# A New Approach for Protecting Elections Integrity in South Africa

Bassey Isong
Department of Computer Science and Information System, University of Venda South Africa

Ndwamato Netshipise
Student, Department of Computer Science and Information System, University of Venda South Africa

Gilbert Dzawo
Department of Computer Science and Information System, University of Venda South Africa

## ABSTRACT
The transparency and trustworthiness of any electoral system is what characterized it to be free and fair that in turn is indispensable to democracy sustenance. Although elections in South Africa (SA) has been free and fair as reported, the system neither completely guarantees one man registers/votes once nor assures that a vote is cast by authentic persons. Consequently, election fraud as multiple registration, multiple voting, figure falsification and impersonation are not exception, though remains unnoticed. It may be as a result of lack of strong security measures in place at both voter registration centers and voting stations. With situation of this kind, the trustworthiness and the integrity of the elections may be threatened or compromised, and even result resulting to failure or corruption of the democracy. Therefore, integrity of the elections has to be upheld. This requires the application of relevant information and communication technologies (ICTs) tools into the electoral process to enhance both voter registration and identification of voter processes. In this paper, the objective is to propose a form of real-time voter registration and identification. In addition, a novel system called VOTEX is developed that implements the stated problems using radio frequency identification (RFID) and biometric technologies. Also, the benefits and limitations of the application to the SA government are discussed.

## Keywords
Elections, Voters, e-democracy, Real-time, Registration, identification, Finger print

## 1. INTRODUCTION
The transparency and trustworthiness of any electoral system is what characterized it to be free and fair [1]. Accordingly, having regular free and fair elections constitutes one of the cornerstones of democracy. In a healthy democratic setting, an important product of free and fair elections is having election results that are generally accepted by the entire public. This goes with organizing and conducting elections in an unbiased and fair way, free of election frauds or malpractices [2]. The fact is that trust and confidence in democracy are only promoted when the electoral system process is transparent and allows for the participation of all electoral stakeholders [3]. Case and studies in existing literature have shown that when citizens lack full confidence that their elections are free and fair, a decline in levels of voter participation is always the result [4],[5]. Hence, for democracy to be established and sustained, confidence in electoral processes is perhaps a precondition. SA is not an exception. To achieve this, it is important that the electoral system incorporates e-democracy that is not only limited to the communications of policies, but also employ in both registration and voter's identification in order to enhance the transparency of the process.

E-democracy is the use of ICTs tools such as the Internet to engage citizens support the democratic decision-making processes and strengthen representative democracy [6]. It is at the junction of traditional democratic processes and internet technology aim to strengthen democratic processes and institutions. E-democracy can improve the democratic course, increase the opportunities for communication and facilitates electronic input to policy development [6]. As a welcome development, the use of ICTs on electoral processes in most developed nations; electronic voting (i.e. e-voting) in particular, has been useful, characterized by effectiveness in the voting process. This is evidenced in many nations of the world such as the US, UK, France, Brazil, India, etc. [7]. Despite the reported flawed of e-voting [8], with e-voting approach, election winners and the general public can be contented with the results if it is adequately transparent, accurate, free, and fair since it is based on the strong procedures and working methods [2],[9].

However, the practice of e-democracy and the application of ICTs in the electoral system in Africa are at the infant stage. For instance, though SA employs some forms of ICTs in its electoral process, such tools are not fully utilized at all levels of the process – voter registration and Election Day, and activities are highly dominated by paper work. In addition, with the current scheme, it is impossible to track down election frauds. It does not fully guarantee one registration for a voter or one person vote only once. Consequently, possible election fraud in the form of multiple registration, multiple voting, figure falsification and impersonation are not exceptional, though remains unnoticed. It is believed that if electoral systems of this kind continue to exist, the trustworthiness and the integrity of the elections will be threatened, resulting to failure or corruption of democracy [2],[10]. Therefore the integrity of the South African elections has to be upheld.

To uphold the integrity of the elections, it has to be made more transparent, trustworthy, accurate and reusable. This begins with addressing election frauds emanating from voter's authentication and verification during registration and identification of voters. With this approach, eligible voters can register only once and votes only once. Therefore the objective of this paper is to propose a new approach of voter registration and identification during elections in order to ensure election integrity in SA. Furthermore, to authenticate this idea, a novel system called VOTEX System that implements the afore-mentioned issues is developed. Tools such as RFID, biometric technologies and secure wireless network are utilized. Also, the benefits of the system to the SA government and its citizens are discussed.

