International Journal on Advanced Science Engineering Information Technology

Vol.10 (2020) No. 1
ISSN: 2088-5334

Exploring the Use of Biometric Smart Cards for Voters' Accreditation: A Case Study of Nigeria Electoral Process

Akande Noah Oluwatobi[#1], Toba Paul Ayeni[*], Tayo Oladiran Arulogun[+], Adebiyi Ayodele Ariyo[^], Kayode Anthonia Aderonke[#]

[#] *Data and Information Security Research Group, Computer Science Department, Landmark University, Kwara State, Nigeria*
Email: [1]akande.noah@lmu.edu.ng

[*]*Department of ICT/Voters' Registry, Independent National Electoral Commission, Ekiti State, Nigeria*
Email: tobyeni@yahoo.com

[+]*Computer Science and Engineering Department, Ladoke Akintola University of Technology, Oyo State, Nigeria.*
Email:otarulogun@lmu.edu.ng

[^]*Department of Computer and Information Sciences, Covenant University, Ota. Nigeria*
Email: ayo.adebiyi@covenantuniversity.edu.ng

***Abstract*— Voting remains an integral component of every democratic electoral process. it is an avenue for citizens to exercise their rights in order to elect those who will lead them in various vacant political offices. However, enhancing voters' trust and confidence in electoral processes are significant factors that could encourage the active participation of citizens in elections. Eligible voters tend to decline to participate in an election when they have a feeling that their votes may not eventually count. Furthermore, electoral processes that lead to the emergence of candidates must be adjudged to be free, fair and credible to a high degree for the result to be widely acceptable. Unacceptable election results could lead to protests and total cancelation of the election thereby resulting in loss of time and resources invested in it. To ensure that only registered voters cast their votes on election days, measures must be put in place to accredit voters on election days effectively. Therefore, this article explores the use of biometric smart cards for voters' verification and identification. With the Nigerian electoral process in view, the existing Nigerian voting procedure was reviewed, lapses were identified and solutions based on the use of the biometric smart card were proffered. If adopted, the proposed adoption of biometric smart cards for voters' accreditation will enhance the country's electoral process thereby ensuring that only registered voters cast their votes. The approach presented could also reduce the number of electoral processes and personnel required during election days, thus reducing voting time and cost.**

***Keywords*— data security; information security; Nigeria elections; permanent voters card (PVC); smart card reader; vote buying.**

I. INTRODUCTION

Biometric systems have come to stay as a secure way to guarantee confidentiality, maintain integrity and ensure the availability of an individual's data and information through identification and verification processes. Verification is one to one security procedures aimed at affirming if the identity of a user belongs to him. In the voting context, it helps to affirm that voters that troop out to vote on election day are the actual eligible voters that registered before the voting day. In contrast, identification is one too many security procedures that attempt to assert the identity of an individual among many other individuals. In the voting context, voters' verification helps to confirm if voters that presented themselves on election day are registered voters among other registered voters. These two processes are very germane to the credibility of an electoral process and the eventual result that arises from the process. A series of consecutive activities that result in voting on election day is complex; therefore, mechanisms must be put in place to guarantee the security, reliability, and auditability of the processes [15].

The advancement in Information and Communication Technologies (ICT) has led to the introduction of electronic voting (e-voting) or internet voting (i-voting) systems towards improving or gradually phasing off the archaic traditional system of voting. While e-voting entails the incorporation of ICT tools in the electoral process, i-voting involves the conduct of election over the internet.

Regardless of the electoral system adopted, authenticating and verifying the identity of voters remains a significant component of every credible electoral process. Besides, validating voters, time taken by an individual voter to complete the voting process need to be reduced to the barest minimum. Instances, where voter's verification or the actual voting requires a long period, could disenfranchise some voters from participating in the election [38]. With an emphasis on the 2019 Nigeria general election, the country's electoral body- Independent National Electoral Commission (INEC) revealed that a total of 84 million people applied for Permanent Voters Card (PVC). Of these, 86.63% collected their PVC, perhaps intending to participate in the election holding across 119,973 polling units in the country (INEC, 2019). This connotes that an average of 607 voters is expected to be accredited to vote between 8 am and 2 pm. If the validation process is not fast or there are logistic challenges, then not all registered voters will be accommodated.

However, not all registered voters will eventually participate in the election; an entire electoral process should make provision for all registered voters. Every e-voting system should be tailored towards providing ease of voting, maintaining the integrity of the voting process, facilitating the speedy release of election results, decreasing the time needed to cast and count the vote, reducing the cost of the election process and increase the accuracy of the results [1]. The adoption of e-voting systems could increase participation of eligible voters in the electoral process as well as yielding an improved election outcome [2]. Similarly, the introduction of e-voting could significantly lead to the massive turn out of young, educated and internet-ready proportions of registered voters [30]. This is major because its introduction will earn voters' trust in the credibility of the voting process, thereby assuring voters that their votes are secured and will eventually count. Examining the distribution of registered voters released by Nigeria's INEC revealed that 26.57% of registered voters are largely young students, educated and internet ready. This is followed by farmers (16.23%), housewives (14.10%), business (12.87%), traders (9.01%), civil servants (6%), artisans (5.33%), public servants (2.73%) and others (7.17%).

Therefore, if introducing e-voting could cause a massive turn out of the youths, then every serious-minded government should be interested in adopting it. E-voting systems are not entirely free from attacks. Three sources of attacks are from voters with forged identifiers, poll workers who have access to storage media, and voting device developers [36]. Therefore, every e-voting system must be designed to curtail these sources of attacks. With an emphasis on effective accreditation of voters to ensure that only registered voters cast their votes once, biometrics cum smart card technology could be employed as a way out. It involves the use of unique human physical, behavioral and chemical characteristics in validating the identity of its users. These characteristics aptly called biometric traits to include iris, fingerprint, retina, palmprint, face, etc. Since no two human beings can have the same biometric traits, they have been widely employed in validating voters' identity [5], [14], [26], [35]. Smart cards simply credit card-sized plastic cards that have an embedded Integrated Circuit (IC) for data storage and retrieval. Recently, these two technologies have been merged to invent a biometric smart card. This special smart card has an IC that could be used for storing data as well as a fingerprint sensor for authenticating the identity of an individual. This article intends to explore the use of this biometric smart card for voters' authentication and verification during elections.

II. Materials and Methods

To have a better grip on the challenges bedeviling electoral processes via e-voting in Nigeria, the principles and internationally acceptable world standards were extensively studied and solutions were proffered based on the findings deduced.

A. Functional Requirements of an E-Voting System

Several works of literature have proposed different desirable features that any e-voting system should be designed to exhibit [2], [24], [33], [36], 37]. These features include:

1) Integrity: this feature maintains the sanctity of a vote cast; it ensures that a vote cased must not be altered or manipulated in any way. Once the vote is valid, it must be upheld as valid and must count as a valid vote. Also, should a vote cast be invalid, such vote should never be adjudged to be valid.

2) Authenticity: this feature emphasizes that, before voters can cast their votes, they must declare their identity. Having met all criteria, the same voter that registered to vote must be the same voter that came to vote on the election day. Voting cannot be done by proxy; hence;, mechanisms must be put in place to guarantee the authenticity of voters participating in an election process.

3) Eligibility: Certain conditions would have been set before the election as regards those who can vote and those who cannot vote. Therefore, only eligible voters must be allowed to vote, and no disenfranchisement should be allowed.

4) Privacy: this stipulates that there should not be any form of interference that could alter or influence voters' choice of the candidate while the vote is being cast. Voting must be done openly but in secret. After voting, nothing should be able to link voters to their votes.

5) Uniqueness: a voter is expected to cast a single vote for a candidate. No voters should be allowed to vote more than once for the same candidate. Also, under no circumstance should a voter be allowed to re-cast a vote. Voting should be a once and for all processes. Therefore, every e-voting system should be tailored to guarantee this.

6) No receipts: it is not a desirable feature for voters to be able to prove to a third party whom they vote for. Mechanisms must be put in place to guarantee that no third party will be able to view the content of a ballot while the election is still ongoing. Also, after the election, no one should be allowed to trace a vote to a voter.

7) Mobility: this emphasizes that voters should be able to cast their votes anywhere. There should not be a designated

location where voters should cast their votes. A location bound voting exercise has been proved to lead to voters' disenfranchisement. So, a voting exercise should be simple, flexible, and easy enough for any eligible voter to participate. The voting exercise should come at a minimal and affordable cost to voters. Therefore, voting centers should be designated at places closer to voters. For instance, there could be dedicated voting centers to students most especially private Universities students who may not be allowed to exit their campuses to participate in the election.

8) Uncoercibility: voters must not be forced to vote. Their choice on whom to vote for on election day should not be influenced in any way.

9) Fairness: while voting is ongoing, no individual should be able to predict or reveal the result of the election until the voting process has been completed. Releasing partial results of elections could cause a swing in a vote to be cast. Voters should have a mind that their candidate will win as no voter wants to vote for a candidate that will eventually lose. Therefore, in the spirit of fairness, partial results of the election should not be released until the whole election process is complete.

10) Completeness: A voting system is acclaimed to be complete if all valid votes are counted and count; if no valid vote is disqualified and if invalid votes remain invalid.

11) Usability: The tools that will be used in the election process should be simple enough for voters to use. Instructions on how to use these tools must have been properly spelled out before the election day. This could be achieved through voters' education and orientation before the election day.

12) Verifiability: voters must be able to ascertain that their valid votes cast reflected in the result declared. An assurance that all valid votes will count will encourage eligible citizens to participate in elections.

13) Fault tolerance: a perfect e-voting system must be able to be robust to a great extent. It must not breakdown frequently. Should its breakdown, a fail-safe mechanism must be in place to guarantee that the breakdown will be temporary and the system will eventually be restored. Mechanisms must be put in place to guarantee that a breakdown of any tool in use will not undermine the electoral process.

14) Multi-user: an e-voting system should be able to accommodate any number of eligible voters that are interested in participating in an election.

15) Multi-election: an e-voting system should be a guarantee that multiple elections can take place simultaneously at different accredited locations.

B. Nigerian Voting Procedure

Polling stations on election day are expected to be opened for accreditation and voting between 8:00 am to 2.00 pm. The voting process can be divided into four main stages:

- PVC verification
- Voters fingerprint authentication using SCR
- Voters' details confirmation on the voters Register and inking of the voters' cuticle
- Issuance of the ballot paper and proceeding to the voting dock to cast a vote

Voters, Assistant Presiding Officer III (APO III), Assistant Presiding Officer II (APO II), Assistant Presiding Officer I (APO I), and the Presiding Officer (PO) are the main actors during the voting process. On arriving a polling unit, voters are expected to be on a queue for the accreditation and voting exercise.

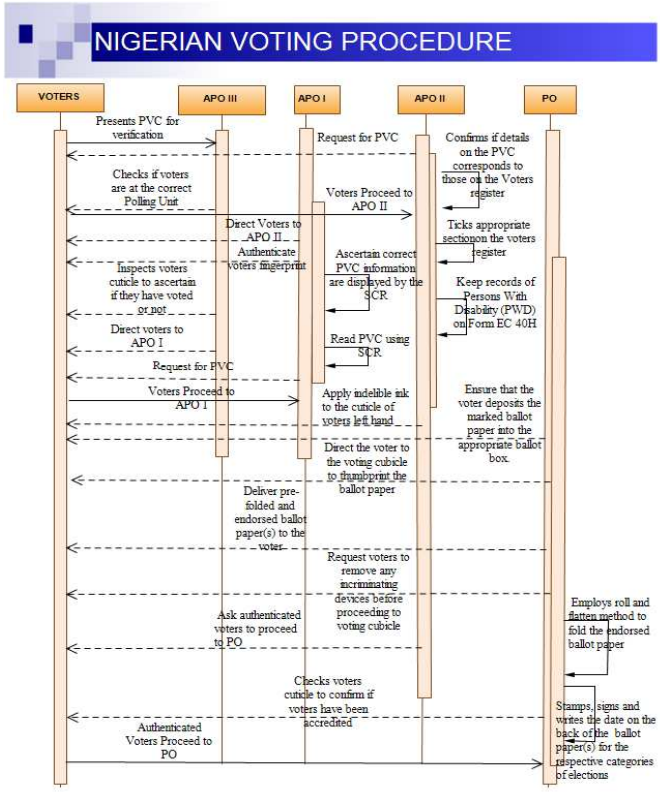

Fig. 1 Sequence Diagram for Nigerian Voting Process

Fig. 1 presents a sequence diagram that exhaustively illustrates the series of activities that a voter must go through in order to cast his vote.

C. Challenges of Nigerian Voting System

Nigeria- the most populous country in Africa and seventh in the world remains the fastest growing population in the world [44]. Her population remains her major source of strength and yet reasons for her impending challenges in every sector of the economy. With an emphasis on the Nigerian electoral process, there have been gradual improvements based on the challenges we face each election year. Recently, the new turn to our electoral challenges in Nigeria is "vote-buying". It could be as old as democracy itself as instances where participants or parties use money or material things to influence voters' decisions have been around for a long time [8]. It is an act of presenting material gifts or cash to voters in exchange for their votes during elections [19]. Vote-buying [21] is defined as:

> *"a form of political clientelism which characterizes instrumental and reciprocal relationships of mutually*

beneficial exchange between actors of unequal social, economic, and political status."

It is illegal and unexpected behavior that should not be exhibited among actors (voters, politicians and electoral body) in any democratic setting. Despite the adoption of secret balloting, vote-buying thrives across nations of the world [19]. Another study identified other forms of vote-buying [31], such as: distributing contingent benefits to legislators (legislative vote-buying), providing infrastructure projects in regions with opposition members to win their political support (non-excludable vote buying) and sharing material benefits to individual, groups of people or organization without necessarily mandating them to provide political support (non-binding vote-buying). Interestingly, all these forms of vote-buying have characterized and marred the Nigerian electoral process. However, Nigeria is not the only African country where vote-buying thrives; a survey carried out [39] as shown in Fig. 2 on vote-buying thrives across many African countries.

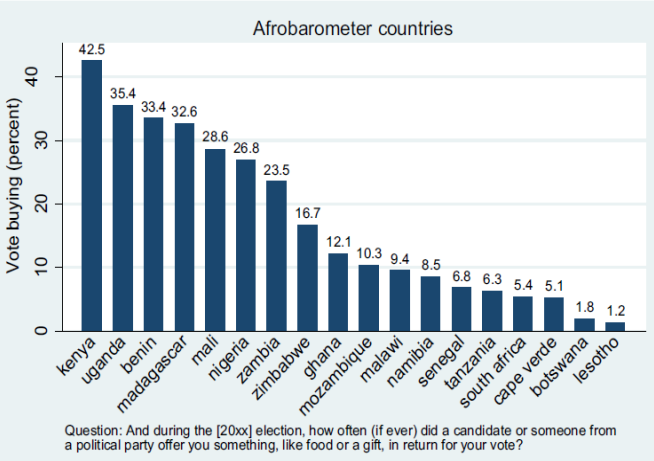

Fig. 2 Trends of Vote Buying in African Countries [21]

Besides Africa, cases of vote buying have been reported in countries like Jordan [25], Argentina [6], Lebanon [13], Mexico [28], Taiwan [48], Philippines [16], [22], [40] and Latin America [11].

Vote-buying flourishes in countries where the principles of secret balloting are not strictly adhered, and party agents could monitor how voters cast their votes [23]. Also, the level of information voters has about contestants could determine if vote-buying will thrive or not. Should voters know that an incumbent has not performed to expectation, they could demand a higher price in exchange for their votes and still refuse to vote for them. However, in instances where voters have little information about contestants, they could go-ahead to sell their votes at any price. Above it all, greater poverty [40], [42] and lack of basic social amenities are major factors facilitating the growth of vote-buying. Nevertheless, vote-buying may be minimal in urban areas compared to rural areas [9].

Recently, a new twist to the problems bedeviling our voting system is different cases of stolen PVC reported few days to the 2019 general election. These stolen PVC could be distributed to voters to influence election results in favor of a particular aspirant. The e-voting system being practiced in Nigeria has not fully mandated biometric authentication as a requirement for voting. It laid more emphasis on PVC authentication than voters' biometric authentication via fingerprint. According to section 11(b) and (e) of the election guideline released by INEC, it says:

"11b) Where a voter's PVC is read but his/her fingerprint is not authenticated, the APO I shall refer the voter to the APO II who shall: (i) request the voter to thumbprint the appropriate box in the Register of Voters; (ii) request the voter to provide his/her phone number in the appropriate box in the Register of Voters; (iii) continue with the accreditation of the voter, and (iv) refer the voter to the PO or APO (VP) for issuance of ballot paper(s)"

"11e) Where a voter's PVC is read and the SCR shows the details of another person, rather than the details of the cardholder as printed on the PVC, the APO I shall: (i) Refer the voter to APO II to confirm that the details of the voter in the Register of Voters correspond to those on the PVC; (ii) APO II if satisfied that the holder of the card is on the Register of Voters, shall record the phone number of the voter in the appropriate box on the Register of Voters, and (iii) Proceed with the accreditation of the voter "

These loopholes could be explored in rigging the election. Unfortunately, some logistic challenges that led to the postponement of elections in 2015 general elections still surfaced during the 2019 general elections. Cases of malfunctioning smart card readers perhaps as a result of empty batteries or the failure of the SCR in accrediting voters fingerprint; late arrivals of INEC officials as well as voting materials, inability of registered voters to find their names on the voters' register, snatching of ballot materials are some inadequacies that sprung up even in the 2019 general elections. Voters' education remains an integral component of any electoral process that could ensure that votes eventually cast count. It could significantly reduce the number of invalid votes that will be canceled. Before elections, voters ought to be oriented about how to vote, the right finger to use (the use of thumb was discouraged in 2019 general elections as the number of parties participating in the election was many and the space allotted for thumb printing was small), the right ballot paper to use for respective candidate.

Due to the number of political offices available, three different political offices were voted for on the first election day. However, the ballot paper for each elective post was the same though the ballot boxes were different. Hence, many voters had to check the ballot paper after thumb printing before dropping it inside the ballot boxes. This act violates the principle of the secret ballot system in which adequate voters' education would have possibly eliminated. Furthermore, the Nigerian voting system is characterized by different cases of over-voting on election days. This could connote instances where the total number of votes cast at a polling unit exceeds the number of registered voters in the Polling unit. This could also be seen in cases where the total number of votes cast at a Polling unit exceeds the total

number of accredited voters [17]. In the Nigerian context, over voting always result from the manipulation of PVC, SCR, and the Electronic Voters Register (EVR). This will be greatly minimized when EVR is completely replaced with BSC.

D. Existing Solutions to Challenges faced by Nigerian E-voting System

Several proposals aimed at improving the present Nigerian e-voting system have been put forward by various researchers. Human control and manipulation of specific technological devices are one of the challenges of the Nigerian e-voting system [45]. Therefore, an automated polling system that minimizes human supervision thereby guaranteeing transparency and accuracy of the voting process was proposed. For literate voters in internet-enabled areas, ATM internet-enabled voting, mobile internet voting and internet-enabled polling units were proposed. However, for illiterate voters in internet-enabled areas as well as remote areas, the standalone electronic voting unit was proposed. A framework for the Nigerian e-voting system was presented in [32]. PVC was retained for voters' authentication while Direct recording electronic voting machines was proposed for balloting.

Similarly, a biometric framework for e-voting was proposed [5]. Voters' authentication and the actual vote casting were to be done via voters' fingerprints. Internet availability and constant power supply are critical factors that will determine the success of the proposed approach. The huge cost of printing ballot papers used during elections was identified [3] as a major area of concern to the Nigerian electoral system. Therefore, the possibility of casting a vote via an android application was proposed. The android application uses the Global Positioning System (GPS) feature of the phone to retrieve the voters' location. A timer to keep track of the time frame and system status that could be used to activate or deactivate the application.

However, the usability of the application in remote areas was not addressed and the literacy level of the voters remains an issue of concern. Security remains a major issue of concern for every e-voting system. Therefore, a secured e-voting system that uses fingerprint and crypto-watermarking was proposed [34]. Voters' authentication was carried using their fingerprints. After successful authentication, access will be granted to the e-voting software application. Afterward, two-layer security through Advanced Encryption Standard (AES) cryptographic technique and wavelet-based watermarking were employed to ensure the integrity and confidentiality of the vote cast. In the same vein, a bio-cryptographic e-voting system was proposed [29]. The proposed technique employed voters' fingerprint for authentication and Lifting Wavelet Transform (LWT) based Steganographic video algorithm for securing votes cast. Firstly, the digital ballot was hashed using the SHA-512/256 hashing technique; the resultant hashed ballot was then embedded in a cover video before transmission. During the auditing process of the vote cast, the extracted ballots are compared with the hashed ballot in order to ascertain the integrity of the votes cast.

III. Results and Discussion

This study proposed Biometric Smart Card (BSC) as a tool that could be used to verify the authenticity of voters participating in electoral processes on election day. It could be programmed to store voters' biographic details as well as a fingerprint that could be used for their verification on election day.

A. Biometric Smart Cards

A Biometric Smart Card (BSC) is simply a smart card that possesses a biometric sensor (majorly fingerprint sensor for now) and can self-authenticate itself. Biometric security entails capturing the needed biometric trait, pre-processing the captured trait, extracting features from it, template generation and finally template matching; all these stages are also carried out within the BSC. The data capturing and matching stages using a smart card is illustrated in Fig. 3. Before the introduction of BSC, two similar concepts have been introduced: The Template on Card (ToC) and Matching on Card (MoC) approach.

1) Template on Card Approach: ToC approach offers an additional way to authenticate the identity of a user by retrieving and storing a specific biometric trait of the user on the smart card as in Figure 3 below.

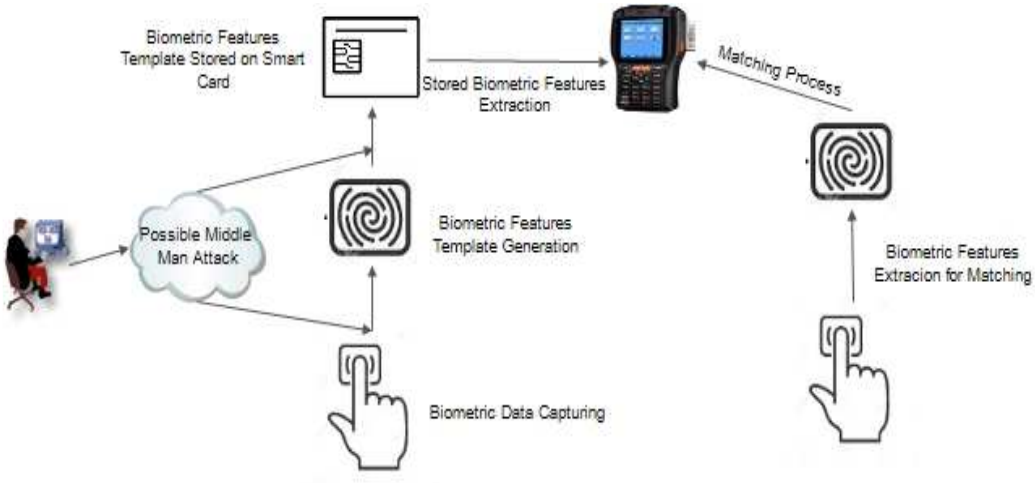

Fig. 3 Template-on-Card Approach

Separate biometric sensors are used to retrieve the biometric trait while the retrieved traits are then stored on the secure element segment of the smart card. This is illustrated in Fig. 3; such was implemented in the form of extracted iris features were saved on the smart card [27]. Another study [10] also saved facial features on smart card chip; extracted features of sclera and ear were stored on smart card chips [43], and another study [46] stored extracted fingerprint features on smart cards. Unlike a BSC where all the biometric features acquisition stages are done on the smart card, the ToC approach uses a separate biometric sensor to retrieve and generate the features template to be stored on the smart card. During matching, the features stored on the smart card are retrieved and compared to the features extracted at the authentication point.

2) Matching on Card Approach: ToC approach only guarantees the security of the biometric template stored on the smart card and exposes the matching template to an open environment, as in Figure 4.

