American Journal of Engineering Research (AJER)
e-ISSN : 2320-0847 p-ISSN : 2320-0936
Volume-02, Issue-10, pp-180-190
www.ajer.org

Research Paper Open Access

Enhancing E-Voting Systems By Leveraging Biometric Key Generation (Bkg)

*V. C. Ossai[1], I.C. Okoro, E.O. Alagbu, A.O. Agbonghae and I.N. Okafor
[1]*Electronics Development Institute, Awka. National Agency for Science and Engineering Infrastructure.*

Abstract: - The adoption of e-voting methods in electioneering processes will effectively reduce cost as well as enhance election activities. What makes an e-voting model reliable and acceptable is its ability to properly authenticate voters and provide a secure means through which a voter can express his/her franchise. This paper therefore proposes a design of an e-voting system that leverages a Biometric Encryption scheme known as Biometric key Generation (BKG) which is a secured strategy that entails using of biometrics to generate secure cryptographic keys. The main objective of this research is to improve on the already existing E-voting systems adopting a secured bio-cryptographic technique vis Biometric key Generation (BKG) as well as using a secure transmission channel for confidential datasets of a voting process. This work develops a simulation model of an E-voting system which adopts relevant algorithms with emphasis on biometric key generation schemes. The simulation of a prototype model of the electronic voting system is developed using Proteus 7.6 application software. The prototype model would consist of electronic kiosk polling booths that are all networked to the state electoral collection center and collection centers that are networked to the national electoral collection center via a VPN backbone. The proposed e-voting system uses a Virtual Private Network (VPN) as the means of communication between the various polling booths and collection points. The results of validation show that the proposed model facilitates the adoption of E-governance in the developing countries.

***Keywords*: -** *Biometric Key Generation, Cryptography, E-voting Booths, Privacy, Security.*

I. INTRODUCTION

Election is a process by which members of an organization or a society select people to hold positions of authority [1].

The term "e-voting" encompasses all voting techniques involving the use of electronic voting equipment including voting over the internet, using booths in polling stations (e-booths) and sometimes even from remote sites (e.g. via SMS). According to [2] e-voting is any voting method where the voter's intention is expressed or collected by electronic means. The following e-voting approaches have being identified by this literature viz;

- Kiosk voting (e-booths)
- Remote electronic voting
- Internet voting (I-voting)

Basically, this work uses the term e-voting with the specific emphasis on kiosk voting (e-booth) over the internet (through a secured public network infrastructure). An Electronic Voting System has as its main components [2]:

i. The Electronic Voters Register.
ii. Authentication- which is done prior to balloting.
iii. Voting, Collation and Transmission.

Owing to the fact that there are a lot of vulnerabilities in the current voting schemes currently used in e-voting systems, there is a need to develop a secure, reliable and trusted means of voting so as to reduce the vulnerabilities associated with voting, increase flexibility and security as well as reducing the cost of elections.

In this work, the use of some of Direct Recording Balloting Machines (DREs) connected over a VPN (secure internet facility) is adopted and characterized. This will completely eliminate the cost associated with the printing of several million ballot papers.

This work leverages Biometric Key Generation (BKG) technique and a secured communication channel to transmit voting results which is being characterized in this simulation model. This would help reduce to the barest minimum the fraud and irregularities associated with elections. Worthy of note is that BKG has not yet been adopted in E-voting systems.

II. LITERATURE REVIEW

2.1 Related Works

The work in [3] presented e-voting Schemes and explained that e-voting is a promising application of cryptography, which can have positive impact on democratic process. The work discussed cryptographic aspects of constructing e-voting schemes and tried to generate a preliminary framework on the notion of choice. The author added that on the internet, implementing cryptographic protocols like digital encryption and signature has been widely accepted.

The authors in [4] described the theory behind a practical voting scheme based on homomorphic encryption which entails the application of arithmetic operation like addition to encrypted numbers without previously decrypting them. The resulting encrypted sum can then be revealed with a private decryption key. The homomorphic encryption scheme ensures that individual numbers cannot be decrypted with the private decryption key alone. The major drawback is that homomorphic approaches do not allow complex multi-candidate elections. Most of them are restricted to simple yes/no votes which are easy to count. The work presented the most important goals for electronic voting schemes viz: Privacy, Robustness, Universal verifiability and freeness.

Other Fundamental approaches to electronic voting are known in the literature include the use of blind signatures and anonymous channels [5]

In Anonymous channels on the other hand messages to be sent anonymously, i.e. such that a recipient cannot trace the received messages back to the senders. The most prominent technique for building anonymous channels is mix nets and onions [6], [7]. They are comprised of a collection of anonymization servers whose task is to shuffle a given input sequence of encrypted messages. To ensure that mix-servers or onion routers do not drop or substitute messages, it is necessary that the servers provide proofs of correct operation. The resulting anonymous channel is then called verifiable. Although most existing verifiable anonymous channels are relatively inefficient, progress has been reported recently.

