ACSIJ Advances in Computer Science: an International Journal, Vol. 3, Issue 4, No.10 , July 2014
ISSN : 2322-5157
www.ACSIJ.org

ACSIJ
WWW.ACSIJ.ORG

A Secure Model for Remote Electronic Voting: A Case of Tanzania

Sylvester Kimbi[1], Irina Zlotnikova[2]

The Nelson Mandela African Institution of Science and Technology (NM-AIST)
School of Computational and Communication Science and Engineering
(CoCSE)
P.O. Box 447, Arusha, Tanzania
E-mail: {kimbis[1], irina.zlotnikova [2]}@nm-aist.ac.tz

Abstract

Tanzania is still using paper ballots system as the only voting channel despite the fact that other countries have already implemented remote electronic voting systems for their general and parliamentary elections. With the rapid evolution of Information and Communication Technology (ICT) in today's world, Tanzania should as well seize the opportunity presented by ICT to modernize its electoral process. However, prior to the implementation of remote electronic voting technology, one of the key issues that should be addressed is the security. The importance of security in electronic voting system has been recognized for some time now but implementing a comprehensive security solution has been a challenging task. This paper proposes a secure model for implementation of remote electronic voting via mobile phone or Internet to be used for future presidential and parliamentary elections in Tanzania. We reviewed several remote electronic voting models, analyzed them, and identified their strengths and weaknesses as well as their components. As a result of this review and analysisthe secure remote electronic voting model was developed to meet the requirements of Tanzanian citizens. Data was collected using structured questionnaires. The data was collected from (1) experts in the area of information security, (2) lawyers, and (3) election officials.

Keywords: *Remote Electronic Voting, Information Security, e-Government, Public Key Infrastructure, Electronic Identity.*

1. Introduction

1.1 Background and Rationale for the Research

Citizens' participation in the political process is essential for democracy to be meaningful and feasible. Voting, though it requires little initiative and cooperation with voters, is the most critical and a widespread form of citizen involvement [1]. Traditionally, voting has been a manual and work-intensive operation in Tanzania. There are numerous problems associated with the current electoral system. For example, the reports of general elections of 2005 and 2010 [6] [17] have made reference to irregularities in counting. There is also a serious problem concerning voters' turnout. According to the International Institute for Democracy and Electoral Assistance (IDEA), voters' turnout statistics from recent elections in Tanzania shows a serious declining trend. For example, voters' turnout in presidential election of 2010 was 42.8 percent against 72.4 percent and 84.4 percent in presidential elections of 2005 and 2000 respectively. As the country is striving to improve its democracy, this alarming situation needs to be addressed. Countries with similar problems have introduced electronic voting via mobile phone and/or Internet in an attempt to alleviate low voters' turnout problem. These countries include Brazil, Canada, Estonia, France, Germany, India, Ireland, Italy, Netherlands, Nigeria, Norway, South Africa, Switzerland, United Kingdom (UK), and United States of America (USA) [3].Literature review shows that electronic voting was successful in some countries including Estonia and Switzerland while others such as USA and UK have stopped using them due to security concerns [1][18]. With rapid evolution of ICT and significant investments in ICT, it is important for the government to start initiating the remote electronic voting project. However, prior to the implementation of remote electronic voting in the country, one of the most important issues to be addressed is the security. This paper proposes a secure model for implementation of remote electronic voting via mobile phones or Internet to be used for future presidential and parliamentary elections in Tanzania. The model is also grounded on our earlier study which measures readiness of citizens for remote electronic voting in Tanzania [12].

1.2 General Objective

The general objective of this research was to develop a secure model for implementation of the remote electronic voting system via mobile phones or Internet to be used for future general and parliamentary elections in Tanzania.

1.3 Specific Objectives

Towards achieving the general research objective, specific objectives were as follows;

i. To identify security challenges from the technical perspective that hinder the implementation of remote electronic voting in Tanzania.
ii. To identity security requirements for the remote electronic voting system.
iii. To design a secure remote electronic voting model for Tanzania to overcome security challenges.

2. Related Work

2.1 Current Status on ICT Infrastructure Development in Tanzania

According to data provided by ITU in 2013, over 2.7 billion people used the Internet, which corresponds to 39 percent of the world's population. Tanzania accounts only for 5 percent of the mobile phone users in Africa [11]. According to figures from the Tanzania Communication Regulatory Authority (TCRA), in 2013 there were 169,165 landline and 26.5 million mobile phone users in Tanzania. Like most of the African countries, Tanzania has recorded exponential growth in mobile phones as depicted in Fig. 1.

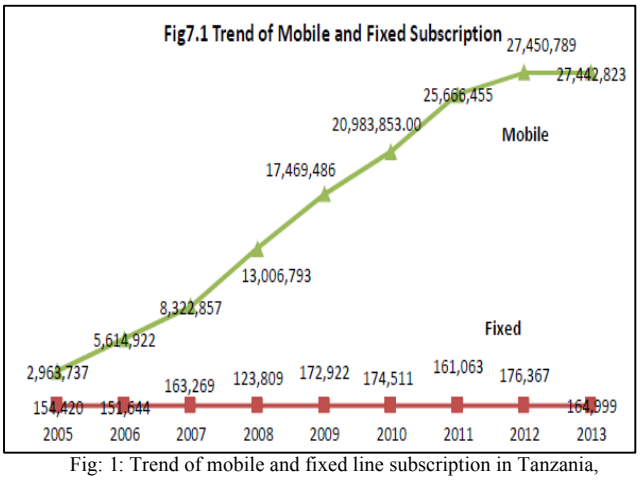

Fig: 1: Trend of mobile and fixed line subscription in Tanzania, adopted from TCRA [20].

Although indicators show rapid growth in the Tanzanian ICT infrastructure, communication facilities are available mainly in the urban areas leaving the rural areas (where the majority of Tanzanians live) being underserved owing to the challenges of cost, electricity and connectivity [19]. According to the statistics of 2013, only 18.4 percent of the total population was connected to the national power grid with two percent of these being in the rural areas [16].This is one of the reasons why rural areas have less ICT facilities and infrastructure as compared to urban areas. Moreover that the government of Tanzania spent over 250 billion in investment of National Information and Communication Technology Broadband Backbone (NICTBB), but still the NICTBB is not being fully utilized to its potential. The backbone is currently operating at less than 10 percent of its installed capacity and even lower at its design capacity [13]. This will affect largely the use of remote electronic voting via internet especially in urban areas.