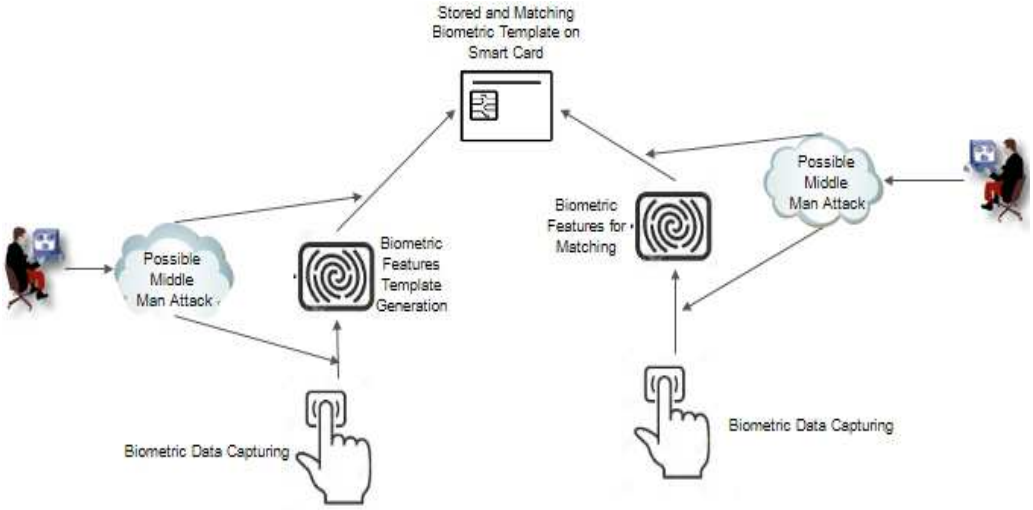

Fig. 4 Matching-on-Card Approach

As a result of this, Matching-on-Card (MoC) approach was introduced to ensure the maximum security of the stored biometric template as well as the matching template. Unlike, ToC approach where the matching is done on a separate biometric sensor, matching is done on the smart card in the MoC approach. To achieve this, both biometric templates are stored on the smart card [12], [20], [47]. However, since a separate biometric sensor will initially acquire the biometric traits before being stored on the smart card, an intruder could retrieve the template. Fig. 4 illustrates the MoC approach.

B. Structure of a Biometric Smart Card

Unlike the existing smart card, BSC has some additional components such as a biometric sensor, secure element, battery, power button, status Light Emitting Diodes (LED), sensor controller, a digital display etc. As shown in Fig. 5, a BSC could have a flat non-replaceable and non-rechargeable battery that can provide 3 to 5 years' operation life under normal usage conditions or a supercapacitor that can absorb charge from the card reader to power the smart card's chip as well as the sensor. As a result of this, a power button is used to switch the card on or off. A status LED is used to show the state of the BSC; when it is booting, the orange light is seen which becomes green when it is active.

When the power button is pressed, the green led turns red. The BSC's buzzer beeps when the card is being used; this is used to communicate with the user. The length and number of beeps specify the particular operation the BSC is presently undergoing. Besides, a BSC has a digital display that could display if the BSC is on or off. The activities of the major components of the BSC are synchronized by different Integrated Circuits (IC) that are available on the smart card. Such as RF IC used to control the BSC's antenna; the display driver IC that controls the digital display; fingerprint sensor IC that controls the fingerprint sensor.

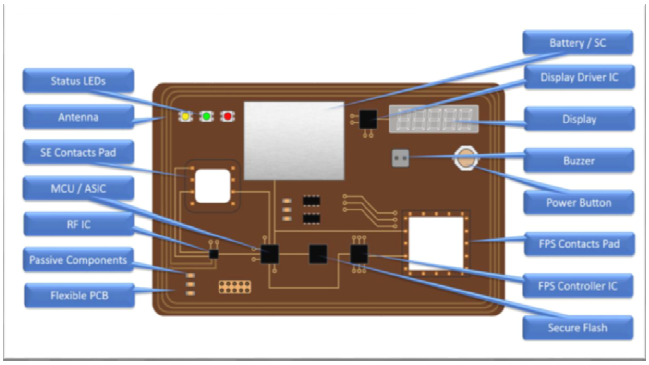

Fig. 5 Structure of a Biometric Smart Card [7]

C. Features of Nigerian Smart Card Reader (SCR)

The SCR shown in Fig. 6 is an Emp5500 device that uses a highly secure cryptographic technology. It has ultra-low power consumption, with a Dual Core Cortex A7 Central Processing Unit (CPU), a single-core frequency of 1.2GHz, a baseband version MOLY.WR8.W1315.MD.WG.V23 and an Android 4.2.2 operating system [33]. In addition to these specifications, it has a screen touchpad through which its icons can be activated; a speaker for generating voice prompts like indicating a successful accreditation; keypads as an input device; a card slot for reading the PVC; a fingerprint sensor for reading voters fingerprints; a USB port

for connecting it to a personal computer for configuration purposes and a 4000mAh battery that can last for about 24 hours when fully charged. The device hibernates when not in use to save and lengthen its battery life. Once configured, the SCR can only read PVCs issued by INEC. The SCR also has a fingerprint sensor with which fingerprints of voters' can be authenticated. The SCR also keeps the statistics of PVCs successfully read or rejected on election days. These transmitted to a central INEC server via its GSM data service. Information transmitted to the server is used by INEC to audit results from polling units and other statistical analysis that may be needed by the electoral body.

Fig. 6: Nigerian Smart Card Reader [33]

D. Accreditation Procedure with the Smart Card Reader

When an accreditation officer successfully logs in to the SCR, the home page of the SCR with six icons will be displayed, as shown in Figure 8. The verification icon is used for voters' verification and fingerprint authentication. The query icon is used to check the database for Voters Identification Number (VIN) and their accreditation status. The communicate icon is used to transfer accreditation statistics to INEC's backend server while the Close-V icon is used for closing accreditation at the end of the poll.

Voters' accreditation with the SCR on the election day can be divided into three steps:

1) Verification: On the election day, an attempt will be made to establish the originality of the PVC when inserted into the SCR. When the verification icon on the SCR is selected, the page shown in Figure 8 will be displayed. Afterward, the first icon at the bottom of the screen will be tapped once to display voter's as shown in Fig. 7.

Fig. 7 SCR's Verification Page [18]

2) Voters' Identification: this is achieved by comparing the voter's face to the image available on the PVC. Afterward, the face of the PVC holder is compared with the image displayed on the SCR when the PVC has been inserted into it. This is illustrated in Fig. 8:

Fig. 8 SCR showing Voter's Details

3) Authentication: - a biometric authentication procedure using a fingerprint is carried out to affirm the identity of the voter further. With the smart card still in the SCR, voters are expected to put their fingers on the SCR and the authentication icon is clicked. The fingerprint features stored on the PVC are then compared with those extracted during the accreditation exercise. If the accreditation is successful, a green circle with a green mark as shown in Figure 8) is displayed else a red circle with an exclamation mark as shown in Figure 9) is displayed. Once a PVC has been read and accredited by the SCR, the Voter Identification Number (VIN) is stored on the SCR and subsequent accreditation on that same day will not be allowed by the SCR. Under normal circumstances, the accreditation process is expected to take an average of 10 to 20 seconds per voter. To prevent fraudulent use of the SCR, the device is configured to work with PVC's of assigned polling units except otherwise reconfigured by authorized INEC personnel.

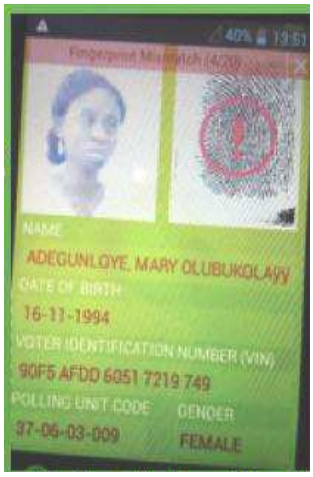

Fig. 9 Failed Authentication Process [18]

E. How Smart is Nigeria's Permanent Voters Card

In quest to achieve a free, fair and credible election that will produce peoples' preferred candidate during the election; PVC, as well as smart card reader, was introduced in 2015 general election. Its usage greatly reduced the rate of rigging that would have occurred and led to the election being adjudged by many local and international observers as being fair to some extent [4]. It was used to replace the temporary voters' card that was given to voters in 2011. It is meant to be a means of identifying registered voters and it is expected to be valid for at least ten years. The PVC as shown in Fig. 10 has specialized features such as base substrate; high technology watermarked printing features and lamination as well as an embedded chip [17].

Fig. 10 Nigerian Permanent Voters Card

The embedded chip is expected to store voters' biometric traits, demographic data, and personal voting information. The PVC has been programmed in such a way that it can only work on election days and the smart card reader could read the only PVC issued by INEC. However, several cases of PVC theft in large volumes reported before the 2019 general election has signified attempts by certain group of individual to use the stolen PVC to influence the results of the 2019 general elections. A few days to the 2019 general election, cloned samples of PVC were seen listed for sale on a popular Chinese e-commerce website. How the stolen PVC could be used to undermine the integrity and credibility of the election remains a mystery waiting to be unraveled.

What makes a card smart is the presence of the Integrated Circuits (IC) chip embedded into it. That led to the questioning of if the PVC is a smart card is claimed to be. Physical examination of the PVC revealed that besides the barcodes and different embossed images, it has no IC chip embedded into it; therefore, it does not satisfy the requirements of being a smart card as documented in ISO/IEC 7810 specification. There are several other cards according to ISO/IEC 7810 specification which are machine-readable cards without magnetic stripes that could be used for identification purposes. Such cards could also have images embossed on them with barcodes to store information. This specification perfectly matches the features of the current PVC being used by INEC. If these observations are to be true then the current PVC is not totally safe from being acquired, reprogrammed and used to rig elections. To curtail this, the feasibility of adopting a smart card reader as a perfect replacement for the current PVC is being explored in this article.

F. Biometric Smart Cards Authentication Framework

A BSC could be the solution to recent attempts to use stolen PVCs to rig elections as reported few days to the Nigerian 2019 general elections. Should a BSC be stolen, it cannot be used to rig elections as voters' authentication will be done simultaneously as the BSC is being verified. With this technique, fingerprint authentication becomes an integral component of the electoral process. Also, the use of BSC could reduce the time taken to accredit voters and the number of electoral processes involved. In the existing electoral process shown in Fig. 1, 25 processes must be carried out by four electoral officers before the voting process will be complete. This can be reduced to 15 processes with two electoral officers if BSC is employed. A BSC can be programmed to handle more information than any other store cards. Two polling officers can adequately handle the electoral processes as against four used in the existing voting procedure. Activities assigned to APO III and APO II are those that can be handled by two polling officers one the BSC has been programmed to handle them. Also, the manual examination of voter's details in the voters' register after PVC verification and fingerprint authentication can be totally eradicated. This marred the results of 2019 general elections as many voters whose PVC were confirmed to be authentic and whose fingerprint authentication was successful were not allowed to vote because their names were not on the manual voters' register. The BSC can be programmed to be the only authentication device to be used on election day. After inserting the BSC into the SCR, voters can be asked to place their thumb on BSC's fingerprint sensor for fingerprint authentication. Immediately after this, the next icon that will generate the voters' registration details can be clicked to pop up this information. The information could include Polling Unit ID that will be used to ensure that the voter is voting at the right polling unit, voters photograph (although, if the fingerprint authentication is successful, there may be no need to check voters photograph), voters' identification number, voters PWD status etc. All these electoral processes can be divided into stages to be carried out on the SCR by a single polling officer. Similarly, the SCR can be programmed to automatically generate other information that may be required to carry out post-election auditing once the voting process for each voter has been terminated. Furthermore, the post-election data transmitted to INEC's central server can be used to validate the results announced at the polling units and those eventually announced at the central collating centers in different states perhaps before announcing the results.

So, as illustrated in the sequence diagram depicted in Fig. 11. APO is expected to be the authentication officer in charge of SCR's operations. He is expected to request for voters PVC, slots it into the SCR, request voters to place their fingers on the BSC's fingerprint sensor for authentication, confirms other required information required on the SCR, then paints the cuticle of the voters to indicate a successful authentication process. Afterward, the PO is expected to stamp, sign and write dates on the back of the ballot paper(s) for the respective categories of elections. He is also expected to employ roll and flatten method to fold the endorsed ballot paper, deliver pre-folded and endorsed ballot

paper(s) to the voters, request voters to remove any incriminating devices before proceeding to voting cubicle, direct the voter to the voting cubicle to thumbprint the ballot paper and finally ensures that the voter deposits the marked ballot paper into the appropriate ballot box. With these, it is believed that the time required to complete a voting process will be reduced, the number of voting processes will be reduced, the cost of personnel required at polling units will also be reduced and a more credible accreditation process will be achieved.

