DEVELOPMENT OF A SECURED E-VOTING SYSTEM WITH OTP AS SECOND ORDER AUTHENTICATION

By

HABU J. SALAMI * O. S. ADEBAYO ** A. O. ISAH ***

K. H. LAWAL **** JOHN K. ALHASSAN *****

* Information Technology Services, Federal University of Technology, Minna, Nigeria.
-*-***** Department of Cyber Security Science, Federal University of Technology, Minna, Nigeria.
**** Department of Computer Science, Federal University of Technology, Minna, Nigeria.

Date Received: -/-/- Date Revised: -/-/- Date Accepted: -/-/-

ABSTRACT

Electronics voting has become the most preferred and generally acceptable voting method in the 21st century. Advanced and developed countries are constantly reviewing their e-voting systems. However, the attendant cyber security problem associated with the e-voting system has been giving concerns to cyber security experts and researchers. The authentication methods employed in the existing e-voting system is for a voter to input a unique identification number that has been assigned after accreditation, this is to enable confirmation of the voter's details in the voter registration data base. This paper seeks to develop a secured e-voting system that integrates a second order authentication in the form of One-Time Password to again and finally confirm the voters' details in the registration data base before voting is allowed. Java programming language was employed in coding the OTP algorithm into the existing e-voting system algorithm. The e-voting system is more secure with this work.

Keywords: E-voting, Security, OTP, Authentication, Development.

INTRODUCTION

The process of elections is a process that allows communities, groups, organizations or the generality of the people to willingly bring their interest to bear in other to decide their representation in a politically arranged manner or platforms through contests. This contest includes nominations and voting, different forms of voting are considered in attaining the political interest.

According to (Stephan, 2012), voting has its origin from time immemorial. Specifically, way back to the 5th Century B.C with an ancient Greek wine cup showing the earliest form of voting. To decide who claims the armour of the fallen Achilles, voting was done to choose between two heroes Ajax and Odysseus during the Trojan War. Casting of pebbles into an urn and bean-counting pattern to indicate choice are also historical form of voting by the ancient Greeks.

Manual voting which includes papers or direct head counting has been in existence and has been the legacy method. To have some credibility in the contest therefore, there are rules guiding the contests. The adherence to the rules is basically influenced by the method of voting adopted and other factors. These rules are well known and understood by all players and are accepted from the onset. To have a credible election, it is required that every player have the opportunity in the process since the rules are known to every stake holder.

Problems associated with manual voting system are numerous ranging from lack of cost effectiveness, delays, frauds and all other forms of manipulations. The whole essence of voting is for people's voice to be heard and making their choice of leaders. In the manual voting system, corruption, disenfranchisements and other various frauds associated with it like the ballot papers system, is making the people voiceless, it then means that the need for voting does not even arise.

Governments are required to convert their paper-based election systems to electronic form to guaranty "One

Person – One Vote (Brownback, 2018). According to the author, this will eliminate fraud and corruption, the author went further to give examples of flaws associated with paper voting citing the Haitian elections which was invalidated due to fraudulent paper ballots that were produced in Dubai and were used to stuff the ballot boxes, the author observed also that this flaw cost the Haitaian government $100,000,000 approximately. Also, in an American election, the ballot papers ran out of stock and additional white ballot papers instead of the normal blue ballot papers, were being printed for voters which they quickly filled and stuffed in the ballot boxes, these were done in a manner that they were not traceable. This according to the author, underscored the point that even the first world countries could have problems with paper-based ballots.

Electronic voting has become inevitable in view of the flaws associated with all forms of manual voting systems as highlighted earlier. More countries are embracing the e-voting system. The e-voting system is however, with its own problems among which is majorly authentication. Understanding Biometrics: Benefits of Electronic Voting, (2014) there are an increasing number of countries and organizations around the world that have implemented or piloted electronic voting systems. The author observed that although, countries and organizations implementing the system encounters different experiences, the increasing adoption of these new technologies testifies to the fact that

the innovation of electronic voting system offers more benefits over manual methods of voting.

