# A FRAMEWORK FOR A MULTIFACETED ELECTRONIC VOTING SYSTEM

****OKEDIRAN O. O. (Corresponding Author)***
**OMIDIORA E. O.**
**OLABIYISI S. O.**
**GANIYU R. A.**
**ALO O. O.**
Department of Computer Science & Engineering
Ladoke Akintola University of Technology
P.M. B. 4000, Ogbomoso, Nigeria
E-mail: dotunokediran@yahoo.com*

**ABSTRACT**

*The rapid advancement in information and communications technologies has given rise to new applications that were impossible just few years ago. One of these applications is e-voting. The term "e-voting" is defined as any voting method where the voter's intention is expressed or collected by electronic means. This paper details the requirements, design and implementation of a generic and secure electronic voting system where voters can cast their votes anytime, anywhere and using a number of electronic devices including private computer networks, web and mobile phones.*

**Keywords:** e-voting, three tier architecture, Short Message Service (SMS), Virtual Private Network (VPN), Proxy Server, Database Server and Internet.

## *1. INTRODUCTION*

"While democracy must be more than elections, it is also true it cannot be less" former United Nations Secretary General, Kofi Annan once said (Annan, 2000). Democracy is a form of government in which the supreme power is vested in the people and exercised directly by them or by their elected agents under a free electoral system. Election on the other hand is a process in which voters choose their representatives and express their preferences for the way that they will be governed (Kohno et al., 2003) and (Malkawi et al., 2009). Democracy and elections have more than 2500 years of tradition (Krimmer et al., 2007). However, technology has always influenced and shaped the ways elections are held (Held, 2006). In times past, different voting systems that are based on traditional paper ballots, mechanical devices, or electronic ballots were developed for elections (NSF, 2001) and (Malkawi et al., 2009). However, these voting systems have littered history with example of elections being manipulated in order to influence their outcome. Allegations of violence, intimidation, ballot stuffing, under-age and multiple voting, counting error, complicity of the security agencies and the absence or late arrival of election materials etc often trail elections conducted using these systems of voting (NSF, 2001), (Fischer, 2003), (Muir et al, 2005), (Boniface, 2008) and (Malkawi et al., 2009). In Africa, most elections are conducted using paper ballots. However, there have been countless reported cases of eligible voters being unable or prevented from exercising their right to vote as stated in the Universal Declaration of Human Rights of the United Nations (United Nations, 1948), sometimes due to violence and intimidation, lack of information on physical location of voting poll sites, social discrimination; and by other natural causes like advanced age, physiological disability, terrain, floods, and poor communication infrastructure (Boniface, 2008).

Therefore, there is the need of a significant alternative to this conventional system in the delivery of trusted elections. The advancement of information and telecommunications technologies has allow for a fully automated online computerised election process whereby electoral vote counts are done in real time that by the end of elections day, the results are automatically out (Rubin, 2002). This type of election process is referred to as electronic voting (e-voting). E-voting is any voting method whereby at least the voter's intention is expressed or collected by electronic means (Buchsbaum, 2004), (Magi, 2007) and (Nestas, 2010). The term e-voting is being used from tabulating the votes by electronic means to integrated electronic systems of voters' and candidates' registration to the publication of election results (Buchsbaum, 2004). In general, two main types of e-voting can be identified: e-voting supervised by the physical presence of representatives of governmental or independent electoral authorities, e.g. electronic voting machines at poll sites popularly known as Direct Recording Electronics (DRE); and e-voting within the voter's sole influence (remote e-voting), not physically supervised by representatives of governmental authorities, e.g. voting from one's own or another person's computer via the internet, by mobile phones (including Short Message Service, SMS), or via digital television (Buchsbaum, 2004).

The emergence of e-voting will undoubtedly enable voters to cast their vote from a place other than the poll site in their voting district, facilitate the casting of the vote by the voter, facilitate the participation in elections by those who are entitled to vote, widen access to the voting process for voters with disabilities or those having other difficulties in being physically present at a poll site, increased voter turnout by providing additional voting channels, reduce overtime, the overall cost to the electoral authorities of conducting an election, deliver voting results reliably and more quickly amongst many other benefits (Buchsbaum, 2004). This paper details the requirements, design and implementation of a generic e-voting system, where voters can cast their votes anytime, anywhere and using a number of electronic devices including web and mobile phones. Section 2 details a high-level set of requirements that an e-voting system must satisfy. The architecture of an e-voting system that satisfies the stated requirements is presented in section 3. Section 4 and 5 outline description and the implementation of a prototype for the e-voting system. Finally, section 6 presents some concluding remarks.

