International Conference on Computing, Networking and Informatics

ICCNI 2017

Theme:

Evolution of Grid to Revolution in Cloud

Venue: Centre for Entrepreneurial Development Studies, Covenant University, Ota.

Date: 29 – 31 October 2017

http://iccns.covenantuniversity.edu.ng/

Proceedings of the

IEEE International Conference on Computing, Networking and Informatics (ICCNI 2017)

29-31 October, 2017.
Covenant University, Canaanland, Ota, Ogun State, Nigeria.

IEEE Catalog Number: CFP1492F-ART
ISBN: 978-1-5090-4642-3

Editors
Sanjay Misra
Victor Olu Matthews
Adewole Adewumi

PREFACE

The ICCNI is an international conference that seeks to promote development and advancement through research, innovation and networking. The areas covered by ICCNI include, but not limited to, developmental issues, entrepreneurship and industrialization related fields such as information & communications technologies (ICT), computer networks, software engineering, telecommunications, electrical & electronic engineering, computer science, and applied science. With the main aim to build these industries in the African continent through solicited help from professional and experts around the world, it provides an excellent and affordable opportunity for research collaboration and networking between African-based professionals and their international peers.

ICCNI 2017 includes a keynote speech and invited talks by eminent internationally renowned experts and scholars. It is a fully refereed, international conference, which used a peer-review process to ensure a high quality of scientific submissions. It provides a viable forum for exchange of experiences, ideas and discoveries amongst researchers, professionals, practitioners and experts in various related fields. It also comprises of dedicated sessions where participants gain viable practical knowledge and know-how about the latest Information Technology concepts, theories, tools, models, methodologies, etc.

The Department of Electrical and Information Engineering and the Department of Computer and Information Sciences, Covenant University jointly hosted the conference. The sponsors include: Covenant University and Covenant Microfinance Bank. The conference held from 29-31 October 2017.

We trust that the ICCNI Conference and Proceedings open you to new vistas of discovery and knowledge.

Sanjay Misra
General Chair

Table of Contents

Developing Multifactor Authentication Technique for Secure Electronic Voting System

Oke B. A[1,a]., Olaniyi, O. M[1,b]., Aboaba A. A[2,c]., and Arulogun O. T[3,d].
[1]Department of Computer Engineering, Federal University of Technology, Minna, Nigeria
[2]Department of Computer Engineering, University of Maiduguri, Borno State, Nigeria
[3]Department of Computer Science and Engineering, Ladoke Akintola University of Technology, Ogbomoso, Nigeria
[a]oke.pg612187@st.futminna.edu.ng, [b]mikail.olaniyi@futminna.edu.ng, [c]abdulfattahaa@gmail.com, [d]otarulogun@lautech.edu.ng

***Abstract*— There has been significant research efforts towards replacing the traditional voting approach with electronic voting (e-voting) because technological advancements have called for faster and more reliable means of voting. There are several nationwide voting systems in use all over the world. However, each of these systems has their various shortcomings. In this paper, a multi-factor authentication technique using biometrics fingerprint and cryptographically secured smart card is proposed for secure e-voting system's authentication. The technique involves the combination of an enhanced Feistel block cipher and first moment feature extraction technique for securing both confidential data on voters' smart card and voters' fingerprint template. Results obtained from experimental simulation shows the viability of the proposed technique to avert common problems encountered in voters' authentication during electioneering process in digitally divided environment.**

Keywords—multi-factor; authentication; e-voting; biometrics; cryptography

I. INTRODUCTION

Due to worldwide advancements in computer and telecommunication technologies and the underlying infrastructures, electronic voting (e-voting) is no longer a North American or Western phenomenon. This high technological method of casting a ballot has spread far beyond the United States, expanding throughout the entire world [1]. E-Voting, along with its benefits and mishaps, can now be found from the developed countries of Europe to the developing countries of Asia and Africa. The introduction of electronic voting has been the biggest change to the Irish electoral system since the establishment of the state 80 years ago [1].

