I.J. Information Engineering and Electronic Business, 2020, 1, 19-29
Published Online February 2020 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijieeb.2020.01.03

A Review of Electronic Voting Systems: Strategy for a Novel

Prof. Adewale Olumide S.
Department of Computer Science, School of Computing, Federal University of Technology, Akure, Nigeria
Email: adewale@futa.edu.ng

Dr. Boyinbode Olutayo K.
Department of Information Technology, School of Computing, Federal University of Technology, Akure, Nigeria
Email: okboyinbode@futa.edu.ng

Salako E. Adekunle
Department of Computer Science, School of Computing, Federal University of Technology, Akure, Nigeria
Email: salakoea@futa.edu.ng

Received: 02 June 2019; Accepted: 17 November 2019; Published: 08 February 2020

***Abstract*—**The voting system in the world has been characterised with many fundamental challenges, thereby resulting to a corrupt contestant winning an election. Researchers have been emotionally, physically, socially and intellectually concerned about the election malpractices recorded at various levels of electing a representative. Questions on how corrupt stakeholders in elections could be prevented from fraudulent activities such as rigging and impersonation called for discussion and answers. Consequences of declaring a corrupt contestant as a winner are bad governance, insecurities and diversification of public funds for personal gains. There must be approaches to tackle the problems of voting systems. This paper focused on a comprehensive review of electronic voting systems by different scholars as a platform for identifying shortcomings or drawbacks towards the implementation of a highly secured electronic voting system. The methods used by different scholars were technically reviewed so as to identify areas that need improvement towards providing solutions to the identified problems. Furthermore, countries with history on the adoption of e-voting systems were reviewed. Based on the problems identified from various works, a novel for future work on developing a secured electronic voting system using fingerprint and visual semagram techniques was proposed.

***Index Terms*—**Review, Electronic Voting System, Implication, Novel

I. Introduction

Voting is a process that involves citizen or a group of people in an institution to collectively make a choice on a particular contestant among listed contestants based on rules and regulations. Voting is an expression of choice through ballot. A contestant is usually declared winner in an election having scored the required number of ballots or votes and fulfilled the specified conditions that govern the declaration of winner.

For many years in the world, the paper-based voting system has been used as a method to vote during elections. This approach is stressful as voters need to line up to register for election before they are permitted to vote [1]. In a large population, the paper-based voting system requires days to conduct an election and announce the final results. Reference [2] reported that the paper-based system allows a voter to register and vote more than the acceptable requirement of one voter, one vote. Many bad politicians use this opportunity to engage the voters to poll votes in multiple times. The problem of multiple votes by a voter has resulted in unwanted candidate been emerged as the winner.

The paper-based voting system allows the alteration of the election results. The manual counting of votes polled by the voters can be easily manipulated to favour a particular candidate. At present, after manual collation, the results of the election are being scanned and transmitted through an unprotected network using mobile phones, i-pads and tablets. This procedure is not reliable and can be made to favour a particular candidate. In many existing voting systems, the votes polled by the voters has not been verified by the voters. This makes the voters doubt the integrity of the election system. In addition, few people have been involving in the voting system which makes the alteration easier.

Elections being a fundamental pillar of leadership selection in any democracy, has an indisputably characterized with challenges such as ballot padding, candidate imposition, fighting, voters' impersonation, multiple voting by false voters, snatching of the electoral materials such as ballot boxes, ballot papers by unauthorized group of people, massive rigging by party agents in collaboration with the elections' officials,

insecurity of votes, poor funding, bad attitudes of the political class and inability to prosecute election offenders. It is very obvious that traditional methods of voting using papers, ballot boxes and manual counting of votes have provided rooms for the corrupt politicians to alter election results; this, in turn, makes the populace to lose confidence in the integrity of the election across the globe [3]. Electronic voting (e-voting) was basically introduced to solve the problems identified in traditional voting systems. E-voting systems involved integration of electronic devices into voting system. However, various challenges had been identified with e-voting systems. Attackers or fraudsters in collaboration with corrupt politicians and election officers had been falsified scores thereby providing unlawful opportunities for false contestant to emerge as winner.

Therefore, researches of various scholars were examined towards designing a highly secured e-voting system that would prevent corrupt politicians and election officers from rigging and any form of fraudulent activities. The world cannot trade a credible election for anything. This paper would create a platform to critically review papers and e-voting systems of different scholars, identify shortcomings for designing a highly secured e-voting system using fingerprint biometric and visual semagram techniques.

II. Literature Review

Reference [4] discussed the historical background of the electronic voting system, types of voting technology, and the manual experience of balloting system in Nigeria. The research was motivated towards providing solution to the problems of election malpractices such as impersonation, multiple voting, false counting of votes and deliberate disenfranchisement of voters by the polling officers. The objectives of the research were to design and implement a secured voting system that was not prone to manipulation, rigging, and complaints from citizens and political parties. The design was achieved on a three-tier web-enabling application such as apache as a web server with extended capacity for Hypertext Pre-processor (PHP) scripting language and MySQL relational database. The research achieved authentication and simplicity as measures of fulfilling the electronic voting requirements. The research could not achieve confidentiality, integrity, secrecy, transparency, convenience and auditability of e-voting functional and security requirements.

Reference [25] proposed a biometric-secure cloud based e-voting system for election processes. The researcher was motivated by the problems of duplication of votes and high cost of ballot paper production. The objectives of the research were to design and develop a secure e-Voting system based on biometric fingerprint method. Two methods used were Histogram Equalization and Fourier Transform for fingerprint and iris identification. The authentication of the voters was achieved. The research could not achieve confidentiality, integrity, secrecy, transparency, convenience and auditability of e-voting functional and security requirements. Also, the use of fingerprint and iris for authentication is economically expensive because the system requires more memory capacity for data storage.

Reference [11] research was on an advanced microcontroller based biometric authentication voting machine. The research was motivated so as to solve the problem of counting ballot paper time, reducing the expenditure incurred on manpower and carrying of photo identity cards for recognition. The objectives of the research were to design and develop a secure e-Voting system based on biometric fingerprint method. The e-voting system was designed and implemented using fingerprint biometric and ATmega328 microcontroller to achieve authentication and Visual Basic programming language was used to develop the application. Passwords were used by the election officers. The fingerprint ridges patterns were formulated and used for authentication of the voters. The research could not achieve confidentiality, integrity, secrecy, transparency, convenience and auditability of e-voting functional and security requirements. Also, the password of polling officers could be detected by the fraudsters for alteration of election results.