With regards to security, the government is currently issuing national digital identity cards equipped with a computer-readable microchip. The microchip contains all the information and personal data of the citizens, cryptographic keys, random number generators and algorithms needed to carry out all the computations on behalf of the voter. It also contains an image of the citizen, as well as their fingerprints [21]. The problem with the current digital electronic cards being issued is that a complete PKI support is yet to be implemented [12]. However, plans are underway to have the complete PKI implemented.

2.2 International Experience with Remote Electronic Voting

Several remote electronic voting models have been implemented worldwide using various security controls Qiuel *et al*. discuss mobile devices mediated electronic voting system based on the distributed encryptions [22]. The authors apply the standard cut-of-the-choose method to avoid the computational zero knowledge proofs and show that the proposed scheme is efficient and secure in the simulation-based paradigm. Another model of interest is a Secure Electronic Registration and Voting Experiment (SERVE) which was introduced in 2004 in USA. SERVE is the Internet based voting system built for the Department of Defense's federal voting assistance program. However, the project was abandoned due to anonymity issue where the web server could know the vote of each voter. There were no public key infrastructure and digital identity cards used for authentication in SERVE [17]. UK embarked on electronic voting project aiming at modernizing the electoral system However, despite extensive research, part of the problem with the UK trials is that time for testing and developing the system was inadequate and as a result the experiments were terminated due to security concern [1]. In 2009 Norway initiated a procurement procedure for "E-valg 2011", an electronic voting pilot project for 2011 municipal and regional elections [3]. The main feature of the Norwegian electronic voting model is its openness. Thus Norwegian government attempted to

build trust on electronic voting by making all the documents related to voting publicly available [3]. The model provides security measures against the two major security issues, compromised computers and coercion. Two independent channels were introduced (postal mail and SMS) to provide safeguard against compromised voter's computer. The Norwegian model also uses double envelope system to insure integrity of votes and voter's secrecy [3].

Many other remote electronic voting models, such as Australian and Canadian models have been implemented over the years. However, most of these models have limitations. For example, Canadian and Australian modes they both lack secrecy protection measures [3]. In this view, our work focused on analyzing two remote electronic models: Estonian model [10] and the Swiss model [9] which address most of the security issues.

2.3 Security Requirements for Remote Electronic Voting

As a general rule the remote electronic voting system must comply with all the principles of democratic elections and referendums. Remote electronic voting must be reliable and secure as traditional democratic elections and referendums which do not involve the use of electronic means [4]. In particular, security requirements for remote electronic voting are as follows:(1) to keep all votes secret (2), to ensure accuracy of the system without interference or errors, (3) to achieve democracy by allowing legal voters to vote only once, (4) to provide individual and universal verification to ensure that votes are counted correctly, and (5) to ensure the system is available and accessible for all voters and free from possibility to declare results before the election closes [4].

2.4 Analysis of the Selected Models

We reviewed and analyzed several remote electronic voting models with respect to security. Strengths and weaknesses of each model were identified. Based on this review and analysis the most secure models (Swiss and Estonian) were customized and enhanced to produce a secure model that suite the requirements of Tanzanian. This section gives a detailed review and analysis of the selected models with respect to security.

2.4.1 Estonian Model

Estonia is one of the few countries in the world continuously using an Internet voting system [5] The Estonian model is based on three principles: (1) the identity card for voter identification, (2) the possibility of re-voting electronically with only the final ballot counting, and (3) the priority of traditional voting (should an elector vote by paper ballot on election day their electronic ballot is deleted). Other key requirements to which the model is required to comply with include reliability, security, transparency and auditability [2]. Fig.5 shows a high level architecture of the Estonian model.

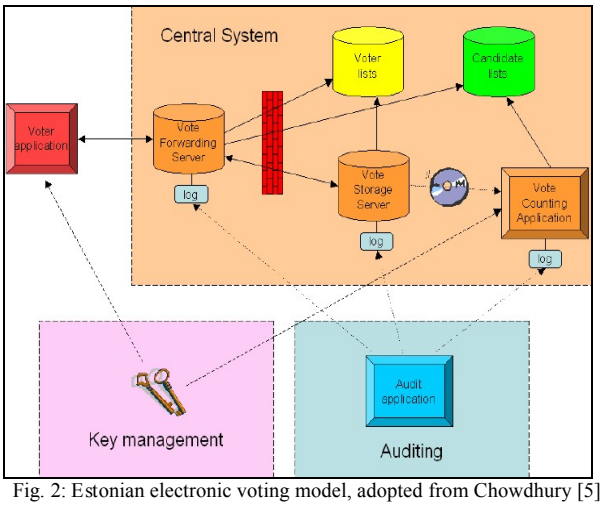

Fig. 2: Estonian electronic voting model, adopted from Chowdhury [5]

Remote electronic voting in Estonia is meant to supplement the traditional methods of voting. The idea is to give voters the possibility to vote from the location of their choice without the necessity of going to the polling station [15].

2.4.1.1 Security Analysis

Despite its acceptability by majority of Estonians, the model has problems that have not been addressed. Foremost, the implemented electronic voting model is only provided in Estonian language despite the fact that there is a very large Russian-speaking population in Estonia. This has created a barrier resulting in many Russian speakers not voting online [2]. The Estonian electronic voting system is also vulnerable to many security attacks. The common sources of vulnerabilities are described below [5].

(i) **Voter Computer (VC):** The computer could be virus affected or affected by any kind of malware. A malicious computer can cast a vote without concern of the voter.

(ii) **Voter Forwarding Server (VFS):** The communication link between voter's computer and VFS is Internet. There are different kinds of attack in this communication link. Internet connection provider can stop the traffic or delay the traffic. Since VFS is in open Internet, denial of service attack is also possible against VFS.

