KINETIK, Vol. 4, No. 2, May 2019, Pp. 115-126
ISSN : 2503-2259
E-ISSN : 2503-2267

Development of A Fingerprint Biometric Authentication System for Secure Electronic Voting Machines

B. U Umar*[1], O. M Olaniyi[2], L. A Ajao[2], D. Maliki[3], I. C Okeke[4]
[1,2,3,4]Federal University of Technology, Minna/Department of Computer Engineering
buhariumar@futminna.edu.ng*

Abstract

Democratic government in the world today rely on electronic voting as the foremost means of providing credible, transparent and fair elections for the electorate. There is a need for developed electronic voting systems to be security enhanced to ensure the authenticity of the developed system. Traditional paper balloting systems suffer from vote tampering, multiple voting and illegal voting by unregistered voters. They are also, susceptible to under-aged voting due to the difficulty in authenticating the identity of prospective voters. Manual collation and publication of vote results also lead to slow response times and inaccuracies in published results. This research paper proposes a system to combat the current challenges through the development of a fingerprint biometric authentication system for secure electronic voting machines. It uses a fingerprint biometric sensor, integrated via Python to verify users of the system. The inclusion of biometrics improves the security features of the system. The secure voting system is built using PHP and easy to use Graphical User Interface was designed using HTML and CSS. Users are required to interact with the machine via a 7" touchscreen interface. From the results, it shows that the developed machine has a minimum response time of 0.6 seconds for a specific operation, a FAR of 2%, FRR of 10% and overall system accuracy of 94%. The developed machine is able to combat the challenges of authentication of users, thereby guaranteeing the transparency, credibility, integrity and vote authenticity of the elections.

Keywords: *Fingerprint Authentication, Biometric Security, Electronic Voting, Integrity*

1. Introduction

Democracy is a system of governance of the people, by the people and for the people. The backbone of this governance system is the existence of elections, the right of governing citizens to choose their leaders. Voting is the process through which elections are carried out. The outcome of voting is the expression of the electorate, opinion and decision that is accepted by everybody. It means that the integrity of elections is the most important factor in the success of the democratic process [1].

Nigeria has been operating paper-based electoral systems for all her elections. This system involves printing ballot paper on which votes will be cast and distributing this paper to polling booths before the days of the election. After all, votes have been cast on election day, sealed boxes containing votes are opened before all legitimate members of the booth and counted. This information of counted votes is then submitted to a centralized station along with the paper evidence in the boxes. It is the duty of the central station to comply and publish the names of the winners and losers through television, radio or other official channel. This entire system, as with any other electoral system is only useful if the system is transparent [2].

However, this has not been the case in Nigeria. Most citizens are of the opinion that elections held in Nigeria today are neither free nor fair. [3] put forward that "elections as an essential component of the democratization process remains weak and undeveloped in the country with the biggest challenge of transparency of the voting system". Consequently, they argue, this leads to a loss of confidence and trust in the electoral process. Other challenges associated with the paper-based electoral system currently employed by the Independent National Electoral Commission (INEC) include and are not limited to, missing names of some registered voters, intimidation and disfranchisement of voters, multiple and underage voting, snatching or destruction of ballot boxes, miscomputation and falsification of results. These challenges stimulate post-election related violence with the far-reaching consequence of eroding peoples' trust and confidence in the democratic process [3].

Umar, B., Olaniyi, O., Ajao, L., Maliki, D., & Okeke, I. (2019). Development of A Fingerprint Biometric Authentication System for Secure Electronic Voting Machines. Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, and Control, 4(2). doi:http://dx.doi.org/10.22219/kinetik.v4i2.734
Receive December 19, 2018; Revise February 08, 2019; Accepted February 21, 2019

With this in view, it is necessary to adopt a better method of the electoral process. There is evidence pointing to electronic voting systems as the only means of achieving credible, fraud-free and fair elections in Nigeria [4]

Electronic voting is simply the use of some electronic means or machinery that is more or less computer supported in voting, where election data is recorded, stored and processed primarily as digital information. Electronic voting ensures better security, reliability and transparency. It promises greater efficiency, better scalability, faster speed and lower cost [5].

This research work proposed an accurate and responsive electronic voting system that will not only mitigate the challenges of conventional paper-based systems but will improve upon existing systems as regards efficiency, transparency and mobility. The system employed fingerprint biometrics for voter verification and encryption of the template of each enrolled fingerprint for security. The result of this work is an electronic voting machine that is power-efficient, secure and easy to use for the electorate. It characterizes elections with credibility, integrity and vote authenticity.

