing systems, proposes a mechanism where voter can audit the numbers of votes garner by his/her intending contestant only before and after his vote to ensure credibility of the vote. In the lieu of this; the proposed architecture is described as three tiers architecture in this paper.

Pre-vote Audit: In this tier, voter is expected to login using his fingerprint to validate and authenticate his detail information in the database during registration. Successful login will affords voter to access the number of votes garner by his intending contestant/party **only** before his vote can be casted. That is; voter cannot access the number of votes garner by other contestants or parties. This is to ensure secrecy and data privacy of other parties. Once a voter accesses a contestant's numbers of votes; his vote must automatically be casted for such contestant or party as the case may be.

Vote: In this mid-tier, a vote is casted and goes to the secured database of the system. Expectedly, the vote will definitely cause increment to the relations (database) of benefited contestant and that of total votes respectively.

Post-vote Audit: In order to avoid and eliminates any acts of suspicious, the researchers come up with this final tier (otherwise known as confirmatory tier) of the architecture. This tier finally confirms and ensures that vote casted goes to the intending contestant. This tier checkmates vote against some contemptible acts like causes vote to be miscounted by tampering with the source codes or configuration; insert backdoors into codes; among others.

The architecture is further represented in Figure2 using flowchart. Voter is expected to log-in using finger-print biometric and some other personal details. If the inputs are correct, a pre-vote audit is expected is expected to be carried out for the intending contestant or party as the case may be. A vote is casted and equally expected to carry out a post-vote audit before login out of the system. All these functions to forestall any forms of despicable acts that could be carried out by different categories of people especially malicious software engineers that can illegitimately set some computer codes to create, delete or modify vote.

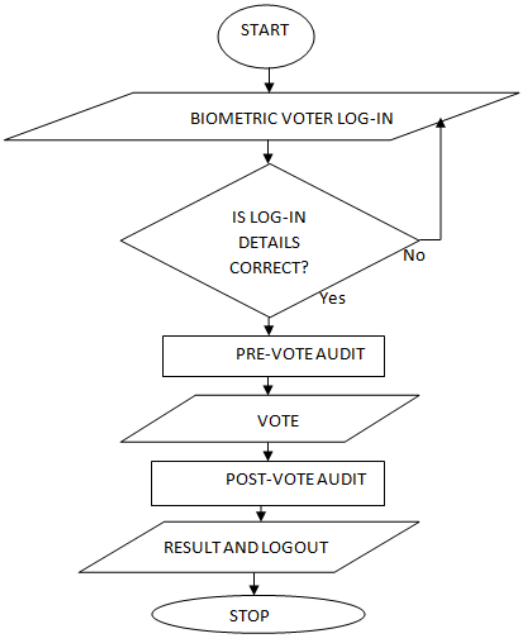

Figure 2. Representation of the Framework using flowchart

IV. MODELING THE PROPOSED FRAMEWORK USING USE CASE AND SEQUENCE DIAGRAM

In order to strengthen the aim of this research work and make a strong case for it, the proposed framework is further represented by using some models: use case model for Figure3 and sequence model for Figure4. This is because use case diagram affords a better model to describe the proposed functionalities of any new system; and sequence diagram – a unified modeling tool that

provides a graphical means of depicting objects interactions over time.

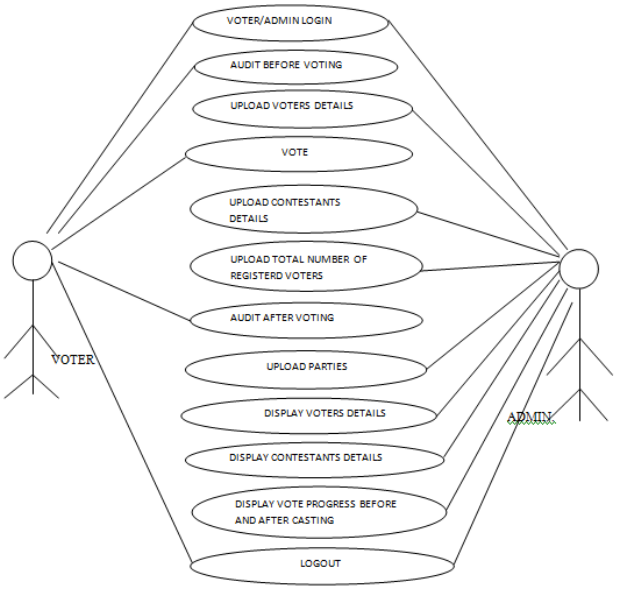

Figure 3. Use Case Modeling of the Proposed Framework

With the use case diagram in Figure3, the detail functionalities of the administrator in the proposed framework are captured. Among the functionalities during requirement analysis are upload: voters, contestants and political parties details, total number of registered voters. It is sole responsibility of the administrator to ensure that every eligible voters who shown up for the exercise are duly registered and ensure to upload their registration details into the database. A voter in this context means those that can vote and be voted for. At the end of it, total number of registered voters should be made available to the voters. Also in the case of parties, admin own the duty to equally register parties accordingly.

The work flow of Figure 4 is as follows: at this point it is assumed that every eligible voter has duly registered. Therefore, for vote cast exercise; voter can access the system by applying thumbprint via a fingerprint detector which is being forwarded to the database for onward verification and authentication. Once the system authenticates the thumbprint to be valid, a successful message is generated to the system interface. Then, voter can navigate the system to select audit before vote (pre-vote audit) and from the database the system display the valid number of accredited voters and various contestant or parties. Once voter select the intending contestant/party that will benefit his vote cast, the system will generates the total number of votes garner by the contestant and the system will prompt the voter to cast his vote automatically for that contestant. Thereafter, a post-vote audit is expected to carry out in order to validate and ensure that your vote is casted for the intending party; and finally logs-out.

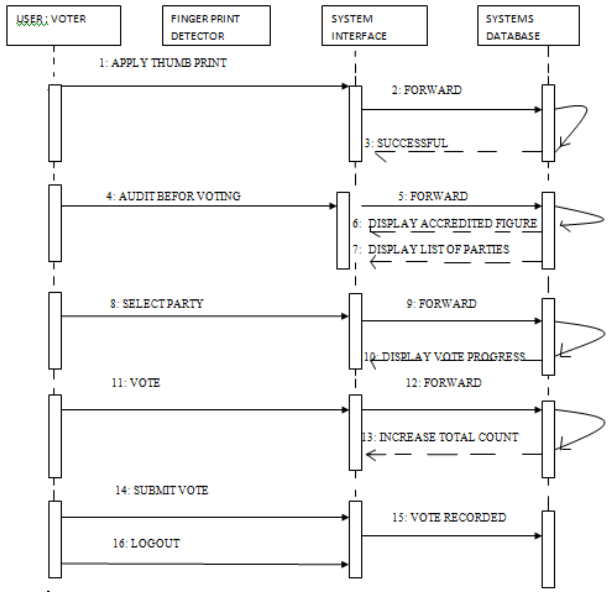

Figure 4. Sequence Diagram representation of the Proposed Framework

V. CONCLUSION AND RECOMMENDATIONS

It is a known fact that a large number of countries in Africa, for example, Nigeria; still uses ballot paper system for election. However, considering the common position of the related works reviewed in section II, it is long overdue for country like Nigeria to key-in into this invention called (enhanced) electronic voting system in order to build confidence and credibility for the Electoral College that would in turn ameliorate electoral violence. Thus, in this research paper, the credibility of electronic voting systems has been extended further by the proposed framework that prospective voter should be able to audit the number of votes garner by his/her beneficiary's contestant or party before and after vote is casted. With this proposed framework, election result's credibility is assured; electoral related violence as a result of suspicious feelings are eliminated; malicious manipulation of the system by unscrupulous and unethical information technology experts are firmly monitored. It is worth mentioning that pre and post auditing of votes can only be carried by voter strictly on his/her benefitted contestant or party. That is; the data privacy of other contestants or parties who are not beneficiaries of the prospective vote should be protected. However; the work is still in progress. In the nearest future, the full implementation is expected to be completed where evaluation and test of the developed system will be carried out. At that point, a case will be made for its electioneering adoption in Nigeria and beyond. Furthermore, the proposed system is recommended for institutions for example institutions of higher learning for student union elections on the small-scale applicability.

