BIO-CRYPTOGRAPHIC TECHNIQUE FOR ENHANCED E-VOTING SCHEME

NWABUEZE C. A.[1], NWOSE F. C.[2] and MUOGHALU C. N.[3]
[1,3]Department of Electrical/ Electronic Engineering, COOU, Uli.
[2]Post-graduate Student of EEE, Dept. COOU, Uli.
Email: [1]canwabueze@yahoo.com, [2]francisnwose@yahoo.com, [3]cnmuoghalu@yahoo.com

ABSTRACT
This paper presented a simulation model of an enhanced e-voting system based on bio-cryptographic schemes. A lot of work has been done on e-voting systems using biometrics as well as cryptographic schemes but not fusing both. This work provides an improvement on the already existing E-voting models by fusing and adopting biometric and cryptographic techniques as well as using a secure transmission channel for confidential datasets in the voting process. A model of an e-voting system leveraging on Biometric Encryption using Biometric key binding on fingerprints for the proposed **SMARESIM (**Self-monitoring analysis and reporting E-voting simulation model) has been developed and simulated. In the bio-cryptographic scheme, a digital key is randomly generated during enrollment. This key and the fingerprint are monolithically bound using cryptographic algorithms, that is, the randomly generated key is hidden within the biometric sample collected using bit replacement algorithms. When the user presents the fingerprint sample and it matches the biometrically encrypted key, the randomly generated key during enrollment will be regenerated and thus the user will be authenticated. The **SMARESIM** minimizes vulnerabilities associated with the conventional voting schemes, leading to minimization of electoral fraud.

Keywords: *Bio-cryptography, Security, E-voting, Real-time System.*

1.0 INTRODUCTION
Voting process plays an important role in any democracy which allows citizens to vote freely to produce an acceptable result [1]. Unfortunately, history shows that elections can be manipulated, leading to unacceptable results. In Nigeria, compromising of electoral processes has led to destruction of both lives and property, simply because the rule of the game was not adhered to. People usually want to impose themselves on the voters, so they use all sorts of means to get into office. This has continued to cause a lot of harm and has made the citizens poorer in spite of the abundance of natural and human resources in the country [2]. On May 29, 2009 Nigeria celebrated a decade of democracy. Many Nigerians said it was not worth celebrating, because the electoral system is a flawed exercise. Our political and electioneering process is branded with so many irregularities, ranging from ballot box snatching, stuffing of ballot boxes, political killings, using of political thugs to harass opposing candidates and finally weak Electoral Act. This mainly, is due to the fact that electoral processes in Nigeria are done manually and the result of such manual electoral process inevitably produces questionable electoral results.

Rapid application of Information and Communication Technology (ICT) in all facets of life has provided several potential benefits including improved efficiency, convenience with reduced costs and productivity. The application of ICT in the proper execution of democratic rights has made Electronic Voting (E-Voting) systems one of the paramount pillars of e-governance [3]. E-Voting is an election system that allows a voter record his or her secure and confidential vote. E-Voting is casting a vote electronically by tabulating votes using the Internet. The main goal of a secure e-voting system is to ensure privacy of the voter's and accuracy of votes.

Most electronic system of voting offers the following multiple advantages over the traditional paper-based voting: increased participation in democratic governance as more citizens have access to express their opinion, reduced costs as the materials required for printing and distributing ballots as well as the manpower required to govern poll sites are considerably reduced, flexible as it can be tailored to support multiple languages, greater speed and accuracy in placing and tallying votes as e-voting step by step processes help minimize the number of miscast and rejected votes, lower election fraud in endangered countries with young democracies [4].

This paper focuses on **kiosk voting** (i.e. e-booth) over the internet through a secured public infrastructure, particularly the **SMARESIM** (Self-Monitoring Analysis and Report E-voting Simulation Model).

1.1 The Components

In an Electronic Voting System the main components of the process include:

- **The Electronic Voters Register**- which is a comprehensive database of eligible voters.
- **Authentication-** which is done prior to balloting. This is based on the use of a secure biometric identification algorithm and schemes.
- **Voting, Collation and Transmission**- the election results directly from each of the polling stations are sent to designated collation centers in **REAL TIME**. In this case, it will involve the use of some Direct Record Balloting Machines (Electronic Voting Machines) connected over a VPN (Virtual Private Network). This will completely eliminate the cost associated with the printing of several million ballot papers [5].