The integration of Information and Communication Technology (ICT) in democratic decision making process through electronic voting (e-voting) has provided several potential benefits including improved efficiency, convenience with reduced costs and availability of decision making services to the populace [2]. E-voting as an important e-participatory governmental service has attracted attention as cost effective and electronic decision making alternative to conventional voting [3].

It has been argued that the introduction of e-voting system will have the following salutary effects: increased participation for disadvantaged communities, an antidote to voter apathy, greater voter convenience in terms of voting time and location, access for people with disabilities, money saving, and greater accuracy. A case could be made for the Nigeria electoral system were a voter is required to vote only at closer premises of prior registration. Consequently, this will definitely require time and money and might probably reduce participation. According to some literatures [4,5], an e-voting system should meet certain requirements among which are eligibility, verifiability, security, fairness, anonymity, and transparency, reliability, auditability, and uniqueness. These requirements are still an open area of research especially in developing countries. The requirements selected for the proposed approach herewith were selected based on some challenges faced in the March and April Nigerian elections. Thus, this paper will focus on authentication, issues in verifying and validating eligible registered voters using Smart card readers (SCRs), a low power technological device for the accreditation of voters through Permanent Voter's Cards(PVC).

These issues range from Failed SCR's [6]; Subscriber Identification Module (SIM) issues [7]; Voter's biometrics fingerprint verification issues [8]. Despite these avoidable technical issues, the use of the SCRs encourages voters' confidence in the electoral processes and reduces post electoral legal tussles attributed to previous traditional elections [6, 7].

A novel solution solving these issues will lead to a trusted and transparent electioneering process in Nigeria and developing countries with similar technical, social, administrative and legal electoral frameworks. Therefore, a multi-factor authentication technique is proposed to solve these aforementioned problems.

Our contribution in this paper is part of our overall research goal of addressing security vulnerabilities of the Nigerian Semi-automated voting system by developing novel countermeasures to meet voter's authentication, vote confidentiality and post-election auditing security issues. In particular, the problem of incessant failure in the fingerprint authentication and verification process will be addressed. Multi-factor authentication (MFA) is a security approach of using more than one means of authentication from independent available credentials to verify voter's eligibility to vote. It is widely recognized as the most secure method for authenticating access to data or application [10]. The more factors used to determine a person's identity, the greater the trust of authenticity. In this paper, an MFA approach using fingerprint and smart card secured with enhanced Feistel block cipher is proposed.

The rest of this paper is organized as follows. Section II presents review of related works, Section III discusses the proposed methodology, while Section IV presents discussion of our preliminary results obtained from the approach. The paper is concluded in Section V.

II. RELATED WORKS

A number of related works exist in literature. Review of recent works, merit and demerit, are thus presented.

In [11], an electronic voting system with emphasis on administrative aspect of electioneering processes was proposed. The authors described the responsibilities and privileges of the different actors involved in the electronic voting process as this is necessary to formulate an operational framework that complements the technological security features of the e-voting system. Recommendations were made in [11] for the need to extend the authentication process such that users' action can be validated before the e-voting system is updated. The authors did not address security critical issues such as post-election auditability and system availability.

An electronic voting system which uses voter's fingerprint for authentication was proposed in [1] for handling electronic ballots with multiple scope such as presidential, municipal, and parliamentary. In [12], a secure e-voting system using unimodal fingerprint biometrics and wavelet-based crypto-watermarking approach was proposed. The approach of [12] was capable of preventing falsification in voter's authentication, addressed security issues of vote confidentiality stored in the voting server. The authors did not consider the issue of availability as the use of a single means of authentication (user's fingerprint) can deny eligible voters from voting. This case was widely experienced in the March and April, 2015 general election as the biometric machine fails to detect the fingerprint of many eligible voters [6,7]. This can be solved by introducing multi-authentication means. Finally, the proposed approach did not provide means for voters to have evidence of the candidates they voted for.

