Computer Engineering and Applications Vol. 12, No. 2, June 2023

Voice Recognition Systems for The Disabled Electorate: Critical Review on Architectures and Authentication Strategies

Olayemi Mikail Olaniyi[1*], Jibril Abdullah Bala[2], Shefiu Ganiyu[3], Yunusa Simpa Abdulsalam[4], Chimdiebube Emmanuel Eke[5]

[1]*Department of Computer Engineering, Federal University of Technology, Minna, Nigeria.*
[2]*Department of Mechatronics Engineering, Federal University of Technology, Minna, Nigeria*
[3]*Department of Computer Science, Kampala International University, Kampala, Uganda*
[4]*Department of Information Technology, Federal University of Technology Minna, Nigeria.*
[5]*Department of Computer and Communication Science University Mohammed VI Polytechnique Morocco*
**mikail.olaniyi@futminna.edu.ng*

ABSTRACT

An inevitable factor that makes the concept of electronic voting irresistible is the fact that it offers the possibility of exceeding the manual voting process in terms of convenience, widespread participation, and consideration for People Living with Disabilities. The underlying voting technology and ballot design can determine the credibility of election results, influence how voters felt about their ability to exercise their right to vote, and their willingness to accept the legitimacy of electoral results. However, the adoption of e-voting systems has unveiled a new set of problems such as security threats, trust, and reliability of voting systems and the electoral process itself. This paper presents a critical literature review on concepts, architectures, and existing authentication strategies in voice recognition systems for the e-voting system for the disabled electorate. Consequently, in this paper, an intelligent yet secure scheme for electronic voting systems specifically for people living with disabilities is presented.

Keywords: authentication; biometrics; e-voting; security; voice recognition

1. INTRODUCTION

Democratic communities are established on the threshold of inclusiveness and participation. These characteristics ensure fairness and wholesome accountability by including a community's eligible citizenry in the democratic voting process of electing leaders. Recent observations identified a wide gap between the People living with Disability (PWD) community and mainstream society owing to a lot of misinterpretation of the roles and responsibilities of the underrepresented disability community who are involved in affairs of democratic governance [24]. This phenomenon results in some state policies and development programs designed at the exclusion of persons with disabilities [11]

By global statistics, more than one billion persons are PWDs, and 0.125% of the national population are living with one form of disability or the other [11]. Imperative to these looming statistics, the National Population Commission of Nigeria (NPopC), estimates PWDs to be 19 million in the country [36,54] . Although, recent statistics show a staggering figure of 25 million people, and that number is still increasing[17,30].

The Nigerian Constitution guarantees equal citizenry rights to vote for persons that have attained the age of 18 years. The ratification of the United Nations Convention on the rights to vote with Disability (UNCRD) and its operational protocol specifically made adjustments in the context of personal assistance, accessible communication, and prioritization at the polling stations[55]. However, literary evidence indicated that many PWDs continue to experience discrimination and exclusion, including the right to vote and disability-specific challenges. Key obstacles to voting include lack of access to the polling booths, ballot boxes, long wait before the casting of vote, discrimination, and embarrassment [11][51]

Voting provides individuals the opportunity to influence decisions that affect their lives, and many eligible voters among the PWDs do not vote as it could have an impact on their well-being and their overall development. Although, multiple reasons account for the inability of the PWDs to vote, in many cases, the inability of the electoral body to find out and consider the specific election-related needs of the PWDs appears to be one of the strongest factors [11]. A case study in [11] further discriminated the population data of eligible voters living with disabilities in seven Nigerian states involving a total of 26,854 persons. The percentage of disabled people with difficulty in speech, and/or hearing issues was estimated at 16.92% and is shown in Table 1. This segment of the disabled voting population cannot authenticate effectively using their voiceprints and are therefore not considered in the scope of this study.

TABLE 1.

Population estimate of disabled persons in seven Nigerian states [11]

State	Disability Cluster						
	Physical Disability	Deafness	Blindness	Leprosy	Albinism	Total	Percentage
Abia	1410	661	807	295	597	3770	14.04
Enugu	192	11	103	28	31	365	1.36
Gombe	614	219	321	63	07	1224	4.56
Kano	9178	3270	3767	346	1179	17740	66.06
Lagos	944	258	254	785	206	2447	9.11
Plateau	435	89	157	06	06	693	2.58
Rivers	502	35	56	07	15	615	2.29
Total	1375(49.43)	4543(16.92)	5465(20.35)	1530(5.70)	2041(7.60)	26854	100

Primarily, the purpose of this study is to critically review existing literatures on voice recognition and authentication schemes for secured electronic voting (e-voting) systems for both able and PWDs, and use the observed gaps to make a technical design case for an intelligent voice recognition system. The system would be able to recognize voice features using text-dependent recognition to ensure voter verification and authentication for PWDs thereby increasing their active participation and inclusiveness in the electoral process. It should be noted that only eligible voters shall be able to cast their respective votes, while the voting system records the votes correctly with valid and demonstrable authentic election records. The remaining sections of this paper are organized as follows: Section 2 presents a background of some concepts of electronic voting, Section 3 reviews related literature, and an

ISSN: 2252-4274 (Print)
ISSN: 2252-5459 (Online)

analysis of the works reviewed is presented in Section 4. Section 5 presents the proposed system and Section 6 concludes the paper.

2. RELATED FUNDAMENTAL CONCEPTS

This section reviews background concepts of e-voting, biometrics, voice recognition, and the different methods implemented in state of art voice recognition systems. This section also presents and critically examines speaker identification and speaker verification as major concepts considered in the development of voice recognition systems.

2.1 ELECTRONIC VOTING (E-VOTING)

A major downside of traditional paper-based voting systems is that it allows alteration of election results. Election results can be easily altered to favour a particular candidate since manual counting is usually adopted by these traditional voting systems [3]. Faults like this in traditional paper-based voting systems required optimal solutions hence the advent of electronic voting systems. Simply put, an electronic voting system is a progressive and innovative component of electronic governance. It seeks to avail citizens of voting age the fundamental right to choose their leaders irrespective of location, time, and physical wellbeing. The e-voting system is a digitised procedure that is meant to circumvent the manual and tedious processes of a paper-based voting system [1][32]. However, e-voting has been constantly bedevilled by some security challenges such as authentication and privacy of voters at one hand, and the confidentiality, integrity, and transparency of the voting process on the other hand [1][35]. Simply put, an authentication challenge arises when an e-voting system is infiltrated physically or digitally by unauthorized people. In addition, hackers could obtain the authentication credentials of e-voters via attack vectors like man-in-the-middle, spoofing, malicious software, and social engineering amongst others [50]. This challenge can be addressed by ensuring that voters are whom they claim to be during voter registration and voting session. Thus, several authentication methods including typical biometric features, multi-modal biometric authentication, two-factor authentication, and blockchain have been proposed and developed to reinforce the security of e-voting systems [1,2,5,6,8,16,31,32,35,40,59]. Although, hand gesture recognition_wearable glove-based sensor approach and the camera vision-based sensor approach [25] as well as [60] can also be applied for the deaf with appropriate design considerations. In addition to authentication, an e-voting system should possess the following attributes for it to meet democratic standards:

i) **Integrity:** Electronic voting systems can foster integrity by setting up measures to ensure that votes cannot be modified, forged, or deleted without detection.
ii) **Uniqueness**: An electronic voting system should allow no room for any voter to be able to vote more than one time.
iii) **Accuracy:** Accuracy of e-voting systems is a prime requirement. It is the ability of an electronic voting system to record the votes correctly. Virtually, all stakeholders will lose interest in a result emanating from a compromised election exercise.

iv) **Eligibility:** The e-voting system must ensure that only eligible voters who meet the established voting conditions are allowed to cast their votes.

v) **Audit trail:** Trails of important interactions by all stakeholders should be logged by the e-voting system. Records of the interactions must be secured, preserved, and presented in ideal formats for future forensic audit and election result reconciliations.

vi) **Transparency**: The procedures guiding the operations of the e-voting system must be transparent to all parties. Sufficient stakeholder meetings must be conducted to explain and demonstrate the working processes of the systems. All concerns and agitations relating to transparency must be resolved before deploying the system.

vii) **Anonymity:** The candidate voted for by an electorate must be anonymous, that is, should not be disclosed to candidates or parties. Furthermore, the system must make it impossible to trace back any vote to an electorate.

viii) **Robustness:** It should be agile enough to withstand an unexpected voter turnout, including the individual and general demands of voters in such a situation.

ix) **Flexibility:** The e-voting system must be flexible enough to accommodate last-minute changes that may be required by the law before election time, without jeopardising other attributes.

x) **Total Experience:** The e-voting system must leave all the election stakeholders satisfied at the end of the voting process by establishing open communication among stakeholders throughout the election lifecycle.

