Challenges & Solutions Of Adoption In Regards To Phone-Based Remote E-Voting

Hermann Ken Jamnadas, Mohammed Farik

Abstract: Remote Voting Systems has not been universally adopted by most countries for their elections such as in the case of Fiji. Although mobile phones are quite prevalent around the world and the amount of smart phones sold is increasing at a rapid rate, there have not been many elections which have capitalized on the use of Mobile Phones as a remote voting tool. This paper is a limited review of previous papers on remote voting systems. The aim was to study challenges of adoption of remote e-voting systems such as through a mobile phone and suggest innovative solutions to those challenges. As such we propose a combination of new policy solutions and technical solutions such as the use of QR code and checksum for vote verification, the use of real time facial recognition systems, and the leveraging of existing mobile hardware to ensure a secure, anonymous and trustworthy remote voting system like it has never been before.

Index Terms: Digital Divide, Internet Voting, Mobile voting, Remote E-Voting, Security, Trust, Usability

1 INTRODUCTION

E-VOTING is defined as the use of electronic computerized tools to aid in casting and counting of votes [1], [2]. The vote may be casted over the internet using a web application or a smart phone application which is referred to as internet voting [3]. This paper is focused on the use of remote e-voting which is simply the casting of votes anywhere without the direct supervision of the election supervisors with the use of internet and smart phones [1]. There are evidence of some nations moving towards the use of e-voting tools such as Estonia, Norway, Pakistan, Brazil, India and so on [2]. Many perceived benefits of e-voting in comparison with their paper based counterparts are the perceived reduction of costs in terms of printing distributing paper ballots and counting efficiency [2]. Furthermore internet voting or remote e-voting systems are more likely to be perceived as convenient compared to e-voting machines located at polling venues as they allow for remote casting of votes anywhere. Hence they are more likely to raise participation of voters in the election [4] which should be encouraged to ensure successful democracy [2], [5]. The paper presented here focus on challenges to adoption of a mobile phone based remote e-voting system and the solutions to such challenges from a limited review of papers. The paper is organized as follows. Section 2,3 and 4 describes the current problems/challenges of adopting remote e-voting systems and explains current and our innovative solutions to those problems. Section 5 describes some recommendations for future research. Section 6 ends the paper with a conclusion.

2 SECURITY PROBLEMS

2.1 Vote Verification

For any election tool used for casting votes, it is essential that such systems allows for vote verification to ensure that their votes was correctly recorded [6] especially in regards with remote e-voting such as voting through mobile phones. This is especially true in regards to ensuring votes was casted as intended without errors as was apparent in certain old voting equipment used in the 2000 American Elections that did not allow for easy vote verification resulting in higher invalid votes casted [7]. While proper design of voting technology can eliminate most voting errors such as *over-voting* (which is when voters select more than one candidate for office) or *under-voting* (which is when voters neglect to vote for a candidate for a specific office) [7], remote voting systems are most likely to involve insecure channels like the internet for casting votes [6]. Hence votes may be intercepted and delayed or stopped in a classic denial of service attack or modified by malicious attackers [6]. As such for remote voting systems there would be a need to ensure votes was successful sent and that votes was not modified. Storer *et al.* [6] study focused on a scheme designed to ensure anonymity and vote verification with the use of voting credentials provided to the voters such as *voter id*, *candidate id* and *receipt id* (receipt id is used only for vote verification purposes) for every candidate. The receipt ids are unique to every voter meaning that the same candidate for every voter will have different receipt id. Once the vote has been casted containing the voting details such as voter id and candidate id, the election office will publish a receipt id on a public website. The voter then has to compare his receipt id for the candidate he/she has chosen with the published receipt ids. If the voter is able to confirm the existence of his receipt id then the vote has been successfully casted. Anonymity according to the authors is ensured as long as voters do not share their voting credentials [6]. This scheme however poses problems such as the data initially must be stored to ensure a link between *receipt id*, *voter id* and *candidate id*, thus posing problems of

- *Hermann Ken Jamnadas is currently pursuing Postgraduate Diploma in Information Technology in The University of Fiji, E-mail: hjamnadas@hotmail.com*
- *Mohammed Farik is a Lecturer in Information Technology, in The School of Science & Technology, at The University of Fiji, E-mail: mohammedf@unifiji.ac.fj*

