Extending E-Democracy to Enhance Voter Registration and Identification: *South Africa Elections Perspective*

Isong Bassey
Department of Computer Science and Information Systems
University of Venda
Thohoyandou, South Africa
bassey.isong@univen.ac.za

Ndwamato Netshipise
Student, Department of Computer Science and Information Systems
University of Venda
Thohoyandou, South Africa
netshipise.ndwamato@gmail.com

Abstract— **The increase in information and communication technologies (ICTs), especially the Internet has been useful and yielded positive impacts in today's e-society. With e-democracy in particular, ICT can help build trust by engaging citizen in the policy process, promote open and responsible government and aid in preventing corruption. In the same way, ICT can also help protect the integrity of the elections especially during registration and identification of voters. This will go a long way to promote transparency and trustworthiness of the system, and possibly eliminates all forms election frauds - multiple registrations, voting and impersonation. Therefore, the objective of this paper is to propose a new improved form of electoral process that aim at providing stronger security measures to protect and uphold its integrity. The approach requires the use of relevant ICTs tools to enhance both voter registration and identification processes on a real-time mode in order to fully guarantee that one person registers or votes only once. In this paper, we discuss in the perspective of South Africa (SA) elections. In addition, we developed a prototype called VOTEX to substantiate our idea, making use of biometric technology.**

Keywords- Finger print, Voters, E-democracy, Real-time, Registration, Identification

I. INTRODUCTION

With the progress in science and technology in today's e-society, modern information systems that have resulted only do not provides ease for people to obtain information, but also provides opportunity for people to express their wills [1, 2]. The exponential growth of information and communication technologies (ICTs), especially the internet has been useful and yielded positive impacts. Several studies have witnessed these positive impacts, for instance, in healthcare, e-government and public administrations, education [2, 3, 5] etc. ICT have been useful to the e-society in various aspects of life such as getting public services to carrying out day-to-day work via e-services and e-practices. With e-services, ICT has brought about a whole new and better government (i.e. e-government) that is seen to be more open to the needs and aspirations of citizens, more democratic, and more efficient [3, 5]. One major aspect of e-government is the improvement of e-democracy that engages citizens to support the democratic decision-making processes and strengthen representative democracy through the use of ICTs tools [3]. In particular, the application of ICTs on electoral processes in most developed nations, mainly, electronic voting (e-voting) have been remarkable. For example, e-voting in the US, though some reported flaws [6,7].

In Africa, e-democracy and ICTs application in electoral process is at infancy stage where emphasis is gear towards providing public information and services, promoting citizen participation, building trust between government and citizens, etc. However, much has not been done to protect the integrity of our elections (i.e. voter registration and voting process). In the SA elections perspective, though employed some ICTs in its electoral process, relevant tools are not effectively employed during voter registration and voting. Furthermore, with the current electoral system, it is difficult, if not impossible to track down election frauds, implying that one voter, one registration or one vote is not guaranteed. Consequently, election frauds such as multiple registration, multiple voting, figure falsification and impersonation are not exception, though remains unobserved. Nevertheless, we believe that when electoral systems of this kind exist, the trustworthiness and the integrity of the elections can be threatened or lead to failures and corruption of democracy [8]. To promote and

protects the integrity of SA elections, a new approach that is more transparent, trustworthy, accurate and reusable is indispensable. The approach should start with addressing the problems associated with voter's registration and identification of voters during actual voting. With this, eligible voters will only register once and only votes once thereby promoting its integrity. Therefore, the objective of this paper is to propose a new approach of voter registration and identification during elections in SA. The proposed approach is the real-time registration and identification that utilizes biometric technologies and secured wireless network. To substantiate our idea, a novel system prototype called VOTEX System is implemented. We believe that when relevant ICT tools are taken advantage of in our electoral processes, it will go a long way to rid fraudulent elections practices and uphold elections integrity.

This paper is organized as follows: Section I is the introduction, section II is an overview of SA elections and issues, section III is the proposed approach and solution, and section IV presents the VOTEX system. The discussions and conclusions are given in sections V and VI respectively.