The authors in [8] propose a secure electronic voting protocol that is suitable for large scale voting over the Internet. In their work, the protocol allows a voter to cast his or her ballot anonymously by exchanging untraceable yet authentic messages. The protocol ensures that (i) only eligible voters are able to cast votes, (ii) a voter is able to cast only one vote, (iii) a voter is able to verify that his or her vote is counted in the final tally, (iv) nobody, other than the voter, is able to link a cast vote with a voter, and (v) if a voter decides not to cast a vote, nobody is able to cast a fraudulent vote in place of the voter. The following assumptions were made in the context of this protocol viz [8]:

i. Hard-to-invert permutations
ii. Blind Signature on messages
iii. Secure Transit

In their final analysis, the work concludes that the protocol is suitable for large scale voting over the Internet and that satisfies the core properties of secure voting systems – namely accuracy, democracy, privacy and verifiability.

The idea of blind signatures is to apply a blinding function to a message before sending it to a signing party. Based on a simple RSA-like scheme, this can be done such that the blinding function can be inverted on the blinded signature to finally obtain a regular RSA-based digital signature. At the end of this process, in which the content of the message has been entirely disguised from the signer, the signature is ordinarily verifiable using the signer's public key [4]. The idea in such a scheme is that a voter prepares a ballot in clear text, i.e. a message stating for whom he votes [4]. He then interacts with an authority that can verify that he is eligible to vote and has not already voted. If this is the case, the authority issues a blind signature on the ballot. Informally, this means that the voter obtains the authority's digital signature on the ballot, without the authority learning any information about the contents of the ballot. On the other hand, a voter cannot obtain such a signature without interacting with the authority, and is therefore prevented from voting several times [4]. A major drawback of the protocol is that voters need to be active in at least two phases to ensure verifiability and fairness, which restricts its usability intrinsically.

The work in [9] presents an evaluation of e-Voting systems equipped with voter-Verified Paper Records. The work stated that owing to the need to increase public confidence, various states are increasingly considering electronic voting systems that provide voter verified paper records. In the work, an analysis and evaluation of New Jersey's criteria against several different e-voting machine types revealed potential threats and possible solutions on privacy, security, and performance issues.

The authors in [10], observed that the traditional methods of electioneering is characterized by long period of preparation, fake voting, faulty voting, mistakes made in counting the votes, long period of counting and high cost of voting process, in order to avoid these limitations; the system applied biometric fingerprint authentication. In the work, a biometric based e-voting system is designed for providing a secure election on electronic environment for the electors. Technologies such as XSL language which is compatible with Asp.Net, Framework 2.0, Java Script, Xml is used but can be deployed in Microsoft Windows operating system [10]. Again, the, biometric based software libraries are also used for integrating the fingerprint control to the system. In this regard, the elector identification system is programmed with C# language and equipped with an optical fingerprint scanner SDK (Suprema Inc®) to accept a scan, recognize the elector, and open the correct elector record in the database and verify system (Suprema, 2010). This module uses a dynamic link library (DLL) that can be displayed in a web application. Attacks are indispensible in biometric based systems, hence besides privacy issues, the major identified limitations of the works discussed above is presented. Applying texture-based feature extraction techniques to fingerprint authentication is very vulnerable. In this case, its security properties considering biometric integration is very vulnerable as attackers, Trojan horses, etc. Biometric technologies may add a new level of authentication and identification to applications, but are not, however, without their risks and challenges. There are important technological challenges such as accuracy, reliability, data security, user acceptance, cost, and interoperability, as well as challenges associated with ensuring effective privacy protections. Some common security vulnerabilities of biometric systems include: spoofing; replay attacks; substitution attacks; tampering; masquerade attacks, trojan horse attacks and overriding Yes/No response [11]. All feature extraction e-voting models are weak. A traditional biometric system will store the original templates in a database, for use in authentication/identification comparisons. If an attacker can gain access to the database (despite its security measures) then all template data (X) can be compromised [11].

III. DESIGN METHODOLOGY

In this research, an acceptability Index score was obtained from primary data sources (from local electoral regulatory bodies). Consequently PROTEUS ISIS version 7.6 was used to develop a real time simulation that characterizes the voting scenario using program description language which later was coded with Assembly language. The implementation was characterized with various components to realize the expected simulation behaviour. Also, the control program of the chips was encrypted. The algorithm was captured in the codes and simulated modules/classes include: the Fingerprints Processing Unit (FPU), the Remote Polling Booths (RPB), State Collection Centers (SCC) and the National Collection Center (NCC), all linked via a VPN communication backbone. The methodology used here has embedded in it a certain degree of gate level oriented design in the sense that gate level components are logically connected together and used to characterize various components in this system and programmable VLSI (Very Large Scale Integration) techniques (due to the fact that very complex designs where embedded on chips throughout this design). Also programmable microcontroller chips were embedded in this design to serve as the CPUs of the various blocks in the model, hence conceptualized as *HYBRID MODELING AND SIMULATION METHODOLOGY*. All the logical components characterized or modeled to describe the real life scenarios. After the configurations, the model was run in a simulation environment depicting a contextual voting scenario.

3.1 Multi-Protocol Label Switch -Open Virtual Private Network

This work identifies MPLS-VPN as an important solution to security threats surrounding the use of public networks. It offers a secure network connection between a sender and a receiver over a public non- secure network. A VPN transforms the characteristics of a public network into those of a private secure network and provides the means to securely transmit data between two networked devices over an insecure transport medium [12]. A VPN creates a secure virtual links between their co-operate headquarters and remote sites via the internet. When compared to other solutions e.g. leased lines, VPNs are relatively inexpensive.