This paper is organized as follows: Section 1 is the introduction, section 2 is an overview of SA elections and issues, section 3 is the proposed approach, and section 4 presents the VOTEX system. Section 5 shows the system security implementation and the benefits of VOTEX are shown in section 6. Finally limitations and conclusion are given in sections 7 and 8 respectively.

## 1.1 Why Traditional Electoral System and Not E-voting?

Many voter's registration techniques and voting systems exist but despite of these, electoral systems still suffer large scale election frauds world wide. Modern electoral systems such as e-voting systems in particularly have been commendable, though there was widespread lack of significant public confidence on the use of the system as well as its results due to several flaws reported specifically in the US [8]. 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, etc [2],[7],[8].

Particularly in Africa, the problems associated with e-voting are complicated and cannot be handled due to the technological complexities involved. However, African countries can only embrace modern technologies embedded in e-democracy into its electoral system in a form that can handle. By this, the traditional electoral system needs to be re-engineered by employing some basic relevant ICT tools which can help alleviate the existing problems; multiple registrations, multiple voting, impersonation, rigging, etc. This however forms the basis of this paper. We aim at proposing an approach that can protect election integrity in SA.

# 2. SA ELECTIONS SYSTEM

In any state like SA, the authority of the government can only be derived from the will of the people as expressed in genuinely free and fair elections [11]. SA is a multi-party democratic nation and conducted its first democratic, non-racial general elections in 1994 under a system of proportional representation (PR) [1],[12],[13]. The election process begins with the voter's registration, actual voting, counting and the announcement of election results. Elections are spearheaded by the Independent Electoral Commission (IEC) body and elections types are the national, provincial elections and the Local elections [1].

Since 1994 till date, SA elections have been free and fair despite the rated flawed in the world Democracy Index survey carried out by Economist [1]. However, the electoral system used does not fully pledge its integrity and needs to be enhanced. 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 [3]. In addition, the legitimacy of the electoral process is critical to the establishment and maintenance of a strong democracy [14]. Table 1 gives details of the current elections scheme while Figure 1 and 2 shows the representation of the voter registration and voter's identification/voting respectively.

**Table 1. Current election process in SA**

| **Election Process** | |
|---|---|
| **Voter Registration** | **Voting** |
| **On a public Registration Day:**<br><br>i) At the registration centre, voters present their **bar-coded green ID book** or a temporary ID document and validate their residential area.<br><br>ii) A special machine (Zip-Zip) in each registration centre is used to scan the bar-coded ID book and automatically records the correct information about the name and ID number for the voter's roll. Duplicates are avoided due to the uniqueness of each unique national ID number.<br><br>iii) At the end, a sticker is printed and paste on ID book as proof of registration | **On a Election Day:**<br><br>i) At the voting center, voter presents their **bar-coded green ID book** or a temporary identification certificate to the voting officer.<br><br>ii) Voting officer checks if the voter is a registered voter on the voters' roll. If the name is not found on the voters' roll, but have proof of registration, the Presiding Officer must validate the proof of registration otherwise, sent not allow to vote.<br><br>iii) Once validated and the voting officer is satisfied that the voter have not already voted, the voter's name is marked off, the ID book stamped, and thumbnail inked.<br><br>iv) The voter is then given a ballot paper and allowed to cast vote secretly. |

## 2.1 Issues with SA Elections

There are several issues in SA electoral process originating from the current used scheme as shown in table 1, Figure 1 and 2. These issues are discussed in two perspectives: registration and identification. Firstly, the role of the voter

registration is basically important when it comes to emerging democracies as it can make or break an election [11]. One issue with the SA electoral system is that the voter registration method employed does not fully protect the integrity of the elections. Although considered free and fair, yet the system neither guarantee that one man registered only 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 [15]. In this way, possible avenue for election frauds such as impersonation and multiple registrations could 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 someone. This may exist because there are no strong security measures to track and point out these forms of frauds.

