Building a Multimodal, Trust-Based E-Voting System

Musa Adebola G.[1], **Ayo Charles K.**[2], **John Samuel N**[3]**.**
Covenant University, Ota, Nigeria
[1,2]Department of Computer and Information Sciences
[3]Department of Electrical and Information Engineering

Abstract: *This paper addresses the issue of voter identification and authentication, voter participation and trust in the electoral system. A multimodal/hybrid identification and authentication scheme is proposed which captures what a voter knows – PIN, what he has – smartcard and what he is – biometrics. Massive participation of voters in and out of the country of origin was enhanced through an integrated channel (kiosk and internet voting). A multi-trust voting system is built based on service oriented architecture. Microsoft Visual C#.Net, ASP.Net and Microsoft SQL Server 2005 Express Edition components of Microsoft Visual Studio 2008 was used to realize the Windows and Web-based solutions for the electronic voting system.*

.

Keywords: Multimodal, Multi-trust, Internet voting, Service-Oriented Architecture, Electronic voting, Remote voting

1. Introduction

In a democratic system of governance, election is very crucial and the integrity of the electoral process is sacrosanct. The electoral process includes registration of voters, voting, tallying and collation.

The Council of Europe recommendations defined electronic voting (e-Voting) as "the use of electronic means in at least the casting of the vote" [1]. e-Voting is a major issue of concern in governance especially in developing nations. Electronic elections are still an emerging field [1].

The punch card was the earliest e-Voting system used in the 1960s [2]. The optical scan machine is another e-Voting system that can read a voter's mark on a ballot. The Direct Recording Electronic (DRE) machine is the most recent. The voter enters his choices into electronic storage via a touch-screen, push buttons, or similar device. The voter's choices are stored in these machines via a removable memory

cartridge, diskette or smart-card and added to the choices of all other voters. Bellis affirmed that the DRE machine has been extensively used in Brazil, India, Venezuela and United States of America [2]. In

2004, more than 27% of US counties used DRE technology, an increase of 13% over 2000 election [3].

In kiosk/polling place e-Voting, dedicated machines are used in polling stations to enable the voters cast their votes. This form has the advantage that it can be thoroughly supervised. In remote e-Voting, voters are able to mark and cast their votes on the Internet or telephone but supervision

is limited. Though, remote e-Voting has an advantage of convenience [4] for the voter which can enhance turnout, it is fraught with problems which include: privacy and anonymity infringement, vote buying, vote coercion, vulnerability to attack, audit trail may not be possible, etc [5, 6, 7, 8, 9].

Internet voting (i-Voting) had been employed in countries like United Kingdom, Estonia, Canada and Switzerland. Table 1 shows the list of countries with e-Voting projects by type and year of first usage and figure 1 shows the world map of e-Voting

Table 1:List of Countries with e-Voting Projects by Type and Year [20]

Country	Type	Date
Belgium	Polling place e-Voting	First trial in 1991
Brazil	Polling place e-Voting	First in 1996
Germany	Remote e-Voting	First tested in 1999
UK	Polling place e-Voting, Remote e-Voting	First in 2000
Ireland	Polling place e-Voting	First tested in 2000
Australia	Polling place e-Voting	First in 2001
Switzerland	Remote e-Voting	First in 2003
Norway	Polling place e-Voting	First in 2003
Austria	Remote e-Voting	First in 2003
Canada	Remote e-Voting (Internet and Telephone)	First in 2003
France	Polling place e-Voting, Remote e-Voting	First in 2003
India	Polling place e-Voting	First in 2003
Spain	Remote e-Voting	First in 2003
Estonia	Remote e-Voting	First in 2004
Portugal	Polling place e-Voting	First in 2004
The Netherlands	Polling place e-Voting, Remote e-Voting	First in 2004

