I.J. Information Engineering and Electronic Business, 2016, 6, 9-21
Published Online November 2016 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijieeb.2016.06.02

Framework for an E-Voting System Applicable in Developing Economies

Lauretta O. Osho
Email: laurettachristi@gmail.com

Muhammad B. Abdullahi[1] and Oluwafemi Osho[2]
[1]Department of Computer Science
[2]Department of Cyber Security Science
Federal University of Technology, Minna, 920001, Nigeria
Email: {el.bashir02, femi.osho}@futminna.edu.ng

***Abstract*—**Information technology has pervaded virtually every facet of human life. Even in the delivery of governance, information technology has gradually found a place. One of its applications is the use of electronic voting, also known as e-voting, as opposed to the traditional manual method of voting. This form of voting, however, is not immune to challenges generally associated with voting. Two of these include guaranteeing voting access to all eligible voters, and providing necessary voting security. The challenge of accessibility is especially peculiar to developing countries where IT adoption is still relatively low. This paper proposes a framework for an e-voting system that would most benefit developing economies. It ensures availability of the system to only eligible voters and integrity of the voting process through its capacity to identify and prevent ineligible voters and multiple voting. To guarantee accessibility to all eligible voters, it supports both online and offline voting capabilities. Adopting electronic form of voting would provide a more robust, easier to use, and reliable system of voting, which, consequently, would contribute towards enhancing the delivery of democratic dividends.

***Index Terms*—**e-voting, cloud computing, democracy, election, security, availability.

I. Introduction

E-voting is seen as the ability of a nation to improve her electoral process. Non-electronic voting systems are often replete with many flaws including high cost and easy manipulation. Paper ballots, direct counting, and other manual electoral processes have proved unreliable due to rigging, misplacement of ballot papers, over-counting or undercounting of votes, mixing up votes and changing of ballot papers and results.

Most of these flaws could be avoided through the adoption of e-voting system. Electronic form of voting provides many advantages. These include ensuring access to the voting process for people living with disabilities, reducing the cost and time of elections, increasing turnout at elections, and providing services that can be trusted [1], [2]. The adoption of e-voting has the potential to boost voters' confidence [3].

Many countries, especially the underdeveloped and developing, have found it almost impossible to adopt the use of e-voting system in their electoral processes due to a barrage of problems. None or only few have been able to engage substantially electronic means of voting. This contrasts with countries in advanced economies, including Austria, Australia, Brazil, Canada, Switzerland, Estonia, France, Great Britain, Japan, Russia, Sweden, and USA, that have gone beyond holding pilots and trials, to legally binding e-voting or remote e-voting implementation [4].

Generally, there is a wide gap between developed and developing countries in terms of information and communication technology (ICT) usage. For instance, according to the International Telecommunication Union (ITU), in 2014, internet usage per 100 inhabitants in developing countries was 32.4, compared to 78.3 applicable for developed countries. Fig. 1 presents the statistics from 2005 to 2014 for developed and developing countries and the world average for each year [5]. This statistics is particularly alarming for some countries. Countries like Eritrea, Timor-Leste, Myanmar, Burundi, Somalia, Guinea, Niger, Sierra-Leone, and Ethiopia all have less than 2 persons per 100 inhabitants using the internet. The statistics for the thirteen least countries in terms of internet penetration is displayed in Fig. 2 [6].

An e-voting system must be accessible to every eligible voter, and provide a high level of security. However, this system has been found to be vulnerable to various security challenges and threats, including stored central data leakage/disclosure, selling of votes, and the presence of certain malware on voter's machine, to mention but a few [7]. Although, there are strong encryption schemes applicable to address issues concerning confidentiality, integrity, and authenticity, there is need for further technological implementations to address issues of availability, which consequently enhances overall security [2]. Essentially, electronic voting requires a level of security higher than the other components, including e-commerce [4]. It is a complex

system where every stage of its implementation must be secured.

From the foregoing, the implication of this common challenge of low internet penetration among developing countries is that, adopting an e-voting system that is strictly internet-based would not provide equality of access to all eligible voters. This implies a need for a system that can function both online and offline, to provide voting opportunity for eligible voters in areas without internet infrastructure, whilst ensuring a level of security required for an e-voting system.

This paper presents a framework for an e-voting system that supports both online and offline voting capabilities, ensures accessibility and security, and is suitable within the setting of a developing economy to guarantee a free and fair election. The components of security focused on in the study entails the capacity of the system to identify and prevent ineligible voters and multiple voting, thereby ensuring availability of the system to only eligible voters and integrity of the voting process.

The rest of the paper is organized as follows: section two reviews existing e-voting frameworks and systems. The generic, security, and functional requirements, to be satisfied by the proposed system, are defined in section three. In section four, the proposed framework is presented. The system components and process design are thereafter elaborated. Other components of the framework, including result synchronization and addressing of security requirements are then discussed.

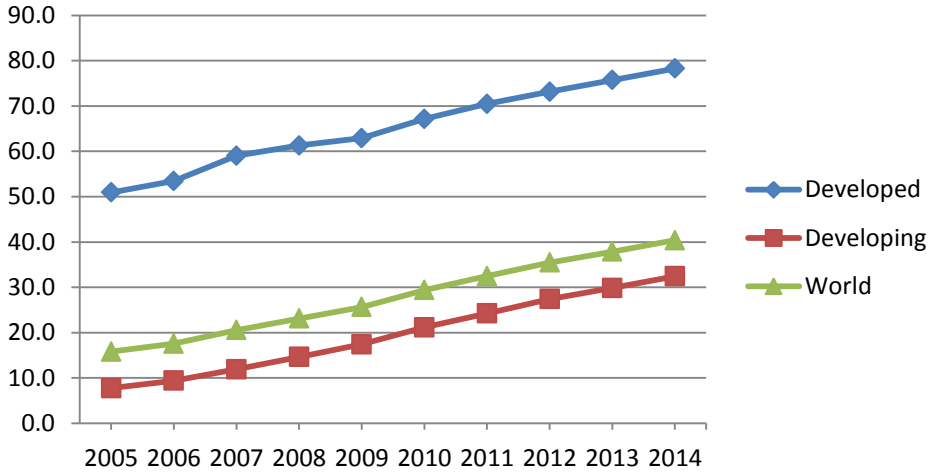

Fig.1. Number of internet users per 100 inhabitants for years 2005 to 2014 in developed and developing countries, and the world