2.2 BIOMETRICS

Biometrics is a useful method of identifying and verifying individuals in a rapid and effective manner by utilizing unique biological features. Biometric systems typically register people when one or more of a person's physical and behavioural traits are acquired, processed by a numerical algorithm, and eventually recorded in a database. The algorithm generates a digital representation of the biometric data. If the user is new to the system, he or she enrols, which implies that the biometrics' digital template is saved in the database. Each subsequent attempt to utilize the system, or authentication, necessitates the user's biometric being recorded and processed into a digital template. To identify a match, that template is compared to those already in the database. Each time a user attempts to authenticate to the system, the process of converting the collected biometric into a digital template for comparison is performed. A Hamming distance is used in the comparing procedure. This is a metric for determining how similar two-bit strings are. Two identical bit strings, for example, have a Hamming distance of zero, but two completely different ones have a Hamming distance of one [37]. For better subject security application of biometrics, using multimodal biometric traits are more secured than unimodal applications [12].

ISSN: 2252-4274 (Print)
ISSN: 2252-5459 (Online)

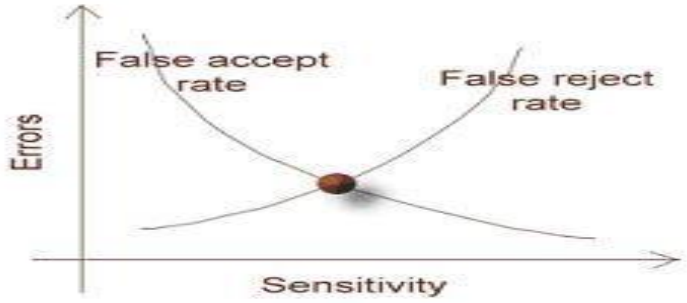

FIGURE 1. Performance Evaluation of Biometric Systems [37]

Performance of a biometric measure shown in Figure 1, is usually referred to in terms of the false accept rate (FAR), the false non-match or reject rate (FRR), and the failure to enroll rate (FTE or FER). The FAR measures the percent of invalid users who are incorrectly accepted as genuine users, while the FRR measures the percent of valid users who are rejected as impostors. In real-world biometric systems, the FAR and FRR can typically be traded off against each other by changing some parameters. One of the most common measures of real-world biometric systems is the rate at which both accept and reject errors are equal: the equal error rate (EER), also known as the crossover error rate (CER). The lower the EER or CER, the more accurate the system is considered to be.

[44] segregated biometric systems into two distinct parts; identification and verification and their respective relationships in datasets are explained thus:

Identification (1: n): 1: n signifies a one-to-many kind of mapping. Biometrics could be used to establish a person's identity even without his or her consciousness or approval. For example, by scanning a crowd with the help of a camera and using face recognition technology, one can confirm matches that are already stored in a database.

Verification (1:1): This is a one-to-one type of mapping. Biometrics is also be used to verify a person's uniqueness. Such as one can allow physical access to a secured residence by using finger scans or can gain access to a bank account at an ATM by using a retina scan.

Authors in [43] identified the properties that determine the usability of biometrics systems to include:

a) **Permanence:** Biometric systems should be able to generate the same results for each individual and over time.
b) **Universality:** The biometric trait to be used by the biometric system must be common to all individuals involved.
c) **Measurability:** The biometric parameters used by the biometric system should be easily measured to determine its performance.

d) Uniqueness: The biometric trait or parameter to be adopted by any biometric system should be different, unique, and exist for every individual over a reasonable time frame.
e) Performance: A biometric system should be fast, accurate, and robust in the identification and authentication process.
f) Acceptability: This is the general affirmation of biometric systems by the users for ease of use and minimal or no inconvenience.
g) Invasiveness: Does the biometric system require the introduction of an instrument into a body part? For example, DNA requires blood for testing.
h) Collectability: How efficient does a biometric system capture and quantify the biometric traits.

Based on the properties of biometric systems, [47] drew a comparison based on the different biometric traits to determine their usability. Table 2 gives a summary of their individual properties.

TABLE 2.
Comparison of biometric data [47]

Property	Iris	Retinal	Finger Print	Palm Print	Hand Geometry	Face	Ear	DNA	Voice
Uniqueness	H	H	H	H	M	M	M	H	L
Permanence	H	H	H	H	L	M	M	H	L
Universality	H	H	M	M	H	H	H	H	M
Measurability	M	L	H	H	H	M	M	L	M
Collectability	H	M	M	M	H	H	M	L	M
Invasiveness	M	H	M	M	M	L	L	H	L
Performance	H	H	M	M	M	L	L	H	L
Acceptability	M	L	H	H	M	H	M	H	H

- H=High L=Low M=Medium

2.3 VOICE RECOGNITION SYSTEMS

Voice recognition and speech recognition are technologies that are interchangeably used. Despite being similar, they are quite different in their uses and applications. Primarily, the purpose of speech recognition is to arrive at words that are spoken. Hence, speech recognition systems eliminate features such as accents to detect words. Voice recognition systems on the other hand aim to identify the person speaking the words, rather than the words themselves. Voice recognition is also referred to as speaker recognition and it disregards language. Authors in [27] categorized voice recognition systems into two parts:

I. Speaker Identification: The process of identifying a voice of a given speech from a dataset of speakers is called speaker identification. The speaker whose maximum voice traits match with the stored voice is identified. The known sets of voices are divided into two parameters called open-set mode and the close-set mode. In the Open set mode, the speaker need not be known within a dataset. This is used in some criminal cases where out of several suspects, the identity of the main criminal is revealed. In close-set parameter mode, the

ISSN: 2252-4274 (Print)
ISSN: 2252-5459 (Online)

speaker's voice is already available in the database. This method is used for authentication purposes to identify the authorized person out of multiple claimed persons.

II. **Speaker Verification:** The speaker verification process, accepts or rejects the identity claim of a speaker. It is used for the verification of a person claiming for authentication. This process is generally referred to as an open set mode as it requires checking the authentication of voice from the set of speakers already known

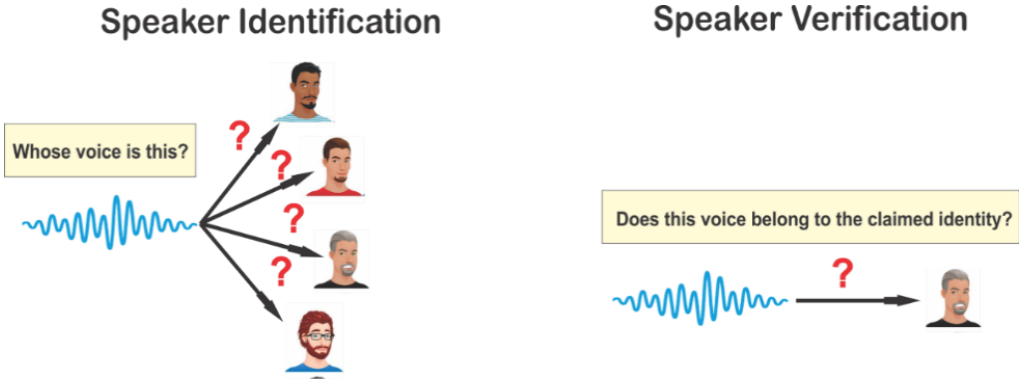

FIGURE 2. Speaker identification vs speaker verification [58]

2.4 SPEAKER VERIFICATION SYSTEMS

Speaker verification systems authenticate voices from the set of already known speakers. These systems accept or reject a claimed identity based on a given speech utterance from the claimed speaker. Speaker Verification Systems are generally classified as text-dependent and text-independents systems. Text-dependent systems use fixed text passphrases for the verification process whereas text-independent systems make speaker verification possible with spontaneous speech [46]. Speaker verification systems usually consist of the five components as shown in Figure 3.