Contemporarily, end users have dealt with electronic transactions or e-transaction and it is gradually becoming a part of daily life, for example, the online or mobile banking.

There is however a slight difference in the operations of an e-voting system when compared to an e-transaction system. In an e-transaction there is always a possibility to dispute about the content of the transactions. Users get printed notifications to prove their participation in transactions but in e-voting, there are no printed notifications to indicate a choice [5].

2.0 E-VOTING SURVEY

Gritzalis [6] expressed the fact that elections are very critical for the normal functioning of a society and it serves as a means by which the society can express their opinions thereby granting power to selected officials and also helps in building trust in the government and their support for democracy.

Chaum [7], introduced mix-nets where each layer of a sent message from a sender e.g Alice to a receiver, e.g Bob is decrypted by each mix-server along the way from sender to receiver and at the end an external observer cannot observe the relationship between any sender in particular and recipient. This message is first encrypted with the public key of each of the mixes. This type of mix-net proposed by Chaum is a decryption type mix-net and is not very resilient to failure unlike the re-encryption mixes which has greater resilience.

Choonsik et al. [8], proposed a scheme which improved on the Chaum's mixnet. Their scheme improved on the message expansion issue Chaum's mix-net scheme had because in Chaum's scheme the number of MIXes increases in relation to the length of the message making it less efficient than their scheme in which the length of the message is irrelevant to the number of mixes used. In a second scheme Choonsik et al., proposed, an improvement on the original Chaum's scheme which provides very little level of correctness (i.e. a mix-net should ensure that an output corresponds to the input) and does not satisfy the fairness property meaning that if one vote is disrupted, the outcome of the election can be learnt before the final tally is announced.

Mayasuki [9], proposed a robust e-voting scheme based on mix-net that is universally verifiable where the amount of mix-servers does not determine the amount of work done by the verifier i.e. the work done by a verifier is not dependent on the number of mix-servers.

Jakobsson [10], introduced a scheme which eliminates the use of zero-knowledge proof, making it more efficient than previous schemes based on mix-nets and also eliminates the issue of encryption of the same plain text resulting into similar cipher text that could be detected.

Neff [11], proposed an efficient verifiable mixing technique that can be used to achieve universally verifiable elections. Voter's credentials are mixed before the election commences rather than mixing encrypted votes (cipher texts) after the vote collection centre has received the ballots.

In the mix-net proposed by Acquisti [12], resilience is increased due to the collaboration in the exchange of ballot between the voters and third parties, although this protocol was generic, it can be applied to an e-voting scheme. At the end of the exchange of messages, nobody observing can tell the relation between any particular voter and votes cast. In this scheme, a third party (electoral official) verifies the identity of the voter to ascertain eligibility.

Chaum et al. [13], proposed a scheme for electronic voting where voters get encrypted receipts to verify their votes and the tellers ensure there is no link between the encrypted version and decrypted ballot receipts by performing anonymizing mixes.

Ryan et al. [14], later proposed another scheme which uses re-encryption mixes in the anonymizing tabulation phase instead of decryption mixes. This has an advantage over the RSA decryption mix used in the earlier schemes by Chaum because it is more tolerant to failure of any of the mix tellers and enables full independent rerun of the mixes and audit if necessary.

Benaloh, et al. [15], proposed a scheme based on homomorphic property of a probabilistic encryption method that provides the first verifiable secret-ballot election protocol that prevents vote selling and coercion. They assumed the existence of a voting booth which should help prevent coercion and the fact that voters are not given a receipt would prevent vote selling. They also proposed two protocols in this scheme. One is a single

authority voting protocol which does not achieve the secrecy of votes and the second which achieves vote secrecy, is a multi-authority scheme.

Nathan et al. [16], describe a Biometric based Software Solution for E-Voting using networking. For the software analysis and graphic display, they used the C# programming language with SQL database support and fingerprint security. In order to launch the program, a password login page appears. This ensures that only the registered administrators are allowed to launch the program. At the end of the elections, the voting results from the various polling units are uploaded to the central server (web server) via the internet for onward publishing of results by the central administrator. The super administrator is the only authorized personnel to publish the final election results for public viewing via the internet.