A. E-democry and Importance

E-democracy or simply electronic democracy is a new form of democracy that is enhanced by e-government. It takes advanced ICT, network and relevant technologies such as the Internet to improve democratic processes within a democratic nation [3]. It is seen as the computerization of political communication, process and policy-making with the intent of enhancing and increasing citizen participation in the policy and decision-making processes of government via a variety of activities [5]. These activities include and not limited to voting (i.e. e-voting) electoral campaigns, communication exchange, participation, consultation, public opinion polling, etc. the reasons for the development of e-democracy has been political democratization trend, abuse of democratic representative system, citizens' desire of partaking in political affairs, development of social economy, advanced ICTs [3,5]. E-democracy is at the junction of traditional democratic processes and Internet technology. Though the internet is not naturally democratic, it is used to strengthen the democratic processes and institutions. The impacts ICT brought into governance has been commendable, though is hard to see usually because often times the positive impact is not that obvious to the impacted. It is evident that ICTs can be used to enhance the democratic process, in which citizens are able to effectively impact the decision-making process and building trust between government and citizens [3,4]. With trust, ICT can help citizen engage in the policy process, promote open and accountable government and helping to prevent corruption. In addition, ICTs make it possible for connecting e-democracy to civil society with e-government at the local and national levels.

In Africa, ICTs in e-democracy has always been channeled towards achieving the various goals stated above. No effort has been made to employ relevant ICTs in protecting elections integrity. It is obvious and without doubt that voter registration and the actual voting are always prone to election frauds. It is of great importance to extend ICT (i.e. Internet) into these activities so that election frauds may be put to check in a real-time basis. This will go a long way to improving the quality of democracy, transparency and increase the participation since lack of confidence that elections are free and fair may lead to decline in levels of voters participation [10].

B. Justification for Re-engineerig Traditional Electoral System and Not E-voting

There are several voter's registration techniques and voting systems that exist in the world, yet the electoral systems still suffer large scale election frauds. Modern electoral systems, e-voting systems in particular, have been quite impressive. However, there has been widespread lack of significant public confidence on the use of the system as well as its results owing to several flaws reported specifically in the US [7,12]. The reported flaws were confusing ballots, registration mix- up, software errors, poor user interfaces, systems failure on Election Day, recount impossibility, absentee ballot problems that caused the losses of millions of votes [6,7,8].

Particularly in Africa, the problems associated with e-voting are complicated and cannot be contained due to the technological complexities involved. However, African countries can embrace modern technologies embedded in e-democracy into its electoral process in a form that can be handled. By this, African traditional electoral system needs to be re-engineered by employing some basic relevant ICT tools that may help improve the quality of the existing democracy, make it more attractive and alleviate the problems of verification and identification- multiple registration and voting, rigging, etc. This however, forms the basis of this paper. We propose an approach that can protect election integrity in SA.

II. ELECTIONS AND ISSUES IN SA

SA is a multi-party democratic nation and conducted its first general elections in 1994 under a system of proportional representation (PR) [13,14,15]. Elections are spearheaded by the Independent Electoral Commission (IEC) and elections types are the national, provincial elections and the Local elections [13]. Since the birth of democracy, SA elections have been free and fair despite the rated flawed in the world Democracy Index survey carried out by Economist [13]. However, the electoral system used does not fully assure the

integrity and needs to be enhanced to increase its trustworthiness. This stems from the fact that trust in democracy is promoted when the voter registration and the voting process are transparent, not corrupted or fraudulent.

The role of voter registration is especially important when it comes to emerging democracies as it may make or break an election [11]. One issue with South Africa electoral system is that the voter registration method employed does not fully protect the integrity of the elections. Although believe to be free and fair, yet the system do not guarantee that one man only register once. For instance, the zip-zip barcode reading machines employed for capturing voter's information is only concerned with automatic recording and matching of voter's information with no visible verification and identification that is transparent to every voter [17]. In this way, possible avenue for election frauds such as impersonation and multiple registrations may be created and exploited. For example, it is possible for a voter to register twice or more in same or different location if he/she has more than one ID book in possession or even registers for some one. This may exist because no strong security measures that is in place to track and point out these forms of frauds.