In [13], an approach using Radio Frequency Identification (RFID) and enhanced least significant bit audio steganography was proposed for a secure e-voting system. The proposed technique focused on authentication and verification of voters as well as integrity and confidentiality of the casted vote. However, the use RFID only for authentication and verification of eligible voters cannot solve the issue of impersonation. Similarly, the proposed technique does not provide voting receipt for voters as an evidence in case of future reference. A multi-factor authentication approach for secure e-voting system using cryptography hash function have been proposed in [10]. The authors focused majorly on authenticity and integrity of vote transmitted over insecure wireless medium. Voters can cast their vote online via a PC or using mobile phone. This approach is likely to suffer from availability, coercion of voters, and impersonation. Therefore, the approach can further be improved by including biometric sensor to capture the real identity of voter.

Most previous works make use of a single authentication credential to authenticate voters, hence creating a possible means for impersonation, and single point of attack. In [10], an MFA approach was introduced, the proposed MFA has advantage over SFA in that it was able to provide integrity check on the e-voting process, especially during voters' verification, however, the secondary means of authentication involves the use of SMS which might result in delay of voters' authentication. So, in this paper, an MFA approach which:

- Use a proposed enhanced Feistel block cipher, to ensure confidentiality of registered data stored on the smart card,
- and an enhanced voter's fingerprint template using first moment extraction algorithm to verify the authenticity of valid real-time voters, which can remove the likely delay in voters' authentication is proposed herewith.

III. METHODOLOGY

The methodology proposed herewith combines the application of secure authentication algorithms on smart card and fingerprint biometrics to achieve a reliable MFA technique. Each voter requires a smart and his/her fingerprint to vote. Each voters' data is stored in their respective smart card after encryption using the developed enhanced Feistel block cipher. The voter's fingerprint template is enhanced using first order moment feature extraction algorithm. This section discusses our contribution for each of the two authentication means:

A. Design consideration for selecting fingerprint biometric and smart card

A multi-factor authentication approach is proposed to authenticate voters. Multi-factor authentication technique employs the use of more than one means authentication from available credential to identify users. Several factors were considered in selecting combination of credentials for the authentication process. These comprise: user acceptability, time to authenticate a voter, memory requirement for the chosen credential. In [6], the authors combined the use of grid card and one time SMS as a way of providing multiple means of authentication of voters. However, there is no doubt that the use of SMS will introduce delay in the authentication process. In this work, a combination of biometric and smart card is proposed. To select the biometric trait to be used, the various biometric traits were compared under the following criteria and results of comparison is tabulated in Table I.

1. Universality: refers to possession of such features in all individuals.
2. Uniqueness: implies the discriminatory power of the feature amongst individuals.
3. Permanence: connotes the stability of the features such that it does not change overtime due to different constraints like environmental condition, weight, age or perhaps due to wear and tear as a result of manual labour.
4. Collectability: indicates ease of acquiring the biometrics feature data. Also, the robustness, reliability, as well as cost effectiveness for the application is also of a great concern.

The requirements for practical application of biometrics systems are:

5. Performance: this is a measurement of the accuracy of the biometric trait in all aspects and ramification in other to achieve the desired result.

6. Acceptability: is a biometrics system requirement which indicates the extent to which people are willing to acknowledge it.

7. Circumvention: indicates how easy or difficult imposters can have access to the biometric trait.

Table I shows the relationships among various biometrics traits and how combining these seven criteria could aid multi-factor authentication design technique for securing voter's credential. From Table I, the physiological biometrics features are more universal and unique than the behavioral features. Eye pattern biometrics features specifically, iris and retina are good features that can be recommended for high security demanding applications due to its low circumvention rate but these two features have less acceptability rate and most importantly are difficult to collect. Analyzing the hand based biometrics, the uniqueness, performance and stability of fingerprints and palm print is equally high, however, it is much easier to collect fingerprint than palm print.

In this paper, FPM10A fingerprint sensors with a False Accept Rate (FAR) of less than 0.001%, False Reject Rate (FRR) less than 1.0%, and search time less than 1.0s was selected as a viable option to achieve the set requirement for authentication of voters. The target is to achieve fast voter's authentication process with low rejection rate. The embedded system to control the fingerprint sensor will be developed as part of this research.

