Journal of Engineering and Applied Sciences 14 (11): 3732-3740, 2019
ISSN: 1816-949X

Image and Password Multifactor Authentication Scheme for e-Voting

[1]Adebayo Omotosho, [1]Emmanuel Asani, [2]Paula Fiddi and [1]Noah Akande
[1]Department of Computer Science, Landmark University, Omu-Aran, Nigeria
[2]Department of Computer Science, University of Oxford, England, United Kingdom

Abstract: The credibility of an electronic voting process depends on several factors such as authentication mechanism, correctness measure and security of votes. Authentication phase is so important because it is usually the first step to initiate a voting process. The inability of the system to correctly identify voters and authorize their votes can result in the same irregularities that are common to the non-electronic approach. This study presents an electronic voting system that makes use of multifactor authentication to verify voters before voting. The authentication mechanism relies on user's ability to remember passwords and unique images chosen at registration. System testing was carried out 30 days after user's registration. The system was evaluated by 50 user's and it was found that the process is feasible, going by the fact that all 50 voters were able to vote successfully. However, the ratio of users who remember images on the first attempt to those unable to remember on the first attempt is 1:2.

Key words: Authentication, electronic voting, multifactor, passwords, security, irregularities

INTRODUCTION

Security is an essential factor in modern computerized systems used in banking, health, schools and so on. It ensures that only authenticated and authorized individuals can use a system and term generally, encompasses authentication, confidentiality and integrity (Omotosho and Emuoyibofarhe, 2014; Omotosho *et al*., 2017). Human errors and manipulations, multiple voting, long time needed to count the vote, huge cost of election process and security are some of the irregularities that have characterized and flawed traditional voting systems. Electronic voting aptly called e-Voting leverages on the advent of Information and Communication Technology (ICT) to provide an electronic platform for eligible voters to cast, protect and count their votes. The beauty of e-Voting is seen in the fact that it can be modelled to meet the specific peculiarity and need of respective countries. These specific needs are categorized into three by AboSamra *et al*. (2017), they are system, scheme and voter requirements. System-related requirements specify factors that must be put into consideration when developing the e-Voting system. These include auditability, cost-effectiveness, correctness, efficiency, flexibility, integrity, receipt-freeness, reliability, robustness, scalability, verifiability, voter mobility among others. Scheme related requirements postulate features that must guarantee the viability of the e-Voting process, this could be measured using metrics like practicality, justice and fairness, equity, clarity of rules, security, etc. Voter related requirements identify the voters as the most important component of any electoral process and dictates factors that must be put in place to ensure that only eligible voters cast their votes. These factors include authentication, awareness, convenience, eligibility, orientation, registration, transparency, non-reusability or duplicability of the vote cast, privacy, scheme simplicity among others. Every e-Voting system is modelled to put these requirements into consideration.

e-Voting could be achieved using several ICT tools such as the internet (as in remote internet voting, kiosk internet voting, polling place internet voting and precinct internet voting), web, Short Messaging Service (SMS), smart cards, etc. Regardless of the ICT tools deployed, election commissions in developed countries who have adopted e-Voting have testified that it is less expensive when compared to the traditional voting systems makes the voting process easier and flexible thereby leading to large voter's turnout, reduces time used and errors encountered when counting votes, guarantees a wide coverage area, yields an accurate and faster election result release (Mursi *et al*., 2015; Hapsara *et al*., 2017).

As a condition of voting, all eligible voters are expected to meet certain predefined requirements before the actual voting exercise takes place. In Nigeria, voters are expected to be above 17 years of age. However, measures must be put in place to guarantee and ensure that only eligible and registered voters cast their votes

Corresponding Author: Adebayo Omotosho, Department of Computer Science, Landmark University, Omu-Aran, Nigeria

once. The process of achieving this is termed voters authentication. Putting an effective authentication technique in place will guarantee the credibility of the election process and in turn, save cost that may be accrued if the election process were to be canceled. There is a need to ensure that only eligible voters can vote and that the system is fool-proof in defending accidental and intentional misuse, all of which is captured in the authentication process a huge sum of $500 was reported to have been wasted when Kenya's 2017 election was cancelled by her supreme court due to irregularities and illegalities (Nyabola, 2017). A little fraction of this cost would have been successfully invested in an alternative e-Voting system.

