Transforming Voting Paradigm – The Shift From Inline Through Online To Mobile Voting

Thakur, S., Olugbara, O.O., Millham, R.
Department of Information Technology
Durban University of Technology
Durban, South Africa

Wesso, H.W., Sharif, M.
iKamva National e-Skills Institute
Department of Communications
Pretoria, South Africa

Abstract— **Traditional poll-site voting methods poise multiple administrative and logistical challenges inter alia scalability, cost and miscount. Moreover, there is a noticeable decline in the turnout rate of eligible voters, particularly the youth. This work proposes a novel mobile voting model that uses common-off-the-shelf (COTS) mobile phones, in conjunction with a Near Field Communication (NFC) tag technology and a pragmatic biometric verification scheme. The mobile voting application being proposed in this work is launched by leveraging the auto-coupling capability of NFC, which also serves for storing baseline information about voters. The auto-coupling feature mediates device familiarity requirement, which is a limiting factor for using mobile phones to administer elections satisfying transparency and ease of use. The baseline information stored in the NFC tag provides local biometric reference data that mediate intensive bandwidth consumption, computational requirement, provide for match-on-a-card features and satisfy the constraint that only the eligible voter may vote. This work notes all security requirements for this model and addresses some architecture, design and security issues that will arise if such a choice is made.**

Keywords— **biometric; mobile; tag; voting**

I. INTRODUCTION

In this paper, we systematically delineate the evolution of voting practices from ancient times in order to put in context, the challenges and opportunities that each development introduces. An electronic voting system (e-voting) is an integrated device that uses electronic components to perform one or more of the following functions - ballot presentation, vote capturing, vote recording and vote tabulation [1]. E-voting introduces technology, which impacts transparency, ease of use, auditability and has further costly requirements such as developmental cost, electricity and training overheads.

An engineering requirements method is used to develop the e-voting model using Commercial Off-The-Shelf (COTS) mobile phones to enhance transparency because of device familiarity to voters. The other concurrent reasons for this innovation, include an opportunity to engage with voters through the use of technology they understand, thereby permitting voter mobility, addressing shut-in voters and mediating deployed distant voters such as diplomats, nomads, military and diaspora. The innovative contribution of this study is leveraging the unique electronic storage capability and the auto-coupling feature of the Near Field Communication (NFC) tag technology along with biometric verification. NFC is a short-range, standards-based wireless connectivity technology that uses magnetic field induction to enable automatic seamless communication between electronic devices in a close proximity. This enables users to perform intuitive, safe, contactless transactions, access digital contents and connect electronic devices by simply touching or bringing devices in a close proximity [2, 3]. Auto-coupling is an important ingenious feature of NFC that removes all navigation skills. The Electoral Management Board (EMB) purchases, prepares, enables and affixes the NFC tag onto an Identity (ID) document to automatically launch the voting application. In addition, the NFC is used to store voter biometric data for a local comparative test during a remote server connection, thereby reducing traffic while retaining voter authentication integrity.

978-1-4799-4998-4/14/$31.00 ©2014 IEEE

II. THE EVOLUTION OF VOTING SYSTEM

The original practice of voting was by showing of hands or vocal votes (viva voce, pre-Industrial era). This was adjudged a transparent practice, which regrettably allowed coercion of voters. The voting process progressed, through systemisation, by the use of ballot tokens such as broken pottery (ostraka, ancient Greece), black and white balls (Ballotta, Renaissance), palm leaves (Panai olai, 900 A.D. India) and paper (Australian paper ballot, Industrial era). These mechanisms introduced challenges to the illiterates inter alia, scalability and slow tabulation. These tokens positively introduced voter secrecy and ease of use [4, 5, 6, 7, 8].

Large scale elections became unwieldy to administer as population sizes increased [9]. This led to the mechanisation of voting - mostly in the United States of America (USA) - with the introduction of lever machines, which introduced new challenges such as logistics, equipment failure, and training requirements, while removing transparency. The increasing prevalence of computers led to the automation of votes through programmed computers. This signaled the advent of the e-voting era [5].

Punch card systems employ cards and a small clipboard-sized device for recording votes. In using these systems, voters punch holes in the cards (with a supplied punch device) opposite the choice of their candidates. This may be tabulated electronically or by hand at the poll-site. Punch cards, for a while, were perceived to reintroduce transparency and auditability with a paper trail mechanism [5]. This beneficially

introduced tallying speed and automatic ballot count, removed voter monitoring, mediated voting irregularities such as ballot stuffing, ballot interpretation, chain voting and finally prevented over voting. On the other hand, it detrimentally removed both transparency and auditability [6]. Nevertheless, the events of the 2000 USA elections in Florida challenged the persistent use of the punch machines for voting. Here, many deployed punch systems, did not punch holes clearly on the ballot, leading to hanging portions now famously called hanging, dimpled or pregnant chads. This further led to legal interpretative challenges of over voter intent. This was exacerbated by the poor ballot design, famously referred to as the butterfly ballot [10].