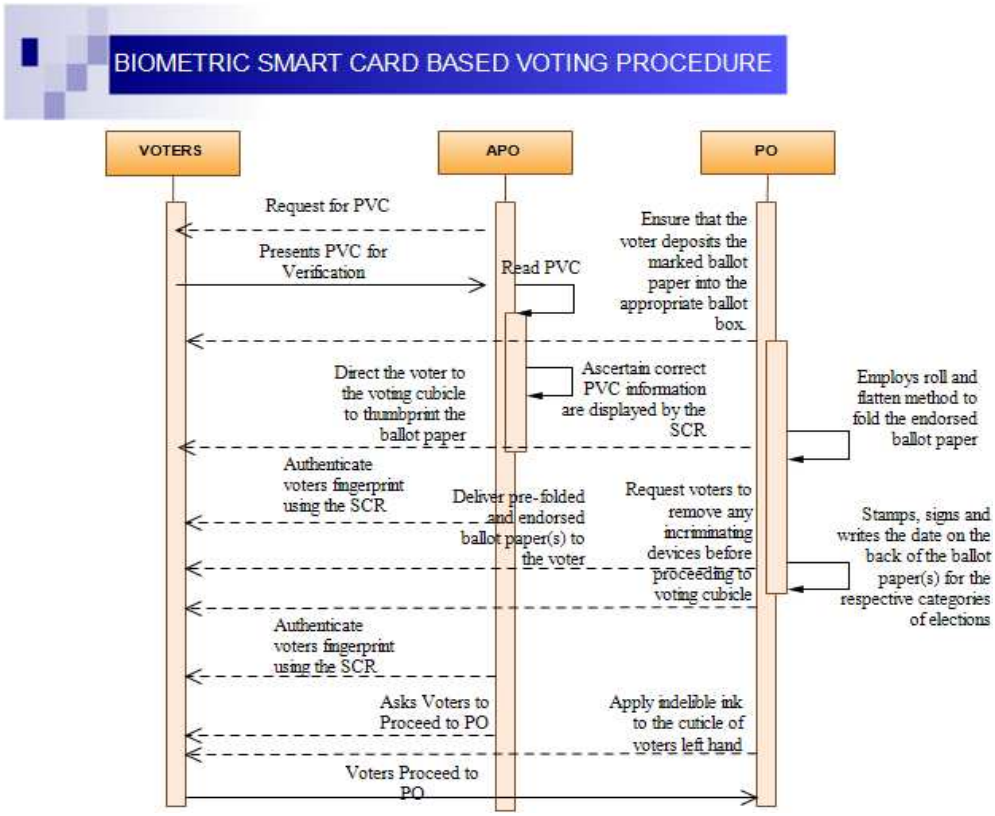

Fig. 11 Proposed Biometric Smart Card Authentication Procedure

IV. CONCLUSION

A free, fair, and credible electoral process must be put in place for the outcome of an election to be acceptable. This article as discussed extensively the challenges bedeviling Nigerian electoral process and the modus operandi of the adopted e-voting system. The article identified voters' accreditation process as an essential process that must be improved upon for the result of an election to be adjudged free, fair and credible. A biometric smart card authentication technique for voters' accreditation has been proposed and the modality for its use in the Nigerian context has also been provided. If adopted, the BSC authentication technique could help ensure that only registered voters can vote on election days. Furthermore, the proposed accreditation technique could reduce the number of personnel and electoral processes required for the accreditation process.

ACKNOWLEDGMENT

Authors appreciate Landmark University Centre for Research and Development, Landmark University, Omu-Aran, Nigeria, for fully sponsoring the publication of this article.

REFERENCES

[1]. Abosamra, K. M., Abdelhafez, A. A., Assassa, G. M. R., & Mursi, M. F. M. (2017). A practical, secure, and auditable e-voting system. *Journal of Information Security and Applications*, *36*, 69–89. https://doi.org/10.1016/j.jisa.2017.08.002

[2]. Adeshina, S. A., & Ojo, A. (2017). Factors for e-voting adoption - analysis of general elections in Nigeria. *Government Information Quarterly*, (November 2015), 1–12. https://doi.org/10.1016/j.giq.2017.09.006

[3]. Adeshina, S. A., Ismaila, L. E., Ibrahim, K. U., & Ojo, A. (2017). Design and Implementation of Electronic Ballotting System; A case study of Nigeria. International Journal of Computer Techniques, 4(1), 1–8.

[4]. Agbu, O. (2016). Election Rigging and the Use of Technology: The Smart Card Reader as the Joker in Nigeria's 2015 Presidential Election. *Journal of African Ellections*, *15*(2), 90–111. https://doi.org/10.20940/JAE/2016/v15i

[5]. Akintoye, K. A., & Araoye, O. I. (2015). A Biometric E-voting Framework for Nigeria. *Jurnal Teknologi*, *77*(13), 87–91.

[6]. Auyero, J., 2001. Poor People's Politics: Peronist Survival Networks and the Legacy of Evita. Duke University Press, Durham, NC.

[7]. Antonio D'Albore (2018), "How a Smart Card is made", accessed on 1st March, 2018. Available on https://embeddedsecuritynews.com/2017/03/how-a-smart-card-is-made-part-2/

[8]. Bradburn, N., S. Sudman, E. Blair, and C. Stocking (1978). Question threat and response bias. Public Opinion Quarterly 42(2), 221–234.

[9]. Bratton, M. (2008). Vote buying and violence in Nigerian election campaigns q. *Electoral Studies*, *27*(4), 621–632. https://doi.org/10.1016/j.electstud.2008.04.013.