Some literature on e-Voting authentication techniques: Although, diverse electronic voting systems that use a variety of authentication methods have been proposed and developed, there still exists security problems related to the authentication phase in e-Voting. The various authentication methods used in e-Voting include knowledge-based methods, token-based methods, biometric-based methods amongst others. The biometric-based authentication is regarded to have the highest security level, since, it has security traits that cannot be altered or stolen (Abu-Shanab *et al*., 2013). However, this authentication technique has several drawbacks as a single biometric measure is always subject to security breaches if not properly administered. A few of the works on authentication and authorization are discussed briefly as follows.

Motivated by the impracticability and somewhat cumbersome process involved in existing authentication protocol for e-Voting (Falkner *et al*., 2014) proposed an authentication method enhanced with a QR code and visual cryptography. Their method was meant to simplify the voting process for persons who have limited technical abilities while still retaining the security of the voting process. The system generates a secure randomized password for voters and then encodes them as QR-codes. The QR-code is encrypted using the visual secret sharing scheme which splits the image into sub-pixel called shares and decrypted when they are stacked using OR-operation. During voting, the QR code is generated to the user if She/He can provide the public key K1 and share S1 that matches the corresponding share S2 in the database, thus, stacking the shares to decrypt the QR code. The user scans the QR-code to reveal the secure password that gives him/her access to voting. Nwangwu (2015), investigates the role of the biometric smart card reader in improving the credibility of the Nigerian 2015 general elections. The use of card reader designed to read biometric information and authenticate the fingerprints of voters is seen to have greatly reduced the electoral violence and caused a significant drop in the number of election petitions by aggrieved electoral candidates. Results of this election also show that the use of the e-Voting system builds the confidence of Nigerian voters as there was an overall increase in voter's turnout in comparison with previous election processes. Deshpande *et al.* (2015) proffered a solution to the inconvenience and discomfort of the traditional voting system by proposing an e-Voting system that uses an android application. The proposed system allows voters to vote from any remote location from any device that supports the Android OS. The system makes use of a two-factor authentication method which includes Face recognition and the generation and verification of a One Time Password (OTP). The voter is identified via the facial recognition, then the OTP is generated and sent as SMS before verification takes place then the voter can cast his or her vote.

Rana *et al.* (2015) also discussed the necessary constraints for a secure e-Voting system and propose a framework consisting of two modules. One of which is the voter identification and authentication system where a 16-digit key is generated with a hash algorithm and sent to the user. The second module takes care of the anonymity of users. This is a novel approach intended to increase the efficiency and feasibility of the electoral system. Olaniyi *et al.* (2016) developed an e-Voting system that adopts two-levels of security. The voters are first authenticated using the radio frequency identification technique and the votes cast are protected using enhanced least significant-bit audio stenography method. They provide counter-measures for authentication, confidentiality and verifiability measures through their proposed system. Each voter is given an RFID tag which is authenticated with the RFID reader. The developed system is found to be effective and efficient after evaluations against set security standards were made. Olaniyi *et al.* (2016) developed a secure e-Voting system which uses fingerprint biometrics and the AES wavelet-based crypto-watermarking approach. The AES cryptographic system preserves the assertion of data integrity, i.e., the use of a private key and the watermarking technique allows the vote to be kept confidential. The proposed system was tested, proven to be secure and superior to other voting methods in its dual layer of security. However, a multiplatform authentication parameter to enable integration with other electronic devices is suggested. Oke *et al.* (2017) addressed the security vulnerabilities in the current Nigerian e-Voting system, i.e., the use of smart card readers as well as a device to accredit the Permanent Voter's Card (PVC). The previous voting techniques make use of a single

authentication system leading to impersonation during the voting process. This study, therefore, proposes a technique which involves multifactor authentication using biometric fingerprint and a cryptographically secure smart card. The multifactor technique is recognized as one of the most secure methods for authentication. A novel approach using both finger print and smartcards with an enhanced Feistel block cipher is developed to take care of the shortcomings of the previous e-Voting system.