Reference [17] provided security to an online voting system with secure user authentication by providing biometric and password features to the e-voting system. The researcher was motivated towards providing solution to the problems of rigging and to increase the accuracy and the speed of the election process. The objectives of the research were to review and design an online voting system using biometrics and steganography. The voter's fingerprint and password were used to achieve authentication while the least significant bit (LSB) was used to hide the results and MD5 to achieve integrity. The research achieved the authentication and confidentiality requirement of e-voting system. The problems of secrecy, transparency, convenience and auditability of e-voting functional and security requirements were not tackled. A MD5 technique raises suspicion on the hidden message, thereby providing room for attacks.

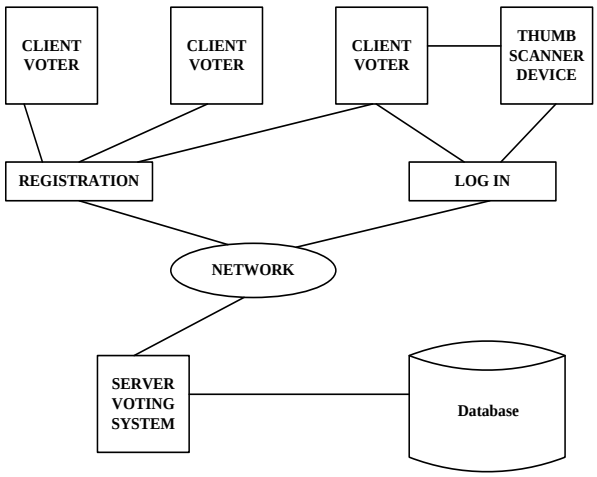

Fig. 1. Block diagram of [17]

The paper of [29] focused on simple, low-cost fingerprint based electronic voting machine using the ARM9 microcontroller. The researchers were motivated based on the problems of the voters' impersonation thereby leading to false result that was contrary to the decision of majority populace. The objectives of the research were to design, develop and test a more convenient and highly secured e-voting system. A KY-M6 fingerprint sensor was used to capture the voter's fingerprint. The codes were developed in the WINCE6 development environment for interfacing the ARM processor. Formulation of a fingerprint pattern technique to achieve authentication in fulfilling the security requirements of the electronic voting system was achieved. The system could not achieve confidentiality, integrity, secrecy, transparency, convenience and auditability of e-voting functional and security requirements. The password used by the authorized officers could be detected by the imposters for results' alteration.

Reference [5] developed an anti-corruption biometric voting machine. The inability electronic voting systems to distinguish the voters was the fundamental motivation. The objectives of the research were to design and develop an anti-corruption biometric voting machine using fingerprint. Fingerprint R-305 scanner, ATmega microcontroller, transformer were among other materials used. The research achieved authentication using fingerprint. The system could not achieve confidentiality, integrity, secrecy, transparency, convenience and auditability of e-voting functional and security requirements.

The research of [21] was on biometric fingerprint based electronic voting system for rigging free governance. The consequence of rigging in an election was the major concern of the researchers. The objectives of the research were to design and develop a biometric fingerprint based electronic voting system for rigging free and fair election. The FIM 3030N scanner was used to extract, process and store the ridges of the fingerprint in the database. The research achieved authentication. The problems of confidentiality, integrity, secrecy, transparency, convenience and auditability of e-voting functional and security requirements could not be addressed.

Reference [30] developed a fingerprint enabled electronic voting machine with enhanced security in Bangladesh of almost 90 million voters. The researchers were motivated by the problems of inaccuracy, lack of transparency, insecurity and delay in election result processing and announcement. The objectives of the research were to design and implement a fingerprint enabled electronic voting machine (EVM). ATmega2560 microcontroller, SD cards, crystal oscillator, power jack, a USB connection were among other devices for authentication and voting. The research achieved authentication and it was simple to operate. The problems of confidentiality, integrity, secrecy, transparency, convenience and auditability could not be addressed. Also, the EEPROM of ATmega2560 has limited memory capacity for storage and results stored in the SD card could be altered by the corrupt election officers.

Reference [18] was on iris recognition based voting system. The movement of the voters' ID cards from one geographical location to another could either be lost or forged by the imposters leading to fake voting. The objectives of the research were to design and implement an iris recognition based voting system. The iris pattern of the voter was matched with the pre-stored image in the database which was calculated by the hamming distance. Presentation of a hamming distance technique on voter's iris to achieve authentication. The challenges of confidentiality, integrity, secrecy, transparency, convenience and auditability of e-voting functional and security of e-voting security requirements were not tackled. Also, iris could be attacked by diseases.

Reference [14] proposed a voting method that was secured from fraudulent activity such as rigging using Aadhaar cards and fingerprint biometric. The researchers were motivated by the problem of manual checking of voter's ID card which often lead to illegal voting by false voters and high likelihood of multiple votes by the same voter. The objectives of the research were to design, develop and test a fingerprint and RFID based electronic voting system. The AT89S52 microcontroller was used and it linked with the RFID tags for authentication and voting. Algorithm that integrated RFID of Aadhaar and fingerprint to achieve the authentication e-voting requirement was presented. The challenges of confidentiality, integrity, secrecy, transparency, convenience and auditability of e-voting functional and security requirements were not tackled.

The research of [19] was on an advanced secure voting system with the internet of things (IoT) towards achieving free and fair election. The problems of false voting by the imposters and slow in the collation of election results thereby leading to delay in results announcement. The objectives of the research were to design, implement and test an advanced secure voting system with IoT. The ridge and valley features extraction technique was used for authentication and the election data was transfer to the main database. A ridge extraction technique was presented and used to achieve authentication as a measure towards the attainment of e-voting requirement. The challenges of confidentiality, integrity, secrecy, transparency, convenience and auditability of e-voting functional and security requirements were not tackled. The results over unprotected network are prone to attacks.

Reference [20] developed an electronic voting system using fingerprint biometrics and crypto- watermarking approach. Researchers were motivated by the problems of unlawful voting and election results alteration. The objectives of the research were to design, develop and evaluate a secure electronic voting system using fingerprint biometrics and crypto-watermarking approach. A fingerprint biometric, Advanced Encryption Standard (AES) cryptographic and wavelet watermarking techniques were presented and used. Voter used fingerprint and serially assigned personal identification

number (PIN) for authentication. The voting system was convenient as voter could poll a vote via a PC, and the research also achieved authentication, integrity and confidentiality. The problems of secrecy, transparency, convenience and auditability of e-voting functional and security requirements were not tackled. The serial PIN assigned to each voter could be guessed by the imposters for fake voting. Also, AES has repudiation (refutation) problem and encryption could raise suspicion for attacks on the sensitive results thereby giving room for corrupt contestant to emerge as a winner. A more robust e-voting needed to be designed against any form of suspicion using fingerprint biometric and visual semagram techniques.