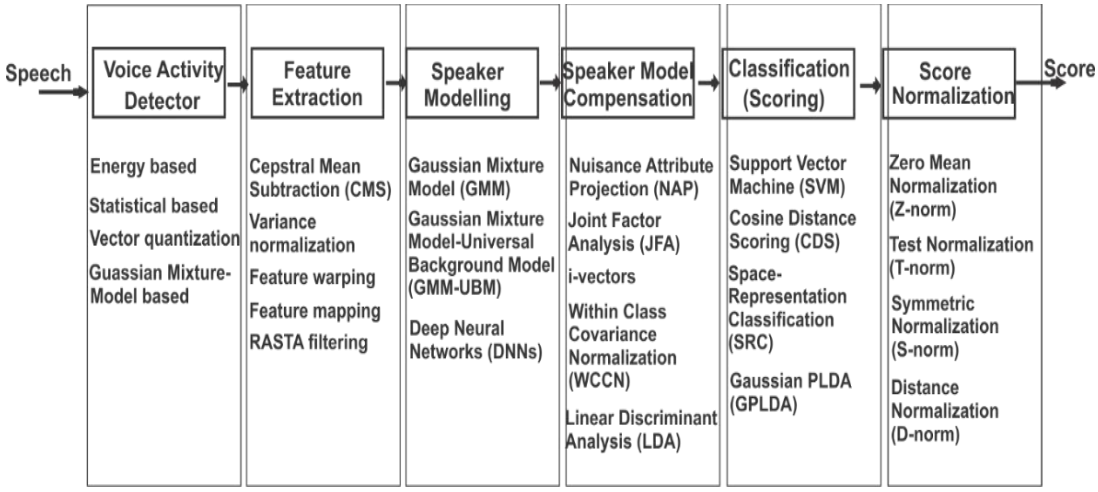

FIGURE 3. Components of speaker verification systems [46]

Voice Activity Detection: identifies and removes non-speech segments from speech segments. Non-speech segments normally include silence, noise, music, and other acoustic signals in an utterance. Usually, audio signals are divided into frames containing features of the audio signal. These features are extracted from the audio signal and then compared to a threshold limit. In situations where the features from the input frame exceed the threshold value, a decision is computed on the existence of speech in the input frame.

Feature extraction: Features are mathematical representations of raw speech waveforms. Features can be short-term spectral, prosodic, high level, or deep features. The Mel Frequency Cepstral Coefficient (MFCC) is the most used feature in voice recognition systems. It captures the magnitude spectrum of the speech signal from human voices better than other features [4]. In the extraction of MFCC features, the speech is transformed to a Fourier domain after passing through a Hamming window. Then, Mel scale filters are then applied to the amplitude spectrum of the transformed speech. Equation (1) is used to convert the normal frequency to the Mel scale with the relation:

$$F_{mel} = 2595 log_{10}(1 + \frac{f_{Hz}}{700}) \quad (1)$$

The log energies of the Mel filtered spectrum are then de-correlated using the discrete cosine transform to obtain MFCCs. Thus, Figure 4 shows the process of MFCC feature extraction.

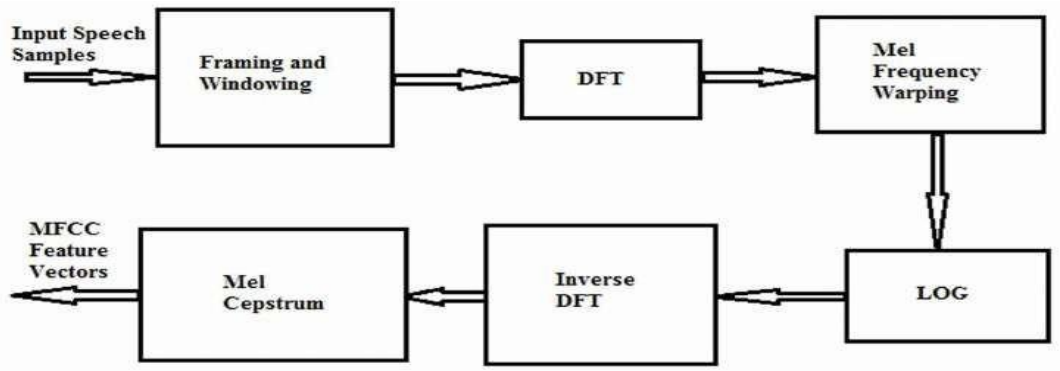

FIGURE 4. MFCC feature extraction [23]

Speaker modelling and Compensation: Extracted features are compared to a speaker model that represents the supposed speaker identity and a background model that represents all other speakers that are not the supposed speaker. Gaussian mixture model – Universal background model (GMM-UBM) is traditionally used for speaker modelling, although there are rising interests in the use of Deep Neural Networks (DNNs) [56].

ISSN: 2252-4274 (Print)
ISSN: 2252-5459 (Online)

Channel Normalization: Normalization is typically a process of reducing the mismatch of channel conditions between training and test data. The channel includes all the spectral characteristics of the voice recording and the microphone, as well as the background noise. Channel normalization could be done at the feature extraction level, the speaker model level, and the score level.

Channel-dependent and speaker-dependent variabilities present major challenges in designing speaker verification systems. Environmental noise, room reverberations and slight changes in recording devices constitute channel-dependent variations whereas speaker-dependent variabilities result from changes in the speaker's voice due to mood, age or sickness [57]. In general, these variations cause mismatch between training data and the test data and possibly limiting recognition accuracy. Hence, achieving a significant level of robustness under noisy conditions is central to designing speaker verification systems. Each of the aforementioned components present various algorithms that can be used to mitigate the effect of noise interference from the pre-processing to post-processing phases of speaker verification systems.

3. REVIEW OF RELATED LITERATURES

The reviewed literature is classified under electronic voting systems and voice recognition systems and also a combination of these systems in the parent work. The aims, methodologies, strengths, and weaknesses are discussed, analysed and evaluated.

3.1 ELECTRONIC VOTING SYSTEM

Several researches have been carried out in the area of electronic voting. To begin with, [53] developed a fingerprint biometric authentication system for a secure electronic voting machine. The author's inclusion of biometrics improved the security feature of the system and tackled the challenges of authentication of users or voters. The electronic voting system was made up of hardware and software components. The software components included the web graphical user interface (GUI), fingerprint registration and the authentication element which were all implemented on a Raspberry Pi 3B+. The performance of the developed system was evaluated using False Accept Rate (FAR), False Reject Rate (FRR) parameters and the response time of the system. The results showed significant improvement from the conventional paper-based system in terms of transparency, mobility and efficiency.