To provide a multi-factor means of authentication of voters, an ISO, PVC blank smart card based SLE4442 chip was selected. According to [14], each card can provide a 256 by 8 bit memory location, erase cycle of more than 100,000 times, and data retention for minimum of 10 years. Consequently, making it a viable option over RFID tag which could easily be impersonated by erring voter. The card was used to store voter's details as well as a digital receipt after voting will be save on the card.

TABLE I. COMPARISON OF VARIOUS BIOMETRICS BASED ON SEVEN DIFFERENT CRITERIA INCLUDING EASY OF COLLECTING THE BIOMETRIC DATA, USER ACCEPTABILITY, UNIQUENESS, AND UNIVERSALITY AMONG OTHERS [15].

Biometrics	**1**	**2**	**3**	**4**	**5**	**6**	**7**
Face	High	Low	Medium	High	Low	High	High
Fingerprint	Medium	High	High	Medium	High	Medium	High
Hand geometry	Medium	Medium	Medium	High	Medium	Medium	Medium
Keystroke	Low	Low	Low	Medium	Low	Medium	Medium
Hand vein	Medium	Medium	Medium	Medium	Medium	Medium	Low
Iris	High	High	High	Medium	High	Low	Low
Retina	High	High	Medium	Low	High	Low	Low
Signature	Low	Low	Low	High	Low	High	High
Voice print	Medium	Low	Low	Medium	Low	High	High
Facial Thermogram	High	High	Low	High	Medium	High	Low
Odour	High	High	High	Low	Low	Medium	Low
DNA	High	High	High	Low	High	Low	Low
Gait	Medium	Low	Low	High	Low	High	Medium
Palm print	Medium	High	High	Medium	High	Medium	Medium
Ear	Medium	Medium	High	Medium	Medium	High	Medium

B. First Order Moment Feature Extraction from FPM10A

The FPM10A fingerprint sensor returns a 512 bytes of user's fingerprint template. The 512 bytes are organized as 8-bits by 512. Traditional approach involves a template matching of the stored 512 bytes to the 512 bytes fingerprint template of the user. Therefore, in the proposed approach, the mean of each user template is computed and stored. To verify the authenticity of an unknown *user y*, the mean of the template of *user y* is computed and compared with the previously stored means.

The mean of each template is computed as in (1).

$$m_k = \frac{1}{512}\sum_{i=1}^{512} x_i \qquad (1)$$

Where k is the k^{th} registered voters, x_i are the different 8-bit content of the template. Considering an unknown *user y*, to authenticate the user the mean of *user y* template is computed as in (2).

$$m_y = \frac{1}{512}\sum_{i=1}^{512} x_i \qquad (2)$$

m_y is compared against all the stored mean as:

$$e_k = m_y - m_k$$

Where e , is the error margin, $k = 1, 2, ..., N$ and N is the total number of registered voters.

Unknown voter y is authenticated as voter k where e_k is minimum error margin.

The average mean square error is given as in (3).

$$mse = \frac{1}{N}\sum_{k=1}^{N} e_k^2 \qquad (3)$$

C. Securing Data on the Smart Card using Enhanced Feistel Block Cipher

The data to be secured on the smart card includes the voter's name, state, local government area, smart card number, voting receipt, and the extracted feature of the voter's fingerprint. These details are first protected using the enhanced Feistel block cipher after which they are written to the smart card.

The Feistel cipher uses the concept of a product cipher which involves the execution of two or more simple ciphers in sequence in a manner that the final result or product is cryptographically stronger than any of the components ciphers. It uses key length of k-bits and block length of n-bits leading to possible transformation (PT) of

$$PT = 2^k \qquad (4)$$

It alternates between substitution and permutation of the plaintext. In substitution, each plaintext element is uniquely replaced by a corresponding cipher text element while in permutation, a sequence of plaintext elements is replaced by permutation of that sequence. The Feistel cipher has an input length of $2w$ bits plaintext, and a key K , while the plaintext is divided into two blocks L and R . The two sub-blocks pass through n-rounds of processing. Each round i has L_{i-1} , R_{i-1} and sub-keys k_i . Each k_i are derived from K, different from each other and the overall key K . All the rounds have the same structure with substitution performed on left half of the data. This is done by using round function F to the right half of the data and then taking the exclusive-OR of the output of that function and the left half of the data. The round function can be express as $F(RE_i, k_{i+1})$ where R represents the right hand of the block, E implies the encryption process. Permutation is then performed by interchanging the two halves of the data. This structure represents a substitution-permutation network (SPN).

