Design and Implemenation of a Unified e-ID Card for Secure e-Voting System (MUSES)

Samuel N. John
Department of Electrical & Information Engineering.
Covenant University,
Ota, Ogun State, Nigeria
Email: samuel.john {at} covenantuniversity.edu.ng

Charles Kayode Ayo
Department of Computer & Information Science,
Covenant University,
Ota, Ogun State, Nigeria

Charles Ndujuiba
Department of Electrical & Information Engineering.
Covenant University,
Ota, Ogun State, Nigeria

Chinonso E. Okereke
Department of Electrical & Information Engineering.
Covenant University,
Ota, Ogun State, Nigeria

Abstract--***Security and convenience in e-Voting system has been a major issue that has been looked into recently in time past. Application of smart card technology has brought breakthroughs which affect this aspect. But there can be improvement in the convenience of a general smart card society by solving the problem of carrying a barrage of smart cards in order to identify with various e-Government and e-Payment systems.***
The general security of an e-voting process was improved by implementing biometric (fingerprint authentication) into the process. Thus, a 3-factor authentication system was developed based on PIN, Smart Card, and Biometrics. Also, attempt was made to develop a multipurpose and multifunctional card for the convenience of all carriers. With these, security and convenience are achieved.

Keywords:--Unified, e-ID, e-Payment, Biometrics, Fingerprint Authentication, e-Government.

I. INTRODUCTION

The advent of Smart Card Technology has brought many positive changes to the society such as security and convenience in the performance of an array of activities. Since its introduction in 1974, the use of smart cards has become increasingly prominent. Over 3.8 billion were estimated to be in use as at the last millennium [1]. The smart card with its many applications has been implemented in Angola, Morocco, Germany, Italy and some other European countries as a medium of electronic identification with a good amount of success. With the tremendous success of smart card technology, it is extremely rare to find individuals from the developed and developing societies and nations with only one card in their carriage. They probably have at least two or more cards each, one serving its distinct function i.e. either for the identification e.g. national ID card, driver's license or as a means of business transaction e.g. E-tranzact card, Bank ATM card etc.

Electronic identity has become a major issue in online commerce and public sector organizations. The problem of identity verification and management will continue to increase in magnitude and importance, thus relying on passwords, and asking customers to remember them may neither be sufficient nor efficient. Any system that relies on password is insecure because there are several software tools around that are used to defeat password security [5, 16, 17].

To conduct a free and fair election, security and proper authentication must be put in place in the electoral system [12]. The use of biometric authentication along with smart card can be a power tool in ensuring security in the Multimodal Service-oriented Electoral System (MUSES).

This paper addresses the issue of voter identification and authentication 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. It also seeks to design and develop a multifunctional and multipurpose e-ID card that incorporates the general and basic purposes and functions of the various present day identity and e-payment cards and therefore unifies all available systems (e-Voting inclusive).

Methodology

The Unified e-ID card System was designed and implemented systematically. Firstly, a general national database using Microsoft SQL Server was developed to store biometric details and needed information about each citizen. A registration application that works and connects with the database was also be developed using Visual Basic.Net and C#. This project incorporates the registration process where citizens are expected to supply their biodata as well as biometric details such as fingerprint for the production of the various e-ID cards. ACOS3 cards were used as electronic identity cards for this project. The next step will be to develop few applications that will work with the electronic ID cards for ATM application (e-Commerce), e-Insurance application and e-Voting application, which is the main aspect of this project (MUSES).

II. SMART CARDS, IDENTITY MANAGEMENT, E-PAYMENT AND SECURITY

A smart card is a card that contains an embedded computer chip that stores and transacts data. Its invention and

implementation improve the convenience and security of any transaction providing tamper-proof storage of user and account identity [2]. These cards can serve diverse functions ranging from SIM cards for calling to E-payment cards to social (ID) cards and access control or a combination of two or more functions i.e. multi-application and multipurpose cards. The ability of a smart card to be used for multiple purposes and multiple applications makes it a powerful tool in implementing unified identity system. Identity management (ID management) is a broad administrative area that deals with identifying individuals in a system (such as a country, a network, or an enterprise) and controlling their access to resources within that system by associating user rights and restrictions with the established identity[3, 9, 10, 11]. Countries have implemented Identity schemes around the world with varying level of security which is dependent on the purpose behind the implementation.