Reference [38] implemented a secure online voting system. The researchers were motivated by the shortcomings of the huge volume of papers, delays in time of processing of election results. The objectives of the research were to design, implement and test a system that would encourage the maximum number of voters to remotely participate and cast votes to a particular candidate. The use of one time password (OTP), interactive voice response (IVR) and password were used. The registration and voting were convenient. The problems of confidentiality, integrity, secrecy, transparency, convenience and auditability could not be addressed. The OTP and the password could be stolen or detected. Also, human voice could be negatively affected by diseases thereby making voice recognition difficulty.

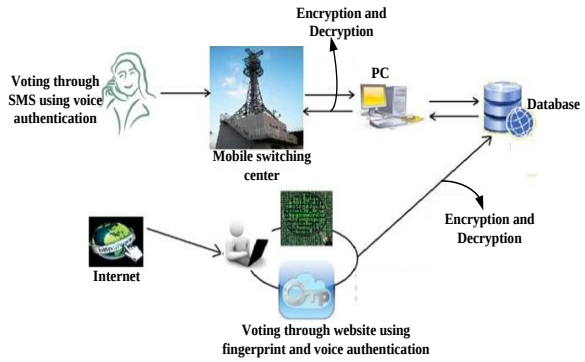

Fig.2. E-voting system of [38]

Reference [8] voting system was on the embedded system based voting machine system using wireless technology. The problems of rigging which lead to the announcement of results contrary to the genuine decision provided by the voters and delay in results collation. The objectives of the research were to design and develop a wireless technology using fingerprint biometric. The ZigBee wireless technology, microcontroller to and fingerprint scanner were integrated to capture and process ridges for authentication. The research achieved authentication and ZigBee wireless technology enhanced the transmission of the election results. The problems of confidentiality, integrity, secrecy, transparency, convenience and auditability of e-voting functional and security requirements were not addressed. Also, the ZigBee is an unprotected wireless network wireless.

The research of [15] was on the Aadhaar based electronic voting machine using Arduino. The researchers were motivated by the problems of voters' ID cards for identification, unlawful voting by the imposters and slow in the collation of election results. The objectives of the research were to design, develop and test an Aadhaar based electronic voting machine using Arduino. The Aadhaar card number and password were used to login by the voter to poll a vote. There was button dedicated to each political party for a voter to press and vote a particular candidate. Formulation of algorithm that used Aadhaar cards and password to achieve authentication e-voting security requirement was presented and voters could verify the votes polled by printing acknowledgement slips. The problems of confidentiality, integrity, secrecy, transparency, convenience and auditability were not addressed. The Aadhaar number and password could be detected by the imposters. Furthermore, high cost of implementation due to dedicated button for each candidate and acknowledgement slips could lead to votes' buying and selling.

Reference [35] described a smart voting system that ensured effective voting procedure and voting count. The researchers were motivated by the problem of manual checking of voter's details for identification. The objectives of the research were to design and implement a smart voting machine. The unique key and fingerprint ID were used for authentication and the results were transmitted to the mobile phone of the election commissioner. The fingerprint biometric and unique key were used to achieve verification. The problems of confidentiality, integrity, secrecy, transparency, convenience and auditability of e-voting functional and security requirements were not addressed. The results communicated through the unprotected network could be intercepted by imposters.

The research of [27] was on distributed server approach for novel e-voting system with biometric authentication using Aadhaar card. The researchers were motivated by the problem of fake voting by the imposters. The objectives of the research were to design, implement and test an e-voting system using biometric for authentication. The Aadhaar number and the voter's fingerprint were used to implement the voting system. The research achieved authentication as the researchers adopted fingerprint biometric and Aadhaar card number. The problems of confidentiality, integrity, secrecy, transparency, convenience and auditability were not addressed. The cost of producing Aadhaar cards is high comparing to a secured fingerprint for authentication. The cost of Aadhaar kits for a polling booth is between RS11,800 and RS68,000 (USD169.64 and USD977.57) [52].

Reference [36] described a smart voting system for an election which was managed in an easier way to cast vote using fingerprint and Aadhaar card. The problem of multiple voting among the voters has made the undesirable candidate to poll the highest number of votes.

The objectives of the research were to design, implement and test a smart voting system using biometric and Aadhaar card. The voter's fingerprint, Aadhaar number and One Time Pin (OTP) were used to implement the voting system. The research achieved authentication, as the researchers adopted fingerprint biometric and OTP. The problems of confidentiality, integrity, secrecy, transparency, convenience and auditability were not solved. The cost of producing Aadhaar cards is high and the cost of mobile phones for OTP are not economically affordable by many voters.

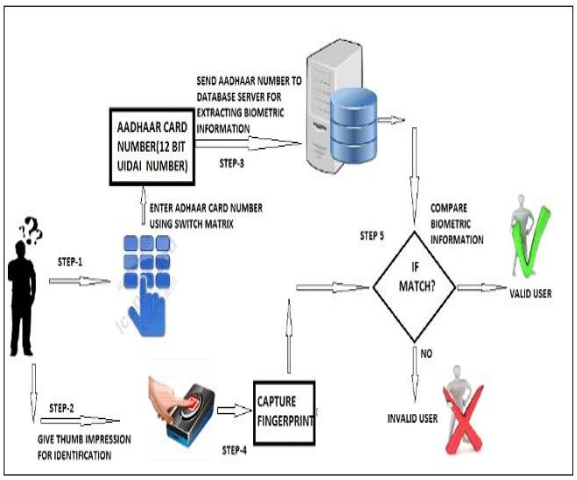

Fig.3. E-voting architecture of [27]

The research of [16] used Aadhaar information to develop a voting system. The use of voter identification card could either be lost or forged by the imposters leading to false voting. The objectives of the research were to design, implement and test a smart voting system using unique identification authority of India (UIDAI). The barcode of Aadhaar and voter's fingerprint were used to implement the voting system. The research achieved authentication, as the researchers adopted fingerprint biometric and barcode of Aadhaar. The problems of confidentiality, integrity, secrecy, transparency, convenience and auditability were not solved. The cost of producing Aadhaar cards is high comparing to a secured fingerprint technique and the barcodes could be technically detected before the election time for false voting by the imposters.

The research of [12] electronically attempted to tackle the problem fraudulence in voting systems. The consequence of rigging in an election was the major concern of the researchers. The objectives of the research were to design, implement and test a biometric based electronic voting system using Aadhaar. The RFID tags and voter's fingerprint were used to implement the voting system. Algorithms that integrated the voter's fingerprint and RFID tag to achieve authentication e-voting requirement was presented. The problems of confidentiality, integrity, secrecy, transparency, convenience and auditability were not solved. The RFID codes could be technically detected before the election time by the imposters for false voting.