The Electronic Voting Machines (EVM's) commonly used for elections in India was discussed by Titus *et al.* (2018). It was found that these EVM's have limitations whereby fake votes are cast and one person casts multiple votes or votes are cast for a candidate whether an individual cast a vote or not. The study proposes a multiple bedded verification method whereby a voter is authenticated via. a fingerprint recognition system as well as a stenography technique which captures the entire voting process, secures the image and makes it available for verification when recounting if necessary. This is done to eliminate discrepancies in the number of votes cast and the number of votes counted. Their results show that the proposed method effectively increases the security and overcomes the drawbacks of their current electronic voting method. The multifactor authentication scheme adopted in this research is discussed in the next research.

MATERIALS AND METHODS

The following scientific approaches were used to achieve the central idea of this research. They are requirement definition and infrastructural model.

Requirement definition of the proposed service infrastructure

Image and password multifactor authentication scheme for e-Voting requirements: This requirement follows from the assumption that to automate a voting authentication system, the system should provide:

- Eligibility: the system should be designed in a way that only allows only citizens above the age of 17 years
- Uniqueness: a user can vote once
- Accuracy: electoral system should be able to count votes with lesser errors and inconsistencies
- Integrity: voting cannot be delegated and votes can only be cast by the registered user by himself or herself alone
- Reliability: the system should work robustly without any loss of voter's data due to a good and reliable database
- Flexibility: more modules of voting operations can be integrated into the system to increase functionality
- Convenience: users should be able to recollect images and passwords with minimal effort

Service provision requirement: The infrastructure should allow the electoral body to monitor: the registration of voters, number of verified and unverified registration, statistics of the number of people that actually voted, the number of invalid votes, the number of trial attempts for voters who forget their chose image, etc.

Infrastructural model and architect

Overall system architecture: The hardware phase integrated into the proposed multifactor authentication system consists of tablets, phones and computer system (for voter's registration and verification). The software phase is divided into two sub-phases front end (application interfaces the users would interact with) back end (database where voter's information is stored). In designing the front end and back end of the system, some development tools required are PHP, JavaScript and CSS for building the graphical user interface and functionalities of the system WAMP server for hosting MySQL database which is fast, robust and easy to use. Components of the proposed system architecture in Fig. 1.

Devices: User devices for registration in the prototyped system are mobile phones and laptops.

Exchange server: The registration process captures voter's personal information and this data is stored in this server once a user has been verified. In order to complete user's authentication verification, a temporary short code is generated by this service.

Telecommunication network provider: The network provider is responsible for sending the code generated as a one-time pin to the user's mobile phone number.

Image file server: This is the repository for the image users will have to choose and remember for authentication during the election in order to be authorized to cast his or her vote successfully. Most of the images are common items that can easily be identified and they are downloaded freely from Google images. In addition to using a username and pin for authentication users selected images will form a part of the multifactor authentication.

Operational phases

Registration phase: The system is designed to authenticate only voters that are eligible to vote the voter would first be required to input his or her personal