In the same vein, the kind of identification done at the voting station on Election Day lacks security strength. The measure employed neither guarantee that one man only vote once nor ensures that the vote is cast by an authentic person. With such approach, a voter may only vote if his/her name and ID number is found on the voter's roll or has any proof of registration. Going by the case of multiple registrations, it is also possible for voter having more than one ID book and registration to vote as many times as registered because no strong security measures is in place to track them down. In addition, the ink on voter's thumbs after voting can easily be washed with strong chemicals with no trace. If this is allow to continue, the integrity of SA elections cannot be upheld and may lead to failure of democracy one day. Hence, it is important to employ an approach that is strong enough to ensure that one man registers or vote only once irrespective of the location or documents at hand. This requires that SA election has to be conducted in a real-time mode.

III. PROPOSED SYSTEM STRUCTURE

A. System Components

The various components that are required for the system to meet the objectives of voter's registration and identification are discussed below:

1) Central Database:

The proposed system requires the creation of the central where information about voters will be stored and retrieved. Since SA elections take place in all the three tiers of government: local, provincial and national levels, the national database (i.e. central database) will be designed to host other sub-databases (i.e. Local databases) which represent each local/municipalities as shown in Figure 1. Valid access point during the registration and voting (i.e. identification) exercise will be at the local level where voter's information are captured. Both registrations and voting stations will be connected directly to the central database on a real-time mode for recording, storing, modification and retrieval of voter's information where applicable for verification and identification purposes. The information that can be captured about a voter and their status is shown in Figure 2.

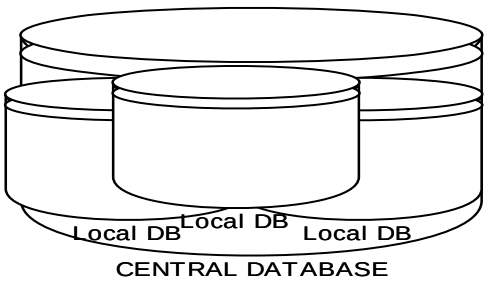

Figure 1. The Central and Local Databases

Within the central database, each local database will have at least three entities: Voter's details, Registration Status and Voting Status. The status will be: disqualified, voted, not_voted, registered, and not_registered respectively. Figure 2 shows the relationship between these entities in the local database. The relationship is given as follows:

- Voters -----> Reg. Status: Several Voters can have 1 Status(Registered or Not_Registered)
- Voters -----> Voting Status: Several Voters can have 1 Status (Disqualified, or Voted or Not_Voted)

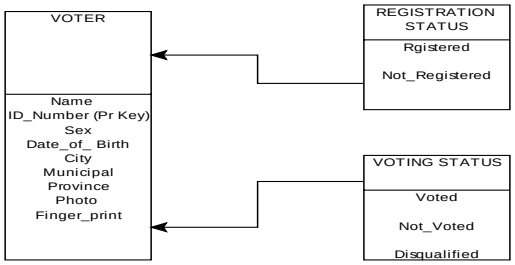

Figure 2. Relationships between the Entities

With the IEC interface, the databases can be accessed via VOTEX (i.e. the proposed prototype) using the Finger Print or voter's ID No as inputs. The database will also keep account of all ***voted*** and ***not-voted*** individuals in order to keep falsification of election results in check. It will also provide support to both governmental and non-governmental sectors that will need verification of the citizenship or in other capacity in a read-only mode.(see Figure 3.)