Reference [34] proposed an integration of biometric sensor with Aadhaar for the voting process. The use of only Aadhaar card by the voter for identification could provide opportunities for the imposters to poll unlawful votes. The objectives of the research were to design and implement an electronic voting system using biometric sensor and Aadhaar cards. The Aadhar cards and voter's fingerprint were used to implement the voting system. Minutiae matching algorithm for authentication and algorithm for the interconnection of local database for the efficiency of the e-voting system were presented. The problems of confidentiality, integrity, secrecy, transparency, convenience and auditability of e-voting functional and security requirements were not solved. The unsecured results were transmitted from one polling unit to other.

Reference [26] developed Aadhaar based biometric electronic voting to avoid rigging. The concern of rigging in an election was the major concern of the researchers. The objectives of the research were to design, implement and test an Aadhaar based biometric electronic voting system. The methodology involved the use of barcode of Aadhaar card and fingerprint for authentication of voters from AT89S52 EEPROM. The research achieved authentication, as the researchers adopted fingerprint biometric and barcode of Aadhaar. The problems of confidentiality, integrity, secrecy, transparency, convenience and auditability were not solved. The AT89S52 has limited memory capacity.

Reference [32] was fingerprint based electronic voting machine towards elimination of illegal voting. The researchers were motivated by the problems of false voting by the imposters. The objectives of the research were to design, develop and test a fingerprint-based electronic voting system. The RFID, fingerprint and Arduino UNO R3 microcontroller were linked to RFID database for authentication and to poll votes. Algorithms that integrated voters' fingerprint and RFID of Aadhaar to satisfy the authentication requirement of e-voting system was presented. The confidentiality, integrity, secrecy, and auditability were not solved. Dedicated push button for each candidate requires high cost of implementation for numerous contestants. Also, The RFID codes could be technically detected before the election time by the imposters for false voting.

Reference [31] was on a novel hybrid biometric electronic voting system. The problems of fraudulent practice such as false voting among the voters during election from single biometric techniques. The objectives of the research were to design, develop, test and evaluate a biometric electronic voting system using fingerprint and face recognition. The fingerprint and face of voters were used with Generalized Principle Component Analysis (GPCA) and K-Nearest Neighbor (K-NN) for authentication Generalized Principle Component Analysis (GPCA) and K-Nearest Neighbor (K-NN) algorithms on fingerprint and face to achieve authentication were presented. The problems of confidentiality, integrity, secrecy, transparency, convenience and auditability of e-voting functional and

security requirements were not tackled. The fusion of fingerprint and face image requires high cost of implementation and the problem of illumination with face recognition [10].

Reference [33] designed an online voting system that allowed the voters to poll votes through mobile application. The problems of multiple votes by a voter and irregularity such as alteration of results at polling booths. The objectives of the research were to design, implement and test an electronic voting system using Aadhaar cards. The methodology involved the use of Aadhaar cards and mobile phones. Techniques on matching the voter's fingerprint and Aadhaar ID to achieve authentication and vote's confirmation (verifiability) were presented. The problems of confidentiality, integrity, secrecy, transparency, convenience and auditability were not solved. Additionally, votes' confirmation by the voters could enhance vote buying and selling, thereby negatively affect the election outcomes.

Reference [23] developed an online voting system that allowed the voters to poll votes at any location. The researchers were motivated by the problems of double voting among the voters and inability of the votes polled to be verified. The objectives of the research were to design and implement a biometric fingerprint method for an online voting system. The methodology involved the use of Unique Identity Number (UID) number and fingerprint to implement the voting system. Algorithms that extracted voters' pattern of ridges, valleys and UID number to achieve authentication and verifiability requirements of electronic voting systems were presented. Election officers used passwords to login for any assigned activities. The problems of confidentiality, integrity, secrecy, transparency, convenience and auditability were not addressed. Also, username and passwords of the administrative officers could be detected for results alteration. In [23], the vote's confirmation enhanced vote buying and selling which is not good for a credible and fair election.

The research of [24] was designed to authenticate the voters as well as allow vote casting. The researchers were motivated by the problem of false voting by the imposters often leading to false winner. The objectives of the research were to design and implement an Aadhaar based voting system using fingerprint method. The methodology involved the use of Unique Identity Number (UIDAI) number and fingerprint to implement the voting system. Algorithm that integrated the voters' fingerprints and Aadhaar numbers was presented. The problems of achieve confidentiality, integrity, secrecy, transparency, convenience and auditability of e-voting functional and security requirements were not addressed.

Reference [22] presented a new voting process which used Raspberry Pi. The researchers were motivated by the problems of paper-based voter's identification technique and false voting by the imposters. The objectives of the research were to design and develop of an electronic voting system for government using Raspberry Pi. The methodology involved the use of Raspberry Pi and voter's ID to implement the voting system. Algorithm for template extraction to achieve authentication as a tactic of fulfilling the security requirement of e-voting system was presented. The problems of confidentiality, integrity, secrecy, transparency, convenience and auditability were not addressed. The Raspberry Pi has a low memory capacity for large population.

Reference [6] designed and developed a fingerprint enabled electronic voting machine (EVM) with the aim of achieving greater security level. The researchers were motivated by the problems of poor voter's identification and the failure to verify the votes polled by the voters as requirements for the electronic voting system. The objectives of the research were to design and develop a secured electronic voting system using biometric technique. The fingerprint and GSM were used to implement the voting system. Algorithms to achieve the authentication and verifiability requirements of electronic voting systems were formulated. The problems of confidentiality, integrity, secrecy, transparency, convenience and auditability were not addressed. The election results through the use of GSM could be intercepted and altered by fraudsters, thereby leading false contestant emerge as a winner.

Reference [28] developed a secured electronic voting machine using aadhaar in IOT platform. The researchers were motivated by the problem of unlawful voting by the imposter as a result of paper-based technique of voter's identification. The objectives of the research were to design and develop a highly secured electronic voting system using Aadhaar and IOT. The materials used were PIC16F874A/877A microcontroller, fingerprint sensor, ZigBee (CC2500), Liquid Crystal display (LCD), buzzer and power supply. Algorithm that integrated the voter's fingerprint and Aadhaar card to achieve authentication was presented and the e-voting system was a simple and convenient system for the voter to operate. The problems of confidentiality, integrity, secrecy, transparency, convenience and auditability of e-voting functional and security requirements were not solved. The PIC16F874A/877A microcontroller has limited memory capacity for large population. The procurement of Aadhaar cards is economically high and not suitable for developing countries.