Angola leads, having the national e-Identity project in Africa which uses optical security technology. Other traces of e-Identity could be found majorly in Morocco, Kenya, Ethiopia to mention a few. E-Identity is also implemented in most part of Europe e.g., Italy, Belgium, Germany but the Republic of Estonia has by far the most highly-developed national ID card system in the world and is a country to learn majorly from as it concerns e-Identity management [13, 15].

In order to design and develop an e-Voting system that is suitable for large-scale elections, Burmester and Magkos [4] identified security as one of the standard requirements which have the properties of (a) Democracy - Only eligible voters can cast votes, and no voter can cast more than one vote. (b) Accuracy – No vote can be altered, duplicated or eliminated without being detected. (c) Privacy - All votes remain secret while the voting process is taking place, and each individual vote cannot be linked to the voter who cast it. (d) Verifiability - 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 - All security requirements are fully satisfied, despite the failure and/or malicious behavior by any coalition of parties (voters, authorities, outsiders).

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 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 identifies himself with his biometric properties e.g. fingerprint. A hybrid of these identification technologies can be explored in e-Voting system [5] for security purposes.

E-payment is a subset of e-governance which is the application of electronic means in the interaction between Government and Citizens and Government and Businesses. It is a form of direct payments and banking without physical appearance at the Bank through the means of electronic, interactive communication channels and other technology infrastructure [6]. Nigeria is predominantly a cash-based economy with a lot of cash in circulation. Nigerian banks have invested greatly in technology, and have widely adopted electronic and telecommunication networks for delivering a wide range of value-added products and services. Within the last decade, all the banks have transformed from manual to automated systems involving the use of various e-banking and e-payment systems. In 2008, the use of e-payment system in Nigeria accounted for N360 billion worth of transactions [7]. However, the level of ICT usage notwithstanding, the level of adoption of e-Banking by the citizen is still very low [8, 14]. Also one of the greatest threats to e-Banking is the increasing trends of identity theft, which is a major challenge to the Internet age. Therefore, there is need for a technology that is safe, convenient and not too demanding on the part of the user because of the level of literacy in the developing nations of the world, particularly Nigeria.

III. THE UNIFIED SYSTEM AND E-ID

As a unified e-ID, its main purpose is to incorporate the purposes of the various e-Government (voter's card inclusive) and e-Payment cards (credit cards) into one card. In order to fulfill such purpose the smart card is designed to display outwardly according to the template shown in figure 1, the template of Unified e-ID card.

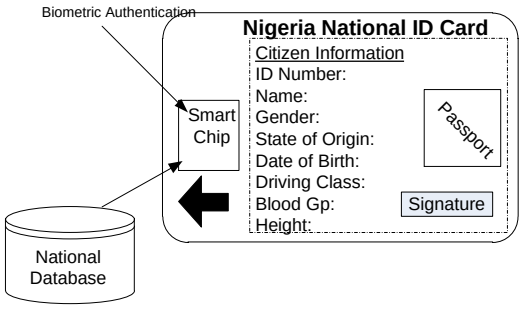

Figure 1: Template of Unified e-ID card

The fields shown on the card are namely: National ID Number, Name, Gender, State of Origin, Date of Birth, Class of License and License Number for the Driver's License), Blood Group, Height, Passport picture and signature.