## *2. REQUIREMENTS DEFINITION FOR THE E-VOTING SYSTEM*

The design of any voting system, whether electronic or traditional paper ballots or mechanical voting system must satisfy a number of sometimes competing criteria (NSF, 2001) and (Nestas, 2010). These requirements are divided into two groups, namely, generic and system-specific. The system is to cater for the following generic requirements:

i. *Privacy*: After casting a vote, no one should be able to link the voter to this vote;
ii. *Authenticity:* Only eligible voters can cast their votes;
iii. *Integrity/accuracy*: Once a voter cast a vote, no alternation to this vote is permitted. Moreover, All valid votes must be counted, whereas all invalid votes must not be discarded;
iv. *Security:* Throughout the voting process, a vote can't be tampered with;
v. *Democracy:* All eligible voters must be able to vote, one person - one vote and no one can vote more than once or vote for others.
vi. *Verifiability*: Voters can independently verify that their votes have been counted correctly and are included in the final tally.

The system-specific requirements of the framework allow:

i. *Multi-user:* A number of voters can vote simultaneously;
ii. *Accessibility:* The system can be accessed by voters from any location using secure Internet and/or mobile devices;
iii. *Availability:* The system must have high-availability during an election campaign.

## *3. ARCHITECTURE OF THE E-VOTING SYSTEM*

To accommodate the requirements presented in section 2, an architecture presented in Figure 1 below, for the e-voting system was developed. The e-voting system was modeled around the three tier architecture: client tier, server tier and database tier.

### 3.1 Client tier

The client tier is made up of the following components:

i. Mobile terminal voters and the mobile network operator: SMS voting is done through mobile terminals. Communication between the mobile terminals and the SMS server is through GPRS which is provided by the GSM network provider.
ii. Remote clients' computers: Remote internet voting is done on the clients' computers (equipped with fingerprint reader) in locations outside the poll sites. The clients' computers connect to the web server to load the web application over the internet via HTTP. The e-vote is sent to the poll site server via TCP/IP (socket programming and .NET remoting). A RSA encryption algorithm was implemented to secure end to end messaging.
iii. Registration Centre and Poll Site Computers: The Registration Centre/Poll Site Computers in practice should be special-purpose computers for voters' registration and poll site voting. Communication between the Registration Centre/Poll Site Computers and the Poll site server is by TCP/IP (socket programming and .NET remoting). A RSA encryption algorithm was implemented to secure end to end messaging.

### 3.2 Application server tier

The application server tier is made up of:

i. The SMS sever which interacts with voters that use their mobile telephone set and the SMS messaging service to access the e-voting system. At the lowest level, the SMS server interfaces to GSM modem(s) that receive voters' SMS messages through a SMS service provider (mobile operator).
ii. The web server which interfaces the e-voting system to web voters. In addition, it stores the different web page(s) containing the code required to interact with the user as well as the database system.
iii. The poll site server which interfaces the e-voting system to the electorates during registration and poll site voting.

### 3.3 Database server tier

Database server is the core service for storing, processing and securing data. The database server provides controlled access and rapid transaction processing to meet the requirements of the client tier. The voters' records, candidates' record and election results database resides on this server. This server is also responsible for authenticating voters and administrators' authorisation.

## *4. EVOLVING THE OVERALL SYSTEM ARCHITECTURE*

The system architecture defines the key components of the proposed system together with the interactions between these components. The overall functional structure of the framework is summarised as follows: an eligible electorate (18 years and above) registers with the electoral body at a gazette registration centre. The person identifies self by providing all the required biodata, phone number and the fingerprints of the person will be scanned and stored in the database. The registered electorate will be given a unique voter identification number and a unique voting code which he/she is expected to keep confidential. A remote internet voter (client) runs the Uniform Resource Locator (URL) for the e-voting system through a web browser. The web application prompts the voter to download the voting application package that should be installed on the voter's computer. The voting application runs remotely on the client's computer. Voting is done via the voting application installed on the client's computer by selecting the political party of choice and a fingerprint scan. A remote mobile terminal voter votes via SMS. Poll site voters cast their electronic ballots at designated Poll sites. The voter selects the political party he/she wants to vote for on the voting interface and scans a fingerprint to cast the vote.