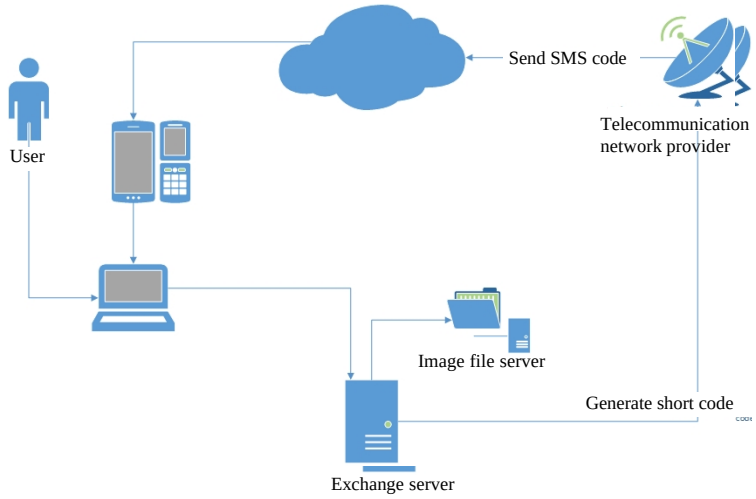

Fig. 1: System architecture

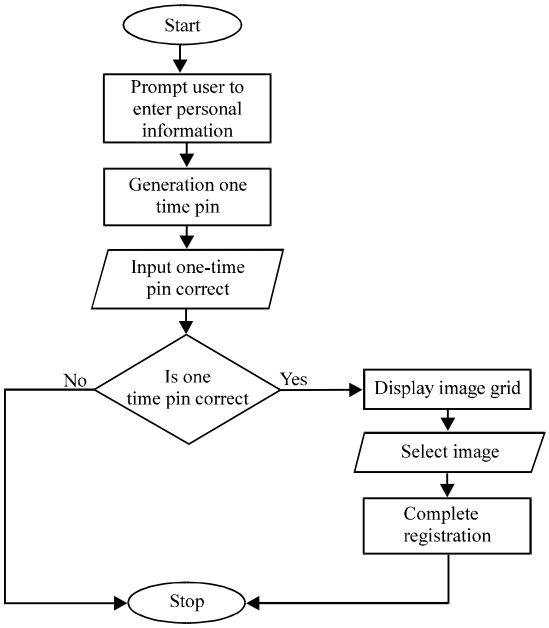

Fig. 2: Flowchart of the registration phase

information during this phase. Once this step is completed successfully, the system automatically generates a unique one-time pin which would be sent to the phone of the registered voter as short message service. The one-time pin together with the mobile phone number is used to access an image grid from which the future voter would be mandated to pick an image he or she would have to remember during the election phase. The system flow chart of this phase is shown in Fig. 2.

Election phase: The election phase is the voting phase and is depicted in Fig. 3. Voting process starts with the voter's login password and then ends with choosing the

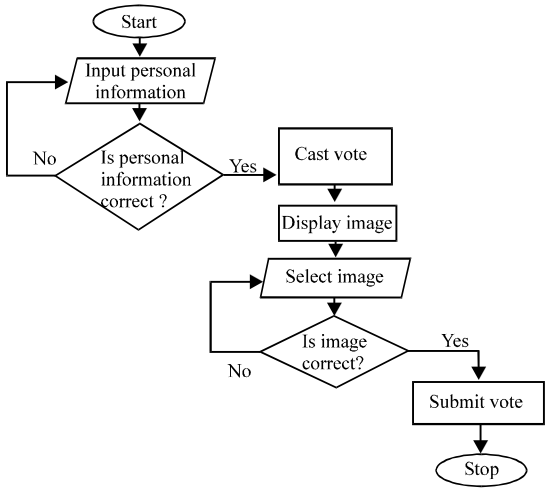

Fig. 3: Flowchart of election phase

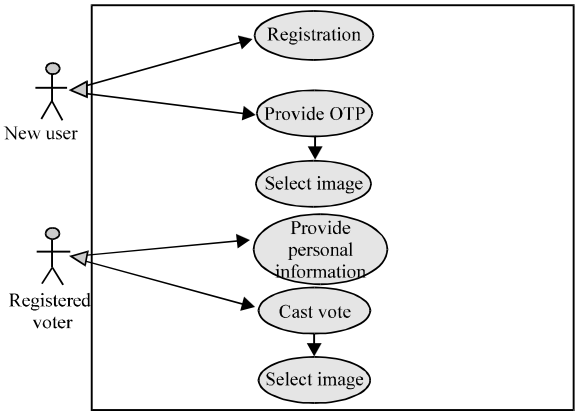

Fig. 4: Use case diagram of the system

unique image selected during registration, if this is successful, the vote is cast. Use case model of the proposed system is shown in Fig. 4.

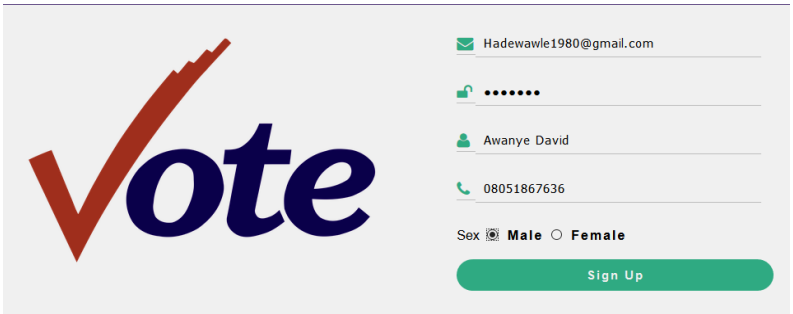

Fig. 5: Registration interface

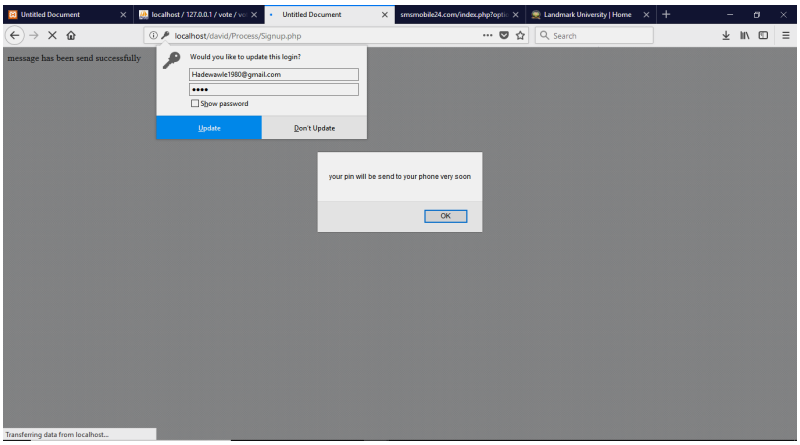

Fig. 6: One-time pin sent interface

RESULTS AND DISCUSSION

The registration interface of the system prototype is shown in Fig. 5 this is where an eligible voter can register into the system. The system is designed to accept some mandatory inputs from the user such as user's email, the user's password user name and the user's phone number. In Fig. 6, a one-time pin is sent to the user's phone number for validation and when they click on the ok button, it takes them to the screen where they would be required to input this one-time pin. A phone interface receiving one-time pin is shown in Fig. 7, the user would be requested to input this one time pin and the phone number he or she used for registration into Fig. 8 in order to gain access to the image grid where he or she would be required to select animage. Figure 9 and 10 show the randomized grid of images the registering user would have to choose an image he or she will be able to remember during voting. The image grid contains simple images and the prospective voter can only choose one out of all these images to proceed. Once the user registered an image, the registration process ends and he or she is now granted approved to vote during the election. During the election, eligible voters can log-in into the e-Voting system by

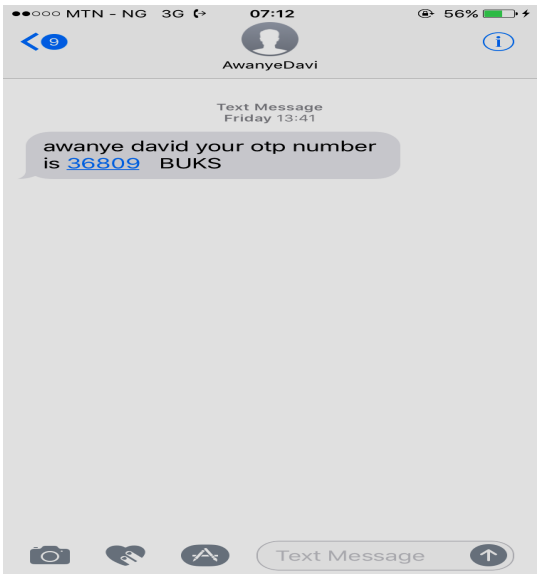

Fig. 7: Phone interface

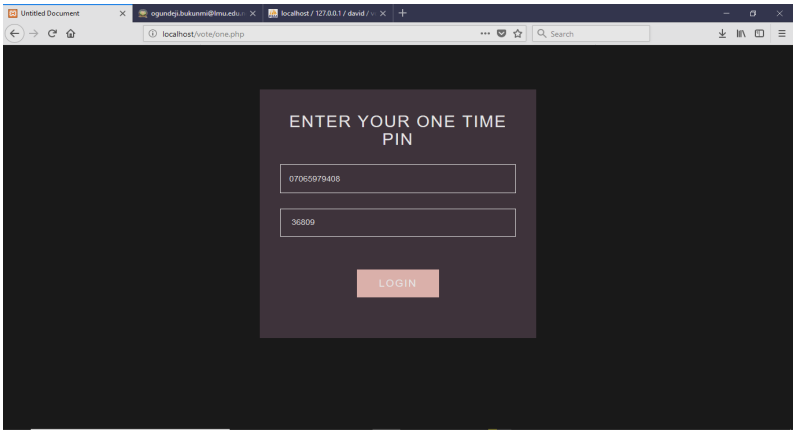

Fig. 8: Enter one-time pin interface

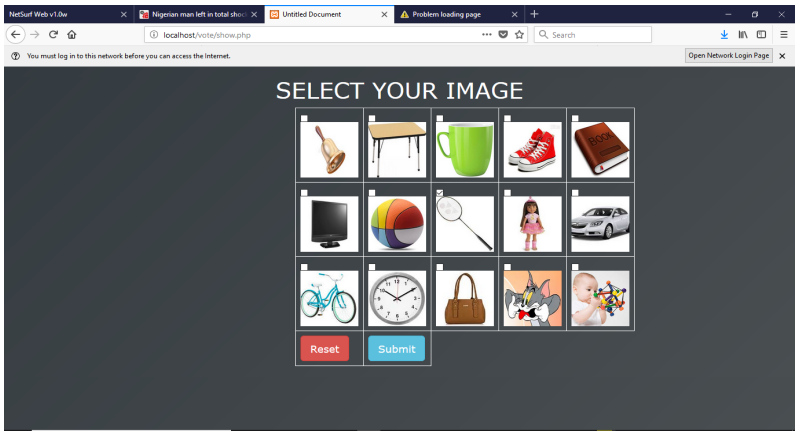

Fig. 9: Image grid interface

Fig. 10: Voters login interface

supplying email and password that was used to register into Fig. 10. The voting page in Fig. 11 provides voters with the option of selecting just a candidate to be voted for. In this prototype, it consists of the party logo, the name of the party and the name of the candidate. Image grid in Fig. 12 pops up immediately after the voter has selected a candidate that he or she would like to vote. Next, the voter would be mandated to select the same

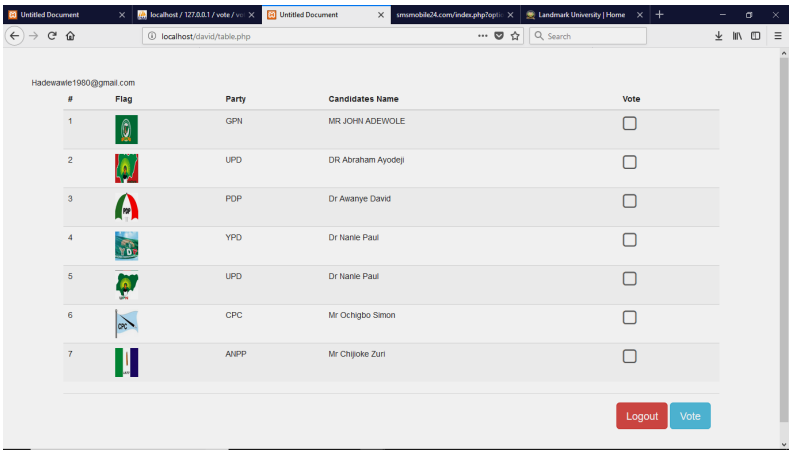

Fig. 11: Voting interface

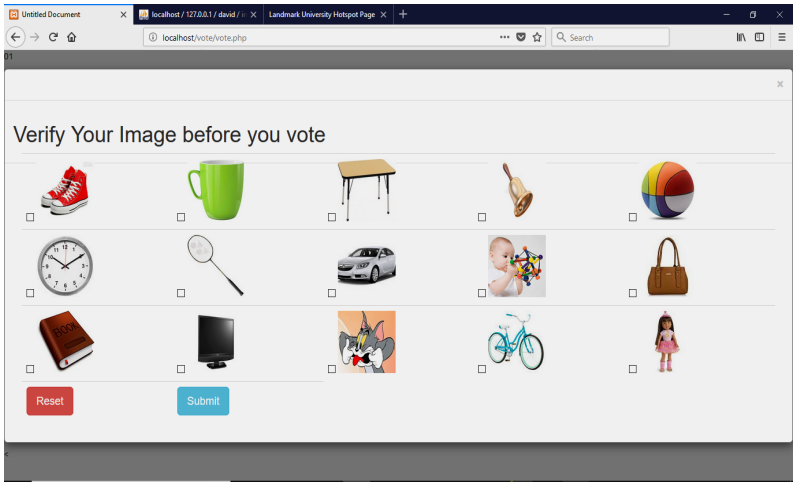

Fig. 12: Image grid interface

image that was chosen during the registration phase before his or her vote can be submitted. This helps to ensure that the vote is cast by the right person. The voter only has three trials and if the voter is unable to remember the image he or she chose during the election the vote will be void. Figure 12 loads another random set of images per voter from an image database. The randomized grid ensured that users do not have the same image grid at all times Fig. 13. The selected image at registration is always among the displayed images. If the correct image is selected, the vote is cast successfully.