2. Basic Concepts and Related Works

Electronic Voting provides a means by which members of a democratic society are able to choose their leaders. This is a culmination of the synergy between technology and politics [6]. Two types of electronic voting exist – Poll site voting, where voters must be physically present at designated polling units and Remote voting which does not have that requirement. Electronic voting systems could also be Online [6] systems that need constant internet connections or Offline [7] systems that do not need to be connected online. Electronic Voting Machines (EVMs) are specialized hardware built specifically to implement electronic voting systems. As with all computing equipment, they receive voting data inputs, analyze the inputs and produce voting results that correctly reflect the choices of the electorate. Some benefits of applying these systems to existing traditional methods are not limited to increased trust in the voting system, convenience, improved safety and reliability. Also, the speed and accuracy of vote counting and result publication cannot be overlooked.

Fundamental to achieving this research was the inclusion of biometrics in the developed electronic voting system. Biometrics simply means correctly determining the identity of individual features that are unique to that individual [7]. Those features are physiological or behavioural. Physiological features are those attributed to the composition or shape of the human body, such as ear, eye, hand and fingerprints. On the other hand, behavioural features use the behavioural pattern of the mannerisms of a person for identification. Mannerisms include gait and voice signature. Biometric traits include DNA, facial recognition, fingerprint recognition, gait, voice and vein recognition [8]. This research focuses on fingerprint recognition as a means of identity determination. For fingerprint biometrics, templates (fingerprint images showing bifurcations and ridge endings) are captured and stored. Identity verification is through comparison of the current image with that of stored template. The bifurcations and ridge endings, collectively known as minutiae are the features through which each individual's fingerprints are distinguished. The fingerprint identification process is shown in Figure 1.

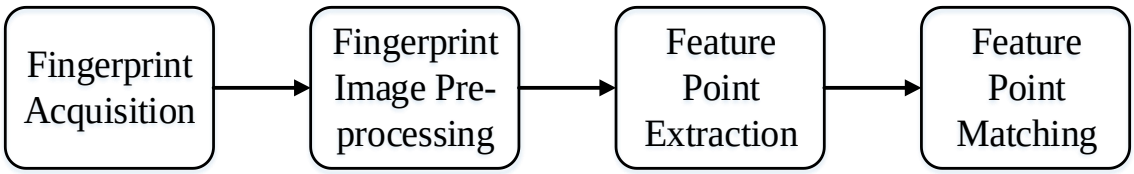

Figure 1. Steps in Fingerprint Identification System

There are certain requirements that are standard in the design of secure electronic voting systems. This is to ensure the actual security of that voting system [9]. The security definitions which must be met by this work include:

1. Transparency: Voters must not be in doubt about the concept and methods of usage of the adopted voting system. It is paramount that with a working knowledge of the system, they can testify to the transparency of the election process.

2. Auditability: Provisions should be made such that whenever doubt may occur as to the accuracy or authenticity of election results, it can be successfully proven that the voting system results are indeed infallible.
3. Uniqueness: This definition for the system implies its specifications for the age, citizenship and eligibility of each voter to partake in elections.
4. Simplicity: According to [10], complexity is the bane of security. Hence, such voting systems, however secure, must also include simplicity amongst design priorities.
5. Integrity: It must be said that developed systems must be tamperproof – no single vote can be altered or deleted in any form.

False Acceptance Rate seeks to find out what ratio of incorrectly accepted users of the system to a total number of system users. On the other hand, False Rejection Ratio is the ratio of false rejects to total users. These are two majorly used metrics in performance analysis of fingerprint biometric systems [11].

There are various instances in the literature that aimed at deploying similar systems using fingerprint biometrics in secure electronic voting. Some of these literature and the progress made as well as the challenges currently being faced by the existing body of knowledge are captured in this section.

[12], designed a voting machine for the Bangladesh electorate that utilized a biometric scanner to register and eventually identify voters. Fingerprints are collated in conjunction with voter ID in the database. The designed machine had a Control Unit in charge of voter registration, Ballot Unit displayed candidate information while the Power Unit's function was to provide a charge in case of power failure and to monitor the charge level of the machine. An Arduino Uno, LCD display, a biometric scanner and membrane keypad were the major components used to achieve the machine. The developed machine is cost friendly, power efficient and scalable. It also prevents multiple voting. However, the database needs to be preloaded before the election period. Also, the system does not have an appealing user interface for easy user interaction.

Another electronic voting machine developed by [6], was realized using a microcontroller, LCD and fingerprint module. It used mechanical switches for voters to indicate choice of candidate. In addition to the developed algorithms for extraction and matching, the system was shown to have a faster response time by reducing the counting time but was limited in the number of registerable candidates (9) and maximum votes accorded to each candidate (10,000).

In [2], multiple trait verification techniques were developed using fingerprint and facial recognition. The system had an accuracy of 91% for facial recognition and 98% for fingerprint recognition. The developed system though showing high accuracy had slow response times as the number of features extracted and stored in the biometric template increased. The system was significantly more compute-intensive than other biometric authentication systems reviewed in this work.

The authors in [13], developed an online poll site voting platform, using an Arm9 microcontroller and KY-M6 fingerprint sensor. It had two units – Balloting Unit where voting takes place and Control Unit which is handled by the poll presiding officer. The system prevents multiple voting and had a maximum of 64 candidates per poll. The system rejected unregistered voters from using the system but required an online database to pull photos used for visual identification.