The developed e-voting system was designed to allow many voters to voting simultaneously while ensuring highly availability during the electioneering process. Authentication into the voting system is either by biometrics or voter identification number (voter ID) and voting code generated for each voter after registration. Poll site voting and internet voting requires a fingerprint scan for ballot casting while SMS voting requires combination of mobile number (SIM) of the electorate, the generated voter ID and voting code, which are unique for voter. A voter ID and voting code sent to a particular SIM after registration cannot be used on another SIM for voting. The security considerations of the system were based on a RSA encryption algorithm which was implemented to secure end to end messaging, the Transport Layer Security (SSL/TLS) which is a VPNs' cryptographic tunneling protocol and firewalls in form of proxy servers. Furthermore, the web server only hosts the web page of the e-voting system. Actual ballots casted by web voters are sent to the Poll site server which is on a VPN. Ballot casted are record in the data tables at the backend of the database as binary templates.

The system ensures only one-person, one-vote (democracy) property of voting systems. The voter's fingerprint, voter's SIM, voting ID and voting codes of a voter intending to cast his/her ballot are matched at every voting attempt to prevent multiple voting. During registration, fingerprints of new electorate about to be registered are matched against exiting fingerprints in the database to prevent multiple registrations.The overall system was developed base on the derived system requirements and on the .NET framework using Visual C#, GrFinger SDK (version 4.2) and Ozeki message server (version 6).Web applications were developed using ASP. NET while the data tables at the backend in the database server were developed using MS SQL Server 2008.

## *5. E-VOTING SYSTEM IMPLEMENTATION*

Following the architecture presented in section 3, a prototype for the e-voting system was developed. The system is divided into the client systems and the Application server system.

### 5.1 Client Systems

The developed client-side systems are the subsystems for registration, poll site voting and internet voting. The client-side subsystems interface the electorates to the e-voting system during the registration and voting processes.

### 5.1.1 Registration Centre Subsystem

Figure 2 depicts the voters' Registration Centre subsystem. The Register Voter module allows voters' information to be stored in the system. During the registration process, the picture of each voter is stored against his/her biodata (which must include mobile phone number) and the fingerprints of the voter are scanned into the system. A SMS containing voter identification number (voters ID) and a voting code is sent immediately after registration to voters as receipt acknowledging their registration. Figure 3 shows the Register Voter module of the Registration Centre subsystem.

### 5.1.2 Poll Site Voting Subsystem

The poll site voting subsystem is a client-side application system which electorates use to vote under the supervision of the electoral body or other relevant government agencies on Election Day. This subsystem can be viewed as the electronic version of the conventional tradition paper ballot casting However unlike traditional paper ballots which restrict ballot casting to electorate's ward/precinct (or point of registration) the poll site subsystem allows ballot casting at any poll site. Figure 4 depicts the poll site voting subsystem.

### 5.1.3 Internet Voting Subsystem

The internet voting subsystem is a client-side application system which electorates can use to cast their ballots outside the poll site anywhere and at anytime (though within the voting period timeframe) on election day. Figure 5 depicts the web page of the developed e-voting system.

### 5.2 Application Server

The developed application server is a software framework dedicated to the efficient execution of procedures (programs, routines, scripts) for supporting the construction of applications. The sever has five menu options, namely New Contestant (use to register new contestants), Voter's List (use to view list of registered electorates), Registered Party (use to register new political parties), Election Process (use to initiate and terminate a particular election) and Election Result (use to view the result of a particular election). The developed e-voting system requires that the Application Sever must be running before any client action could take place. Figures 6 – 8 depict the some menu options that make up the application server menu.

## *6. CONCLUSION*

Elections allow the populace to choose their representatives and express their preferences for how they will be governed. Naturally, the integrity of the election process is fundamental to the integrity of democracy itself. The election system must be sufficiently robust to withstand a variety of fraudulent behaviors and must be sufficiently transparent and comprehensible that voters and candidates can accept the results of an election. However, this cannot be said for conventional voting systems. Electronic voting is emerging as significant alternative to these conventional systems in the delivery of reliable and trusted elections. This paper details the requirements, design and implementation of a generic e-voting system, where voters can cast their votes anytime, anywhere and using a number of electronic devices including private computer networks, web and mobile phones.