3.0 METHODOLOGY

The method adopted in this paper has embedded in it a certain degree of gate level oriented design and programmable VLSI in the sense that gate level components are logically connected together and used to characterize various components in the system. For example, logical components were used in the design of this model called the **SMARESIM (Self-Monitoring Analysis & Reporting E-voting Simulation Model),** to characterize the behaviour of various components of the model such as the Bios crypt Fingerprints Processing Unit (BFPU), the Remote Polling Booths (RPB), State Collection Centers (SCC) and the National Collection Center (NCC) all linked via a characterized MPLS-VPN (Virtual Private Network) backbone.

The block diagram of figure 1 gives an overview of the SMARESIM leveraging on Biometric Key Binding (BKB). It is a fusion of the voter registration and authentication processes along with the actual voting and collection processes.

At the enrollment stage, the biometric trait is collected and the biometric template is extracted. The template is then bound within a cryptographic framework with a randomly generated N-bit digital key which is appended to the BE template database. During the verification stage, a fresh biometric sample collected is then combined with the biometrically encrypted template in the database via a key retrieval algorithm. If the N-bit key of the initial randomly generated code is regenerated, the voter is allowed to cast a vote electronically.

After the voter casts a vote, the results from the vote is then split into packets, encapsulated and then transmitted to the collection center via a secure communication link (VPN backbone). At the collection centers the encapsulated votes are de-encapsulated and sent to the various applications attached to the systems. The administrators at the collection center can only access the voting results still with the aid of their fingerprints because their passwords are equally biometrically encrypted (the administrators at the various collection centers are also enrolled as administrators prior to the elections. They would have to undergo verification during the elections for them to be able to have access to election results). It is at the various collection centers (State

Collection Centers and the National Collection Center) that the election results are electronically tallied and displayed.

It is on this basis that the model as shown in figure 2 which categorically shows the cryptographic key binding and its retrieval after the fingerprint image processing is fused with the actual voting process is developed.

During the *enrollment phase*, the sensor scans the user's fingerprint and converts it into a digital image. The minutiae extractor processes the fingerprint image to identify specific details known as *minutia points* that are used to distinguish different users. Minutia points represent locations where friction ridges end abruptly or where a ridge branches into two or more ridges. A typical good-quality fingerprint image contains about 20-70 minutiae points; the actual number depends on the size of the sensor surface and how the user places his or her finger on the sensor. After the features are extracted, they may be jiggled slightly, to generate different hashes and a template created for the user. That is, the features are moved incrementally, to compensate for a user not placing his or her finger in exactly the same location as when generating the original cryptographic key (Error Correction Codes) [5].

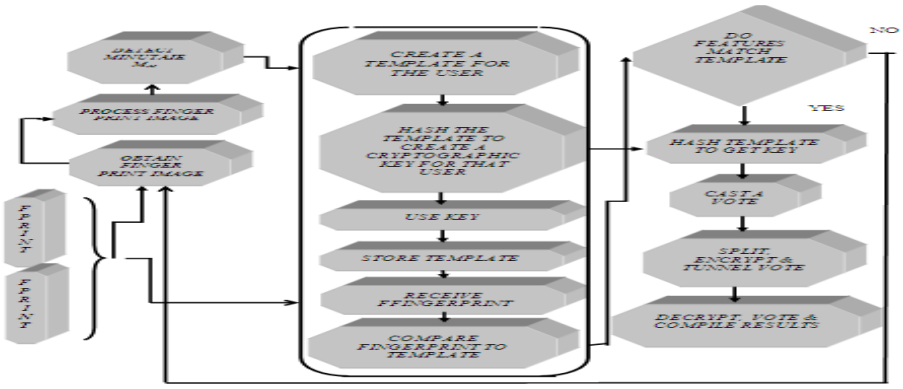

Figure 1: *A diagrammatic representation of the Biometric Key Generation (BKG) technique Adopted and Characterized in the Proposed E-Voting System [5]*.