An online voting system was proposed by [5]. Short Messaging Service (SMS) was used as a token to aid user authentication via username and password. The system used a well-designed GUI for both the user and the administrator. The proposed system was less-expensive and easy to acquire; it is an online system. However, the system did not incorporate biometrics for any kind which reduces the system's ability to withstand security breaches.

An electronic voting system was proposed by [14] which incorporated biometrics such as fingerprints, finger vein, iris acquisition, iris segmentation and facial recognition to enhance its security and to aid authentication of voters. The proposed system could be implemented as an online or offline voting system. These features together with the Global System for Mobile communication (GSM) module made the system robust and averse to human or mechanical errors. While the system also promised lesser cost and improved accuracy, it does not incorporate any form of encryption, which means that private biometric data can be illegally obtained. The system also lacks fast response time owing to waiting times for One-Time-Passwords (OTPs).

At the end of reviewing related literature and progresses in electronic voting systems development, it has been clear that significant strides have been made in ensuring the security of developed electronic voting systems. Biometrics have played an important role in voter identity

verification and authentication. Developed systems, however, are mostly rigid in their user interfaces, requiring a learning process to efficiently use such machines. It is possible to reinforce the accuracy of the developed systems. It is also true that online voting systems or remote voting systems tend to have high latency which impacts the overall user experience. This research used fingerprint biometric authentication to enhance the security, resilience of [5]. It also reduces the response time in [12], while maintaining an accuracy of 94% compared to the 91% achieved by [2].

3. Methodology

3.1 Hardware System Design

The electronic voting machine is made up of the hardware and software components. The hardware is comprised of: Raspberry Pi 3B+ (1.4GHz SoC, 1GB RAM, 40-pin GPIO, DSI port, 5V, 2.5A), ZFM-60 Fingerprint Sensor (UART interface, 3.3V, 65mA, 57600 baud rate) and 7" Touchscreen (DSI data interface, 5V, 200mA, 800x480px)

The software components are the web GUI and the fingerprint registration and authentication element. The electronic voting machine block diagram shows the interaction between different components. The Pi 3B+ functions as the control unit of the machine. It is the component that receives user input data from the touchscreen unit, manipulates the data and provides feedback to the touchscreen unit. The fingerprint sensor sends in input when registering and verifying user identity. The touchscreen functions as the output unit to display data for user interaction and final results of user operation. The overall integration of these units will result in the intended electronic voting machine as shown in Figure 2. The components used in the system and the designed overall package is shown in Figure 3.

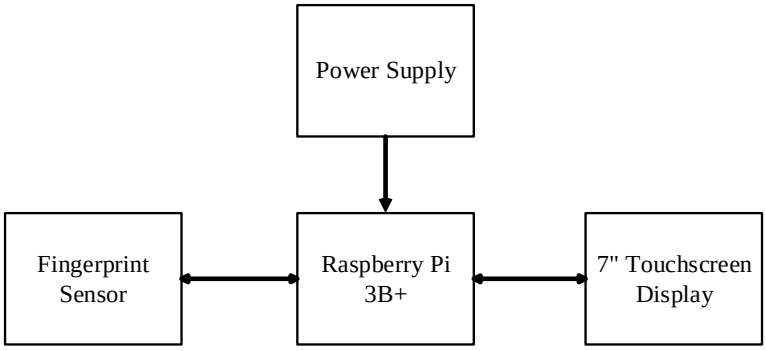

Figure 2. Electronic Voting Machine Hardware Block Diagram

Figure 3. Designed System Hardware – Side View

3.2 Software System Designed

The electronic voting machine was designed for two types of users – administrators and voters. The block diagram in Figure 4 gives an overview of the system design. Firstly, the admin is in charge of voter registration, candidate registration, auditing of casted votes and finally result in publication. Voter registration occurs before the election day. During registration, the system makes use of the fingerprint module to capture fingerprint templates of new users. The voter data is stored in the voter database while the fingerprint template is encrypted and goes into the fingerprint database. The templates are used for matching comparisons during the voting process. The admin audits the vote records and publishes the results accordingly.

