

Article Citation Format

Adewale, O.S., Boyinbode, O.K. & Salako, E.A. (2020):
An Innovative Strategy for Satisfying Data Integrity Requirement of
Electronic Voting System. Journal of Digital Innovations & Contemp Res. In
Science., Engineering & Technology. Vol. 7, No. 1. Pp 1-12

Article Progress Time Stamps

Article Type: Research Article
Manuscript Received: 14th Nov, 2019
Review Type: Blind
Final Acceptance:: 5th January, 2020
Article DOI: [dx.doi.org/10.22624/AIMS/DIGITALV8N1P1](https://doi.org/10.22624/AIMS/DIGITALV8N1P1)

An Innovative Strategy for Satisfying Data Integrity Requirement of Electronic Voting System

¹Adewale, O.S., ²Boyinbode, O.K. & ³Salako, E.A.

^{1&3}Department of Computer Science,

Department of Information Technology

Federal University of Technology, Akure, Ondo State, Nigeria

E-mails: ¹adewale@futa.edu.ng; ²okboyinbode@futa.edu.ng; ³salakoea@futa.edu.ng

ABSTRACT

The ultimate intention of corrupt politicians is to win elections at all costs. This is evident as corrupt politicians strategically buy votes, engage political thugs to snatch ballot boxes, pay election officers to manipulate results and pay fraudsters to intercept and alter the election results along the communication channels for selfish gains. However, a series of attempts such as passwords, secure hash functions, message authentication code, have been made to curtail the unlawful practices of results' modification by fraudsters. The existing approaches have issues on data authentication, data repudiation and integrity. This paper presented a new technique that would satisfy the data integrity requirement of the electronic voting system using fingerprints. Design and formulation of mathematical technique that would fuse the fingerprints of polling and collation officers were presented. It was highlighted that the technique would solve the problems of passive and active attacks on sensitive election results thereby satisfying the integrity demand of the electronic voting system. Future work would involve the implementation and evaluation of the technique presented in this paper using standard metrics.

Keywords: Strategy, Satisfying, Integrity, Requirement, Electronic, Voting System

1. INTRODUCTION

An election is a principal and formal process to express a decision on a thing or an individual who would occupy a political office or other significant offices. In a democratic society, an election implies an expression of choice on a candidate who is selected to be in the position of authority for efficient governance. The formal choice made by a person on a candidate in an election is referred to as a vote. A collection of votes can be referred to as results which determine who wins an election based on specified guidelines of the election. The significance of election results cannot be under-rated as the determinant force on who governs a democratic society. The election results remain sensitive pillar that validates the credibility of an election. The elections are used as fundamental guidelines on how a winner would be declared on the basis of specified rules and regulations.

The votes polled by the voters at different polling booths are counted and recorded for each candidate participating in an election. In an ideal situation, the politicians rely on the votes of the voters or delegates as specified by the rules and regulations to win an election [1]. However, the bad ambition of corrupt politicians has negatively affected the outcomes/results of different types of election. The corrupt candidate in an election could engage the services of corrupt election officers and fraudsters to alter the sensitive results for selfish interest, thereby leading to false results and undesired candidate emerges as a winner. For instance, there were records of ballot snatching, shooting sporadically, votes' buying and selling in Kogi and Bayelsa 2019 governorship election [2, 3]. It was lamented by a voter that the votes in the election might not count as there were incidences of snatching of ballot boxes at different polling booths by political thugs and fraudsters to manipulate the results of the election for a particular candidate [3, 4].

This unlawful practise of snatching ballot boxes was possible as polling officers or returning officers manually collated and recorded the election results. Also, the manually recorded results were either transported by cars or transmitted to the collation centre through public unprotected networks. As the sensitive results transit from the polling booths to the collation centres by cars and attackable networks, the fraudsters could intercept and modify the results. This implies that the trustworthiness and integrity of the sensitive results received at the collation centres are questionable. This is remarkably noted as there were court cases on the election results [4].

The advent of computer technology promised to tackle a series of challenges recorded from different types of elections across the nations of the world [5]. The integration of electronic devices into voting systems exclusively depends on the identified security and functional challenges. It is on these challenges that the security and functional requirements of the electronic voting (e-voting) system were highlighted to tackle specific problems that are peculiar to a society [6]. The security and functional requirements deal with specific demands on how an e-voting system ought to secure the election data and perform function towards achieving a credible and fair election. Basically, the security requirements included system integrity, data integrity, secrecy/privacy, reliability, authentication, availability and confidentiality, among others [6]. Also, functional requirements included flexibility, transparency, auditability, mobility, verifiability, documentation and assurance among others [6, 7]. This paper focused on a new strategy to accomplish the data integrity requirement of electronic voting systems.

1.1 Data Integrity Defined

In the security term, the data integrity certifies that the sensitive data are free from alteration or any form of modification once recorded. Data integrity deals with the assurance of accuracy and constituency of data over the entire life cycle [8]. This implies that data integrity is the wholeness, accuracy and consistency of data over its entire lifetime which suggest that data is intact and has not been modified. Fundamentally, the objective of data integrity is to ascertain that data has not been altered during transmission and over its lifetime. The data integrity checks prevent modification, forgery and deletion. Any alteration on data would be detected by data integrity check-test.

Basically, there are two types of threats to data, these included passive and active threats. The passive threats are due to different accidental errors such as noise, collision and corruptions in transmission channels. The active threats on data deal with the interception and alteration made by the fraudsters or attackers [9]. In passive threat, information is monitored while in active threat, information is altered [8, 10]. The data integrity tests allow the data to be verified for either acceptance or rejection of the sensitive data. At present, many measures for data integrity check-test have been proposed. These measures included hash-functions, such as Message Digest (MD), Secure Hash Function (SHA), Integrity Primitives Evaluation Message Digest (RIPEMD) and Whirlpool. These hash functions had been used to detect attacks and any alteration on sensitive data. The limitation of hash functions as identified by in [9] was lack of data authentication. This implied that the hash functions would not authenticate the originator or sender of the sensitive data. In an attempt to authenticate the source of the sensitive data, a cryptographic technique called Message Authentication Code (MAC) was introduced [9, 10].

The MAC is a cryptographic technique that establishes the source of the sensitive data by the use of a shared symmetric key between the sender and the receiver. The use of MAC requires a key between the sender and the receiver prior to the transmission of the sensitive data. The limitation of MAC included the likelihood of fraudsters gaining access to the shared key before the transmission. This implied that MAC has not provided the adequate data integrity check on the sensitive data as fraudsters and attackers could gain access to the shared key for alteration. Also, MAC would not be able to affirm the data origination when there is a dispute between the sender and the receiver on the sensitive data. Furthermore, digital signatures were introduced as attempts to tackle the limitations of MAC on data integrity. The digital signatures are cryptographic values obtained by the use of a secret key and data. A cryptography digital signature requires a secret key between the sender and receiver. A private key is used by the sender to sign the data while a public key is used by the receiver to verify the data [9].

1.2 Statement of the Problem

The results of the election received at the collation centre have data integrity issues as there is a likelihood of interception and alteration by the corrupt politicians, corrupt election officers and fraudsters. How could the collation officers affirm that the election results received have not been tampered with by the corrupt politicians, corrupt election officers and fraudsters? There is a problem of repudiation between the sender (polling officer at the polling booth) of the election results and the receiver (collation officer at the collation centre). In the existing work, the polling officer could deny sending the election result to the collation officer. This is a serious problem that needs urgent attention for a credible and fair election.

The digital signature using private and public keys has challenges of data authentication and repudiation when keys are not technically selected. At present, numeric, text and special characters are used to generate the private and public keys. These types of keys could be guessed by the fraudsters to alter sensitive data for personal gains. There could also be a problem of repudiation between the sender and the receiver when attackers guess the keys. The security of a cryptosystem is ultimately a function of types of keys and how the keys are secured and managed against attacks. The researchers adapted a cryptography digital signatures technique to formulate a new strategy to achieve data integrity requirement of e-voting system using fingerprints of the sender (polling officer) and receiver (collation officer).

1.3 Objective

The specific objectives of this paper are to design and formulate a new mathematical technique that fuses the fingerprints of a polling officer and collation officer towards achieving the integrity requirement of e-voting systems.

2. PROPOSED TECHNIQUE

Figure 1 shows a block diagram of the proposed technique.

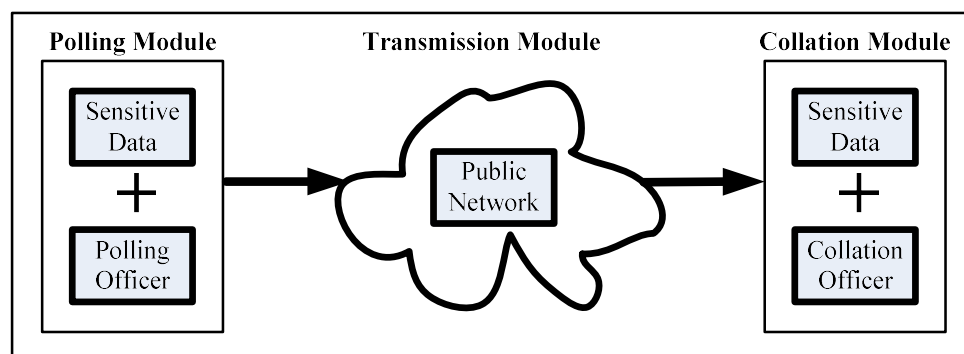


Figure 1: Block Diagram

Basically, there are three modules in the proposed design of satisfying the data integrity requirement of e-voting system. These modules are the polling, transmission and collation modules. At the polling module, the sensitive results (election results) would be signed using the fused fingerprints of the polling officer (sender) and collation officer (receiver). The digitally signed results would be transmitted through the transmission module (public unprotected network). Furthermore, at the collation module, the signed results would be verified by fused fingerprints of the polling and collation officers.

2.1 Election Officers Fingerprint Minutiae Point Analysis

Fingerprint minutiae describe the specific plot of points or features of a fingerprint. Such minutiae include ridge-end, bifurcation, independent ridge, lake, dot or island (isolated), spur, crossover [11]. Ridges and bifurcations are used for this framework for a higher probability of accuracy when compared with other minutiae [11]. Crossing number (C_N) identification technique (Equation 1) would be adopted to identify the voter's minutiae. The fingerprint pre-processing involves Normalization, Segmentation, Fingerprint Image Enhancement and Binarization as illustrated in Figure 2.

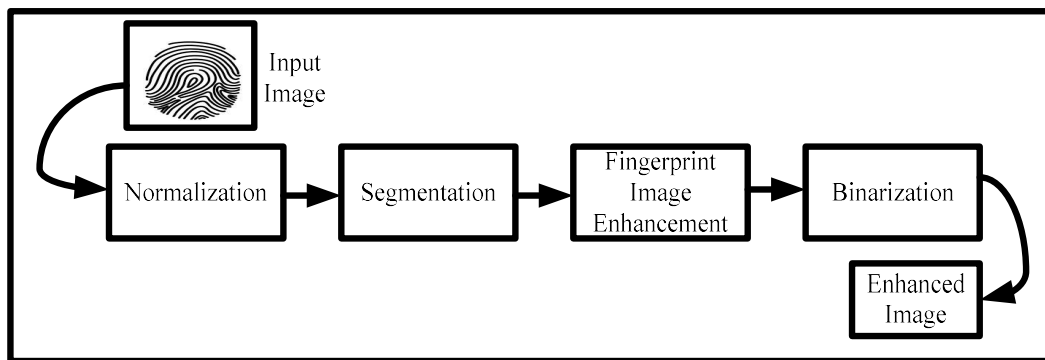


Figure 2: Fingerprint pre-processing

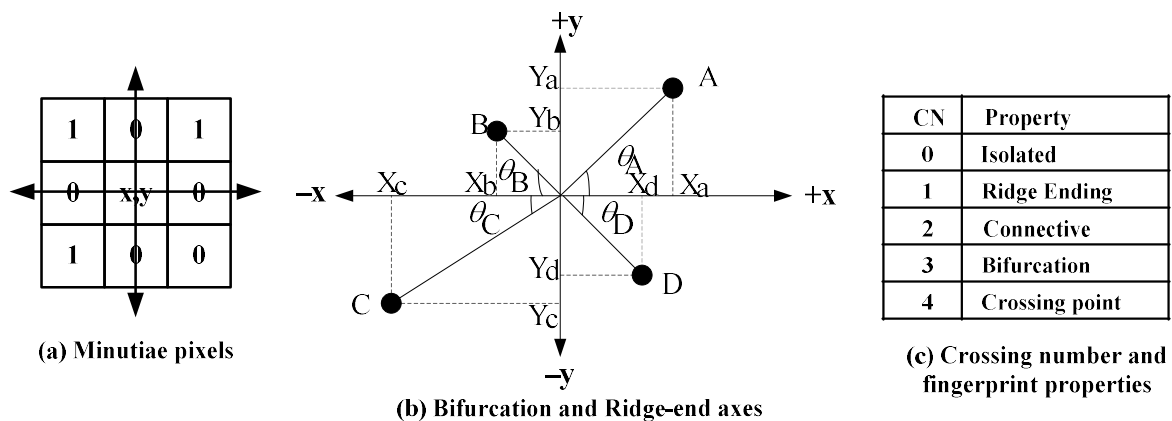


Figure 3: Ridges end and bifurcations detection

$$CN = \frac{1}{2} \sum_{i=1}^8 |P_i - P_{i+1}| \quad (1)$$

In Equation 1, $P_9 = P_1$.

The distances and ridge-end and bifurcation scores would be measured using Equation 2 while angles of ridge-ends and bifurcation would be measured using Equations 3, 4 and 5.

$$R_distance \text{ or } B_distance; |OA| = \sqrt{Y_a^2 + X_a^2} \quad (2)$$

$$R\theta \text{ or } B\theta; \theta_A = \tan^{-1} \left[\frac{Y_a}{X_a} \right] \quad (3)$$

$$R\theta = \left(\frac{\theta_A \times \pi}{180} \right) + (wdt) \quad (4)$$

The extracted officer's fingerprint features would be represented by a score, V_f and it would be expressed as:

$$P_f = C_f = \left| \left(\sum_{j=1}^{R2} (RD_j) + \sum_{n=1}^N (R\theta_n) \right) - \left(\sum_{i=1}^{B2} (BD_i) + \sum_{m=1}^M (B\theta_m) \right) \right| \quad (5)$$

Where P_f and C_f are the fingerprints' scores of the polling and collation officers respectively.

2.2 Fusion Technique

A fusion technique presented by [5] would be adapted to fuse the fingerprints' scores of polling and collation officers as follows:

$$K(P_f, C_f, \beta) = \left(\frac{1}{\beta} \right) * \left(\frac{P_f}{P_f + C_f} \right) \quad (6)$$

The Beta β is a mathematical constant and it would be used as officers' sensitivity that controls the difference in the scores between a genuine election officer and a fraudster. In addition, the parameter ρ (Pho) in Equation 7 would be the agents' fingerprints to sign the election results and the election results signed by the agents would be stored in a dedicated database for forensic investigation (audit).

$$K_A(P_f, C_f, \beta, \rho) = \left(\frac{1}{\beta} \right) * \left(\frac{P_f}{P_f + C_f} \right) * \left(\frac{1}{\rho} \right) \quad (7)$$

The fused score of the polling and collation officers' fingerprints would be used as the signature key (K) at a polling booth and the verification key (K) at the collation centre to establish the data integrity requirement and origin of the election results. The fingerprints could be acquired for processing by use of offline and live images' acquisition [12]. Thus, the C_f would be made available at the polling booth as offline image while P_f would be live for the polling officer to generate the signature key that would be used to sign the results and the P_f would be made available at the collation centre as offline image while C_f would be live to generate the verification key that would be used to verify the results prior to the transmission of the sensitive results on the public and unprotected networks.

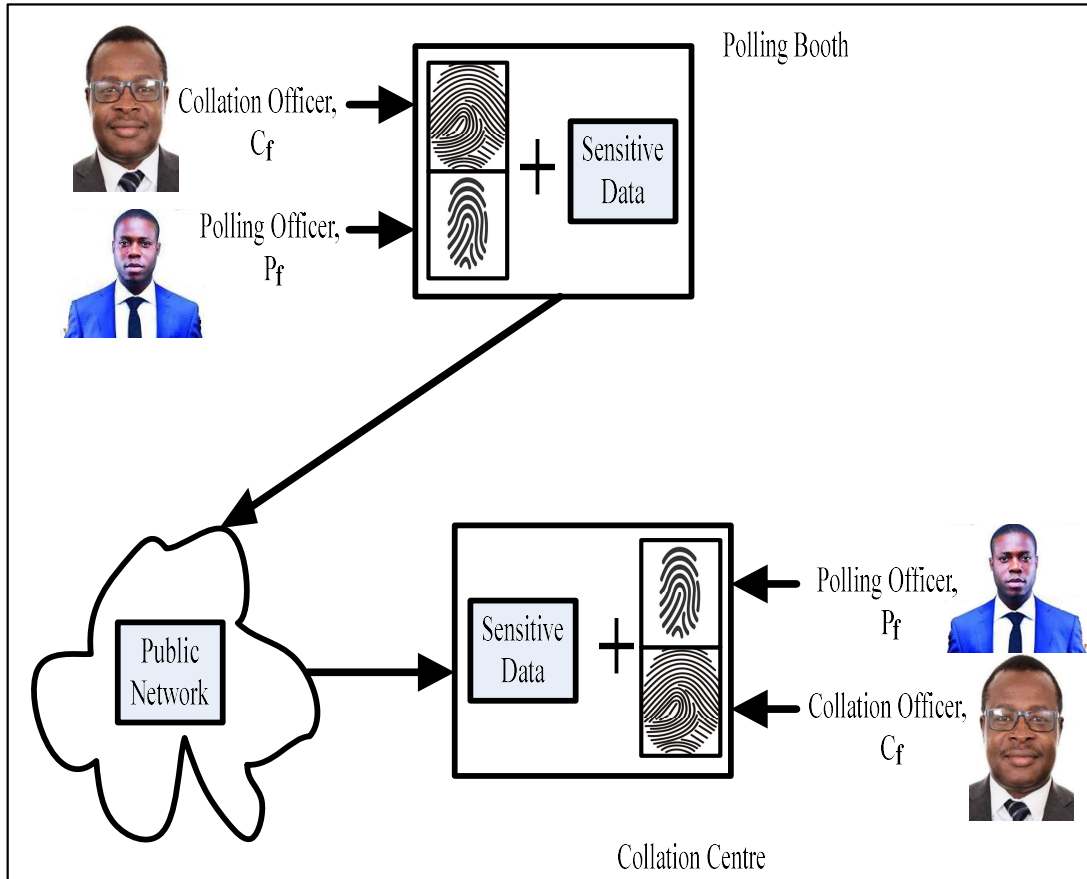


Figure 4: Signing and Verifying of Results by Election Officers

The polling officer signed the original results, M by key, K to produce digitally signed result, T . The digitally signed result, T would be digitally concatenated with the original results, M to produce a message, H . Mathematically, let election result be Matrix M , signature and verification key be Matrix K .