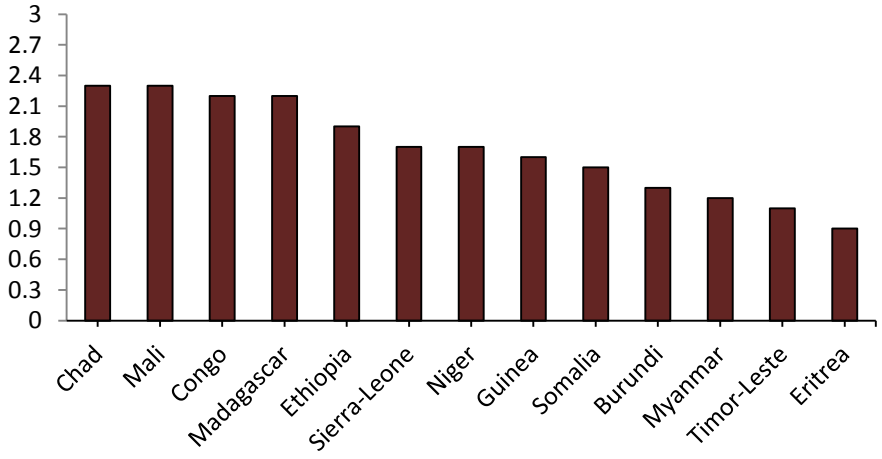

Fig.2. Countries with least internet penetration rate

II. Review of Existing E-Voting Frameworks/Systems

In this section some existing e-voting systems are reviewed. The bases for evaluating the performance of the systems are the level of ubiquity – capacity to provide equality of access – and security supported.

In the development of any system, e-voting systems inclusive, certain requirements must be considered as primary objectives, since having a perfect system is almost infeasible. One common requirement is security. Most voting data and process security are based on

encryption schemes via public key infrastructure, and certificate, e.g. in [4], [8], [9], [10]. This can be used in conjunction with biometric and/or smart card for secure authentication, as in [11], [12], [13] and [14]. On the other hand, [15] mainly focused on security at the authentication level via implementation of both biometric and smart card technology. Security must be given high priority to ensure voters' trust and the success of the election. Voting data; voting process; voting channels, including access control channel, communication channel; and all voting tools and technologies must be secured. The implication is that, security only at one level or aspect of the voting process leaves other levels vulnerable. Attackers could easily leverage on this to compromise the integrity of the entire process.

Another important factor, crucial for a successful voting process, is developing a system architecture that actually supports security. This is known as security by architecture. For instance, using centralized server architecture, as in the case of [10], [14], and [15], creates a single point of attack. A successful attack against the server compromises the entire voting process. For [16], adopting solely the use of mobile platform to deplore elections in a country like Nigeria is not reliable. This is due to the fact that the success of the elections would largely have to depend on the country's mobile providers. The system proposed by [17] also depends largely on the use of mobile technology, for receiving one-time password, used for authentication. Attacks against communication infrastructures would render the election unsuccessful. For [11], one major drawback is allowing prospective voters to install the voting application on their local computer systems. A compromised system can be used to launch attacks against the remote voting server.

One of the determinants used to assess the level of success in any election process is the percentage of eligible voters actually enfranchised. One method of achieving this lies in the use of multiple voting channels, e.g. in [11], [18].

Typically, e-voting systems, on a large scale, are deployed for online voting. However, considering the challenge of disenfranchising voters in areas without internet, which is common in most developing and under-developed nations, some authors developed their systems either only for offline use, for instance, in [19], or for both online and offline, e.g. [13].

Most developing countries use the manual voting system during elections. This possibly could have motivated some authors to develop e-voting systems applicable only to their respective countries. Examples include e-voting systems developed by [19], applicable for elections in Lebanon; [20] for use in Ghana; [16], which incorporated an integrated multilingual voting service platform for online elections in Nigeria; and [14], which integrated the India's Integrated Unique Identification (UID) mechanism as one of the requirements for authentication of prospective voters.

Recently, some authors have highlighted the possibilities of deploying e-voting systems on the cloud, for example in [4], [14]. While the e-voting system proposed in both studies combined distributed server and cloud architectures, they differed in the components to be deployed in the cloud. For [4], the cloud desktop, service distributor, validating server, and publishing server were all located in the cloud. On the other hand, [14] proposed hosting the technologies for handling user request and authentication and service management, and vote counting server on the cloud.

Table 1 summarises the features of some existing e-voting systems, with the methodologies used, their strengths and weaknesses.

A review of existing proposed e-voting systems reveals some characteristics that make them not suitable for implementation especially in developing countries. Basically, the existing e-voting solutions possess either or both of two problems: limitation in inherent capacity to provide voting security, and inability to guarantee equality of access to all eligible voters.

A potential taxonomy in respect of e-voting security could consider security from two perspectives, namely security by architecture and security supportable by the cryptographic scheme used. Security by architecture focuses on the choice, arrangement, and integration of the e-voting infrastructures, including voting platforms, servers and communication channels. This inherently contributes to the security of voting process. Many of the existing e-voting systems adopt the use of server-client architecture. The location(s) of the servers used in the system can easily become target of attack. On the other hand, the cryptographic scheme used determines security of voting data and channels.

Lack of universality, that is, non-guarantee of voting access for every eligible voter, regardless of locations, implies some eligible voters are bound to be disenfranchised. For instance, in Nigeria, many rural areas do not have internet facilities. High speed broadband internet penetration in Nigeria is between 4% and 6% [21]. And the digital divide between urban and rural areas is very wide. In 2006, out of a population of more than 140 million, more than 72 million were eligible voters [22]. If this is extrapolated to the end of 2012, where population was estimated to be 166.21 million, assuming the same growth rate, approximately 86 million of the country's population was eligible voters. By the end of 2012, there were 32.88 internet subscribers per 100 inhabitants in Nigeria [23]. This implies that an e-voting system that is strictly internet-based could potentially disenfranchise around 57.7 million eligible voters.

III. Definition of Requirements of Proposed System

Building an e-voting system entails an in-depth understanding of a host of requirements, ranging from legal to regulatory, functional to security. It is essential to ensure voters authentication, voting process security, and security of voting data [13] are given top priority during development life cycle.