In the characterization of the proposed e-voting system, the polling booths at the various wards would be characterized as the remote INEC offices, the state INEC collection centers would be characterized as the branch offices while the INEC headquarters is characterized as the co-operate office.

VPN makes use of many security mechanisms e.g. encryption, the use of digital signature to ensure that data cannot be modified without detection. It uses tunneling process to transport the encrypted data over the internet. Tunneling is mechanism for encapsulating one protocol in another protocol [12]. The VPN architecture consists of the VPN client, Network Access Server (NAS), A Tunnel terminating device (VPN sever), and a VPN protocol.

3.1.1 Open VPN Solution

OpenVPN is a VPN solution adopted in this work. Characterization of tunneling, encapsulation and transfer of data is also enshrined in the simulation of this work. The OpenVPN makes use of VNI (Virtual

Network Interface) for capturing in coming traffic before encryption and sending outgoing traffic after decryption. The VNI appears as the actual network interface to all applications and users.
Essentially, an OpenVPN performs the following viz:

1) Receives packets of data (votes) from the polling booths using after receiving the packets, it compresses the packets.
2) After compression, it encrypts the packets.
3) It tunnels the packet to the receiving end.
4) On receiving the encrypted traffic, the OpenVPN performs the reverse of cryptographic operations to verify its integrity and authenticity.
5) It then decompresses the packets.
6) The decompressed data is passed by the VNI to the user interface.

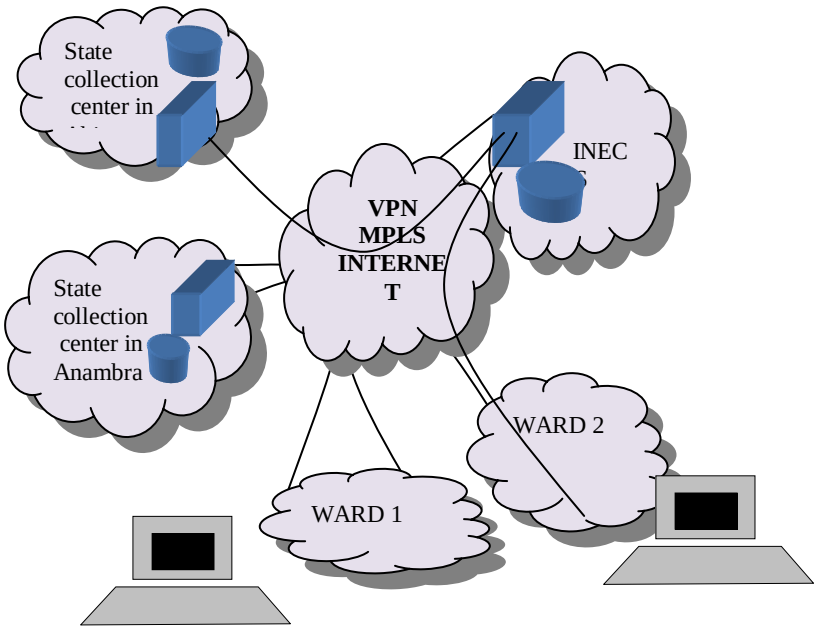


Figure 1: The Communication link diagram of MPLS -VPN backbone for the proposed E-voting system

Fig 1 shows the flow diagram of information between the various polling booths in different wards, the state and national collection centers as characterized in this work

3.2 Biometric Encryption (BE) Adopted in the Proposed Model

The concept of Biometric Encryption (BE) was first introduced in the mid-'90s by [13] and is adopted in this proposed E-voting model. BE is a process that securely binds a key to, or extracts a key from, a biometric, such that neither the key nor the biometric can be retrieved from the "helper data" (also called a "private template") created by this process and stored by the application, except upon presentation of the correct live biometric sample for verification. In essence, the key is "encrypted" with the biometric — a 'fuzzy' process due to the natural variability of biometric samples. It securely binds a digital key to a biometric or generates a digital key from the biometric, so that no biometric image or template is stored. What is stored is the BE template otherwise known as a ''bio-metrically encrypted key'' or ''helper data''. Neither the digital key nor the biometric can be retrieved from the stored BE template which stored [14].

3.2.1 Adopted BE Operational Models

A system and method for generating an encryption key using physical characteristics of a biometric sample is adopted. In this method for generating key using biometric features, the biometric feature from a sample is analyzed to generate a feature vector. After discretizing the features, the resultant feature vector is translated into a bit vector. The bit vector is the secure biometric key that results from the biometrics. The secure biometric key is used to generate at least one cryptographic key. A similar process is used to access the cryptographic key secured by the secure biometric key [15]. If the access biometric key matches the secure biometric key, the cryptographic key is revealed and access is allowed providing a method and apparatus for generating cryptographic keys using biometric data [15]. This technique adopted by the proposed E-Voting

system provides a method for generating a cryptographic key using biometric data. The method includes segmenting an image of a biometric into at least two quadrants, detecting at least one biometric feature associated with the biometric, determining which of the at least two quadrants the feature is located in, generating a subkey value from a quadrant location value derived from the quadrant the at least one feature is located in and a biometric feature type, and generating a cryptographic biometric key by concatenating the subkey value with a predetermined number of other subkey values derived from other quadrant location values and other feature types associated with other biometric features of the biometric [15]. These steps are characterized in the Simulation for the proposed E-Voting system.