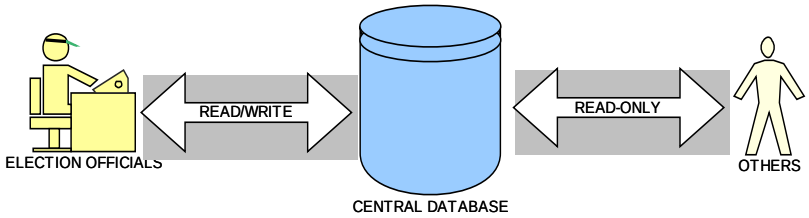

Figure 3. Central Database Access

2) Other Components and Devices

Other devices that are critical to the realization of the system are the Mobile PC with strong wireless network capabilities, Biometric devices (i.e. Finger print readers) and cameras for capturing finger print images and voter's photo images respectively. All devices will be connected to the mobile PC physically during both registration and voting identification exercises where applicable as shown in Figure 4. Another important component is the secure, fast and reliable IEC network facility that can cover all nooks and corners of the country. The fast network connection between the central database and the IEC stations (i.e. registration and voting) is vital to enhance fast storage and retrieval of voter's information. We recommend connection in the form of a wireless local area network (WLAN).

B. System Architecture

The architecture of the proposed system as well as the components required at both Registration Station and Voting Station is shown in Figure 4. Details of how the architecture works are explained along side the operation of VOTEX system in subsequent sections.

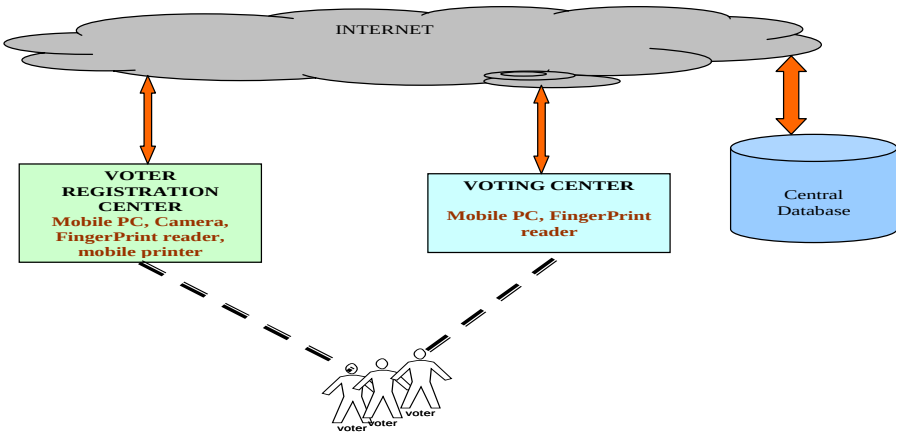

Figure 4. System Architecture

IV. SYSTEM IMPLEMENTATION

A. *System Requirements*

Based on the overall goal, the two basic functional requirements that are expected to be satisfied by the proposed system, ignoring all other requirements are as follows: (1) R1: the system shall allow a voter to register **only** once for an election, and (2) R2: the system shall allow one man to one vote **only** once. With these requirements, the task is to design and implement an electoral system that will satisfy the above R1 and R2. R1 is the key requirement that implements one person, one registration, while R2 implements one man, one vote.

B. *VOTEX System*

Our proposed system is called VOTEX and is a web-based system developed to provide two services: voter registration and voter identification on a real-time manner. VOTEX is not a voting system or party related system but a system to help combat the issues of election frauds. It is a prototype implemented with the requirements that are critical to the goals of this paper. At the left hand side of the home page shown in Figure 5 is the VOTEX Login where access can be granted to only authorize users. With VOTEX, only two types of users are allowed access to the system: IEC system administrators and IEC officials authorize to register and identify users.

Figure 5. IEC Home Page

1) *User Login*

When an IEC official logon to VOTEX, the user is redirected to a page where applicable operations can be chosen- VoterRegistration and VoterIdentification as shown in Figure 6.