Table 1. Summary of characteristics of existing e-voting systems

S/No.	Author(s) and system Year	Methodology/Features	Strength of Method	Limitation of Method
1.	Ray, Ray and Narasimhamurthi (2001) [8]	System employs three agents: a ballot distributor, certifying authority, and vote compiler; and public-key cryptography.	Supports adequately requirements including accuracy, democracy, privacy and verifiability	▪ Suitable only for online (internet) voting, ▪ Cannot prevent vote buying, ▪ Poor fraud detection, and ▪ Cast ballot can be traced back to IP address.
2.	Diehl and Weddeling (2006) [9]	Use of blind signature, and public key infrastructure	Ensures public-ness and transparency of voting.	▪ Suitable only for online voting.
3.	Malkawi, Khasawneh, and Al-Jarrah (2009) [15]	Client and server side architecture, incorporate biometric and smart card authentication.	Increased level of authentication security. Capable of handling elections with multiple scopes simultaneously.	▪ Voting process would not be secure since local voting station and central DB server were placed on the same local network.
4.	Zissis (2011) [4]	Combination of cloud and distributed server architectures, and public-key cryptography.	Enhanced security of voting process and data	▪ Suitable only for online voting.
5.	Okediran, Omidiora, Olabiyisi, Ganiyu, and Alo (2011) [11]	Uses a 3-tier architecture: client, server, and database tiers, biometric for authentication, and RSA algorithm and SSL/TLS for securing communication.	The system accommodates voting via mobile terminals, remote personal computers, and on-site polling stations.	▪ Installing voting application of client's computer could be exploited by malicious voters. ▪ The architecture would not support the principle of secrecy of elections.
6.	Ofori-Dumfuo and Paatey (2011) [20]	Uses a 3-tier architecture: client, server, and database tiers, with authentication achieved via ID and password.	Ease of implementation of system for a small scale election.	▪ Suitable only for online voting. ▪ Encryption scheme used not discussed.
7.	Olaniyi, Adewumi, Oluwatosin, Bashorun, and Arulogun (2011) [16]	Uses a 3-tier architecture which consists of the front end, middle tier and back end.	Provides a platform that would benefit majorly rural and sub-urban communities using voter's mother tongue	▪ Suitable only for online voting. ▪ Google Android OS cannot provide adequate security required for e-voting. ▪ Application of mobile platform only would imply that the success of the election would have to primarily rely on mobile service providers.
8.	Visvalingam and Chandrasekaran (2011) [12]	Uses biometric token and iris pattern for authentication, and employed the internet as the sole medium of communication, in which case entire voting and verification processes are achieved on a single transaction.	Reduced voting process time.	▪ Suitable only for online voting. ▪ Complete reliance on internet makes the system susceptible to many attacks.
9.	Alaguvel and Gnanavel (2013) [13]	Uses facial recognition, RFID smart card and finger veins sensing for offline e-voting system, and GSM one-time password for online voting.	Multi-level authentication ensures security against unauthorized voters.	▪ The combination of facial recognition, fingerprint, and smart card technology, for authentication will significantly increase voting time.
10.	Olaniyi, Arulogun, Omidiora, and Oludotun (2013) [10]	Uses multifactor authentication and cryptographic hash function.	Ensures the integrity of voting process and data.	▪ Using a centralized server creates a single point of attack against voting data.
11.	Gupta, Dhyani, and Rishi (2013) [14]	Implemented using cloud architecture, with country's Integrated Unique Identification (UID) mechanism and biometric for authentication.	Reduced operational cost. Increased security of voting process.	▪ Suitable only for online voting. ▪ Using a centralized server creates a single point of attack against voting data.
12.	Njogu (2014) [18]	Uses client-server architecture	Provides platform for multiple voting channels.	▪ Suitable only for online voting. ▪ One server is responsible for storing, processing and securing data.
13.	Biswas (2015) [17]	Uses one-time password sent to voter's mobile phone	Ensures voter's anonymity and provides secure authentication.	▪ Dependent largely on mobile technology.

A. Generic Requirements

These are baseline requirements that an e-voting system must satisfy. Some of the generic requirements include [4], [24]:

- Scalability: ability of the system to be expanded to meet growing demands, whilst still maintaining its performance level.
- Flexibility: ability of a system to be compatible with different standard technologies and platforms. This is also used to describe a system that is accessible to the disabled.
- Mobility: the ability of a system to provide no restrictions in the location where prospective voters can cast their votes.
- Robustness: ability of the system to cope with execution errors, or continue to operate correctly despite incorrect inputs.
- Democracy: the system must ensure the principle of 'one man-one vote,' that is, no one can vote more than once. It must also ensure no voting by proxy.

B. Security Requirements

Zissis [4] highlighted some security requirements for the different phases of elections. Some of these requirements include:

- The system shall identify and authenticate the voter before accepting and storing the e-vote.
- The system shall protect the confidentiality of the transmitted e-votes.
- The system shall verify the integrity and authenticity of e-votes.
- The system shall protect the integrity and authenticity of e-votes.
- The system shall communicate only with the authentic and unaltered client-side voting system.
- The system should be tamper-resistant and tamper-evident.

C. Functional Requirements

They constitute system-specific requirements peculiar to the e-voting system. It constitutes functionality, required input, expected output, and what is to be stored. Some of these requirements are as follows:

- Every eligible voter must be able to access the system.
- An ineligible voter must not be able to access the system.
- An eligible voter must not be able to vote more than once.
- The system must provide alternative accessibility platforms for voters.
- An eligible voter should be able to select alternative voting platforms within a specified deadline.
- More than one voter should be able to vote simultaneously.

IV. Proposed Framework For A Secure E-Voting System

The main focus of this study is to develop an e-voting system that supports universality of access to all eligible voters, provides security by architecture, and ensures integrity of voting process. We propose a hybrid electronic voting system that combines the capabilities of the Direct-Recording Electronic (DRE) and online electronic voting system, offering a platform for online and offline voting. Specifically, it supports voting via direct-recording, online poll-site, and remote e-voting systems.

To support online voting, it is implemented as a cloud application. This implies a Platform as a Service (PaaS) arrangement, where operating system, servers, network, memory and other hardware resources are provided by the cloud provider.

As a cloud application, voting is done online either remotely through a PC connected to the internet, or at an e-voting polling kiosk. For eligible voters who reside or intend to cast their vote in locations where internet is inaccessible, the DRE, administered at a polling kiosk, is implemented with a computer with keyboard or touch screen to cast their votes, with vote tally stored on the computer memory storage, after which the results are synchronized with the cloud. The system also provides an audit system for logging every process. The architecture of the system is depicted in Fig. 3.

The e-voting system provides flexibility in the choice of voting mechanism. For instance, a voter who registers to vote via a voting platform has the opportunity to select any other alternative platform within a stipulated deadline, subject to satisfying stipulated requirements.

The use of multiple servers, with separation of duties, ensures that an attack against any of the servers will not necessarily lead to the end of the election.

V. System Components

The architecture of the proposed e-voting system possesses an underlying structure that supports security. This is accomplished by the segregation of the different components of the voting process, with each process handled by a sub-system or server. This inherently protects the entire process as a single point of failure or susceptibility to attack is avoided.