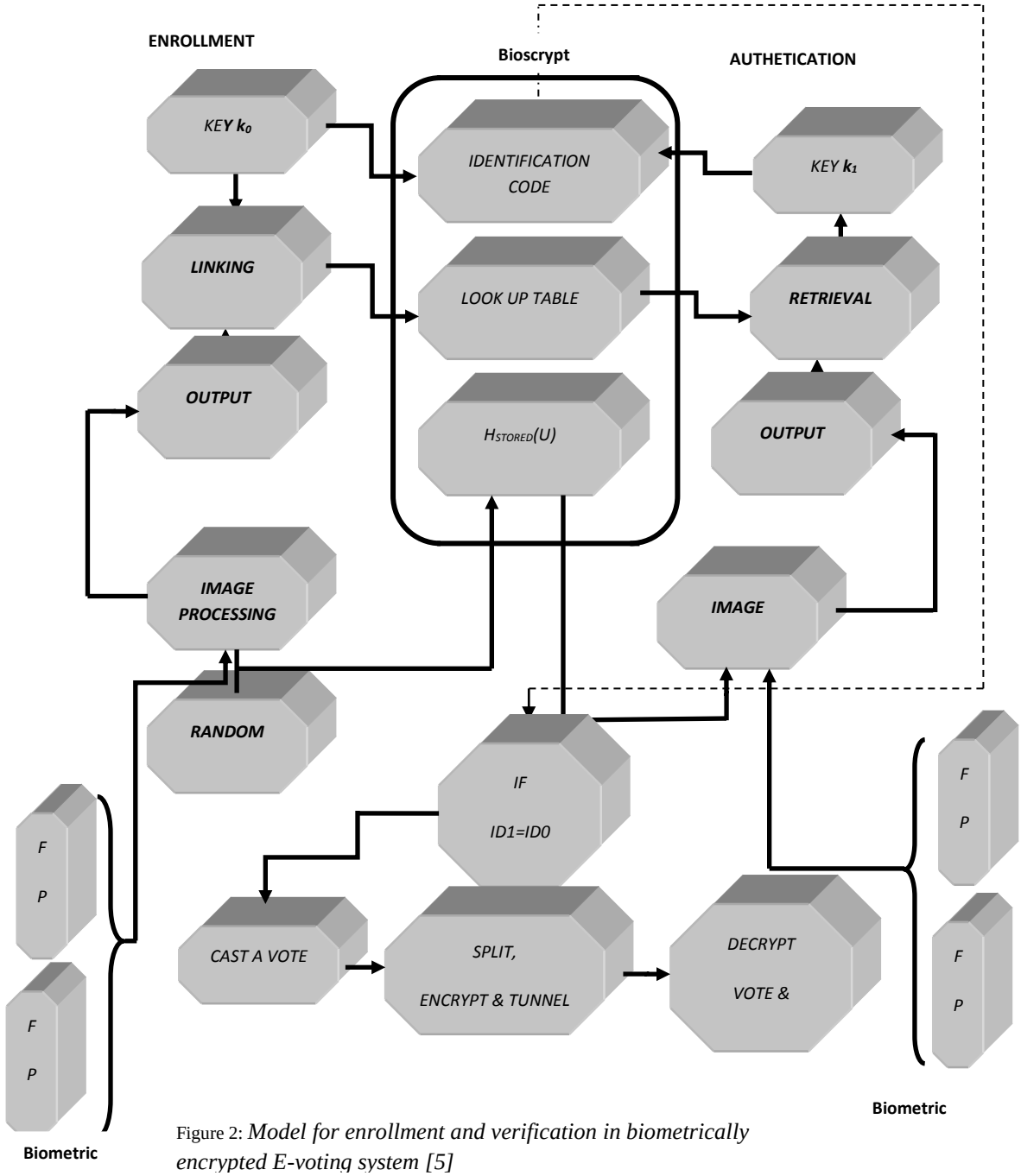

Figure 2: *Model for enrollment and verification in biometrically encrypted E-voting system [5]*

During the *verification phase*, the user touches the same sensor, generating a new fingerprint image called a *query print*. Minutia points are extracted from the query print, and the matcher module compares the query minutia set with the stored minutia templates in the enrollment database. The comparison tests whether the fingerprint received belongs to the same user as the template. If the features do not match the template, the system jumps back to obtain a new set of fingerprints. The template is again hashed to create a cryptographic

key. On correct matching of the fingerprint, the first cryptographic key used to create the template is regenerated. It is this cryptographic key obtained that now allows the verified voter, access to the e-voting system.