3.2.2 Proposed E-Voting Model

An innovative technique for securing a key using a biometrics i.e. biometric key generator is adopted in this E-Voting system. The digital cryptographic key is generated from a biometric trait during enrollment, and this key is later regenerated using the same biometric trait during verification.

A fingerprint images are received from the user. The fingerprints are protected with a time and date stamp which is included in the encrypted fingerprint to assure that the fingerprint was not generated previously and resent. If the fingerprint is encrypted it is decrypted a digital fingerprint image is generated. The features of the fingerprint are then extracted. These features may include one or more of the following: minutiae, including location and orientation; spatial frequency; curvature; ridge count; ridge distance/curvature between points; relation to global features; code words generated by vector quantization to encode subunit spatial characteristics; etc.

A template is created for the user. A template includes at least some of the features extracted from the fingerprint. After the features are extracted, they may be jiggled slightly, to generate different hashes. That is, the features may be 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). The initial features extracted are an initial condition for the cryptographic key. The hash generated from the initial features is used to search the local key space.

The template is hashed. This hash is the cryptographic key. This cryptographic key is identified with the specific fingerprint, and thus with a specific user. For this public key encryption, a private key is generated based on the hash. A public key is generated to correspond to the cryptographic key. Methods of generating a public key which corresponds to a private key include Standard Hashing Algorithms (SHA). Public key/private key pairs are used to authenticate documents, encrypt documents, etc.

The cryptographic key is used. The cryptographic key is generated in order to do something specific. The template is stored. The cryptographic key itself is not stored anywhere on the system. The template is stored with the file for which it was used. The initial use of the key is now complete. A file may have been encrypted. Such a file may be stored on the system, sent, or otherwise disposed of by the user. If the user wishes to decrypt an encrypted document, or otherwise use the cryptographic key again.

The fingerprint is received from the user. The features of the fingerprint are extracted.

The fingerprint features, newly extracted, are compared to the template. The template includes some or all of the features previously extracted from the fingerprint. The comparison tests whether the fingerprint received belongs to the same user as the template.

A comparison is done to see if the features match the template. If the features do not match the template, it jumps back to obtain a new set of fingerprints. The template is again hashed to create a cryptographic key. Since the template was used to generate the first cryptographic key, the same key is generated. The key can then be used in the above described manner. . It is this cryptographic key obtained that now allows the verified voter, access to the e-voting system.

After the voter cast his vote for the party of his choice, the votes is split into packets of data, which is encapsulated another packet with headers and then tunneled over a secured network facility (a VPN for this model). At the receiving end (collection centers), the encapsulated packets is de-encapsulated (the encapsulation and de-encapsulation is done via AES 128 encryption standards). The votes are now tallied at the respective collection centers and the final tally is done at the INEC national headquarters in Abuja.

Fig 2 which shows an analytical representation of the Biometric Key Generation (BKG) technique adopted and characterized in the proposed E-Voting system**.**

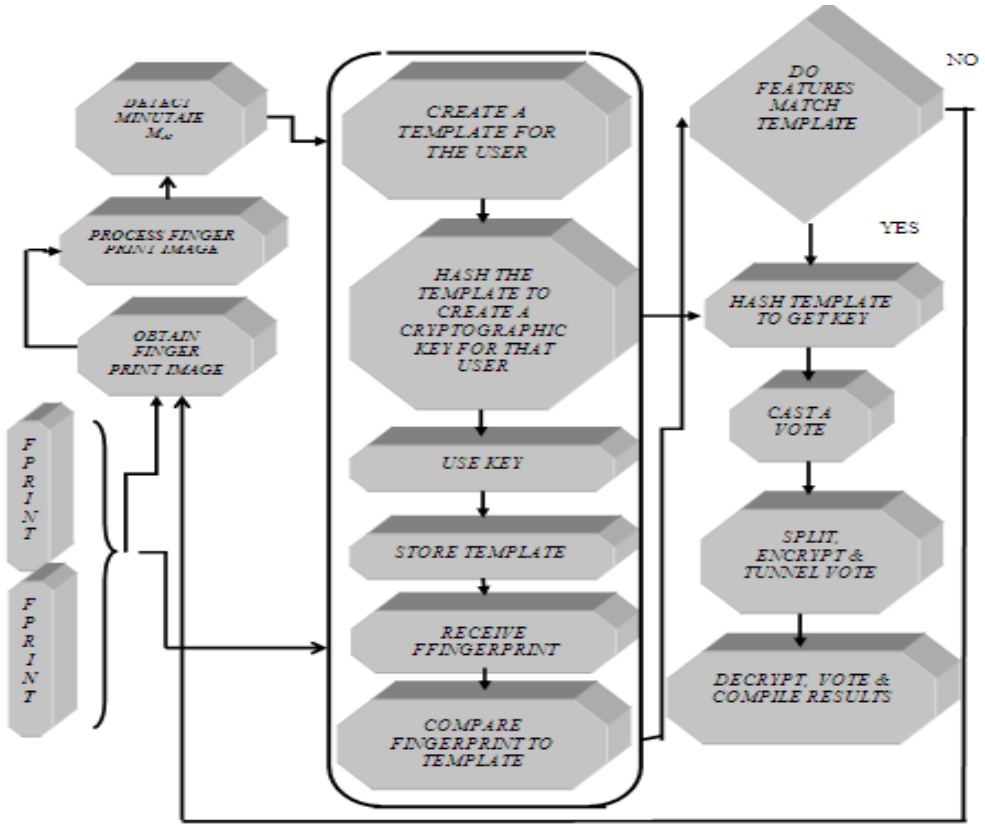


Figure 2 an analytical model for enrollment and verification in a biometrically encrypted E-voting system vis BKG.