There are various components that make up the e-voting system, each with one or more functions. These include the following:

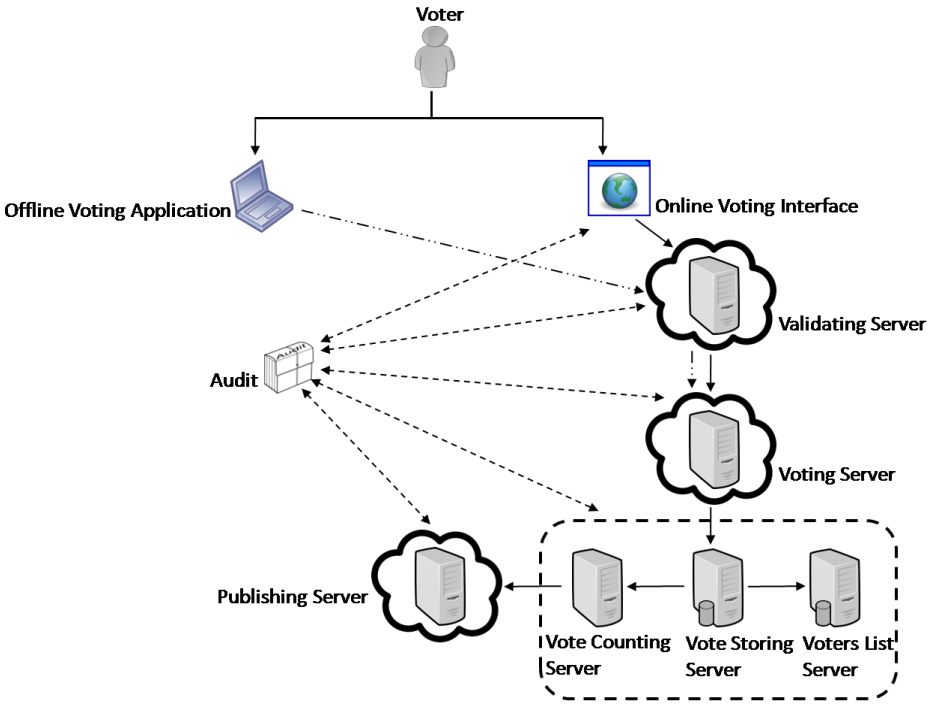

Fig.3. Architecture of proposed e-voting system

- **Offline Voting Application**: this is a stand-alone component of the entire e-voting system, the Direct-Recording Electronic (DRE) machine, made up of a computer with keyboard or touch screen for casting votes, and other essential peripheral devices, with vote tally stored on the computer memory storage.
- **Online Voting Interface**: this is a cloud-based desktop interface used at the online poll-site and by remote voters to access the e-voting system located in the cloud.
- **Validating Server**: it contains the registration details of all eligible voters. Hence, a voter must be validated on this server before access to the voting server is granted.
- **Voting Server**: this provides the functionality for casting of votes.
- **Vote Storing Server**: each vote cast is stored by the Voting Server on this server.
- **Voters' List Server**: the Voting server separates the details of voters from the votes cast. The votes are stored in the Vote Storing Server, while the details of the voters are stored on this Voters' List Server.
- **Vote Counting Server**: used for counting the votes. Votes for each candidate vying in the election are separated in this server.
- **Publishing Server**: publishes the results of the election(s).
- **Audit**: this is an audit service that provides for auditing of the entire process.

VI. Process Design

Generally speaking, voting can be divided into three phases: registration (pre-election), voting (election), and tallying (post-election) phases [4]. Part of the activities under the first phase is registration of voters. This section discusses these phases.

A. Registration Phase

This is the period for registration of prospective voters. During this phase, the e-voting system (both online and offline) is configured only for registration. This means all functionalities that support the election and post-election phases are disabled. Likewise during election phase, and through the stipulated election period, functionalities that support other phases are disabled. Once the stipulated election period elapses, all functionalities other than those for the post-election phase are disabled.

Registration Requirements

Registration can be done either online, only at an e-voting polling kiosk, or offline, depending on the location of the individual being registered. The following are required to be provided during registration:

- Bio-data. This includes full name, date of birth, sex, nationality, state of origin, local government area, and other personal details.
- Contact Address.
- Biometric (fingerprints) details.
- Facial image.

- Preferred voting medium. This determines the voting category of the voter being registered.
- Mobile number. This is applicable for those registering online.

Fig. 4 is a use-case diagram of the registration requirements.

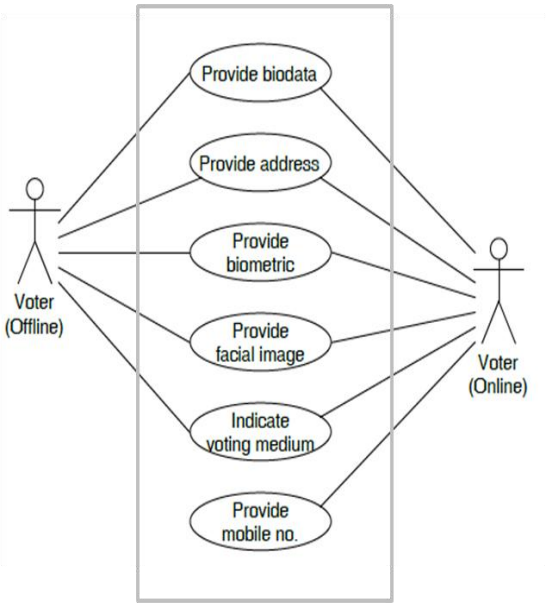

Fig.4. Registration use case

Registration Procedures

Once a prospective voter satisfies the registration requirements, two unique Identification numbers are generated by the system. One is a permanent voter ID number, which combines the state, local government and registration center IDs, and a unique serial number. For instance, using Nigeria as an example, a prospective voter registers in Gwagwalada local government area of the Federal Capital Territory (FCT), in a polling kiosk with ID number 001, assuming FCT is assigned code FT, and Gwagwalada the code GWA, the permanent voter ID number of a prospective voter could be FT/GWA/001/0001.

The second is a voting ID that is generated based on the medium the voter indicated to use for voting. For instance, if a prospective voter, during registration, selects to vote online using e-voting polling kiosk, assuming this is assigned the code ONK, the voting ID number could be ONK/0001. The codes ONP and OFF for online voting via PC and offline voting respectively are assumed. This mechanism would help prevent multiple-voting.

A prospective voter can update his registration details and/or preferred voting platform not later than a stipulated time before election date. Once an intended voting medium is changed, a new voting ID, which overrides the previous one, is generated for the individual.