On the application of biometric to e-voting security,[8] proposed a secured electronic voting system that attempted to prevent bogus voting using a multi-modal biometric authentication system. Also, the architecture of the proposed system could mitigate adversary attacks through firewalls and encryption of vital data. However, the authors did not implement proposed system. In addition,[5] proposed a biometric authentication scheme for user authentication and multi-key security measure for secured communication between pooling stations that are collaborating in an e-voting

environment. Essentially, the system proposed by [5] focused on system usability and security of election processes. For instance, the multi-key security control enabled the system to survived Sybil, wormhole, and HELLO flood attacks. Also, the experimental validation conducted by the authors to ascertain the level of user satisfaction, effectiveness, and efficiency of the developed voting system showed impressive results.

By applying cryptographic concepts, [14] developed a crystographic system that combined post-quantum cryptography with steganography to ensure that the security of electronic voting is maintained. The main objective of the authors was to ensure the confidentiality of information about voters and their respective votes. A Multi-party Quantum Private Comparison (MQPC) secured e-voting framework was designed, implemented and tested. The developed electronic voting security system was compared with Rivest-Shamir-Adleman (RSA) and Elliptic Curve Cryptography (ECC) based systems in terms of computation time, size of their outputs and their throughput. Results showed that the proposed MQPC secured e-voting system generally performed better compared to the ECC and RSA based ones. Similarly, [29] developed a secure electronic voting system using a hybrid cryptosystem and steganography. The security scheme was based on a hybrid Rivest-Sharma-Adelman (RSA) algorithm and Advance Encryption Standard (AES) algorithm with Least Significant Bit (LSB) algorithm for securing ballot information and to tackle the problems of privacy, verifiability and integrity. User performance evaluation indicated a high acceptance amongst the proposed users for its full adoption in the electioneering process. Further performance evaluation showed that the system satisfied majority of the security requirements for electronic voting.

Leveraging on the security feature of blockchain, [39] designed an electronic voting system using a blockchain network which ensured integrity of the voting system. The authors adopted a private blockchain network in which data is not accessible from the internet and the system does not need to use any platform. The system consisted of two unrelated databases containing information of people authorized to vote, the blockchain information and both database entities each with different attributes. A voting cell system architecture was used to guarantee the reliability of the system. Overall, the system was able to maintain the secrecy of the vote. However, the presence of malware in the mining computers and in the interconnected devices can alter transactions in the blockchain which is thus a major vulnerability.

Furthermore,[10] proposed a blockchain-based electronic voting system for running elections in Turkey. The authors aimed to ensure security, data integrity of votes and voter's privacy. The system procedures were classified under three major phases which included authentication, voting and counting phases. In authentication, a node on a blockchain gets a voter credentials and sends it with its node identity to the e-government system which validates or rejects the voter's credential. A vote is then added to blockchain and the chain information is updated for all voting machines without revealing any information about the vote. After the voting phase, the total votes for each candidate are then counted using the highest-level chain and the final blockchain can be distributed to any third party to inspect the anonym votes with. The system was regarded as generalizable as it could be modified for different elections

ISSN: 2252-4274 (Print)
ISSN: 2252-5459 (Online)

with ease. Likewise, [2] proposed a mobile voting (m-voting) framework that utilised blockchain and multi-factor authentication security mechanisms. The authors deployed blockchain technology to secure electorate votes and multi-factor authentication to ensure that only eligible voters are allowed to cast their votes.

3.2 VOICE RECOGNITION SYSTEM

In the area of voice recognition systems,[20] designed a robust speech recognition system using conventional and hybrid features of MFCC, Linear Prediction Coding Coefficients (LPCC), Perceptual Linear Prediction (PLP), Relative Spectral Transform - Perceptual Linear prediction (RASTA-PLP) and Hidden Markov Model classifier in noisy conditions. The aim of the authors was to investigate the performance of the extraction algorithms in noisy conditions. The methodology comprised of both statistical and signal modelling. Signal modelling involved the extraction of acoustic features from input speech signal whereas statistical modelling entails matching the features with a reference model to generate a recognition result. The proposed system used a voice dataset of 208 different adult speakers and were evaluated in both training and testing process. Experimental results showed that MFCC obtained the highest recognition rates in very low noise conditions (5db-10db), LPCC method provided the best recognition rates at higher noise conditions (30db) and LPCC and PLP had the best recognition rates for clean speech data.

Also, a deep learning-based voiceprint text-independent authentication system was designed by [9]. The aim of the authors was to utilize the proposed system for both speaker identification and recognition tasks. The methodology involved extraction of audio features MFCC, then a Support Vector Machine (SVM) neural network algorithm was used to train and classify unique audio data. Experiments were carried out using datasets from LibriSpeech with an open-source corpus of almost 1000 hours of open-source speech data. Pre-training experiments showed that lower coefficients (20) used as input to the SVM provided the best accuracies while training and testing. Also, audio files were analysed and segmented in ranges of 2 to 4 seconds depending on the data availability. Based on these findings, two systems were created and tested, the first trained 10-person and 40-person sets from the dataset in LibriSpeech while the other used in-house audio recordings. The system was considered robust because it could accurately handle both regular volume audio and whispering audio.

Similarly,[34] attempted to implement an optimized approach to improve accuracy in Internet of Things (IoT) devices that use voice recognition. The aim of the authors was to reduce Hidden Markov Model (HMM) deficiency by implementing Artificial Neural Networks (ANN) more specifically Multi-Layer Perception (MLP). A mathematical model was derived for the optimized approach. Feature extraction was done using MFCC algorithm and ANN was used for the classification of phonemes due to its high discriminative power. The algorithms were implemented in a Raspberry Pi for home mechanization, robot appliance and soon to identify spoken words. The testing and training were observed to be much faster using this approach.

Likewise, author in [15] designed and developed an integrated biometric voice system that uses continuous speech recognition. The aim of the authors was to implement the designed system in home automation and robotics. In the methodology, Google speech API was used for speech recognition and MFCC for speaker identification. Three different tests were conducted, the first with real registered users, then fake users inclusive and the last included unregistered users. Final results showed an overall system efficiency of 96.4%. The authors suggested the system could be more robust if adapted to effectively function in noisy environments.

Relatedly,[23] designed a cloud based organizational information access system using voice as a means of authentication. The aim being to tackle security and privacy issues in cloud computing as it increasingly becomes an in-demand technology. In the designed voice authentication system, MFCC was used for feature extraction due to its combining power of cepstrum analysis with a perceptual frequency scale in critical bands and Dynamic Time warping (DTW) was implemented in the speaker recognition model, mainly for its efficiency in solving time alignment problems. Experimental results showed some levels of optimal performance. However, it was concluded that the accuracy of the voice recognition could be significantly increased by considerable use of statistical recognition models.

Furthermore,[26] worked on a user identification system powered by biometrics speaker recognition using MFCC and Dynamic Time warping (DTW) alongside signal processing techniques. The aim of the author was to build a robust user identification system that uses precise voice recognition to increase data security and reduce to the barest minimum or possibly eliminate illicit access. The methodology comprised of several digital processing steps which were carried out for noise removal and extraction of voiced segment, then feature extraction was performed using MFCC and DTW was used for comparison for voice samples. All experimental results and simulations were carried out in MATLAB. The results showed significant variations between different speaker's signals and no variation for the same speaker signals. The system was however, tested using a few numbers of speakers and also voice input and the author stated that consideration should be made using existing methods for a much larger domain of users.

In addition, research was carried out by [7] to evaluate the performance of noisy input in a continuous speech signal using both Voice Activity Detection (VAD) and Speech Enhancement Algorithm (SEA). The authors made use of a speech-to-text system using continuous word recognition with a vocabulary of ten words. An 8-bit Pulse Code Modulation (PCM) with an 8kHz sampling rate was used to record the continuous words during the training phase and then save it as a wave format file. Features were extracted using Linear Predictive Coding (LPC) Coefficients then, Hidden Markov's Model (HMM) was used to model each given word in the vocabulary and train them. The methods were carried out using MATLAB. The proposed speech recognition system achieved an overall Recognition Accuracy (RA) of 72.45%. It was concluded that an increase in the Signal to Noise Ratio (SNR) value will lead to a percentage increase of the Automatic Speech Recognition (ASR) system. Also, results indicated that the variation of average speech recognition accuracy is consistent in all SNR conditions.

