International Journal of Innovative Research in Education, Technology & Social Strategies
p-ISSN: 2465-7298 | e-ISSN: 2467-8163
Volume 12, Number 1 May, 2025

IJIRETSS

Development of An Autonomous Voting System for Nigeria's Elections

[1]Opani M. Aweh, [2]Toba Paul Ayeni, [3]David Nzadon, & [4]Abiola Kehinde
[1,2,3&4]Department of Computing, College of Sciences,
Afe-Babalola University, Ado-Ekiti, Ekiti State, Nigeria

Article DOI: 10.48028/iiprds/ijiretss.v12.i1.18

Abstract

This study observes that elections are an important aspect of the democratic process, and voting in such elections is at the core of the election process. Owing to the time it takes for voters to register and cast their votes during elections, and the fact that voters must perform this duty at a designated time. This trend discourages some voters from participating in elections. This study, therefore, develops a semi-autonomous voting system that is secure, where votes can be verified using a collection of appropriate software development tools that are interfaced with a national database of the voting population. This study intends to use the Nigerian national identity card database; however, due to the inability to obtain the application programming interface, the bank verification number was employed in this system. The developed system was then tested rigorously, and the required features and functionalities of the proposed system were duly achieved.

Keywords: *Election, Voting, Autonomous, Voter, Nigeria*

Corresponding Author: Opani M. Aweh

Background to the Study

An Electronic Voting (E-Voting) system is a voting system in which the election process is notated, saved, stored, and processed digitally (Adeshina & Ojo, 2020; Esan and Ayeni, 2018; Lee & Ha, 2023; Yang et al., 2023). Getting voters to participate in elections has been a subject of concern to election stakeholders across various countries. The manual method of voting has made voting a cumbersome exercise, most especially in developing countries (Ayeni et al., 2024). It is no doubt that the use of technology makes the voting process convenient and reliable and can encourage voter turnout. Various requirements needed to be met for electronic voting to be realisable. These include usefulness, secrecy, genuineness, democracy, and proof, to mention a few (Bajaj et al., 2022; Adeshina & Ojo, 2020; Esan & Ayeni, 2020; Umar et al., 2022). To achieve this desired requirement, there is intense study on securing the voting process, making it easy and convenient and ensuring a smooth voting process devoid of interference (Yang et al., 2023). In all of these, information technology is at the core of the research. There is intense research on online voting using the web and mobile technologies; these include Yang et al. (2023), Ayeni et al. (2024), and Yu & Hui (2023). One of the major problems that must be resolved to achieve this desired objective is the problem of correct identification and authentication of voters at the front end, the voting system design, and the proper recording and collation of votes in a manner that can be easily verifiable at the backend of the voting system. This is what this study seeks to achieve.

In developed countries, voters go to perform their civic responsibilities at a convenient time within the period designated for voting, and in some cases, it happens in such a way that there are no long queues and hence no wasting of productive time. Information technology has eased most of the tasks and operations that were otherwise time-intensive (Ayeni & Esan, 2018). Some of these operations include bank transactions, using postal services and telephone service. This convenience has not been properly applied to sensitive civic duties like voting in elections, whereby the electorates can go to designated voting centres (polling units) and perform their civic responsibility of voting, with the polling unit agents and observers only watching. Evolving, this type of system with its attendant desirable security and reliable features is a current area of intense research. There are some propositions on how this can be achieved, and several approaches based on uniquely identifying and correctly distinguishing among the electorates are being intensely studied. One of the core areas of identification that is being considered is biometric identification. Several biometric approaches have been suggested and researched. Some of the examples are: Radio Frequency Identification System (RFID) (Zhao et al., 2023), external biometrics such as fingerprint (Yang et al., 2019), iris (Xiong et al., 2019), ear (Gao et al., 2019), face (Meden et al., 2021), finger veins (Shaheed et al., 2022), hand geometry (Oldal and Kovács, 2020), Voice analysis (Abdelfatah et al., 2024, Sebastian et al., 2023), Signature (Okawa, 2023; Chaurasia & Sengupta, 2024), Retinal Scanning (Meenaksh and Padmavathi, 2010; Devi et al., 2022). Additionally, traits such as fingernails and finger knuckle prints (Alghamdi et al., 2022) are used for biometric identification. of all these biometrics techniques, Facial Recognition seems to be the most widely suggested and studied. Therefore, in this study a facial recognition approach is proposed as the second factor authentication process in the design of an Autonomous Voting System.

Literature Review

Face Recognition Technologies

Face recognition technology has gained attention in the domain of network multimedia information access, particularly in areas such as network security, content indexing and retrieval, and video compression, where it offers notable benefits (Lin, 2000). As a biometric technology, face recognition relies on identifying the unique facial features of individuals. This process involves the collection of facial images, which are automatically processed by recognition systems (Li et al., 2020). The interest and debate surrounding video surveillance and face recognition systems surged following the September 11 terrorist attacks in the United States. Proponents argue that face recognition technology provides a powerful tool for enhancing national security, while critics raise concerns about potential privacy invasions reminiscent of Orwellian scenarios. Given the evolving nature of this technology and the associated societal concerns, face recognition remains a key issue in discussions about the social impact of technological advancements. In this context, we explore the balance between technical developments and the social implications of using video surveillance for personal identification (Boyer, 2004).

Nonetheless, apprehension is growing amongst several individuals concerning the role of facial recognition technologies in democratic societies (Andrejevic and Selwyn, 2020). Some important issues raised included issues of eroded accountability, compromised civil rights, and limitations on the concentration of power. First is the possibility for and the repercussions of misrecognition. For all its sophistication, computer-based facial recognition technology remains fallible (Andrejevic & Selwyn, 2020). There have also been several reports over the past years that have indicated the inability of facial recognition systems to identify African American faces due to the racially biased datasets that the models have been trained on (Andrejevic & Selwyn, 2020; Noble, 2018). Moreover, the problem of 'glitches', where identical twins are able to confuse facial recognition systems, remains a serious concern. (King, 2019). As such, there are concerns about large-scale misidentification (Brandom, 2018) and machine bias in the form of systematic misrecognition by skin colour or ethnic background (Crawford & Paglen, 2019; Andrejevic & Selwyn, 2020). Recent research also suggests that we are still some ways short of having facial recognition systems that can precisely identify individuals in a large crowd (Reilly, 2018). Similarly, some facial recognition systems appear to perform better on certain demographic groups than others (Simonite, 2018; Andrejevic & Selwyn, 2020).