(iii) **Voter Storage Server (VSS):** VSS database application faults enable irregular access to data and ignoring restrictions, therefore the fault-freeness of VSS applications is also a major security issue.

(iv) **Voter Counting Server (VCS):** VCS is the most important component in the system. The public key of VCC is open to all voters and used in encryption of the vote. VCA private key should under no conditions become public and must not under any circumstances be destroyed or become unusable. The source of vulnerability in VCS is from operating system, memory or any kind of virtualization.

(v) **Voter Anonymity:** VSS has encrypted and signed vote. VSS can identify the voter from this encrypted and signed vote but cannot decrypt the vote. Only VCS can decrypt the vote. If VFS and VCS both are corrupted then it can violate the voter's anonymity. Because VSS can unwrap the digital signature and mark the vote by time stamp or any other means then can send this to VCS. VCS can decrypt the vote and learn about the choice. Now if VSS and VCS collaborate together it can identify the voter and learn about his choice.

2.4.2 Swiss Model

The remote electronic voting model used in Switzerland is an adaptation of its postal model. From security perspective Switzerland does not use digital signatures like Estonia. However, the system operates similarly with respect to the envelope feature which keeps the ballot and voter's identity separate [3]. Fig. 6 shows architecture of the Swiss electronic voting system.

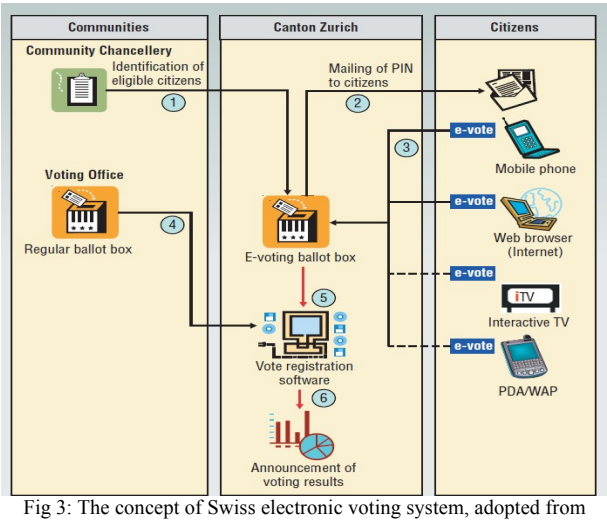

Fig 3: The concept of Swiss electronic voting system, adopted from Giampiero [9]

2.4.2.1 Security Analysis

Despite its success, Switzerland faces security challenges. With the system used so far in electronic voting trials "citizens cannot verify if their vote has been registered and counted correctly [7]. Like Estonian system. Swiss system is also subjected to various security threats. These threats include (1) denial of service attack, (2) vote buying and coercion, and (3) web spoofing [8].

2.4.3 Comparison of the Selected Model

We conducted comparative study of security aspects of the two selected remote electronic voting models (Swiss and Estonian). Based on this comparison, the Tanzanian model was then developed addressing the identified security gaps. Table 1 shows a comparison between Estonian and Swiss models.

Table 1: A comparison of electronic voting models against voting principles.

S/N	Criteria	Estonian Model	Swiss Model
1	Legal basis	Electoral Act is in place but there are no detailed and comprehensive regulations on remote electronic voting.	The constitutional disposition on remote electronic voting has been adopted in a popular vote in February 2009.
2	Advance voting	Advance voting is allowed for electronic voting.	Advance voting is allowed for electronic voting.
3	Voter identification mechanisms	(i) ID card, (ii) digital ID card (without picture, signature and other ID features), (iii) mobile ID.	(i) Password, (ii) birth date, (iii) municipality of origin.
4	Intellectual property rights of the Internet System	The owner of the system is the National Electoral Committee.	The state of Switzerland owns the intellectual property rights.
5	Vote verification mechanisms	Neither return codes nor end-to-end measures are foreseen.	None for the voters.
6	Secrecy protection mechanism	Beyond the cryptographic measures, the system also allows multiple voting and paper ballots during the advance period.	The voter register uploaded into the system is fully anonymous. Voters are only

			identified by their one-time voter number.
7	Open/closed source code	Not all source codes are disclosed to the public.	Not fully available to the public The conditions for accessing the source code are set by the government.
8	System testing and certification mechanisms	Formal certification is not foreseen.	Formal certification is not foreseen.
9	Voting and results audit mechanisms	No specific voting and results audit mechanisms.	Forensic statistic tests are systematically performed on the result of the electronic voting channel.
10	Supported languages	Estonian	Multilingual (Italian, French, Rhaetian and German).

3. Methodology

3.1 Identification of Security Challenges

In identifying security challenges hindering the implementation of remote electronic voting data was collected using structured questionnaires from (1) experts in the area of information security, (2) lawyers and (3) election officials.

3.2 Population and Sampling Method

Our sample was drawn from the governmental organizations. We only selected those government organizations which have direct responsibility of managing electoral process and supporting role to facilitate elections in the country. These organizations are referred to as organizations A and B. The actual names of these organizations are not revealed in this paper due to confidentiality concerns. Organization A is an independent entity responsible for managing electoral process in the country whereas. Organization B is a government agency responsible for overseeing the implementation and management of national identity system in the country. The total population was 342. The sample size was computed by the following formula [14]

$$n = \frac{Z^2 \times p \times q \times N}{e^2 (N-1) + Z^2 \times p \times q} \quad \text{.....(1)}$$

Where N = size of population, n = sample size, e = acceptable margin error (the precision = 0.05), Z= Z value at 95 percent confidence level (1.96), p = sample proportion, q = 1 – p; where q= 0.5.
The calculated sample size of the population was 181. Table 2 presents the estimated number of personnel in each of the selected organizations.

Table 2: Number of personnel in the selected organizations

Position	Organization A	Organization B	Total
ICT and ICT security personnel	16	18	34
Legal officers	5	3	8
Operations personnel	127	132	269
Upper management	10	31	41
Total workforce	158	184	342

3.3 Data Collection

Primary data was collected using structured questionnaires from (1) experts in the area of information security, (2) lawyers, and (3) election officials. We also conducted literature review on remote electronic voting models implemented in other countries.

