Computing, Information Systems, Development Informatics & Allied Research Journal
Vol. 15 No. 4, 2024 - www.cisdijournal.net

Design and Implementation of a Bimodal Voter Accreditation and Voting System

Jimoh Abdulafeez Alani[1], Olabiyisi Stephen Olatunde[2], Baale Abimbola Adebisi[3]
[1&2]Department of Computer Science
[3]Department of Information Systems
Ladoke Akintola University of Technology
Ogbomosho, Oyo State, Nigeria
E-mails: [1]aajimoh@pgschool.lautech.edu.ng; [2]soolabiyisi@lautech.edu.ng; [3]aabaale@lautech.edu.ng

ABSTRACT

Voting is fundamental to democracy but encounters issues like ballot padding and voter impersonation. In Nigeria, the Independent National Electoral Commission (INEC) launched the Bimodal Voter Accreditation System (BVAS) to address these problems, though it does not facilitate electronic voting. The manual voting process in the 2023 general elections resulted in vote buying and legal disputes. To improve reliability, the Bimodal Voter Accreditation and Voting System (BVAVS) was developed, allowing for electronic voting and real-time vote counting, thereby enhancing public trust. Developed using a waterfall methodology, the BVAVS features a fingerprint scanner and facial recognition camera, implemented in PHP with MySQL for voter data, and Firebase for biometrics. Modified C++ (Arduino) was used for coding the embedded BVAVS Scanner. The research involving fifty participants used a 5-point Likert scale questionnaire, with analysis performed via SPSS Version 20. Evaluation results show that the BVAVS achieves a usability score of around 4.44, an accuracy score of 4.8, and a security rating of 4.05, indicating a generally positive user experience. Its reliability rating is about 4.21, while user satisfaction averages 4.45, highlighting strong approval for its effectiveness. In light of Nigeria's growing demand for secure electoral processes, this research is timely and essential, instilling hope for trust and reliability in INEC and Nigeria as a nation. The BVAVS has the potential to complement or replace the current BVAS and could serve as a foundation for future research efforts.

Keywords: Design, Implementation, Bimodal, Voter, Accreditation, Voting, System

CISDI Journal Reference Format
Jimoh, A.A., Olabiyisi, S.O. & Baale, A.A. (2024): Design and Implementation of a Bimodal Voter Accreditation and Voting System (BVAVS). Computing, Information Systems, Development Informatics & Allied Research Journal. Vol 15 No 4, Pp 11-28. Available online at www.isteams.net/cisdijournal. dx.doi.org/10.22624/AIMS/CISDI/V15N4P2

1. INTRODUCTION

Voting is a vital decision-making process where citizens select candidates based on specific rules. A winner is declared by receiving the necessary votes and meeting the criteria [1]. For a democracy to thrive, citizens must express their political views and choose candidates who represent their interests [2]. The traditional voting system involves in-person voting using paper ballots or mechanical machines, requiring voters to visit designated polling stations during specific hours [3].

This system faces challenges such as ballot padding, candidate imposition, violence, voter impersonation, rigging by party agents, and poor security, which allow corrupt politicians to manipulate results and undermine electoral integrity [4]. On the other hand, electronic voting includes various techniques that use electronic systems for casting and counting votes, such as online voting and polling booths [5]. This technique aims to improve traditional voting practices by addressing the issues facing the old-style voting systems [6]. However, while e-voting offers potential benefits, it faces challenges related to functionality and security, particularly influenced by corrupt politicians, which can erode voters' trust in the system (6, 7). It's important to note that, unlike e-commerce, which offers tracking numbers and receipts, allowing for recovery from mistakes, e-voting regulations prevent this due to basic rules [8]. To ensure a reliable e-voting system, it is crucial to meet key requirements, including security, confidentiality, fairness, verifiability, and non-coercion [9].

Biometrics is an intriguing field focused on using unique physiological or behavioural traits such as fingerprints and facial recognition for individual identification. However, unimodal systems that rely on a single biometric trait face challenges including data noise, variability, and vulnerability to spoofing [10]. To overcome these issues, bimodal recognition systems that combine two traits enhance identification and verification processes, utilizing components like sensors and feature extraction [11]. In the context of voting, biometric-enabled e-voting offers a secure alternative to traditional methods. Bimodal biometric technology effectively identifies and prevents impersonation, ensuring a reliable voting process and supporting the democratic right to govern [12].

Nigeria's electoral history is quite intriguing. The Electoral Commission of Nigeria (ECN), established in 1959 and later renamed the Federal Electoral Commission (FEC) in 1964, saw controversial elections that contributed to the collapse of the First Republic. Following the establishment and disbandment of the Federal Election Commission (FEDECO) in 1978 and 1983, the National Electoral Commission (NEC) was created in 1987. After Abacha's death, the commission was renamed the Independent National Electoral Commission (INEC), which successfully conducted elections to inaugurate the Fourth Republic in 1999 [13]. More so, The Electoral Bill 2022 repealed the 2010 Act, legalized technology in elections, redefined over-voting, and mandated support for persons with disabilities. Nonetheless, concerns about the Bimodal Voter Accreditation System (BVAS) and the INEC Result Viewing Portal (IREV) persist, impacting transparency and public trust [14].

Previous research has primarily concentrated on minimizing irregularities in traditional elections through the use of electronic voting systems. However, concerns persist regarding security, data privacy, reliability, integrity, and transparency. Furthermore, Nigeria, the largest country in Africa, has yet to fully implement an electronic voting system, continuing to rely on manual voting along with the Bimodal Voter Accreditation System (BVAS) for the accreditation process. Consequently, this research intended to enhance Nigeria's voting framework by designing and implementing a Bimodal Voter Accreditation and Voting System (BVAVS) to improve security, accuracy, and reliability.

2. REVIEW OF RELATED WORKS

[15] introduced biometric voting systems that utilized Aadhaar cards alongside voters' iris patterns and fingerprints for enrollment and authentication. However, iris recognition can be affected by certain diseases, and the success of multimodal systems depends on the employed data and fusion techniques [4]. Additionally, Jatain's system requires substantial computational power, and significant memory capacity [16], and incurs considerable implementation costs.

[6] developed an electronic voting system using fingerprinting and visual semagram methods, tested during a deanship election. The system achieved an impressive equal error rate of 0.0019, sensitivity of 0.9962, and accuracy of 99.81%. However, its performance could be further enhanced by incorporating bimodal biometric techniques, such as combining fingerprints with facial recognition. [17] devised a robust bimodal voting framework for Nigerian elections, utilizing timed coloured Petri nets to ensure security. The framework aims to enhance accessibility, voter privacy, verifiability, and result integrity. Comprised of five key modules, the framework aligns with the 1999 Constitution and INEC's 2019 presentation. However, further investigation into this new framework is urgently required with the recent implementation of the Electoral Act of 2022. [18] presented an innovative voting system that uses biometric identification via the Aadhar Database. This system stores voter information like name, age, and location, utilizing fingerprint registration for access. By allowing votes to be cast using Aadhar numbers, it reduces the risks of hacking and fraud. However, the system's success depends on the accuracy of biometric data and may not be accessible to all voters, raising valid security concerns regarding the Aadhar database.

[19] Proposed an IoT-enabled remote electronic voting system featuring dual biometric authentication through fingerprint verification and facial recognition. This system uses RFID-based smart cards to store voter information and employs Haar cascade and LBPH algorithms for facial recognition. However, it has not yet been implemented. Similarly, [20] developed a user-friendly online voting system for Nigerian elections that enhances user experience and includes three modules for easy interaction. Users log in with a username and password to prevent invalid votes, while the system allows for remote voting and real-time result viewing, encouraging participation from Nigerians abroad and reducing election costs. Nonetheless, concerns regarding security, privacy, reliability, and integrity remain.

3. METHODOLOGY

3.1 System Design Architecture

Fig. 1 illustrates the system architecture developed, which consists of five modules. The voter registration module captures and stores biographical information, including names and addresses, while assigning each voter a unique VIN. It employs bimodal verification through fingerprints and facial recognition for authentication. The corresponding algorithm for this module is shown in Algorithm 1. The next component of the system is the voter verification module, which employs both fingerprint and facial recognition for authentication. Biometric devices are integrated to capture and verify the necessary biometric data. Algorithms are utilized to match and extract the captured information with the data stored during the verification process. The sequential steps involved are outlined in Algorithm 2.

Transitioning to the third module, the voting module offers a user-friendly interface for secure voting. Algorithm 3 provides a detailed step-by-step procedure for this module. The fourth module functions as the central database, storing voter information, biometric data, and voting records. It implements stringent access controls to ensure that only authorized personnel can access and modify the database. The fifth module is dedicated to backup and recovery mechanisms, designed to maintain data integrity in the event of system failures or disasters.

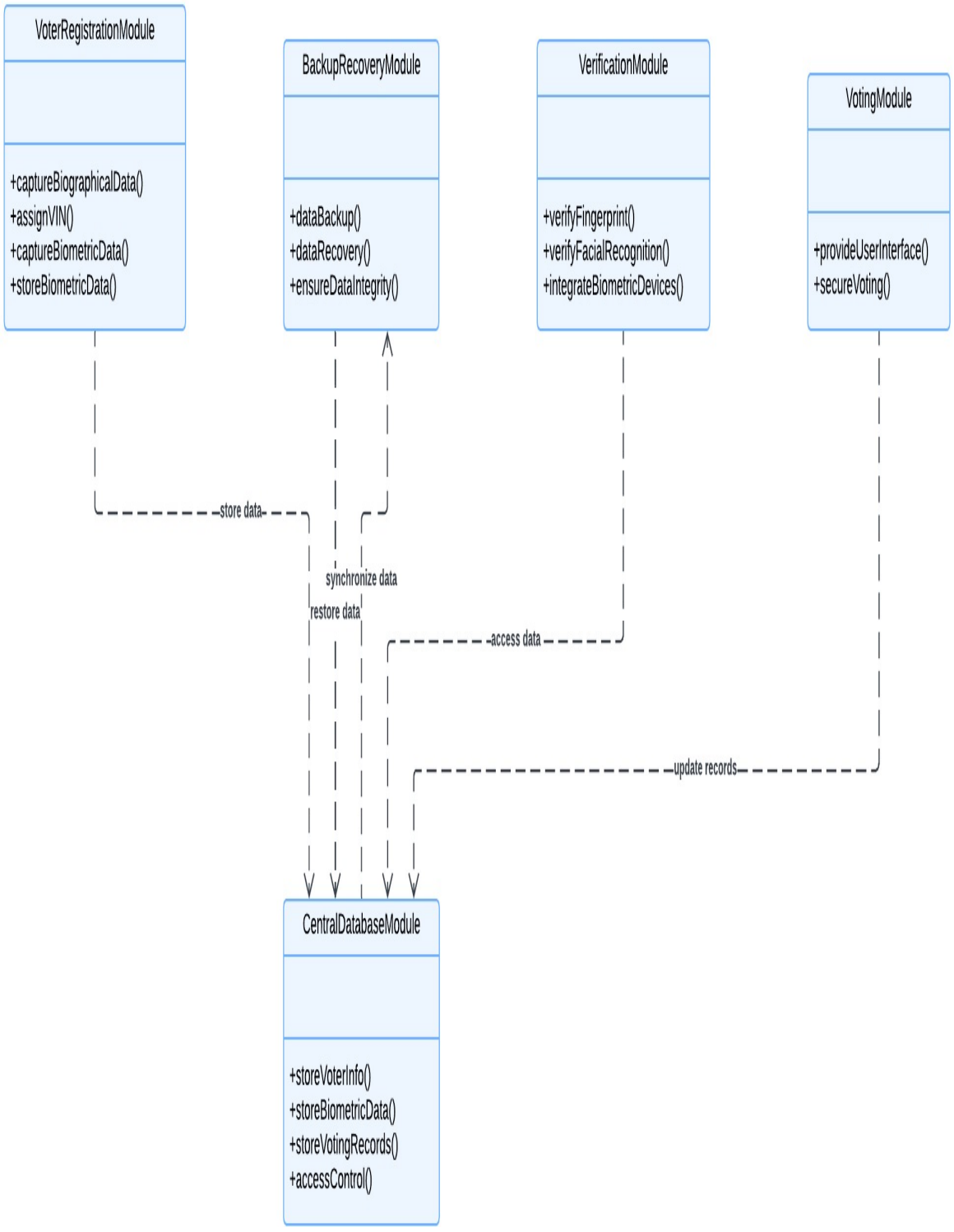

Fig. 1: Architecture of the Developed System

Algorithm 1: Voter's Registration Module

1: Start
2: Collect voter's data
3: Initialize fingerprint reader and facial camera
4: Process fingerprint and facial recognition
5: Create fingerprint template, Vf_1, and facial recognition Vf_2
6: Search for existing template
7: If an error or template exists
    N=0
    While N<=3
    N= N+1
    Go to step 3
    Else
    Go to step 8
8: Display "Registration not successful"
9: If an error or template does not exist
10: Generate Voter's VIN
11: Fuse Vf_1 and Vf_2
12: Generate Voter's ticket Vt
13: Display "Registration successful"
14: Stop

Algorithm 2: Voter's Verification Module

1: Start
2: Initialize fingerprint reader and facial camera
3: Collect the voter's fingerprint and facial recognition sample
4: Verify voter's fingerprint and facial recognition
5: If the verification does not match
    N=0
    While N<=3
    N= N+1
    Go to step 3
    Else
    Go to step 6
6: Display "Verification not successful"
7: If the verification match
8: Display "Verification is successful"
9. Stop

Algorithm 3: Voting Module

1: Start
2: Initialize voting
3: Initialize fingerprint reader and facial camera
4: Collect the voter's fingerprint, facial recognition, and VIN
5: Process voter's ticket
6. If the information does not match
    N=0
    While N<=3
    N= N+1
    Go to step 3
    Else
    Go to step 7
7: Display "Voter is rejected"
8: If the information match
9: Allow voters to vote
11. Display "Congratulations! Voting is successful"
12. Stop

3.2 System Hardware Requirements

The developed system includes several hardware components: a fingerprint scanner, a facial recognition camera, and a personal computer. Fig. 2(a) shows the BVAVS fingerprint scanner, while Fig. 2(b) outlines the components for fingerprint creation, including a fingerprint module, two NodeMCUs, two electrical switches, jumper wires, a data cable, and a protective casing. The fingerprint module captures and processes fingerprint data for biometric identification. The NodeMCU serves as a microcontroller board with Wi-Fi capabilities, essential for IoT applications. The first NodeMCU is used for registration, and the second for verification, with switches facilitating the transition between them. During registration, the left switch is on and the right is off; this setup is reversed for verification. The data cable is crucial for power supply and data transmission among the components.

Jumper wires are essential for connecting components within a fingerprint scanner, especially in prototyping or custom builds. The scanner's casing is also important for protection, usability, durability, and functionality. For facial recognition, the Hikvision DS-2CD2185FWD-I is a top choice, featuring an 8-megapixel (4K) resolution and a progressive scan CMOS sensor. It offers fixed lens options of 2.8mm, 4mm, or 6mm, and operates in temperatures from -30°C to +60°C. To ensure optimal performance, the PC should meet these minimum requirements: an Intel Core i5 processor, 8GB of 2666MHz RAM, a 256GB SSD, integrated Intel UHD Graphics 630, and Windows 10 Pro (64-bit).

3.3 Choice Of The Programming Languages Aad Databases

The BVAVS was developed using PHP, a robust choice for web development, ensuring scalability and security in a bimodal voter accreditation and voting system. Voter information is stored in MySQL, a trusted relational database, while fingerprint and facial recognition data are managed in Firebase. Firebase is ideal for real-time applications, offering easy integration, and support cloud storage with minimal infrastructure management. Visual Studio Code and Google Colab were used as the integrated development environments (IDEs).

Visual Studio Code offers excellent functionality and extension support for maintaining a secure, scalable system, while Google Colab allows users to write and execute Python code in an interactive notebook format. Lastly, modified C++ (Arduino) was selected for the BVAVS Scanner because of its suitability for embedded systems and user-friendliness.

Fig. 2(a): The BVAVS fingerprint scanner

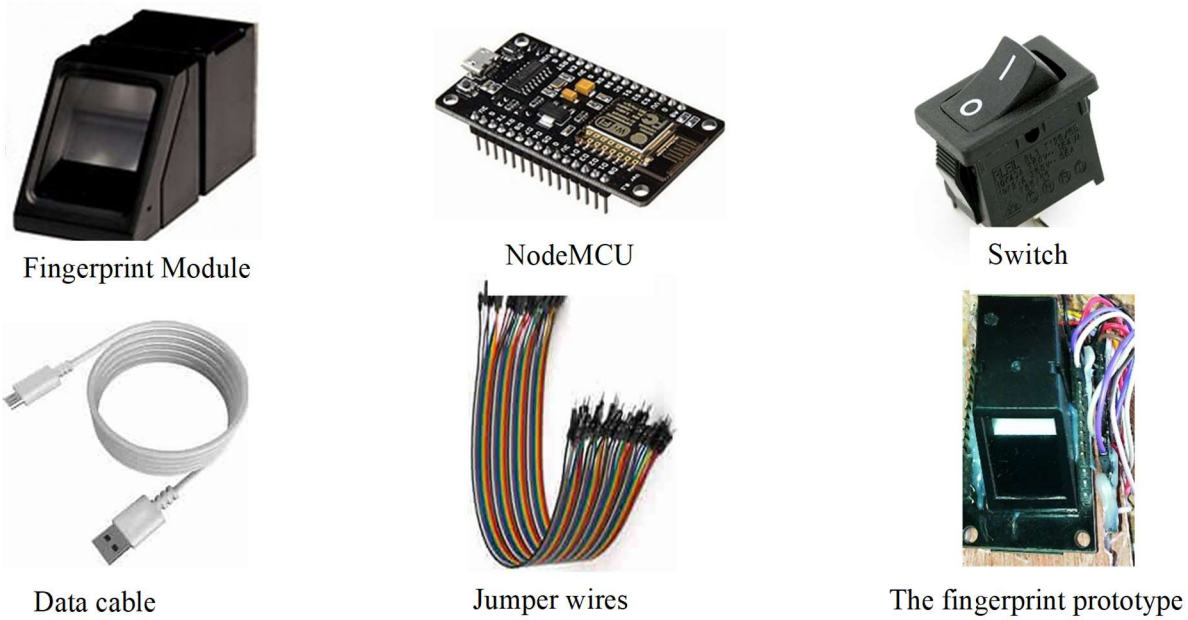

Fig. 2(b): Components of the BVAVS Fingerprint Scanner

3.4 Data Collection Procedures

Variables involved in this research, such as security, accuracy, reliability, ease of use, and user satisfaction, were clearly defined. Quantitative data was collected from fifty users through questionnaires during the use of the developed BVAVS.

3.5 Data Analysis Plan

To facilitate numerical analysis, a 5-point Likert scale was employed, ranging from 1 (strongly disagree) to 5 (strongly agree). The collected data were analyzed using the Statistical Package for Social Scientists (SPSS) software (Version 20). Descriptive statistical values, such as mean scores, were utilized to address the research questions. The overall frequency mean score for each identified variable was determined by averaging the positive responses along with the reverse-coded negative items. This method provided valuable insights into the effectiveness of the developed system.

4. RESULTS AND DISCUSSION

4.1 Voters Interfaces Of The Developed BVAVS

Users log into the voter dashboard with their identification number and password. New users provide their biodata, including NIN, email, and phone number. Voters register fingerprints and undergo facial recognition to create a biometric template linked to their VIN as shown in Fig. 3 and Fig. 4 respectively. Each voter has a personalized dashboard with navigation options as depicted in Fig. 5. Before voting, they must verify their identity as represented in Fig. 6(a), Fig. 6(b), and Fig. 6(c) respectively. Election results, showing candidate names and vote counts, are available in real-time before and after voting as illustrated in Fig. 7.

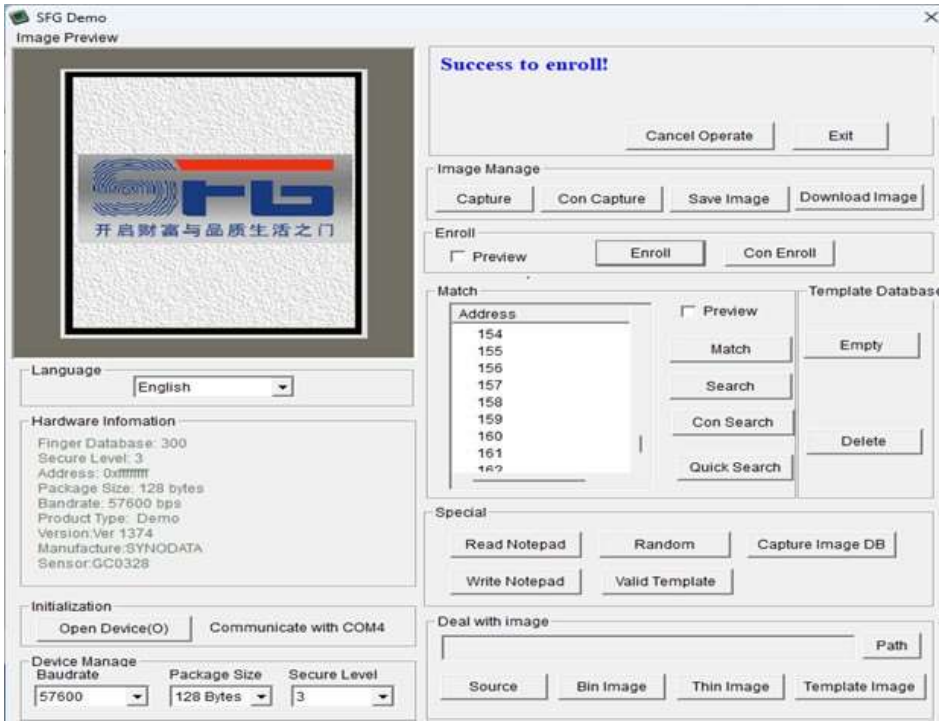

Fig. 3: Fingerprint Enrollment Module

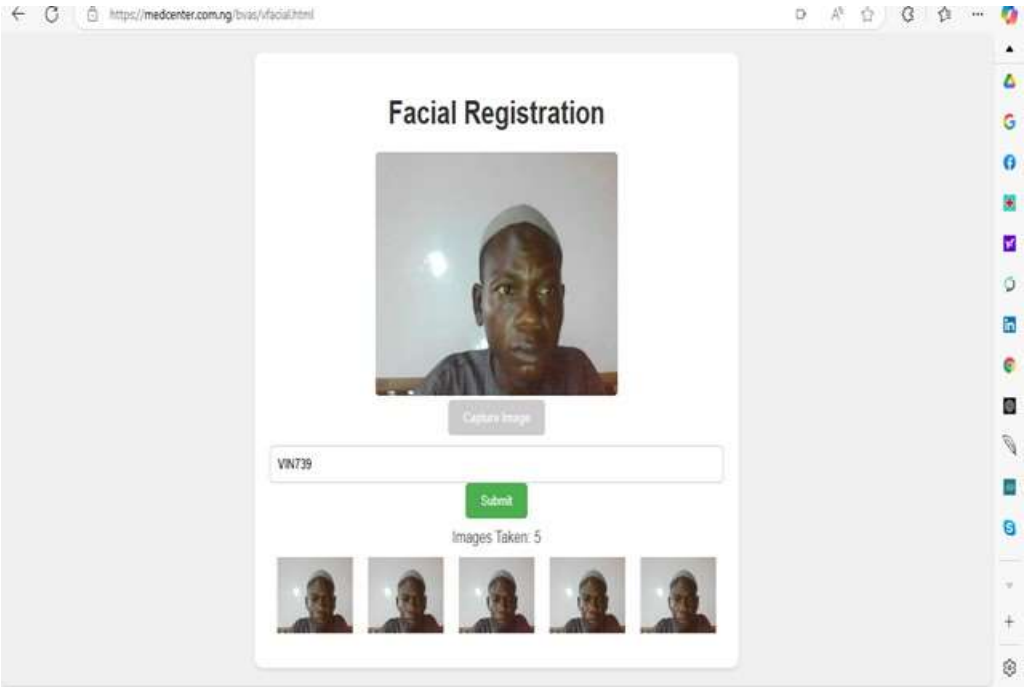

Fig. 4: Facial Registration Page

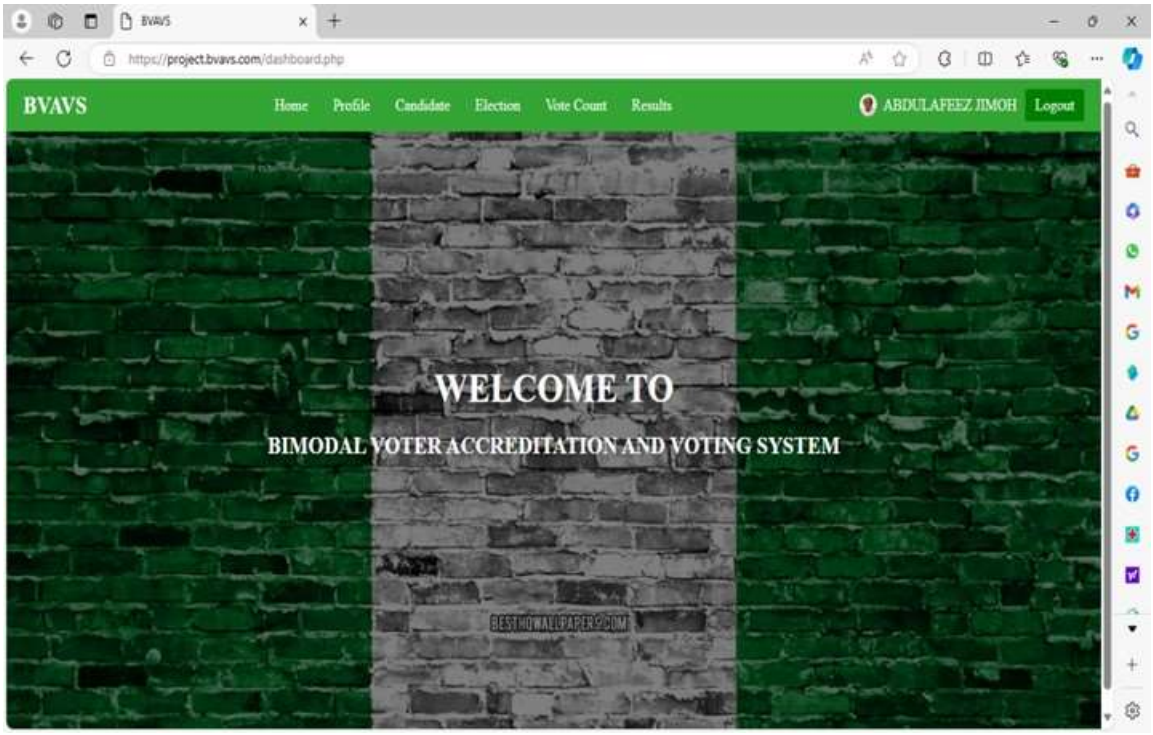

Fig. 5: Voter's Dashboard

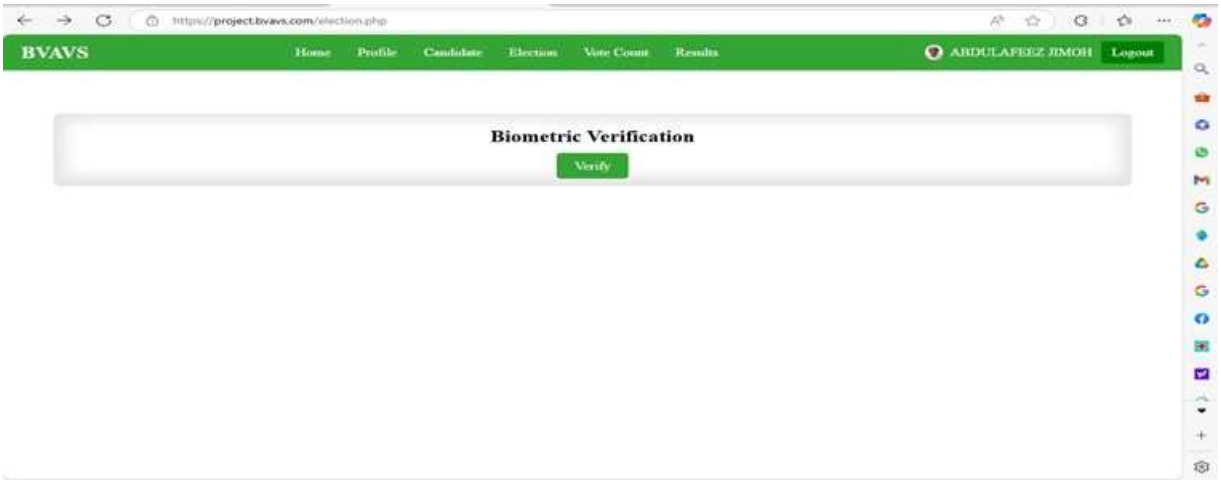

Fig. 6(a): Election Page

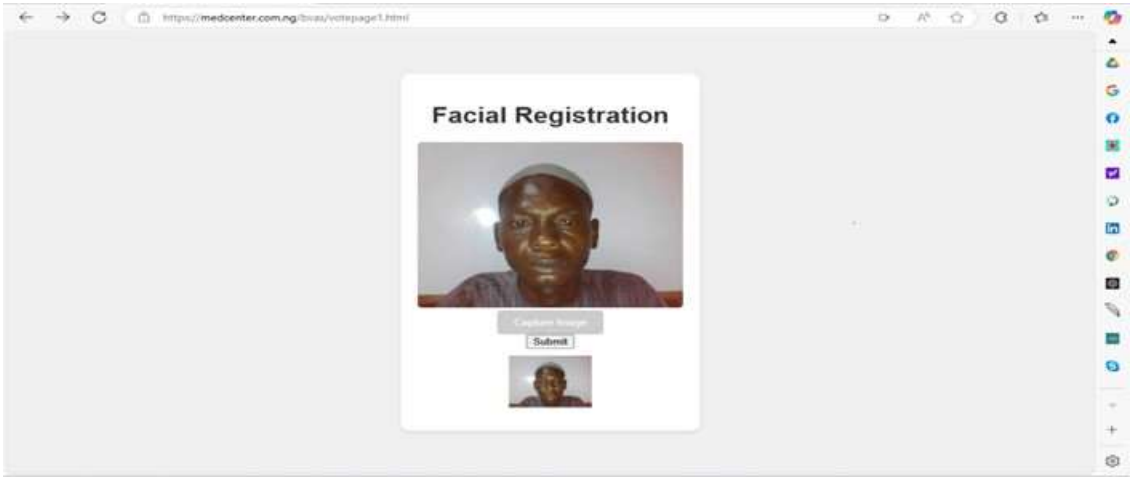

Fig. 6(b): Facial verification page

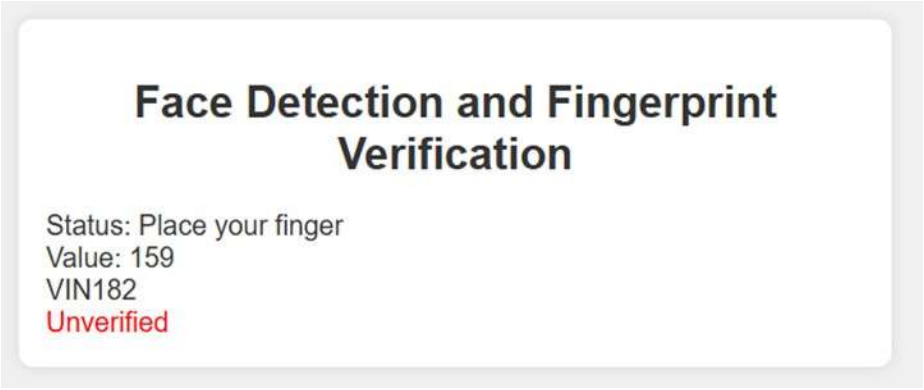

Fig. 6(c): Fingerprint Verification Page

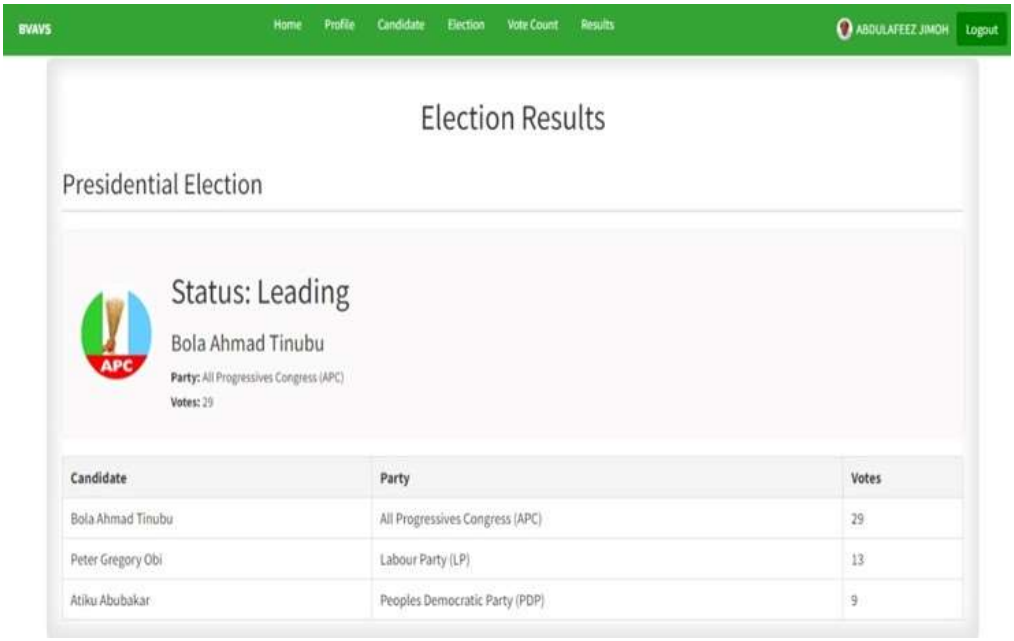

Fig. 7: Election Results Page

4.2 Admin Interfaces of the Developed BVAVS

The administrator's dashboard includes several interconnected pages as displayed in Fig. 8. The voters' list page contains a comprehensive record of eligible registered voters as shown in Fig. 9. Fig. 10 demonstrates the electronic ballots page, displaying candidates' names and party logos, with buttons that allow voters to select one candidate per position. Fig. 11 depicts the voting page, which tracks votes for each candidate, essential for post-election audits. Finally, the developed BVAVS is hosted by Hostinger under the domain name “project.bvavs.com.”

Fig. 8: Admin Dashboard

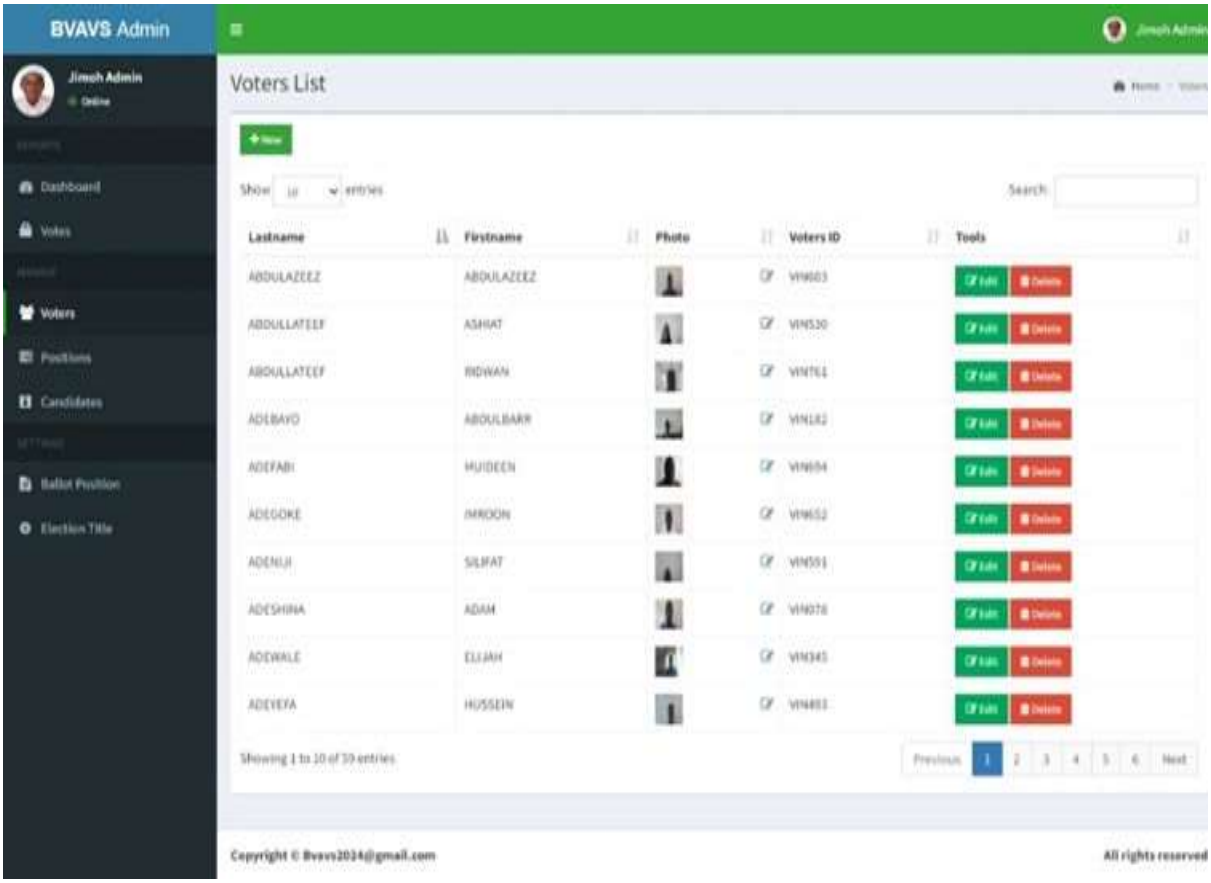

Fig. 9: Voters List Page

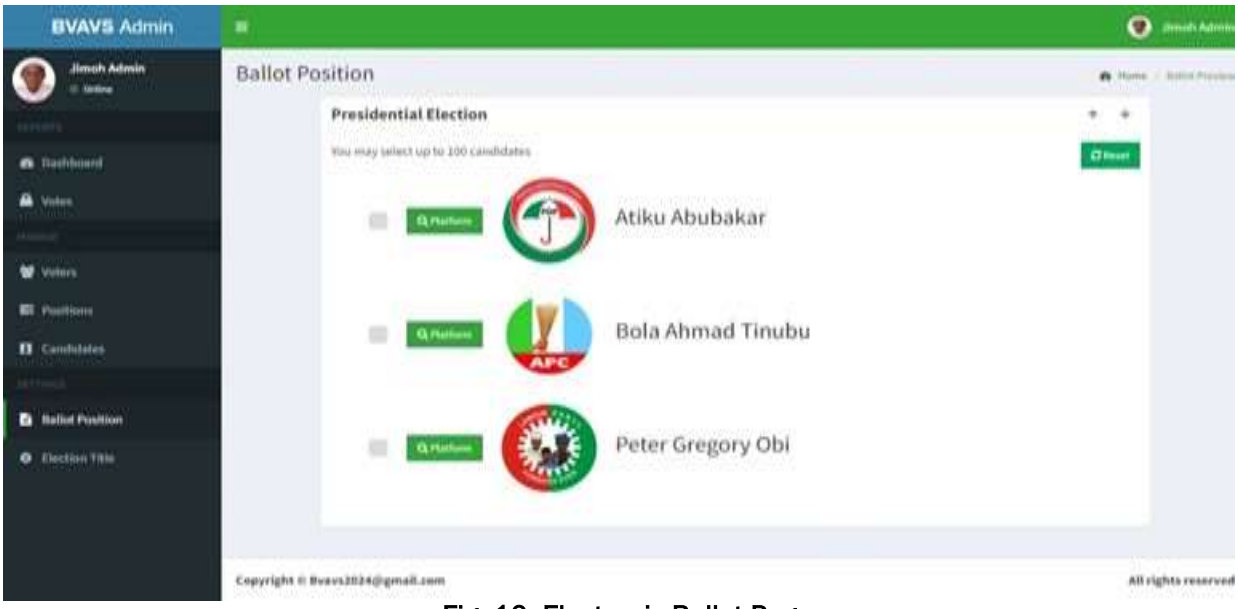

Fig. 10: Electronic Ballot Page

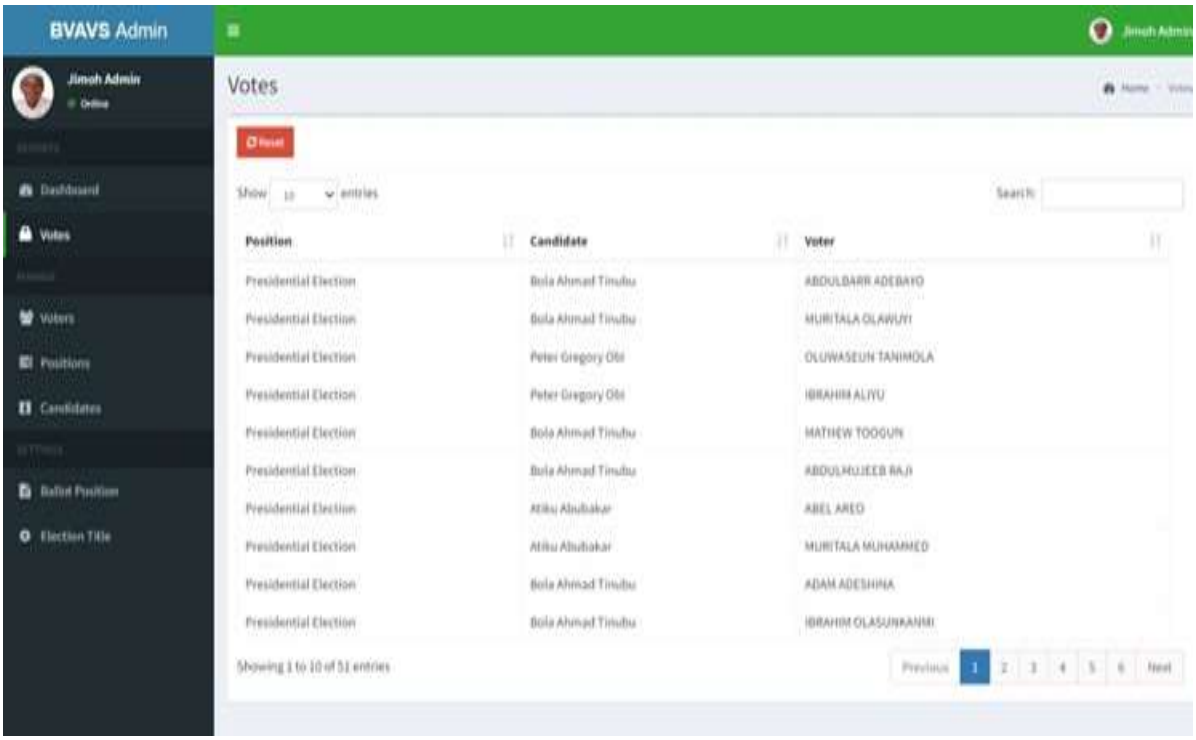

Fig. 11: Admin Votes Page

4.3 Users' Perspectives on the Ease of Use of the Developed BVAVS

The data in Table 1 shows that users perceive the BVAVS system as user-friendly, with easy navigation and low complexity. High mean scores of 4.54 for intuitiveness and 4.40 for ease of learning reflect a positive usability experience, significantly above the 3.00 average. In contrast, lower scores for difficulties (1.72) and confusion (1.54) suggest most users faced no significant challenges using the system. The overall usability score of approximately 4.44 indicates that users generally found the system intuitive and straightforward.

Table 1: Users' perspectives on the ease of use of the developed BVAVS

ITEMS	MEAN
The system interface was intuitive and easy to navigate.	4.54
Learning to use the system was straightforward.	4.40
I encountered difficulties while using the system.	1.72
The system was confusing to operate.	1.54
I found it hard to understand how to use the system.	1.50

4.4 Users' Perspectives On The Accuracy Performance Of The Developed BVAVS

The data in Table 2 highlights the strong reliability of the BVAVS system. Users reported a mean score of 5.42 for identity verification through bimodal authentication and an even higher score of 5.68 for vote recording accuracy, indicating significant confidence. Confidence in the vote tallying process was also notable, with a score of 4.60, still above the typical benchmark of 3.00. However, scores for errors, such as discrepancies in recorded votes (1.86) and identity verification failures (1.84), were much lower, suggesting these issues are rare. Overall, the BVAVS system achieved a total accuracy score of approximately 4.8, reflecting strong performance with minimal reported discrepancies.

Table 2: Users' Perspectives On The Accuracy Performance Of The Developed BVAVS

ITEMS	MEAN
The system accurately verified my identity through the bimodal authentication process (face and fingerprint).	5.42
The system accurately recorded my vote without any discrepancies.	5.68
I am confident that the system accurately tallied the votes cast.	4.60
There were discrepancies between my intended vote and the vote recorded by the system.	1.86
The system failed to accurately verify my identity during the accreditation process.	1.84

4.3 Users' Perspectives On The Security Measures Of The Developed BVAVS

Table 3 reveals strong user confidence in the BVAVS system's security during the voting process. Users reported an average confidence score of 4.50 for the protection of their voting information, with privacy safeguards rated even higher at 4.54. However, concerns about security breaches, including unauthorized access and personal information protection for voter accreditation, were lower, scoring 2.54 and 2.60. These scores, below the overall mean of 3.00, suggest that while some users have reservations, most express minimal concerns. Overall, the BVAVS system's security score is around 4.05, indicating a generally positive perception of its protective measures despite some lingering apprehensions.

Table 3: Users' Perspectives On The Security Measures Of The Developed BVAVS

ITEMS	MEAN
I felt confident in the security measures implemented to protect my voting information.	4.50
I am concerned about the possibility of unauthorized access to my voting data.	2.54
The system adequately protected my privacy during the voting process.	4.54
I trust that the system has measures in place to prevent tampering with the voting results.	4.34
I am worried about the security of my personal information used for voter accreditation.	2.60

4.4 Users' Perspectives On The Reliability Of The Developed BVAVS

The data in Table 4 assessing the BVAVS system's reliability shows that users generally find it consistent and largely free from significant technical issues. The statement "The system consistently performed without any technical glitches" received a mean score of 4.12, indicating a seamless experience for most users. Confidence in handling high vote volumes during peak times scored 4.24. Reports of negative experiences, such as errors (1.78), system crashes (1.58), and access delays (1.94), were below the overall mean of 3.00, suggesting minimal disruptions. Overall, the BVAVS system achieved an aggregate reliability score of approximately 4.21, reflecting dependable performance even during high usage periods.

Table 4: Users' Perspectives On The Reliability Of The Developed BVAVS

ITEMS	MEAN
The system consistently performed without any technical glitches.	4.1200
I encountered errors or disruptions while using the system.	1.7800
The system crashed or became unresponsive during my interaction.	1.5800
I experienced delays in accessing the system or casting my vote.	1.9400
I am confident in the system's ability to handle a large volume of votes during peak times.	4.2400

4.5 Users' Perspectives On The User Satisfaction Of The Developed BVAVS

Table 5 illustrates a strong level of user satisfaction with the BVAVS system. Users rated the system's support for individual preferences and accessibility at an average of 4.42. The response time during accreditation and voting processes received a favorable score of 4.08, indicating minimal delays. Clarity of instructions rated even higher at 4.54, while trust in the accuracy of vote recording scored 4.52. Notably, the system achieved the highest score of 4.68 for maintaining the anonymity and confidentiality of votes, reflecting users' confidence in privacy protections. Overall, the BVAVS system earned an approximate user satisfaction score of 4.45, demonstrating general contentment with its features.

Table 5: Users' Perspectives On The User Satisfaction Of The Developed BVAVS

ITEMS	MEAN
The system adequately supported user preferences and enhanced accessibility for diverse users.	4.42
I experienced no delays or lags in the system's response time during the accreditation and voting processes.	4.08
The system provided clear instructions and guidance throughout the accreditation and voting processes.	4.54
I felt confident in the accuracy of the system in recording and tallying votes without errors.	4.52
The system effectively maintained the anonymity of my vote, ensuring privacy and confidentiality.	4.68

In summary, the BVAVS system achieves an impressive usability score of approximately 4.44, an accuracy score of 4.8, and a security rating of 4.05, collectively indicating a generally positive user experience with few concerns. Its reliability rating is about 4.21, while user satisfaction averages around 4.45, demonstrating strong approval of its performance and protective measures. This underscores the BVAVS's superior efficiency and overall acceptance compared to the findings of [21], which reported average scores of 2.76 for security, 2.64 for user-friendliness, 2.72 for dependability, 2.8 for platform compatibility, and 2.94 for robustness.

5. CONCLUSION AND RECOMMENDATION

5.1 Conclusion

This research aimed to improve the electoral voting process in Nigeria by designing and implementing the BVAVS for the Independent National Electoral Commission (INEC). The developed system significantly enhances security, accuracy, reliability, usability, and user satisfaction in electronic voting and real-time vote counting. Given the increasing demand for secure electoral processes within Nigeria's socio-political landscape, this research is both timely and essential. It rekindles hope among Nigerian citizens for trust, confidence, and reliability in the INEC and in Nigeria as a nation. The BVAVS has the potential to complement or replace the current BVAS upon full implementation and could serve as a foundation for future research endeavours.

5.2 Recommendation

Here are some streamlined recommendations for the future of the BVAVS:

i. INEC should collaborate with agencies like NIMC, NITDA, and NPC to reduce financial implications by leveraging their resources.
ii. To address biometric registration challenges from poor internet connectivity, the system should adopt technologies such as edge computing, local data storage, or a mix of offline and online modes.
iii. Future research should explore incorporating cryptographic methods, blockchain, and one-time authentication tokens to enhance vote transparency while protecting voter anonymity.
iv. Additionally, scanning all ten fingers of prospective voters during registration can help prevent double registration attempts.

REFERENCES

[1] Eggers, A. C., and Nowacki, T. (2024). Susceptibility to strategic voting: A comparison of plurality and instant-runoff elections. *The Journal of Politics*, *86*(2), 000-000.
[2] Sintomer, Y. (2023). The government of chance: Sortition and democracy from Athens to the present. Cambridge University Press.
[3] Park, S. (2023). The Right to Vote Securely. *U. Colo. L. Rev.*, *94*, 1101.
[4] Adewale, O.S., Boyinbode, O.K., and Salako, E.A. (2020). *A Review of Electronic Voting Systems: Strategy for a Novel*. *February*, 19–29. https://doi.org/10.5815/ijieeb.2020.01.03
[5] Baudier, P., Kondrateva, G., Ammi, C., and Seulliet, E. (2021). Peace Engineering: The contribution of blockchain systems to the e-voting process. *Technological Forecasting and Social Change,* 162, 120397.

[6] Adewale, O. S., Boyinbode, O. K., and Salako, E. A. (2021). An Innovative Approach in Electronic Voting System Based on Fingerprint and Visual Semagram. *International Journal of Information Engineering and Electronic Business*, ***13***(5), 24–37. https://doi.org/10.5815/ijieeb.2021.05.03

[7] Awortu, E. C. (2022). Addressing the Challenge of Over-Voting in Nigeria: A Hindrance to True Democracy in a Technological Age. *Law and Political Review*, *7*, 24-43.

[8] Omolara, A. E., Alabdulatif, A., Abiodun, O. I., Alawida, M., Alabdulatif, A., and Arshad, H. (2022). The Internet of Things security: A survey encompassing unexplored areas and new insights. *Computers and Security*, *112*, 102494.

[9] Odighi, M. O., John-Otumu, A. M., Egbon, C. C., and Nwokonkwo, O. C. (2020). A fuzzy logic model for evaluating the standard performance of a prototype online voting system. *Journal of Advances in Science and Engineering*, *3*(2), 57-67.

[10] Palma, D., and Montessoro, P. L. (2022). Biometric-based human recognition systems: an overview. *Recent Advances in Biometrics*, *27*, 1-21.

[11] Sun, Z., He, R., Wang, L., Kan, M., Feng, J., Zheng, F., Zheng, W., Zuo, W., Kang, W., Deng, W., Zhang, J., Han, H., Shan, S., Wang, Y., Ru, Y., Zhu, Y., Liu, Y., and He, Y. (2021). Overview of biometrics research. *Journal of Image and Graphics*, ***26***(6). https://doi.org/10.11834/jig.210078

[12] Okokpujie, K., Abubakar, J., John, S., Noma-Osaghae, E., Ndujiuba, C., and Okokpujie, I. P. (2021). A secured automated bimodal biometric electronic voting system. *IAES International Journal of Artificial Intelligence*, ***10***(1), 1–8. https://doi.org/10.11591/ijai.v10.i1.pp1-8

[13] Suleiman, A. S., Gambo, A. A., and Kehinde, K. S. (2021). The historical evolution of Nigeria's present model of election and its unique features. ***9***(8), 185–193.

[14] Apalowo, T. O., Osigwe, A. C., and Adejumo, O. A. (2023). Nigeria's Electoral Integrity and Bimodal Voter Accreditation System: An Assessment of Public Opinion and Voting Behavior. *African Journal of Law, Political Research and Administration*, ***6***(2), 22–40. https://doi.org/10.52589/ajlpra-pue9qojb

[15] Jatain, A. (2020). Design and Development of Biometric Enabled Advanced Voting System. *SSRN Electronic Journal*, *3*, 50–53. https://doi.org/10.2139/ssrn.3670189

[16] Salman, W., Yakovlev, V., and Alani, S. (2021). Analysis of the traditional voting system and transition to the online voting system in the Republic of Iraq. *HORA 2021 - 3rd International Congress on Human-Computer Interaction, Optimization and Robotic Applications, Proceedings*, *August*. https://doi.org/10.1109/HORA52670.2021.9461387

[17] Olayinka, O. A. (2021). Development of a Model for a Secured Bimodal Voting Framework Using Timed Coloured Petri Nets. *Academia.Edu*, *January*, 5–7. https://www.academia.edu/download/64628661/2020_E-Vote-ID_Taltech_Press.pdf#page=439

[18] Deepa, G., Subramanian, B., Vennila, A., Kalaiselvi, T. C., Yeshvanth, B. N., Sountharya, N., Sowndharya, K. M., and Sivasamy, M. (2022). Biometric Based Voting System Using Aadhar Database. *Proceedings of the 2nd International Conference on Artificial Intelligence and Smart Energy, ICAIS 2022*, 1071–1075. https://doi.org/10.1109/ICAIS53314.2022.9743138

[19] Suraj, H. P. (2022). Arduino Based Smart and Remote Voting System with Smart Card Implementation and Dual Biometric Authentication. *International Journal for Research in Applied Science and Engineering Technology*, ***10***(7). https://doi.org/10.22214/ijraset.2022.45834.

[20] Okeke, P. C. (2023). *Development of new online voting methods for the integration of technology in the Nigeria electoral system*. International Journal of Recent Research in Mathematics Computer Science and Information Technology, **10**(1), 1–10. https://doi.org/10.5281/zenodo.7824503.

[21] Awotunde, J. B. (2017). Automated voting system using bimodal identification and verification technique. *Annals. Computer Science Series*, *15*(1).