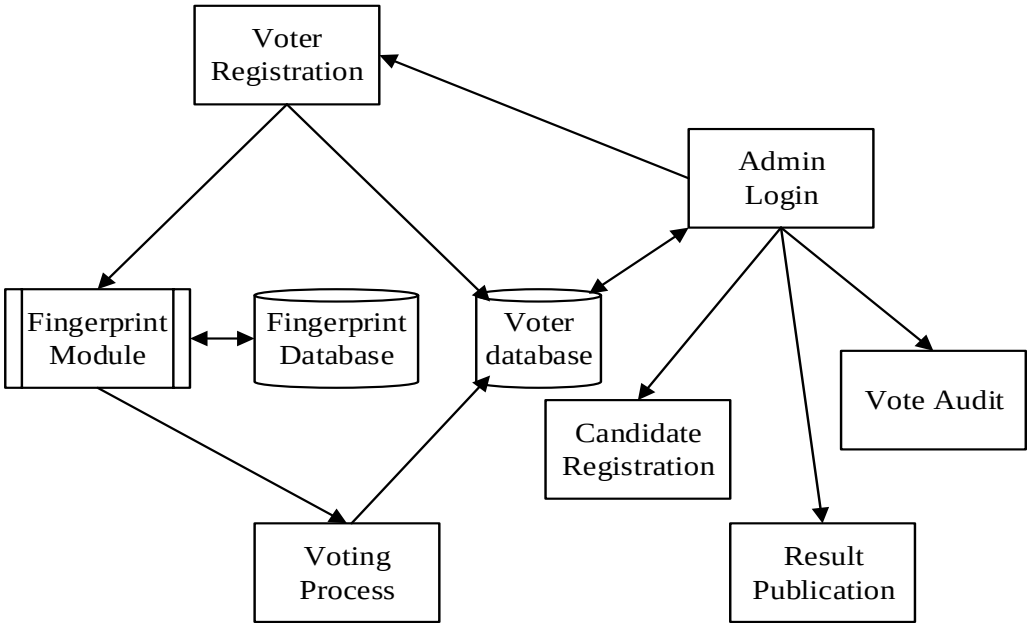

Figure 4. Electronic Voting Machine Block Diagram

The flow chart of the designed system shows the progressions during the usage of the electronic voting system. It shows the transfer of information to and from user to system, and how this information determines the next process for the user. The electronic voting process flow chart is shown in Figure 5. The system begins by requesting the user to authenticate their registered fingerprint. Access is only granted to users with valid fingerprints after which they input their Voter ID. Once verified, they are allowed to vote only if they have not previously voted. Logging out of the system by the voter indicates the end of the system usage.

The software development was concerned with the Raspberry Pi control program that controlled inputs from the input unit, controlled the flow of data within the control unit, as well as the elements to be displayed on the output unit. Raspberry Pi is a fully-fledged computer that is the size of a credit card. It has the capacity to run programs written in different languages such as C, C++, Python and QT applications just to name a few.

The Raspberry Pi software features code that initialized all the output and input units, collected and compared data from the fingerprint module using Python scripts and used matching algorithms to compare the data, used HTML, CSS and JavaScript for the display to render info to the user in a simple User Interface through the touchscreen. PHP and MySQL are used for communication between the web interface and the database tables that hold voter and voting data.

Use-case diagrams are employed here for better understanding of the system usage by both the administrator and the user. Use-case diagrams are a part of the Unified Modelling Language which helps to conceptualize the system behaviour. The use case model shown in Figure 6 details the functionalities of the Admin such as voter registration, candidate registration and vote audit. Those for the user are not limited to voter login, fingerprint enrollment and authentication.