$$T = K \times M \quad (8)$$

i. Let the election results (Matrix M) be represented as:

$$M = \begin{bmatrix} M_{11} & M_{12} & M_{13} & M_{14} & . & . & . & M_{R1} \\ M_{21} & M_{22} & M_{23} & M_{24} & . & . & . & M_{R2} \\ M_{31} & M_{32} & M_{33} & M_{34} & . & . & . & M_{R3} \\ . & . & . & . & . & . & . & . \\ . & . & . & . & . & . & . & . \\ M_{C1} & M_{C2} & M_{C3} & M_{C4} & . & . & . & M_M \end{bmatrix}$$

ii. Let the key (Matrix K) be represented as:

$$K = \begin{bmatrix} K_{11} & K_{12} & K_{13} & K_{14} & . & . & . & K_{R1} \\ K_{21} & K_{22} & K_{23} & K_{24} & . & . & . & K_{R2} \\ K_{31} & K_{32} & K_{33} & K_{34} & . & . & . & K_{R3} \\ . & . & . & . & . & . & . & . \\ . & . & . & . & . & . & . & . \\ . & . & . & . & . & . & . & . \\ K_{C1} & K_{C2} & K_{C3} & K_{C4} & . & . & . & K_K \end{bmatrix}$$

iii. Multiply the Matrix K (private key) by the Matrix M (original results) to obtain Matrix T.

$$T = \begin{bmatrix} T_{11} & T_{12} & T_{13} & T_{14} & . & . & . & T_{R1} \\ T_{21} & T_{22} & T_{23} & T_{24} & . & . & . & T_{R2} \\ T_{31} & T_{32} & T_{33} & T_{34} & . & . & . & T_{R3} \\ . & . & . & . & . & . & . & . \\ . & . & . & . & . & . & . & . \\ . & . & . & . & . & . & . & . \\ T_{C1} & T_{C2} & T_{C3} & T_{C4} & . & . & . & T_T \end{bmatrix}$$

Matrix **T** is the digitally signed result that would be concatenated with the original election results, matrix **M** to produce new matrix **H**. Matrix concatenation is a technique of joining one or more matrices to produce a new matrix.

$$H(T, M) = \begin{bmatrix} T_{11} & T_{12} & T_{13} & T_{14} & M_{11} & M_{12} & M_{13} & M_{14} & . & . & . & p \\ T_{21} & T_{22} & T_{23} & T_{24} & M_{21} & M_{22} & M_{23} & M_{24} & . & . & . & q \\ T_{31} & T_{32} & T_{33} & T_{34} & M_{31} & M_{32} & M_{33} & M_{34} & . & . & . & r \\ T_{41} & T_{42} & T_{43} & T_{44} & M_{41} & M_{42} & M_{43} & M_{44} & . & . & . & s \\ . & . & . & . & . & . & . & . & . & . & . & u \\ . & . & . & . & . & . & . & . & . & . & . & v \\ . & . & . & . & . & . & . & . & . & . & . & w \\ T_1 & T_2 & T_3 & T_4 & M_1 & M_2 & M_3 & M_4 & T_5 & . & . & x \end{bmatrix}$$

The matrix **H** is the digitally concatenated matrix that has Matrix **T** and original results, Matrix **M**, and it would be transmitted from the polling booth to the collation centre for data integrity check.