1. Some of the advantages of electronics voting.

- Prevention of frauds associated with manual voting is drastically reduced by electronic voting system.
- Detection and rejection of invalid vote cast is instantly achieved.
- In electronics voting system, overhead cost spent on electoral officers, administrations and logistics are lesser compare to the huge funds expended in manual voting.
- The speed of voting process is faster since it is just a matter of tapping a key or a party logo
- Mobility is another advantage of electronic voting since electronic voting system could implemented to be compatible with some mobile devices. It means that voter with a mobile device like phones can cast his or her vote anywhere without necessarily going to the voting venue.
- It is much more convenient in electronic voting since voting can be done at the voter's time within the period allowed for the voting exercise.

B. Disadvantages.

- Despite the advantages enumerated above, the electronic voting system is not without its own disadvantages.
- Cyber security issue is the major challenge of electronic voting system since the system access and authentications could be compromised.
- Network congestion could also be a serious challenge especially, where the voting is done online via internet network.
- Due to the different level of literacy among voters, the electronic voting system could pose some serious challenges to the less educated or illiterate voters. Hence, there is need for serious advocacy and orientation for these categories of voters on how to use the system.

2. Review of Related E-voting Systems

Wasiu & Luisa, (2017) discussed the various methods of voting during elections which includes voice, physical counting of heads, electronics and manual, they also discussed the various demerits of the manual voting system that gave rise to advancement by researchers to come up with the electronics voting technologies. In their contribution to the technology of electronic voting system, the author used the open source Microsoft Visual Basic Environment (MVBE) and the ASP.NET Model-View-Controller to design an online voting portal with program coding to achieve an online E- voting platform. The authentication employed by the authors in their design was a token pre-issued during registration. This kind of authentication however, could be improved upon by another level of

authentication which is the focus of our paper to provide a second order real-time authentication in the form of OTP to guarantee e- voting system.

Al-Ameen and Talab, (2013) introduces electronics voting systems in this research and highlights the to deploy its usage in a manner and process that boosts confidence in the electoral activities by outlining the various ways voters can vote, the different phases and stages in e-voting system. The authors thereafter discuss the security issues and vulnerabilities e-voting systems as important factors to put into consideration. However, the research lacked a well stated methodology or survey and thus there were not results and recommendations were not made based on facts.

Falkner, Kieseberg, Simos, Traxler, and Weippl, (2014) propose an e-voting authentication scheme combined with QR-codes and visual cryptography as a methodology for improving the security of e-voting systems. The research makes sure that the ease of use is made simple to reduce the technical requirements needed to deploy the systems for electoral processes. Users only must handle a device like a smartphone containing a QR-code reader. The e-voting passwords for authentication are encoded as QR-codes and later encrypted into shadow transparencies. The performance evaluation of the proposed system shows a robust scanning process.

Aggarwal, (2016) discuss issues in the implantation of electronic voting system in India. Online voting systems requires clients, servers and networks that are exposed to the threat of denial of service attacks and the possibility of the invasion of electronic voting systems by viruses. The research is concerned about the security challenge associated with remote internet voting, the feasibility of running national elections over the internet, and the security limitations of existing infrastructure for electronic voting that includes social engineering and digital divide. However, the research is not able to proffer a technical method such as One Time Password authentication for enforcing secured electronic voting.

Rexha, Neziri, and Dervishi, (2012). analyze and propose a new efficient architecture for electronic voting system in Kosovo, the threat vectors and their avoidance in such systems. The authors use the combination of public key encryption systems, digital signature, digital certificates and smart cards, as a methodology for improving authentication and transparency of electronic voting systems, to enable citizens to cast their vote in any polling station, in contrast to manual paper form of voting where citizens are linked to the predefined polling stations they are registered with. However, the use of One Time Password to establish security measure against session hijack was not suggest in the authentication model.