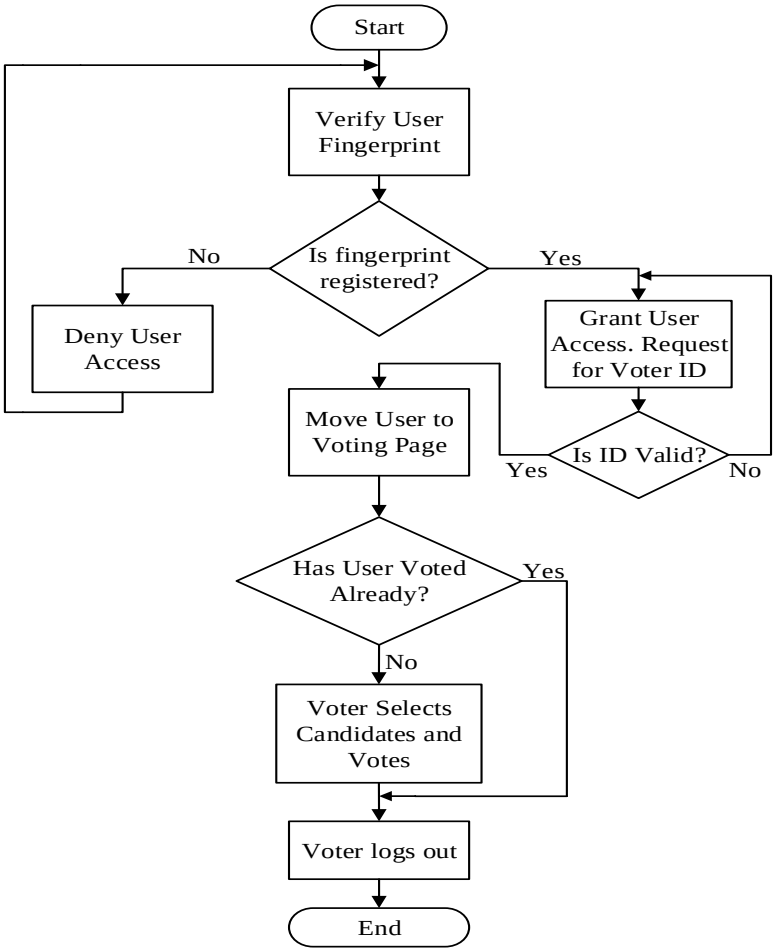

Figure 5. Electronic Voting Process Flow Chart

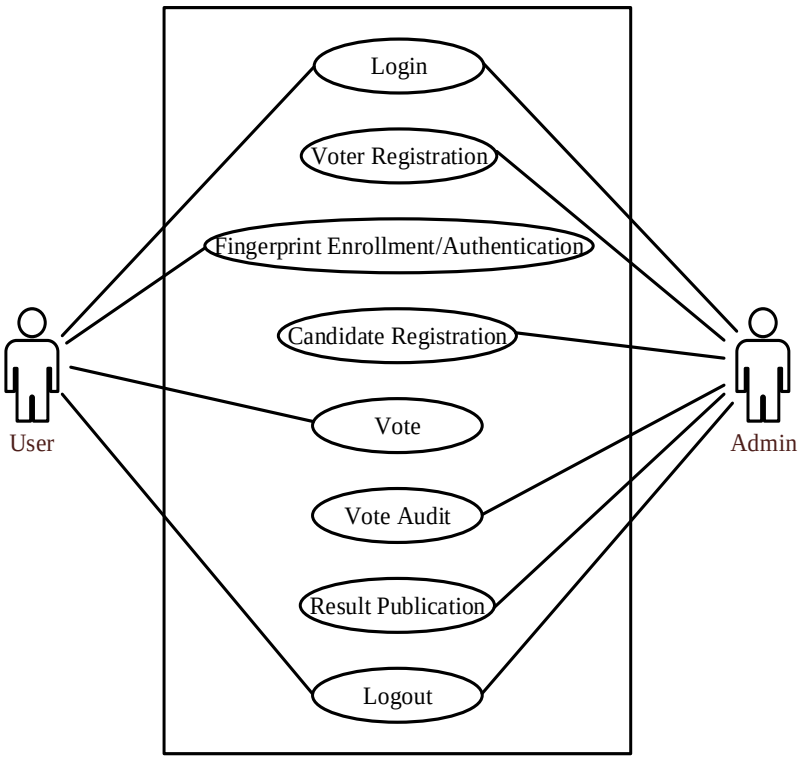

Figure 6. Use-Case System for Developed System

4. Results and Discussion

The electronic voting machine prototype was implemented according to the design as shown in Figure 7. The hardware components selected for the developed system (Raspberry Pi 3B+, ZFM-60 fingerprint sensor,7" touchscreen display) are all enclosed in the designed package. The top holds the touchscreen for the user interaction and the opening for the fingerprint sensor. The entire package is held together by screws for easy assembly and disassembly. It also has slits by the front of the power connection cable (microUSB) and left side to connect peripherals for debugging. It should be noted that these slits are dust proof. The entire package has its weight less than 2kg, making it very mobile.

The developed system uses PHP and MySQL to implement the voting system. PHP MyAdmin has used the view the system tables as shown in Figure 8. The tables – admin, nominees, organization, positions, voters and votes help the system to properly manage its data. The admin is also able to view the voter for each vote for a particular candidate. This way they can audit and verify that each casted vote is valid since each vote is tied to a particular voter. Figure 8 also, shows the votes database table as described. The votes table shows how many votes each candidate in each category has accrued. It also exhibits the system's ability to export votes if needed.