Once registration is completed (or updated), a voter e-card is generated, downloadable in pdf format. This contains all registered details of prospective voter.

B. Voting Phase

This is the main election phase of the entire exercise. It begins with authentication of voters. Only those who are authenticated are allowed to cast ballots. Due to the availability of multiple voting platforms, voters have different categories. Each voter category has different authentication requirements before a prospective voter, in that category, could be allowed to cast a vote.

Voter Categories

The e-voting system presents three modes and corresponding platforms for voting, viz. offline, via a polling kiosk; online, via a polling kiosk; and online, via a PC remotely connected to the system. Consequently, these form the three different categories of voters.

Voting Requirements

The requirements for authentication of a voter before being allowed to vote depend on the category of the voter. Based on the foregoing, authentication under the three mechanisms of voting are considered:

- Offline, via a polling kiosk,
- Online, via a polling kiosk, and
- Online, via a PC.

The authentication requirements for each voter category, which stem directly from the registration category, are summarized in Fig. 5.

It must be stated that while it is expected that a voter's registration category strictly determines the voter category, the proposed system allows for flexibility in the choice of voter category. For instance, a prospective voter who registered offline may choose immediately, or at a later time change, as long as the permitted time frame is yet to elapse, to vote under any of the other two categories.

Authentication Process

For offline and online voting via polling kiosk, the system uses a 3-level authentication. A prospective voter supplies the voter and voting IDs. The fingerprint is then scanned. The system verifies if these details correspond to those in the database or cloud (in the case of online voting). If the details do not correspond the prospective voter is allowed to repeat the steps again. After three attempts, if failure is still recorded the voter is rejected, and the processes are logged. However, if the captured details are correct, other details of the voter, including bio-data, address, and facial image are displayed. The voting administrator physically verifies if the displayed image is the same as the prospective voter. If yes, the voting administrator confirms the identity of the voter (clicking on a button). The voting interface is then presented for the voter to cast his/her ballot. Else, if the displayed image does not correspond to the face of the voter, the voting administrator disapproves of the voter. This means, the voting interface is not presented. All system processes are logged.

On the other hand, for remote online voting, the system also uses a 3-level authentication. The same process of filling in voter and voting IDs, and supplying fingerprint image are followed. In the event that the captured details are correct, a random 6-digit token is then generated, and sent to the prospective voter's mobile phone (which acts as a token device). The voter enters the value. If incorrect, the prospective voter is rejected, else, if the entered value is correct, other details of the voter, including bio-data, address, and facial image are displayed. The voter can then proceed to cast his/her vote. All system processes are likewise logged.

The authentication processes for all categories are presented in a flowchart depicted in Fig. 6.

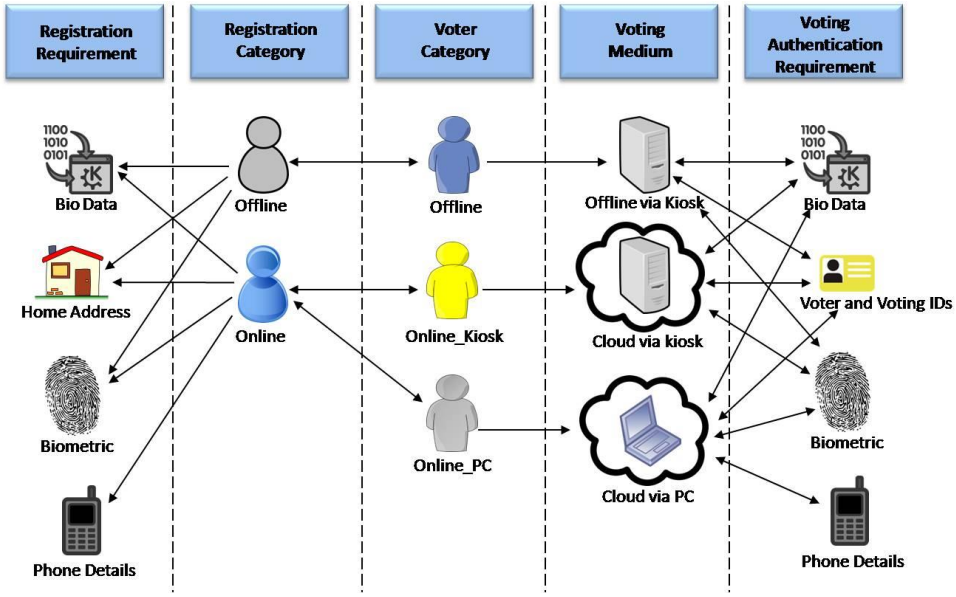

Fig.5. Registration and voting requirements, categories of registration and voters, and respective voting media

Voting Process

The process of voting varies depending on whether voting is done online or offline. For online voting, either via polling kiosk or PC, the following steps are involved:

- A voter
  a. Is authenticated by the Validating Server.
  b. Is connected to the Voting server to be able to vote.
  c. Makes a choice of candidate. In the case of multiple elections, such voter indicates the elections he/she wants to be part of, and goes on to select candidates accordingly.
  d. Encrypts the ballot and personal data using the public key of the Vote Storing server, and sends it to the Voting server.
- The Voting server
  a. Signs the ballot.
  b. Forwards the signed ballot to the Vote Storing server.
- The Vote Storing server
  a. Separates the digital signature and the ballot.
  b. Decrypts the ballot, and separates the voter's details from the vote.
  c. Encrypts the voter's details with the public key of the Voters' List server, and
  d. Forwards these details to the same server.
  e. Encrypts the vote with the public key of the Vote Counting server, and
  f. Forwards the vote to the same server.

For offline voting, voting is consisted in the following:

- A voter
  a. Is authenticated.
  b. Makes a choice of candidate. In the case of multiple elections, such voter indicates the elections he/she wants to be part of, and goes on to selects candidates accordingly.
- The system
  a. Encrypts the ballot and voter's personal data using the public key of the cloud Vote Storing server, and
  b. Stores them on the system's database.

In both methods of voting, each activity throughout the entire process is usually logged. Fig. 7 is a sequence diagram for online voting.