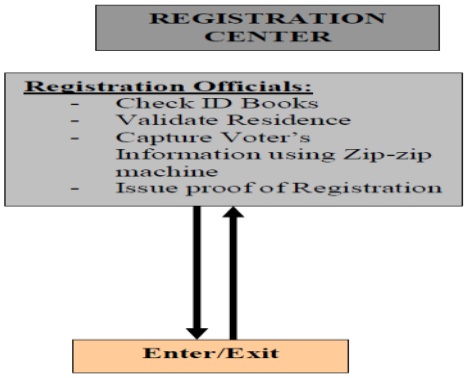


**Fig 1: Voter Registration**

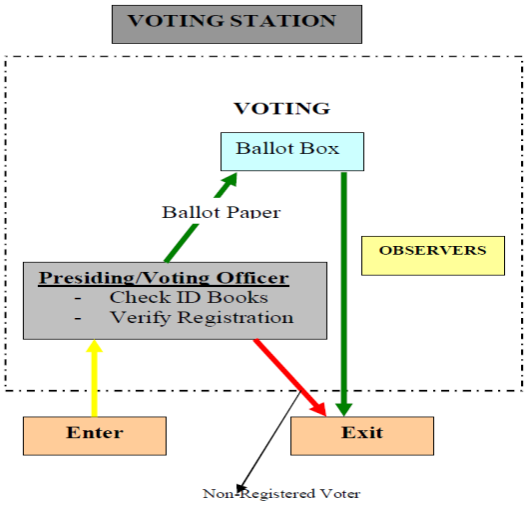


**Fig 2: Voter's Identification and Voting**

Secondly, the type of identification done at the voting station on Election Day lacks security strength. The measure employed neither guarantee that one man votes only once, nor ensures that the vote is cast by an authentic person. With such approach, a voter can 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 register to vote as many times as registered because they are no strong security measures in place to track them down. In addition, the ink on voter's thumbs after voting can easily be washed with strong chemicals without any trace. If this is allowed to continue, the integrity of SA elections cannot be upheld and can 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. This requires that the SA election has to be conducted in a real-time mode – the goal of this paper.

# 3. THE PROPOSED APPROACH

## 3.1 System Requirements

There are several requirements that are expected to be satisfied with our proposed system. However, based on the overall goal and objectives, the three basic functional requirements, ignoring all other requirements are stated below:

Req1: The system shall allow a voter to register **only** once for an election

Req2: The system shall allow one man to one vote **only** once.

Req3: The system shall not allow any forms of unauthorized access or receive malicious input.

With these requirements, the task is to design a system that will satisfy the above stated requirements. Req1 is the key requirement that implements one person, one registration, while Req2 is the one man, one vote. Lastly, Req3 implements the minimum security that protects the system.

## 3.2 System Components

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

### *3.2.1 The Central Database*

The creation of the central is indispensable to the proposed system. SA elections take place in all the three levels of government: local, provincial and national levels, which requires the creation of a national database, otherwise called central database with sub-databases (i.e. tables) - provincial and local databases. Each provincial database will in turn host different databases (or tables) that represent each local/municipalities that resides under it. (see Figure 3).

Valid access point during the registration and voting (i.e. identification) exercise is at the local level where voter's information is captured and retrieved. 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 information capturing, identification and verification purposes. The information that can be captured about a voter and their status is shown in Figure 4.

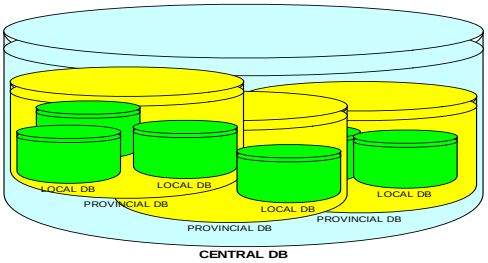


**Fig 3: The Central DB, Provincial DBs and Local DBs**

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. The relationships between these entities in the local database are shown in Figure 4. 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)*

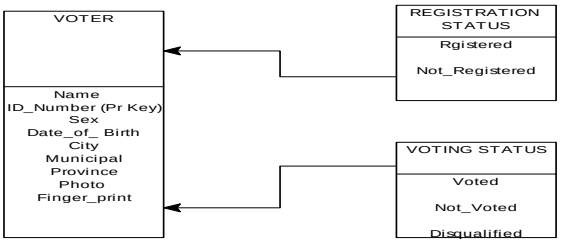


**Fig 4:** Relationships between the Entities

With the IEC interface, the databases can be accessed via VOTEX using VoterID no. or the Finger Print. The database will also keep account of all ***voted*** and ***not-voted*** individuals in order to keep falsification of election results in check as well as provide support to governmental and non-governmental sectors that will need verification of the citizenship or in another capacity in a read-only mode. (See Figure 5)