Figure 7. Electronic Voting Machine

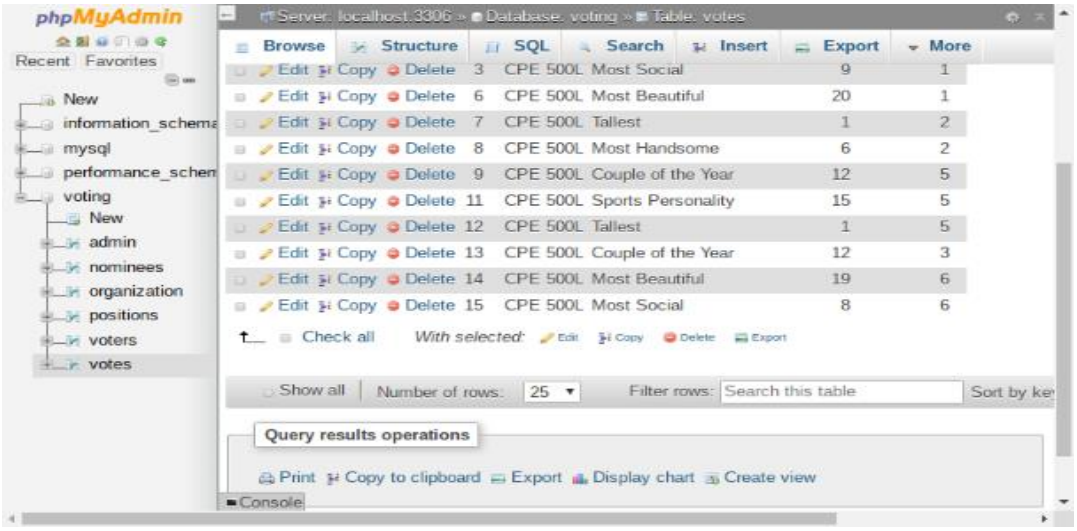

Figure 8. Votes Database Table

4.1 Voting System GUI

The developed GUI has a home panel for the admin. The admin has many menus through which they select the particular functionality they wish to use at the time such as creating candidates, categories and registering voters. Figure 9 shows one of such functionalities which is voter registration.

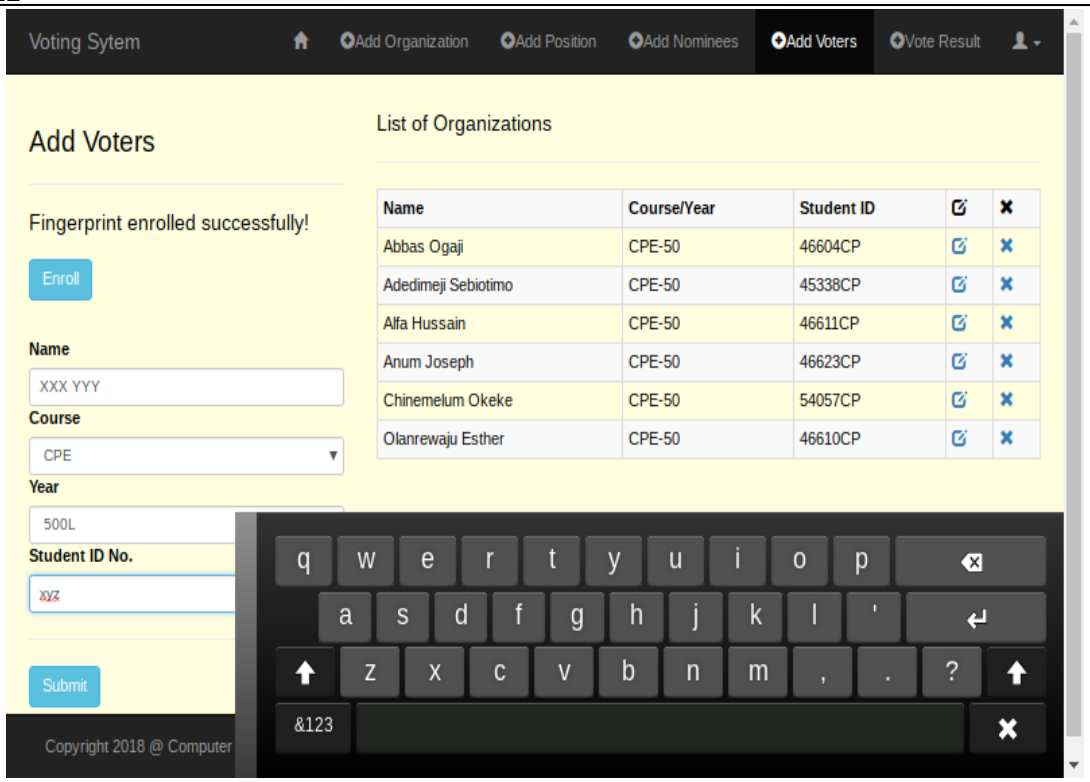

Figure 9. Register Voter Panel

For the users, there is a welcome screen where they are required to verify their fingerprints. The page is only shown if the user fingerprint is verified. After verification and ID input, the user is taken to the voting page where they select the candidate from the dropdown menu and each vote is cast by selecting the vote button. The voting screen is shown where they only need to tap on their choice for the machine to record their votes (Figure 10). The system checks and prevents multiple voting.