Sridharan, (2013) presents the implementation of authenticated and secured online voting system with the use of fingerprint biometric, secret voting password, and national universal identification number as a methodology to develop a cost-effective online voting system, ensuring that are eligible voters are not denied their right to vote in a secret ballot system that has integrity. The model proposed helps in achieving the authenticity, non-traceability of vote cast and security with confidentiality also being enforced. The recycling of the same secret password is a vulnerability that can be exploited to compromise the online voting system. Thus, the need for One Time Password that is generated each time voting is required.

Hamid, Radzi, Rahman, Wen, and Abdullah, (2017) developed a scheme that preserves anonymity in electronic voting systems by using voter nonrepudiation-oriented model. The system contains ten modules which are log in, vote session, voters, candidates, open session, voting results, user accounts, initial score logs and reset vote count as features. The performance evaluation of the system reveals that 70% of the users suggest that the system needs improvement in future work, whereas 30% of the users are satisfied with the system. Meanwhile, 50% of the users agree that the system is user friendly, 30% disagree and 20% of users were not sure if the system is user friendly or not. On the other hand, having developed a scheme that preserves anonymity, authenticating the anonymous voters for the integrity of the electoral process was not mentioned.

In all e-voting systems, security and the veracity of results are major challenges which (Abdulhamid, Adebayo, Ugiomoh, & AbdulMalik, 2013) try to address in their paper.

However, further authentication is required to complement the author's efforts which this seek to achieve.

3. Methodology

A. Development of a secured e-voting system with OTP as second order authentication.

The methodology for this proposed system is experimental. The OTP authentication model is introduced after the first order of authentications in the string of the e- voting programming codes, when the condition for the order of authentication is met by the prospective voter, the system allowed access to the voting pad or burton for the voter to simply tap or press. But for the proposed system, the programing at the back end will automatically proceed to interface with the API of the OTP message generating program to request for the provision of the generated OTP code which is usually a string of numbers via the voters' phone or email. This will then form the second credential or PIN for the voter to enter into the system before the voting is allowed. Figure 1 and Figure 2 show the model for the existing system with first order authentication level and the proposed system with the second order authentication level respectively.

Figure 1 is the existing e-voting system with the first authentication level. At this level, the system is not free from manipulation because all the credentials required at this level are mostly supplied during registration and accreditation process.

1) Algorithm for the existing e-voting system with the first order authentication level

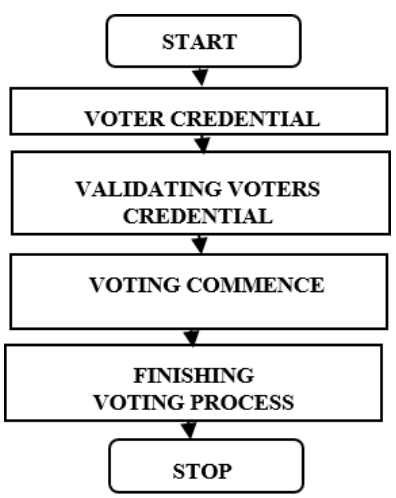

Figure 1. Existing e-voting system with first order authentication level

INPUT:

VOTERS CREDENTIAL

VALIDATES VOTER'S CREDENTIAL

ACCESSING STUDENT MATRICULATION NUMBER

CHECKING PERSONAL IDENTIFICATION NUMBER (PIN)

IF SUCCESSFUL,

PROCESS:

VOTING PROCESS COMMENCES

DISPLAYING CANDIDATES FOR VOTING

OUTPUT:

FINISHING VOTING PROCESS

Figure 2 is the proposed system with OTP implementation as the second order authentication level. In this system the level of manipulation associate with the first order authentication is drastically reduce and prove very hard to by-pass since the OTP generation is instant and real time. It is also in itself identifying the real voter since the phone