In the proposed approach, each round is not the same as the traditional Feistel cipher. The original network of the Feistel block (SPN) was enhanced by randomly combining between the substitution-permutation (SP) and permutation-substitution (PS) network. It alternates between SP and PS, i.e. round 1 could be SP while round 2 be PS depending on the output of a random function. This was necessary to harden the cryptanalysis of the network. Fig. 1 shows the structure of the Feistel block cipher with the different stages

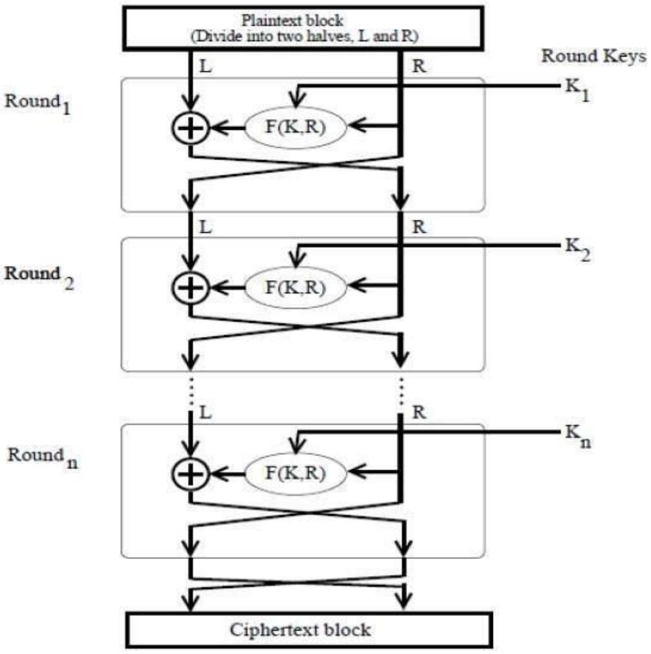

Fig. 1. Structure of the Feistel block cipher

The structure represents a substitution-permutation paradigm in each of the stage. However, the modified approach alternates between substitution-permutation and permutation-substitution in the different stages. Hence, making it difficult for an eavesdropper to predict the sequence that generated the cipher text. This was made possible through the introduction of a random function *r* to generate the pattern of the structure. Fig.

2 shows the block diagram of the enhanced block cipher, where K is the encryption key, and r is the randomness generator.

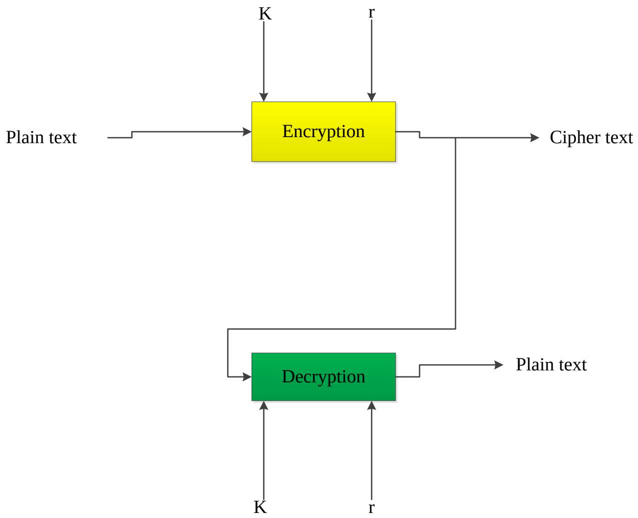

Fig. 2. Block diagram of the modified Feistel block cipher

The random binary number generator r, generates a sequence of 1's and 0's which determines the network of SP and PS to be used in generating the cipher text of a particular voter's data. The traditional Feistel block cipher consists of 16 rounds of SP network. Therefore, a two bytes data which determines the network sequence in our own case is obtained using (5).

$$r = round(lb + (ub - lb) * rand) \qquad (5)$$

Where $lb = 0, ub = 1$. Equation (5) generates random sequence of 1's and 0's. During encryption, the key k and r is used by the network. Same k and r are used during the decryption process to obtain the original plain text. This approach makes it difficult for a potential attacker to decrypt the message. Preliminary results obtained using the enhanced Feistel cipher is presented in the next Section.