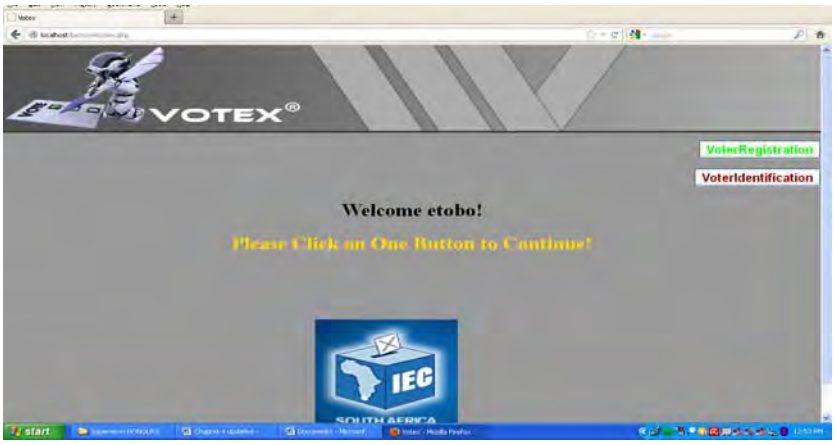

Figure 6. IEC Home Page

The VoterRegistration opens a voter registration page which is equipped with the following functionalities: (see Figure 7)

- Check Registration Status: Where individuals are checked against registered already or not.
- Register Voter: Where unregistered individuals are register

- Update/Delete Voter: Where modifications to already registered individuals are done.

On the other hand, VoterIdentification opens Voter Identity another page where voters are identified or check vote_status. The page is equipped with the following functionalities:

- Identify Voter: Where a voter is checked against information stored in the database during registration exercise.
- Check Vote Status: Where identified voter is check against voted or not_voted
- Register Vote: Where *not_voted* voter's status is changed to *voted* after voting.

For security reasons, the VoterRegistration page is only enable during voter registration exercise and is disable during Election Day. Accordingly, VoterIdentification page is enable during Election Day and is disable during voter registration exercise.

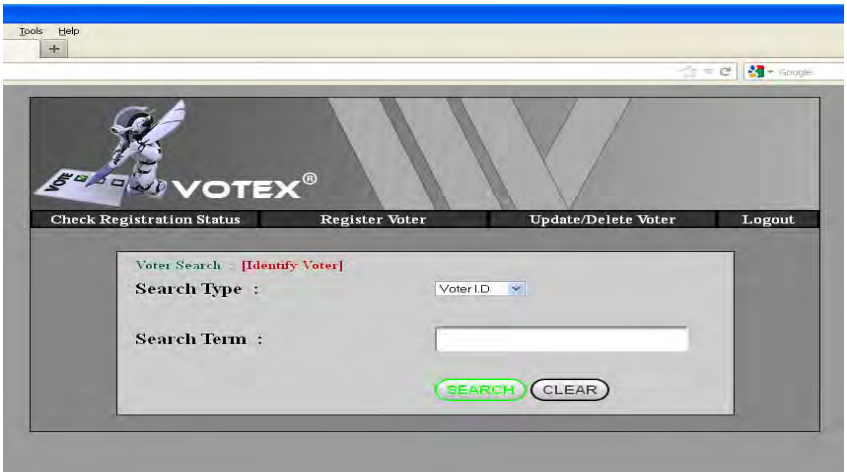

Figure 7. Voter Registration Page

2) Admin Login

When an administrator logon to VOTEX, the admin is directed to the admin page which is equipped with the following functionalities:

- Create/View User's Account/Clear table
- View Voter/Print Database/Clear table
- View Registered Vote Database/Clear table
- Check System Security/Clear Logged Intrusions, etc

With these functionalities, an administrator can view, create and print out all the tables stored in the database.