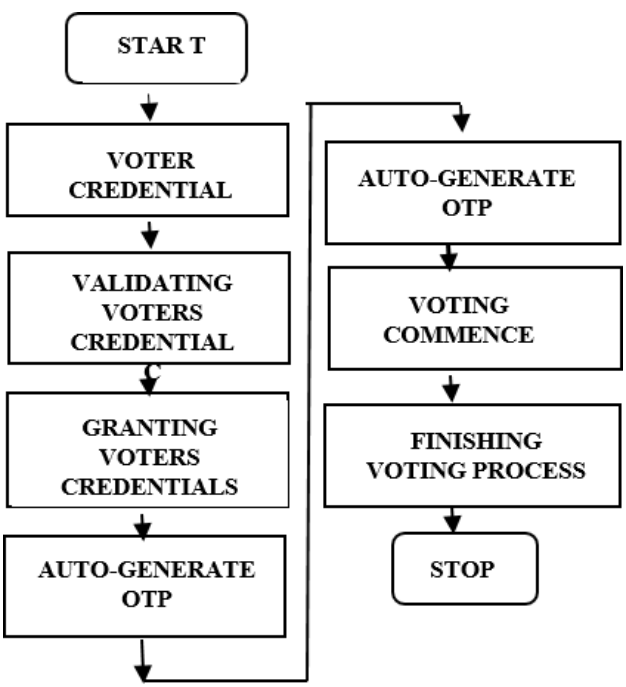

Figure 2. Proposed e-voting system with the OTP as the second order authentication

which the OTP code is sent normally belongs to the voter.

1) Algorithm for the proposed e-voting system with the OTP

INPUT:

VOTERS CREDENTIAL

VALIDATES VOTER'S INPUT THROUGH

MATRICULATION NUMBER

PERSONAL IDENTIFICATION NUMBER (PIN)

IF SUCCESSFUL,

PROCESS:

AUTO-GENERATE ONE TIME PASSWORD (OTP) SENDING OTP VIA SMS

PROMPTS FOR ONE TIME PASSWORD VALIDATING OTP

IF SUCCESSFUL,

PROCESS:

VOTING PROCESS COMMENCES DISPLAY CANDIDATES FOR VOTING

OUTPUT:

FINISHING VOTING PROCESS

1) Flowchart of the proposed system

Figure 3 is the flowchart of the proposed model of e-voting system utilizing OTP as the second order authentication. In the existing e-voting system, the authentication level of voters is done at the voters' credential level, these may comprise of user names, passwords and any other form of identification numbers that are normally issued during voters' registration and accreditation process. All authentications at this level are an order of authentication. Due to the introduction of the OTP algorithm, the system is further strengthened by requesting for the generated OTP as confirmation of the first order credentials.

1) Existing System interfaces.

Figures 4-6 shows the existing system interfaces

Here the voters are expected to type in their identification number and PIN as provided during accreditation of voters, if the identification number and Pin is correct it will take us to Figure 5 otherwise it will show Figure 4 requesting to try again.

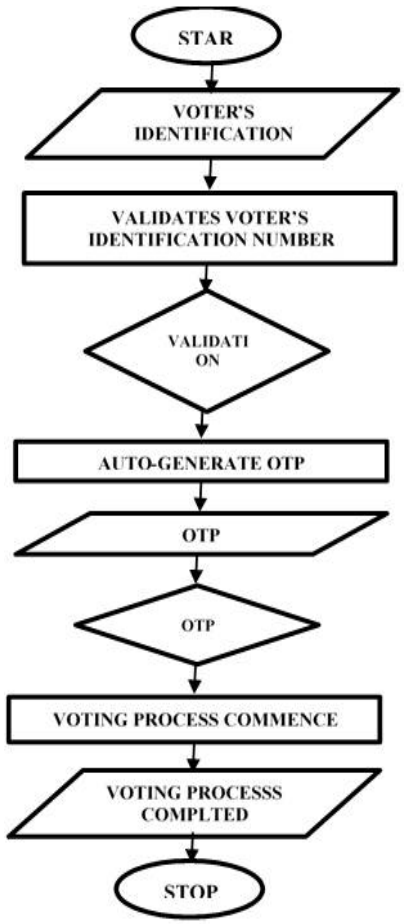

Figure 3. Flowchart of the proposed model

Figure 4. Index and login page

If the login parameter is not correct this page shows otherwise the system takes us to voting page

After the voters has passed through the authentication huddle the next thing is to start casting votes

Figures 7-11 shows the proposed system interfaces.