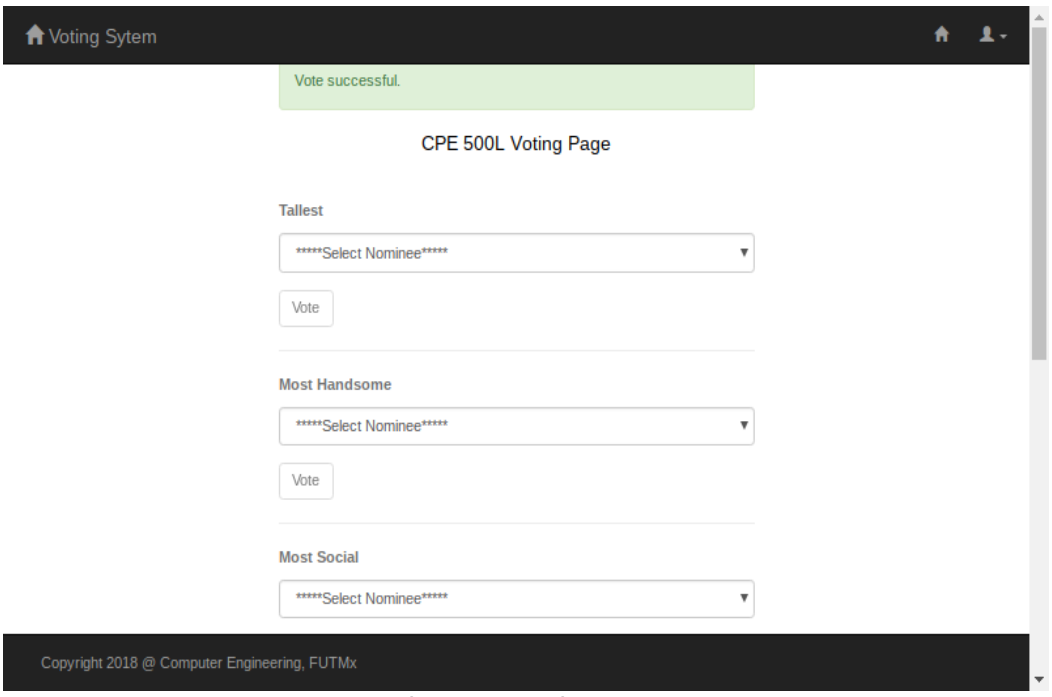

Figure 10. Voting Page

4.2 Performance Evaluation

The developed system's performance was evaluated using False Accept Rate, False Reject Rate, accuracy and response time of the system. The rationale of using FAR is to see how well the system keeps out or correctly invalidates unregistered users while FRR is used to determine the system's ability to correctly authenticate registered users of the system.

A total of 45 unregistered fingerprints was tested on the system. A single fingerprint from the total was falsely accepted giving the system a FAR of 2% as seen in Table 1 and Figure 11, indicative the system is characterized with rejecting unregistered and ineligible voters. This characteristic maintains the integrity of the election process and the correctness of the election outcome. For evaluating the FRR, five different registered users each tested the system ten times and the results in Table 2 were obtained. The worst result for a particular user was two incorrect rejections. The best result was no rejection for a registered user. The overall FRR is 10%. It is to be noted that incorrect/improper placement of the finger on the sensor was the most common reason for a false rejection. Proper positioning of the finger on the sensor will mostly validate the registered fingerprint.

Table 1: FAR for the Developed System

Matching Tries	Accepted	Rejected	FAR
45	1	44	2%

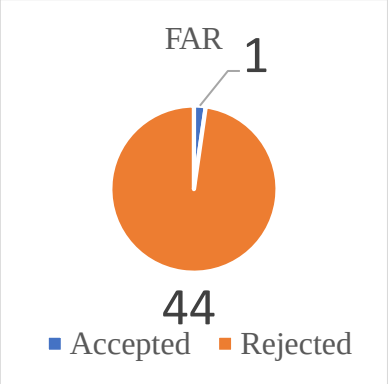

Figure 11. Accepted to Rejected Fingerprint Ratio

Table 2. FRR for the Developed System

Matching Tries	Accepted	Rejected	FRR
50	45	5	10%

The FAR of 2% shows good performance of the system in keeping out unregistered voters, hence preventing illegal voting, unregistered voting and underaged voting – which forms some of the objectives of the developed system.

The response time of the system is the time difference from user action, input to the system to the corresponding reaction of the system to the input. It is concerned with the latency observed during system operation. The measured response times of the system for different scenarios are shown in Table 3. Accuracy is the degree of proximity of a measured value to the true or actual value. The accuracy of the fingerprint verification system has been determined, both for verification of registered fingerprints and invalidation of unregistered fingerprints. The Results obtained are shown in Table 4.

Table 3. System Response Times

Action	Response Time (s)
Voter Login	3.4
Voting	0.6
Admin Login	0.8
Admin Register Candidate	0.9
Admin Register Voter	9

Table 4. The accuracy of the Fingerprint Verification System

Fingerprint Sensor Operation	Measured Outcome	True Outcome	Accuracy (%)
Verify Registered	45	50	90
Invalidate Unregistered	43	44	98
Total	88	94	94

As seen in Table 3, the developed machine exhibits fast response times for user operations. The response time of 9 seconds for Admin Voter Registration is due to users requiring fingerprint capturing twice in order to get a high-quality template for future fingerprint matching. Also, the system has achieved an accuracy of 94%, which, is better. From the results of the system development, it shows that the system has improve on the upon the conventional paper-based system by improving the efficiency and transparency and mobility of the voting process because the developed system is portable to move around. it has also, been determined that the system can: Prevent multiple voting; Prevent illegal voting and unregistered users; Encrypt fingerprint templates, hence preventing snooping or hacking and Improve the security, resilience of electronic voting through implementing fingerprint biometric authentication. Although, the research is limited to prototype.