ISSN: 2252-4274 (Print)
ISSN: 2252-5459 (Online)

Also, [18] designed a corpus for a forensic speaker recognition system. The aim of the authors was to design a speaker recognition system that uses audio recordings as forensic evidence in trials or security systems. The speaker's voices were recorded in Spanish dialect. In the methodology, MFCC was used for feature extraction and Gaussian Mixture Model (GMM) was used to create the model characteristics of the signal speech by comparing voice models from each speaker in the training corpus with the test data. Then, maximum likelihood estimation was used to classify the voice samples due to its computing ease. Results showed a high accuracy of more than 93% identification of a speaker under any condition. A limiting factor as stated by the authors was that the system could falter if processing was put under a time constraint.

Consequently, [48] carried out research to evaluate the performance of algorithms used for discrimination in speech recognition systems by using each algorithm or combinations of both. The objectives of the research were to develop an application that integrates different discriminative algorithms, study the effects of the integration on overall recognition accuracy and obtain the highest accuracy possible in minimal time. The experiments were carried out in a room using a low-quality microphone. Major conclusions drawn from the results were that more training samples improved recognition rate and that the integration process enhanced greater stability in the overall recognition process under different conditions. However, the author made mention that more effective ways in aiding noise removal would definitely improve the throughput of speech recognition systems.

[30] designed an electronic voting system to address voter's authentication and verification specifically for people living with disabilities. The system authenticates voters by taking in their unique voice biometric, using MFCC for feature extraction which is proven to have a high perception level of the human voice and Dynamic Time warping (DTW) as a classifier for feature classification. However, the system classifier can only handle a limited number of templates. Tables 3 and 4 presented summaries for related works in electronic voting systems and voice recognition systems respectively.

TABLE 3.
Comparison of related works in electronic voting systems

S/N	Authors	Title	Method Used	Problem Solved	Limitations
1	[53]	Development of a secure electronic voting machine that uses fingerprint biometric for authentication	Fingerprint Biometrics	Voter's Authentication	Slower response time as voter's fingerprint needs to be captured twice during registration.
2	[14]	Development of a new crystographic system that combines	Cryptography & Steganography	Ballot Confidentiality	Crystographic technique is not cost feasible due

		post quantum cryptography with steganography to ensure secure electronic voting			to the need for quantum computing.
3	[10]	Proposal of a blockchain-based electronic voting system for running elections in Turkey	Blockchain Technology	Anonymity, Ballot Integrity	The electronic voting system was designed specifically for elections in Turkey.
4	[39]	Design of a electronic voting system using a blockchain network	Blockchain Technology	Ballot Integrity	Malware in the mining computers and associated devices can alter transactions in the blockchain
5	[29]	Development of a secure electronic voting system using hybrid cryptosystem and steganography	Cryptography & Steganography	Anonymity, Ballot Integrity	Prone to DoS and DDos attacks
6	[30]	V-Authenticate: Voice Authentication System for Electorates Living with Disabilities.	Voice Biometrics	Voter's Authentication	DTW can handle only a limited number of templates
7	[5]	Development of biometric user authentication and secured pooling station communication	Biometric and Multi-key information encryption	Message exchange between pooling stations	Only finger print was used for user authentication
8	[42]	Trustworthy Electronic Voting Using Adjusted Blockchain Technology	Blockchain Technology and Biometrics	Security of Voting Data	Unsuitable for realtime implementation based on the assumption that there is uninterrupted connectivity
9	[19]	Decentralized Electronic Voting System Based on Blockchain Technology Developing Principals	Blockchain Technology	Reliability, transparency and anonymity of voting process	Absence of biometrics for voter validation increases the risk of identity theft

ISSN: 2252-4274 (Print)
ISSN: 2252-5459 (Online)

10	[8]	On the Design and Implementation of a Blockchain Enabled E-Voting Application Within IoT-Oriented Smart Cities	Blockchain Technology and IoT	Security of IoT based e-voting systems	Study provided simulation results and no information on realtime performance
11	[38]	SeVEP: Secure and Verifiable Electronic Polling System	Multifactor and Cryptographic Technique	Verifiability, multiple voting and prevents double voting.	Lacks scalability and usability in a real-world deployment
12	[13]	Blockchain 3.0: Towards a Secure Ballotcoin Democracy through a Digitized Public Ledger in Developing Countries	Blockchain Technology	Security e-voting systems in a Digitized Public Ledger	Lacks key requirements of secure voting system, such as confidentiality, and privacy.
13	[52]	Votereum: An Ethereum-Based E-Voting System	Blockchain Technology	Security and privacy requirements in voting	Lacks resistance towards coercion and receipt-freeness.
14	[28]	Developing Multi-factor Authentication Technique for Secure Electronic Voting Systems	Multifactor and Cryptographic Technique	Authentication and Confidentiality security requirements in secure voting	Fails to secure the integrity of the cast votes stored in the database
15	[22]	Blockchain-enabled e-voting.	Blockchain Technology	Allows voters to pay a certain amount to cast votes without the problem of double-spending.	Lacks scalability due to the excessive workload on nodes during simultaneous executions.

TABLE 4.
Comparison of related works in voice recognition systems

S/N	*Authors*	*Title*	*Feature Extraction*	*Classification*	*Remarks*
1	[20]	Robust Speech Recognition System Using Conventional and Hybrid Features of MFCC, LPCC, PLP, RASTA-PLP and Hidden Markov Model	MFCC	HMM	MFCC obtained the highest recognition rates in very low noise conditions (5db-10db)

		Classifier in Noisy Conditions			
2	[9]	Development of a Deep Learning-Based Voiceprint Authentication System	MFCC	SVM	Developed system could handle both regular volume audio and whispering audio samples
3	[34]	Optimized Approach to Voice Recognition Using IoT	MFCC	HMM-ANN	ANN was added in classification to reduce HMM deficiency
4	[15]	Continuous Speech Recognition and Identification of the Speaker System	MFCC	Google Speech API	System was limited to low noise environments
5	[23]	Design of a cloud based organizational information access system using voice authentication	MFCC	DTW	DTW is a less efficient classifier compared to statistical models
6	[26]	Development of a User Identification System Using Biometrics Speaker Recognition by MFCC and DTW along with signal processing package	MFCC	DTW	Limited to a few numbers of speakers
7	[7]	Performance evaluation of a hybrid model of robust automatic continuous speech recognition systems	LPC	HMM	Limited vocabulary helped improve voice recognition rate
8	[18]	Design of a forensic speaker recognition system using a voice corpus with audio recordings as forensic evidence	MFCC	GMM	Processing time was not prioritized in development
9	[48]	Performance evaluation of algorithms used for discrimination in speech recognition systems	MFCC, PLP, ZCR	ANN	ANN requires large amount of training data to obtain good recognition rates
10	[30]	V-Authenticate: Voice Authentication System for Electorates Living with Disabilities.	MFCC	DTW	DTW is a less efficient classifier compared to

ISSN: 2252-4274 (Print)
ISSN: 2252-5459 (Online)

	statistical models

4. ANALYSIS OF EXISTING SYSTEMS

Following close observation of previous related literature, some observations are made and certain conclusions are stated below:

1. Among all the proposed electronic voting systems reviewed, only [30] was specifically designed or had consideration for the physically challenged or disabled electorate.
2. With the exception of [7] all Voice Recognition Systems and ASR's used Mel Frequency Cepstral Coefficients for feature extraction obtaining high recognition at the tail end.
3. Greater stability was attained during the recognition process in [48] when MFCC was combined with one or more extraction algorithms.
4. Voice Activity Detection enhances the overall performance of speaker and speech recognition systems as seen in [7].
5. Electronic voting systems that applied blockchain technology, steganography, and cryptography or hybridized forms in their methodology were majorly focused on solving problems relating to data integrity, voter's confidentiality and authentication. Some of these works [10][14][29][39]. There was less focus on the participation of disabled voters.
6. [53] implemented dual authentication usually with the fingerprint biometric and another means of authentication (RFID, OTP). The designed system made no specific consideration for disabled voters.
7. Distributed and Secure e-voting systems in [6] [13] [19] [22] [31] [39] [42] [52] lacked design consideration for the disabled voters.
8. Comparative review of recent studies in hand gesture detection and classification conducted by [21][33][41] using computer vision techniques, deep learning, segmented augmented reality and interactive digital multimedia could be explored for the deaf voters with appropriate software and design considerations to imbibe requirements of secure e-voting specified in section 2.2.

According to the research works reviewed, a major portion of the literature disregards persons living with disabilities as the major rationale for the work. The literature study reveals researchers' enthusiasm to use MFCC features for extraction in low-noise environments and ensure participation and inclusiveness for non-deaf disabled voters. Furthermore, it has been demonstrated in the literature that the use of statistical models and neural networks in classification greatly improves recognition rates over earlier linear models. The proposed system design given in section 5 aims to overcome the identified research gaps while also incorporating the reviewed works' strengths.

5. PROPOSED DESIGN AND METHODOLOGY

5.1 HARDWARE SYSTEM DESIGN CONSIDERATIONS

The embedded system comprises both hardware and software components. The hardware is comprised of Raspberry Pi 4B, a microphone, a microSD card, and Touchscreen LCD. The software components are the GUI (mobile and web based) and the voice authentication module. The general system block diagram shows the interaction between different components as seen in Figure 5. The Pi 4B acts as the central controller of the system. It receives user input data from the touchscreen unit, manipulates the data behind the scene and provides feedback to the touchscreen unit. The microphone takes in analogue voiceprints of voters converting them to digital signals during voter's enrolment and authentication stages. The touchscreen serves as both an input and output unit displaying data for user interaction and final results of operations.

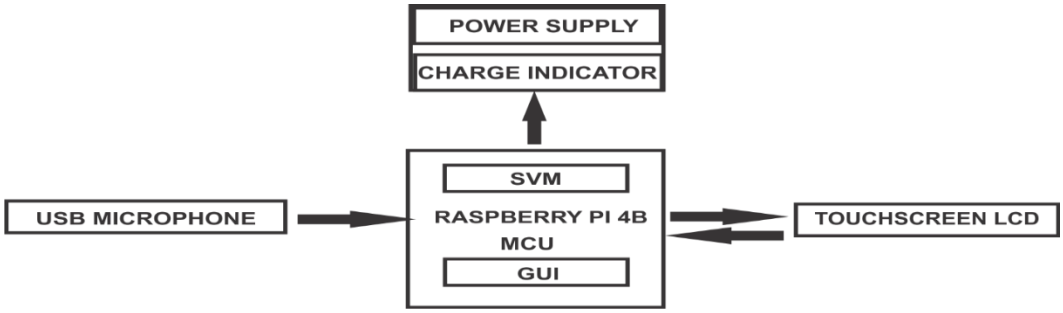

FIGURE 2. System hardware block diagram

5.2 SOFTWARE SYSTEM DESIGN

Administrators or electoral officers and the voters are the end users of this device. Figure 6 describes the system architecture at the different election phases. Voter's registration, candidate registration, auditing of casted votes and results collation are done by administrators. During voter's registration, voters are required to recite two words specific to each user multiple times using a microphone. The voice samples are run through series of algorithms in the voice authentication/verification unit. The features of each unique voter's voiceprint are extracted, classified and modelled for each voter. Each voter voice model is stored in a database and is compared with respective voter's voice samples during the voting process depending on whether a match is found or not. If a match is found, the voter is automatically authenticated and the system allows the voter to cast his/her vote else the system repeatedly rejects authentication when a match is not found.

ISSN: 2252-4274 (Print)
ISSN: 2252-5459 (Online)

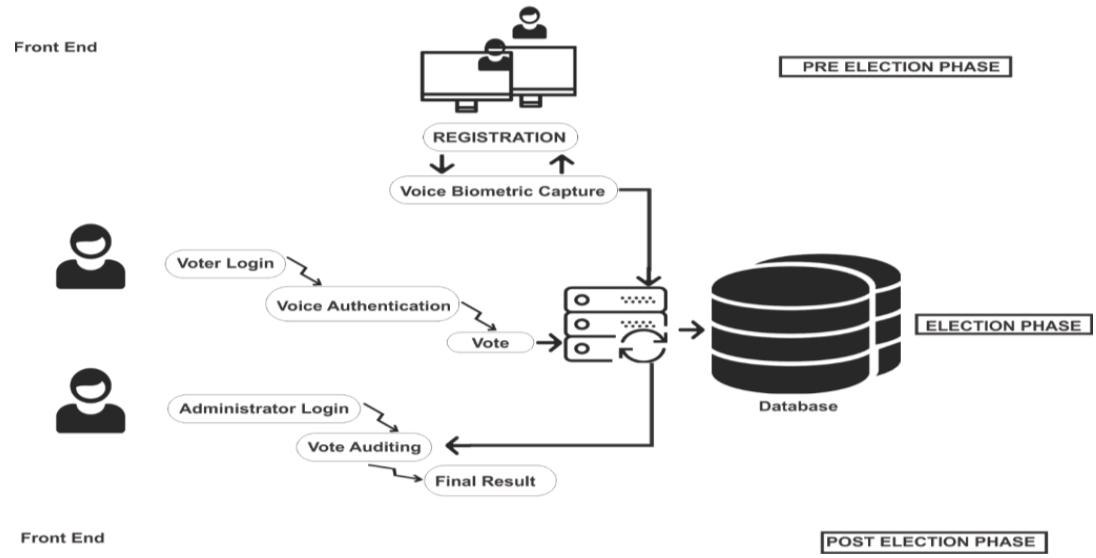

FIGURE 3. Block diagram of the voice authentication unit

6. CONCLUSION AND FUTURE WORKS

Electronic voting systems are ever-evolving and researchers are improving on already existing e-voting systems to satisfy the qualities of voting processes. A critical literature review on existing electronic voting systems and voice recognition systems has been presented with huge gaps for PWD's. Conceptual design for an intelligent voice authentication system has been proposed to address the problem of e-participation of disabled voters in e-democracy. Thus, this study intends to develop the proposed intelligent voice recognition system enabling electronic voting amongst the disabled electorate and evaluate its performance. At this point, the research is open to progressive criticisms and further suggestions.

REFERENCES

[1] Abayomi-Zannu, T. P., Odun-Ayo, I., Tatama, B. F. and Misra. S. (2020) 'Implementing a mobile voting system utilizing blockchain technology and two-factor authentication in Nigeria', *Proceedings of First International Conference on Computing, Communications, and Cyber-Security (IC4S 2019)*, pp.857-872, Singapore.

[2] Abayomi-Zannu, T.P., Odun-Ayo, I.A. and Barka, T.F. (2019) 'A proposed mobile voting framework utilizing blockchain technology and multi-factor authentication', *Journal of Physics: Conference Series*, Vol. 1378, No. 2019, doi:10.1088/1742-6596/1378/3/032104

[3] Adekunle, S. E. (2020). 'A review of electronic voting systems: Strategy for a Novel', *International Journal of Information Engineering & Electronic Business*, Vol. 12, No. 1, pp.19-29.

[4] Admuthe, S. and Patil, P. H. (2015) 'Feature extraction method - MFCC and GFCC used for speaker identification', *International Journal for Scientific Research & Development*, Vol. 3, No. 04, pp.1261–1264.