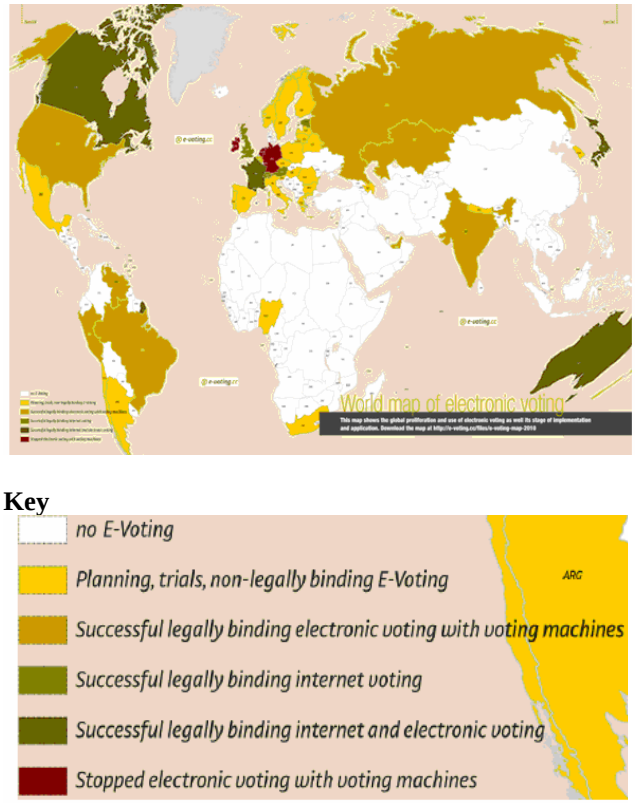

Figure 1: World Map of E-Voting [29]

In order to design and develop an e-Voting system that is suitable for large-scale elections, it is expedient that some acceptable public standards be observed. Burmester and Magkos in [14] identified some of these standard requirements as follows:

(1) *Security* [8, 15]. This standard includes the following properties (a) Democracy [18, 19] - Only eligible voters can cast votes, and no voter can cast more than one vote. (b) Accuracy [18, 19] - No vote can be altered, duplicated or eliminated without being detected. (c) Privacy [8, 16, 19] - All votes remain secret while the voting process is taking place, and each individual vote cannot be linked to the voter who cast it. For uncoercibility, no voter should be able to prove the value of his/her vote to another party. (d) Verifiability [8, 17, 18, 19] - Any observer can be convinced that the election is accurate and that the published tally is correctly computed from votes that were correctly cast and (e) Robust [16, 17] - All security requirements are fully satisfied, despite the failure and/or malicious behaviour by any coalition of parties (voters, authorities, outsiders).

(2) *Practical*. This standard includes the following properties (a) Convenience [15, 16, 17, 19] (b) Conformance with standard platforms and technologies. (c) Accessibility by the disabled [15, 17]. (d) Performance irrespective of the size of the election, and (e) Extensive testing - so as to enhance trust and confidence from officials and the public.

The electoral process includes registration of voters, voting, tallying and collation. Kofler et al., (2003) identified two fundamental elements in any e-Voting system (i) The registration process during which the voters is identified and authenticated and (ii) The voting process where the voter cast his vote.

Before a voter can cast a vote, he has to register. In order to identify a voter, three fundamental criteria can be used to differentiate the technologies. These according to Krimmer et al., (2007) are: (a) what he knows, (b) what he has and (c) what he is. Biometrics is what you are. These following techniques of identification are used in e-Voting system: (i) Username and Password (Personal Identification – PIN) - the voter is identified because he knows the PIN. (ii) Transaction Number (TAN) - the voter possesses something that identifies him. (iii) Smart-Cards - this also identifies him when his properties are read as stored on the card and (iv) Biometrics - the voter himself identifies himself with his biometric properties. A hybrid of these identification technologies can be explored in e-Voting system.

In PIN-based e-Voting systems, the voter logs in to the system with his PIN and he is identified. He is then allowed to access and fill the ballot. An example is the Active Transport Society Elections [21]. The voter logins with a one-time security code, fill the ballot and cast his vote, where cryptography is used to secure the communication between the browser and the election server. In this system, security is based on the integrity of the election commission and server administration.