3.3 Modeling Assumptions

In this research, the proposed E-voting system is assumed to fit into the Nigerian environment which has 36 states as independent remote blocks. The BKG algorithm, we assume that multiple fingerprint samples F_0 are collected during the enrollment exercise and processed. The fingerprint samples collected from the individuals during the enrollment or registration process are processed and from the processed fingerprints, cryptographic keys *Nk* which are going to be used to encrypt the votes would be generated. *Nk* would be regenerated on representation of the same fingerprint sample *F1* of which $F1 \approx F0'$.

In this security and privacy based algorithm for the proposed E-voting system, the communication link used between the various polling modules {*pm1, pm2,……, pmn*} and collection points {*cp1,cp2,…Σcp*} in this model is the Open VPN backbone given as O*VPNx* where encrypted data (individual votes) *En* is tunneled via a secure and private network *VPNx* that is built on top of existing physical network in context of VPN Multi-Protocol Label Switching(MPLS).

It is assumed that *VPNx* maintains data privacy through the use of a tunneling protocol, AES 128 encryption protocol and other security procedures.

This work assumes the use of two most common types of VPN setups; Remote access VPN and site-to-site VPN. The Remote Access VPN configuration is used to allow the individual polling booths located at remote sites to be able to communicate in a secure manner with the state collection centers while the site-to-site VPN allows for creation of dedicated, secure connections between the various INEC state collection centers and the national collection center across the open Internet or public connection.

Fig 3 gives a block diagram representation of the flow of information from the Remote Polling booth units (RPBU) to the INEC State Collection Centers (SCC) and the INEC National Collection Center (NCC) i.e. the end to end flow of information in the proposed E-voting system.

Each polling booth has these modules:

- Function keypad buttons
- Visual Display Unit
- The finger print module
- Secure Crypto-processor:
- Virtual Network Interface.

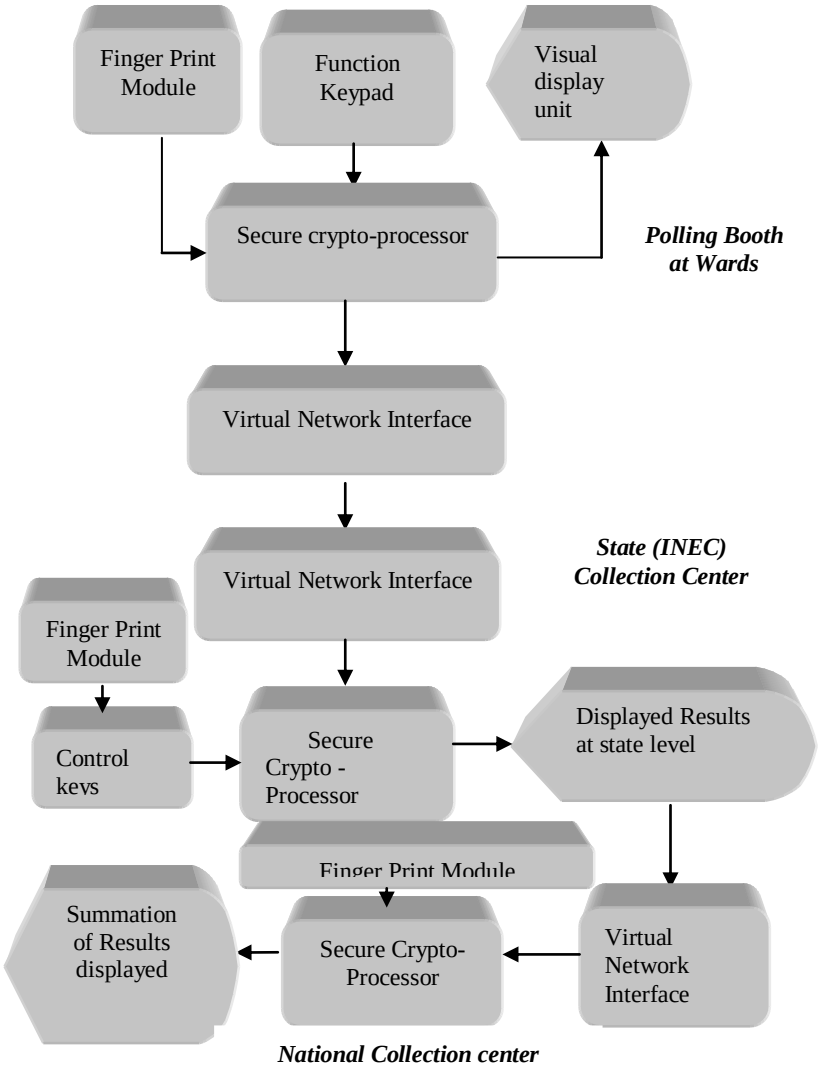


Figure 3: Flow diagram for the proposed E-voting

Each states collection centers and the national collection center will have the following:

- Control keypad
- The finger print module
- Secure Crypto-processor
- Virtual Network Interface

IV. IMPLEMENTATION& EVALUATION

4.1 Simulation Design with Proteus 7.6

In the proposed the proposed E-voting system, Proteus 7.6 ISIS was used to characterize the individual E-polling booths and collection centers. It provides the platform through which the various voting processes were characterized. Typical applications of Proteus 7.6 ISIS include standard-based electronic and logical component feature characterization. The Proteus 7.6 ISIS environment is organized into; probe/simulation environment, component editor, sub circuit editor with a comprehensive collection of work tools that were used to characterize the proposed E-voting system The Proteus 7.6 ISIS environment provides several modules for the simulation comprising a vast enterprise of digital and analog tools which with friendly graphical user interface that can be manipulated to achieve desired results.

3.3 Program Description Language (PDL) for the proposed E-voting system that leverages BKG

A) Polling booths PDL

START

Generate Hashed Key from Finger Print

IF Hashed Finger Print = 1 THEN

DO UNTIL Keypad = 1

Display Chosen Party

```
                    Transmit Vote
                END DO
        ELSE
Display "Voter not allowed"
        END IF
END
```

B) Collection Centers PDL

```
START
        Generate Hashed Key from Finger Print
        IF Hashed Finger Print = 1 THEN

                DO UNTIL Control Keypad = 1
                        Select Polling booth
                        Tally Votes
                END DO
        ELSE
                Do not grant access
        END IF
END
```

The PDL shown above is a summary of the lengthy code used in the characterization of the proposed E-Voting system that leverages BKG.

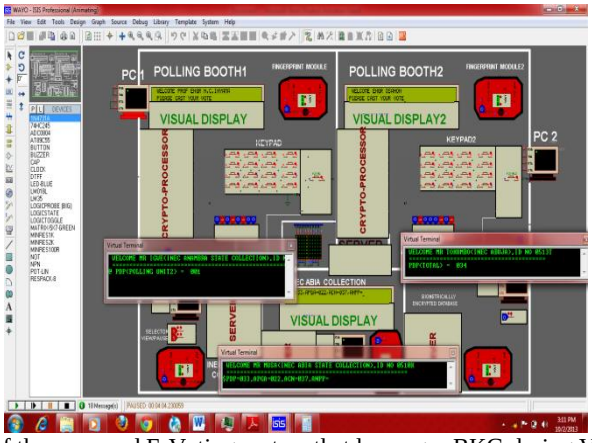


Figure 4: Proteus snapshots of the proposed E-Voting system that leverages BKG during Voting and Collection of total results

Fig 4 presents a Proteus simulation snapshot of proposed E-voting system with the administrators of the state and national collection centers having access to election results as the coming from the various polling booths. It also shows two voters at different polling booths. An MPLS-VPN backbone for the proposed E-Voting system that leverages BKG was characterized based on the parameters in Table 1.

OPNET modeler generates Trace files which are event scripts generated by the OPNET engine after a successful compilation. The OPNET modeler has object palettes with block sets that are configurable with real time or production values. It is these values fed into the OPNET engine that was used to characterize and configure the VPN communication link and it is on that basis that the graphs in fig 7 a-d where generated

4.3 Results and Analysis

The results obtained from the simulation model test bed are presented. The tallied election results are illustrated in pictorial capture on Proteus in the figure 5. The results were obtained from the proposed E-voting system. OPNET was used to evaluate the communication metrics; latency, throughput, stability margin and resource utilization.

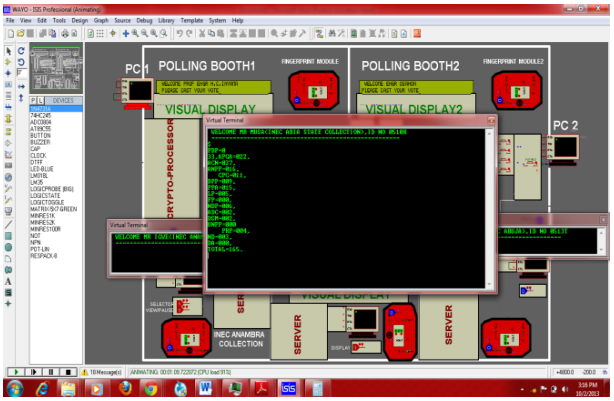


Figure 5 Proteus snapshot capture of proposed E-Voting system that leverages BKG at the national collection center displaying total results on Proteus 7.6

4.4 Validation of Model's Communication Link

For the purpose of validation of the proposed E-voting system communication link, OPNET modeler was used to validate the traffic engineering in the system. OPNET was used to evaluate the end to end latency between the polling modules and the collection centers, its throughput and its network resource utilization. It is seen from the graphs that the VPNMPLS communication backbone for the proposed E-voting system would have low end to end latency, high throughput and efficient resource utilization considering the design layout for deployment of the proposed E-voting system