5. Conclusion

This research work has presented a robust electronic voting machine that adequately resolves the challenges of authentication, transparency and credibility of traditional voting systems. It has demonstrated the quick response in voting processes as well as vote collation and publication. It has shown high accuracy comparable to those established in the literature. The developed authentication system prevents unauthorized users from using a secure voting system. The system used the ubiquitous touchscreen interface for easy user interaction with the system. Therefore, the combination of the fingerprint biometric authentication and secure voting enables the system to provide a means of holding credible, free and fair elections. This restores the public's trust in the election process which provides a much better democratic experience for society. In future, it will be worthwhile to explore the possibility of a combination of online voting systems that incorporate multiple biometric traits as a means of voter authentication. It is also imperative that such future systems will demonstrate faster response times than other online voting systems with better fingerprint sensor.

References

[1] M. K. Alhasnawi, & Alkhalid, A. S. , "Secure Online Voting using Steganography and Biometrics," *International Journal of Current Engineering and Technology,* Vol. 7, No. 3, Pp. 1097 - 1104, 2017.

[2] S. S. Najam, Shaikh, A. Z., & Naqvi, S. , "A Novel Hybrid Biometric Electronic Voting System: Integrating Finger Print and Face Recognition," *Mehran University Research Journal of Engineering and Technology,* Vol. 37, No. 1, Pp. 59–68., 2018.

[3] S. Ahmad, Abdullah, S. A. J., & Arshad, R. B. , "Issues and challenges of transition to e-voting technology in Nigeria " *Public Policy and Administration Research,* Vol. 5, No. 4, Pp. 95–102., 2015.

[4] R. I. Salimonu, Osman, W. R. B. S., Shittu, A. J. K., & Jimoh, R. G., "Adoption of E-Voting System in Nigeria : A Conceptual Framework.," *International Journal of Applied Information System,* Vol. 5, No. 5, Pp. 8-14, 2013.

[5] D. W. S. Alausa, & Akingbade, L. O. , " Electronic Voting : Challenges and Prospects in Nigeria ' s Democracy," *The International Journal of Engineering and Science,* Vol. 6, No. 5, Pp. 67-76, 2017.

[6] P. Saxena, Prakash, S., & Pandey, P. , "Design of Biometric Electronic Voting Machine.," *International Journal of Advanced Research, Ideas and Innovations in Technology,* Vol. 3, No. 6, Pp. 211 - 214, 2017.

[7] E. bañez, Galdámez, N., Estrebou, C., Pasini, A., Chichizola, F., Rodríguez, I. P., & Pesado, P. M. (2009), "Biometric identification in electronic voting systems," *In Ciencias de la Computación*, Pp. 1295 - 1303, 2009.

[8] G. Patni, & Sharma, S. , "Biometric System Introduction with its various Identification Techniques," *International Journal of Scientific Research in Computer Science, Engineering and Technology,* Vol. 2, No. 3, Pp. 866 - 871, 2017.

[9] O. M. Olaniyi, Taliha, F. A., Abdullahi, I. M., & Abdusalam, A. K. , " Design and Development of Secure Electronic Voting System Using Radio Frequency Identification and Enhanced Least Significant Bit Audio Steganographic Technique.," *Journal of Computer Engineering,* Vol. 17, No. 6, Pp. 2278 - 2661, 2015.

[10] O. M. Olaniyi, Taliha, F. A., Ahmed, A., & Joseph, O. , "Design of Secure Electronic Voting System Using Fingerprint Biometrics and CryptoWatermarking Approach," *International Journal of Information Engineering and Electronic Business,* Vol. 8, No. 5, Pp. 9 - 17, 2016.

[11] H. Srivastava., "A Comparison Based Study on Biometrics for Human Recognition.," *IOSR Journal of Computer Engineering (IOSR-JCE),* Vol. 15, No. 1, Pp. 22 - 29, 2013.

[12] M. J. Hossain, Shakur, A. S., Ahmed, M. J., & Paul, B. , "Designing a Cost-Effective , Reliable and Scalable Electronic Voting Machine for National Election of Bangladesh," *Recent Advances in Circuits, Systems and Automatic Control*, Pp. 79 - 88, 2015.

[13] M. Sudhakar, Divya, B., & Sai, S. , " Biometric System Based Electronic Voting Machine Using Arm9 Microcontroller.," *IOSR Journal of Electronics and Communication Engineering* Vol. 10, No. 1, Pp. 2278 - 2834, 2015.

[14] G. Alaguvel R., G., & Jagadhambal K. , "Biometrics using Electronic Voting System with Embedded Security," *International Journal of Advanced Research in Computer Engineering & Technology,,* Vol. 2, No. 3, Pp. 2278 - 1323, 2013.

ISSN: 2503-2259; E-ISSN: 2503-2267