## *7. REFERENCES*

Annan K., (2000). UN Secretary General Kofi Annan's Closing Remarks to the Ministerial on June 27th 2000, at http://www.demcoalition.org/pdf/un_secertary_gen_kofi_annan.pdf.

Boniface M., (2008). A Secure Internet-Based Voting System for Low ICT Resourced Countries. Master of Information Technology Thesis, Department of Information Technology, Makerere University, Uganda.

Buchsbaum T. M., (2004). E-voting: International Developments and Lessons Learnt. Proceedings of Workshop on Electronic Voting in Europe –Technology, Law, Politics and Society, Austria, at www.subs.emis.de/LNI/Proceedings/Proceedings47/ Proceeding.GI.47-4.pdf.

Fischer E. A., (2003). Election Reform and Electronic Voting Systems (DREs): Analysis of Security Issues. Congressional Research Service, Library of Congress, November 2003.

Held D. (2006). Models of Democracy. Polity Press, Malden, Cambridge, Third edition.

Kohno T., Stubblefield A., Rubin A. Wallach D. S., (2003). Analysis of an Electronic Voting System. Johns Hopkins University Information Security Institute Technical Report TR-2003-19.

Krimmer R., Triessnig S. and Volkamer M. (2007). The Development of Remote E-voting around the World: A Review of Roads and Directions" at http://www.e-voting.cc/files/VOTE-ID-2007/pdf.

Magi T., (2007). Practical Security Analysis of E-Voting Systems. Master of Information Technology Thesis, Department of Informatics, Tallinn, University of Technology, Estonia.

Malkawi M., Khasawneh M., Al-Jarrah O., (2009). Modeling and Simulation of a Robust E-voting System. Communications of the IBIMA, Volume 8, 2009. ISSN: 1943-7765.

Muir H, Laville S. and Gillan A., (2005). New Fears over Postal Vote Fraud. Accessed at http://politics.guardian.co.uk/election/story/0,15803,1458341,00.html.

Nestas L. H., (2010). Building Trust in Remote Internet Voting. M. Sc Thesis, Department of Informatics, University of Bergen.

NSF, (2001). Report on the National Workshop on Internet Voting: Issues and Research Agenda, National Science Foundation. At http://news.findlaw.com/cnn/docs/voting/nsfe-voterprt.pdf.

Rubin A. D., (2002). Security Considerations for Remote Electronic Voting. Communications of the ACM, 45(12):39–44, December 2002.

United Nations, (1948). Universal Declaration of Human Rights. At http:// www. un.org/ events/humanrights/2007/.../declaration%20_eng.pdf.