[10]. Bourlai T., Kittler J. and Messer K. (2010), "On Design and Optimization of a Face Verification System that is Smart-Card-Based", Journal of Machine Vision and Applications, vol. 21, no. 5, pp. 695-711.
[11]. Carreras, M., & Irepo, Y. (2013). Trust in elections, vote-buying , and turnout in Latin America, *32*, 609–619.
[12]. Chen T. P., Yau W. Y., and Jiang X. (2015), "Fast match-on-card technique using in-matcher clustering with ISO minutia template," International Journal of Biometrics, vol. 7, pp. 119-146.
[13]. Corstange, D., 2012. Vote trafficking in Lebanon. Int. J. Middle East Stud. 44 (3), 483-505.
[14]. Enoch, J. D., & Saturday, N. R. (2017). Biometric Online Voting System in Nigeria, (July). https://doi.org/10.14445/22312803/IJCTT-V49P104
[15]. Fernandez, E. B., La, D. L., & Peláez, J. I. (2013). A conceptual approach to secure electronic elections based on patterns. *Government Information Quarterly*, *30*(1), 64–73. https://doi.org/10.1016/j.giq.2012.08.001
[16]. Hicken, A., Leider, S., Ravanilla, N., & Yang, D. (2017). Temptation in vote-selling: Evidence from a field experiment in the Philippines, *131*(August 2016), 1–14.
[17]. INEC, (2019). INEC explains a-z about an electronic card reader. Retrieved from https://thewillnigeria.com/news/inec-explains-a-z-about-electronic-card-readers/ on 19th Feb 2019
[18]. INEC Manual for Election Officials (2015): Funded by the European Union through the UNDP Democratic Governance for Development (DGD II) Project.
[19]. Khemani, S. (2015). Buying votes versus supplying public services: Political incentives to under-invest in pro-poor policies. *Journal of Development Economics*, *117*, 84–93. https://doi.org/10.1016/j.jdeveco.2015.07.002
[20]. Kishor Krishnan Nair, Albert Helberg and Johannes van der Merwe (2016), "An Approach to Improve the Match-on-Card Fingerprint Authentication System security", Sixth International Conference on Digital Information and Communication Technology and its Applications (DICTAP), Pp. 119-125.
[21]. Kramon, E. (2016). Where is vote buying effective? Evidence from a list experiment in Kenya. *Electoral Studies*, *44*, 397–408. https://doi.org/10.1016/j.electstud.2016.09.006
[22]. Labonne, J., Chase, R., 2011. Do community-driven development projects enhance social capital? Evidence from the Philippines. J. Dev. Econ. 96 (2), 348–358.
[23]. Lehoucq, F., 2007. When does a market for votes emerge? In: Schaffer, F.C. (Ed.), Elections for Sale: The Causes and Consequences of Vote Buying. Lynne Rienner Publishers, London, pp. 33-45
[24]. Li, C., Hwang, M., & Liu, C. (2008). An electronic voting protocol with deniable authentication for mobile ad hoc networks q. *Computer Communications*, *31*, 2534–2540. https://doi.org/10.1016/ j.comcom. 2008.03.018
[25]. Lust-Okar, E., 2006. Elections under authoritarianism: preliminary lessons from Jordan. Democratization 13 (3), 456-471.
[26]. Maria, L. (2008). Panama modernizes its national and voter ID system. *Biometric Technology Today*, (March), 2008.
[27]. Mohammed A. M. Abdullah, Al-Dulaimi F. H. A., Waleed Al-Nuaimy and Ali Al-Ataby (2015), "Smart card with iris recognition for high-security access environment", Proceedings in 1st Middle East Conference on Biomedical Engineering, IEEE Explore, Pp. 382-385.
[28]. Magaloni, B., 2006. Voting for Autocracy: Hegemonic Party Survival and its Demise in Mexico. Cambridge University Press, New York.
[29]. Mikail, O. O., & Arulogun, T. (2018). Bio-Cryptographic Technique for Secure Electronic Voting System Bio-Crystographic Technique for Secure Electronic Voting System. Advances in Electrical and Telecommunication Engineering, 1(2), 55–64.
[30]. Nemeslaki, A., Aranyossy, M., & Sasvári, P. (2016). Could on-line voting boost the desire to vote? – Technology acceptance perceptions of young Hungarian citizens. *Government Information Quarterly*, *33*(4), 705–714. https://doi.org/10.1016/j.giq.2016.11.003
[31]. Nichter, S. (2014). Conceptualizing vote-buying. *JELS*, *35*, 315–327. https://doi.org/10.1016/j.electstud.2014.02.008
[32]. Okediran, O. O., & Ganiyu, R. A. (2015). A Framework for Electronic Voting in Nigeria. International Journal of Computer Applications, 129(3), 12–16. https://doi.org/10.5120/ijca2015906786
[33]. Omolaye, P. O., Daniel, P., & Orifa, A. O. (2015). Systemic Evaluation of Semi-Electronic Voting System adopted in Nigeria 2015 General Elections, *3*(1), 15–21. https://doi.org/10.12691/ajis-3-1-2
[34]. Olaniyi, O. M., Folorunso, T. A., Ahmed, A., & Joseph, O. (2016). Design of Secure Electronic Voting System Using Fingerprint Biometrics and Crypto- Watermarking Approach. International Journal of Information Engineering and Electronic Business, 5(September), 9–17. https://doi.org/10.5815/ijieeb.2016.05.02
[35]. Philippe, W.-G. (2006). *Mexico deploys multi-biometric voting system*. *Biometric Technology Today*.
[36]. Pujol-ahullo, J., Castella, J., Viejo, A., & Jardı, R. (2012). Study on poll-site voting and verification systems, *1*. https://doi.org/10.1016/j.cose.2012.08.001
[37]. Qadah, G. Z., & Taha, R. (2007). Electronic voting systems: Requirements, design, and implementation, *29*, 376–386. https://doi.org/10.1016/j.csi.2006.06.001
[38]. Rae, L., Ann, L., Hall, T. E., Saunders, K. L., & Alvarez, R. M. (2010). A new barrier to participation: Heterogeneous application of voter identification policies. *Electoral Studies*, *29*(1), 66–73. https://doi.org/10.1016/j.electstud.2009.08.001
[39]. Sandholt, P., & Justesen, M. K. (2014). Poverty and vote-buying : Survey-based evidence from Africa, *33*, 220–232.
[40]. Schaffer, Frederic C., 2005. Clean elections and the great unwashed: vote-buying and voter education in the Philippines. Paper Number 21, April 2005. School of Social Science, Institute for Advanced Study, Princeton, NJ.
[41]. Schaffer, Frederic C., 2007. Elections for Sale: The Causes and Consequences of Vote buying. In: Schaffer, Frederic C. (Ed.), Lynne Rienner Publishers, Boulder, CO.
[42]. Stokes, S., 2005. Perverse accountability: a formal model of machine politics with evidence from Argentina. Am. Polit. Sci. Rev. 99 (3), 315–325.
[43]. Tamezheneal R., Sumathi S. (2017), "Implementation of the biometric smart card using multibiometrics", Proceedings of International Conference on Trends in Electronics and Informatics, IEEE Explore, Pp. 777-782, Pp. 1-5
[44]. United Nations, (2017). *World Population Prospects: The 2017 Revision, Key Findings and Advance Tables* (No. ESA/P/WP/248.).
[45]. Uzedhe, G. O., & Okhaifoh, J. E. (2016). A Technological Framework for Transparent E-Voting Solution in the Nigerian Electoral System. Nigerian Journal of Technology (NIJOTECH), 35(3), 627–636.
[46]. Victor Teoh De Zhi and Shahrel Azmin Suandi (2015), "FingerCode for identity verification using fingerprint and smart card", Proceedings in 10th Asian Control Conference (ASCC), Pp.1-6.
[47]. Vibert B., Rosenberger C., and Ninassi A. (2013), "Security and performance evaluation platform of a biometric match on the card," World Congress on Computer and Information Technology (WCCIT), pp. 1-6.
[48]. Wang, C.S., Kurzman, C., 2007. The logistics: how to buy votes. In: Schaffer, F.C. (Ed.), Elections for Sale: The Causes and Consequences of Vote Buying. Lynne Rienner Publishers, London, pp. 61-78.