Table 1: VPN-MPLS Parameters

LDP Configurations	Values
Status	Enabled
No. of Tunnel Sources with Names	[2]-Anambra Polling Booth 1&2
No. of Destination centers with Name	[1]-Headquarter.Network Server
Encryption delay	0.05sec
Decryption delay	0.05sec
Advertisement Policy	No Delay
Signaling DSCP	CS6/NC1
Reoptimization Timer(sec)	3600
Delay (sec)	20
Retry Timer (sec)	120
Propagation TTL	Enabled
Traffic Engineering	BGP
Fast Reroute Status	LSP Config
Revert Timer (Sec)	LSP Config
Label Space Allocation	Global GLA
CSPF Optimization Metric	TE Link Cost
Number of Shortest path	5

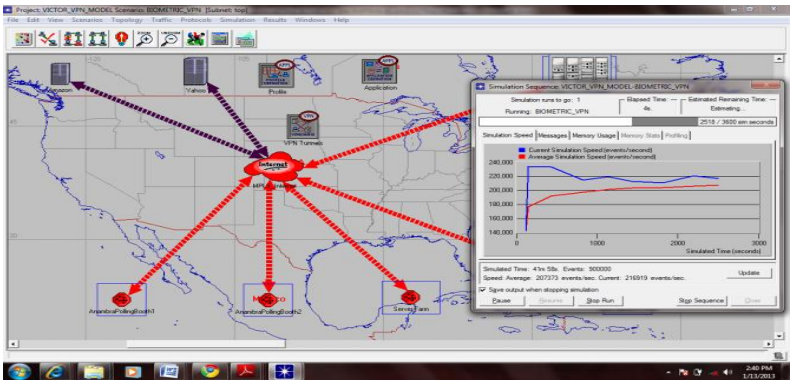


Figure 6: Snapshots capture of the OPNET modeler, showing how tunnels are created from end to end links in the MPLS VPN communication channel.

4.5 Discussion of Results

OPNET was be used to evaluate the end to end latency between the polling modules and the collection centers, its throughput and its network resource utilization. This formed the basis for validation of the proposed E-Voting model that leverages BKG.

It is seen from the graphs in fig 7a, 7b, 7c; the MPLSVPN communication backbone for the proposed E-voting system had high throughput, low end to end latency, and efficient resource utilization considering the design layout for deployment of the proposed E-voting system.

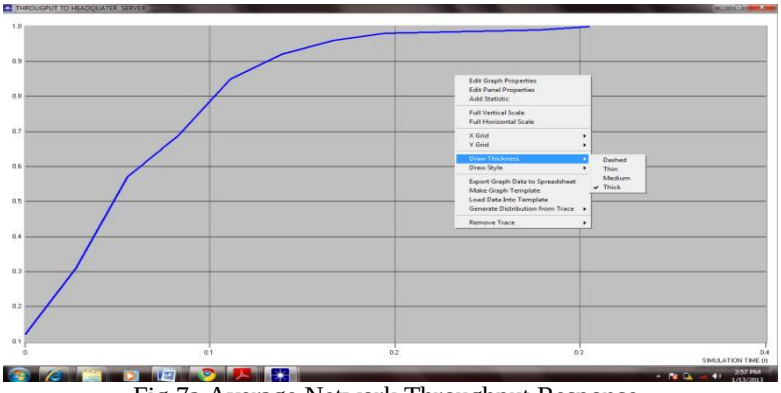


Fig 7a Average Network Throughput Response

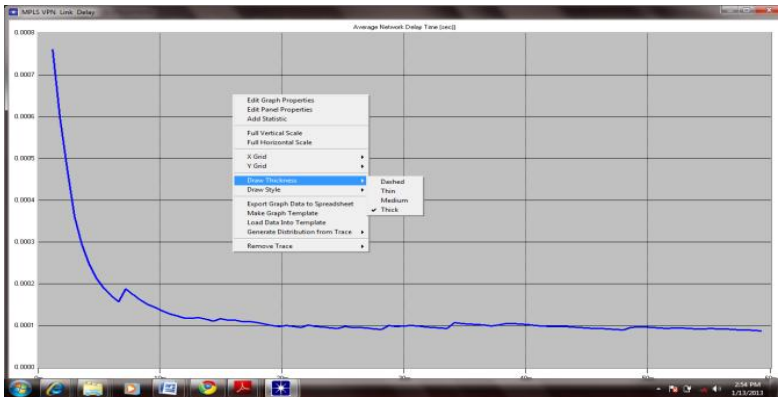


Fig 7b Average Network Delay Response

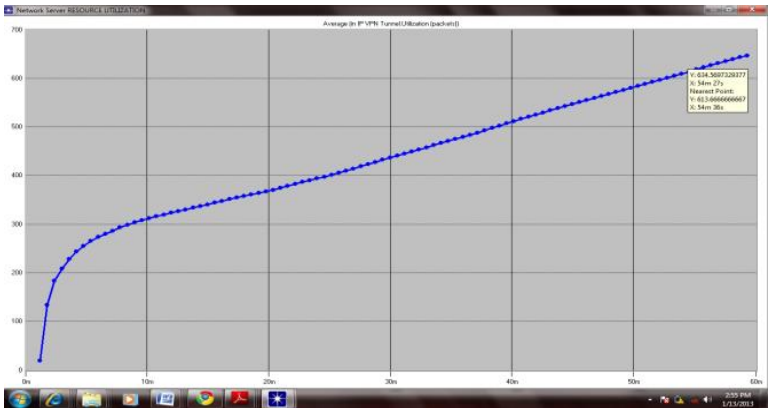


Fig 7c Average Resource Utilization

V. CONCLUSIONS

A simulation model of an e-voting system leveraging on Biometric Encryption viz Biometric Key Generation (BKG) technique for the proposed E-Voting system has been adopted and characterized. An MPLS VPN backbone as its communication link has been successfully adopted and characterized. The communication link has also been validated using metrics like end to end latency, Throughput, Network Stability and Tunnel resource utilization. Worthy of mention is the fact that Biometric Key Generation (BKG) technique has not yet been adopted in any E-voting system.