Since, the multifactor authentication proposed in this research relies on user's memorability of selected images, system performance evaluation carried out captures each voter's number of attempts at selecting the right image before completing a vote. This test was carried out 30 days after user's first registration. From the analysis on

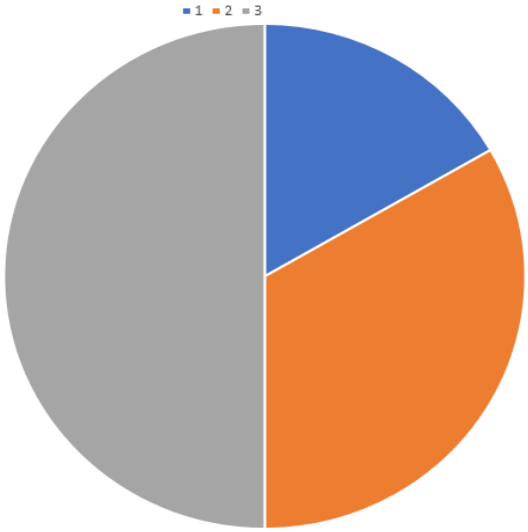

Fig. 13: Distribution of the number of attempts of image re-identification

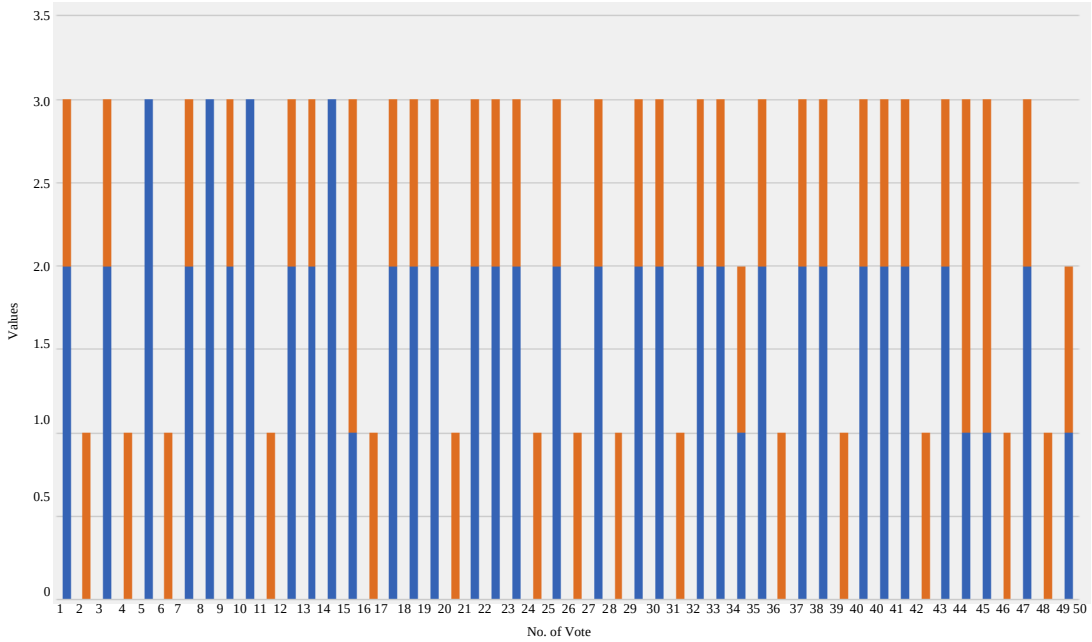

Fig. 14: Number of attempts per vote

image re-identification in Fig. 13, out of the 50 registered users 30% of the users were able to vote with just one attempt, 4% of the users voted with two attempts and 66% were able to vote successfully after with attempts. Figure 14 shows the number of attempts for each successful vote.