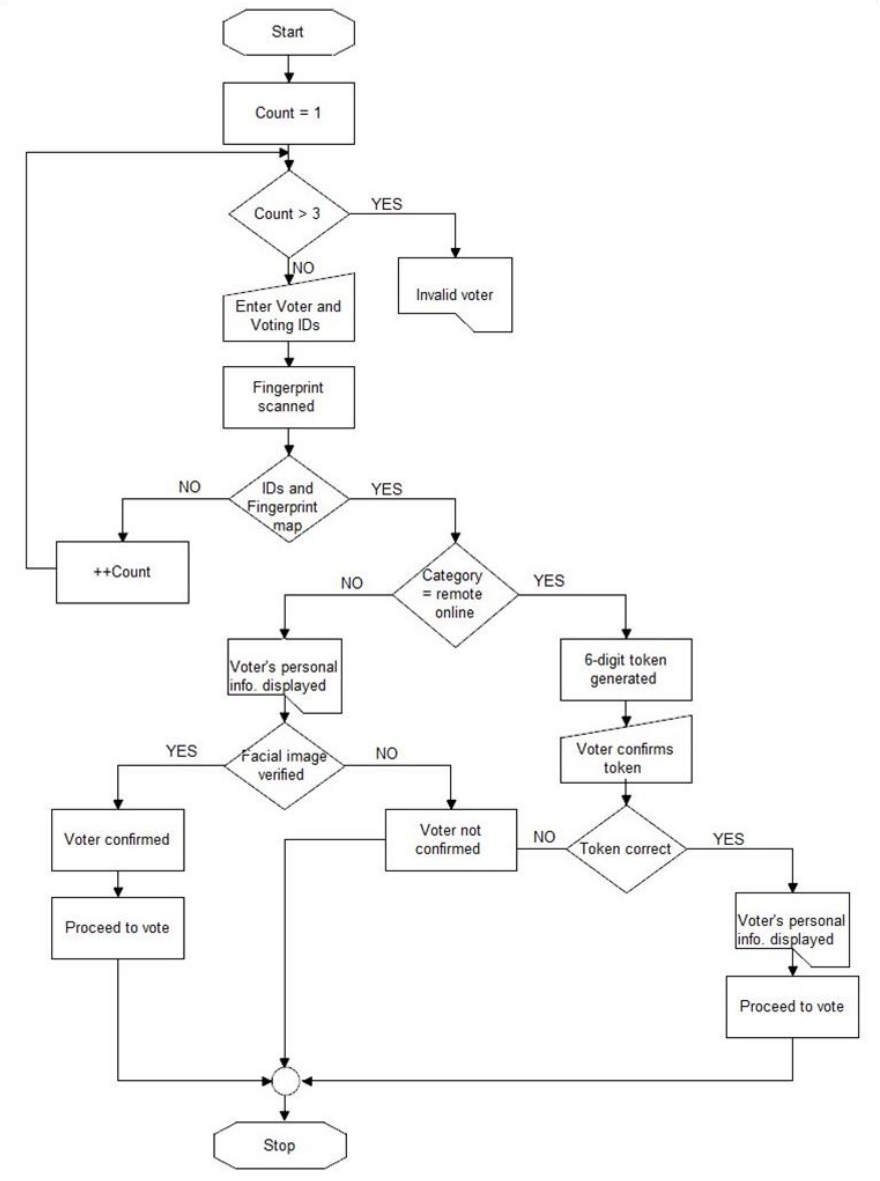

Fig.6. Voting authentication process

C. Tallying Phase

Tallying, also known as counting, involves collation of the number of votes for each candidate, and publishing the results of the election. For electronic form of voting, tallying is usually done automatically, even while voting is still ongoing.

For offline voting, the results generation is synonymous to report generation. The amount of votes for each candidate is pulled from the database by the system and published. For online voting, the Vote Storing server separates the votes from the voters' details. The votes are sent to the Vote Counting server. The summary of results for the candidates is sent to the Publishing server.

However, before the final results are published, results from offline systems are synchronized with results on the cloud, for final collation.

VII. Synchronizing with the Cloud

Synchronization is essentially between offline systems used for voting and the cloud. After completion of voting, an offline e-voting system is brought to the collation center, which essentially has internet access. In order to synchronize cast ballots with the cloud, the system is authenticated by the Validating server. Using a combination of the global unique identifier of the computer system and voting application certificate, a secure SSL connection is created between the system and Validating server, thus encrypting exchanged data and guaranteeing their security through the cloud infrastructure. Upon validation, each ballot, together with the voter's personal data, in the database stack is popped up, signed by the Voting Server and then forwarded to the Vote Storing Server. Subsequent procedures are similar to those for online voting.