The next evolution of voting systems is the Optical Scan System (OSS), which combined an automated vote capturing system with a vote counting system and gained prominence in the 1970s. The OSS intrinsically resolved the security problem of auditability, provided speed and transparency while conversely introducing added cost, complexity and maintenance [11, 12].

The Americans and the Dutch began the development and deployment of computer-based e-voting terminals referred to as Digital Recording Electronic (DRE) equipment. DREs are called Electronic Voting Machine (EVM) in India, while the Brazilians refer to them as urnas, with the Filipino naming them PreCinct Optical Scan (PCOS) [9]. The DRE/EVM is a programmed device that operates as a vote capturing terminal [12]. An immediate problem was that the votes were captured and a black box result was produced by the lack of a paper trail. This led to Mercuri [13] proposing a Voter Verifiable Audit Trail (VVAT), which is a printed equivalent of the computer choice for voters. EVMs with VVAT are now being implemented in some parts of India, many parts of the USA and across the world.

The progression of desktop computing to web-based applications led to further innovations for creating two fundamental streams of e-voting systems. These are controlled voting, sometimes called poll-site e-voting and uncontrolled voting, also referred to as remote e-voting, remote site voting or Internet voting. A controlled voting environment is a secure area that the Electoral Management Board (EMB) temporarily sets up, by installing equipment and implementing a clearly defined process flow [6]. An uncontrolled voting environment refers to the possibility of a voter to remotely access a system from own locality and successfully registering a vote [10]. Norway and Estonia are two countries that allow for Internet voting [9]. The voting on a mobile is a very special form of e-voting called uncontrolled voting.

III. A Case for M-voting

This work refers to mobile internet voting as m-voting for convenience. Mursi, Assassa, Abdelhafez and Abo Samra [14] compiled a wide-ranging list of twenty-six security requirements that an e-voting system must satisfy. Some of these requirements unavoidably conflict with each other. For example vote secrecy conflicts with auditability. Their security requirements are eligibility, authentication, uniqueness, privacy, convenience, transparency, fairness, incoerciblity, accuracy, soundness, verifiability, integrity, robustness, flexibility, reliability, auditability and scalability. Many of these security requirements render the traditional paper based voting untrustworthy. As a result, an overarching critical success factor in adopting e-voting has been the ability of machines to unemotionally mediate vexing impediments confronting voters. This refers in particular to stakeholders such as the elderly, illiterate, unilingual, deployed citizens, nomads and disabled.

EVMs introduced speed and accuracy, as well as computer-related challenges such as software bugs, denial-of-service attacks, security, auditability [15] and off-grid challenges such as power, usability, and access [9]. In addition, these traditional election technologies are context sensitive, they do not support user mobility and appear to benefit certain countries [16]. Processing speed and accuracy of results are not the only reasons for considering e-voting. The voter turnout is dropping for reasons such as apathy, contentment, anger, boycott, disengagement, disinterest or fear [9]. For example, it is increasingly apparent that the youth are participating less in elections than other demographic groups. Allen [17] believes that youth participation will improve with e-voting, asserting that “for a democracy to command respect, it must operate in the same way as people do everything else in their lives”. A survey of 1,200 Canadians by Goodman at Carlton University [18] established that young citizens would vote online, if provided with an Internet option.

The use of e-voting systems has demonstrated marginal improvement in voter turnout in India since EVMs were adopted in 1961, which is a reversal of the worldwide declining trend. In India - the world’s largest democracy - with 741 million registered voters, e-voting is almost obligatory. The Indians point out that EVMs help the illiterate to vote more easily [19]. In India, far from introducing a digital divide, the introduction of EVMs assisted elderly and illiterate voters as they only had to press a button next to the party colours. This avoided the challenge of literacy, the non-trivial requirement of folding the ballot paper six times and the multi-lingual design challenge in this democratic behemoth [9]. In other measures to increase voter turnout or voter participation in local government (Panchayati Raj) Gujarat made voting compulsory and has considered SMS voting and Internet voting [20]. The introduction of the None-Of-The-Above (NOTA) vote is an innovation that offers the Indian voter the choice to participate while democratically rejecting all candidates [21].