In the same way, people are worried about these technologies being misused, especially by strict governments or businesses looking to make profit (Andrejevic & Selwyn, 2020). Similarly, facial recognition systems such as ones used to identify and publicly shame jaywalkers by displaying their names on electronic billboards and equipping the police with 'smart' glasses that identify criminal suspects have been deployed by some Chinese cities (Dodds, 2018). Facial recognition systems are also being used to target political dissenters as well as regulate their access to services including train and airplane travel (Carney, 2018; Andrejevic & Selwyn, 2020).

Facial Recognition Approaches

Naeem et al. (2015) provided an overview of different face recognition approaches. These techniques are subdivided into four groups, which are the hybrid-based approach, the feature-based approach, the model-based approach and the holistic-based approach. The whole face is treated as a single feature in the holistic approach. Statistical and AI approaches are further classes of a holistic approach. The feature-based system considers the facial features of an individual, such as the eyes, nose, mouth, mole, and ears; it then seeks to match the similarity between the images. This accounts for one of the major differences between the feature-based and the holistic approach. In the model-based face recognition approach, the facial model is acquired using both active and passive means. This involves extensive deployment of the active image acquisition technique, which is mostly the infrared laser beam. In the hybrid approach, feature matching and a holistic approach are used. It is presumed that the hybrid approach is comparatively the best approach, as it uses two approaches, so the hybrid approach is considered the best approach. Facial recognition systems are defined as providing authentication as well as some other biometric adaptive answers based on application specifications such as gender identification, complexion identification, age identification, etc. But as the number of associated operations and relative applications becomes complex, it requires more adaptive images and a vaster image set. The accuracy of the recognition system on different associated vectors (Madhan & Ahlawat, 2015).

Methodology

The study adopted an object-oriented analysis and design (OOAD) approach. The Unified Modelling Language (UML) was employed as the primary modelling tool. Specifically, a use case diagram was developed to illustrate the functional requirements that the proposed system is expected to fulfil.

System Requirements

Based on the review of some literature, which includes Esan et al., (2020), Ayeni et al., (2024), Alamleh & AlQahtani (2021), Suharsono et al (2021) and a survey. The following are highlighted as the requirements for the system:

1. **User-Friendly Interface:** The system must be easy to use. This is achieved by applying principles from human-computer interaction (HCI) studies to enhance user experience.
2. **Face Recognition for Authentication and Voting:** The system must support seamless face recognition for both authentication and voting. This is achieved through effective system design and implementation, which minimizes performance issues and reduces the occurrence of false positives.
3. **Event Tracking and Logging:** The system must maintain detailed logs of all events. This is accomplished through the database design, which includes event-listening functions to track actions within the system.
4. **Candidate List Viewing:** Voters must be able to view the list of available candidates before casting their vote.
5. **Voter Profile Access:** Voters must have access to their personal profiles.

6. **Voting Capability:** Voters must be able to cast their votes for their preferred candidate.
7. **Privacy:** After casting a vote, it must be impossible to link the voter to their specific vote, ensuring full voter privacy.
8. **Authenticity:** Only eligible voters are allowed to cast votes, ensuring that the voting process remains authentic and secure.
9. **Integrity/Accuracy:** Once a vote is cast, no changes can be made to it. All valid votes must be counted, and any invalid votes must be appropriately handled.
10. **Verifiability:** Voters must have the ability to independently verify that their votes have been counted correctly and are included in the final tally

System Design

Figure 1 explains the voting procedure of the new system. The voting process begins with an online voter card scan, allowing voters to verify their identity remotely without the need to visit a polling unit. The voter scans their card's barcode online, and the system retrieves their details for initial verification. Following this, the voter undergoes facial authentication, where their live facial features are matched with stored data to confirm their identity.

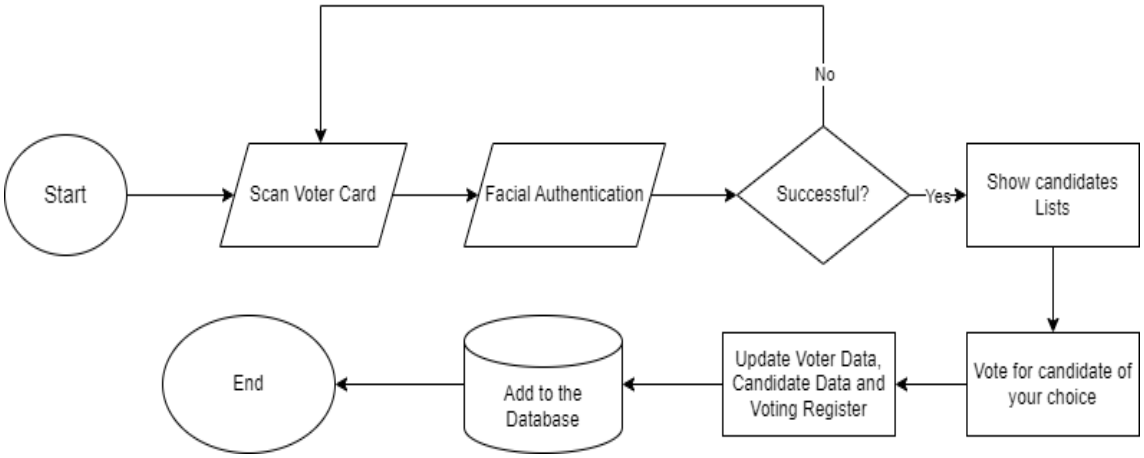

Figure 1: Proposed System flow

If authentication is successful, the voter is directed to an online dashboard displaying a list of candidates. If the authentication fails, the voter is prompted to retry the verification process. Once authenticated, the voter selects their preferred candidate(s) from the list. After casting the vote, the system updates the voter's data, candidate information, and voting register to reflect the transaction. Finally, the candidate's counter is incremented, and all information is securely stored in the database, ensuring accuracy and transparency throughout the online voting process.

