A Bi-Factor Biometric Authentication System for Secure Electronic Voting System

Buhari Ugbede Umar
Department of Computer Engineering.
Federal University of Technology
Minna, Nigeria
buhariumar@futminna.edu.ng

Olayemi Mikail Olaniyi
Department of Computer Engineering
Federal University of Technology
Minna, Nigeria
mikail.olaniyi@futminna.edu.ng

Abisoye Blessing Olatunde
Department of Computer Engineering
Federal University of Technology
Minna, Nigeria
b.abisoye@futminna.edu.ng

Ademoh Agbogunde Isah
Department of Electrical and Electronic Engineering
Federal University of Technology
Minna, Nigeria
ademoh.isah@futminna.edu.ng

Arifa Khatoon Haq
Department of Computer Engineering Federal University of Technology
Minna, Nigeria
arifa@futminna.edu.ng

Isaac Taiye Ajayi
Department of Computer Engineering
Federal University of Technology
Minna, Nigeria
smeplegacy@gmail.com

***Abstract*—Because voting is the most important way for people to express their thoughts and choose their preferred candidates or administrations, it is an essential aspect of the democratic process. The Nigerian Independent National Electoral Commission (INEC) employed a partial e-voting device with the use of a card reader to identify and authenticate the electorate in general elections in 2015 and 2019. As a result of the deployment of the card reader, the country's voting processes have improved considerably in terms of legitimacy and trustworthiness. This great concept, however, was not without problems, since a lack of fingerprint recognition and identification prevented a substantial number of people from voting. This is due to the continual shifting of the skin of the finger as a result of the vast majority of voters in this category's farming and tiresome work. If this remains unchecked, it will not only disenfranchise a large number of voters, but it will also call into question the process' legitimacy. This work proposed a voting system with a bi-factor biometric authentication mechanism to address these concerns (fingerprint and iris). This will speed up the voter identification and authentication procedure, as well as prevent voting fraud and voter disenfranchisement as a result of the card reader failing to identify them. An accuracy of 94 percent was obtained as a result of the analyses. The Iris response time for voter enrolment and verification is 15s and 20s, respectively, while the fingerprint response time is 3s and 9s, respectively.**

Keywords—Fingerprint Authentication, Iris Recognition, Pattern Match, RFID

I. INTRODUCTION

Election is one of the most fundamental parts of democracy, and it applies to all citizen classes. Elections are regarded as the most crucial pillar of democratic governance in any democracy [1]. Free and fair elections are the bedrock of democracy. Electoral fraud, which is common in nascent democracies around the world, is one way that elections can be unfair. A free and fair election is the foundation of true democracy because it encourages individual liberty under the law, allowing citizens to act and express themselves as they see fit [2]. Voting and elections are crucial components of life in a democratic culture. Voting is a fundamental right of every citizen, an important component of democratic action, and one of the most important responsibilities of every citizen [3, 4]. Election turnout is sometimes used as a metric for assessing a democracy's health. Nonetheless, voter turnout is on the decline [5]. The aggregate number of persons who exercised their right to vote in recent Nigerian elections has progressively fallen. This is owing to widespread public distrust of democratic procedures, with the majority of people saying that today's Nigerian elections are neither free nor fair [6], and this is mostly due to the traditional strategy adopted. This is concerning from a constitutional standpoint because, if the cause of the decline is not addressed, doubts about the legitimacy of individuals in positions of power would eventually arise [3]. To reduce voting time, offer confirmation that a vote was properly accounted for, prevent bribery, eliminate ballot-filling errors, and improve the system's usability, the traditional voting system should be automated [5, 7].

Electronic voting is the principal way by which democratic governments ensure that elections are credible, transparent, and fair around the world [6]. Nigeria has also joined the League of Democracies throughout the world in this laudable quest. The Nigerian Independent National Electoral Commission (INEC) employed a partial e-voting system using a card reader to identify and authenticate voters in general elections in 2015 and 2019. The introduction of the card reader has improved the validity and effectiveness of electoral procedures across the country significantly. However, this great concept was not without drawbacks, since a failure of the technology to recognize and authenticate fingerprints prevented a large number of people from voting. Most of the time, the match was a ruse. This is due to the frequent shifting of the skin of the finger as a result of farming and arduous work by the large majority of

978-1-6654-7978-3/22/$31.00 ©2022 IEEE

voters in this category. If this remains unchecked, it will result in the disenfranchisement of a large number of voters, threaten the process' validity, and stifle progress toward the adoption of a fully functional electronic voting system by 2023.

This study proposed a voting system with a bi-factor biometric authentication mechanism to address these concerns. Using one of two biometric methods (fingerprint or iris) to speed up the voter identification and authentication process, reduce voting fraud, voters' disenfranchisement due to not being recognized by the card reader, reduce voting time (due to a long line for identification), and eliminate the manual voting system (as the electorate will be identified using one of the biometric methods).