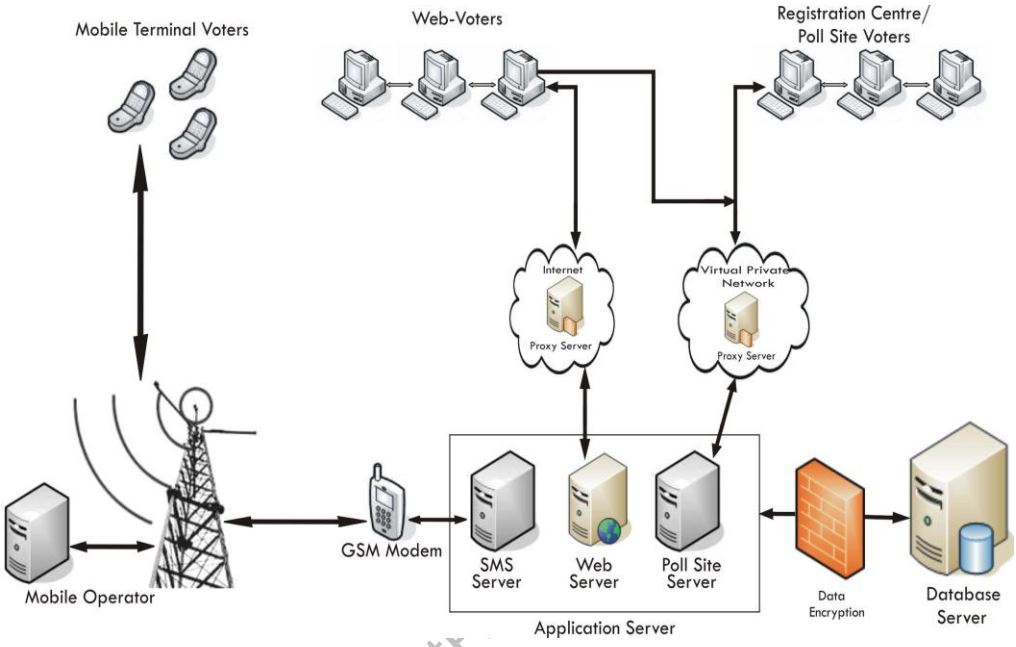


**Figure 1: Architecture of the Developed E-voting System**

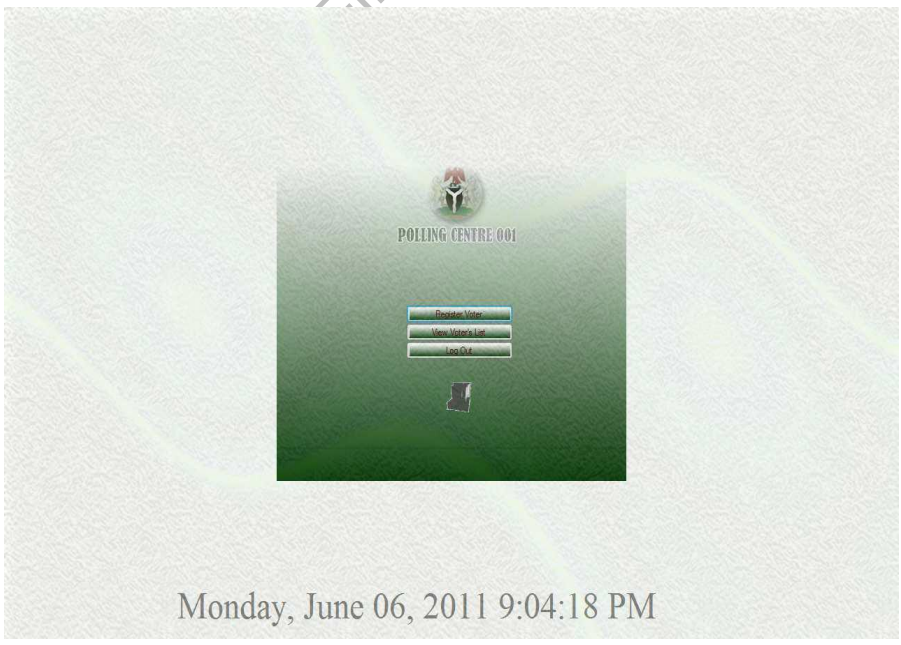


**Figure 2: Registration Centre Subsystem of the Developed E-voting System**

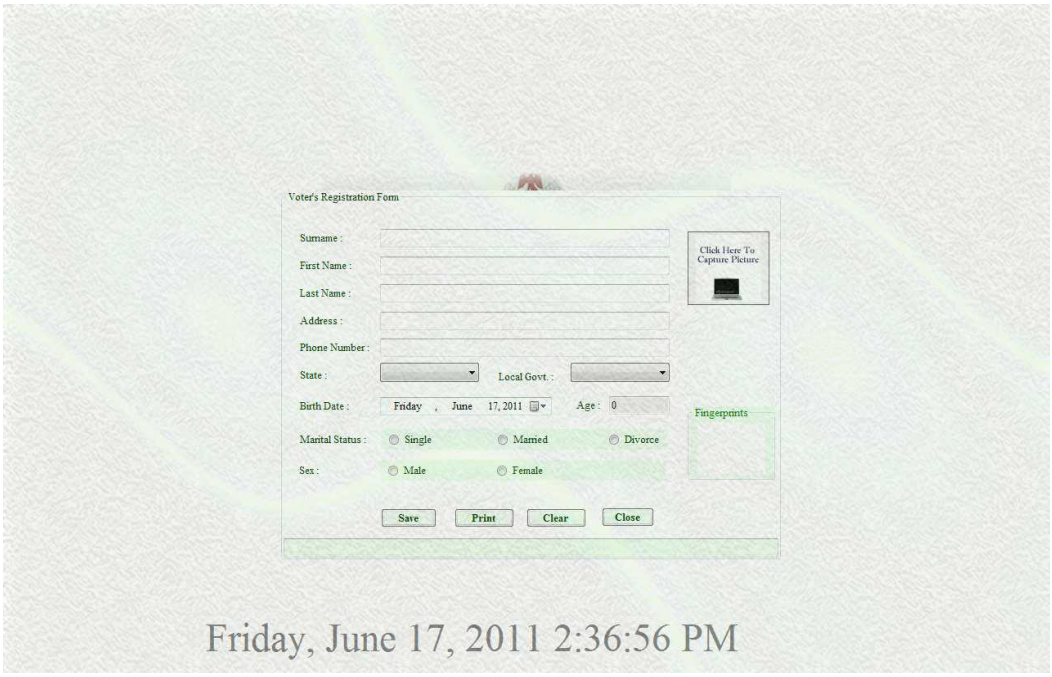