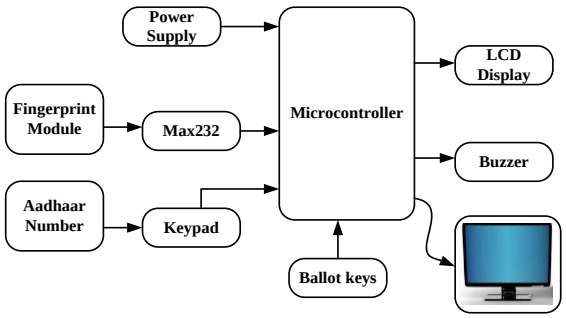

Fig. 4. E-voting and aadhaar card of [28]

The voting system of [9] has been designed and implemented purposefully for organisations and businesses. The researchers were motivated by the

problem of poor voter's identification in the election which often lead to false voting by the imposters. The objectives of the research were to design and develop an android-based voting system using fingerprint and facial recognition techniques. The voter's fingerprint and face were combined with voter's username and password were used to implement the voting system. Algorithm that fused voters' fingerprint and face for authentication as a measure of satisfying the security requirement of e-voting system was formulated. The problems of confidentiality, integrity, secrecy, transparency, convenience and auditability were not addressed. The fusion of fingerprint and face image requires large memory capacity, thereby requires high cost of implementation. The high accuracy of bimodal system is not guaranteed [9]. Therefore, a cheaper but highly secured e-voting system needed to be designed for a credible election.

Reference [37] was on the Aadhaar based biometric voting system. The problem of voters' impersonation in election. The objectives of the research were to design and develop an Aadhar based biometric voting system. Aadhaar cards and the fingerprint for authentication to implement the voting system. Algorithm that integrated the voter's fingerprint and Aadhaar cards to achieve authentication was presented. The problems of confidentiality, integrity, secrecy, transparency, convenience and auditability were not tackled. The cost of producing Aadhaar cards is high.

Reference [13] designed and implemented an electronic voting machine with facial recognition and fingerprint sensors. The researchers were motivated by the problem of voters' impersonation that often lead to unlawful votes thereby providing winning opportunity to corrupt candidate to win. The objectives of the research were to design, implement and test a voting system using fingerprint and facial recognition. The Support Vector Machine and Local Binary Pattern Histogram were used face recognition while High Sensitive Pixel Amplifier (HSPA) was used to fingerprint process. The Visual Basic language was used to implement the voting system. The research achieved authentication requirements of e-voting system. The problems of confidentiality, integrity, secrecy, transparency, convenience and were not tackled. The problem of illumination affects the face recognition and the error rate (FAR or FRR) of the weaker biometric could bring down the overall effectiveness of the system [7].

III. Countries with Electronic Voting Systems

Recently, the urge for e-voting has been described to be the inevitable future of electioneering in many countries across the world. Few countries have legally adopted the use of e-voting systems to elect who govern their societies while governments from other countries are sceptical about the adoption. Undoubtedly, there were technical questions asked on the acceptance and rejection of e-voting systems. Therefore, the uses of e-voting systems in few countries were reviewed and presented as follows.

A. Netherlands

Politically, the Netherlands commenced the electronic voting system in the year 1960 [39]. In 1994, the government of Netherland started the introduction of electronic voting machines. In 2006, a direct-recording electronic (DRE) voting machine was produced. In the municipal elections of March 2006, nearly 99% of the voters polled votes with the use of voting machine (Nedap ES3B). The 2019 Dutch provisional elections in Netherland had security-based problem of authentication, when a voter was turned back because of invalid ID card [50]. Imposters could forge a genuine voter's ID card as well. Also, Erasable Programmable Read Only Memory (EPROM) of Nedap ES3B could be removed and replaced with a tampered memory to favour a particular contestant [40]. The passwords for authentication could be detected by fraudsters for results' alteration. The problems of authentication, integrity, secrecy, transparency, convenience and auditability of e-voting functional and security requirements were identified. Accordingly, a novel on electronic voting in Netherland is required for fair and credible election.

B. United States of America (USA)

The United States of America (USA) is a country of 50 states with a population of about 326 million [42]. There were voting technologies and approaches adopted in the USA for voting. These technologies are Direct Recording Electronic (DRE), Optical Scan and Hybrid Voting Machines. In October, 2016, the United States accused the government of Russia for cybersecurity interference in the US election. Politically, Russia was alleged to have "rigged" the US 2016 presidential election to favour a Republican nominee, Donald Trump by tampering with digital ballots. According to the information made available by [44], the US voters' registration database needed to be highly protected from potentially fraudulent or abnormal activity. In addition, [43] moved for the need to fully integrate biometric technology into the voting system in USA voting process. The US 2016 election had an issue of reliability in the entire process. Principally, reliability is one of the security requirements, thus there is no way security and functional requirements of the e-voting system could be compromised for personal gains. Furthermore, every e-voting system ought to satisfy the security and functional requirements for a credible election. With these controversies, basic security and functional requirements of e-voting needed to be satisfied for credible election in the US.

C. India

India is the seventh-largest country by area, the second-most populous country with over 1.3 billion people [41]. In India, Aadhaar card and fingerprint are major credentials for authentication. There must be a match between already stored credentials and credentials presented on the day of election before a voter could proceed to poll a vote to a particular contestant.This approach calls for high cost of implementation as production of biometric Aadhaar cards is economically

expensive. Also, the transmission of sensitive results over unprotected network was not protected against alteration. This implies that the results were disposed to interception and alteration. Here again, voting system in India required attention and a novel approach that tackle election malpractices and security challenges.

In Indian, Aadhaar cards are regularly presented to voters at no cost after a successful enrolment. However, any correction after the enrolment attracts fees between RS50 and RS500 (i.e USD0.72 and USD7.19) [51]. This could negatively affect poor citizens to participate in an election thereby promoting low turnout of voters and increases the chances of unlawful results' manipulations. Furthermore, the cost of producing Aadhaar cards for authentication is higher than non-biometrci-based cards. This is capital intensive to design, implement and distribute the Aadhaar kits to all the polling booths needed for a specified election. The production and distribution of free biometric-based Aadhaar cards to voters are principally the responsibilities of government and the funds could have been used to develop the country economically. There should be a highly secured but economically cheaper approach to authenticate voters where voters need not make any payment for collection even after successful enrolment.

D. Zurich

Zurich is the largest city in Switzerland and the capital of the canton of Zürich. Zurich used a voting system called the Unisys Internet voting system that was launched in 2002, this system was first used in a student election, after its success it was subsequently used in the public election in Bulach in 2005. The voters could either vote via a personal computer or via SMS, but later on in 2007 the SMS channel was discontinued. Encryption techniques were used to secure votes polled by voters [45].