REFERENCES

[1] O. O. Okediran, E. O. Omidiora, S. O. Olabiyisi, R. A. Ganiyu and O. O. Alo. "A Framework for a Multifaceted Electronic Voting System". International Journal of Applied Science and Technology 135 Vol. 1 No.4; July 2011.

[2] S. Ahmad, S. A. J. Bt Abdullah and R. Bt Arshad. “Issues and Challenges of Transition to e-Voting Technology in Nigeria” Public Policy and Administration Research, Vol.5, No.4, 2015.

[3] A. J. Jegede, G. I. O. Aimufua and N. I. Akosu. “Electronic Voting: A Panacia for electoral irregularities in developing countries”. International Journal of Science and Knowledge, Vol. 1; No. 1; 17-30; 2012.

[4] M. Duruji, C. Ayo, O. Samuel and A. Oni.“Making a Case for e-Voting in Nigeria”, Proceedings of the 15th European Conference on eGovernment: ECEG, Portsmouth, UK, 18-19 June, 2015.

[5] D. O. Nnamani. “Electoral Process and Challenges of Good Governance in the Nigerian State (1999-2011)”. Journal of Good Governance and Sustainable Development in Africa (JGGSDA), Vol. 2, No 3, December, 2014.

[6] A. Abdullahi and R. T. Sakariyau. “Democracy and Politics of Godfatherism In Nigeria: The Effects and Way Forward”. International Journal of Politics and Good Governance, Volume 4, No. 4.2 Quarter II 2013.

[7] L. Olurode. Election Security in Nigeria: Matter Arising. Friedrich-Ebert-Stiftung (FES) September, 2013.

[8] P. A. Oyadiran and O. I. Nweke. An Appraisal of the Nigerian Democratic Journey between 1999 and 2014. JORIND 12 (2) December, 2014.

[9] N. O. Htet and A. M. Aung. “Implementation and Analysis of Secure Electronic Voting System”. International Journal of Scientific and Technology Research Volume 2, Issue 3, March 2013.

[10] M. R. Ayesha and S. Z. Naseem. Enhanced Real Time System of E-Voting using Finger Print, Conference Paper · November 2013.

[11] T. U. Pavshere and S. V. More. “A Survey on Secured E-Voting System Using Biometric”. International Journal of Advanced Research in Science, Engineering and Technology, Vol. 3, Issue 3, March 2016.

[12] C. Vielhauer. Biometric User Authentication for IT Security from Fundamental to Handwriting. Adavnces in Information Security Volume 18, Springer Sciences+Business Media Inc., 2006.

[13] R. Tekadel, R. Kharat, V. Magade, M. Shaikh and P. Mendhe. “E-Voting System using Visual Cryptography & Homomorphic Encryption”. International Journal of Advanced Research in Computer and Communication Engineering Vol. 5, Issue 1, January 2016.

[14] A. A. Akshay, G. R. Manoj, R. S. Rajashree and J. V. Bhagyashree. “Secure Mobile Based E-Voting System”. International Journal on Recent and Innovation Trends in Computing and Communication. Volume: 4 Issue: 4, April 2016.

[15] S. M. Abdulhamid, O. S. Adebayo, D. O. Ugiomoh and M. D. AbdulMalik. “The Design and Development of Real-Time E-Voting System in Nigeria with Emphasis on Security and Result Veracity”. I. J. Computer Network and Information Security 2013, 5, 9 – 18.

[16] M. M. Hoque. “A Simplified Electronic Voting Machine System”. International Journal of Advanced Science and Technology Vol.62, pp.97-102, 2014.

[17] B. Rexha, V. Neziri and R. Dervishi. Improving authentication and transparency of e-Voting system – Kosovo case. International Journal of Computers and Communications Issue 1, Volume 6, 2012.

[18] A. Riera and P. Brown. Bringing Confidence to Electronic Voting. Electronic Journal of e-Governmnet Volume 1 Issue 1. (14-21) 2003.

[19] S. Krassovsky. Security flaws of existing electronic voting systems, 2005.