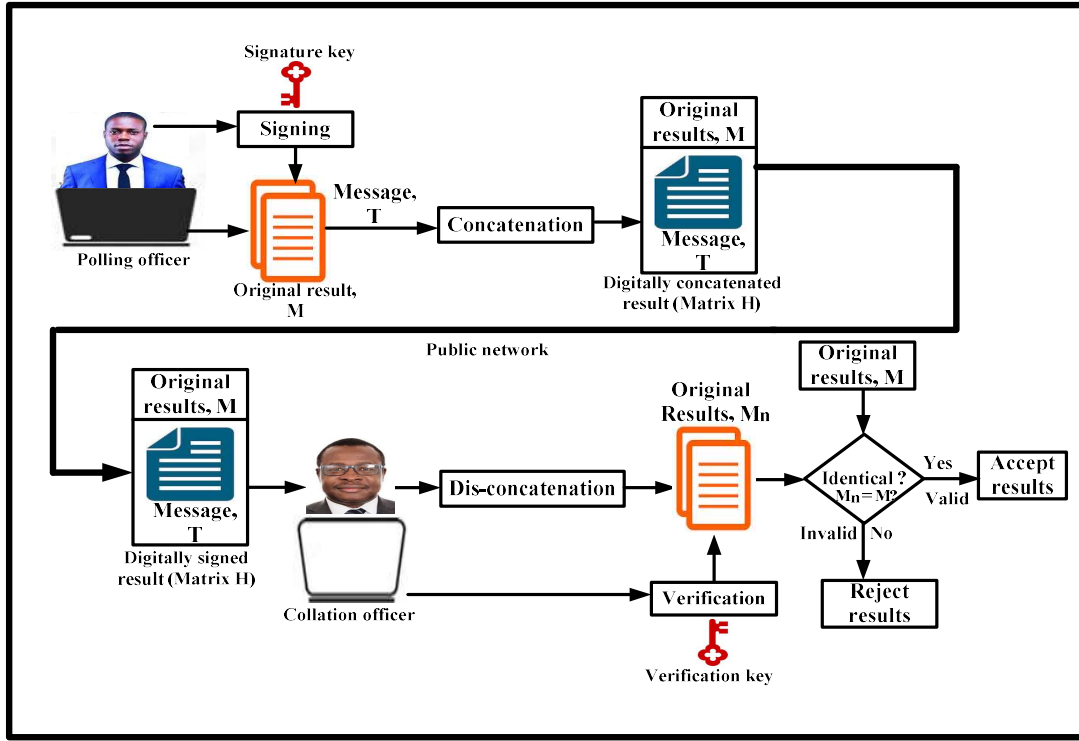


Figure 5: Result integrity verification

At the collation centre, the collation officer would dis-concatenate the Matrix H to obtain Matrix T and original results, Matrix M. A reverse computation of generating Matrix T would be performed by the collation officer using the key, Matrix K.

If

$$K \times M = T \quad (9)$$

Then,

$$(K^{-1} \times K) \times (M) = K^{-1} \times T \quad (10)$$

$$IM = K^{-1}T \quad (I = (K^{-1} \times K) \text{ is the unit matrix})$$

$$IM = K^{-1} \times T \quad (11)$$

$$M = K^{-1} \times T$$

At the collation centre and for the verification of results, the new result (Matrix Mn) could be obtained as follows:

$$M_n = K^{-1} \times T \quad (12)$$

The newly generated Matrix Mn would be compared with the received Matrix M to detect any active attack on the sensitive results. The result is valid and accepted as genuine if Matrix Mn is computationally identical with Matrix M. Furthermore, a detection on passive threat would be carried out to ascertain that there was no data corruption.

This would be achieved using the key, Matrix K as follows.

From Equation 8,

$$K \times M = T \quad (13)$$

$$K \times (M^{-1} \times M) = M^{-1} \times T \quad (14)$$

$$KI = M^{-1}T \quad (I = (M^{-1} \times M) \text{ is the unit matrix})$$

$$IK = M^{-1} \times T \quad (15)$$

$$K = M^{-1} \times T$$

At the collation centre and for the verification of results, the new result (Matrix Kn) could be as follows:

$$K_n = M^{-1} \times T \quad (16)$$

The newly generated Matrix Kn would be compared with the already available Matrix K to detect any passive attack on the sensitive results. To achieve a moderate acceptance and rejection rates of the collation's fingerprint score for results' verification, a threshold value, K_T would be computed as follows.

Let Matrix K, be already stored key of polling and collation officers,

Matrix Kn is a newly generated key at the collation centre,

Matrix K_T is a threshold key to achieve moderate acceptance and rejection rates.

Thus:

$$K_T(P_f, C_f, \beta, \delta) = \left[\left(\frac{1}{\beta} \right) * \left(\frac{P_f}{P_f + C_f} \right) * \delta \right] : \delta = 0.9786 \quad (17)$$

Where δ a mathematical constant of 0.9786 that would indicate the matching level of the fingerprint. The result is valid and accepted as genuine if Equation 18 is satisfied. Also the result invalid and rejected as false or modified if Equation 19 is satisfied.

$$K_T \leq K_n \leq K \quad (18)$$

$$K_T > K_n > K \quad (19)$$

This technique would be used to detect the active and passive attacks on sensitive results and achieve data authentication, privacy, repudiation and integrity requirements of the e-voting system.