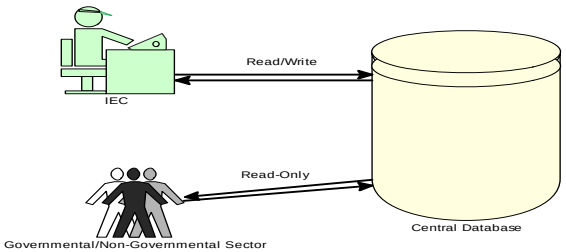


Fig 5: Accessing the Central Database

### *3.2.2 Voter Identification Card*

VoterID is one of the key inputs to the proposed system identification and a ticket for the actual voting. The RFID-based VoterID coupled with the reader is set to replace the Zip-zip machine currently used by SA-IEC. In this study, card designed with passive RFID tag that will be scanned by the RFID Reader is recommended. The tag will contain the Electronic Product Code (EPC) which is a bit like a unique web address for each object (i.e. Voter). The Electronic Product Code (EPC), a scheme designed for universal object identification with the associated standards developed by EPCglobal Inc [16]. (See Figure 6). The RFID tag will take the following format:

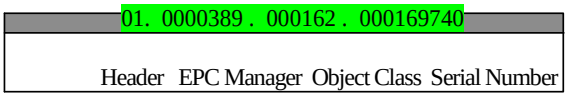


**Fig. 6: Electronic Product Code sample**

1. Header: The Header identifies the EPC format used by the tag. It can be 96-bit, 64-bit or 256-bit.

2. EPC Manager: This will contain the organization, IEC – SA who is responsible for the VoterID the EPC is attached to.

3. Object Class: This will be used to identify a specific Local Database where each voter's information is stored.

4. Serial Number: This will be a unique number of items (i.e. VoterID number) within each Object Class (i.e. the Local Databases). This serial number field is what sets the RFID EPC apart from bar codes used currently by IEC. This is because barcode standards are unable to distinguish the uniqueness of an item. The serial number will be used to query the database via the internet to retrieve, and update stored voter information. In addition the cards will be designed just like VoterID cards found in various nations like Venezuela, Tennessee– USA, Uruguay, Nicaragua, etc. [17]. (See Figure 7).


**Fig 7: Tennessee VoterID Card Sample**

### *3.2.3 Other Components*

Other devices that are essential 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 fingerprint 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. (See Figure 8 and 9) Another important component is a 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 important to enhance quick storage and retrieval of voter's

information. A connection in the form of a wireless local area network (WLAN) is preferable.

### 3.3 System Architecture

This section shows the architecture of the proposed system as well as their interactions with the components both at the Registration Station and Voting Station. (see Figure 8 and 9). Details of how both setup works are explained along side the operation of VOTEX system in the section 4.

## 4. VOTEX SYSTEM

### 4.1 The 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 basis during registration exercises and Election Day respectively. VOTEX is not a voting system or party related system but is designed to help combat the issues of election frauds the two exercises. It is a prototype implemented with the defined requirements that are critical to the goals of this paper. At this stage of the work, functionality such as capturing and finger print usage along side the RFID-based VoterID hasn't been realized yet due to financial constraints. However, we simulated the VoterID No. that is supposed to be embedded on the RFID tag of the VoterID by manually inputting it.

At the left hand side of the home page shown in Figure 10 is the VOTEX Login where access can be granted to only authorize users of the system. With VOTEX, only two types of users are allowed access: IEC system administrators and IEC officials authorized to register and identify users.