Every other personal information about the card holder for the purpose of identification and authentication is accessible through the National ID Number which is stored in the card chip. This information is accessible at the kiosk-based terminal using the software design for this. The design of the database that works with the system is important as most data are stored in the database and not on the card chip. The various

platforms on which the unified card will work have their databases linked to the e-ID card by the national ID number stored in its chip. This way the smart card is unified because it works with a unified database which has the attributes of the national ID card, driver's license, voter's card and ATM card. The database therefore stores the attributes of the mentioned cards as fields for the implementation of the unified e-ID card. This makes the e-ID card unified.

There remains a need to recreate the e-Voting system, e-payment system inclusive, so as to function appropriately with the card. The systems work with the unified e-ID card because they share the same database or a common primary key which is the National ID number stored in the card chip.

The Security of the systems is hinged on the fingerprint biometric authentication process which is reliable [11]. Figure 2 shows the flowchart of the Fingerprint Authentication process of unified e-id-card system.

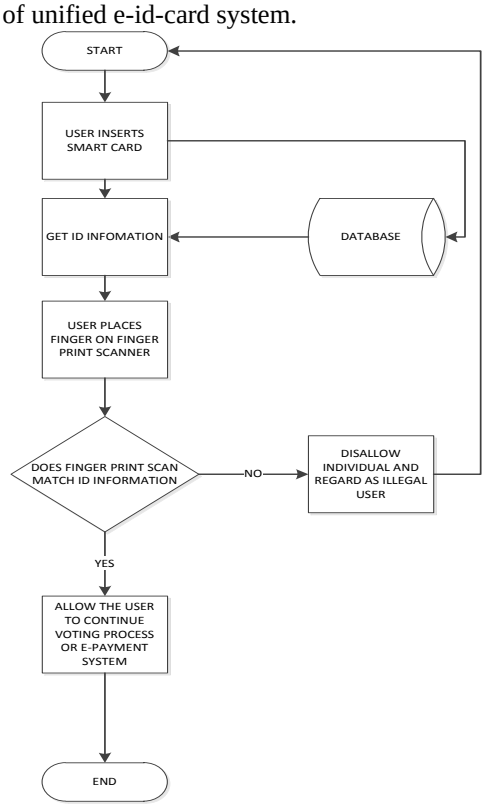

Figure 2 Flowchart of Fingerprint Authentication process

IV. IMPLEMENTATION IN MUSES

The MUSES is made up of the citizen registration module and voting module among others. Citizens register for the voting process prior to the voting day as shown in figure 3, providing their detailed personal information. They also register their fingerprints for authentication before the voting process. After registration the citizen can see the summary of their details which shows they have registered by representing their citizen ID/National ID which they are given during the registration process.

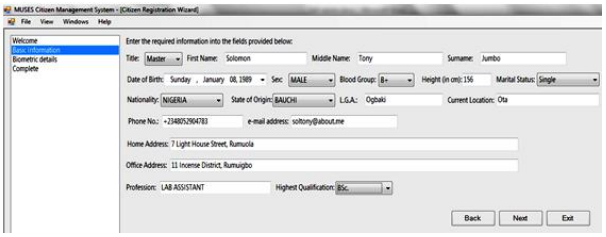

Figure 3 Citizen Registration Page

Figure 4 Biometric Registration: Fingerprint Enrollment

PINs are generated for each citizen in case the citizen wants to use either of the modes of voting apart from kiosk-based voting. It is important to note that the details of the citizens will also be used in other systems such as the e-Payment system with the unified database and for the unified e-ID card processing. Parties also register themselves and their corresponding candidates for political positions.

Before the Election day, the unified e-ID card is processed for the kiosk-based e-voting based on the details provided during the registration using a proprietary card tools and outwardly designed for physical identification as well showing the afore mentioned attributes in template design.

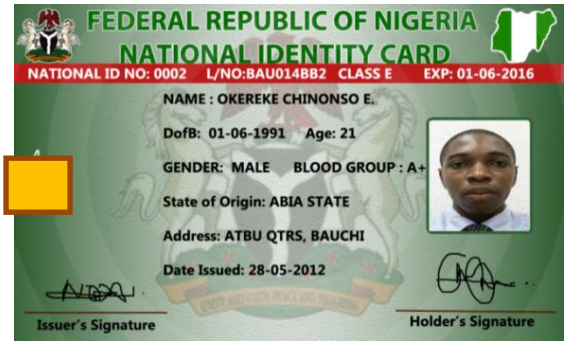

Figure 5: Picture of Unified e-ID card

Figure 6 Back side of the Unified e-ID card

On the Election Day, citizens bring unified e-ID card to authenticate and vote for their preferred candidate at the polling booth as shown in figure 5, figure 6. Figure 7 shows the authentication menu before voting and figure 8 shows the voting process.

Figure 7 Authentication before Voting

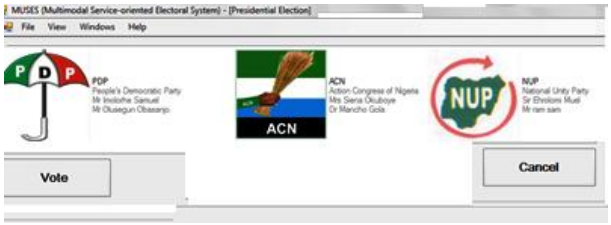

Figure 8 Voting Process

The e-ID card could also be used as an e-Payment card as it stands as unified card embedded with security.

V. CONCLUSION

The Unified e-ID card system was designed and implemented for convenience and security of all e-Government applications. It also ensures security and prevents cases of rigging in an e-Election system in any country and therefore maintains the standard of a free and fair election. Their merits are not limited to e-Election but also add convenience to the e-banking sector. This system which has already been incorporated by some developed nations of the world is a great improvement on the present electoral system. The MUSES uses a secured enterprise-wide network for transaction of messages and storage of data in the database server. It is to be manned by trustworthy administrators. Due to the auditing tools and capabilities provided by the database server, security in the system is also enhanced as actions carried out can easily be traced to the appropriate personnel.

VI. REFERENCES

[1] Fowler, Daniell C. and Swatman, Paula M.C., "Issues Affecting the Implemenatation of Multiple Application Smart Card Systems." University of Baltimore United States of America : s.n.

[2] CardLogix Corpration., "Smart Card and Security Basics." [Online] 2009.

[3] TechTarget., Identity Management (ID management). SearchUnifiedCommunications Website. [Online] 2012. [Cited: 24 April 2012.] http://searchunifiedcommunications.techtarget.com/definition/identity-management.

[4] Burmester, M and Magkos, E., "Towards Secure and Practical e-Elections in the New Era." Secure Electronic Voting, Advances in Information Security. s.l. : Springer, 2003, Vol. 7.

[5] Musa Adebola G., Ayo Charles K., **John Samuel N.**: "Building a Multimodal, Trust-Based E-Voting System", *Proceedings*: The 2011 World Congress in Computer Science, Computer Engineering, and Applied Computing (WORLDCOMP'11), Las Vegas, Nevada, USA, 2011, pp. 273-277.

[6] Dankwanbo, Ibrahim., "Understanding the e-Payment System.", Budget Office Paper presented, Federal Capaital Territory, March 2009.

[7] Charles K. Ayo, Wilfred Isioma Ukpere, "Design of a secure unified e-payment system in Nigeria: A case study." African Journal of Business Management, 4 August 2010, Vol. IV.

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

[9] 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.

[10] Kiayias A., Korman M. and Walluck D. (2006) An Internet Voting System Supporting User Privacy. In proc of Annual Computer Security Applications Conference. IEEE Computer Society, pp 165-174

[11] Kofler, R, Krimmer, R and Prosser, A (2003) Electronic voting: algorithmic and implementation issues. In Proc of

36th Annual Hawaii International Conference on System Sciences, IEEE Xplore.

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

[13] 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

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

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

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

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