CONCLUSION

This research designed and implemented a system prototype for a multifactor authentication electronic voting that relies on two inputs known to the voters a password and an image. Voters have to choose an image from a grid which they must remember together with login password before they can vote successfully. The system was evaluated to test memorability and feasibility. After giving voters a total of three trials to remember their selected images, it was found out that the ability of users to remember their image on the first attempt and not to remember their chosen image on the first attempt is in the ratio 1:2. However, all the fifty register voters were able to vote successfully and this shows the proposed approach is feasible and can be improved. Future research will be conducted to understand voters preferred types of images and evaluation will include older audiences.

ACKNOWLEDGEMENT

Special thanks to Landmark University for financing this publication.

REFERENCES

AboSamra, K.M., A.A. AbdelHafez, G.M. Assassa and M.F. Mursi, 2017. A practical, secure and auditable e-Voting system. J. Inf. Sec. Appl., 36: 69-89.

Abu-Shanab, E., R. Khasawneh and I. Smadi, 2013. Authentication Mechanisms For e-Voting. In: Human-Centered System Design for Electronic Governance, Saeed, S. and C. Reddick (Eds.). IGI Global, USA., ISBN: 9781466636415, pp: 71-87.

Deshpande, M., D. Zambare, P. Mandle, K. Hankare and K. Shelke, 2015. e-Voting system for modern individual. Intl. J. Innovative Res. Sci. Technol., 1: 211-216.

Falkner, S., P. Kieseberg, D.E. Simos, C. Traxler and E. Weippl, 2014. e-Voting authentication with QR-codes. Proceedings of the 2nd International Conference on Human Aspects of Information Security, Privacy and Trust, June 22-27, 2014, Heraklion, Crete, Greece, pp: 149-159.

Hapsara, M., A. Imran and T. Turner, 2017. Beyond organizational motives of e-Government adoption: the case of e-Voting initiative in indonesian villages. Procedia Comput. Sci., 124: 362-369.

Mursi, M.F., G.M. Assassa, A.A. Abdelhafez and K.M. Abosamra, 2015. A secure and auditable cryptographic-based e-Voting scheme. Proceedings of the 2nd International Conference on Mathematics and Computers in Sciences and in Industry (MCSI), August 17, 2015, IEEE, Piscataway, New Jersey, USA., ISBN:978-1-4799-8672-9, pp: 253-262.

Nwangwu, C., 2015. Biometric voting technology and the 2015 general elections in Nigeria. Proceedings of the 2 Day National Conference on the 2015 General Elections in Nigeria: The Real Issues, July 27-28, 2015, The Electoral Institute, America, pp: 1-28.

Nyabola, N., 2017. Why did Kenyas Supreme Court annul the elections?. Al Jazeera English, Doha, Qatar. https://www.aljazeera.com/indepth/opinion/2017/09/kenya-supreme-court-annul-elections-170902115641244.html

Oke, B.A., O.M. Olaniyi, A.A. Aboaba and O.T. Arulogun, 2017. Developing multifactor authentication technique for secure electronic voting system. Proceedings of the International Conference on Computing Networking and Informatics (ICCNI), October 29-31, 2017, IEEE, Lagos, Nigeria, ISBN:978-1-5090-4643-0, pp: 1-6.

Olaniyi, O.M., T.A. Folorunso, A. Aliyu and J. Olugbenga, 2016. Design of secure electronic voting system using fingerprint biometrics and crypto-watermarking approach. Intl. J. Inf. Eng. Electron. Bus., 8: 9-17.

Omotosho, A. and J. Emuoyibofarhe, 2014. A criticism of the current security, privacy and accountability issues in electronic health records. Intl. J. Appl. Inf. Syst., 7: 11-18.

Omotosho, A., J. Emuoyibofarhe and C. Meinel, 2017. Ensuring patients privacy in a cryptographic-based- electronic health records using bio-cryptography. Intl. J. Electron. Healthcare, 9: 227-254.

Rana, A., I. Zincir and S. Basarici, 2015. The security and the credibility challenges in e-Voting systems. Proceedings of the 13th European Conference on Cyber Warfare and Security (ECCWS-2014), July 3-4, 2014, University of Piraeus, Piraeus, Greece, ISBN:978-1-910309-24-7, pp: 229-232.

Titus, A., N.P. Rajam, M. Swetha, S. Ramya, 2018. Multi-factor authentication for secure electronic balloting credentials. Intl. J. Adv. Res. Ideas. Innovations Technol., 4: 1923-1930.