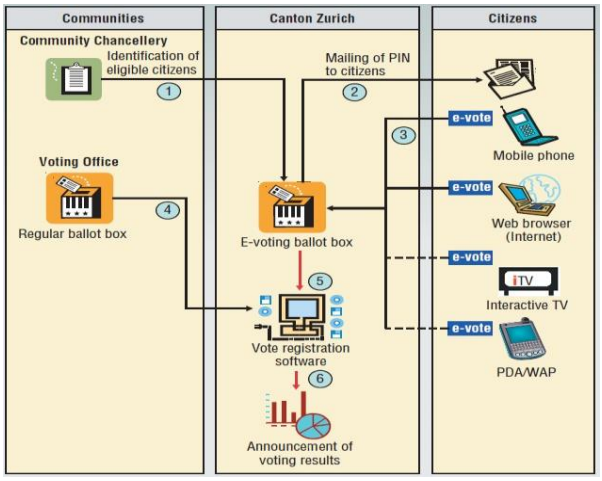

Fig. 5. E-voting in Canton Zurich

E. Brazil

Brazil officially known as the Federative Republic of Brazil, is the largest country in both South America and Latin America. Brazil introduced electronic voting during the 1996 municipal elections. That year, voters in state capitals and cities with more than two hundred thousand voters used the first electronic polling stations. The electronic polling station used Advanced Encryption Technique (AET). However, [46] presented a detailed and up-to-date security analysis of the voting software used in Brazilian elections. The finding of [46] revealed the most in-depth compromise of an official large-scale voting system ever performed.

F. Estonia

Estonia, a country in Northern Europe, borders the Baltic Sea and the Gulf of Finland. According to [47], Estonia was the first country in the world to introduce nation-wide Internet voting system. In Estonian I-voting system, citizens that want to cast their vote would use National ID cards and mobile ID on web site for authentication.

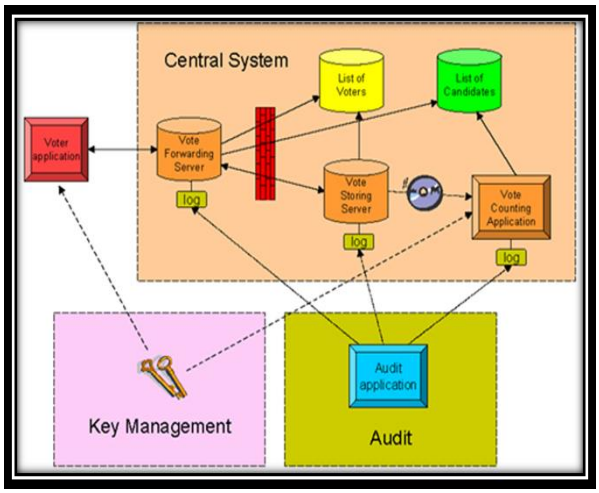

Fig. 6. Estonian system general architecture

All votes are recorded and provisionally stored on Vote Forwarding Server until the completion of election. The resulting encrypted votes were then burned onto Digital Versatile Discs (DVDs). The DVDs are then transferred to the Vote Counting Server, an air-gapped machine that contains the election private key. The counting of votes was carried out by the counter server after a successful decryption. The rigging is possible as encryption and decryption techniques raise suspicion of the sensitive results. Thus, a novel on e-voting system is required.

G. Namibia

The Republic of Namibia is a country in southern Africa whose western border is the Atlantic Ocean. In 2014, Namibia became the first African country to conduct a national election using electronic voting [48]. The voting system used voter's fingerprint and Voter Verification Devices (VVD) for authentication as guided by the Electoral Commission of Namibia (ECN). An integration of VVPAT feature in the e-voting system creates room for votes' buying and selling by corrupt politicians and voters. Thus, the requirement of vote's confirmation (verifiability) is not suitable for a credible and fair election in most parts of the world.

H. Nigeria

The Federal Republic of Nigeria commonly referred to as Nigeria is a federal republic in West Africa, bordering Benin in the west, Chad and Cameroon in the east, and Niger in the north. Its coast in the south lies on the Gulf of Guinea in the Atlantic Ocean. In 2015, Independent National Electoral Commission (INEC) introduced Permanent Voters Card (PVC) and card reader for accreditation. Once a voter had been accredited, then a ballot paper with printed contestants' party logo would be presented for expression of choice by the voter. However, election malpractices such as rigging, false voting and false declaration of winner were identified in 2019 general election. There is need to fully automated the voting system.

On Saturday, May 12, 2018, the government of Kaduna State, Nigeria made history by the use of EMP2710 e-voting machine developed by a Chinese company, EMPTECH. On the day of election, the voters were accredited with the use of Permanent Voters Card (PVC). Afterwards, the voters electronically voted for the chosen party and candidate by selecting and pressing the appropriate icon on the screen of EMP2710 machine.

When the voting exercise ended, an electoral officer brought out printed ballot papers from the machine for manual counting among party agents and officials [49]. The EVM (EMP2710) deployed for voting in Kaduna State 2018 local government election was made voting process faster than the traditional paper balloting system and achieved the convenience functional requirement of e-voting system. However, the polling officers could unlawfully thumb print the ballot papers to favour a candidate. The genuine votes by the genuine voters could be replaced with falsely thumb printed ballot papers by the polling officers or agents of the political parties. Despite the use of PVC and card reader for accreditation, there was no electronically link between the number of accredited voters and the number of votes polled by the voters.

IV. Conclusion

This paper presented a critical review of several studies on e-voting systems and few countries with the use of electronic voting systems. The methods, tools, results, strength and limitations (weaknesses) were identified and studied. The e-voting developed previously to a great extent, could not technically tackle the identified problems of voter's impersonation (authentication), confidentiality, integrity, auditability, transparency, convenience and secrecy. The efforts to prevent corrupt stakeholders such as politicians, election officers and voters from unlawful activities needed urgent attention for a novel on electronic systems. After a critical review of previous work on e-voting systems, the researchers concluded that a highly secured e-voting system based on a novel is required towards achieving a credible election and satisfying e-voting security and functional requirements. Conclusively, e-voting systems were constructively, objectively and logically reviewed and summarized as a piece of relevant information useful for novel and scholarly investigations in academic.

V. Future Work

The researchers have commenced a strategy to develop a secured electronic voting system using fingerprint biometric and visual semagram techniques that would tackle all the drawbacks presented in this paper and satisfy e-voting functional and security requirements towards achieving credible elections at all levels.

References

[1] S. Abdulhamid, S. A. Olawale, O. U. Damian and D. A. Mohammed, "The design and development of real-time e-voting system in Nigeria with emphasis on security and result veracity. *International Journal of Computer Network and Information Security*, 2013, vol. 5, pp. 9-18.

[2] W. E. Naser, "Minutiae-based Fingerprint Extraction and Recognition", 2017, Retrieved February 12, 2018 from: http://www.intechopen.com/books/biometrics/minutiae-based-fingerprint-extraction-and-recognition.

[3] C. Lichun, "Trust and security in the e-voting system", *Electronic Government: an International Journal*, 2018, vol. 6(4), pp. 343-351.

[4] L. B. Ajayi, "A secure electronic voting system," An unpublished master thesis submitted in Computer Science, Federal University of Technology, Akure, Nigeria, 2004.