C. System Operations

1) Real-Time Voter Registration: Voter registration is the first exercise in any electoral process where eligible voter's information is captured for onward use. Real-time registration is the exercise towards ensuring the integrity of the elections and to guard against election frauds. The rationale behind the real-time registration is that, if a voter has finished registering in one centre and decided to go to another centre to register, even if he or she has more than one ID book, the information (i.e. the Finger print or ID No) in the central database will be used to track he or she down and be denied another registration immediately. The procedures to achieve this idea are outlined as follows: (See Figure 4)

Step 1: Data Capturing

i. At the registration station on a public registration day, Voters need to show their bar-coded green ID book or a temporary ID document and proof of residence to validate that they live in the area.

ii. After verifying that the voter lives in the area, the next step is to check the registration status of the person with VOTEX by using the ***finger prin***t as input. If the voter has already registered in another location, the system will display all his/her registered information and will not be allowed to register again. See Figure 8.

iii. If the voter hasn't registered yet, VOTEX will return "**Voter not found**" and then proceed to the next stage which is the actual registration. At this point, the entire voter's information shown in Figure 2 will be captured and stored into the central database in a real-time mode. With VOTEX, voters' information can be collected, recorded, updated, deleted and stored. The mobile printer will be used to print out temporal proof of registration to registered voters.

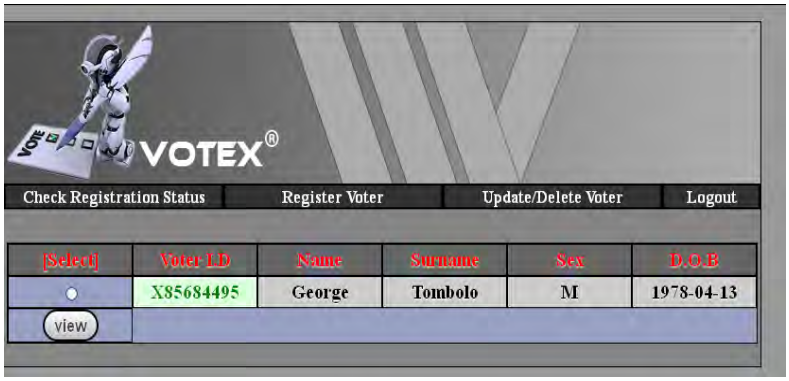

Figure 8. Registered Voter Status

2) Real-Time Voter's Identification and Voting: On Election Day, the first operation at the polling station is the real-time identification of voters. This is very critical to election fraud detection and minimization. During this process, each voter will be individually identified against the information stored in the central database on a real-time manner via VOTEX system.

How it Works:

i. Shown in Figure 4, as a voter enters the voting station, his or her finger is scanned with the fingerprint reader by the electoral official. The output of the operation is then used to automatically query the central database directly in order to identify the voter.

Figure 9. Valid Voter Information

(a) Upon valid match (i.e. valid registered voter), specific stored information about the voter are display by VOTEX as shown in Figure 9.

(b) Upon invalid match, VOTEX will return "**Voter not found**" and he/she will not be allowed to vote, meaning he/she is not a valid or registered voter. The voter is then sent out of the voting station.

ii. With a valid match, the next stage is to check the Voting Status of the voter. That is, check if he or she has ***voted***, ***not_voted*** or ***disqualified*** using the ID No. or the first/surname.

(a) If the status is ***voted***, the system will display the page shown in Figure 10 and will not be allowed vote again. The page will display the voter ID, the city where voting takes place, the vote_status and the exact time he or she voted.

(b) If the voter hasn't voted before or the status is **Not_Voted,** VOTEX will return "**Voter not found**" which signifies the voter should be allowed to vote. After voting, the Vote Status is immediately changed to **Voted**.

With VOTEX, the actual voting can take any strategy either by traditional approach or through the use of voting machine as long as voter's privacy is preserved.