No country in Africa uses e-voting, although Kenya and Namibia have made legislative changes to use e-voting systems. Many countries have, however, introduced the Information Communication Technology (ICT) in their election cycle, for voter registration and/or transmission of tallied paper ballot results. The Independent Electoral Commission (IEC) of South Africa is considering e-voting as part of its core electoral obligations to continually assess voting and counting technologies for future elections [9]. This e-voting decision was presented and extensively discussed at an IEC hosted seminar on electronic voting and counting technologies in Cape Town [22]. The IEC, in a neutral

analysis concluded that paper remains the gold standard of voting in South Africa, given the lack of serious election related violence as well as perceived free and fair elections accepted by stakeholders [9].

Despite the lack of election-related violence, the ensuing period saw at least 112 increasingly confrontational service delivery protests, aimed primarily at councilors, in 2013, suggesting a more demanding citizenry participation [23]. M-voting may encourage direct, local democracy and possibly mediates such tragedies. In order to support democracy, the costs of voter registration, casting and tallying ballots as well as resolving electoral disputes must be met by donor funding, which is increasingly becoming a constraint.

The United Nations Development Programme (UNDP) has spent 1.2 USD billion in the last 12 years supporting democracy. This budget was primarily utilised to purchase equipment for voter registration drives to create a voters roll for electoral efficiency and to mediate electoral fraud such as ballot stuffing. A legacy benefit of this exercise has been the establishment of core adult population register in recipient countries. In fact, the use of NFC for voter biometric capturing and storing will significantly save money to the UNDP, for voter registration. The reason being that capturing the pictures of voters as part of this process requires expensive printers and costly Polaroid quality paper [24, 25].

In general, m-voting offers the following advantages:

- Possible reduction or even elimination of costs of printing and transporting paper ballots [26]. South Africa used 460 tonnes of papers in the 2009 elections (IEC, 2011) while India used 12,000 tonnes of papers to run its last paper-based election in 1996 [19].
- Mobile phone ubiquity is an irresistible medium to engage the youth or digital natives, the rural and even the elderly in elections, irrespective of their geographical locations and specific segments of the population, such as diplomats, soldiers, healthcare workers, nomads and increasingly influential diasporas who cannot make it to the poll-sites [9].
- Mediation of voter mobility or flow because it offers a platform for voting anywhere, anytime and at one's convenience [10]. The world is fast reaching the so-called mobile moment when the number of mobile phones equals the number of people on the planet.
- May be specially designed to assist blind, partially sighted voters and voters with mobility impairments, to cast their vote by allowing access from their own habitats. In this context, it can also help the elderly and disabled who may unable or disinclined to travel.
- Offers multi-lingual instructions without increased printing costs and it eliminates language bigotry.
- Facilitates the concept of Bring-Your-Own-Device (BYOD), which serves to reduce implementation costs.
- Mitigates tempest attacks, which is the electronic monitoring of radiation of voting screens to capture image and therefore monitor the vote, one of the reasons the Dutch stopped e-voting.

However, the challenge of m-voting is a complete national communication infrastructure to prevent perceived regional discrimination or bias. South Africa, like most countries has extensive Global Systems for Mobile (GSM) communication coverage, which is close to 100 percent. But base stations can be installed in areas that do not have coverage, providing a legacy benefit to marginalized disconnected communities, adding perceived value to the electoral process. Consequently, any e-voting model must imaginatively address funding, transparency, ease of use, youth re-engagement, disabled, elderly, language barriers and must be socially or culturally sensitive. But, it is acknowledged that m-voting will mediate some requirements and introduce other quandaries.

IV. Requirements for M-voting Models

M-voting represents a voting methodology, which accentuates challenges such as remote voter verification and secure transmission of votes. A very simplified process of m-voting is - a voter starts his/her mobile phone, launches the voting application, proves his/her identity, casts his/her vote, commits the vote, transmits the vote and quits the application gracefully.

The work at hand, consequently establishes the following overarching requirements to address certain security challenges of e-voting:

- The device must be familiar in look and feel to a wide range of voters. The COTS base device must be easily configurable for voting applications, including software and hardware applications. The device familiarity builds trust and promotes transparency as opposed to a black box solution while using COTS components that make many aspects of the solution open with respect to hardware architecture corresponding with the voting evolution and the reusability analogy as previously discussed. This mediates ease of use, cost-effectiveness, convenience and voter mobility.
- There should be some process to inculcate a ceremony or a ritual towards reflecting the somber act of voting. The NFC token on the ID is a deliberate choice to engender this, which will be reinforced by marketing.
- The process must minimise internet traffic consumption and massive short burst traffic that could arise, especially by voters who are traditionally voting in the eleventh hour. This impacts scalability, practicality and soundness as mobile traffic will be generated. This is achieved by the match-on-the card offering.
- The voters may "bring their own devices" in case they prefer to vote at the poll-site according to the BYOD

principle or choose a device at the poll-site. This mediates reliability and removes black-box related suspicion.

- An independent auditor may either choose a device at a poll-site to audit or apply the BYOD principle to perform parallel auditing. This enhances stakeholder perception of transparency.

V. Components of Our M-voting System

Given the requirements of our model, the proposed system begins with the authentication of a remote voter. In m-voting, the burden of verifiable proof by a remote natural person or a voter renders authentication by the EMB non-trivial. The EMB's requirement is zero deception for all voters, not an acceptable statistical error rate, even though impersonation is a real possibility.

A useful method to almost eliminate voter deception is the use of biometrics. The suggestion that biometric technology provides a more accurate and easy authentication mechanism is supported by a joint PayPal and National Cyber Security Alliance (NCSA) study, where it was found that mobile users were happy with biometric authentication [27]. This introduced the phrase - "your body is the new password." Indeed Khelifi and Shastry [28] suggest the tipping point for mobile adoption in elections to be the progress in (mobile) phone biometric security, suggesting that more people will be tempted to vote.

This mobile biometric verification assurance is based on four separate degrees of confidence comprising traditional systems, which are possessions (what you have), knowledge (what you know), geographical positioning (where you are) and behaviour (what you did). One can add a physiological biometric when cell phones can execute better real-time fingerprint or facial capturing [8]. We have used a multimodal method to aid voter verification, prevent impersonation, mediate coercion and generate solemnity while simultaneously building voter confidence. The Global Positioning System (GPS) feature of a mobile phone ensures voting within the border of the country (geographic confidence) and is an excellent feature to mitigate coordinated (wilful or playful) offshore attacks from hackers.

The multimodal technology of our mobile voting system offers an opportunity to engender respect in a manner that is sensitive to indigenous norms and customs. For example, in some countries touching or photographing an individual, is a taboo. This is encapsulated in the idiom "you take my picture you capture my soul." Women in some contexts may not remove their hajib (or headscarf), while men in other contexts may not remove their dastar (or turbans). These criteria render biometric applications based on fingerprints and photographs problematic, providing a compelling pragmatic case for contextual multimodal solutions.

A. *Voice Biometrics*

The voice or speech authentication attempts to verify that an individual speaker is, in fact, who he/she claimed to be. This is normally accomplished by comparing the voice feature of an individual with a previously recorded "voiceprint" sample of the person's speech. This voiceprint is created, by asking a physical voter to repeat or read a few random expressions in a controlled environment such as during voter registration. This mediates the recording and subsequent fraudulent reuse of a voice biometrics. This is called a "proof of life" test, which has the significant benefit of mediating computer generated login attempts [29].

The recognition based on voice recognition must be contrasted with speech recognition, which refers to what a person says (content) as opposed to who said it (speaker). Voice offers a familiar, non-invasive, non-threatening and a culturally deferential method of capturing voter's biometric. Voice is not as obtrusive or invasive as retinal and finger biometrics. The key strengths of voice recognition are its ability to conduct enrolment and verification without sophisticated equipment and its lack of negative connotations, such as those (perhaps unfairly) currently associated with fingerprints for criminality and iris for discomfort [30].

An important contextual development has been that the South African government has accepted voice as a secure biometric for person recognition. It announced that it will use voice to certify several million of pensioners. The previous system had a high percentage of ghost beneficiaries, with no secure, accurate and beneficiary verification for proof of life [31].

B. *Fingerprint and Face Biometrics*

The fingerprint has been established through a recognition system called Automatic Fingerprint Information System (AFIS). Common challenges during the process of biometric capturing were unreadable prints of old people and physical labourers (for example, the miners and the farm workers) make fingerprint application difficult. This introduces certain exceptions known as False Acceptance Rates (FAR), where an invalid print through error or subterfuge is accepted and False Rejection Rates (FRR), where a valid print is similarly rejected. Fingerprint has associated social and cultural issues and may suffer from gummy finger attacks, especially when the voter has much time. Harris [32] reflects on 'an unspeakable irony, a challenge that Sierra Leone voter ID biometrics collector is facing is how to get fingerprints from people whose hands were cut off.' This strengthens the case for multimodal authentication, if fingerprint must be used. The Apple 5s application is the first mobile technology to allow for fingerprint authentication and has already been hacked on the day after the launch, although the hacker, Rogers [33] still believes in finger biometrics. The European Association for Biometrics (EAB) lauded the 5S development as 'heralding a paradigm shift' although they caution about privacy issues [34].

The face modality is considered to be the most commonly used biometric trait by humans. Hence, it is almost a standard practice to incorporate face photographs in various tokens of authentication such as ID cards, passports and driver's licenses. Face has several advantages that make it a preferable choice in many biometric applications. Face, unlike

fingerprint, can be captured at a longer standoff distance using non-contact sensors. On the other hand, the burka, hajib, dastar, which vary in style, drastically impact facial recognition systems. This biometric may be used to discriminate against these and other faith-based garment wearers. It has been shown that you could take a photo of someone and put it in front of the phone to unlock it (illegal impersonation). Although security vendors are researching this using options such as video, as opposed to still photos, or human motion, rather than someone absolutely still [35]. However, the process of automated face recognition is beset with several challenges such as variations in age, pose, illumination and facial expressions and it exhibits changes in appearance because of makeup, facial hair or accessories. The inter-class similarities further compounds the difficulty of recognizing people based on their faces.

C. *Near Field Communication*

The auto-coupling software feature implies no matter the state of a mobile phone when bringing it into contact with an NFC, it will instantly launch the software encoded in the tag. This, in a sense, temporarily converts the mobile phone into an EVM or DRE automatically with little or no navigational skills on the phone or its features needed by a user.

A further benefit is that the NFC may be retrofitted to any current national ID system in a non-disruptive manner. The NFC may be printed with a hologram making it cheaper and less susceptible to fraudulent duplication. An important feature of a developing country is the rapid urbanisation and migrant (sometimes seasonal) nature of desperate job seekers, who typically live in informal settlements, making poll-site determination for them problematic. By having their biometric data stored on an NFC, voters are able to cast their ballots and thus, this feature mediates this form of mobility as well.

D. *The Estonian i-Voting as our Base Model*

The model being proposed in this work, contextually builds on the current uncontrolled voting practises such as Estonia and Norway. The Estonian model is presented, which uses an ID-card:

- The voter inserts the ID-card into a card reader and opens the web page for voting.
- The voter enters the PIN1 of the ID-card for verification purpose.
- The server checks if the voter is eligible by using the data from the population register.
- The voter is shown the list of candidates of the appropriate electoral district.
- The voter makes a voting decision, which is encrypted.
- The voter confirms his/her choice with a digital signature by inputting the PIN2-code.
- The voter receives a notification on the computer screen that the vote has been accepted [36, 37].

We now incorporate the Estonian model in the South African context and the proposed mobile m-voting is now presented.

VI. Implementing Our Model

The first stage of the implementation of our model is enrolling the voter (Fig. 1.). Enrolment is undertaken during the registration cycle by the EMB, which is familiar to South African voters. Here a voter is physically authenticated as a natural person and then vetted for eligibility using an appropriate legal process. For example, voters under a certain age or with certain types of criminal records may be deemed ineligible. An obvious difference the Estonia model and the South Africa model is the lack of a Smart ID card along with pervasive readers as well as the absence of public and private encryption keys. In order to address these deficiencies in our proposed model, it requires voters to enrol to capture their biometric data onto an NFC tag for baseline verification.

The eligible voter is then enrolled and certain biometric (Secret Question, Voice) is captured and stored in a write-once NFC tag. This write-once makes the tag read-only and impervious to overwriting false data. This information is for a local 'match-on-card' or a decoupled comparison during the ballot casting or the voting process. This match-on-card design is deliberate as it reduces biometric data traffic and overhead, which can cause denial-of-service attacks or may even be surreptitiously monitored by the man-in-the-middle attacks or captured.

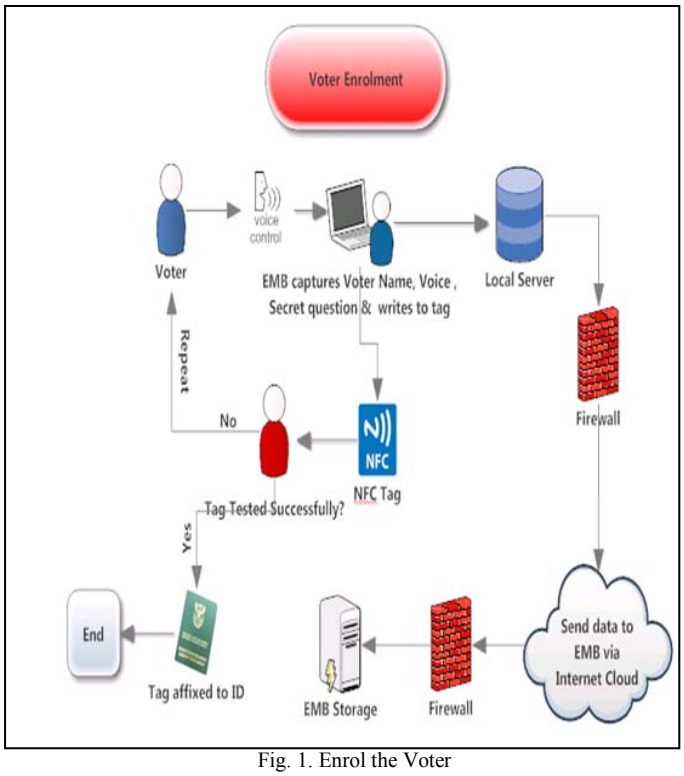

Fig. 1. Enrol the Voter

After enrolment, the NFC is affixed onto the ID document of the voter. The NFC tag is printed with an EMB hologram and affixed to the smart ID card, voter card or ID book and the voter may be given training on the use of the application. The

tag will provide for physical voter registration verification, implying that the person with the tag is entitled to vote. The biometric verification mechanism will verify the aspirant or the voter as legitimate.

A. Election Day

On the election day, an eligible voter will fetch his/her ID, which already has the NFC tag and tap it on his/her mobile phone. This is an important physical activity as it has a ceremonial factor that hopefully introduces solemnity and elevates the voting process to something more than an online interactive session. As a result, tapping or proximity movement automatically launches a voter applet with the built in details of the voter.

The application is launched (Fig. 2., Step 1 & Factor 1 satisfied). The location is verified (Fig. 2., Step 2 & GPS factor 3) and the voter choice module is started. The voter is asked a secret question or password (Fig. 2., Step 3 & Factor 2 satisfied). The voter is then asked to repeat a phrase for biometric validation. This biometric is compared with data stored on the NFC for verification (Fig. 2., Step 4 & Factor 4 satisfied). The voter is then asked to proceed with his/her vote.

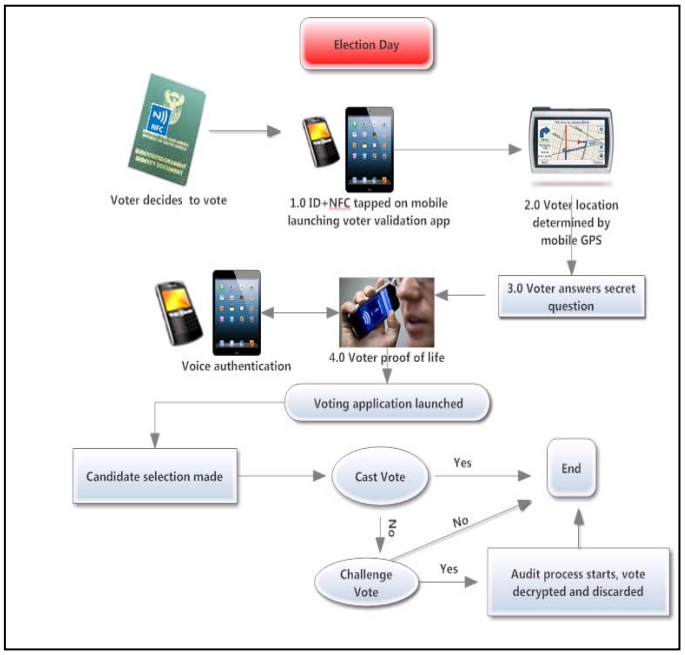

Fig. 2. Election Day Voting Model

The voter's vote is captured in an envelope encoded using this private key and transmitted to the EMB. This system will determine if the person has already voted. If so the application will overwrite the virtual envelope with no credence to the contents. This re-vote option is designed to prevent coercion. At the end of the voting process, all links between voters and votes are removed and all votes in the virtual envelope are transmitted to another server for tabulation.

B. Authenticate the Voter

The authentication mechanism of our m-voting model ensures that a voter is neither a deceitful imposter nor a bot attacker, an automated computer programme attempting ballot stuffing, a cracker or a hacker. After all, the legal imperative is on the EMB to authenticate only eligible voters in an easy to use and culturally sensitive manner.

The authentication mechanism merely matches the biometric encased within the tag (captured at the electoral office) with voter biometric captured on the mobile (during the voting session). If for any reason, a voter is removed from the voter roll, he/she will still be authenticated, but cannot cast vote in the next section.

C. Cast and Capture Vote

The voter must be allowed to optionally cast vote, in all, any or some of the elections currently permitted. In our system, we only allow for valid voting, which prevents over-voting, invalid, NOTA or spoiled ballots.

The system described also allows a voter to re-vote as many times as desired before the election day to reduce possible coercion. In this case a link between the electronic envelope containing a vote and the voter is maintained and with each successive vote, the envelope is simply overwritten. However, on the election day, as shown in Figure 2, the voter may only vote once on a poll site. If he/she already cast a vote, it is overwritten on the envelope and the link is deleted [36].

D. Commit or Challenge and transmit Ballot

The vote must be transferred freely, securely and safely to the Electoral Server without monitoring, interception or diversion.

Our model further allows for real-time auditing. In this case, the voter rather than commit and cast votes, or challenge the vote. In this case the envelope is decertified as a valid ballot and decrypted. The voter or auditor is asked to state what votes were captured and the terminal prints that were captured. This feature may also be used by opposition parties or other stakeholders as the results must be correct to the extent that all stakeholders, particularly the losers accept the outcome [12, 22].

E. Quit

The user gracefully logs out of the application.

VII. Conclusion

In this paper, we provide a model for m-voting that utilizes biometric, NFC, mobile phone and location based technology.

The model provided, leverages the ubiquity of mobile phone to address voter mobility, transparency, fairness, convenience and cost overhead. The combination of mobile pervasiveness with biometrics, stored in the NFC could address voter verification in a socially and culturally sensitive manner. In addition, this will mitigate ineligibility,

impersonation and will address the network congestion issues on the voting day. The NFC tag adds security flavour and privacy of voting. Moreover, the operational use of re-voting addresses incoerciblity that may occur in reality.

It is important for democracy that an election is not just 'a census of those who vote' particularly as voter turnout numbers are diminishing. This is why Electoral Management Boards (EMBs) all over the world, constantly, albeit carefully innovate to foster participation. Our m-voting model shows potential to re-engage the youth voter population and enable voting for disadvantaged groups, such as the elderly. M-voting is a promising research area that we hopefully intend to contribute towards. Future work will include real-life deployment of our system to test for its adoption and usability.

REFERENCES

[1] Voting Guidelines. US Election Assistance Commission, 'Voluntary Voting System Guidelines', Vol.1.0, Ver. 1.0, 2005.

[2] K. Ok, V. Coskun and M. N. Aydin. Usability of Mobile Voting with NFC Technology, Proceedings of the Publications International Conference on Software Engineering (IASTED), Innsbruck, Austria, 2010, 151-158.

[3] K. Ok, V.Coskun, M.N. Aydin and B. Ozdenizci. Current benefits and future directions of NFC services," Education and Management Technology (ICEMT), International Conference on. doi:10.1109 /ICEMT.2010. 5657642, 2010, 334-338.

[4] R. K. Sinclair, Democracy and Participation in Athens. Cambridge University Press, ISBN 0-522-42389-9, 114-9, 1988.

[5] R. G. Saltman. The history and politics of voting technology: In quest of integrity and public confidence. Palgrave Macmillan, 2006.

[6] D. W. Jones. A brief illustrated history of voting. University of Iowa Department of Computer Science. (Online) Available: http://www. cs. uiowa. edu/~ jones/voting/pictures/. Revised., 2003.

[7] Temple of Democracy. Rural development and Panchayat raj department Policy note 2012-2013. Online Available: www.tn.gov.in/policynotes /pdf/ rural_ development.pdf. [Retrieved 2 February 2014].

[8] A.A. Ross, A.K Jain and K. Nandakumar. "Information fusion in biometrics." Handbook of Multibiometrics Springer, 2006, 37-58.

[9] S. Thakur, Electronic Voting – The Cross National Experience. The Electoral Commission of South Africa, 2012.

[10] R. M Alvarez and T. E. Hall, "Point, click, and vote: The future of Internet voting". Brookings Institution Press, 2004.

[11] M. Bellis, "History of Voting Machines", (n.d)., (Online) Available: http:// inventors.about.com/library/weekly/aa111300b.htm.

[12] M. A McGaley, Electronic voting: A safety critical system (Doctoral dissertation, Department of Computer Science, National University of Ireland), 2008.

[13] R. T. Mercuri, Electronic vote tabulation checks and balances. Ph.D. Dissertation University of Pennsylvania School of Engineering and Applied Science, Department of Computer and Information Systems, 2001.

[14] M.F.M. Mursi, G.M.R Assassa, A. Abdelhafez and K.M. Abo Samra. On the Development of Electronic Voting: A Survey. International Journal of Computer Applications, 61(16), 2013, 1-11.

[15] T. Kohno, A., Stubblefield, Rubin, A. D., & Wallach, D. S. Analysis of an electronic voting system. Security and Privacy. Proceedings IEEE Symposium on. IEEE 2004, 27-40.

[16] A. Oostveen. Context Matters. PhD Thesis. UniSversity Of Amsterdam, 2008.

[17] R Allen. UK Government Report. Implementing electronic voting in the UK. (online), (Oline) Available: www.communities.gov.uk/ corporate/ [Accessed 20 January 2010].

[18] M. Reid. (Online) Available: http://www.newbrunswickbeacon.ca/6687/ e-voting-a-new-electronic-way-to-vote/.[Retrieved 2 February 2014]

[19] SS. Sampath, E-voting: The Indian Experience Lecture at Electoral Commission of South Africa Seminar on Counting Technologies, Cape Town, 2013.

[20] SMS, Gujarat SEC mulls over voting through SMS, Internet, The Hindu,29 January 2010. Available: http://www.thehindu.com/ news/national/other-states/gujarat-sec-mulls-over-voting-through-sms-internet/ article96860.ece.

[21] Electoral Commission of India. "Press release 13 September 2013", (Online) Available:http://eci.nic.in/eci_main1/current/PN27092013.pdf.

[22] S. Thakur. E-voting: a X-National Experience Keynote Address at Electoral Commission of South Africa Seminar on Counting Technologies, Cape Town, March 11, 12, 2013.

[23] P. Alexander. "Rebellion of the poor: South Africa's service delivery protests–a preliminary analysis." Review of African Political Economy 37(123), 2010, 25-40.

[24] S. Thakur and R. Davila. The path towards effective solutions: A study on voter registration experiences and technology. Draft for UNDP. November, 2013.

[25] A.I. Naidoo, Evaluation of UNDP contribution to strengthening electoral systems and processes, Evaluation Office of UNDP, New York, UNDP, 2012.

[26] S. Thakur, and R. E Boateng, -Voting for good governance and a Green World, Conference Abstract, - In Proceedings of the Africa Digital Week, July 26-29, Accra, Ghana: African Institute of Development Informatics and Policy, 2011, 55-81.

[27] J. Zogby, and J. S. Kuhl. First Globals: Understanding, Managing and Unleashing, the Potential of Our Millennial Generation.2013.

[28] Khelifi Adel, Yasmin Grisi, Dima Soufi, Dalya Mohanad, and P. V. S. Shastry. "M-Vote: A Reliable and Highly Secure Mobile Voting System." In Information and Communication Technology (PICICT), 2013 Palestinian International Conference on, IEEE, 2013, 90-98.

[29] R. Sanjith and Y. Deokaran. Interview OneVault Voice Biometric Company, 5 November 2013.

[30] A. Wong. Biometrics market: where are we now? Biometric Technology Today, (14) (9), 7-9, http:// dx.doi.org/10.1016/S0969-4765(06)70591-4, 2006.

[31] The Mercury. South African Social Security Agency (SASSA), Proof Of Life Certification Call for grant recipients, page 7, The Mercury, 31 January 2014.

[32] B. Harris, "Black Box Voting, Black Box Voting E-voting forum" (online). Available: http:// www.ronpaulforums.com/showthread. php?432518-Stay-Tuned-for-the-new-BLACK-BOX-VOTING.

[33] B. Rogers, B. "Why I Hacked Apple's TouchID, and Still Think It Is Awesome, Lookout." (Online). Available: http://www.lookout.com.

[34] EAB Position paper. iPhone 5S: heralding a paradigm shift? European Association for Biometrics, Available at: http://www.eab.org/files/ documents/2013-11-04_EAB-EABAC_ paper_on_ iPhone5s.pdf.

[35] P. Crossman, "The case for voice biometrics". American Banker. (Online) Available from http://search.proquest.com/docview/ 1117917525?accountid=10612, 2012.

[36] Estonia.."Estonian e-voting system". Available: http://estonia.eu/about-estonia/economy-a-it/e-voting.html.

[37] T. Kalvet, "Management of Technology: The case of e-Voting in Estonia". *International Conference on Computer Technology and Development. ICCTD'09*.. IEEE, 2009, 512-515.