In TAN-based e-Voting systems, the voter is issued with a transaction number with which he can cast his vote. The number is usually generated by a trust center. The connection between a voter and the election server is also cryptographically secured [26]. The European Union (EU) student vote system is a TAN-based Internet application system used to vote for EU student council [22]. The communication between the voter and the election system is encrypted with a key issued by a trust center [26]. Another example of a TAN-based election system is the one for the election of the Jugendgemeinderat (young city council), an advisory board at Fellbach, German, 2001 [23]. Figure 2 expresses the various levels of elections.

Levels	Leg. Binding	Org. Binding	Non-Binding
1st Level: national	☑		
2nd Level: regional, local	☑		
3rd Level: org., assoc., companies	(☑)	☑	
4th Level: shadow, parallel			☑
5th Level: technical test			☑

Figure 2: Levels of Election [1]

First and second level elections are legally binding and of higher political importance. They are regulated by law (example - the Nigerian Electoral Act 2010) and the results of the elections have consequences. The most rigid legal framework being the first level elections. Though PIN-based and TAN-based election systems are relatively cheap to implement, they do not have a legal foundation as a basis of identification and authentication. Distribution of TAN for each election can be expensive and susceptible to error. Hence, PIN-based and TAN-based systems cannot be used for first and second level elections.

The use of smartcard is another means of identification in e-Voting systems. Some smartcard-based e-Voting system uses smartcard for digital signature and enables cryptographic protocols. The Sensus system [24] and the German i-Vote [25] system utilize the blind signature based

algorithm. The algorithm follows a one-stage approach where the voter fills a ballot sheet which is then blinded and signed. It is encrypted and sent to the registration server which authenticates the digital signature of the voter. The authenticated ballot sheet is then sent to the ballot server. In this type of system, registration and voting is done in a single phase. The limitation [26] is that if the registration server and the ballot box server are able to collude, voter anonymity can be compromised and his privacy infringed upon.

Kalu-Mba and Ofodile, (2010) developed a secure e-Voting system where voters identification and authentication is multimodal based on biometrics, smartcard and Voter Identification Number (VIN) [12]. In their work, they incorporated multilingual audio facilities in English and three major Nigerian languages: Yoruba, Hausa and Igbo to allow the active participation of the disabled/impaired ones. Voters' participation is limited to citizens living in the country alone. Nigerians living outside the country cannot participate. Election system architecture is one-phased.

Ayo and Babajide in [27] developed a secure i-Voting system where identification and authentication was based on multimodal features also, such as biometrics and PIN. Audio was also incorporated. The limitation was that the architecture was one-phased.

In this work, the objective is to emphasis on e-Voting model implementation in developing nations and one of which is Nigeria. We also address the issue of security by employing a multimodal means of identification and authentication that captures what the voter knows, what he has and what he is [12, 13]. Also, massive voter participation issue is considered where voters in and out of the country are given chances to participate in the democratic government of their country. The system has two channels through which vote can be cast and these channels are integrated. These are: through the kiosk (e-Voting Machine (EVM)) and the Internet. Trust issue is very paramount in e-Voting system. The voters need to have confidence in the voting system so that they can believe in it. Hence, we leverage on service oriented computing theory to develop a multi-trust e-Voting system.

The remaining part of the paper is succinctly arranged as follows: section 2 enunciates on the service-oriented computing theory, section 3 discusses the architectural framework and section 4 the conclusion.

2. Service-Oriented Computing

According to Papazoglou [10], Service Oriented Computing (SOC) is the computing paradigm that utilizes services as fundamental elements for developing applications using Service Oriented Architecture (SOA). Service Orientation is a paradigm for developing and deploying application quickly and cost effectively [30]. SOA applications are developed using component-based software development approach, with reuse in mind. In SOA, software components are encapsulated as services. SOA builds applications by seeing components therein as a set of interacting services. Services encapsulate business functionality. It is a function performer. Services are autonomous and platform-independent. Services enable access to one or more capabilities with prescribed interface. Services can be described, published, discovered, and dynamically assembled for developing massively distributed, interoperable, evolvable systems [11]. Other service characteristics are: loose coupling, reusability, autonomy, statelessness. Services can also be composed to provide higher functionality for distributed applications [31].

3. Architectural Framework

Based on Purba in [28], we proposed a 3-tier Enterprise Application Architecture as represented in figure 3, with the introduction of the SOA services layer to the business tier.

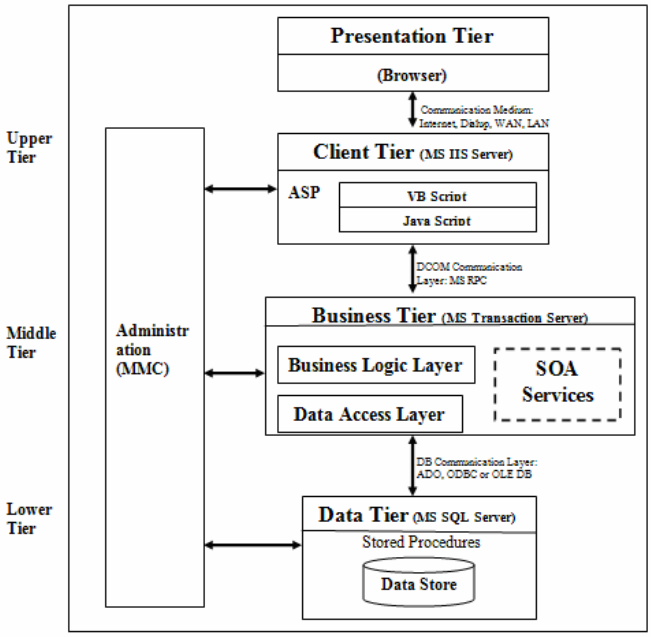

Figure 3: Enterprise Application Architecture

A trust-based multi-phase voting protocol was used while the election process was done in phases and they were rendered as web services.

The SOA-based e-Voting services are illustrated in figure 4.

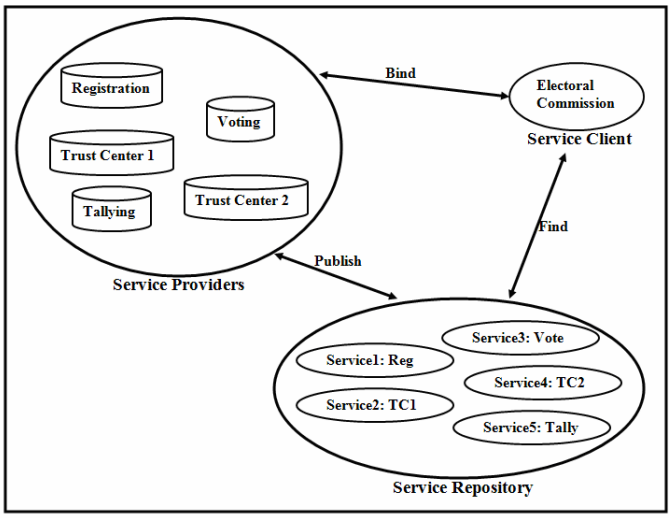

Figure 4: SOA-Based e-Voting Services

In figure 4, the service providers advertise their services by publishing to the service repository. The electoral commission is the service client/consumer. The service client finds related services from the service repository and composes services using service orchestration paradigm. After which the service client binds to the appropriate service providers at the instance of each voter. A sample voter interaction with such system is shown in figure 5.

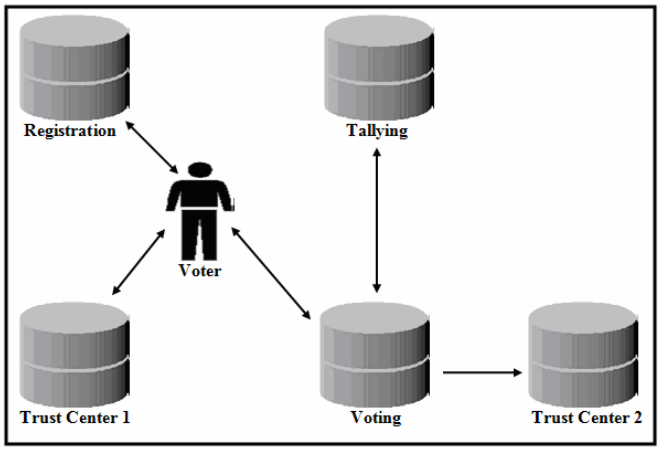

Figure 5: Voter Interaction with the e-Voting System

Trust, in this model, is distributed among the following participants in the system: Registration authority, trust center 1, voting authority, tallying authority and trust center 2.

Voter interaction with the system is as follows:

Step 1: Eligible voters register before the start of elections. Registration is done continuously except at a legislated time. For example, according to the amended Nigeria Electoral Act 2010, it is 30 days before the commencement of the elections.

Step 2: On the Election Day, a voter is authenticated as eligible by the registration authority and given a token.

Step 3: A voter also obtain another token from the Trust Center 1. This is to reduce the possibility of collusion in order to break the voter's privacy property [26].

Step 4: These two tokens are presented to the voting authority to request for a ballot.

Step 5: He fills the ballot, cast it and obtain a receipt. The cast ballot is transmitted to trust center 2 as a backup for security reason.

At close of election, the votes are collated by the tallying authority and result is announced.

4. Conclusion

The advent of electronic voting is indeed a revolution of the traditional paper based voting system. e-Voting system has helped in the automation of the traditional voting system and hence its efficiency. Electronic model of voting has been largely embraced in the developed world from Estonia to Switzerland and the United States of America to mention a few. There is a need for developing nations to embrace the technology in their democratic system. It is also necessary to fully explore the benefits entrenched in the e-Voting model.

The multimodal, multi-trust, integrated e-Voting model ensures voters' identification and authentication, massive voter participation in and out of country of origin and enhances voters' trust. Its underlying voting scheme is such that the trust assumptions are distributed on many trusted authorities. The e-Voting system also takes cognizance of the universal e-Voting system standards and requirements in its implementation.

5. References

[1] Krimmer, R, Triessnig, S and Volkamer, M (2007) The Development of Remote E-Voting Around the World: A Review of Roads and Directions. Springer Lecture Notes in Computer Science, Volume 4896/2007, 1-15

[2] Bellis, M (2009) The History of Voting Machines Available at http://inventors.about.com/library/weekly/aa111300b.htm Accessed on 5th Feb. 2011

[3] Card, D, and Moretti, E (2007) Does Voting Technology Affect Election Outcomes? Touch-screen Voting and the 2004 Presidential Election. The Review of Economics and Statistics Vol. 89, No. 4, Pages 660-673

[4] Norris, P (2002) E-Voting as the Magic Ballot? KSG Working Paper Series RWP 02-016

[5] Schneier, B (2000) Voting and Technology Available at http://www.schneier.com/crypto-gram-0012.html Accessed on 5th Feb. 2011

[6] Karlof, C, Sastry, N and Wagner, D (2005) Cryptographic Voting Protocols: A Systems Perspective. Proceedings of the 14th conference on USENIX Security Symposium, Vol 14

[7] Rubin, A. D (2002) Security considerations for remote electronic voting. Communications of the ACM, Volume 45 Issue 12, December 2002

[8] Clarkson, M.R, Chong, S. and Myers, A.C (2008). Civitas: Toward a Secure Voting System. IEEE Symposium on Security and Privacy, pp. 354 - 368

[9] Spycher, O., Haenni, R., and Dubuis, E. (2010) Coercion-Resistant Hybrid Voting Systems. In Proceedings of Electronic Voting EVOTE2010, pp 269-282

[10] Papazoglou, M.P. (2003) Service-Oriented Computing: Concepts, Characteristics and Directions. In IEEE Proceedings of the 4th International Conference on Web Information Systems Engineering (WISE'03)

[11] Papazoglou, M.P., Traverso, P., Dustdar, S., Leymann, F. and Kramer, B.J. (2006) Service-Oriented Computing: A Research Roadmap. In Dagstuhl Seminar Proceedings

[12] Kalu-Mba, N and Ofodile, W. (2010) Development of a Secure Electronic Voting System. Bachelor thesis, Covenant University, Nigeria.

[13] Ayo, C, K, Daramola, J.O, Obi, G.M.M and Sofoluwe, A.B. (2010) An End-to-End e-Election System Based on Multimodal Identification and Authentication. In Proceeding of The 6th International Conference on e-Government, pp. 10-17

[14] Burmester, M and Magkos E. (2003) Towards Secure and Practical E-Elections in the New Era. Springer Series: Book Chapter in Secure Electronic Voting, Advances in Information Security, Vol. 7

[15] Institute of Governmental Studies, University of California, Berkeley. Electronic Voting - Overview and Issues. Accessed on 24th Jan, 2011 at http://igs.berkeley.edu/library/research/quickhelp/policy/government/e_voting.html

[16] Kohno, T, Stubblefield, Adam, Rubin, A. D. Wallach, D. S. (2004). Analysis of an Electronic Voting System. 2004 IEEE Symposium on Security and Privacy

[17] Arah, U.O.A (2010). Designing Arah-You Voting Machine and Automated Accreditation System from the Nigerian Perspective. Proceeding of the 23rd National Conference of Nigeria Computer Society, Vol 21, pp 129-140

[18] Smyth, B, Ryan, M Kremer, S.(2009) Election verifiability in electronic voting protocols

[19] Joaquim R, Zúquete, A, Ferreira, P (2003) Revs – A Robust Electronic Voting System

[20] ACE Encyclopedia (2011) Requirement for e-Voting. Accessed on 7th March, 2011 at http://aceproject.org/ace-en/focus/e-voting/countries

[21] Vote-Now System (2011), Accessed on 22nd Feb, 2011 at https://secure.vote-now.com/elections/ Gen/demo/

[22] EU Student Vote (2002) Accessed on 25th Feb, 2011 at http://www.eu-studentvote.org/

[23] Youth Council (2001) Accessed on 25th Feb, 2011 at http://www.fellbach.de/text/371/de/jugendgemeinderat.html

[24] Sensus (2001) A Security Conscious Electronic Polling System. Accessed on 25th Feb, 2011 at http://lorrie.cranor.org/voting/sensus/

[25] German i-Vote (2001) Accessed on 25th Feb, 2011 at http://www.forschungsprojekt-wien.de/

[26] Kofler, R, Krimmer, R and Prosser, A (2003) Electronic voting: algorithmic and implementation issues. In Proceedings of the 36th Annual Hawaii International Conference on System Sciences, IEEE Xplore.

[27] Ayo C.K and Babajide, D.O (2007) Design and Implementation of a Secure i-Voting System. The Journal of Computer Science and its Application. Vol 14 No 2, pp. 38-51

[28] Purba,S (2002) Architecture for E-Business Systems: Building the Foundation for Tomorrow's Success. CRC Press LLC.

[29] World Map of Electronic Voting 2010. Accessed on 7th March, 2011 at http://www.e-voting.cc/static/evoting/files/e-voting-map-2010.pdf

[30] Papazoglou, M.P. (2008) Service-Oriented Computing Research Roadmap. International Journal of Cooperative Systems Vol 17 No 2, pp 223-255

[31] Hubbers, J.W., Ligthart, A and Terlouw, L (2007) Ten Ways to Identify Services. SOA Magazine. Accessed on 14th Mar, 2011 at http://www.soamag.com/I13/1207-1.php