3.4 Reliability and Goodness of Fit Measurement

The reliability test was conducted by using Statistical Package for Social Sciences (SPSS) to analyze the internal consistence of the questions; the calculated Cronbach's alpha was 0.993 and was most suitable. Furthermore, a Chi-square test was conducted to assess goodness of fit for all research questions. The results show statistical significance.

3.5 Data Processing and Analysis

The content analysis technique was used for processing and analyzing descriptive data. We also used SPSS and Microsoft Excel to analyze data and present the results.

3.6 Designing of a Secure Remote Electronic Voting Model

The second research objective was to design a secure remote electronic voting model. The model was mainly designed using the desk review technique. We reviewed several remote electronic voting models, analyzed them, and identified their strengths and weaknesses as well as their components. During the design process a number of

electronic voting professionals were also consulted. These professionals included (1) experts in the area of information security, (2) lawyers, and (3) election Officials These professionals were selected using a purposive sampling technique

4. Results and Discussions

4.1 Security Challenges

4.1.1 Low Robustness and Security of ICT infrastructure

Although the government has established a National Information and Communication Technology Broadband Backbone, there is no government-wide established ICT security architecture and standardization. The majority of respondents (69 percent) affirmed that the existing ICT infrastructure was established without taking into consideration ICT security issues.

4.1.2 Client- Side Attacks

Voters will be using their mobile phones or computers connected to the Internet to cast their votes. Mobile phones and computers are vulnerable to attacks and cannot be controlled by National Election Commission and therefore it is difficult to apply countermeasures at client side. The majority of the respondents (77 percent) were concerned that unreliable voters computers or mobile phones would create serious problems leading to compromising the integrity of the entire election. Depending on the nature of the attack, possible risks could be as follows: (1) an attacker may randomly alter a voter's choice without the user noticing, (2) an attacker can impersonate a real voter and cast the vote instead of the real voter, (3) an attacker could tamper with secrecy by recording the voter name and choice to then be made public, and (4) an attacker can also launch a denial of service attack to the voter's machine and hence hinder the possibility of the voter to vote. Fig. 2 illustrates an attack to voter's computer or mobile phone.

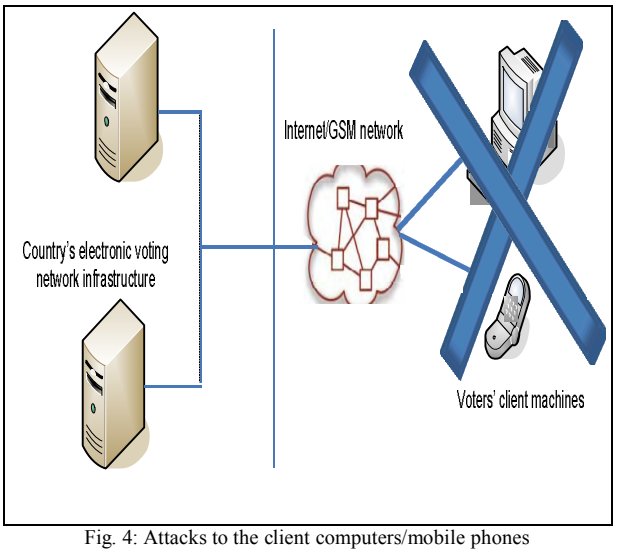

Fig. 4: Attacks to the client computers/mobile phones

Other security threats at the client side include voter coercion and vote buying which are described in detail later in this paper in sub-section 4.6.

4.1.3 Internet-Side/ GSM Attacks

Respondents (84 percent) were concerned that, since electronic votes will be transmitted via Internet or GSM network, an attacker can affect integrity, availability and confidentiality of the votes. Fig. 3 illustrates attacks to internet or GSM infrastructure.

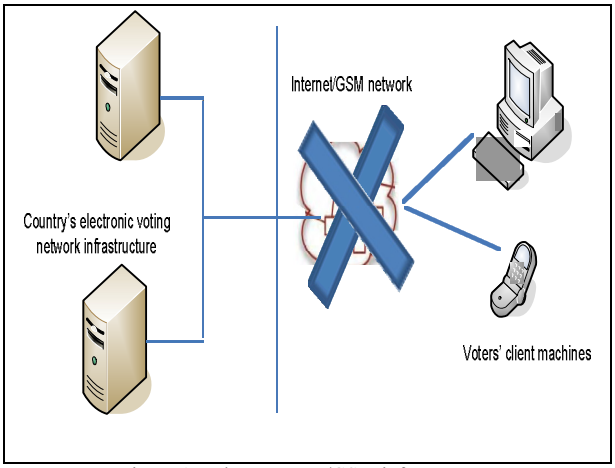

Fig. 5: Attack to Internet/GSM infrastructure

4.1.4 Server-Side Attacks

Respondents (92 percent) were concerned that there was a possibility for an attacker to interact with the remote electronic voting system, its interfaces or parts of it to exploit vulnerabilities. This may compromise security and affects all voting system components. This can be

initiated by political groups which may commit a wide-scale fraud in order to safeguard their political interests. There is also a possibility for denial of service attack that would prevent voters from casting their vote in the system. This may result into having the legitimacy of the whole election being compromised. Fig. 4 illustrates attacks to electronic voting servers

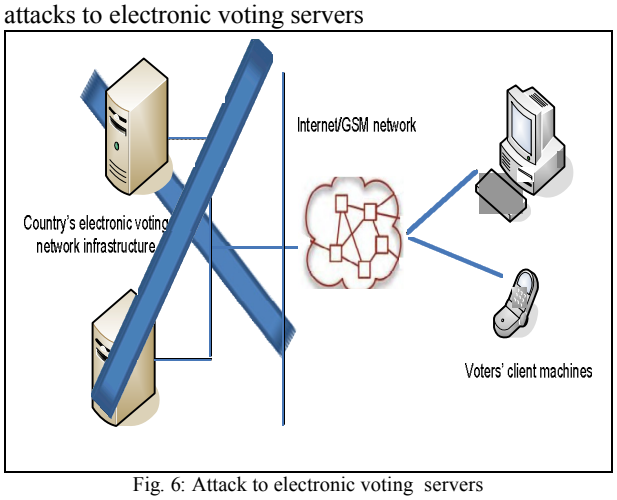

Fig. 6: Attack to electronic voting servers

4.1.5 Voter Coercion and Vote Buying

The majority of respondents (84 percent) were also concerned that, unlike in developed countries, remote electronic voting in Tanzania would present a greater opportunity for voter coercion or vote-buying. Coercion or vote buying takes place when a voter is pressured by others to vote in a way that he or she would not have otherwise. This high level of vote buying and coercion was linked to the high level of corruption and poverty in the country.