[5] Ahmad, M., Ur Rehman, A., Ayub, N., Alshehri, M.D., Khan, M.A., Hameed, A. and Yetgin, H. (2020) 'Security, usability, and biometric authentication scheme for electronic voting using multiple keys', *International Journal of Distributed Sensor Networks*, Vol. 16, No. 7, doi: 10.1177/1550147720944025

[6] Ajao, L.A., Umar, B.U., Olajide, D.O., Misra, S. (2022). Application of Crypto-Blockchain Technology for Securing Electronic Voting Systems. In: Misra, S., Kumar Tyagi, A. (eds) Blockchain Applications in the Smart Era. EAI/Springer Innovations in Communication and Computing. Springer, Cham. https://doi.org/10.1007/978-3-030-89546-4_5

[7] Babu, C. G., Sampath, P., Hariharan, S., Balakumar, S. and Noufal, M. (2018) 'Performance analysis of hybrid model of robust automatic continuous speech recognition system', *Proceedings of the International Conference on Inventive Computing and Informatics, ICICI 2017, Icici*, pp.303–306. https://doi.org/10.1109/ICICI.2017.8365360

[8] Bhatti, J., Chachra, S., Walia, A. and Vishal, V. (2019) 'Secure electronic voting machine using multi-modal biometric authentication system, data encryption, and firewall', *International Journal of Performality Engineering*, Vol. 15, No. 10, doi: 10.23940/ijpe.19.10. p2.25702577

[9] Boles, A. and Rad, P. (2017) 'Voice biometrics: Deep learning-based voiceprint authentication system', *2017 12th System of Systems Engineering Conference, SoSE 2017*, doi: https://doi.org/10.1109/SYSOSE.2017 .7994971

[10] Bulut, R., Kantarci, A., Keskin, S. and Bahtiyar, S. (2019) 'Blockchain-based electronic voting system for elections in Turkey', *UBMK 2019 - Proceedings, 4th International Conference on Computer Science and Engineering*, pp.183–188, doi: https://doi.org/10.1109/UBMK.2019.8907102

[11] Centre for Citizens with Disabilities. (2019) *Report on mapping for the needs of persons with disabilities for 2019 General Elections*, 7 June, Retrieved from https://drive.google.com/file/d/1l2ZilOEnAdiLRhxQ19B6ERPCuHxtV1Zg/view?usp=sharing

[12] Channegowda, A. B. and H. N. Prakash. (2021) 'Multimodal biometrics of fingerprint and signature recognition using multi-level feature fusion and deep learning techniques', *Indonesian Journal of Electrical Engineering and Computer Science*, Vol. 22, No. 1, pp.187-195, doi: 10.11591/ijeecs.v22.i1.pp187-195.

ISSN: 2252-4274 (Print)
ISSN: 2252-5459 (Online)

[13] Dogo, E.M., Nwulu, N.I., Olaniyi, O.M., Aigbavboa, C.O. and Nkonyana, T. (2018). 'Blockchain 3.0: Towards a secure ballotcoin democracy through a digitized public ledger in developing countries', *I-Manager's Journal on Digital Signal Processing*, Vol. 6, No. 2, pp. 24, doi: 10.26634/jdp.6.2.15593.

[14] Gabriel, A. J., Alese, B. K., Adetunmbi, A. O., Adewale, O. S. and Sarumi, O. A. (2019) 'Post-Quantum crystography system for secure electronic voting', *Open Computer Science*, Vol. 9, No. 1, pp.292–298, doi: https://doi.org/10.1515/comp-2019-0018

[15]Guffanti, D. (2018) 'Continuous speech recognition and identification of the speaker system', *Proceedings of the International Conference on Information Technology & Systems (ICITS 2018)*, pp.767-776. doi:10.1007/978-3-319-73450-7_72

[16] Hardwick, F. S., Gioulis, A., Akram, R. N. and Markantonakis, K. (2018) 'E-voting with blockchain: An e-voting protocol with decentralization and voter privacy', *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, pp. 1561-1567.

[17] Haruna, M. (2017) 'The problems of living with disability in Nigeria', *Journal of Law, Policy and Globalization*, Vol. 65, pp.103–113.

[18] Herrera-Camacho, A., Zúñiga-Sainos, A., Sierra-Martínez, G., Trangol-Curipe, J., Mota-Montoya, M. and Jarquín-Casas, A. (2019) 'Design and testing of a corpus for forensic speaker recognition using MFCC, GMM and MLE', *ACM International Conference Proceeding Series, October*, pp.105–109. https://doi.org/10.1145/3369318.3369330

[19] Isirova, K., Kiian, A., Rodinko, M. and Kuznetsov, A. (2020) 'Decentralized electronic voting system based on blockchain technology developing principals', *CMIS*, pp.211-223. Retreive from: CEUR-WS.org/Vol-2608/paper17.pdf

[20] Këpuska, V. Z. and Elharati, H. A. (2015) 'Robust speech recognition system using conventional and hybrid features of MFCC, LPCC, PLP, RASTA-PLP and Hidden Markov Model classifier in noisy conditions', *Journal of Computer and Communications*, Vol. 03, No. 06, pp.1–9, doi: https://doi.org/10.4236/jcc.2015.36001

[21] Kerdvibulvech, C. (2020) 'Recent multimodal communication methodologies in Phonology, Vision, and Touch', in Kurosu, M. (Ed.): *Human-Computer Interaction. Multimodal and Natural Interaction*, LNCS 12182, pp.392–400.

[22] Kshetri, N. and Voas, J. (2018) 'Blockchain-enabled e-voting' *IEEE Software*, Vol. 35, No. 4, pp.95-99.

[23] Lokapavani, Y. and Akila, A. (2018) 'Cloud based organizational information access system using voice authentication' *International Journal of Pure and Applied Mathematics*, Vol. 118, No. 5 Special Issue, pp.555–562.

[24] Martinez, R.M. and Vemuru, V. (2020) *Social inclusion of persons with disabilities in Nigeria: Challenges and opportunities*, 7 June, Retrieved from https://blogs.worldbank.org/nasikiliza/social-inclusion-persons-disabilities-nigeria-challenges-and-opportunities

[25] Mitra, S. and Acharya, T. (2007) 'Gesture recognition: A survey', *Published in: IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, Vol. 37, No. 3, pp.311–324.

[26]Muttaqi, T., Mousavinezhad, S. H. and Mahamud, S. (2018) 'User identification system using biometrics speaker recognition by MFCC and DTW along with signal processing package', *IEEE International Conference on Electro Information Technology*, *2018-May*, pp.79–83, doi: https://doi.org/10.1109/EIT.2018.8500256

[27] Nisha. (2017) 'Voice recognition technique: A review', *International Journal for Research in Applied Science & Engineering Technology (IJRASET)*, Vol. 5, No, V, pp.262–268.

[28] Oke, B. A., Olaniyi, O.M., Aboaba, A.A. and Arulogun, O.T. (2017) 'Developing multi-factor authentication technique for secure electronic voting systems', *Proceedings of IEEE International Conference on Computing, Networking and Informatics (ICCNI 2017)*, pp.48-53, doi: 10.1109/ICCNI.2017.8123773 .2017

[29] Okediran, O., Sijuade, A. and Wahab, W. (2019) 'Secure electronic voting using a hybrid cryptosystem and steganography', *Journal of Advances in Mathematics and Computer Science*, Vol. 34, pp.1–26, doi: https://doi.org/10.9734/jamcs/2019/v34i1-230201

[30] Olaniyi, O. M., Bala, J. A., Ndunagu, J., Abubakar, A. and Haq, A. I. (2019). 'V-Authenticate : Voice authentication system for electorates living with disabilities', *Proceedings of Cyber Secure Nigeria 2019 Conference (CSNC 2019)*, Abuja, Nigeria, pp.29-38.