Here the voters are expected to type in their identification

Figure 5. Checking entries parameters

number and provided during accreditation of voters, if the identification number and Pin is correct it will take us to figure 8 otherwise it will show figure 7 requesting to try again

If the login parameter is not correct this page shows otherwise the system takes us to SMS (OTP) page.

Figure 9 is a typical phone showing the instant generated OTP code message received by a voter who has supplied the first authentication credentials.

If One Time Password (OTP) entries does not match it displays this page and want you to try again, however if One time Password (OTP) entries is correct, it takes you to figure 11 to start casting your votes.

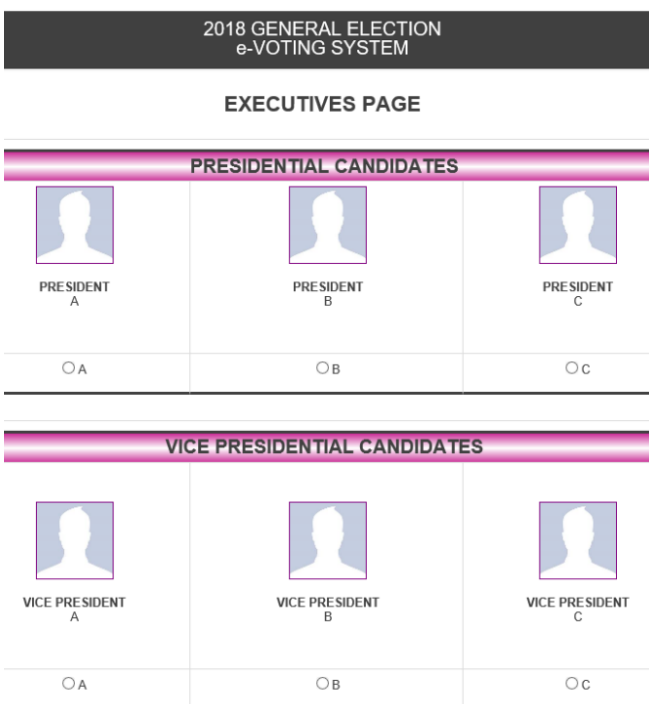

Figure 6. Example of voting page

Figure 11 is the example of voting interface displaying the photo of the candidates for the election. After the voters has passed through the two authentications huddle the next thing is to start their casting votes.

Discussion

The result of this proposed model from the foregoing clearly showed the general sequence of operation of both the existing and the proposed e-voting system in the order of voter credential, validating voters credential, granting voters' credential, auto-generation of OTP, commencement of vote and finishing the voting process. Voters supplied their credential to gain access to voting software after which they login, the voter is subjected to validation to check credentials (We used matriculation and PIN as example credentials in this paper). The

Figure 7. Index and login page

Figure 8. Checking entries parameters

Figure 9. Generated OTP code sent to the voters' phone.

Figure 10. One time Password (OTP) entries

validation of these credentials is done to make sure they are correct and to avoid double voting in the case of existing system, this is testing and granting first level authentication. OTP which is a password that is valid for only one login session is then introduced, OTPs avoid several shortcomings that are associated with traditional (static) password-based authentication. This will subject the voter to another level authentication through one time password (OTP). At this point the system generate digits code and send it to voter phone (SMS) and email address.

If OTP validation is was successful, the voter is allow to commence the voting process. At this point, all candidates contesting for position are display, voters can vote by