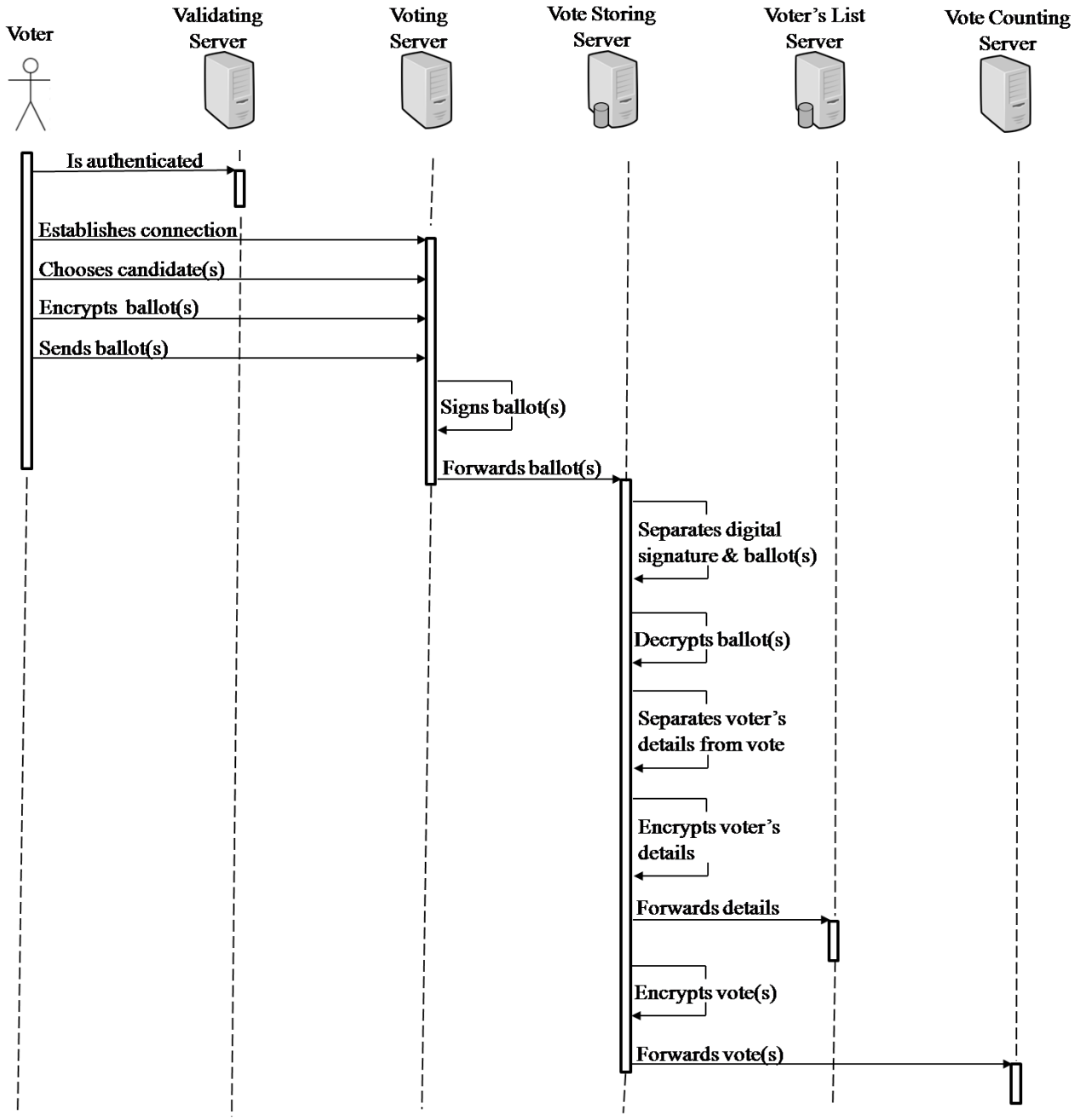

Fig.7. Online voting process sequence diagram

VIII. Addressing Security Requirements

This study majorly tackles security from the architecture point of view. This aids security of voting process. However, successful election is closely tied to satisfying as many security requirements as possible. The implication of this is that the security of voting data and communication channels cannot be neglected.

In the course of elections deployed through electronic means, data, in digital form, is transmitted from one system to the other. For instance, the Voting server transmits a signed copy of the ballot to the Vote Storing server. An attacker could gain unauthorized access to this data on transmit. It is therefore necessary to make it as difficult as possible for the attacker to make sense of the accessed data.

A. Public Key Cryptographic Scheme

For an e-voting system, cryptographic implementation contributes to the security of the voting data and channels. However, the cryptographic scheme to be adopted must ensure a balance between security, usability, and accessibility of the system.

For the proposed e-voting system, the RSA encryption scheme is proposed. RSA was invented by R. Rivest, A. Shamir, and L. Adleman, and has over the years become one of the most widely used encryption schemes. Its

security is based on the intractability of the integer factorization problem [25]. It is used to provide secrecy and digital signature, has been shown to be significantly faster in encrypting and decrypting than some other encryption schemes, including ElGamal [26], and can be implemented with Extensible Authentication Protocols (EAP) to secure cloud data [27].

For instance, for online voting, one of the procedures involves the Vote Storing server encrypting the voter's details with the public key of the Voters' List server, and forwarding the details to the same server. Using RSA for encryption, the encryption and decryption processes are as follows:

Encryption**:**

- Vote Storing server obtains Voters' List server's authentic public key (*n, e*), where *e* is the encryption exponent and *n* is the modulus.
- Vote Storing server represents the voter's details as an integer *m* in the interval [0, *n* – 1].
- It then computes $c = m^e \bmod n$.
- And send the ciphertext *c* to the Voters' List server.

Decryption:

- The Voters' List server uses its private key *d* to recover $m = c^d \bmod n$.

B. Randomized Authentication Token

This is used to provide an added layer of security during authentication of online voters accessing the voting system remotely. It is essentially a non cryptographic solution [4] that involves tokens generated randomly and sent to voter's mobile devices.

C. Digital Signature

Blind signature is the electronic equivalent of the traditional signing technique [4]. It is a number that relies on the some secret known only to the signer, and the content of the signed message [25]. For the system the voter encrypts the ballot and personal data using the public key of the Vote Storing server, and sends it to the Voting server. The Voting server then signs the ballot and forwards it to the Vote Storing server. Thereafter, the Vote Storing server separates the digital signature and the ballot.

The Voting server uses the RSA algorithm for signing the votes. The signing process is presented as follows: the Voting server has a public key (*n, e*) and private key *d*. *b* is the ballot to be signed, and *k* is a random number between 1 and *n*.

- The Voting server computes $\tilde{b} = k(b)$, an integer in the interval [0, *n* – 1].
- It then computes $s = \tilde{b}^d \bmod n$.
- The signature of the Voting server is *s*.

The Vote Storing server verifies the Voting server's signature *s* and recovers the ballot *b* using the following steps:

- It obtains the Voting server's public key (*n, e*).
- It computes $\tilde{b} = s^e \bmod n$
- It then computes $b = k^{-1}(\tilde{b})$.

D. Separation of Duty

It is an architectural framework that involves separation of functions, where a server is dedicated for each function. This technique supports security of voting. For instance, to ensure privacy of votes, Vote Storing server separates voters' details from ballots, while voter's details are sent to Voters' List server, the ballots are sent to Vote Counting server.

IX. CONCLUSION

The benefits of electronic means of voting as against the use of manual voting method cannot be over-emphasized. This study has contributed to existing knowledge primarily by presenting a system with a architectural framework that guarantees accessibility to virtually all categories of voters to be enfranchised, and supports security of voting data and processes.

The architecture of the system presented inherently supports security of voting data, by separating and assigning duties to different servers. However, this assertion was not evaluated. Hence, this area is open for further studies. This study has focused on two elements of information security – integrity and availability. It is suggested that future research endeavours could consider confidentiality in the entire process. Another area worthy of further exploration is the consideration of different cryptographic schemes to determine which would best be suitable for the system, especially considering its cloud nature.

REFERENCES

[1] V. Gupta, "e-Voting: Move to intelligence suffrage," *SETLabs Briefings*, vol. 9(2), pp. 3–8, 2011.

[2] D. Zissis, and D. Lekkas, "Securing e-Government and e-Voting with an Open Cloud Computing Architecture," *Government Information Quarterly*, vol. 28, pp. 239–251, 2011.

[3] O. Osho, V. L. Yisa, and O. J. Jebutu, "E-Voting in Nigeria: A Survey of Voters' Perception on Security and Other Trust Factors," Proceedings of the International Conference on Cyberspace Governance, Abuja, FCT, pp. 202–211, November 2015. doi: 10.1109/CYBER-Abuja.2015.7360511.

[4] D. Zissis, "Methodologies and Technologies for Designing Secure Electronic Voting Information Systems," 2011. Unpublished PhD thesis, University of Aegean.

[5] ITU. "ITU Key 2005 – 2014 ICT Data," 2015. Retrieved May 17, 2015 from http://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2014/ITU_Key_2005-2014_ICT_data.xls

[6] Internet Society. "Global Internet Penetration." Retrieved May 17, 2015 from http://www.internetsociety.org/map/global-internet-report/?gclid=CPi5mqrwxsUCF UT n wgodrxUALg
[7] S. Chaeikar, M. Jafari, H. Taherdoost, and N. Chaeikar, "Definitions and Criteria of CIA Security Triangle in Electronic Voting System," *International Journal of Advanced Computer Science and Information Technology* vol. 1 (1), pp. 14–23, 2012.
[8] I. Ray, I. Ray, and N. Narasimhamurthi, "An Anonymous Electronic Voting Protocol for Voting over the Internet," Proceedings of the Third International Workshop on Advanced Issues of E-Commerce and Web-Based Information Systems, San Juan, CA, pp. 188–190, June 2001.
[9] K. Diehl, and S. Weddeling, "Online Voting Project-New Developments in the Voting System and Consequently Implemented Improvement in the Representation of Legal Principles," *Electronic Voting*, pp. 213–222, 2006.
[10] O. M. Olaniyi, O. T. Arulogun, and E. O. Omidiora, "Design of Secure Electronic Voting System Using Multifactor Authentication and Cryptographic Hash Functions," *International Journal of Computer and Information Technology*, vol. 2(6), pp. 1122–1130, 2013.
[11] O. O. Okediran, E. O. Omidiora, S. O. Olabiyisi, R. A. Ganiyu, and O. O. Alo, "A Framework for a Multifaceted Electronic Voting System," *International Journal of Applied Science and Technology*, vol. 1(4), pp. 135–142, 2011.
[12] K. Visvalingam, and R. M. Chandrasekaran, "Secured Electronic Voting Protocol Using Biometric Authentication," *Advances in Internet of Things*, vol. 1, pp. 38–50, 2011. doi:10.4236/ait.2011.12006.
[13] R. Alaguvel, and G. Gnanavel, "Offline and Online E-Voting System with Embedded Security for Real Time Application," *International Journal of Engineering Research*, vol. 2(2), pp. 76–82, 2013.
[14] A. Gupta, P. Dhyani, and O. P. Rishi, "Cloud based e-Voting: One Step Ahead for Good Governance in India," *International Journal of Computer Applications*, vol. 67(6), pp. 29–32, 2013.
[15] M. Malkawi, M. Khasawneh, O. Al-Jarrah, and L. Barakat "Modeling and Simulation of a Robust e-Voting System," *Communications of the IBIMA*, vol. 8, pp. 198–206, 2009.
[16] O. M. Olaniyi, D. O. Adewumi, E. A. Oluwatosin, M. A. Bashorun, and O. T. Arulogun, "Framework for Multilingual Mobile E-Voting Service Infrastructure for Democratic Governance," *African Journal of Computing and ICT*, vol. 4(2), pp. 23–32, 2011.
[17] S. Biswas, "GSM Verification Based Secure E-Voting Framework," *International Journal of u- and e-Service, Science, and Technology* vol. 8(1), pp. 231–238, 2015.
[18] J. I. Njogu, "E-Voting System: A Simulation Case Study of Kenya," 2014. Unpublished MSc. Thesis, University of Nairobi.
[19] M. Hajjar, B. Daya, A. Ismail, and H. Hajjar, "An E-Voting System for Lebanese Elections," *Journal of Theoretical and Applied Information Technology*, vol. 2(1), pp. 21–29, 2006.
[20] G. Ofori-Dwumfuo, and E. Paatey, "The Design of Electronic Voting System," *Research Journal of Information Technology*, vol. 3(2), pp. 91 – 98, 2011.
[21] Presidential Committee on Broadband. "Nigeria's National Broadband Plan 2013 – 2018." Retrieved February 27, 2014 from: http://www.phase3telecom.com/The%20Nigerian%20National%20Broadband%20Plan%202013_19May2013%20FINAL.pdf
[22] National Population Commission. "2006 Population and Housing Census. Priority Table, Vol. 4," 2010. Retrieved February 10, 2014 from http://www.population.gov.ng/images /Priority%20table%20Vol %204.pdf
[23] ITU. "Percentage of Individuals using the Internet," 2013. Retrieved February 10, 2014 from http://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2013/Individuals_Internet_2000-2012.xls
[24] G. Z. Qadah, and R. Taha, "Electronic Voting Systems: Requirements, Design, and Implementation," *Computer Standards and Interfaces*, vol. 29, pp. 378–386, 2007.
[25] A. J. Menezes, P. C. Van Oorschot, and S. A. Vanstone, "Handbook of Applied Cryptography," CRC Press, 1996.
[26] T. Z. Nwe, and S. W. Phyo, "Performance Analysis of RSA and ElGamal for Audio Security," *International Journal of Scientific Engineering and Technology Research*, vol. 3(11), pp. 2494–2498, 2014.
[27] S. Marium, Q. Nazir, A. Ahmed, S. Ahthasham, and M. A. Mehmood, "Implementation of EAP with RSA for Enhancing the Security of Cloud Computing," *International Journal of Basic and Applied Science*, vol. 1(3), pp. 177–183, 2012.

Authors' Profiles

Lauretta Oluwafemi Osho holds a B.Tech. degree in Mathematics/Computer Science and an M.Tech degree in Computer Science. Her research interests include cloud computing and software development.

Muhammad Bashir Abdullahi received B.Tech (Honors) in Mathematics/Computer Science from Federal University of Technology, Minna, Nigeria, and Ph.D. in Computer Science and Technology from Central South University, Changsha, Hunan, P. R. China. His current research interests include trust, security and privacy issues in data management for wireless sensor and ad hoc networks, cloud computing, big data technology and information and communication security.

Oluwafemi Osho is currently a lecturer in the Department of Cyber Security Science, Federal University of Technology, Minna, Nigeria. He holds a B.Tech. degree in Mathematics/Computer Science and an M.Tech. degree in Mathematics. Before joining the institution, he served as Head of the IT Department of one of the leading mortgage banks in Nigeria. His current research interests include cybersecurity, mobile security, and security analysis. He is a Certified Ethical Hacker (CEH).

How to cite this paper: Lauretta O. Osho, Muhammad B. Abdullahi, Oluwafemi Osho,"Framework for an E-Voting System Applicable in Developing Economies", International Journal of Information Engineering and Electronic Business(IJIEEB), Vol.8, No.6, pp.9-21, 2016. DOI: 10.5815/ijieeb.2016.06.02