Use Case Diagram

Figure 2 describes how the voter first has to present a voter's card for identification and then use the face recognition feature for authentication. The system then validates the credentials, in which the user is allowed to cast a vote if the credentials are valid and the voter has not cast a vote before.

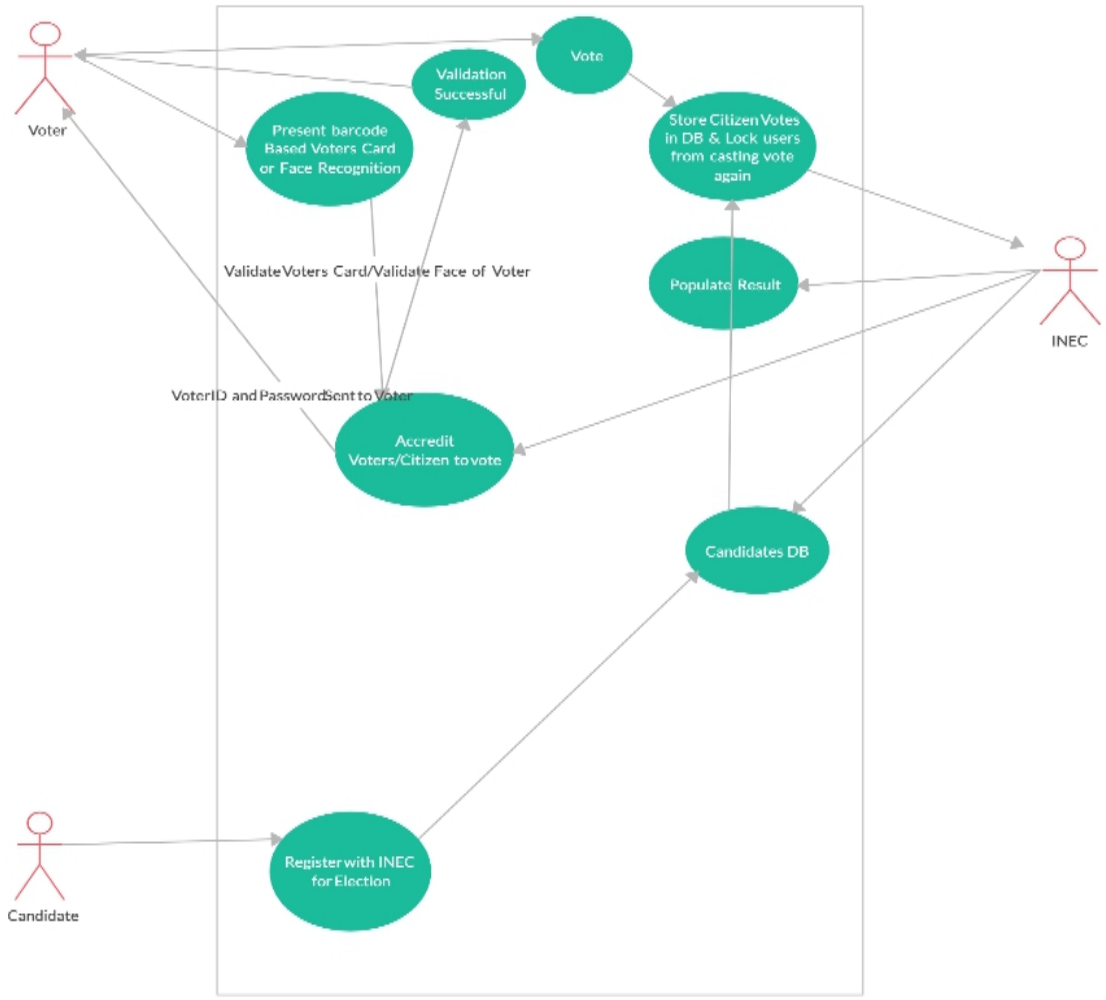

Figure 2: Use Case Diagram Explaining the Entire Process of the Proposed Voting System

Activity Diagram for the Administrator and the User

The activity diagram in the figure 3 below explains the entire process of the proposed voting system. The admin first captures the profile and biometrics of the voter. On the election day, the face of voter is verified after which the list of candidates is shown on the dashboard where voters are allowed to select the candidates of their choice. The list of attendance, updated voters' data are submitted alongside.