4.2 A Proposed Tanzanian Secure Model for Remote Electronic Voting.

We propose a secure model for remote electronic voting system that suits the needs of Tanzanian elections. Our model is based on the country's electronic government framework. The proposed model was developed following the customization of Estonian and Swiss Models. Unique features that distinguish our model from Swiss and Estonian models are as follows: (1) introduction of bilingual local content (Swahili and English) to enable majority of Tanzanians to utilize the system effectively, (2) implementation of public key infrastructure and the use of three-factors authentication mechanism which is enabled by using Tanzanian electronic identity cards for identification and authentication of voters, (3) the use of confirmation code for transparency while maintaining secrecy of the votes, and (4) introduction of an independent body for system testing and accreditation.

Other key principles to which the model is required to comply with include: (1) reliability, (2) auditability, (3) capability to vote several times electronically with only the final ballot counting, and (4) an option to vote at a polling station. The proposed model is also characterized by its modular and service-oriented architecture (see Fig. 8), which allows the integration of mobile phones and Internet for electronic voting. Moreover, the model is grounded on our earlier study which measured readiness of citizens for remote electronic voting in Tanzania [13].

4.2.1 Technical Aspects of the Proposed Model - Addressing the Technical Security Challenges

4.2.1.1 Voters Identification and Authentication Mechanism

We propose three-factor authentication mechanism for identification and authentication of eligible voters. This will be enabled by Public Key Infrastructure (PKI) and a national electronic identity card (e-ID card).Before a vote is cast, a voter must be provided with e-ID card with PKI capability. Currently the government is issuing e-ID but a complete public key infrastructure is yet to be established The proposed processes for producing an e-card with PKI enabled are illustrated in Fig. 7.

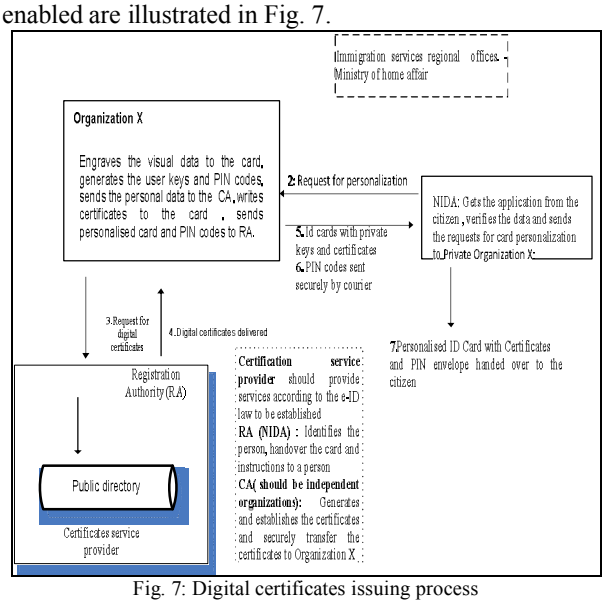

Fig. 7: Digital certificates issuing process

4.2.1.2 System Architecture and Participating Parties

In this sub-section, we specify the proposed system's components and describe their functionality and interfaces. We also describe the participating parties in the system. Fig. 8 presents the proposed system architecture.

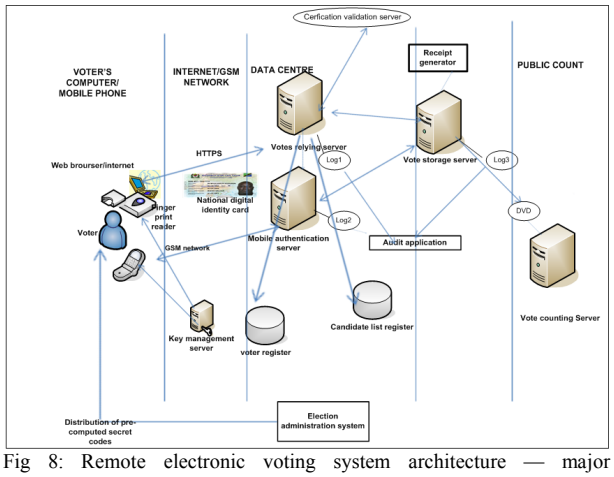

Fig 8: Remote electronic voting system architecture — major components of the system, and how information flows between them.

As shown in Fig. 8, the proposed model consists of the following components.

(i) **Electronic Voting Client Application (e_VCA):** This is an application that runs on voter's computer or mobile phone. The application consists of the candidate information, the key storage and generation functions

(ii) **Electronic Voting Central System (e_VCS):** This is a core system responsible for collection of electronic ballots, storage and tabulation. The roles of the e_VCS are fulfilled by four different servers as follows.

(a) Mobile Authentication Module (MAM) which is an entity within GSM network but is considered as part of electronic voting central system. This component is used to authenticate voters who would like to vote via mobile phones. MAM generates the authentication parameters and authenticates the mobile phone users.

(b) Vote Relying Server (VRS) which is responsible for authenticating voters who would like to vote via internet, distributing electronic ballot to voters and accepting the votes.The VRS should be available over the Internet.

(c) Vote Storage Server (VSS) which is responsible for storing the electronic votes over the period of time and for the anonymization of the votes before the actual tabulation is done. The VSS should be kept behind a firewall.

(d) Vote Counting Server (VCS) which is responsible for the tabulation process. VCS should be offline at all the times to avoid attack.