[31] Olaniyi, O.M., Dogo, E.M., Nuhu, B.K., Horst, T., Abdulsalam Y.S. and Folawiyo Z. (**2022**), A Secure Electronic Voting System Using Multifactor Authentication and Blockchain Technologies. In: Misra S., Kumar, A. (eds) *Blockchain Applications in the Smart Era. Springer Innovations in Communications and Computing* (pp. 41-63). Springer Nature Switzerland.https://doi.org/10.1007/978-3-030-89546-4_3

[32] Oluwatobi, A.N., Ayeni, T.P., Arulogun, O.T., Ariyo, A.A. and Aderonke, K.A. (2020) 'Exploring the use of biometric smart cards for voters' accreditation: A

ISSN: 2252-4274 (Print)
ISSN: 2252-5459 (Online)

case study of Nigeria electoral process', *International Journal on Advanced Science, Engineering and Information Technology,* Vol. 10, No.1, pp. 80, doi: 10.18517/ijaseit.10.1.8459.

[33] Oudah, M, Al-Naji, A. and Chahl, J. (2020) 'Hand gesture recognition based on computer vision: A review of techniques', *Journal of Imaging*, Vol. 6, No. 8, pp.73, doi:10.3390/jimaging6080073

[34] Patel, N. P. and Kale, A. (2018) 'Optimize approach to voice recognition using IoT', *2018 International Conference On Advances in Communication and Computing Technology, ICACCT 2018*, pp.251–256, doi: https://doi.org/10.1109/ICACCT.2018.8529622

[35] Pawlak, M. and Poniszewska-Marańda, A. (2021) 'Trends in blockchain-based electronic voting systems', *Information Processing and Management*, Vol. 58, No. 4, doi:https://doi.org/10.1016/j.ipm.2021.102595.

[36] Premium Times. (2018) *19 million Nigerians living with disability – Official*, 9 November, Retrieved from: https://www.premiumtimesng.com/news/more-news/288954-19-million-nigerians-livingwith-disability-official.html

[37] Psychology Wiki. (2021) *Biometrics*, 15 March, Retrieved from: https://psychology.wikia.org/wiki/Biometrics

[38] Qureshi, A., Megías, D. and Rifà-Pous, H. (2019) 'SeVEP: Secure and Verifiable Electronic Polling System', *IEEE Access, 7*, pp.19266-19290.

[39] Rathee, G., Iqbal, R., Waqar, O. and Bashir, A. K. (2021) 'On the design and implementation of a blockchain enabled E-Voting Application within IoT-oriented smart cities', *IEEE Access*, Vol. 9, pp.34165-34176.

[39] Ribon, C. A., Leon, J. M., Corredor, O. F., Castellanos, H. E., Sanz, F. A., Ariza-Colpas, P., Landero, V. and Collazos-Morales, C. (2019) 'Design of an electronic voting system using a Blockchain network', *Communications in Computer and Information Science*, Vol. 1052, No. October, pp.511–522, doi: https://doi.org/10.1007/978-3-030-31019-6_43

[40] Sathya, V., Sarkar, A., Paul, A., and Mishra, S. (2019) 'Blockchain based cloud computing model on EVM transactions for secure voting', *Proceedings of the 2019 3rd International Conference on Computing Methodologies and Communication (ICCMC),* Erode, India, 27–29 March 2019; pp.1075–1079.

[41] Satybaldina, D. and Kalymova G. (2021) 'Deep learning based static hand gesture recognition' *Indonesian Journal of Electrical Engineering and Computer Science*, Vol. 21, No. 1, pp.398-405, doi: 10.11591/ijeecs.v21.i1.pp398-405

[42] Shahzad, B. and Crowcroft, J. (2019) 'Trustworthy electronic voting using adjusted blockchain technology', *IEEE Access*, Vol. 7, pp.24477-24488.

[43] Singh, N., Agrawal, A. and Khan, R. A. (2018) 'Voice Biometric: A technology for voice based authentication', *Advanced Science, Engineering and Medicine*, Vol. 10, No. 7, pp.754–759, doi: https://doi.org/10.1166/asem.2018.2219

[44] Singha, A. K., Singla, A. and Pandey, R. K. (2016) 'Study and analysis on biometrics and face recognition methods', *EPH-International Journal of Science and Engineering*, Vol. 2, No. 6, pp.37-41.

[46] Sriskandaraja, K. (2018) *Spoofing countermeasures for secure and robust voice authentication system: Feature extraction and modelling*, Unpublished Doctoral dissertation, The University of New South Wales.

[47] Srivastava, H. (2013) 'A comparison based study on biometrics for human recognition', *IOSR Journal of Computer Engineering*, Vol. 15, No. 1, pp.22–29, doi:https://doi.org/10.9790/0661-1512229

[48]Talib Mahde, A.H. (2019) 'Speech recognition by improving the performance of algorithms used in discrimination', *International Journal of Computer Science and Information Technology*, Vol. 11, No. 01, pp.19–29, doi: https://doi.org/10.5121/ijcsit.2019.11102

[50] Tas, R. and Tanrıöver, Ö.Ö. (2020). 'A systematic review of challenges and opportunities of blockchain for E-Voting', *Symmetry*, Vol. 12, No. 8, pp.1328, doi: https://doi.org/10.3390/sym12081328

[51] The Tide. (2017) *Involving persons with disabilities in electoral process*, 6 November, Retrieved from: http://www.thetidenewsonline.com/2017/11/06/involving-persons-with-disabilities-inelectoral-.

[52]Thuy, L.V., Cao-Minh, C. K., Dang-Le-Bao, C. and Nguyen, T.A. (2019) 'Votereum: An Ethereum-Based E-Voting System', *Proceedings of the 2019 IEEE-RIVF International Conference on Computing and Communication Technologies (RIVF)*, Danang, Vietnam, 20–22 March 2019; pp. 1–6.

[53] Umar, B. U., Olaniyi, O. M., Ajao, L. A., Maliki, D. and Okeke, I. C. (2019) 'Development of a fingerprint biometric authentication system for secure electronic voting machines', *Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, and Control*, Vol. 4, No. 2, pp.115–126.

[54] Vanguard. (2018) *NPC puts Nigeria's Disabled Population At 19 Million (6th October, 2018)*. 7 November, Retrieved from

ISSN: 2252-4274 (Print)
ISSN: 2252-5459 (Online)

https://www.vanguardngr.com/2018/10/npc-puts-nigerias-disabled-population-at19million.

[55] Virendrakumar, B., Jolley, E., Badu, E., Murphy, R. and Schmidt, E. (2018) 'Disability inclusive elections in Africa: a systematic review of published and unpublished literature', *Disability & Society*, Vol.33, No. 4, pp.509-538, doi: 10.1080/09687599.2018.1431108.

[56] Virkar, S., Kadam, A., Raut, N., Mallick, S. and Tilekar, S. (2020) 'Proposed model of speech recognition using MFCC and DNN', *International Journal of Engineering Research and Technology*, Vol. 9, No. 05, pp.570–572.

[57] Wan, Q. (2017) *Speaker verification systems under various noise and SNR conditions*, Unpublished MSc Thesis, Ottawa-Carleton Institute for Electrical and Computer Engineering, University of Ottawa.

[58] Zewoudie. A. (2020) *Speaker recognition and verification*, 4 January, Retrieved from: https://wiki.aalto.fi/x/_pvXCQ

[59] Zhang, W., Yuan, Y., Hu, Y., Huang, S., Cao, S., Chopra, A. and Huang S. (2018) 'A Privacy-preserving voting protocol on blockchain'. *Proceedings of the 2018 IEEE 11th International Conference on Cloud Computing (CLOUD)*, San Francisco, CA, USA, 2–7 July 2018; pp.401–408.

[60] Zhigang, F. (1999) 'Computer gesture input and its application in human computer interaction' *Mini Micro Syst*, Vol. 6, pp.418–421