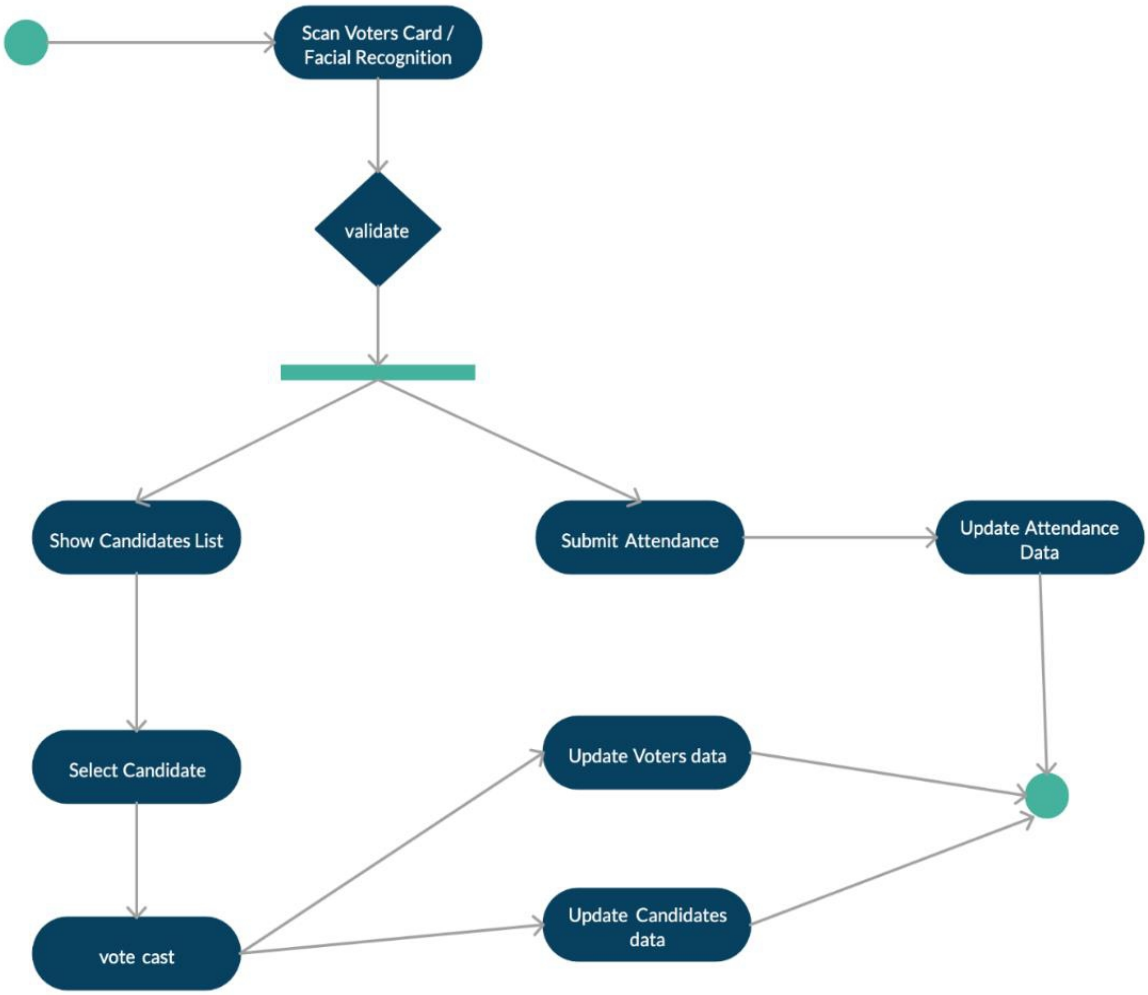

Figure 3: Activity Diagrams for the Administrator and the User

E-voting System Class Diagram

Figure 4 describes the class diagram for the system design. The class diagram models the structure of the proposed e-voting system. It defines the main entities, their attributes, and the operations they perform.

1. **Voter/Voter Profile**: Represents the user of the system, identified by an ID, name, and password. Voters can cast votes and view results. The Voter Profile stores additional information.
2. **Candidate**: Contains candidate details such as ID, name, party symbol, and constituency. Candidates can submit or cancel nominations.
3. **Cast Vote**: Records the act of voting, linking the voter to a candidate with a timestamp. It includes operations to submit or cancel a vote.
4. **Voting Server (Result Process)**: Manages vote processing by recording voter IDs, candidate IDs, timestamps, and vote counts. It can count votes and send reports.

5. **Result**: Stores candidate ID and party symbol provides the total votes obtained and displays the outcome.
6. **Admin**: Oversees the process by submitting reports based on voter IDs and votes recorded.