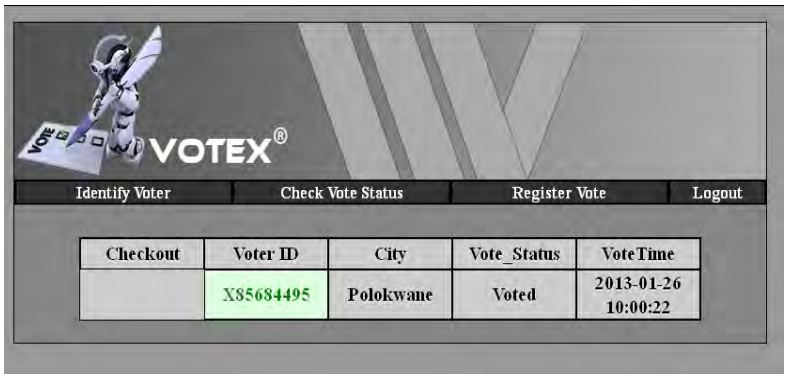

Figure 10. Voter's Voting Status

V. DISCUSSIONS

The transparency and trustworthiness of any electoral system is what characterized it to be free and fair which in turn, is one of the cornerstones of democracy. The fact is that, in any democratic setting, free and fair election is linked to having a generally acceptable result that goes with organizing and conducting elections in an unbiased and fair manner, devoid of frauds or malpractices [8]. This is because trust and confidence in democracy is only promoted when the electoral system process is transparent and open to all electoral stakeholders [11]. These are the issues we intend to avoid in the SA elections viewpoint. With the operations of the proposed system, it is evident that our proposed system shall set a simple and clear standard for protecting the integrity of the elections if implemented (i.e. if adopted for use). The approach will not only be beneficial to the SA government, but also to other developing countries in Africa where impersonation, multiple registrations and voting are the order of the elections. This is because, where such situations flourished, failure of democracy is imminent. VOTEX idea is designed to close the security gaps created by the current election process used in SA as discussed in section 2. With VOTEX, irrespective of the location and amount of green ID book a voter has, it is impossible to register or vote more that once in an election.

Another important aspect of VOTEX, is the benefits that may be derived from it usage. Firstly, until now, states in the US have been debating on voter's ID to combat elections fraud, though the idea has not been generally supported by the entire Americans. It is obvious that with this idea, voter's ID may not be necessary during voting since identification shall be done online. This shall in turn saves the cost of procuring voter's ID card or trying to win parliamentary support for its implementation since finger print is the only vital information needed for identification. Secondly with VOTEX, falsifications of election figures or results as common among African nations shall be put under check to promote transparency. For instance, it may be used to support vote count audit where the number of voters who actually voted shall be compared with the number of votes obtained during the counting process. With the information in the central database, discrepancies can be checked before results are officially announced. Lastly, with this proposed method, the central database can be implemented and maintained especially where it never existed. This shall save the cost of creating new ones every time. In addition, the database will also provide supports to other sector of the government and the NGOs (i.e. in a read-only mode) where identification is essential.

In spite of all the benefits discussed above, we perceived some limitations with VOTEX that are critical to its operations. Firstly, because of its mode of operation (i.e. web-based) coupled with the exponential growth of the internet threats where lots of sophisticated malicious activities exist, operation of VOTEX may be negatively affected. Another issue is resistance to change that may manifest due to selfish and conflicting interest of politicians to continually committing election frauds in order to remain in power. Lastly is the maintenance issue which requires regular maintenance of the database. With these negative factors, we believe if carefully addressed with due attention, it can go a long way to enhance the operations and the implementation of the system, that in turns shall protect the integrity of the elections.

VI. CONCLUSION

Today's e-society benefits from ICT in various aspects of life ranging from getting ordinary public services to supporting everyday work. The impact of ICTs on elections has been valuable. It can be used to enhance the democratic process - engage citizens or build trust with the government. Trust building with ICT can also be extended to election processes to promote its transparency. SA elections system needs trustworthiness and transparency in its processes. In this paper, we have presented solutions in the form of real-time registration and

identification of voters in order to protect election integrity. With this approach, eligible voters will be allowed to register and votes only once. As proof of the solution, we designed and developed a novel system called VOTEX that will be used to counter election fraud during the two exercises. We have also highlighted the benefits of such system. We therefore conclude that when relevant ICT tools are taken advantage of in our electoral processes, it can go a long way to rid fraudulent elections practices and uphold its integrity. As part of our future work, we intend to implement other essential functionalities in VOTEX, introduce stronger security measures and finally propose the system to IEC for adoption and implementation.