3. CONCLUSION

Every desperate and corrupt politician would like to win an election by all means even if it is to engage fraudsters and political thugs for snatching of ballot boxes and manually altered the sensitive results for personal gains. The results transported by cars or transmitted through public unprotected networks could be intercepted by fraudsters for either destruction or alteration. These unlawful acts of interception and alteration breach the integrity of data and could lead to a false winner in an election. This paper presented the use of fingerprints of polling officer (sender) and collation officer (receiver) to achieve data integrity requirement of e-voting system. The use of fingerprints of the polling and collation officers would securely establish the data integrity requirement of e-voting systems as against the use of numerical and textual data which could easily be guessed and attacked by the fraudsters for selfish gains. Any attacks on digitally signed results by fraudsters would produce invalid results because the fingerprints are not the same.

4. FUTURE WORK

The future work would focus on the implementation and evaluation of the technique presented in this paper using standard metrics to achieve data authentication, privacy, repudiation and integrity of e-voting system requirements.

Acknowledgement

The researchers acknowledge the persons whose photographs have been used in this research. Thank you for your co-operation.

REFERENCES

- [1] Varsha, N. G., Sangamesh, J., Shravya, R., & Shivaraja (2018). Aadhar based biometric voting system. *International Journal of Advance Research, Ideas and Innovations in Technology*, 4(3), 424–427.
- [2] Post-Election row hits APC. (2019, November 23). *The Nation*, p. 9.
- [3] Tony, A., Nicholas, K., & James, A. (2019, November 17). Violence, ballot box snatching mar polls. *The Nation*, p. 5.
- [4] Andrew, A., Yusha'u, A. I., Richard, P. N., & Abubaker, A. (2019, November 23). Appeal court upholds Ganduje, Tambual's election. *Daily Trust*, p. 7.
- [5] Adewale, O. S., Boyinbode, O. K., & Salako, E. A. (2019). A new metadata fusion technique for effective e-voting authentication. *African Scholar Journal of Pure and Applied Sciences (AJPAS)*, 15(9), 1–16.
- [6] King-Hang, W., Subrota, K. M., Ki, C., & Xiaoheng, X. (2017). A review of contemporary e-voting: requirements, technology, systems and usability. *Data Science and Pattern Recognition*, 1(1), 31–47.
- [7] Olayemi, M. O., Taliha, A. F., Aliyu, A., & Olugbenga, J. (2016). Design of secure electronic voting system using fingerprint biometrics and crypto- watermarking approach. *International Journal of Information Engineering and Electronic Business (IJIEEB)*, 8(5), 9–17, DOI: 10.5815/ijieeb.2016.05.02.
- [8] Prakhar, G., Rajesh, D., & Palak, L. (2015). A review on network security threats and solutions. *International Journal of Scientific Engineering and Research (IJSER)*, 3(4), 21–24.
- [9] Tutorialspoint (2019). Threats to Data Integrity. Retrieved November 22, 2019 from https://www.tutorialspoint.com/cryptography/data_integrity_in_cryptography.htm
- [10] Shilpa, P., Ashutosh, G., & Ratul, D. (2017). Different type network security threats and solutions, a review. *IPASJ International Journal of Computer Science (IJCS)*, 5(4), 1–10.
- [11] Sudeepthi, B., Imaduddin, M., & Kavitha, D 2014, 'Comparison of fingerprint minutiae matching technologies', *Journal of Electronics and Communication Engineering (IOSR-JECE)*, vol. 6, no. 6, pp. 71-76.
- [12] 12Nitin, C., Ajit, D., Simran, B., Shilpa, K., & Manjushree, M. (2017). Real-time voting system using biometrics. *International Journal of Scientific Engineering and Technology*, 6(12), 364–367.