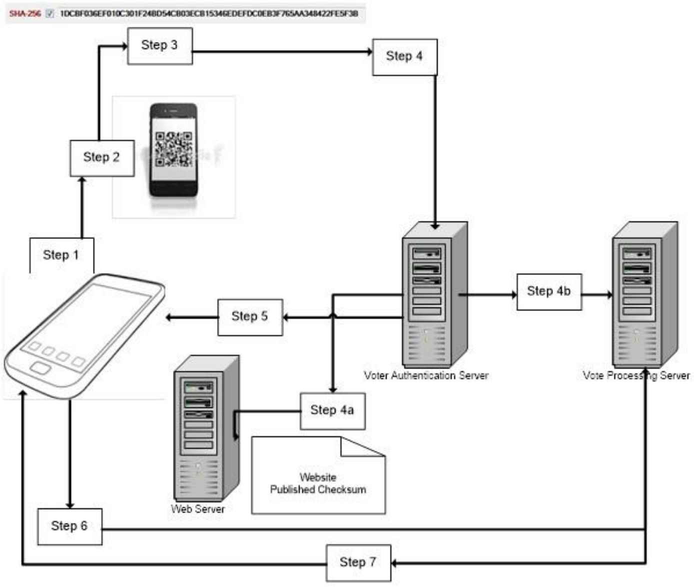

Fig. 1 *Vote Verification System using QR codes and Checksum*

anonymity if the database storing such information has been compromised or misused by election management authority employees. Meaning anyone with access to the database containing all voter credentials can use such credentials with the published *receipt id* information to figure out who voted for which candidate. We suggest that vote verification with anonymity could be done with the use of *Quick Response (QR) codes* and *checksum*. *A QR code is* a special barcode that can typically hold more information than other types of barcode [1]. Most smart phones can handle QR codes since there are free mobile applications that take advantage of the phones camera for QR code scanning [8], [9]. *Checksum* created using a hashing function, is used to check the integrity of files that was distributed to ensure files has not been corrupted or modified [10].The vote verification will be done based on a similar model proposed previously by Storer *et al*. [6] where in place of a receipt id used for verification purposes we instead use a QR code and checksum of the QR code for verification purposes, as well as an envelope model used in the Estonian remote e-voting systems for casting votes and ensuring anonymity [11]. The scheme we propose will rely on two different servers, the use of QR codes, checksums of QR codes and two different public key/ private encryptions and the envelope method used in Estonia remote e-voting system. This scheme is illustrated in Fig. 1 above.

First, the voters will first cast a vote using a mobile app. The vote itself may travel through some insecure medium such as the internet.

Second, the app will encrypt the vote details as a QR code using the public key of a server used to process and count votes (vote processing server).

Third, the app will then create a checksum of the QR code using SHA-2 or SHA-3 hash function. The App will enclose or encrypt the voter's details with the QR code in a packet using the public key of a server for voter authentication (Vote Authentication Server).

Fourth, the encrypted packet is then transmitted to the *Voter Authentication Server (VAS)* which decrypts the packet to obtain the voters details and the encrypted QR code. The *VAS* then authenticates the voter and once authenticated as a valid voter, the *VAS* calculates the checksum of the QR code and submits the checksum back to the voter's mobile app.

a. At this stage the *VAS* could also publish the checksum on a public website just like in the scheme proposed by Storer *et al*. [6] since it does not containing identifying information and the publication is only meant to assist in verification purpose. The voter can compare his checksum stored on his/her phone with the one published online.
b. Furthermore the *VAS* will then strip all identifying voter information and submit only the *QR code* containing the encrypted vote to the *Vote Processing Server (VPS*) which then reads the encrypted vote from the *QR code* and decrypts the encrypted vote and tallies the vote accordingly. The reason for the two servers is to ensure anonymity such as in the case of the *Estonian* remote E-voting system where no part of the system should have both the identifying information about voters and also the private keys to decrypt the vote information [11].

Fifth, when the mobile app has received the checksum from the *VAS* it will compare both the checksum (one it receives from the *V.A.S* and the one it calculated earlier) and if it is the same, the mobile app will then display the message that the vote was successfully delivered and was not in any way modified.

Sixth, with the *QR code* stored on the mobile phone, it can also be used to verify if the vote was for the right candidate. For example if the voter wants to check afterwards if the vote was for the right candidate, all the voter has to do is scan or upload the *QR code* from the app or other designated devices to the *VPS*.

Last, the *VPS* can then read the encrypted vote from the *QR code*, decrypt it and then transmit it back (preferably the vote information transmitted back should be encrypted with the public key of the voters).

2.2 Authentication

To ensure that the elections represent the will of voters it is essential that any voting system used for casting votes has sufficient capability to *authenticate* users as eligible voters [12], [13]. In a manual voting system, such authentication would be done by the election official at the polling venues who will verify voter's identity through some physical documentation such as voter ID cards [12]. A remote e-voting system should provide the same capability to ensure only eligible voters can vote [11]. Security issues in regards to e-voting are a prime concern and there are many possible venues of attacks which may be difficult to mitigate [12]. In regards to authentication solutions, there has been many ways to authenticate eligible voters. Jagan *et al*. [1] have proposed in their paper the use of *QR codes* for authentication purposes. The *QR code* contains voter details such as *voter id, voter name, phone number* and *password* and will be obtained by the voter after registration. After obtaining *QR code*, the voter can then use the *QR code* to authenticate himself for voting by scanning the *QR code* using the phone. In Estonia, most eligible voters are provided with an ID card with embedded smart chips that store a unique digital signature of each voter [11]. According to Maaten [11], the digital signatures are used to authenticate the voters as eligible voters. In order to use such Voter ID cards for the remote voting system it is essential that the voter has the requisite software installed on a computer as well as a card reader [11]. This raises some issues as noted by the author about digital divide where certain constituents may not have card readers, required software or the skills needed to work with digital signatures [11]. Furthermore in another paper by Ghatol & Mahale [12], they propose the use of biometrics technologies to authenticate eligible voters. Specifically fingerprints of voters will be used to help authenticate voters in remote voting systems through mobile phones [12]. All of the papers mentioned so far in the previous paragraph have not accounted for the problem of continuous or real time authentication that is since the remote voting is usually unsupervised, election officials cannot assure that the person casting the vote is the same person that was authenticated [14]. Hence we suggest the use of biometrics facial recognition to ensure continuous or rather real time authentication where we can ensure the person who is voting is the same person who was authenticated previously. This is especially relevant for mobile phones, where most smart phones come equipped with front facing cameras. While such cameras available on phones are normally low quality it does allow for some facial recognition capability [15]. However the reliance on low quality cameras to obtain recognition of user's facial features means it is possible that other people may be recognized as the authorized user or be spoofed simply with an image of the authorized user [15]. We suggest that to ensure proper facial recognition, such phones must be equipped with an infrared cameras [15]similar to Intel *RealSense* 3D camera which would allow it to sense the 3D features of faces [16] and hence avoid the problems of photos of authorized users being used to spoof facial recognition systems. Fig. 2 shows how a mobile phone equipped with a front facing infrared camera will ensure continuous or real time authentication of voters.

First the voter launches the voting application on the phone.

Second, the phone application will then capture the 3D images of the voter using the front facing infrared camera and send the data to a server which will authenticate the voter. The application will continuously send real time video feeds of the voter to the authentication server during the duration of the vote casting process.

Third, If the authentication server detects during the live feed multiple faces or different facial features than the one the voter has, the server will pause the vote process

Last, the application will then be shutdown to ensure that only the eligible voter who was authenticated initially is allowed to vote.

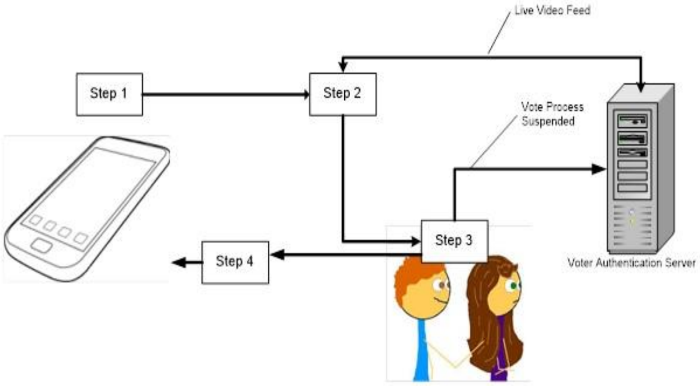

Fig. 2 Authentication System using Real Time Facial Recognition

2.3 Secrecy of Vote

Anonymity or secrecy of votes should be maintained to ensure that voters cannot be coerced or bought to vote in a certain way [14]. Furthermore if a particular voting technology is perceived as not ensuring the privacy of voters it may impair the chances of adoption of that technology [2] which is especially significant for remote voting as since remote voting is not supervised by election officials there will be no assurance that voting is done privately [11]. Some ways in which anonymity can be assured is by ensuring that the vote information and voter credentials are processed separately in different parts of the system such as in the Estonia remote e-voting system [11]. This ensures the system at no point in time, should be able to identify the voter and at the same time be able to decipher the encrypted vote information in only one part of the system [11]. Also in a remote voting scheme studied by Storer *et al*. [6], anonymity is maintained by ensuring that receipt IDs used for verification purposes cannot be tied to a particular voter or candidate unless secret voter credentials are shared by the voters themselves.

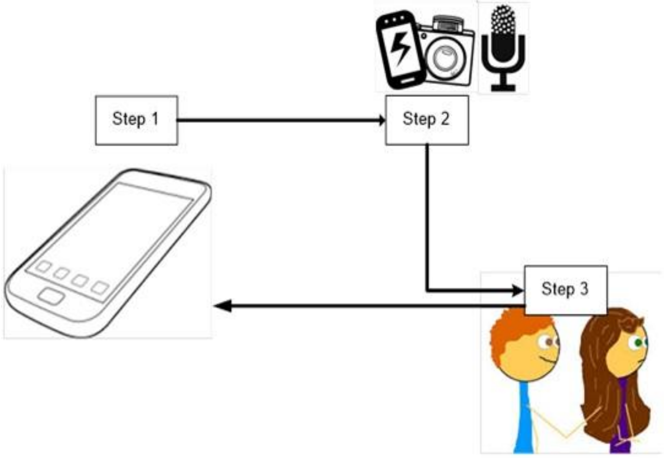

Fig. 3. *System forcing Privacy by leveraging existing phone hardware*

The methods discussed in the previous method in no way ensures that such remote e-voting takes place in a private setting such as in the case of a supervised voting where election officials can force voters to vote alone in a privately secured voting booth [11]. We suggest that we can leverage the existing microphone and camera features of mobile phones to ensure that voters can only vote in such a private setting. Fig. 3 above illustrates how this feature would ensure anonymity or secrecy of vote.

First the voter attempts to vote by launching the required voting application.

Second, the application will access the video capturing and audio capturing devices of the phone. Both front facing cameras and rear facing cameras are used to capture live video feeds. At the same time the microphone can be used by the application to capture live audio feeds.

Third, if both cameras and audio capturing devices indicate the presence of multiple people in close proximity in the room, the voting application can pause the voting process and minimize the application such as if someone looks over the voter's shoulder while he/she is voting.

2. 4 Mobile Phone Software Vulnerability

There is an increasing problem of viruses and Trojan horses designed for mobile phones which can compromise the integrity of the mobile phone as a voting tool [17]. Furthermore such remote voting systems are highly dependent on the security design of mobile voting applications and other software such as Operating Systems [18]. We suggest that voters can install special antivirus software for their mobile phones. An example of a mobile phone antivirus software can be found at: https://play.google.com/store/apps/details?id=com.antivirus&hl=en).

3 TRUST PROBLEMS

Trust by voters and election stakeholders in the results and process of the elections is very important to ensure legitimacy and successful democracy [13]. The election results should be able to be trusted by stakeholders (including voters) to reflect the will of the voters [13].

3.1 Trust in Government Agency Overseeing Elections

As such any stakeholders in the election such as voters, political parties and others must be able trust in the independence and neutrality of the agency tasked with overseeing the elections [13]. According to one paper the intention to adopt or participate in the use of a voting technology can influence whether a voter will participate in the election [19]. If there is any mistrust by the electorate, then adoption of any election technology (or any election reform for that matter) such as remote voting technologies will be looked on with suspicion, resistance or non-participation by the election stakeholders [13].Results of the election are also more likely to be questioned and challenged by the participants such as by voters and competing parties [13]. One way in which the election management authority may be looked with suspicion is if the members or people in-charge of supervision of the authority is appointed by the head of state or head of government [13]. That is instead of the executive members chosen through a consultative process perhaps through scrutiny of the parliament which would ensure a more balanced membership, the members are instead appointed by one party (specifically the president who is from one party) who might ensure the authority is filled with members sympathetic to that party. Kimbi *et al*. [13] has suggested that trust can be increased in the government body tasked with overseeing the elections by ensuring that personnel charged with supervising the election management authority be independent and not be appointed only by the president but through a consultative process involving the parliament.

3.2 Trust in Remote Voting Systems

User perception of benefits and obstacles of voting technology can influence adoption of any voting technology [2]. Hence previous knowledge and experience of electronic systems that have been plagued by security and privacy issues may adversely affect the voters' perception of the security and privacy protections of remote electronic voting [2] such as voting through a mobile phone platform. We suggest that to improve the voters trust in remote voting technologies, it is essential to demonstrate how privacy and security of the remote voting system is ensured. This can be done through education campaigns by government and by ensuring the system can be tested either by experts or directly by the voters themselves. For example, voters when registering with election officials can be guided through a demonstration of how the remote voting system works on the mobile phone platform. The demonstration will achieve several objectives, one namely that familiarity of the system will be acquired if the voter is shown how the vote is done and second that voters will see the security features of the system themselves.

4 OTHER PROBLEMS

4.1 Increasing Convenience of Voting Vs Turnout

Voting is an important component for any democracy and to ensure successful democracy, voter participation should be highly encouraged [2]. One of the reasons for adopting new forms of election technologies and methods such as absentee voting or remote voting is to boost voter turnout or participation by increasing the convenience of voting [5]. This has logically been assumed to boost voter participation by decreasing the costs and complexity of voting (time and effort taken to vote), such as ease of registrations and alternative ways to vote. However one study suggests that alternative voting methods designed to boost voter turnout may not actually significantly improve voter participation [5]. This has relevance to the use of mobile phones as an election tool to boost voter turnout. Fitzgerald [5] has suggested that the only way to significantly boost voter turnout is through increasing voter interest and resources of such voters in elections. The more interest and resources a voter has towards an election the more likely a voter is likely to exert effort to participate and vote. This has been correlated with another study by Bakon & Ward [3] whereby a person involvement or interest in politics is relevant to their adoption or use of any e-voting tool including remote voting systems through mobile phones.

4.2 Usability

Usability of any voting system is important for a successful democratic election as it affects how users understand ballot information displayed and how to use the system, thus affecting the accuracy and timeliness of their votes casted. This has been apparent in certain elections such as in the case of the 2000 Presidential Elections (in United States of America) where the use of the voting systems of that time may have adversely affected the results of the elections due to significant voter troubles with the voting systems used that time [20]. In the case of smart phones as an election voting tool, there has not been as much studies conducted on the usability of such devices for remote voting [20]. There is an assumption that the use of voter's own smart phones for remote casting of votes would be more usable and familiar (since they would be using these device frequently) in comparison with other tools/methods specifically tailored for casting votes (since they would most likely be using such tools infrequently). However surveys conducted previously may suggest that older voters may prefer traditional paper ballot forms of voting in comparison with newer electronic forms of voting [20]. Moreover there are other issues to consider such as the diverse range of phones, frequent introduction and turnover of mobile technologies, small screen size, awkward data entry and potentially slow or congested networks [20]. Moreover there are perceptions or concerns that education levels of voters may influence the difficulty of using remote voting technologies for casting votes especially for illiterate citizens and elderly [2]. In an experiment conducted by Campbell *et al*. [20], it was discovered that a proposed *mobile voting system* (MVS) on smart phones was easier to use (more effective in terms of reduced errors) and faster (more efficient in terms of time to cast votes) for educated and owners of smart phones in contrast with less educated or non-owners of smart phones. However in comparison with non-mobile systems it was found that users took longer to cast a vote on MVS [20]. To avoid errors of omission, the authors Campbell *et al*. [20] elected to ensure that multiple contests were shown on separate screens(due to small screen size) and the button to advance and submit votes were placed at the bottom forcing users to scroll down the screen. However we suggest that this could have been improved with the use of bigger screens as the trends of mobile phone production and adoption seems to be towards bigger screens as evident by the introduction of *phablet* type of phones by a number of manufacturers. A *phablet* is a phone which is between the size of a normal phone and a tablet hence the term *phablet*. Examples of *phablets* can be found at: https://www.google.com/search?q=phablet&source=lnms&tbm=isch&sa=X&ved=0CAkQ_AUoA2oVChMItuO50o6SyAIVYiqmCh22iQCw&biw=1536&bih=755 . Furthermore with the smart phone market increasing, it is more likely that nearly all population including the older voters would become more familiar with smart phones. To improve familiarity and understanding of the mobile voting system, we can ensure that election officials allow or take people through a demonstration of the mobile voting system. This can be done when people come for face to face registration. We also suggest that governments ensure that IT courses are introduced as early as primary school level to ensure familiarity of computer technologies. Governments may also ensure that free workshops on the use of computer and mobile phones apps are available for the elderly.

4.3 Digital Divide

Equality is an important concept for any election where every voter has an equal chance to vote and every candidate has an equal opportunity to be elected [13]. Introduction of remote electronic voting is most likely to create unequal opportunities for voters due to the digital divide where financially affluent citizens are most likely to be able to afford and use the technologies required for remote voting in comparison with less affluent voters who may not be able to afford and hence not able to participate in remote voting [13]. In fact voters who are familiar with online banking and use of online services are more likely to view remote e-voting as consistent with how they interact with other people and organizations [2] and hence concurrently those that are not familiar with such technologies would not view e-voting as consistent with how they interact with other parties. According to Maaten [11] steps undertaken to reduce digital divide involve free education on the use of computers and internet. Furthermore this has been supplemented with increasing access to internet and computer services through provision of computers with relevant software and equipment and internet access in public libraries [11]. It must also be emphasized that remote voting systems should act as a supplement to other methods to cast a vote and not the dominant method of voting due to digital divide issues [11]. We suggest that some other ways to reduce the digital divide especially in regards to remote-voting through mobile phones is the supply of free phones with requisite software and hardware to poor communities. This can also be provided at the polling venue. Furthermore to ensure familiarity with the concept of online services, the government can ensure welfare payments and other services provided to poorer constituents are offered online which can be accessed with a free government mandated phone with requisite software and hardware included. During voter registrations with election officials, voters may also be shown and demonstrated the process of voting using a mobile phone. The voter himself/herself may participate with a test or demo mode of the remote voting system and made familiar with the remote voting system through mobile phones.

4.4 IT Skill & Sufficient Training of Election Officials

The election management authority must have sufficient personnel with the requisite IT skills and training to properly maintain and implement a remote voting system [13] such as voting through mobile phone platforms. Insufficient training of election officials tasked with overseeing the election may cause unnecessary delays or problems such as in the 2009 South African Elections where misunderstandings about the counting process and the correct procedures to follow led to delays [2]. As suggested by Kinbi *et al*. [13] training and development of the required IT skills must be increased to support deployment and maintenance of remote voting systems. We suggest that this can be done through scholarships and deployment of personnel in the IT department of the Election Management Authority to relevant IT workshops as well funding attachment with election authorities of countries that have successfully implemented some form of remote voting such as Estonia [3] to learn from their election authority's IT department.

5 Recommendations for Future work

This paper is a limited review focused on identifying problems that pose as an obstruction to the adoption of remote e-voting systems through mobile phones. Hence not all problems may have been taken into account. In reference to some of the technical solutions suggested for security related problems, additional research will need to be carried out to address their feasibility. Moreover findings of this research can be adopted by the constituents and relevant election stakeholders in future elections.

6 CONCLUSION

One of the greatest *concerns* of election officials in regards to remote e-voting systems is the issue of security. Many e-voting projects have failed due to problems of security. This is apparent by the number of problems that are related to security such as secrecy of vote, authentication, mobile software vulnerabilities, and vote verification. While problems such as *Digital Divide*, Trust in Election authority and Training level of election officials can be solved with simple policy, administrative and legislative changes, other problems such as Security are likely to involve some technical solutions. We believe that the technical solutions we suggested in combination will ensure a secure, convenient, anonymous and trustworthy remote e-voting system based through mobile phones. This will however need to be tested in future research for technical and operational feasibility.

REFERENCES

[1] A Jagan, P Akila, and N Nasrin, "QR Code Based E-voting System Using an Android Smart Phones," International Journal of Emerging Technology in Computer Science & Electronics, vol. 13, no. 2, pp. 263-267, March 2015.

[2] M. Achieng and E. Ruhode, "The Adoption and Challenges of Electronic Voting Technologies Within the South African Context," International Journal of Managing Information Technology, vol. 5, no. 4, pp. 1-12, November 2013.

[3] K.A. Bakon and T. Ward, "Web 2.0 And Elections: A Study Of Factors Influencing Diaspora Voters Adoption Of E-Voting System," International Journal Of International Systems And Engineering, vol. 1, no. 1, pp. 1-9, April 2015.

[4] R. Krimmer and Volkamer, "Bits or Paper? Comparing Remote Electronic Voting to Postal Voting," in EGOV (Workshops and Posters), 2005, pp. 225-232.

[5] M. Fitzgerald, "Greater Convenience But Not Greater Turnout The Impact of Alternative Voting Methods on Electoral Participation in the United States," American Politics Research, vol. 33, no. 6, pp. 842-867, November 2005.

[6] T. Storer, L. Little, and I. Duncan. (2006, June) ResearchGate. [Online]. http://www.researchgate.net/profile/Ishbel_Duncan/publication/250889738_An_Exploratory_Study_of_Voter_attitudes_towards_a_Pollsterless_Remote_Voting_System/links/5447aac90cf22b3c14e0f845.pdf

[7] M. Tomz and R.P.V. Houweling, "How Does Voting Equipment Affect the Racial Gap in Voided Ballots?," American Journal of Political Science, vol. 47, no. 1, pp. 46-60, January 2003.

[8] Denso Wave Incorporated. History of QR Code. [Online]. www.qrcode.com/en/history

[9] Wikimedia Foundation. (2015) or Code. [Online]. https://en.wikipedia.org/wiki/QR_code

[10] A. Kishore. (2015) What is a Checksum and How to Calculate a Checksum. [Online]. www.online-tech-tips.com/cool-websites/what-is-checksum/

[11] R. Maaten, "Towards remote e-voting: Estonian case," Electronic Voting in Europe, vol. 47, pp. 83-100, 2004.

[12] P.S. Ghatol and N. Mahale, "Biometrics Technology Based Mobile Voting Machine," International Journal of Computer Sciences and Engineering, vol. 2, no. 8, pp. 45-49, August 2014.

[13] S. Kimbi, Y. Nkansah-Gyekye, and K. Michael, "Towards A Secure Remote Electronic Voting in Tanzania Organizational Challenges," Advances in Computer Science: an International Journal, vol. 3, no. 5, pp. 122-131, September 2014.

[14] M.R. Clarkson, S. Chong, and A.C. Myers, "Civitas: A Secure Remote Voting System," Cornell University, Technical Report 2007.

[15] D. Goldman. (2015) Microsoft will let you unlock Windows 10 with your face. [Online]. http://money.cnn.com/2015/03/18/technology/windows-hello-microsoft-face/

[16] A. Piltch. (2015) Intel RealSense 3D: What It Is and What You Do With It. [Online]. http://www.tomsguide.com/us/intel-realsense-guide,news-20286.html

[17] W. Enck, M. Ongtang, and P. McDaniel, "Mitigating Android Software Misuse Before It Happens," The Pennsylvania State University, Technical Report 2008.

[18] S. Estehghari and Y. Desmedt, "Exploiting the Client Vulnerabilities in Internet E-Voting Systems: Hacking Helios 2.0 as an Example," in EVT/WOTE 10, 2010, pp. 1-9.

[19] Z. Irani, P.E.D Love, and A. Montazemi, "e-Government: past, present and future," European Journal of Information Systems, vol. 16, no. 2, pp. 103-105, 2007.

[20] B.A. Campbell, C.C. Tossell, M.D. Byrne, and P. Kortum, "Toward More Useable Electronic Voting: Testing the Usability of a Smartphone Voting System," Human Factors, vol. 56, no. 5, pp. 973-985, 2014.