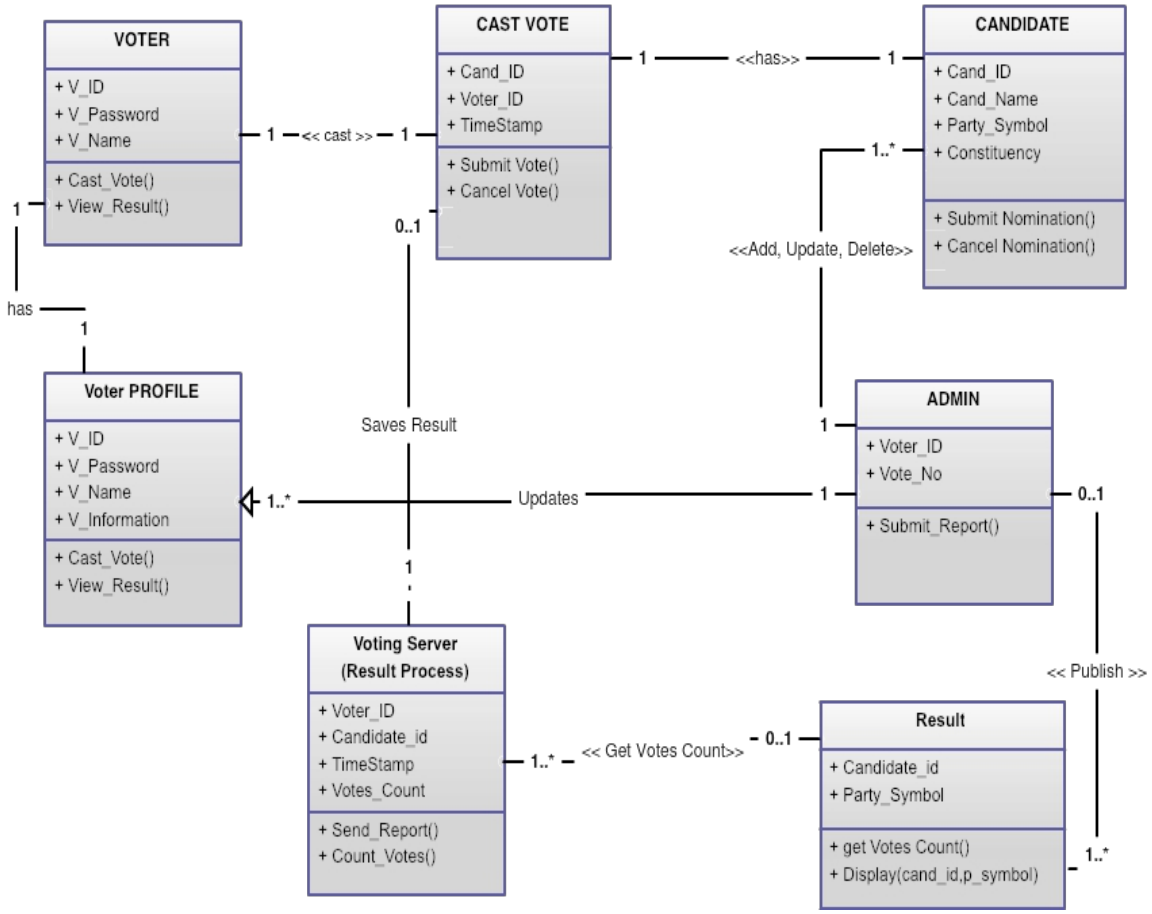

Figure 4: Activity Diagram Explaining the Entire Process of the Proposed Voting System

Implementation Overview

Figure 1 illustrates the spatial appearance of the overall system implementation and deployment architecture.

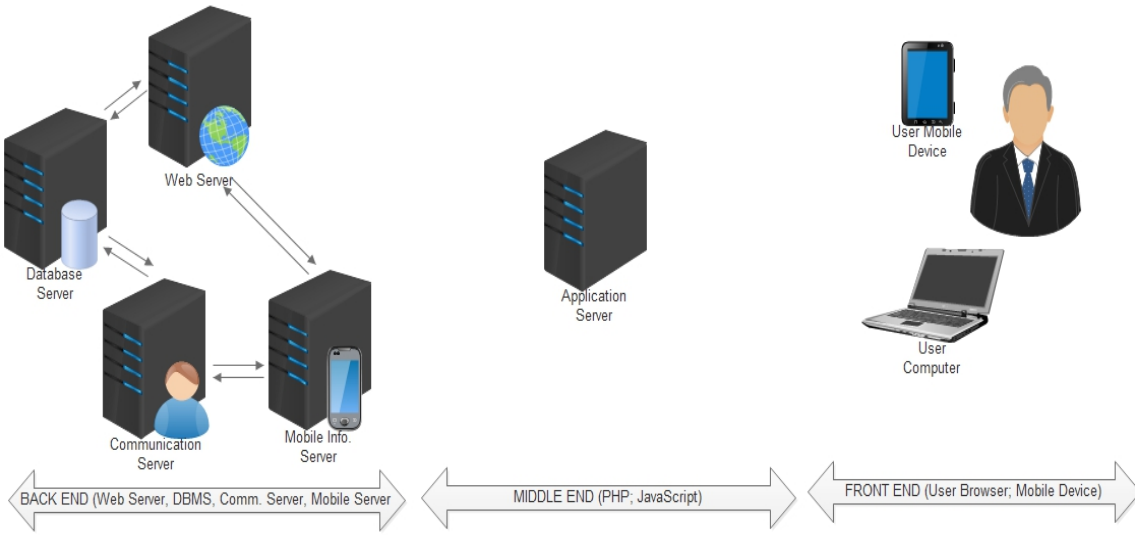

Figure 5: Overall Systems Implementation Tools/Components Architecture

The image in figure 5 shows the components used in the implementation of the system. It's divided into the (back, middle and front) end. The backend has 4 CPUs one has a globe beside it which is the webserver, the second has a cylinder beside which is the database server, the third has a human figure beside it and this is the communication server and the last has a mobile phone beside it and this is the mobile info server. The middle end has a CPU labelled the application server. The frontend has a mobile device, a user computer and a human figure.

System Testing, Deployment and Documentation

The IDE used for the system development allow system development or implementation to go on alongside the system testing. This feature was used extensively in this system implementation and testing. Having tested the system in the implementation environment, the functioning system was then packaged for online deployment. The sample source code listing for this functioning system is contained in Appendix A. The packaged system was deployed online, and it can be accessed at the domain name: sysdemo.com.ng. The system was again tested extensively in the productive online environment to assess its full features and functionalities to compare them with desktop development and testing environment outcome. The outcome of this elaborate testing as well as the documentation for the system are undertaken next.

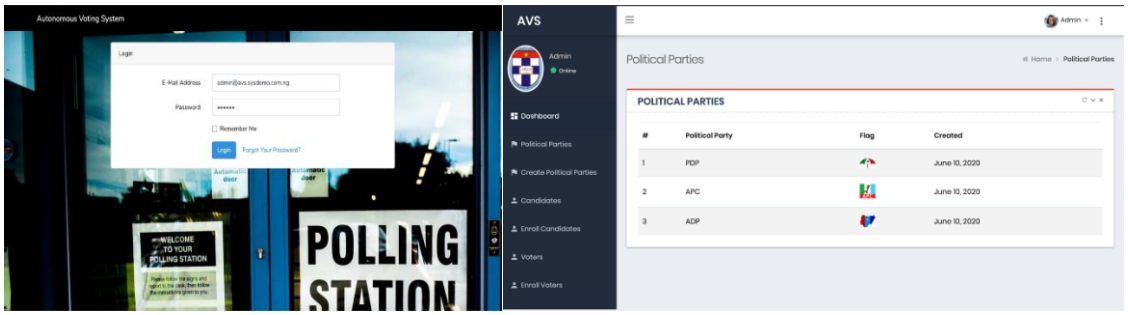

Figure 6 and 7: Showing Admin Login page and political party enrolment form

Figure 6 shows the admin login page. This page has two text boxes, one for an email address and the other for password. The page also has a "remember me" check box, a login button and a "forgot your password?" link.

Figure 7 shows the political party page. This page contains three political parties, their flag and the date they were created. The political parties are PDP which has an umbrella as its flag and was created on the 10th of June 2020, APC which has a broom as its flag and was created on the 10th of June 2020 and ADP whose flag is an image of the Nigerian map and was created on the 10th of June 2020.

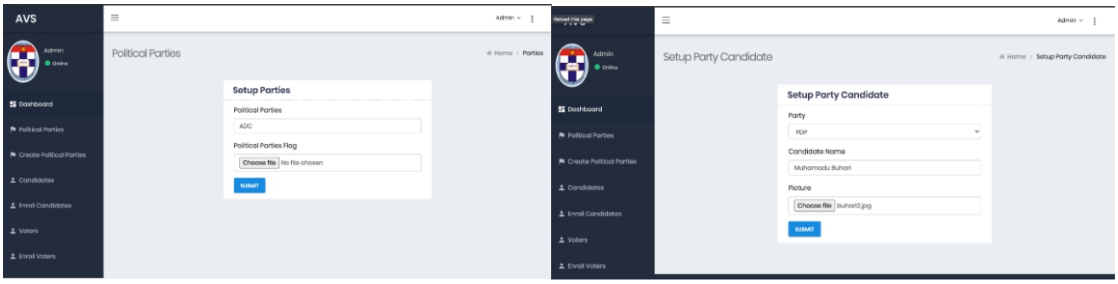

Figure 8 and 9: Showing party enrolment and candidate enrolment templates respectively.

Figure 8 shows the page for the creation of political parties. The image has two text boxes One is for the name of the political party, and the other is for the party's flag. There is a submit button below the second textbox. While Figure 9 shows the page for candidate enrolment. This page has 3 text boxes, The first one is for the political party, the second one is for the candidate's name, and the last one is for the candidate picture. Below the last text box is a submit button.

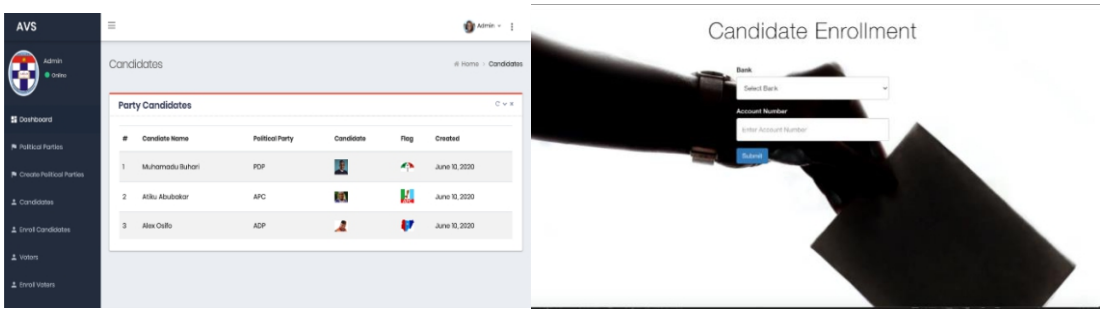

Figure 10 and 11: Showing political parties and their sample candidates as well as user registration points respectively.

Figure 10: The image shows the page for candidates that have been enrolled. The image shows the serial number, political party, candidate picture, the flag of the political party and the date the political party was created. The image shows 3 candidates with all this information filled out. The first candidate is Muhammadu Buhari, with the party PDP, the second is Atiku Abubakar with the party APC and the last is Alex Osifo with the party ADP.

Figure 11 shows how the proposed system appears to users (voter) at designated user's registration points. To enrol into the system, the user only needs to use the bank account number, which will serve as a key to retrieve the user's detailed records which is believed to have been properly verified. The original plan is to use a reliable database of citizens as the bases for enrolling users into the system.

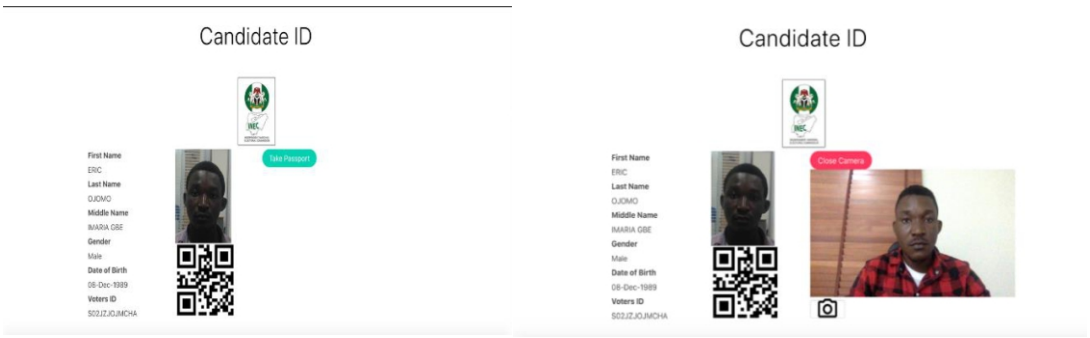

Figure 12 and **13**: Showing Sample data retrieved to be used to enrol the user and photo for face recognition purpose respectively.

Figure 12 shows the candidate ID page with some sample data that has initially been put in the system. It has the following information: first name: Eric, last name: Ojomo, middle name: Imaria Gbe, gender: male, date of birth: 08-Dec-1989, and voter's ID S02JZJOJMCHA. The image also contains a picture of a man and a bar code, and a button labelled "take passport".

Figure 13 shows the candidate ID page with some sample data that has initially been put in the system. It has the following information: first name: Eric, last name: Ojomo, middle name: Imaria Gbe, gender: male, date of birth: 08-Dec-1989, and voter's ID S02JZJOJMCHA. The image also contains a picture of a man and a bar code, and a button labelled "close camera". Below this button the is another picture of the same man.

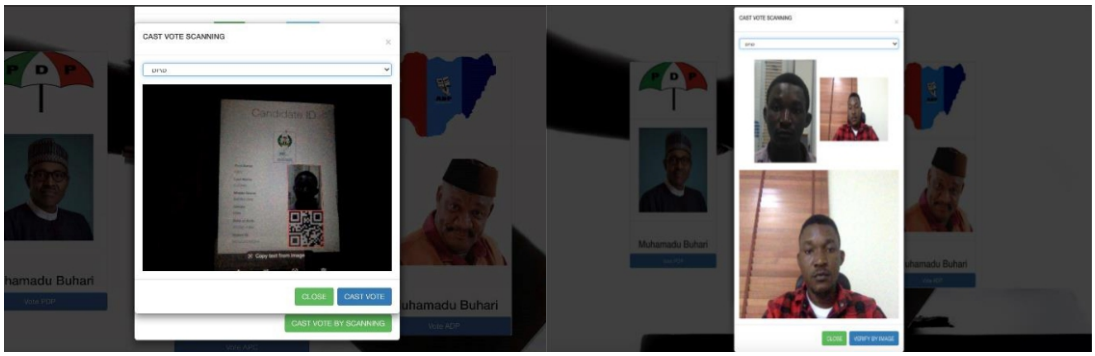

Figure 14 and **15**: Showing Sample view of the voter's interface and Sample view of the face recognition (Authentication) phase respectively.

Figure 14 shows the voter's id through the camera while the camera tries to scan it. There are two buttons, one to close and the other to scan.

Figure 15 shows the facial recognition authentication phase. It shows 3 images of the same man. The image has two buttons one to close and the other to "verify by image"

Figure 16: Sample view of the system voting page.

Figure 16 image shows the picture, name and party of 3 candidates. The actual voting process entails two steps of card presentation for identification and a facial recognition process for authentication. Figures 14 and 15 show the screenshots on which these actions are conducted, after which the real voting page of the candidates against their political parties as set up by the admin for the day is displayed for selection. The study has successfully developed a secure semi-autonomous voting system that enables voter verification through integration with a national database.

Conclusion

The spate of technological innovation and the emerging possibilities and innovations remains the driving force behind addressing different problem areas and functions. Voting especially in national elections has remained a serious concern, globally. There is increasing voter's apathy, rising incidence of frauds such as underage voting, impersonation, thuggery, etc., There is also incidences of international meddling in elections as presented in the election that brought the current United States of America's president, Donald Trump to power. Studies indicate that the scheduling of elections date to specific dates is the factor that has been responsible for low voter's turnout in many countries. The argument is that the process is time consuming, and warranting long periods of waiting by voters, and as such most voters deliberately stay away. Also, the process is sometimes known to be violent, resulting in skirmishes and disruptions.

This study is of the view that if the process of voting can be made more liberal and convenient without compromising security, apathy and disruptions can be checked or minimized. And the way to do this, is to leverage technology, which is already being done in some countries. In this case, the voters are encouraged to register and to vote at a convenient pace, by extending the periods for the exercises and allowing the voters to interact with the voting systems personally under surveillance, and to seek help, if need be. That is, the circuit cameras will be on, the electoral body and political party's/candidate's agents, law enforcement agents and independent observers will all be on guard.

And to achieve this desired state, this study has designed, implemented, and simulated the required features and functionalities for such a system. And for reliability and authenticity of the voter's registration and voting process the system is interfaced with a reliable and secure state information provisioning system that contains only valid information of the population members. The developed system is not only interfaced with this system, but it also practically obtains all its vital biodata from it and then augments the retrieved data with a personal identification number and a face recognition capability. The simulated results were quite impressive.

References

Abdelfatah, R. I. (2024). Robust biometric identity authentication scheme using quantum voice encryption and quantum secure direct communications for cybersecurity. *Journal of King Saud University - Computer and Information Sciences, 36*(5), Article 102062. https://doi.org/10.1016/j.jksuci.2024.102062

Adeshina, S. A., & Ojo, A. (2020). Factors for e-voting adoption: Analysis of general elections in Nigeria, *Government Information Quarterly, 37*(3), Article 101257. https://doi.org/10.1016/j.giq.2017.09.006

Alghamdi, M., Angelov, P., & Williams, B. (2021). Automated person identification framework based on fingernails and dorsal knuckle patterns. In *2021 IEEE Symposium Series on Computational Intelligence (SSCI)* (pp. 01-08). IEEE.

Andrejevic, M., & Selwyn, N. (2020). Facial recognition technology and its integration into public life, including compulsory schooling, *Learning, Media and Technology, 45*(2), 115-128. https://doi.org/10.1080/17439884.2020.1686014

Ayeni, T. P., Aweh, O. M., & Badeji-Ajisafe, B. (2024). Development of a secure framework for electronic voting in Nigeria using Paillier cryptosystem. In *2024 International Conference on Science, Engineering and Business for Driving Sustainable Development Goals (SEB4SDG)* (pp. 1-11). Omu-Aran, Nigeria. https://doi.org/10.1109/SEB4SDG60871.2024.10630288

Bajaj, S., et al. (2022). E-voting using homomorphic encryption. In *Proceedings of the 4th International Conference on Computer and Management (ICCM)*.

Brandom, R. (2018,). Amazon's facial recognition matched 28 members of congress to criminal mugshots, *The Verge*. Retrieved December 14, 2021, from https://www.theverge.com/2018/7/26/17615634/amazon-rekognition-aclu-mug-shot-congress-facial-recognition

Carney, M. (2018). Leave no dark corner. *ABC News*. Retrieved December 14, 2021, from https://www.abc.net.au/news/2018-09-18/china-social-credit-a-model-citizen-in-a-digital-dictatorship/10200278?nw=0&r=HtmlFragment

Chaurasia, R., & Sengupta, A. (2024). Multi-cut based architectural obfuscation and handprint biometric signature for securing transient fault detectable IP cores during HLS. *Integration, 95,* Article 102114. https://doi.org/10.1016/j.vlsi.2023.102114

Crawford, K., & Paglen, T. (2019). *The politics of images in machine learning training sets*. Retrieved December 14, 2021, from https://excavating.ai/

Devi, R. M., Keerthika, P., Suresh, P., Sarangi, P. P., Sangeetha, M., Sagana, C., & Devendran, K. (2022). Retina biometrics for personal authentication. In P. P. Sarangi, M. Panda, S. Mishra, B. S. P. Mishra, & B. Majhi (Eds.), *Cognitive data science in sustainable computing: Machine learning for biometrics* (pp. 87–104). Academic Press. https://doi.org/10.1016/B978-0-323-85209-8.00005-5

Divyarajsinh, P. N., & Mehta, B. B. (2013). Face recognition methods and applications. *International Journal of Computer Technology & Applications, 4*(1), 84-86.