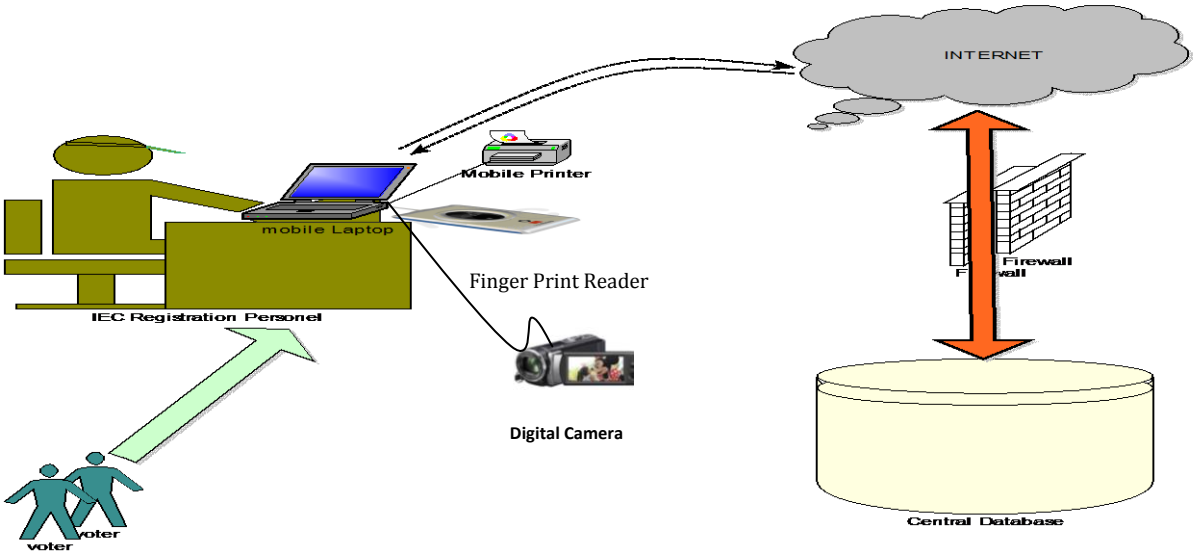


**Fig 8: System Setup at Registration Station**

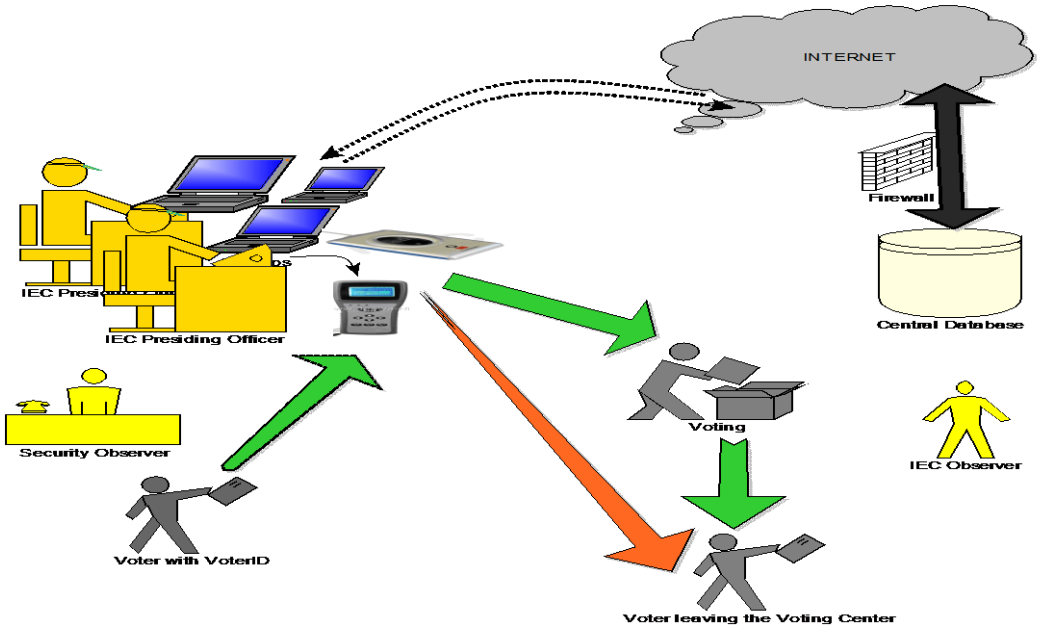


**Fig 9: System Setup at Voting Station**

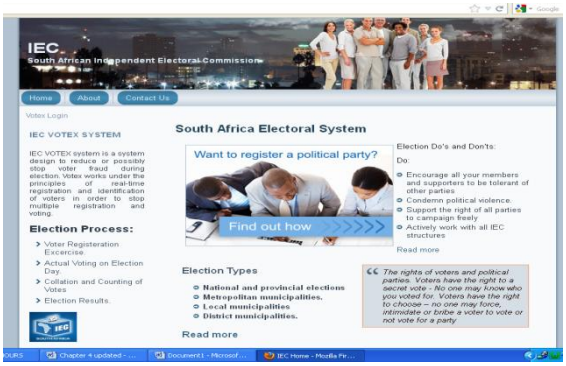


**Fig 10: IEC Home Page**

### *4.1.1 User Login*

When an IEC official logon to VOTEX, he is redirected to a page where applicable operations can be chosen: VoterRegistration and VoterIdentification. The VoterRegistration opens a voter registration page which is equipped with the following functionalities: (see Figure 11)

- Check Registration Status: check whether an individual has already registered or not.
- Register Voter: Where unregistered individuals are registered.
- Update/Delete Voter: Where modifications to already registered individuals are done.

On the other hand, VoterIdentification opens Voter Identity page where voters are identified or vote_status checked. The page is equipped with these 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.


**Fig 11: Voter Registration Page**

### *4.1.2 Admin Login*

When an administrator logon to VOTEX, he is directed to the admin page where the following functionalities are found:

- 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 create, view and print out all the tables stored in the database. For instance, Figure 12 shows a sample of voter registration table in the central database.

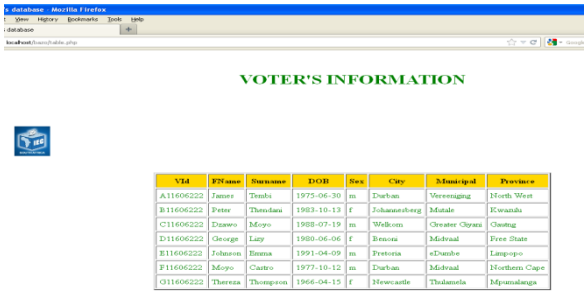


**Fig 12: Voter's Information Table**

## 4.2 Workings of the Proposed System

### *4.2.1 Real-time Voter's 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 has more than one ID book, the information (i.e. the Fingerprint or ID No) in the central database will be used to track him down and be denied another registration immediately. The procedures to achieve this idea are outlined as follows: (See Figure 8).

**Step 1: Data Capturing**

1. 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.

2. 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 ***ID No.*** or ***finger prin***t as input. Fingerprint is more preferable due to its security strength. If the voter has already registered in another location, the system will display all registered information about that person and will not be allowed to register again. (see Figure 13).

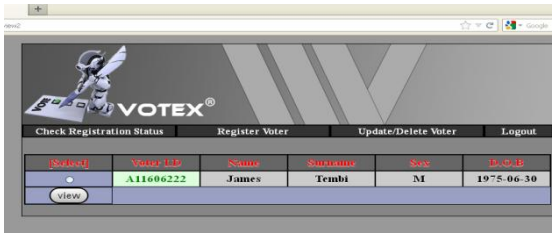


**Fig 13: Registered Voter Status**

3. 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 discussed in section 3.2.1 will be captured and stored into the central database in a real-time basis. With VOTEX, voters' information can be collected, recorded, updated, deleted and stored. The mobile printer is used to print out temporal proof of registration for registered voters.

### *4.2.2 Real-time Voter's Identification*

On Election Day, the first critical operation at the polling station is the real-time identification of voters. During this process, each voter will be individually identified against the information stored in the central database on a real-time mode via VOTEX before one is allowed to vote. The operations within the system are aimed at authentication and verification.

**How it Works**

1. On a general Election Day, as a voter enters the polling station with their RFID-based VoterID, it is scanned with the RFID mobile reader or alternatively, voter's finger scanned with fingerprint reader by the electoral official. The output of the operation is then used to query the central database directly in order to retrieve stored information and identify the voter.(see Figure 9)

   (a) Upon a valid match (i.e. valid registered voter), specific stored information about a voter are display by VOTEX as shown in Figure 14.

   (b) Upon an 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.


**Fig 14: Valid Voter's Information**

2. Upon a valid match and identity, the next stage is to check the Voting Status of the voter. That is, check if he/she has ***voted***, ***not_voted*** or ***disqualified***.

   (a) If the status is ***voted***, the system will display the page shown in Figure 15 and will not be allowed vote again. The page will display the VoterID, the city where voting takes place, the vote_status and the exact time he/she voted.

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

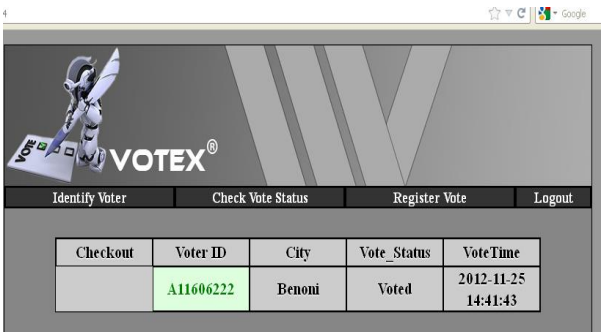


**Fig 15: Voter's Voting Status**

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

## 5. SYSTEM SECURITY

Security is indispensable and of great concern to the proposed system. This is because any system that can operate under network or the internet is always vulnerable to attack like hacking, denial of service (DOS), viruses etc. In order to contain these threats, the proposed design will be one in which the system interface is made available online only during the registration exercise and Election Day. Another level of security is the use of IDS that will monitor the system against all forms of malicious attacks. With IDS, any malicious attack or input thrown against the system will be repelled and access denied immediately.