(iii) **Receipt Generator**. This component is responsible for computation of confirmation codes. The confirmation codes are sent directly to the voters, as shown in Fig. 8, and this has to be done through an independent channel. After receiving this feedback the voter can compare between his choice of options and receipt code, If the receipt codes matches the selected options, the voter can be assured that his vote is recorded as intended.

(iv) **Key Management Server (KMS):** This **component** generates and manages the key pair(s) of the system. The public key (keys) are integrated into e_VCA, private key(s) are delivered to VCS

(v) **Auditing Module**: This component is an application which solves disputes and complaints, using logged information from the central voting system

(vi) **Population Register** : This component is a database for citizens' personal data. It is maintained by National Identity Authority

(vii) **Voters and candidate registers**: This is a database for eligible voters and candidates. The database is maintained by National Election Commission

(viii) **Digital Certificate Validation Server.** This server checks the validity of digital certificates of e-card holders. The server should be operated by independent entity.

4.2.2 Proposed Remote Electronic Voting Process

The proposed model requires that the process of casting a vote start with the voter receiving a voting card from National Election Commission sent by postal/mail or any other secure channel. The voting card should contain necessary information for the voter, as well as pre-computed random generated receipt codes corresponding to possible voting options on the election ballots. These codes will be uniquely generated to the voter, but are random and cannot reveal what the voter voted. When the period of advance voting opens, an eligible voter can use mobile phones or Internet to cast a vote. If the voter decides to vote via Internet, the processes are as follows;

i. The voter launches the client application and inserts her ID card and enters the first PIN number to establish Secure Socket Layer(SSL) connection. The client verifies the server's identity using a hard-coded certificate.

ii. Once a secure connection between a client and VRS is established, the client sends a message with its credentials (second pin number and fingerprint) digitally signed with its private key

corresponding to the public key in voter's digital certificate.

iii. VRS then validates the digital certificate of the voter

iv. VRS checks if the voter is eligible using the data from the population register maintained by National Identity Authority. If the voter is not eligible, a corresponding message is delivered. If the voter is eligible, VRS performs a query from the VSS whether such voter has already voted. If this is the case, the voter is informed about it.

v. The voter receives electronic ballot and select a candidate

vi. VFS asks the user to confirm the choice.

vii. When issued a choice of candidate and political party the voter clicks to submit the vote.

viii. e_VCA encrypts voter's choice and a random number with the public key of the VSS. The voter signs the entire package (as a double envelope scheme) with private key that belongs to him

ix. E_VCA transmits the digitally signed envelope to the VRS which verifies the formal correctness of the received material.

x. The entire envelope is then sent to VSS.

xi. In case of successful vote the VSS sends the VRS a confirmation that the vote has been received. The voter receives an SMS containing the receipt code corresponding to the vote he issues, and can verify this code is correct against the codes on his voting card. By this mean the voter can for instance detect if a malicious program on his computer has changed the ballot. The receipt code can also be used for the voter to verify his vote is present in the latter e-counting process.

xii. An entry about receiving of the vote is recorded in the log-file

xiii. Finally VSS separates inner envelopes from outer envelopes and readies them for the Vote Counting Application(VCS)

If the voter decides to vote through mobile phones, the voting processes are the same as for Internet voting except that the voter uses a mobile phone and authentication is done through the mobile authentication module instead of the vote relying server.

The proposed GSM mobile voting scheme is part of the central voting system and thus voters can choose to vote through the Internet or the GSM network. If voters want to vote through GSM, they have to be registered and obtain a special SIM card with the embedded cryptographic algorithm and national identity. SIM cards should be registered by mobile phone operators in collaboration with National Election Commission

4.2.3 Security Analysis

In this section we critically analyze security of the proposed model and prove that the model conforms to the security requirements presented in Section 2.3.

4.2.3.1 Public Key Management

The core component that provides assurance towards fulfillment of the main security requirements of electronic voting (secrecy and integrity of the votes) is a public key management module. We describe the main concept behind public key management, main risks and possible controls. We use asymmetric cryptograph to ensure the secrecy of voting in the system Under this scheme, a system key pair is generated, the public part of which is integrated into client software and is used to encrypt the vote. The private component of the key pair is used in the vote counting server to decrypt the vote. To increase the security of the private key of the counting server, the key should only be used during counting period. When the election period ends, the private key must be destroyed and should not be used in any other election. The secrecy of electronic voting can be compromised in two ways: an attacker having access, first, to the private key of the system and, second, to the digitally signed votes. Thus to ensure the security the main focus should be on the key management module and especially protecting private key because once the private key is compromised the entire encrypted votes can be decrypted. Generally the private key is subject to two major risks: (1) an attacker may be in possession of digitally signed electronic votes and be able to determine who casts a vote in favor of whom, thus compromising the privacy of the voter, and(2) the private key carrier may be destroyed because of technical errors. When this happens, it becomes practically impossible to decrypt the electronic votes. This is a high concern and therefore we propose that back-ups of the keys pair should be available. These backups have to be properly protected. In our proposed model the key pair is generated in a Public Key Management Module (PKMM) in such a way that the private component never leaves the module. The generation of the key pair and use of the private key is maintained by key managers, there should be several of them. A scheme of "N out of M" is recommended where N is less than M. For National Electoral Committee N members out of M members should be present in order to decrypt the votes.

4.2.3.2 Identification, Authentication and Authorization

The proposed main form of voter identification and authentication for Tanzania is through the use of a

national digital identity card (e-card) with Public Key Infrastructure (PKI). As discussed in sub-section 2.1,currently Tanzania is issuing e-cards but a full PKI support is yet to be implemented. We therefore propose that full PKI and e-cards should be used for authentication and identification of eligible voters. The proposed processes of issuing an e-card with PKI are shown in Fig. 7. If fully implemented, the new e-card will support most authentication technologies, including storing password, one-time passwords, biometric image templates, PKI certificate and supports the generating of asymmetric key pairs. We propose asymmetric and hashing algorithms to be used as cryptographic solutions. Each card should therefore contain two pairs of asymmetric keys. The first pair should be used for authentication and the second one digital signature. Certificates binding the public keys to the cardholder's identity should be stored on the card and in an online database. As an additional security control each key should be associated with a secret code (PIN) to authorize every operation. Unlike Swiss and Estonian models, our model supports three-factor authentication based on (1) something one knows (PIN), (2) something one has (smartcard), (3) something one is (biometric fingerprint). Despite its complexity, three-factor authentication is believed to be the most effective authentication mechanism.