Dodds, I. (2018). Chinese businesswoman accused of jaywalking after AI camera spots her face on an advert, *The Telegraph*. Retrieved December 14, 2021, from https://www.telegraph.co.uk/technology/2018/11/25/chinese-businesswoman-accused-jaywalking-ai-camera-spots-face/#:~:text=Alex-,Chinese%20businesswoman%20accused%20of%20jaywalking%20after%20AI,her%20face%20on%20an%20advert&text=Chinese%20police%20have%20ad

Esan, A. O., Ayeni, P. T., et al. (2020). E-voting in Nigeria: Barriers to full implementation, *International Journal of Soft Computing, 15*, 103-107. https://doi.org/10.36478/ijscomp.2020.103.107

Gao, Y., Wang, W., Phoha, V. V., Sun, W., & Jin, Z. (2019). EarEcho: Using ear canal echo for wearable authentication. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies, 3*(3), 1-24.

Jain, A., Srivastava, A., & Patidar, A. (2018). Face recognition is a genuine technique in electronic voting, *International Journal of Scientific & Engineering Research, 9*(5), 85-90.

King, E. (2019*). Twin faces and algorithmic image cultures. Paper presented at the Resisting Digital Culture Conference,* London: Centre for Digital Culture.

Lee, E. Y., & Ha, W. (2023). Electronic voting in shareholder meetings and the market value of cash holdings. *International Review of Financial Analysis, 89*, 102718. https://doi.org/10.1016/j.irfa.2023.102718

Li, S. Z., & Jain, A. K. (2005). *Handbook of face recognition*, Berlin/Heidelberg, Germany: Springer Science & Business Media.

Madhan, M., & Ahlawat, P. (2015). A study on different challenges in facial recognition methods, *International Journal of Computer Science and Mobile Computing, 4*(6), 521–525.

Meden, B., Gonzalez-Hernandez, M., Peer, P., & Štruc, V. (2023). Face deidentification with controllable privacy protection, *Image and Vision Computing, 134,* Article 104678.

Meenakshi, V. S., & Padmavathi, G. (2010). Security analysis of password-hardened multimodal biometric fuzzy vault with combined feature points extracted from fingerprint, iris and retina for high-security applications, *Procedia Computer Science, 2,* 195–206. https://doi.org/10.1016/j.procs.2010.11.025

Naeem, M., Qureshi, I., & Azam, F. (2015). Face recognition techniques and approaches: A survey, *Science International (Lahore), 27*(1), 301–305.

Noble, S. (2018). *Algorithms of oppression: How search engines reinforce racism*, New York: New York University Press.

Ohlyan, S., Sangwan, S., & Ahuja, T. (2013). A survey on various problems and challenges in face recognition. *International Journal of Engineering Research & Technology (IJERT), 2*(6), 2533–2538.

Okawa, M. (2023). Synergy of on-surface and in-air trajectories: Exploratory analysis of forensic online signatures implementing lessons learned from biometrics. *Forensic Science International: Reports, 8,* Article 100340. https://doi.org/10.1016/j.fsir.2023.100340

Reilly, C. (2018). *Facial-recognition software inaccurate in 98% of cases*, Retrieved December 14, 2021, from https://www.cnet.com/news/facial-recognition-software-inaccurate-in-98-of-metropolitan-police-cases-reports/

Sebastian, S., Mathews, S. S., Gowri, M., Kumar, M., & Mathew, J. (2023). Can there be a biometric parameter for voice? An investigation into the vocal cry of twins, *Journal of Voice.* https://doi.org/10.1016/j.jvoice.2023.09.022

Shaheed, K., Mao, A., Qureshi, I., Kumar, M., Hussain, S., & Zhang, X. (2022). Recent advancements in finger vein recognition technology: Methodology, challenges and opportunities, *Information Fusion, 79,* 84–109.

Simonite, T. (2018). *How coders are fighting bias in facial recognition software*, Retrieved December 14, 2021, from https://www.wired.com/story/how-coders-are-fighting-bias-in-facial-recognition-software/

Umar, B. U., Olaniyi, O. M., Olajide, D. O., & Dogo, E. M. (2022). Paillier cryptosystem-based ChainNode for secure electronic voting. *Frontiers in Blockchain, 5,* Article 927013. https://doi.org/10.3389/fbloc.2022.927013

Xiong, Q., Zhang, X., He, S., & Shen, J. (2021). A fractional-order chaotic sparrow search algorithm for enhancement of long-distance iris image, *Mathematics, 9*(21), Article 2790.

Yang, S., Gupta, A., Pandya, I. Y., Bhatt, A., & Mehta, K. (2023). End-to-end secure e-voting using blockchain and quantum key distribution, *Materials Today: Proceedings, 80*(3), 3363–3370. https://doi.org/10.1016/j.matpr.2021.07.254

Yu, H., & Hui, W. (2023). Certificateless ring signature from NTRU lattice for electronic voting, *Journal of Information Security and Applications, 75*, 103496. https://doi.org/10.1016/j.jisa.2023.103496

Zhao, H., Haacke, C., Sarkar, V., Paxton, A., Huang, Y. J., Szegedi, M., Gao, R., Price, G., Su, F. C. F., Rassiah-Szegedi, P., & Salter, B. (2023). Initial clinical evaluation of a novel combined biometric, radio-frequency identification, and surface imaging system, *Physica Medica, 114*, 103146. https://doi.org/10.1016/j.ejmp.2023.103146

Zhao, W., Rosenfeld, A., Chellappa, R., & Philips, P. J. (2003). Face recognition: A literature survey, *ACM Computing Surveys, 35*(4), 399–458. https://doi.org/10.1145/954339.954342