### 5.1 VOTEX Intrusion Detection System (VIDS)

To guard VOTEX against any form of internet threats, VIDS is developed with the help of PHPIDS. It involves inserting the PHPIDS library in all VOTEX pages via .htaccess file added to the configuration directory to deny all malicious access. The library inspects all the input parameters being passed to the page and compares them to a filter file - pattern based recognition [18].The reporting engine implemented in this work is the database log where the severity level of an event, description, the source IP of the event, the URL upon which the event was detected, and the suspicious payload that triggered the event are logged. In VOTEX, an impact values greater than 40 is considered a serious attack and requires necessary actions to be taken by the system administrator.

To see the effectiveness of VIDS, we simulated several of attacks using malicious codes. VOTEX was found responding positively against the attacks. For instance, whenever any attack is lunched or malicious input sent to the application, the PHP scripts immediately stop executing and display a warning page to the attacker. (see Figure 16)

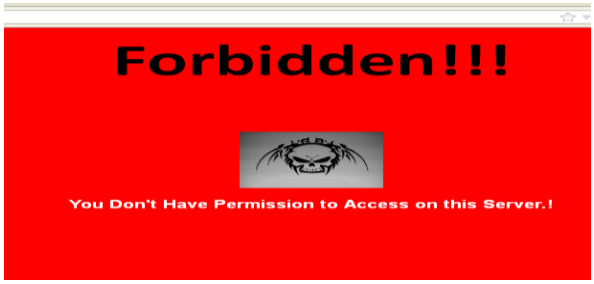


**Fig 16: Access Denial to any attack**

The corresponding database log for the various attacks is shown in Figure 17.

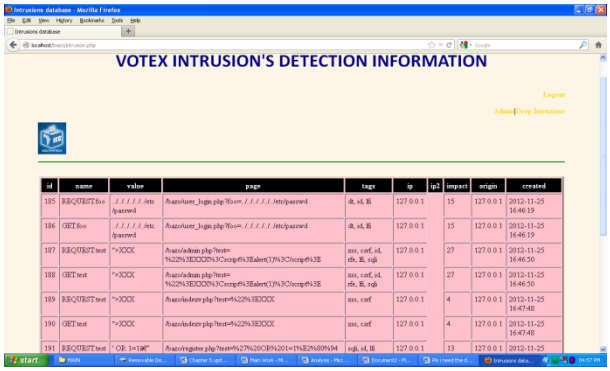


**Fig 17: Logged Intrusions**

The intrusion table in Figure 17 shows the various logged attacks thrown onto the system. The table shows the source of the attack (IP address), the impact value which can prompt necessary actions, the page attacked, the time the attack was throwned, etc. with the logged information, the impact value and the source of the attack can be known to the system administrator and necessary actions taken where applicable.

## 6. VOTEX BENEFITS

Based on its mode of operations, it is clear that this proposed system will set a simple and clear standard for protecting the integrity of SA elections if implemented. It will be of more benefit to the SA government in particular and other developing countries in Africa where impersonation, multiple registrations and voting are the order of the election. This is because where such situations are allowed to continue unnoticed the integrity of the elections can be undermined and even threaten democracy. Hence, elections have to be conducted in a transparent manner and results generally accepted by the public. VOTEX idea is one way to ensure such as it is designed to close the security gaps created by the current election process as discussed in section 2.1. 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 can be derived from it usage. Firstly, until now, states in the US have been debating on voter's identification to curb election frauds, although not generally supported yet by the entire Americans. It is obvious that with this idea, VoterID can serve such purpose and will in turn save the time trying to win parliamentary support for its implementation. In addition, the approach will promote re-usability of the tools. The VoterID can be re-used in present election as well as in subsequent ones, saving SA government the time, effort and cost of procuring sets of new tools. The VoterID card can be used as national ID card in any identification capacity especially where none exists or can replace the existing ones. With this, citizens can use their VoterID instead of going about with green book ID.