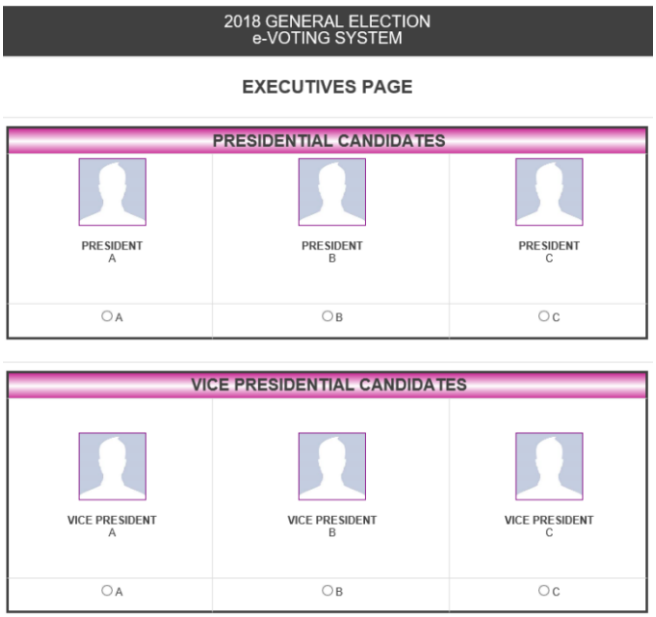

Figure 11. Example of voting page

choosing an option to complete the voting process.

Conclusion and Recommendation

We have been able to show that the problems associated with e-voting system with only first level authentications can be solve by the introduction of the technology of One-time- Password (OTP) as a second order authentication level.

Although, cybercriminals will continue to try to compromise e-voting system, we are recommending that further research should be done to include other form of security and authentication features to be integrated into e- voting system. This is by way of having three or more authentication levels fused together. It is also recommended that e-voting system should be giving more priority by both government, organizations and group of individuals in all election matters.

References

[1]. **Stephan, A. (2012).** Voting with the Ancient Greeks, Retrieved from http://blogs.getty.edu/iris/voting-with-the-ancient-greeks/

[2]. **Brownback, T. (2018).** The problems with a paper-based voting system, Retrieved from http://www.dcag.com/images/WhitePaper_The_problems_with_a_paper_based_voting_system.pdf

[3]. **Understanding Biometrics: Benefits of Electronic**

Voting. (2014). In New Era Live. Retrieved from https://neweralive.na/2014/11/27/understanding-biometrics-benefits-electronic-voting/

[4]. Wasiu, S. 1. A. D., & Luisa, O. A. (2017). Electronic Voting: Challenges and Prospects in Nigeria's Democracy. *The International Journal of Engineering and Science (IJES)*, 6(5), 67-76.

[5]. Al-Ameen, A., & Talab, S. A. (2013). E-Voting Systems Security Issues. *International Journal of Networked Computing and Advanced Information Management (IJNCM)*. 3(1), 25-34.

[6]. Falkner, S., Kieseberg, P., Simos, D. E., Traxler, C., & Weippl, E. (2014). E-voting Authentication with QR-codes. In International Conference on Human Aspects of Information Security, Privacy, and Trust (pp. 149-159). Springer, Cham.

[7]. Aggarwal, K. (2016). Issues in implementing of Online Voting System in India. *International Journal of Engineering Science and Computing*, 6(5), 5285-5288.

[8]. Rexha, B., Neziri, V., & Dervishi, R. (2012). Improving authentication and transparency of e-Voting system–Kosovo case. *International Journal of Computers and Communications,* 6(1), 84-91.

[9]. Sridharan, S. (2013). Implementation of authenticated and secure online voting system. *In Computing, Communications and Networking Technologies (ICCCNT),* 2013 Fourth International Conference on (pp. 1-7). IEEE.

[10]. Hamid, I. R. A., Radzi, S. N. M., Rahman, N. H. A., Wen, C. C., & Abdullah, N. A. (2017). Preserving anonymity in e-voting system using voter non-repudiation oriented scheme. In AIP Conference Proceedings (Vol. 1891, No. 1, p. 020017). AIP Publishing.

[11]. Abdulhamid, S. Í. M., Adebayo, O. S., Ugiomoh, D. O., & AbdulMalik, M. D. (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 & Information Security*, 5(5).

ABOUT THE AUTHORS

** Information Technology Services, Federal University of Technology, Minna, Nigeria.*
--***** Department of Cyber Security Science, Federal University of Technology, Minna, Nigeria.*
***** Department of Computer Science, Federal University of Technology, Minna, Nigeria.*