IV. RESULT AND DISCUSSIONS OF RESULT

The proposed techniques was tested using a typical voter's credential as shown in Tables II and III. The data contains the name, state and local government area (LGA) of the potential voter, among others. For simplicity, the 36 states of Nigeria are represented using codes ranging from 01-36. The local government areas under each state are also represented using code starting from 01 to the number of LGA in that state. These data is encrypted and decrypted using the enhanced Feistel block cipher and results obtained are presented.

TABLE II. PRELIMINARY RESULTS OBTAINED FROM EVALUATION OF THE ENHANCED BLOCK CIPHER USING A TYPICAL VOTER'S CREDENTIAL (SAMPLE 1)

		Code
Voter's Name	Mustapha Bola	
State	Kwara	016
Fingerprint ID		020
Local Govt.	Ilorin west	015
Age		30
Sex	Male	01
Smart card number		015

Each voter's credential was keyed-in in the following sequence: Name, State, local govt., age, sex, fingerprint ID, smart card number. All credentials were automatically converted to hexadecimal code during processing.

The code assigned for Male voters is 1, while for Female voters is 0. Smart card code lies in the range of 1 to 50.

Applying the voter's details to the encryption algorithm gives:

"EB9B437B56D39E88E05CC8553C17D45CAEFFFDE7B35 F1836EB817AA5BE07796ACD766F450148F4F9"

While Applying the decryption algorithm gives "Mustapha Bola, 16, 15, 30, 1, 20, 15–ÿ7z"

There are still some noisy data added to the end of the plain text, during the decryption process, which will need to be filtered.

TABLE III. PRELIMINARY RESULTS USING CREDENTIAL OF ANOTHER VOTER (SAMPLE 2)

		Code
Voter's Name	Oke Babatope	
State	Niger	020
Fingerprint ID		025
Local Govt.	Bida	015
Age		33
Sex	Male	01
Smart card number		003

The cipher text obtained from the above data is given as: "BCFD134FB3487CC3E90A324DDB89E9B3AE4D27BC05 81B5D7596AB5E96FBD2A4E8493C167138BD9EC"

Applying the decryption algorithm gives "Oke Babatope, 20, 15, 33, 1, 25, 3<ý YÏ"

Credentials in Tables I and II are typical voter's data required to vote in most voting systems. Such is the case of Nigeria voting system. To avoid impersonation during electioneering process, such data will need to be verified to authenticate any prospective voter. Most previous voting techniques have used single authentication means thus leading to wide spread impersonation during voting. To avoid this issue, this paper have proposed the MFA technique involving the use of smartcard and fingerprint biometric. First order moment feature extraction is applied on each fingerprint template. The extracted feature alongside other credentials are encrypted and stored in the voter's smart card. This is an advantage over the use of RFID tag which cannot store much details as smartcard. Encrypted data obtained for Tables I and II are as a result of applying the modified Feistel block cipher. Though a stronger cipher text was obtained, however, at the expense of extra variable which determines the network pattern of the cipher block. Consequently, making it difficult for a potential attacker to break.

V. Conclusion

In this paper, a secure multi-factor authentication technique for electronic voting system has been presented. An enhanced Feistel block cipher algorithm was proposed to secure the data on the smart card. To avoid issues of failed fingerprint authentication, a feature extraction technique using first moment approach was adopted. Results presented herewith was obtained as preliminary results of an ongoing research into developing secured e-voting system using MFA for authentication and crystographic model for vote confidentiality. Future works include integration of the MFA and crystographic model for a typical voting scenario.