**Figure 3: Registration Voter Module of the Registration Centre Subsystem**

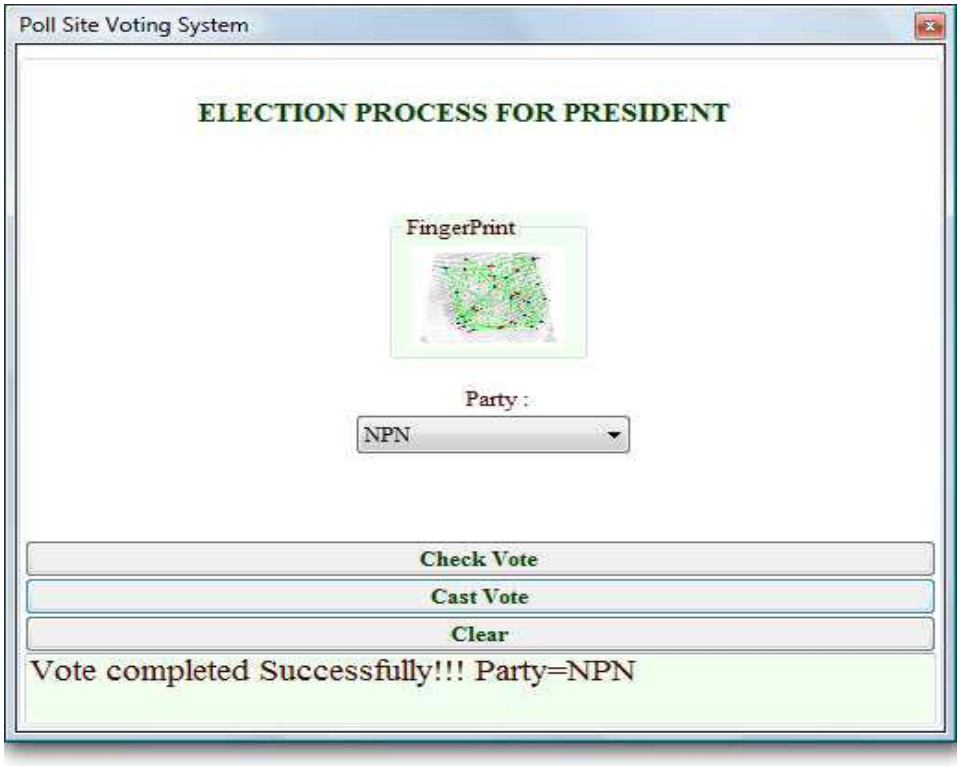


**Figure 4: Poll Site Voting Subsystem**

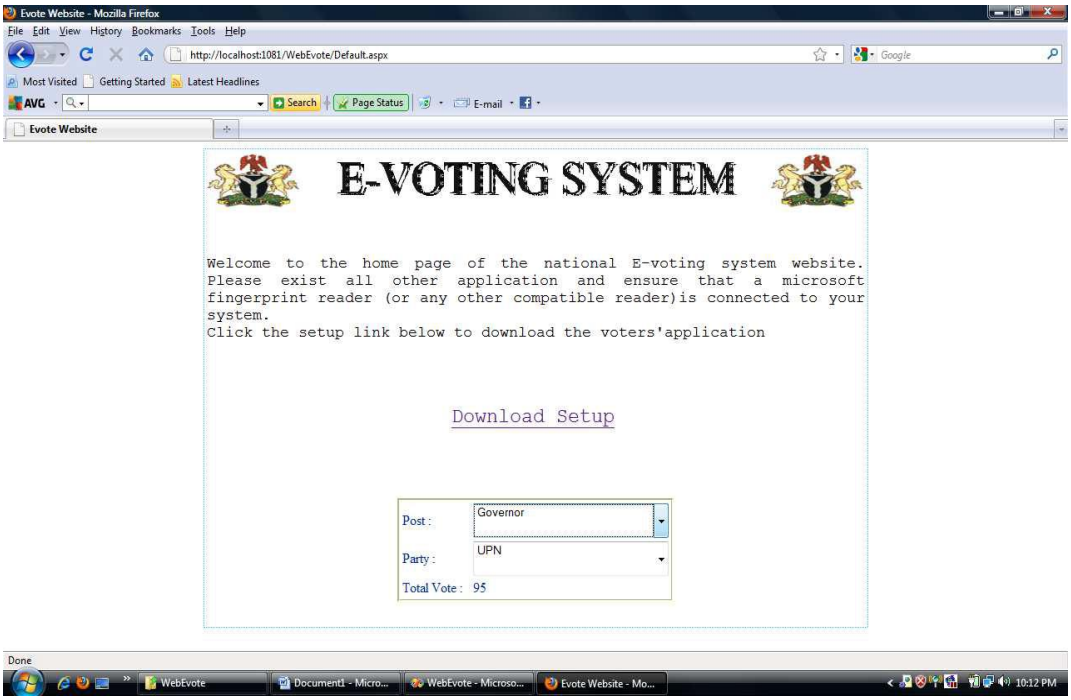