[5] B. Ankita, B. Rana and C. Shamik, "Anti-corruption biometric voting machine," *International Journal of Emerging Research in Management and Technology*, 2015, vol. 4(9), pp. 1–4.

[6] M. Atul, Y. Divyansh, C. Ankit, P. Deepak, and G. Shubham, "A secured electronic voting machine using biometric," *International Journal of Electronics, Electrical and Computational System*, 2018, vol. 7(4), pp. 105–108.

[7] L. Catalin, "Car access using multimodal biometrics," The Annals of The"Ştefan cel Mare" University of Suceava. Fascicle of the Faculty of Economics and Public Administration, 2010, vol. 10, pp. 368–377.

[8] K. M. Dhinesh, A. Santhosh, N. S. Aranganadhan and D. Praveenkumar, "Embedded system based voting machine system using wireless technology," *International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering*, 2016, vol. 4(2), pp. 127–130.

[9] M. Divyank, S. Aaditya and G. Saurabh, "Android voting system using facial recognition," International Journal of Advanced Research in Computer and Communication Engineering, 2018, vol. 7(3), pp. 288–291.

[10] Q. D. Don, "5 Pros and cons of face recognition technology," Tech Funnel, 2018 Retrieved May 25, 2018 from https://www.techfunnel.com/information-technology/5-pros-and-cons-of-face-recognition-technology/

[11] B. A. Farhath, M. Deepa and C. N. Kalaivani, "Advanced microcontroller based Biometric authentication voting machine," *International Organization of Scientific Research Journal of Engineering (IOSRJEN)*, 2014, vol. 4(5), pp. 29–40.

[12] R. Geethamani, V. Nithya, B. Nivetha, R. Pratheebamary and A. Rajakumari, "Biometric based electronic voting system using aadhar," *International Journal of Innovative*

Research in Science, Engineering and Technology, 2017, vol. 6(14), pp. 75–80.

[13] I. P. Jaison, K. R. Kishoritha, B. Ganesh, P. Gokulprashanth and G. Udhayakumar, "Electronic voting machine with facial recognition and fingerprint sensors," *International Journal of Advance Research and Development,* 2018, vol. 3(3), pp. 165–170.

[14] H. H. Mary, G. M. O. A. Owais, D. Sukruthi, K. A. Venu, and C. N. Mahendra, "Fingerprint and rfid based electronic voting system linked with aadhaar for rigging free elections," *International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering*, 2016, vol. 5(3), pp. 1686–1693.

[15] R. P. Murali, B. Polaiah and N. Madhu, "Aadhar based electronic voting machine using arduino," *International Journal of Computer Applications*, 2016, vol. 145(12), pp. 39–42.

[16] M. Nandhini and M. Vasanthakumar, "Smart voting system using UIDAI," *National Conference on Networks, Intelligence and Computing Systems*, 2017, pp. 105–110.

[17] G. Neha, "Study on security of online voting system using biometrics and steganography," *International Journal of Computer Science and Communications (IJCSC),* 2014, vol. 5(1), pp. 29–32.

[18] M. J. Nithya, G. Abinaya, B. Sankareswari and M. L. Saravana, "Iris recognition based voting system," *International Conference on Science, Technology, Engineering and Management (ICON-STEM),* 2015, vol. 10, pp. 44–51.

[19] S. Nithya, C. Ashwin, C. Karthikeyan and K. M. Ajith, "Advanced secure voting system with IoT," *International Journal of Engineering and Computer Science*, 2016, vol. 5(3), pp. 16033–16037.

[20] M. O. Olayemi, A. F. Taliha, A. Aliyu and J. Olugbenga, "Design of secure electronic voting system using fingerprint biometrics and crypto- watermarking approach," *International Journal of Information Engineering and Electronic Business (IJIEEB*), 2016, vol. 8(5), pp. 9–17, DOI: 10.5815/ijieeb.2016.05.02.

[21] S. Panja and S. Mondeddu, "Biometric finger print based electronic voting system for rigging free governance," *International Journal and Magazine of Engineering, Technology, Management and Research,* 2015, vol. 2(12), pp. 526–529.

[22] N. C. Prashantha, Y. C. Arpitha, R. B. K. Preethi, D. Ranjitha and T. Vinutha, "Design and development of security based voting system for government using raspberry pi," *International Journal of Advance Engineering and Research Development,* 2018, vol. 5(5), pp. 379– 384.

[23] N. S. Priya and A. F. Lenin, "Biometric fingerprint authentication approach for an online voting system," *International Journal of Innovative Research Explorer*, 2018, vol. 5(4), pp. 379–384.

[24] M. Ravindra, B. Shildarshi, S. Tushar, J. Shelke, S. Rout and S. Sahastrabuddhe, "Aadhaar based voting system using fingerprint scanner," *International Journal of Advance Research and Innovative Ideas in Education (IJARIIE),* 2018, vol. 4(2), pp. 3660– 3665.

[25] J. A. Samsul and M. B. Limkar, "A biometric-secure cloud based e-voting system for election processes," *International Journal of Electrical and Electronics Engineering Research (IJEEER),* 2014, vol. 4(2), pp. 145–152.

[26] R. G. Sharmila, R. Sridhar, P. Subhash and T. Steffy, "Aadhaar based biometric electronic voting to avoid rigging," *International Journal of Innovative Research in Computer and Communication Engineering,* 2017, vol. 5(3), pp. 4766–4770.

[27] P. P. Shendage and P. C. Bhaskar, "Distributed server approach for novel e-voting system with biometric authentication using aadhaar card," *International Journal for Scientific Research and Development*, 2017, vol. 5(3), pp. 1593–1597.

[28] S. Snega, S. Saundarya and R. Balraj, "Highly secured electronic voting machine using aadhaar in IOT platform," *International Journal of Electrical and Electronics Research*, 2018, vol. 6(2), pp. 41–47.

[29] M. Sudhakar and B. S. S. Divya, "Biometric system based electronic voting machine using arm9 microcontroller," *Journal of Electronics and Communication Engineering,* 2015, vol. 10(1), pp. 57–65.

[30] R. H. Syed, M. A. Miah, B. Prasanta, U. A. Akhlak and K. Robi, "Finger print enabled electronic voting machine with enhanced security," *International Journal of Engineering and Technology,* 2015, vol. 5(6), pp. 368–374.

[31] S. N. Syed, Z. S. Aamir and N. Shabbar, "A novel hybrid biometric electronic voting system: integrating fingerprint and face recognition," *Mehran University Research Journal of Engineering and Technology,* 2018, vol. 37(1), pp. 59–68.