At the start of each election, National Election Commission should publish a set of voting client applications that can run on all the available operating system platforms. We propose applications for Windows, Linux, and Mac OS be available to enable a good number of voters participate in elections. The application should be downloaded from the secure website that has to be maintained by National Election Commission. The current website of the National Election Commission does not use a secure hypertext protocol (shttp) and therefore, unless this anomaly is rectified, cannot be used for remote electronic voting. The client software should be customized for each election and include an election-specific public key.

4.2.3.3 Ensuring Authenticity, Secrecy and Integrity of the Votes

To ensure votes authenticity, secrecy and integrity of the votes, we adopt the double envelope scheme adopted from the Estonian model [10]. Under this scheme, the vote is encrypted with the vote counting server public key, while the corresponding private key does not exist before the polls close (inner envelope). The voter digitally signs the encrypted vote using its private key (outer envelope). The votes are collected, sorted, voter's eligibility is verified and invalid votes are removed. Then the outer envelopes (digital signatures) are separated from inner envelopes (encrypted votes). Voter lists are compiled from outer envelopes. Inner envelopes (which are not associated with the identity of the voter any more) are forwarded to the vote counting server. The vote counting server decrypts the votes using is private key and produces results of electronic voting. Fig. 10 illustrates a double envelope scheme proposed for Tanzanian remote electronic voting system.

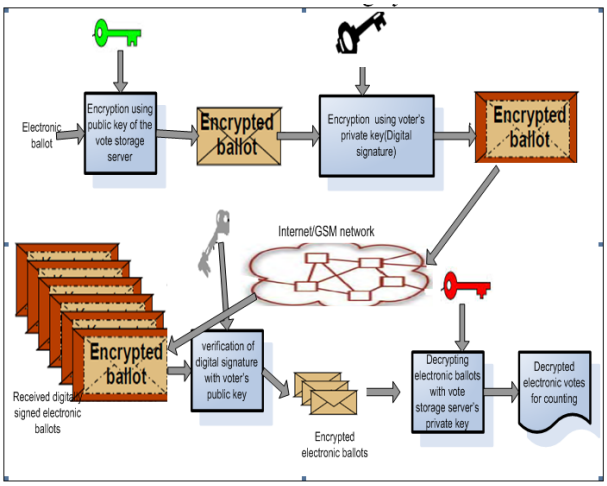

Fig. 9: A double envelope scheme

To ensure integrity of the votes, a client computes a "digital hash" of the encrypted ballot before the voter sends it off. The vote storage server computes the same "digital hash" and returns this hash value to the voter along with the confirming receipt. The voter then checks that the two codes match, thus the voter can confirm that the integrity of the votes has not been compromised. The digital hash is a fixed-length value computed based on the encrypted ballot that makes it impossible for either the contents or length of the encrypted ballot to be recovered by the attacker. The hash value provides a digital fingerprint of the encrypted ballot, which ensures that the ballot has not been altered by an intruder or virus, or by other means

4.2.3.4 Addressing Coercion and Vote Buying Issues

To prevent vote buying and coercion by technical means is practically impossible when voting remotely. To reduce negative consequences associated with this threat, a cancellation right is recommended. In this case voters will be allowed to submit multiple votes in advance with only last vote cast counted. Moreover, the buying of votes is precluded .i.e. a potential buyer can never ascertain that an electronic vote will actually be counted.

4.2.3.5 Addressing a Denial of Service Attacks to the Server

There is no a technical solution that can totally prevent a Denial of Service (DOS) attacks. However, there are administrative controls to reduce the impact of the attack when it occurs. To reduce the impact of DOS we recommend that advanced voting be allowed as discussed in sub-section 5.6.4. Moreover a robust disaster recovery plan should be implemented to minimize the impact associated with DOS attacks.

4.2.3.6 Ensuring Votes Verifiability

To ensure variability of the votes, we introduce two mechanisms: Auditing by independent bodies and a possibility for voters to verify using independent channel that votes are recorded as casted. Through independent auditing we can ensure that every step of the election is working accordingly. Generally, all the processes of the system have to be audited. The voter can also verify that his ballot was included in the counting process. This can be done using vote verification code. The verification codes are computed by receipt generator. The verification codes are sent directly to the voters, as shown in Fig. 8, and this has to be done through an independent channel. After receiving this feedback the voters can compare between their choice of options and receipt code. If the receipt code matches the selected options, the voter can conclude that the vote is recorded as intended.

5. Conclusion

This study identified security challenges from technical perspective that hinder the implementation of remote electronic voting in Tanzania. The study also identified security requirements that remote electronic voting must comply with. These requirements are in line with general principles of democratic elections. We reviewed and analyzed several remote electronic voting models with respect to security. Based on this analysis the most secure models (Swiss and Estonian) were customized and enhanced to produce a secure model that suite the requirements of Tanzanian. We also demonstrate how the developed model if well, implemented will address the identified challenges and hence conforms to the general principles of democratic elections. The model was mainly developed using desk review technique in consultation with information security, information technology and legal experts. From technical perspective we see that the ICT infrastructure was implemented without taking into consideration security issues. In regard to this we conclude that the current ICT infrastructure in Tanzania does not provide a sufficient level of security with respect to authentication, identification and transmission of cast votes. However, there is good reason to believe that the government will improve security of the existing ICT infrastructure to enable secure elections through Internet or Mobile phones. Another issue of concern is vote buying and coercion which is likely to be higher in Tanzania due to high level of poverty and corruption in the country. This will eventually affect principle of secret suffrage. To reduce negative consequences associated with this threat, a cancellation right is recommended. In this case voters will be allowed to submit multiple votes in advance with only last vote cast counted.

Generally, for remote electronic voting to be successful, it is very important that proper security controls are implemented. The current information security landscape in Tanzania does not warrant this level of security. For this reason, we do not at present recommend the implementation of a full-scale remote electronic voting system in the country. Our proposed model and recommendations should be seen as the start of a long term strategic objective. Nevertheless, we do not expect that there will be pressure and rush to introduce remote electronic voting in the country. We strongly recommend that remote electronic voting should not be implemented prior thorough testing and therefore we emphasize the need for the government to initiate a number of pilot and test projects. Properly planned pilot projects and systematic evaluation should be done as soon as possible, with the aim of testing various technical solutions and enhancing the voters' confidence in remote electronic voting.

References

[1] ACE Electoral Knowledge Network. "Focus on E-Voting". Retrieved on 26th July 2012 from the website www. aceproject.org/ace-en/focus/e-voting/countries?toc, 2012.

[2] Alvarez, M. R., Thad, E. H. and Trechsel, A. H. "Internet Voting in Comparative Perspective: The Case of Estonia". Political Science and Politics, 42: 497–505, 2009.

[3] Barrat, J., and Goldmith, B. "International Experience with E-Voting: Norwegian E-Vote Project". Retrieved on 13th September 2012 from the website www.regjeringen.no, 2013

[4] Cranor, L., and Cytron, R. "Sensus: a security-conscious electronic polling system for the Internet". In: Proceedings of the Thirtieth Hawaii International Conference on System Sciences,2007,Vol. 3, pp. 561-570.

[5] Chowdhury, M. J. "Comparison of e-voting schemes: Estonian and Norwegian solutions". International Journal of Applied Information Systems, Vol 6, No 2, 2013,pp 47-54.

[6] The European Union (EU). "Tanzania Final Report – General Elections of October 2010". Retrieved on 16th March 2014 from the website http//eeas.europa.eu,2010
[7] Fennazi, S. "Security questions hang over e-voting plans". Retrieved on 4th January 2014 from the website "http://origin.swissinfo.ch/eng/security-questions-hang-over-e-voting-plans/32567608, 2011.
[8] Gerlach, J., and Gasser, U. "Three Case Studies from Switzerland: E-Voting, 2009". Retrieved on 4th January 2013 from the website http://cyber.law.harvard.edu,2009.
[9] Giampiero, E.G. "E-Voting through the Internet and with Mobile Phones". Retrieved on 27th December 2013 from the website http://unpan1.un.org,2010.
[10] Heiberg, S. "Internet Voting – the Estonian Experience". Retrieved on 6th November 2013 from the website http://cyber.ee,2010.
[11] The International Telecommunication Union (ITU). "ICT facts and figures". Retrieved on 3rd January 2014 from the website www.itu.int,2013
[12] Kimbi, S. G. and Zlotnikova, I. "Citizens' Readiness for Remote Electronic Voting in Tanzania". Advances in Computer Science: an International Journal, Vol. 3, 2014,Issue 2, pp 150-159.
[13] Kowero, A. B,"Exploiting the Potentials of the National Information and Communication Technology Broadband Backbone (NICTBB) in Tanzania". Retrieved on 29th June 2013 from the website http://www.tanzania.go.tz/egov_uploads, 2012
[14] Kothari, C. R. "Research Methodology: Methods and Techniques", New Age Publication", New Delhi, 2004.
[15] Maaten, E. "Towards Remote E-voting: Estonian Case". Retrieved on 6th July 2013 from the website http://subs.emis.de/LNI/Proceedings/Proceedings47/Proceeding.GI.47-9.pdf2004, 2004
[16] Msyani, C. M. "The Current Status of Energy Sector in Tanzania". Retrieved on 14th September 2012 from the website http://www.usea.org/sites/default/files/event-/Tanzania%20Power%20Sector.pdf, 2012.
[17] The National Democratic Institute (NDI). "Report on the 2005 Zanzibar Elections". Retrieved on 23rd January 2014 from the website https://www.ndi.org, 2005.
[18] Schwartz, J. "Online Voting Canceled for Americans Overseas". Retrieved on 3rd April 2012 from the website http://www.nytimes.com, 2004.
[19] Seyondeka, E. "Obstacles in Bridging the Digital Divide in Tanzania". International Journal of Computing and ICT Research, Vol. 6, Issue 1,pp 60, 2012
[20] Tanzania Communication Regulatory Authority (TCRA)."Quarterly Telecommunications Statistics". Retrieved on 29th November 2013 from the website www.tcra.go.tz, 2010.
[21] Tanzania National Identity Authority (NIDA). "National identity Cards Registration – Progress Report". Retrieved on 5th October 2013 from the website www.nida.go.tz, 2010.
[22] Qiuel,.Y, and Zhu, H. "Somewhat Secure Mobile Electronic-Voting Systems Based on the Cut-and-Choose Mechanism". Retrieved on 10th September 2013 from the website http://www.computer.org/csdl/, 2009

Authors Biographies

Sylvester G. Kimbi is a doctoral student at the Nelson Mandela African Institution of Science and Technology. He holds an MBA in Corporate Management from Mzumbe University (2010), MSc Information Technology with Specialization in Information Systems Security from KTH/Stockholm University (2005). He also holds BSc in computer science (with honours) from the University of Dar es Salaam (2001). Mr Kimbi is currently employed at Dar es Salaam Institute of Technology (DIT) as Assistant Lecturer. Prior to joining DIT he was working for Central Bank of Tanzania as Information Security Administrator. He is a Certified Information System Auditor (CISA) and Certified Information Security Manager (CISM). He is a member of Information Systems Audit and Control Association (ISACA) and Tanzania Information Technology Association (TITA).

Prof. Irina Zlotnikova holds a PhD in Theory and Methodology of Computer Science Education (Doctor of Pedagogical Sciences, Moscow, Russia, 2005), a PhD in Solid-State Electronics, Nano- and Microelectronics (Candidate of Technical Sciences, Voronezh, Russia, 1995) and an Engineer Degree in Radiophysics and Electronics (Voronezh, Russia, 1988). She is a Professor of School of Computational and Communications Science and Engineering at the Nelson Mandela Institution of Science and Technology, Arusha, Tanzania.