**Figure 5: Web Page of the Internet Voting Subsystem**


**Figure 6: New Contestant Menu of Application Server**


**Figure7: Voter's List Menu of the Application Server**

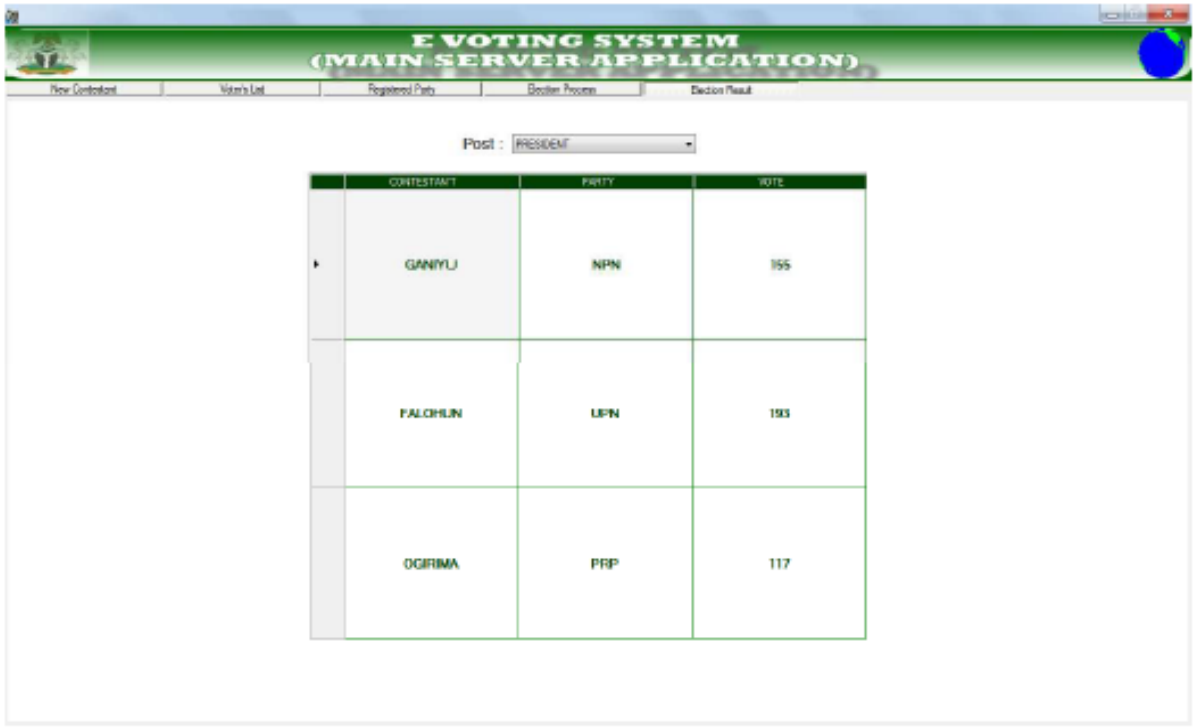


**Figure 8: Election Result Menu of the Application Server**