Secondly with VOTEX, falsifications of election figures or results as common among African nations can be put under check to promote transparency. For instance, it could be used to support vote count audit where the number of voters who actually voted will 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, national database can be implemented and maintained especially where it never existed. This will 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.

## 7. LIMITATIONS

In spite of the above mentioned benefits, in today's e-society there are lots of existing potential threats that can limit the operation of this proposed system. Firstly, due to its web-based operation coupled with the exponential growth of the internet threats where lots of sophisticated malicious activities exist, the perception is that there are lots of threats which could cripple its operation. These threats could affect its operation negatively either physical or logical and deliberate or not deliberate.

Another problematic issue is resistance to change. Resistance to change is very common in today's society and could pose a serious setback to VOTEX. It could manifest due to selfish and conflicting interest to continually committing election frauds in order to stay in power by politicians. Lastly are the maintenance issues of not regularly maintaining the database. This can be a difficult task except during registration exercise. With these negative factors, it is believed that, if carefully addressed with due attention, it can go a long way protecting the system which in turn could protect the integrity of the elections when VOTEX is adopted for use.

## 8. CONCLUSION

Having regular free and fair elections is indispensable to the sustenance of democracy. This goes with conducting elections in an unbiased and fair way which is free of voter frauds because trust and confidence in democracy is promoted when the electoral system process is transparent to all electoral stakeholders. SA needs trustworthiness and transparency in its election process, particularly the general elections. In this paper, solutions in the form of real-time registration and identification of voters have been presented. 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 both registration exercise and actual voting. In addition, VIDS which is embedded in the application to guard against all forms of malicious attacks was also developed. We have also highlighted the benefits of such system to the SA government and people: a.) Serves as national ID card for identification, b.) vote count auditing, c.) creation and maintenance of a central database, d.) re-usability of subsequent elections tools that saves cost and time. In general, we concluded that when electoral systems make full utilization of essential ICTs tools in its processes, it will help rid fraudulent elections and uphold its integrity. Furthermore, some interesting extensions of this work may include implementation of other essential functionalities and extend VOTEX to provincial and municipal elections in SA, introducing stronger security measures and finally proposing the system to IEC for adoption and implementation.

## 9. REFERENCES

[1] "Elections in South Africa". http://www.etu.org.za/toolbox/docs/govern/elections.html (10/10/2012)

[2] 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.

[3] Astrid Evrensel: "Voter Registration in Africa: A Comparative Analysis" EISA, Johannesburg -South Africa, 2006. ISBN: 978-1-920095-93-2

[4] Zovatto, D., Payne, M., Trends in electoral participation in Latin America. Paper prepared for the 2003 CSES Plenary Session, Stockholm, October, 2003.

[5] 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

[6] 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

[7] Dill, D. L: Electronic Voting: An Overview of the Problems, Computer Science, Stanford University, 2004.

[8] Simons, B: Electronic voting systems: the good, the bad, and the stupid, Communications of the ACM, October 2004, Vol. 2 Issue 7

[9] Dill, D. L: Electronic Voting: An Overview of the Problems, Computer Science, Stanford University, 2004.

[10] "Electoral Fraud" http://en.wikipedia.org/wiki/Electoral_fraud. (15/10/12)

[11] Guy S. Goodwin-Gill. "Free and Fair Elections", Inter-Parliamentary Union Geneva 2006, ISBN: 92-9142-277-0

[12] Electoral Institute for the sustainability of Democracy in Africa. www.eisa.org.za/WEP/sousystem.htm. (10/30/2012)

[13] Robert M. and Roger S."Popular Attitudes towards the South African Electoral System", September, 2003. (28/10/2012)

[14] Mozaffar, S., Schedler, A., "The comparative study of electoral governance - introduction". International Political Science Review 23 (1), 2002

[15] EDIFICE "Radio Frequency Identification (RFID)" The European Network for B2B Integration in High Tech Industries, RFID White paper Issue 1, 14 March 2007

[16] Mark Harrison, "The Electronic Product Code (EPC) and Mass-Serialization Issues for Healthcare", MIT, Cambridge, MA, USA 9 December 2004

[17] "The Voter Identification Card" http://aceproject.org/main/english/vr/vra06d.htm (11/09/2012)

[18] Justin, C. K. "Defending Web Applications with PHPIDS"http://www.madirish.net/node/241 (27/11/2012)

[19] 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.