References

[1] M. Khasawneh *et al.*, “A Biometric-Secure e-Voting System for Election Processes,” in *Proceeding of the 5th International Symposium on Mechatronics and its Applications (ISMA08), Amman, Jordan*, 2008, pp. 1–8.

[2] O. M. Olaniyi, A. O O, & O. T. O., and E. O. Okediran, “Enhanced Stegano-Cryptographic Model for Secure Electronic Voting,” *J. Inf. Eng. Appl.*, vol. 5, no. 4, pp. 1–15, 2015.

[3] O. M. Olaniyi, O. . Arulogun, & E.O. Omidiora, and O. O.O, “A Survey of Cryptographic and Stegano-Cryptographic Models for Secure Electronic Voting System,” *Covenant J. Informatics Commun. Technol.*, vol. 1, no. 2, pp. 54–78, 2013.

[4] M. H. Sedky and R. E. M. Hamed, “A Secure e-Government ’s e-Voting System,” in *Science and Information Conference 2015*, 2015, pp. 1365–1373.

[5] D. Petcu and D. A. Stoichescu, “A hybrid mobile biometric-based e-voting system,” in *2015 9th International Symposium on Advanced Topics in Electrical Engineering (ATEE)*, 2015, pp. 37–42.

[6] O. Osho, V. L. Yisa, and O. J. Jebutu, “E-Voting in Nigeria : A Survey of Voters Perception of Security and Other Trust Factors,” in *In Cyberspace (CYBER-Abuja), 2015 International Conference on*, 2015, pp. 202–211.

[7] Vanguard, “Vanguard Nigeria,” 2015. [Online]. Available: http://www.vanguardngr.com/2015/03/after-initial-card-reader-failurenigerians-persevere-vote-in-peaceful-elections/. [Accessed: 19-Sep-2017].

[8] N. Ibeh, “3 card readers fail to accredit Jonathan,” 2015. [Online]. Available: http://www.premiumtimesng.com/news/top-news/179447-3-cardreaders-fail-to-accredit-jonathan.html. [Accessed: 20-Sep-2017].

[9] C. Nwangwu, “Biometric Voting Technology and the 2015 General elections in Nigeria,” in *Conference on the 2015 General Elections in Nigeria: The Real Issues*, 2015.

[10] O. M. Olaniyi, O. T. Arulogun, E. O. Omidiora, and A. Oludotun, “Design of Secure Electronic Voting System Using Multifactor Authentication and Cryptographic Hash Functions,” *Int. J. Comput. Inf. Technol. (ISSN 2279 – 0764)*, vol. 2, no. 6, pp. 1122–1130, 2013.

[11] C. Lambrinoudakis, S. Kokolakis, M. Karyda, V. Tsoumas, D. Gritzalis, and S. Katsikas, “Electronic Voting Systems : Security Implications of the Administrative Workflow,” in *Proceedings of the 14th International Workshop on Database and Expert Systems Applications (DEXA’03)*, 2003, pp. 467–471.

[12] O. M. Olaniyi, T. A. Folorunso, A. Ahmed, and O. Joseph, “Design of Secure Electronic Voting System Using Fingerprint Biometrics and Crypto- Watermarking Approach,” *I.J. Inf. Eng. Electron. Bus.*, vol. 8, no. 5, pp. 9–17, 2016.

[13] O. M. Olaniyi, F. T. Abiodun, A. Ibrahim, and A. K. Abdusalam, “Design and Development of Secure Electronic Voting System Using Radio Frequency Identification and Enhanced Least Significant Bit Audio Steganographic Technique,” *IOSR J. Comput. Eng.*, vol. 17, no. 6, pp. 86–97, 2015.

[14] ATmel Corporation, “Two-wire Serial EEPROM Smart Card Modules,” 2003. [Online]. Available: www.atmel.com/Images/doc1661.pdf. [Accessed: 30-May-2017].

[15] A. K. Jain, A. Ross, and S. Prabhakar, “An introduction to biometric recognition,” *IEEE Trans. circuits Syst. video Technol.*, vol. 14, no. 1, pp. 4–20, 2004.