VI. REFERENCES

[1] Shane, P. (2004) Democracy Online: The Prospects for Political Renewal through the Internet. New York: Routledge

[2] Cramer, R. Franklin M. Schoenmakers B. and Yung M. (2006) Multi-authority secret ballot elections with linear work. *In: Advances in Cryptology,EUROCRYPT'96, Lecture Notes in Computer Science*, pp.72-83.

[3] Oleg Murk,Electronic Voting Schemes, M.Sc term paper,2000

[4] Ivan Damgard, Jens Groth and Gorm Salomonsen, The Theory and Implementation of an Electronic,Voting System, July 31, 2002. Fujioka, T. Okamoto & K. Otha: A practical secret voting scheme for large scale elections, Advances in Cryptology - AusCrypt '92, pp.244-251.

[5] Ohkubo and Abe: A Length-Invariant Hybrid Mix Proceedings of Asia Crypt 00, Springer Verlag LNCS.

[6] Abe: Universally verifiable MIX net with verification work independent of the number of MIX centers; proceedings of Euro Crypt 98, Springer Verlag LNCS.

[7] Indrajit Ray, Indrakshi Ray, Natarajan Narasimhamurthi, ―An Anonymous Electronic Voting Protocol for Voting Over The Internet‖.

[8] www.computer.org/security: Evaluating Electronic Voting Systems Equipped with Voter-Verified Paper Records. IEEE Security & Privacy, 2008.

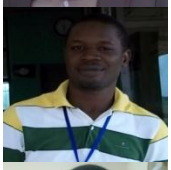
[9] Adem Alpaslan ALTUN and Metin BĐLGĐN, ― Web based secure e-voting system with fingerprint Authentication‖ In Scientific Research and Essays Vol. 6(12), pp. 2494-2500, 18 June, 2011

[10] Available online at http://www.academicjournals.org/SRE.

[11] J.L, Wayman, ―fundamentals of biometric authentication technologies‖ *Int. Image graphics*, vol.1, no.1, pp. 93-113, 2001.
[12] Cranor L. and Cytron R. (2007) Sensus: a security-conscious electronic polling system for the Internet. *In: Proceedings of the Thirtieth Hawaii International Conference on System Sciences*, Vol.3, pp.561-570.
[13] G.J. Tomko, C. Soutar, and G.J. Schmidt. **"**Fingerprint controlled public key cryptographic system‖. U.S. Patent 5541994, July 30, 1996 (Priority date: Sept. 7, 1994).
[14] Uludag U, Pankanti S, Prabhakar S, Jain AK: Biometric cryptosystems: issues and challenges. Proc IEEE 2004, 92(6):948 960.
[15] DIGITALPERSONA, INC., CALIFORNIA "Cryptographic key generation using biometric data" U.S. Patent 6035398 A, November 14, 1997 (Priority date: November 14, 1997).

PROFILE OF AUTHORS

Ossai Victor is an Engineer at Electronics Development Institute (ELDI), a research institute of the National Agency for Science and Engineering Infrastructure (NASENI). He has his research interest in Encrypted Biometrics Securities and Embedded system designs/Simulations; he is currently pursuing his M.Eng. in Electronics / Computer Engineering (Computer and Control option)at Nnamdi Azikiwe University Awka.



Israel Okoro is a Scientific Officer at Electronics development institute, a research institute of the national agency for science and engineering infrastructure (NASENI), He has his research interest in power electronics and embedded systems, he is currently doing a masters degree in physics electronics at Nnamdi Azikiwe University Awka.

Alagbu Ekene is an Engineer at Electronics Development Institute (ELDI), a research institute of the national agency for science and engineering infrastructure (NASENI). He has his research interest in Artificial Intelligence and Neural Systems; he is currently pursuing his M.Eng. in Electronics / Computer Engineering (Computer and Control option)at Nnamdi Azikiwe University Awka.

Agbonghae Andrew is an Engineer at Electronics Development Institute (ELDI), a research institute of the national agency for science and engineering infrastructure (NASENI). He has his research interest in advanced embedded system designs /controls, Digital System Processing and; he is currently pursuing his M.Eng. in Electronics / Computer Engineering (Computer and Control option)at Nnamdi Azikiwe University Awka.

Nneka Ifeyinwa. Okafor holds B.Eng. in Computer Engineering from Enugu State University of Science and technology, (ESUT) while currently pursuing her M.Sc in Digital Electronics and Computer Engineering from University of Nigeria Nsukka,(UNN). She has Oracle 10g Expert Certification. Currently, she works as a Research Engineer in Electronics Development Institute, Awka under National Agency for Science and Engineering Infrastructure, Nigeria. She is a graduate Member of Nigerian Society of Engineers, Awka Chapter and a member of IAENG. Her research interests are on Software Graphics, Animation Modelling, Database Management and System Analysis. Conact: