An Architectural Framework for E-Voting Administration

Shadreck Mudziwepasi

&

Mfundo Shakes Scott

University of Fort Hare, Department of Computer Science, P/Bag X1314, Alice 5700, RSA

{smudziwepasi, sscott}@ufh.ac.za

Abstract- One of the key areas of concentration in achieving harmonious democracy is transparency in the electoral processes. Some countries on the African continent such as Ghana and Kenya have recently had issues of doubt and mistrust of the administration and the management of their Electoral Commission and hence a suspicion of election fraud which has prone threats of violence, economic declination and on the peak, legal implications. There was a claim of double registration, duplicated ballots, lost ballots, wrong count of ballots, failure of biometric registration system, impersonation, and alteration of counted votes in the immediate past election in countries such as Ghana, which led to series of court cases. E- Voting brings about a suitable solution to these. Available Literature at present exclusively reveals that most e-voting systems have presented several failures in design. This raises eyebrows concerning the technical and procedural controls on whether they are sufficient to guarantee trustworthy voting. The best methods possible should be applied in order to come up with the best solutions based on a framework that thoroughly addresses the requirements and standards. Therefore, this paper seeks to optimize the voting processes and governance of the Electoral Commission of respective countries by proposing a trustable e-voting theoretical framework which dwells on biometric data of various candidates as the basis for encryption of ballot, dedicated channel for transmission of counted ballots and/or connecting and disconnecting the database server before and after voting. Various literatures are considered to help propose a robust framework

Keywords: E-Diary Services, UFH network, framework, Development

1. Introduction

The Elections and voting practices are of very much importance to all countries that practice democracy. It is through the process of elections for which citizens have the opportunity to choose the leaders and representatives of their choice (Rexa et al., 2012) At present in most countries, the fundamental right of choosing a leader using a voting system is done mainly in manual and paper form (Kingsley et al., 2014). However, the

administration of the voting process when done manually makes it prone to various electoral problems such as over-voting, wrong count, impersonation, lost ballots, spoilt ballot, declining turnout of voters, difficulty of auditing after voting and poor documentation (Nu'man et al., 2012). This situation calls for immediate attention to the methods used in voting. Around Africa, some countries such as Sierra Leon,

Rwanda and Uganda have had riots because of the poor administration of the electoral process and in all of these countries, the manual paper forms are used for voting (Bamiah et al., 2010). A robust framework to implement E-Voting would really prove to be vital in addressing these challenges

At present and in most countries, the norm is that an Electoral commission (EC) is mandated to be in charge of free and fair elections (Alkasar et al., 2014). The EC is responsible for the organization of elections in most countries (Bamiah et al., 2010).

However, election administration is bringing about a new dimension in the history of most countries, especially where the major opposing parties have doubts of the results and hence they launch court cases against the winning party. The parties would disagree with the results from the EC and in most cases claim that they are fraudulent. This calls for the fact that an effective and trustworthy system would be required to replace the manual system to enhance the trust of the citizens in the voting system (Alkasar et al., 2014).

Therefore, this research work seeks to examine the lapses in the existing voting system and propose a trustable e-voting system framework for which when adopted and implemented would solve the majority of the problems faced. Besides system analysis against requirements, it is also important to carry out an amalicious circumstances scruitiny on occasions when the execution model is susceptible to attack. We therefore outspread system specification by guarding it against compromising attacks (Yeboah et al., 2013). This was supportive in our aim to spot mislaid requirements and conventions respectively regarding system specification. Also, this allowed us to outline counter measure initiatives that can be used alternatively when the system malfunctions to increase the reliability of the system throughout its design.

It is acknowledged in this work that the central problem we find in e-voting applications specification and verification is the challenges in modeling attacks since the different types of attack relay across the structure of the unique performance models, resulting in difficulties in incremental verification (Patey et al., 2014). A robust framework would therefore be necessary to implement a useful e-voting system.

2. Related Research

E-voting is advantageous because of it ensures enhanced turn out and easy accessibility especially for disabled and/or or impaired people including improved efficiency and reliability.

However, e-voting adoption in various countries has been poor and slow and/or being the cause of debate and controversy. This is largely as a result of the largely poor implementation of (some of) the prototype systems currently deployed for elections in other countries such as the United States of America (USA), according to literature (Heitmeyer et al., 2008).

Present literature also shows that such systems have major and serious flaws in specifications and design. Thus, such weaknesses expose the system, and consequently make elections vulnerable to malfunctioning and various threats and attacks, ranging from a denial of service to result alteration. There are several research works done by some researchers in e-voting security and trust issues.

(Alkasar et al., 2014), proposes a framework to manage a secure trustworthy E-voting system, by securing each and every side of the system from its initial stage to finishing stage through implementation of the Trusted Platform Technology (TPM). The TPM serve as a chain of trust that combines hardware and software to provide trusted client device.

However, in their research they failed to provide the design of the TPM and how it was used to secure the vote, channel, the computers, and mobile phones in their framework. Also, on their proposed framework the entire voting process is obscured from the voter and polling agents. They only get to know the result from the polling station only when the entire voting process has ended. This will negatively affect the trust of the voters.

In (Yeboah et al., 2013) is a proposed e-voting framework that will enhance the security of the immediate manual system if adopted. To enhance the security, they implemented it using smart cards and digital certificates. However their framework is expensive because at every polling station they implemented 2 ARC (Archive) redundant servers which invariable stored small amount of records. Also, to secure records, the systems were configured by the national election commission. Their research did not cover the polling agents at this level, for which it can implicate the trust of the system by the voters.

In (Patey et al., 2011), a research work proposed a framework which was aimed at improving authentication and transparency in e-voting systems.

Their systems framework was to replace the manual system so then their citizens will be able to vote

from any polling station. This concept was derived from queue listing dynamic technique which is centered on arrivals and identification of the subsequent voters at the polling station. However, the system could not address how the centralized database could be protected to check for content; whether there are votes or no votes already in the in database before voting starts. Again, their research work did not consider the integrity of casted votes during the time of voting.

The work of Alkassar in (Jones et al., 2009) proposed a solution to security of online voting systems bringing to bare how unsecured malware and corrupt voters activities on the voting system could affect the trustworthiness of the voting process and the voting system entirely. Their solution was based on Trusted Computing in combination with secure operating systems. However, they did not consider the security breach based on amount of time spent within the network and the number of attempts of logging onto the system.

Their framework could have been very much effective if a defined set of parameters were identified to avoid breaches to use of the voting system. Their framework could not detect exactly who is voting, this is because it is done online. The framework lacks physical system administration and monitoring. A system's reliable specification behavior is achieved only if the best techniques are employed.

In this regards, a number of technical approaches to address (some of) the issues mentioned above have been devised and are hereby outlined in this research work. Among these include the implementation of formal methods and robust frameworks which have been proven to improve the reliability and efficiency of complicated systems. No mechanisms were defined to tell genuine citizens are identified to vote anywhere.

Therefore, there is the need for a framework that identifies each voter before the ballot is casted.

3. Framework for the Existing Manual System

The existing frame works exemplified by those mentioned in the related research section can be illustrated by Figure 1 below. This figure basically shows the frame work for the existing voting system currently adopted for use in some countries across the globe (Juels et al., 2005).

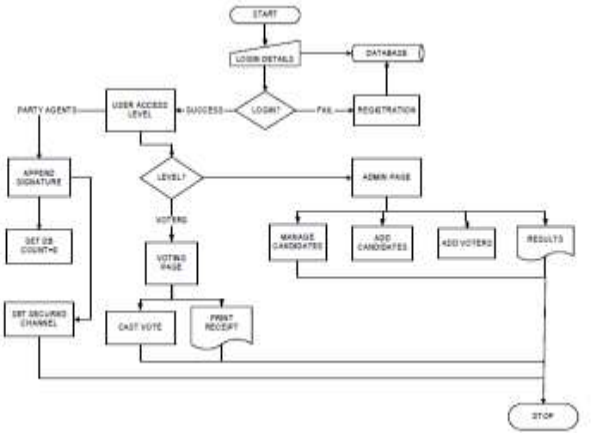

Figure 1: Flowchart of the Existing Voting System

3.1 Current Voting Process

Without any unforeseen circumstances, voting takes place only on the day of election normally starting from 7am up until 7pm. This is not to say one cannot vote when it is 7pm while he/she is already in queue to vote (Alkasar et al., 2014). It is only people who get to the polling stations at 7pm or after that would not be allowed to vote. The voter goes through the following processes:

- The voter is required to check His/her name in the reference list so as to identify himself/herself as an eligible voter. This is done by showing your voters' ID card to the officials who would in turn cross check to see whether you are in the voters' register and also place your thumb on the biometric machine to verify if you are truly the card bearer (Kremer et al., 2014).
- After all necessary information has been checked out, your finger would be dipped into an indelible ink. This is also a measure to prevent double voting. But one must be sure not to stain the ballot paper with that finger since a soiled ballot paper would be rejected (Lowry et al., 2014).
- After receiving your ballot paper, one should carefully check whether it has the ECs official stamp on it before he/she goes to vote otherwise that ballot paper is considered invalid .
- Voting is done in mainly three ways; presidential, parliamentary and local government. After receiving the presidential ballot first, you would proceed to a voting booth where you find an ink to dip your thumb in and then carefully vote in the space provided for your candidate of choice. After which you wipe your finger first and gently fold the

paper into the ballot boxes.

- You then proceed to the next table for the parliamentary ballot paper and also follow the same procedure as the presidential one above and drop the ballot paper in the parliamentary ballot box after which you will also do the same for the local government ballot.

3.2 Predominant Challenges of the Manual System

Poor

- Documentation and Recording: In the past elections in countries such as Ghana, there were several situations of poor recording of total ballots in some of the polling stations. For example; 270 being written in words as twenty seven zero. Their respective meanings are completely different.
- Alteration of Votes: Votes can easily be manipulated because they are directly recorded on paper. The records can be exposed to any voter or official with malicious intention. According to (Martinelli et al., 2002), electoral personnel always replicate the votes which at the normal circumstance would not have been so as compared to e- voting which is claimed to be devoid of such.
- Voter Error: Voters sometimes makes errors. For example a voter may unintentionally thumb print against the picture of a candidate for which he did not intend to have voted for. However, you cannot make changes to the selected option. Also, if a voter does not fold their ballot papers well, the ink can spread to another candidate column, and hence the vote is disqualified and nullified. The Official website of Electoral commission, R&M Department of South Africa provides a summary of rejected ballots from 1992 to 2008 as follows: 3.03, 1.53, 1.58, and 2.13 2.32. by percentage through observation. It is clear that from year to year, the total percentage of spoilt ballots is increasing. In a 2012, December election in Ghana, 251 720 out of 11,246,982 total votes casted were nullified because either voters voted for two different parties at the same time or they were left blank.
- Deferrals in Showcasing Final Results: According to (McDaniel et al., 2014), it has been ascertained that it can take up to 3 days for the IEC of South Africa to eventually publish election results worse still a national election. This situation

prevails because they manually do the collation of results from all the various polling stations, constituency and then the national levels, which is very tedious and cumbersome to be finished within a short period of time such as an hour.

- Ballot Design and Count: Recently, biometric registration and verification were introduced into the electoral processes. However, when voting is done, all the ballot papers are mixed and no voter can be linked to any ballot paper. Also, counting is very difficult, because ballot papers are mixed up in one ballot box and are unorganized. After voting, counting is manually done for each party. Errors may occur during a large count and hence would affect the result.
- Unsecured Medium for Transfer of Ballot Count: Transferring votes from one polling station to the constituency involved can result in inconsistencies and it is was alleged that for most voting nations, there is always a suspicion of transferred votes not matching counted votes at a polling station (Kolano et al., 2007). Methods for transfer would therefore have to be improved to close up on any loopholes.

4. Proposed E-Voting System

4.1 System Requirements

Before system design, a comprehensive requirements gathering process is necessary. These requirements include generic, system and election-specific requirements as presented in Figure 2 below.

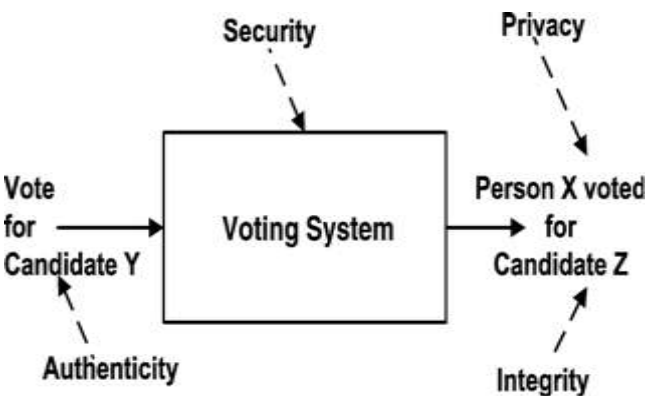

Figure 2: Set of Requirements

4.1.1 System Requirements

The generic requirements apply to any voting system (Patey et al., 2014). These requirements, as shown in Figure.1 above and are further listed and briefly explained below:

- Authenticity: only those eligible registered voters are able to vote;
- Integrity/accuracy: A vote cannot be altered in any way once casted. Valid votes count and invalid votes become spoilt;
- Privacy: A voters vote is his/her own secret;
- Security: No one can temper with a vote throughout the voting process;
- Democracy: qualified voters must vote only once.
- Confidentiality: The system should be very confidential and information should be kept as thus

4.1.2 System-specific requirements

All the system-requirements in general refer to all those requirements that have a lot to do specifically with the on-line digital electronic system of voting.

The system-specific requirements include:

- Multi-user: numerous voters can vote at once;
- Multi-elections: numerous elections can be run at once;
- Accessibility: The accessibility of the system by voters is generally in reference to the ability of the voters to be able to cast their ballots any time on www using any device;
- Availability: this highly speaks volume in the ability of the system to be open to anyone and available during the time of the elections and also during the period of election campaigns.

4.1.3 Election-Specific Requirements

As stated earlier, these types of requirements highly refer to those needs that are needed in any particular singled out election (Alkasar et al., 2014). If we can as an example consider the election specific requirements for student council election:

- A voter is supposed to be a full time registered student of the university;
- A candidate is supposed to be a full time registered student of the university as well;
- A candidate is supposed to have completed have completed at least 2 semester blocks at the university and maybe a particular GPA that can be set is supposed to have been obtained;
- A candidate must have a 1 year term limit.
- A candidate can also vote.

4.2 E-voting System Organization

A architectural system for voting

online and its administration is given in Figure 3 below and as shown, it is supposed to consists of a several components and each of those is explained here.

4.2.1 The Subsequent Election Database monitoring and System of Database Administration

This stores the information and all associated features of the elections in digital form, this will include all information about the candidates and even the voters roll as well as information regarding the polling stations and the officers including the locations of the stations and the subsequent voting times etc. An example of the technology used for such systems include Oracle.

4.2.2 The Web Server and the Web Pages

The main functionality of this feature (server) is to connect our system to IP. Furthermore, it keeps overally keeps track of the pages and the technology and functionality that is required. The web pages can be defined as either stationary/static and/or dynamic. Static web pages remain with their original data while dynamic content can be altered and modified over its entire life. Some technologies that are used in the creation of dynamic webpages include Java Server Pages (JSP).

4.2.3 The SMS Server

The Short Message Service (SMS) server is able to communicate with voters through SMS messaging. The SMS server utilizes the Global System for Mobile Communications (GSM) to relay SMS messages to all voters through a SMS network service provider. Upon completion of the entire voting campaign, the SMS server will then send all registered mobile voters a message with the election results.

It is also vital to be aware of the different e-voting system components. These will determine the budget that is supposed to be set aside for the project and they overally makes it easier to do your system requirements and gathering implementation. Furthermore, the technologies and operating systems used for these components need to be set with the latest versions to avoid any unnecessary loss of data or creation of loopholes for hackers to exploit. The components overally connects the down and uplink and are illustrated in depth in Figure 3 below.

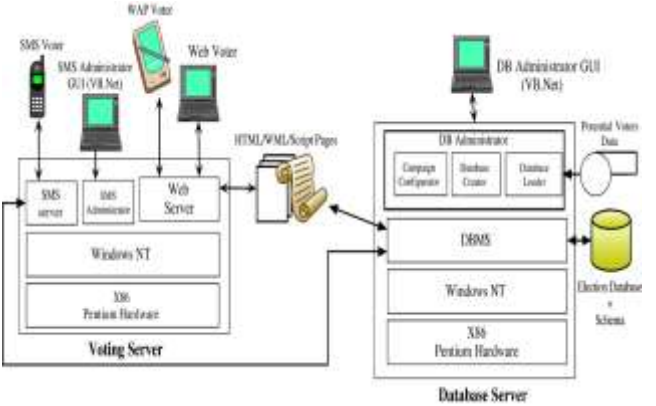

Figure 3: The Components of the Implemented E-Voting System.

4.2.4 The Access Devices

It is clear that numerous mobile devices are used to get hold of the system. These include different brands of personal computers and also different brands and types of mobile phones. The system need to define all the necessary technologies and all the protocols that will ensure compatibility of our system with all these devices. An illustration of the technologies and protocols that are available for all of these different types of devices are hereby illustrated in Figure 4 below:

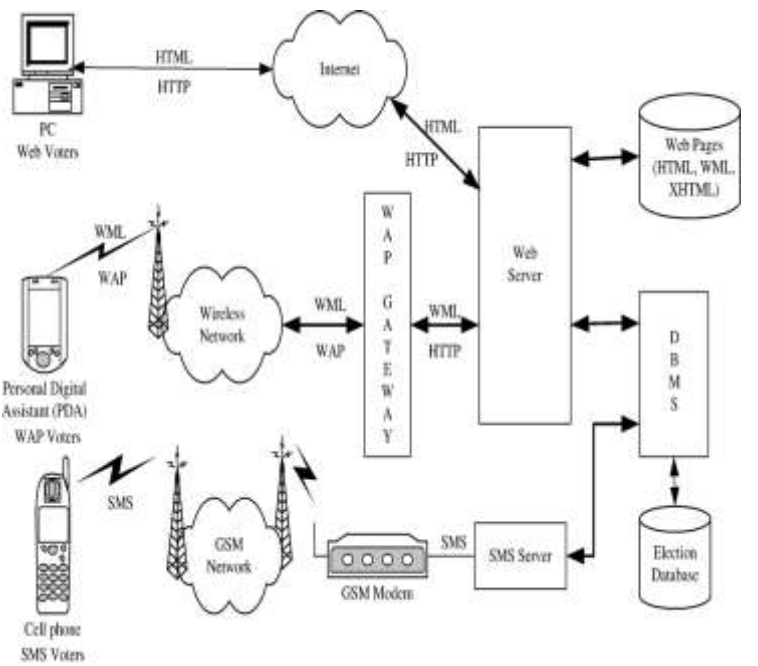

Figure 4: The Organization of a System for Electronic Voting

- **Personal/laptop Computers**: There are two types of connections that are established to and from the system. These are the wired and the wireless connectivity scheme. Computers can generally connect to the system using both systems alconnect through the wired and wireless Internet. They have a great memory for resources and high resolution screen display. Web browsers such as the Internet Explorer or Chrome or Mozilla firefox. These display a whole lot of data and information types e.g. audio and voice. This display is specified by a powerful GUI (Graphical User Interface) and languages such as the latest versions of HTML and/ or Extensible HyperText Markup Language (XHTML). These are all referred to as scripting languages and they are all also enhanced by client scripting languages that include JavaScript and VBScript. HTTP is highly utilized for the information exchange purposes.
- **WAP-enabled Handheld Devices**: These devices overally connect system using mainly a wireless connectivity scheme. It is in this category that we place mobile phones, tablets, all connected through a wireless network. They thus sometimes experience a limited network's bandwidth so they thus make full use of the Wireless Application Protocol (WAP) (Alkasar et al., 2014) framework and the closest gateway for server connection. The use of the gateway is simply to interpret and translate WAP into HTTP and the other way round. It is also very important to note that these devices are overally characterized by lesser memory sizes and processing power which results in them utilizing a limited version of the standard Internet browsers available, which in most cases would be the WAP micro-browser. This is a standard browser that can make use of the Wireless Markup Language (WML) as a specification for all its various user interfaces. The earlier versions of WML were largely based on the Extensible Markup Language (XML) and thus did not really show the major characteristics of the classical HTML language.

However, later versions of WML began to be based on the Extensible HTML (XHTML) markup language. Actually, WML now become sort of a small subset of XHTML which however requires less processing power making it most suitable for mobile devices. We can also note that WML 2.0 and beyond can support tables and simple scripting through WMLScript.

- **Regular Mobile Phones**: On the usual, these are the normal low cost, low processor power and low functionality regular cell phones. They overally utilize the SMS technology in order to establish a connection for users across system. The SMS tool is a common communication toll used by many due to low cost and user friendliness. The low cost is basically as a result of the two major influencing factors which are low cost of sending and/or receiving a message and the low cost of purchasing the mobile phone that can be able to be used in supporting this service.

  The only functionality needed in these devices is just a simple textual editor that can be utilized for composing and displaying the message. We can note one very detrimental disadvantage of an SMS which is that you sometimes cannot be able to construct a very highly interactive dialog between the mobile device and the system using a simple SMS application just like it is difficult to send some complex files with g-mail and you will need google drive to send these.

5. Proposed Architecture

Figure 5 below shows the proposed architectural framework for the E-Voting Application.

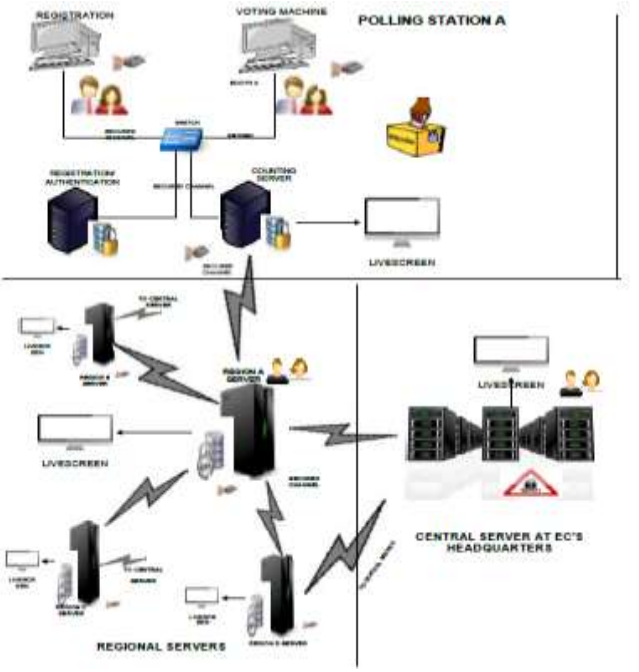

Figure 5: Proposed Framework for Implementing E-Voting Application

The architecture is based on 2-tier architecture. In this architecture, the client of the e-voting system handles the e-voting application while there is a server that will handle the database at the backend. Upon invokement by the client, it establishes a subsequent connection to the server as needed and interacts with the server. The client usually cannot see the database directly and can only access the information/data when active. Therefore server data is more secure. The client-server solution also allows many users database access simultaneously.

6. Ensuring Security

In this section, appropriate methods and techniques for ensuring security on the e-voting architecture is discussed. The network architecture for which the voting software is going to run and the design of the database are considered.

6.1. Master Database

Before the process of voting begins, party agents who are assigned cryptographic keys have to append to attest the fact that the database count is zero. The same agents would have to append their keys to encrypt and isolate the database. Then they would append to encrypt a secured channel from the system to the database server. Voters can then be allowed to cast their votes after channel to the database has been secured by the various political party representatives.

6.2. System Algorithm

* Setting database record count to zero: Use biometrics from party agents

E.g. Xi ⟶ i], where X is party

agents, R is the biometric reset sequence generated by system for

X1 ⟶ [R1]

- X2= [R1]+[R2]
- Xn = [R1]+[R2}+……[Rn]
- X1 + X2 +… Xn = empty db
  db = 0

- **Disconnecting Database from Application Before Voting**: Party agents confirm and disconnect db for authorized connections only.

E.g Xi [Ri], where X is party agents, R is the biometric reset sequence generated by system

X1 ⟶ [R1]
X2= [R1]+[R2]
Xn = [R1]+[R2}+……[Rn]

- X_1 + X_2 +… Xn disconnected db

- **Secure direct encrypted connection for eligible voters**: E.g. assuming we have polling booth [A, B, C] at a polling station,
- **At booth A, B and C**: n number of party agents is required to establish a secured connection from the system to the db.
- Booth A = X1 + X2 +… Xn
  BA = X1 + X2 +… Xn
  [BA X1 + X2 +… Xn]
- Booth B = X1 + X2 +… Xn
  BB = X1 + X2 +… Xn
  [BB X1 + X2 +… Xn]
- Booth C = X1 + X2 +… Xn
  BC = X1 + X2 +… Xn
  [BC X1 + X2 +… Xn]

7. Increased Trustworthiness

The ultimate fairness and subsequent security of all these electronic elections would largely depend on a careful requirements allocation procedures during and after holding of elections

7.1 Preliminary Level

* Auditing of the Voting System: To enhance trustworthiness of the voting system, the system would have to be tested thoroughly. The modules or scripts of the voting software and the dedicated channel would have to be also tested and tried by an auditing team made up of computer programmers and ethical hackers from each of the represented political parties. This will help the parties to understand and accept that the system is robust and hence no errors are going to emanate from the use of the system
* Registration: The registration is done at the second phase after the system has been tested thoroughly. All legible voters will come along with their voters ID card and their details as specified by the Electoral Commission would be captured including their finger prints. Upon completion of the registration, the voter is assigned a unique voters ID that is generated from a set of random

numbers.

* Securing Database and Dedicated Channel: This process is also carried out before the Election day where various representatives from the political parties are assigned biometric keys. These should be kept safe and secure by the responsible parties involved. These keys are to be appended to connect and disconnect the database before and after the main voting. This is to set the database to zero vote count and also the secure the channel for voting. The database security and protection is a very important aspect of the system. If the information in the database is in any way tempered with, then it would mean the whole system's credibility is compromised and its rating drops to unprecedented levels

7.2 Voting Level

* Voting interface: At this point, the voter is required to enter his/her unique ID and biometric data before accessing the voting panel where he/she is presented with the three main voting categories of presidential, parliamentary and local government to vote. Upon selection of each category, the voter is presented with the various candidates' names and pictures for voting. Voting for a candidate in this category is acknowledged and that category immediately disabled to prevent double voting. A receipt is then issued out to the voter which states the political party voted for. This receipt is then placed in a physical ballot box for recounting later in case of disputes. Voting process is made possible when party representatives append their signatures to secure voting channels to database. All these processes must appear graphically on a live screen.

7.3 Events after Voting

* Counting and Tallying: The subsequent ballots that were cast are shown on the live screen prior to this stage to show live results clearly to the public and to also make sure that ballots cast are equal or less than number of people registered. In case there still some doubts, the receipts placed into the ballot boxes can be recounted. Election results from each polling station are then sent to a regional server in a secured encrypted manner which is also authorized by the party agents. At the regional level, various party reps can be assigned with biometric keys to receive data from polling stations and then also send them securely to other regional servers as well as the Electoral Commission's central server. The process of exchanging data between the regional servers before sending them to the central server is to prevent the process of someone hacking into the network to change data on one

communication channel. If such a person even succeeds on that channel, we would have nine additional regional servers to cross check data for accuracy.

8. Conclusion and Future Work

Electronic voting is a system that largely concerns the behavior of all the participating individuals and the associated voting system components. The uttermost assurance of all electronic elections would definitely mean that a thorough and extensive review and investigation of all these various aspects, initiatives and associated techniques in an inclusive and integrated way. A full-bodied design would really mean our system is easy to use and will that the system continues to function even in situations when one or more components are compromised. The researchers in this paper have clearly demonstrated to a large extent considerably the use of a more authenticated and simpler user friendly approach which can be used by a voter with no difficulty when provided with the necessary training. The proposed framework when implemented will do away with most of the inconsistencies in the vote processes and will be very effective. It should be noted that however, in some African states that held elections recently such as Ghana, some voters could not be verified although their biometric data was previously collected during the registration period. Therefore an alternative to biometric data would be very important for further research and future work. Also, most of the existing e-voting systems do not consider the illiterates. Therefore an alternative scheme such as voice instruction should be further studied to see how they could be integrated into voting systems as an addition to the use of the usual input devices (such as keyboard and the mouse).

9. Acknowledgments

This is work is that has been undertaken within the TELKOM Coe in ICTD at the University of Fort Hare computer science department. It has received support in part from Telkom SA. The findings expressed here are those of the authors and none of the above sponsors accepts liability whatsoever in this regard.

10. References

Rexha, V. Neziri, and R. Dervishi. "Marching in the Direction of Framework For the Administration of E-voting:" The Case Of Ghana". Available in International Journal of Computers and Communications. Issue 1, Volume 6, 2012

Kingsley J, K Sarpong, "Towards Improving authentication and due transparency of e-Voting Systems in the Kosovo Case", IJCSI International Journal of Computer Science Issues, Vol. 11, Issue 3, No 2, May 2014

Rexha. B, R. Dervishi, and V.

Neziri. "2011An architectural Framework for the Adoption of E-Voting in Jordan", Retrieved from https://www.google.com.gh/#bav=on 7th August, 2013.

Nu'man.B "We are Increasing the Trustworthiness of e-Voting Systems Using Smart Cards and Digital Certificates A test case of the Kosovo Case.". Electronic Journal of e-Government Volume 10 Issue 2 2012, pp133 – 146, 2012.

Bamiah. M, A. Dehghantanha, and B. Archibald. "Towards Trustworthy Architectural voting systems" http://www.academia.edu/643254/A_Trustable_Electronic Government_Voting_ on 15th August, 2010.

Alkassar. A , A. Sadeghi, and M. Volkamer, "Presenting A Trustable E-Government Voting Management Framework Using TPM. 2010. Online Voting".n.d. https://www.cosic.esat.kuleuven.be/wissec2006/papers/17.pdf on 10th April, 2014.

Yeboah. A, Journal of Information Engineering and Application, Vol. 3, No. 1. 2013.

Ofori-Dwumfuo and E. Paatey. "Electronic Voting in Ghana: Is this Really The Solution To Ghana's Perceived Electoral Challenges After Biometric Registration?", Research Journal of Information Technology 3(2): 91-98, ISSN: 2041-3114. 2011.

The official website of the Independent Electoral Commission of South Africa, http://www.ec.gov.gh/, 2014

Heitmeyer, C.L., Archer, M.M., Leonard, E.I., McLean, J.D., "The Evaluation of Voting Technology". IEEE Transactions on Software Engineering (1), 34, pp. 82–98, 2014.

ES&S Inc, Election Systems & Software: iVotronicTMVoting System, version 9.1.x Election Day Operations Checklist, 2010.

Jones, D.W.,. "Applying formal methods to a certifiably secure software system", Chap 1. Towards the Advances in Information Security. Kluwer Academic, pp. 3–16, 2010

Juels, A., "Proving coercion-resistance of scantegrity II." In: WPES: Proceedings of the 2015 ACM Workshop on Privacy in the Electronic Society, ACM, New York, NY, USA, pp. 61–70.

Küsters, R., Truderung, T., Vogt, A., "Coercion-resistant electronic elections", ICICS, Lecture Notes in Computer Science. Springer, pp. 281–295, 2010

Kemmerer, R.A., "Tools and Techniques for the Design and

Systematic Analysis of Real-Time Systems", 37–50. Kohno, T., Stubblefield, A., Rubin, A.D., Wallach, D.S., "Analysis of an electronic voting system." In: IEEE Symposium on Security and Privacy , p. 27, 2009

Kolano, P., "Of Integrating the Formal Methods into the Development Process. IEEE Software 7 (5). Ph.D. thesis, University of California, Santa Barbara), 2009

Kolano, P.Z., Dang, Z., Kemmerer, R.A., "An Analysis of an electronic voting protocol in the applied Pi-calculus.", in Annals of Software Engineering 7 (1–4), 177–210, 2009

Kremer, S., Ryan, M.D., "The Design and Analysis of imminent Real-Time Systems Using the ASTRAL In": Sagiv, M. (Ed.), of the Programming Languages and Systems—Proceedings of the rare 14th European Symposium on Programming (ESOP'15). Lecture Notes in Computer Science, Springer, Edinburgh, UK, pp.186–200, 2015

Lowry, M., Dvorak, D., "Towards Communicating trust in e-commerce interactions". IEEE Intelligent Systems 13 (5), 45–49, 2008 Ajzen, I. & Fishbein, M. (1972) Attitudes and normative beliefs as factors influencing intentions. Journal of Personality and Social Psychology, 21, 1–9.

Bélanger, F. & Hiller, J. (2005) "In the advent of A framework for collective e-government:" Privacy implications of the Business Process Management Journal, 14, (in press).

Bélanger, F., Hiller & Smith, W. (2012) "Trustworthiness in the electronic commerce industry: the role of privacy, security, and site attributes." Journal, 2–5.

Carter, L. & Bélanger, F. (2013) Mixing the Diffusion of Innovation and Citizen Adoption of E-government Services in The Proceedings of the 1st International E-Services Workshop, 57–63.

Carter, L. & Bélanger, F. (2004) "A Citizen Adoption of E-government Initiatives" in the Proceedings of the 37th Hawaiian International Conference on Systems Sciences, 5–8.

Chadwick, S. (2001) "Analytic Verification of Flight Software." In Management Communication Quarterly, 17, 653–658.

Chau, P. (2013) "in the wake of An empirical assessment of a modified technological acceptance model. Journal of Management Information Systems,13, 185–204.

Cronbach, L. (2007) "The sole

Essentials of Psychology Testing." Harper & Row, New York, USA.

Doll, W., Hendrickson, A. & Deng, X. (2008) "Using Davis's perceived usefulness and ease-of-use instrument for decision making: a confirmatory and multigroup invariance analysis." Decision Sciences journal, 29, 839–869.

Martinelli, F., " The Symbolic inference systems" published in the Proceedings of the 27th International Symposium on Mathematical Foundations of Computer Science, Springer-Verlag, London, UK, pp. 519–531, 2008.ProjectReport,2007