At enrollment, a filter function, $H(u)$, is derived from $f_0(x)$, which is a two dimensional image array (0 indicates the first measurement) [17].

Subsequently, a correlation function $c(x)$ between $f_0(x)$ and any other biometric input $f_1(x)$ obtained during verification is defined by

$$c(x) = FT^{-1}\{F_1(u)F*_0(u)\} \quad (1)$$

Which is the inverse Fourier transform of the product of the Fourier transform of a biometric input, denoted by $F1(u)$, and$F*0(u)$, where $F*0(u)$ is represented by $H(u)$. The output $c(x)$ is an array of scalar values describing the degree of similarity. To provide distortion tolerance, the filter function is calculated as a set of T training images $\{f_0^1(x), f_0^2(x) \ldots, f_0^T(x)\}$. The output pattern of $f_0^T(x)$ is denoted by $c_0^T(x)$ with its Fourier transform as $F_0^T(u)h(u)$. The complex conjugate of the phase component of $H(u)$, $e^{i\phi(H(u)}$,is multiplied with a random phase-only array of the same size to create a secure filter, $H_{stored}(u)$, which is stored as part of the template while the magnitude of $H(u)$ is discarded. The output pattern $c0(x)$ is then linked with an *N-bit* cryptographic key k_0 using a linking algorithm: if the *n-th* bit of *k0*is 0 then L locations of the selected part of $c0(x)$ which are 0 are chosen and the indices of the locations are written into the *n-th* column of a look-up table which is stored as part of the template, termed Bioscrypt, (Jain et al., 2000). During linking, redundancy is added by applying a repetitive code. Standard hashing algorithm is used to compute a hash of *k0*, termed *id0* which is stored as part of the template, too. During authentication a set of biometric images of the Action Client is combined with $H_{stored}(u)$ to produce an output pattern $c1(x)$. With the use of the look-up table, an appropriate retrieval algorithm calculates an *N-bit* key *k1* extracting the constituent bits of the binarized output pattern. Finally, a hash *id1* is calculated and tested against*id0* to check the validity of *k1*.

In contrast to feature-based biometric systems, the Biometric Encryption algorithm processes the entire fingerprint image. The mechanism of correlation is used as the basis for the algorithm [18].

A summary of the algorithms for enrollment and verification is shown below;

Algorithm 1: enrollment of prospective voter [5]

Input: a set of the legitimate Action Client's fingerprint images, a randomly generated phase-only array, R(u), and an N-bit cryptographic key, **k0**. R(u) is generated using a random number generator (RNG).

Output: an identification code **id0** derived from key, **k0**.

Steps:

- *Generate random phase-only array*
- *Generate N-bit cryptographic key.*
- *Collect a set of fingerprint images* T=*n, n>6(fingerprint samples).*
- *Perform Fourier transform the fingerprint image*
- generate *an output function* $c_0(x)$ *and filter function H*stored(u) (*product of finger print and random array*)
- *store H*stored(u) *as part of Bioscrypt*
- *link c0(x) with N-bit key* k_0 *and create a look up table*
- *use* k_0 *to encrypt S-bits of H*stored(u) *to form* id_0
- *append H*stored(u) *to* id_0 *and the look up able*
- *end*

Algorithm 2: verification of prospective voter

Input: a set of the legitimate Action Client's fingerprint images. *Hstored*(u), and an output pattern, *c*1(x).

Output: an identification code **id1**derived from an N-bit cryptographic keyk_1 in which **id1**= **id0**, then **k1**= **k0**, with high probability and **k1**can be released to the system

Steps:

- *Collect a set of fingerprint images T=n, n>6(fingerprint samples).*
- *Perform Fourier transform the fingerprint image*
- *Combine the new set of fingerprints with Hstored(u) and look up table and id0 to check for the validity of N-bit key*
- *Using Hstored(u) from Bioscrypt, , c1(x) is evaluated*
- $C_1(x)$*is used to retrieve N-bit key* k_1
- *use* k_1 *to encrypt S-bits of Hstored(u) to form* id_1
- id_1 *is then compared with* id_0 *, if id1= id0, then k1= k0, with high probability and k1can be released to the system*
- *else display verification failed message*
- *end [5]*

4.0 RESULTS and ANALYSIS

The results obtained from the simulation model test bed are presented. Figure 3 clearly illustrates what happens during the authentication phase whereby this **SMARESIM** performs a mandatory check to find out if the prospective voter is eligible and has not cast a vote previously [5].

Figure 4 clearly illustrates what happens when an eligible voter casts his vote at a polling booth; the voter would get a visual notification to indicate his vote was accepted by this **SMARESIM**. Also the voting administrators at various State Collection Centers (SCC) and the National Collection Center (NCC) get to see

the results as they stream in from the various wards and State Collection Centers respectively as they are been transmitted over the VPN. The administrators at the various collection centers are equally going to undergo a verification process with the aid of a Bioscrypt Finger Print Unit (BFPU) via the Biometric Key Binding (BKB) technique as shown in Figure 3.

Figure 5 illustrates the complete compilation of election results of the sixteen political parties from the various State Collection Centers at the end of the voting process on this **SMARESIM**. As earlier highlighted, the scope of this Simulation model, effectively handles the Authentication process, Voting, Collation and Transmission of the results (we assume that the voter registration has been done).

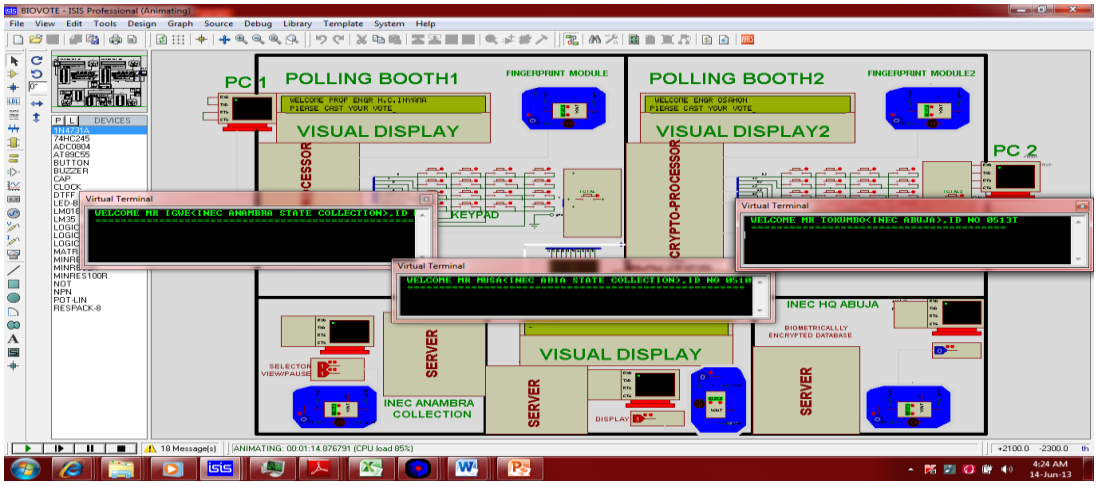

Figure 3: *Voter Authentication Interface [5]*

Figure 3 presents a snap shot of this **SMARESIM** with the administrators of the state and national collection centers already granted access with the aid of the Bioscrypt fingerprint module. It also shows two voters at different polling booths that have just been granted access to the voting machines after being verified as genuine voters who have not voted previously.

Figure 4 presents a snap shot of the **SMARESIM** with the administrators of the state and national collection centers having access to election results coming from the various polling booths (in real time) . It also shows two voters at different polling booths; one of the voters has just been granted access to vote while the other voter has cast his vote for the political party of his choice (PDP) after the authentication process [5].

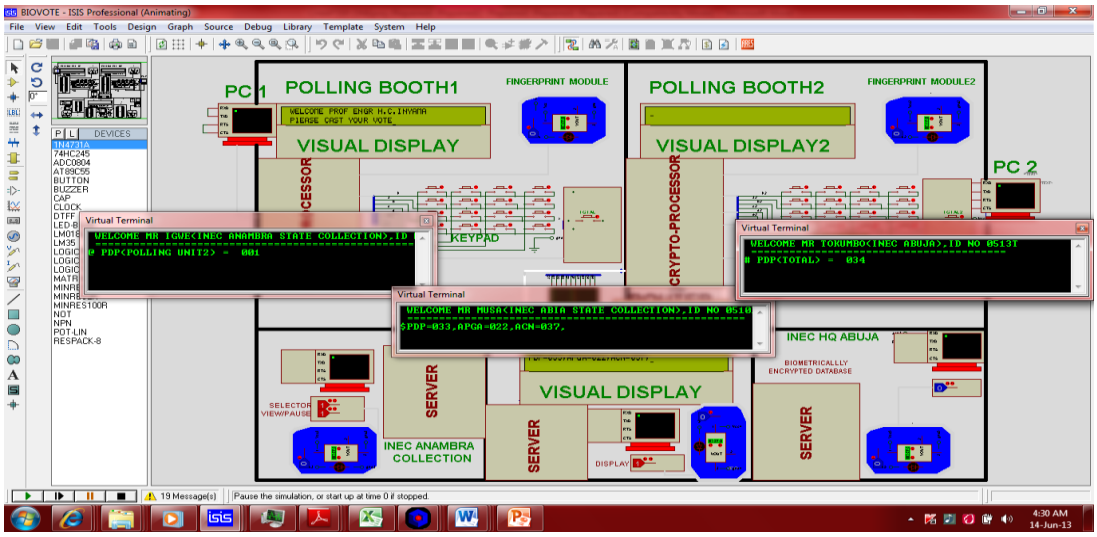

Figure 4: *Voting interface [5]*

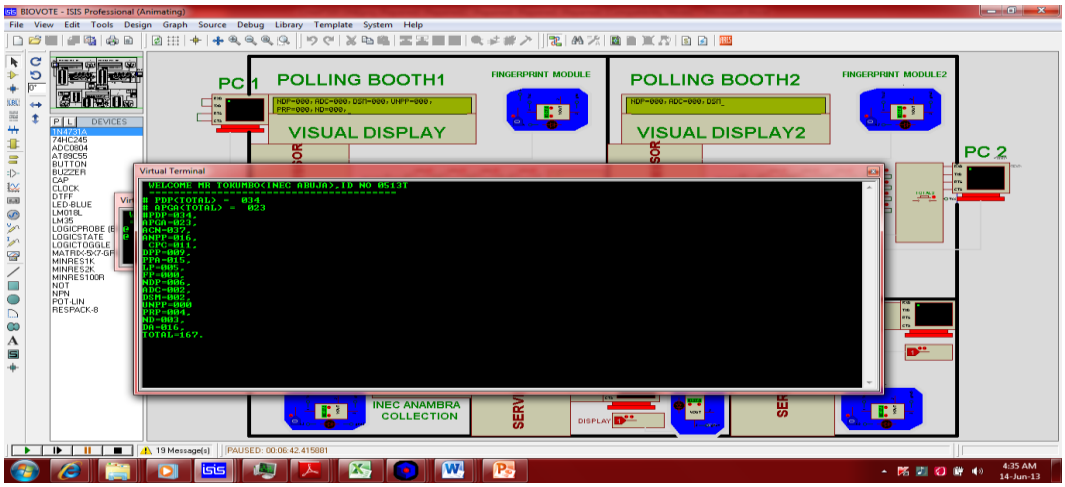

Figure 5: *Voting result collation*

Figure 5 presents a snap shot of the **SMARESIM** with the administrator of the national collection center with granted access receiving the total results of the election as soon as the time for election has elapsed (the collection is done in real time by simply pressing the control button).

CONCLUSION

The proposed scheme Self-Monitoring Analysis and Report E-voting Simulation Model (**SMARESIM**) is an efficient electronic voting scheme that provides essential security requirements and the voter's identity remains hidden. It utilizes the advantages of the bio-cryptography to make the counting of votes submit to group of authority. The secure internet voting system should not only allow all voters to verify the voting result but also avoid ballot paper issuing. With this scheme it is expected to serve as efficient and secure service.

REFERENCES

[1] Afrin, T. and Satao, K. J. (2013), "Detailed Implementation of E-Voting System for on Duty Persons using RSA Algorithm with Kerberos Concept", *International Journal of Innovative Research in Computer and Communication Engineering*, Vol.1, Issue7.

[2] Abdulhamid, A. M., Adebayo, O. S., Ugiomoh, D. O. and AbdulMalik, M. D. (2013), "The Design and Development of Real-Time E-Voting System in Nigeria with Emphasis on Security and Result Veracity", *International Journal of Computer Network and Information Security*, Vol. 5, Pp. 9-18.

[3] Olaniyi, O. M., Arulogun, O. T., Olusayo, O. E. and Olusola, O. O. (2013), "A Survey of Cryptographic and Stegano-Cryptographic Models for Secure Electronic Voting System", *Covenant Journal of Informatics and Communication Technology (CJICT)*, **Vol. 1, No. 2**, Pp. 54-78.

[4] Sodiya, A., Onashoga, S. and Adelani, D. I. (2011), "Secure E-Voting Architecture", *Proceedings of Eighth International Conference on Information Technology*: New Generations, IEEE Computer Society, Pp. 342-347.

[5] Nwose, F.C. (2016), "Development and Implementation of Bio-Cryptographic Protocols for Enhanced E-Voting System", *M.Eng Dissertation submitted to SPGS COOU*, Uli.

[6] Gritzalis, D. (2003), "Secure Electronic Voting". *Boston, Mass: Kluwer Academic.*

[7] Chaum, D. (1981), "Untraceable Electronic Mail, Return Address and Digital Pseudonyms", *Communications of the ACM*, **24,** Pp. 84-88

[8] Choonsik, P., Kazutomo, I. and Kaoru, K. (2003), "All/Nothing Election Scheme and Anonymous Channel". EUROCRYPT '93, *Pre-proceedings, Lofthus, May*, Pp.97-112.

[9] Masayuki, A. (1998). "Universally Verifiable Mix-net with Verification Work Independent of the Number of Mix-servers". *Proceedings of EUROCRYPT 1998. Springer-Verlag, LNCS 1403,* Pp. 437–447.

[10] Jakobsson, M., Juels, A. and Ronald, L. (1999), "Making Mix-nets Robust for Electronic Voting by Randomized Partial Checking", *Proceeding of USENIX '02,* Pp. 339–353.

[11] Neff, A. (2001), "A Verifiable Secret Shuffle and its Application to E-voting". *Proceedings of the ACM Conference on Computer and Communications Security;* Pp. 16–25.

[12] Acquisti, A. (2002), "A User-Centric MIX-Net Protocol to Protect Privacy", *Proceedings of the Workshop on Privacy in Digital Environments: Empowering Users.*

[13] Chaum, D., Peter, Y., Ryan, A. and Steve, S. (2005), "A Practical Voter-Verifiable Election Scheme". *S. De Capitani di Vimercati et al. (Eds.): ESORICS 2005, LNCS 3679*, Pp. 118–139.

[14] Ryan, P. and Schneider, S. (2006), "*Prêt a voter with Re-encryption Mixes*". *ESORICS 2006. Lecture notes in Computer Science*, **4189**: Pp. 13–26.

[15] Benaloh, J. and Tuinstra, D. (1994), "Receipt-free Secret-Ballot Elections," *Proceedings of the 26th ACM Symposium on the Theory of Computing*, Pp. 544-553.

[16] Nathan, D. (2014), Scholars Journal of Engineering and Technology (SJET) 2014; **2(6B):** Pp. 874-881.

[17] Jain, A. K., Prabhakar S., Hong L., and Pankanti, S, *(2000), "Filterbank-based Fingerprint Matching." IEEE* Trans on Image Processing, **9(5)**: Pp. 846-859.

[18] Kothari, C. R. (2004), Research Methodology: Methods and Techniques. *New Age International (P) Ltd., New Delhi*