ACKNOWLEDGMENT

Our special thanks go to the entire staff members of the department of Computer Science and Information systems, University of Venda for the contributions in making this research a success.

REFERENCES

[1] Welch, E. W and Hinnant, C.C., "Internet Use, Transparency, and Interactivity Effects on Trust in Government" Proceedings of the 36th Hawaii International Conference on System Sciences (HICSS'03) IEEE, 2003
[2] Gronlund, A. Democracy in an IT-framed society. Communications of the ACM, January 2001, Vol.44
[3] Guo yanqing, "Analysis on How to Enhance E-Democracy through E-Government", Proceedings of 2011 IEEE International Conference on Management and Service Science (MASS), August, 2011
[4] Deeping Democracy through E-Governance, Pippa Norris, Harvard University, The other e-participation-related article commissioned by the UN as an input into their World Public Sector Report, May 2003
[5] E-Democracy: Putting Down Global Roots, Janet Caldow, IBM Institute for Electronic Government, January 2004
[6] Dill, D. L: Electronic Voting: An Overview of the Problems, Computer Science, Stanford University, 2004.
[7] Simons, B: Electronic voting systems: the good, the bad, and the stupid, Communications of the ACM, October 2004, Vol. 2 Issue 7
[8] Isong, B. E. Ekabua, O. O. and Mbodila, M. "Towards One Person, One Vote via Real-Time Voter's Registration and Identification". Proceedings of the 11th International Conference on e-Learning, e-Business, Enterprise Information Systems, and e-Government (EEE'12). WORLDCOMP'12, Las Vega, Nevada, USA, July 16-19.
[9] Zovatto, D., Payne, M., Trends in electoral participation in Latin America. Paper prepared for the 2003 CSES Plenary Session, Stockholm, October, 2003.
[10] McCann, J.A., Domı´nguez, J.I., Mexicans react to political fraud and corruption: an assessment of public opinion and voting behavior. Electoral Studies 17 (4), 1998
[11] Astrid Evrensel: "Voter Registration in Africa: A Comparative Analysis" EISA, Johannesburg -South Africa, 2006. ISBN: 978-1-920095-93-2
[12] Jones, D.J, "Early Requirements for Mechanical Voting Systems" First International Workshop on Requirements Engineering for E-Voting Systems (Re-Vote'09), 2009
[13] "Elections in South Africa". http://www.etu.org.za/toolbox/docs/govern/elections.html (10/10/2012)
[14] Electoral Institute for the sustainability of Democracy in Africa. www.eisa.org.za/WEP/sousystem.htm. (10/30/2012)
[15] Robert M. and Roger S."Popular Attitudes towards the South African Electoral System", September, 2003. (28/10/2012)
[16] Mozaffar, S., Schedler, A., "The comparative study of electoral governance - introduction". International Political Science Review 23 (1), 2002
[17] "South African Election Types" http://www.elections.org.za/content/Dynamic.aspx?id=575&name=Elections&LeftMenuId=100&BreadCrumbId=220&ekmensel=14ae2c49_100_252_btnlink. (28/10/2012)
[18] Dill, D. L: Electronic Voting: An Overview of the Problems, Computer Science, Stanford University, 2004.
[19] Bertrand Haas, "Engineering Better Voting Systems", DocEng'06, ACM, Amsterdam, the Netherlands, October 10–13 2006, p-56-58
[20] Guy S. Goodwin-Gill. "Free and Fair Elections", Inter-Parliamentary Union Geneva 2006, ISBN: 92-9142-277-0
[21] Gil, Y., Moon, D., Pan, S. and Chung, Y., Fingerprint Verification System Involving Smart Card, InformationSecurity and Cryptology - ICISC 2002 (LNCS 2587), Nov. 2002, Seoul, Korea.
[22] Diaz, Raul. "Biometrics: Security Vs Convenience". SecurityWorld Magazine. 30 August 2010.