[32] P. Tamilarasu, S. Aadhithyan, K. Gowthaman and V. Hariprakash, "Fingerprint based electronic voting machine," *International Journal of Current Engineering and Scientific Research (IJCESR),* 2018, vol. 5(2), pp. 67–70.

[33] C. Tamizhvanan, S. Chandramohan, A. N. Mohamed, P. K. Pravin and V. Vinoth, "Electronic voting system using aadhaar card," *International Journal of Engineering Science and Computing,* 2018, vol. 8(3), pp. 16501–16503.

[34] N. Thamizharasan, and A. Geetha, "Integration of biometric sensor with aadhar for voting process," *Journal of Environmental Nanotechnology,* 2017, vol. 6(1), pp. 19–22.

[35] S. T. Trupti, S. Palak, D. P. Rashmi, K. Samit and K. Saurabh, "Smart voting machine," *International Journal of Science Technology and Engineering,* 2017, vol. 3(12), pp. 143–147.

[36] G. Valarmathy, V. Saranya, R. C. Riya and K. Poovizhi, "Smart voting system using aadhar," *International Journal of Research in Electronics (IJRE),* 2017, 4(1), 14–17.

[37] N. G. Varsha, J. Sangamesh, R. Shravya and Shivaraja, "Aadhar based biometric voting system," *International Journal of Advance Research, Ideas and Innovations in Technology*, 2018, vol. 4(3), pp. 424–427.

[38] Anisaara, N., Rakhi, B., Ashmita, K., Durgesh, G., and Tushar, N. (2015). An implementation of secure online voting system. International Journal of Engineering Research and General Science, 3(2), 1110–1118.

[39] K. M. Isaac, "Citizens' readiness to adopt and use electronic voting system in Ghana," *International Journal of Information and Communication Engineering*, 2016, vol. 10(3), pp. 795–801.

[40] L. Loeber, "E-voting in the Netherlands; past, current, future?" In Proceedings of the 6th international conference on electronic voting (EVOTE). TUT Press, Tallinn, 2014, pp. 43–46.

[41] World Bank, "Population, total". Retrieved May 28, 2018 from https://data.worldbank.org/indicator/SP.POP.TOTL,2018

[42] V. Jonathan and M. A. David, "Demographic turning points for the United States: population projections for 2020 to 2060,"United States Census Bureau, 2018, 1–15.

[43] G. Dave, “Introducing biometrics in the U.S. voting process,” 2016, Retrieved May 28, 2018 from https://www.biometricupdate.com/201610/introducing-biometrics-in-the-u-s-voting-process-qa-with-dave-gerulski.
[44] Brennan Center for Justice, “Election 2016 controversies,” Retrieved May 29, 2018 from https://www.brennancenter.org/sites/default/files/analysis/Fact_Sheet_Voting_System_Security.pdf.
[45] G. P. Omondi, “A mobile web based electronic voting system: a case study of Strathmore University student council,” An unpublished master thesis, Strathmore University, Kenya.
[46] F. A. Diego, Y. S. B. Pedro, N. C. C. Thiago, L. A. Caio and M. Paulo, “The return of software vulnerabilities in the Brazilian voting machine,” 2018, Retrieved May 29, 2018 from https://www.researchgate.net/publication/323470546_The_Return_of_Software_Vulnerabilities_in_the_Brazilian_Voting_Machine
[47] M. Kitsing, “Rationality of internet voting in Estonia,” *Electronic Government and Electronic Participation*, 2014, 55–65.
[48] M. Lilian, “Namibia Becomes First African Country to Adopt E-Voting,” 2014, All Africa. Retrieved May 31, 2018 from http://allafrica.com/stories/201411280145.html
[49] E. Victor, “Inside Nigeria’s first ever electronic voting exercise in Kaduna State,” *Techpoint*, 2018, Retrieved May 30, 2018 from https://techpoint.ng/2018/05/14/kaduna-electronic-voting/
[50] B. Emma, "7 Things to know about the Dutch election results of 2019", 2019. Retrieved May 29, 2019 from https://dutchreview.com/news/politics/5-things-to-know-about-the-dutch-election-results-of-2019/
[51] S. Kumar, “What is the cost of getting an Aadhaar card?”, Quora, Retrieved on June 21, 2019 from https://www.quora.com/What-is-the-cost-of-getting-an-Aadhaar-card at 11.00GMT
[52] Indianmart, “Aadhar kits”, Retrieved on June 21, 2019 from https://dir.indiamart.com/impcat/aadhar-kit.html at 11.44GMT

Authors’ Profiles

Adewale Olumide Sunday is a Professor of Computer Science, Department of Computer Science, School of Computing, Federal University of Technology (FUTA), Akure, Nigeria. He has Ph.D. in Computer Science, Federal University of Technology, Akure, Ondo State, Nigeria in 2002; M.Tech in Computer Science, Federal University of Technology, Akure, Ondo State, Nigeria–1998; BSc Computer Science with Mathematics Ogun State University (Now OOU), Ago Iwoye, Nigeria, in 1991. His Research/Areas of Interest are Cyber Security, Software Engineering, E-Learning and Digital Library. He is a member of many professional bodies. He is a member of Institute of Electrical and Electronic Engineers and Association of Computer Machineries (135763); Member, Infonomics Society, United Kingdom; Member, Computer Professional & Registration Council of Nigeria (CPN). At present, Prof. Adewale is the Dean, School of Computing, Federal University of Technology, Akure (FUTA), Nigeria.

Olutayo Boyinbode (PhD) is an Associate Professor at the Department of Information Technology, Federal University of Technology, Akure, Nigeria. Her research interests are Mobile and Ubiquitous Learning, Mobile Networks, Machine Learning and Internet of Things for Development ((IoT4D). She has several publications in reputable peer-reviewed journals and has also served as a reviewer to several peer reviewed journals. She is a professional member of Association for Computing Machinery (ACM) and Institute of Electrical and Electronics Engineers (IEEE).

Salako E. Adekunle received a degree (B.Eng) in Electrical and Computer Engineering, Master of Technology (M.Tech) in Computer Science from Federal University of Technology, Minna, Niger State. At present, he is a PhD student in Computer Science at the Federal University of Technology, Akure, Nigeria. He is a member of the Nigeria Computer Society and Teachers Registration Council of Nigeria (TRCN). His research interests include Biometric Security, Educational Technology and Control Technology. He has published papers in reputable local and international journals and his published textbooks included Introduction to Computer Logic, Learning Pascal Made Easy, A Handbook on Symbolic Logic and BASIC Programming Language.

How to cite this paper: Adewale Olumide S., Boyinbode Olutayo K., Salako E. Adekunle, " A Review of Electronic Voting Systems: Strategy for a Novel", International Journal of Information Engineering and Electronic Business(IJIEEB), Vol.12, No.1, pp. 19-29, 2020. DOI: 10.5815/ijieeb.2020.01.03