II. REVIEW OF RELATED WORKS

A number of research have been undertaken in the topic of e-voting. We'll look at a few of this research in this section. E-voting system stability design [8]. The study developed a novel e-voting model that complies with e-voting security requirements. This is based on a blind signature plan and the homomorphic characteristic. This system was only meant to be used as a test model. [9] devised a biometric-assisted hybrid mobile e-voting system. Information technology is transforming and shaping today's networked society, and its solutions are becoming essential drivers of human behavior in practically every industry. Biometrics based on Adhar card numbering were used to construct the anti-ragging voting system [10]. The study employs a fingerprint to verify the anti-ragging voting mechanism' effectiveness. By employing a smart electronic voting machine to choose candidates and fingerprint recognition technology to assign each person a rival name. It took a long time for the machine to respond.

Similarly,[11] proposed a fingerprint-based Web-based voting system. To assure high-performance, high-security voting systems, research is being performed that uses internet technologies to make voting systems more realistic. Under the proposed EVS, voters will be required to scan their fingerprints, which will then be compared to a previously saved image in a database. [12] has created electronic voting machines based on RFID. The method demonstrated the use of a gadget that eliminates the need for manual labor and lowers the likelihood of fraudulent elections. There would be a vast number of voters in the real world. Storing them as a string array would fail in that situation.

[13] also presented an iris-based e-voting approach based on the iris recognition Aadhar registry mechanism for a secure and stable Aadhaar-based electronic voting system. The system is too slow, which poses a problem. [14] proposed that the Aadhar Number and its unique biometric identification software be used to notify and prevent fraudulent authorities from incorporating voter data into an e-voting system. A Smart Voting System was proposed [15] using an Android software. To ensure their uniqueness in the scheme, each voter's Aadhar ID and face image are included in the application. This technology eliminates the manual effort of the election committee. [16] devised an online voting mechanism using an Android interface. This request gives the voter a break from the lengthy procedure while also providing security. They can also recognize motions, but the Android platform's biggest issue is authentication. A proposal for an E-Voting Framework for Biometric Security [17] has been made. The device is viewed from two perspectives: that of the server and that of the user. The voting system will print tangible copies of the ballots, as well as a unique number, for voters after they have cast their votes. This unique number, as well as the voter's name and identity number, are all covered. [18] suggested a Fingerprint and Face Recognition-based Smart Voting Machine. The user does not need to bring his or her ID with all of his or her required information to use the Smart Voting Machine. The voter serving as identification merely needs to place his finger in the fingerprint scanner and capture his identity in a web camera at the polling booth counter, allowing him to receive an on-the-spot fingerprint and face. The system worked as promised, although it took a long time to respond.
time.

According to the review, most existing systems have an issue with authentication since they rely on a single way of authentication—using a fingerprint. Furthermore, some of the systems are overly slow to respond, causing additional delays. Finally, they are primarily designed as a test bed and fail miserably when used in large elections. Because it is fast, reliable, uses double authentication, and can be used for big elections, the proposed system will address all of the limitations identified.

III. DESIGN METHODOLOGY

Voting technology that is both modern and secure was used in this study. A Raspberry Pi, fingerprint sensor, RPi night vision camera, RFID, and other components make up the hardware module. In addition to fingerprints and RFID cards, the suggested system uses iris recognition to secure an individual's verification. In addition to fingerprint verification, iris recognition is utilized to provide additional protection in the event that someone attempts to vote fraudulently by using phony fingerprints. The voter will be confirmed for the system if the captured iris pattern matches the iris pattern templates in the database. Figure 1 depicts the schematic building block that makes up the design.

Biometrics are computer-assisted ways for identifying or verifying a person's identity based on a physiological or behavioral trait. Physiological features include hand or finger representations, facial features, and iris recognition. Behavioural characteristics are traits that can be learned or acquired. Behavioral characteristics include dynamic signature authentication, speaker verification, and keystroke dynamics, to name a few. When comparing a registered or enrolled biometric sample (biometric template or identifier) with a newly captured biometric sample, biometric authentication is necessary (for example, a fingerprint captured during voting).

A biometric trait sample is taken at registration, analyzed by a computer, and saved for further comparison. Biometric recognition can be employed in Identification mode, when the biometric system searches the biometric database for a match to identify a person from the total enrolled population. To guarantee that a person has not claimed for benefits under two

978-1-6654-7978-3/22/$31.00 ©2022 IEEE

different names, an entire database might be examined. This is referred to as "one-to-many" matching on occasion. The biometric software in a system can also be utilized in Verification mode, which confirms an individual's claimed identification based on their previously enrolled pattern. Matching on a one-to-one basis is also known as "one-to-one" matching. Instead of inputting a password, the admin swipes an RFID card, and the user is authorized by a quick touch with a finger or a glimpse at a camera. The iris of the eye, which is the colored area around the pupil and fingerprint, is employed in this stage. Iris patterns are regarded to be one-of-a-kind and long-lasting.

To authenticate a user's identification, the fingerprint authentication system scans and reads their fingerprints. A new user's fingerprint must be read, extracted, and stored in the database before he or she may be registered. The retrieved fingerprint is compared to the stored fingerprint in the database to authenticate a registered user. Figure 2 depicts the fingerprint enrolment and authentication process.

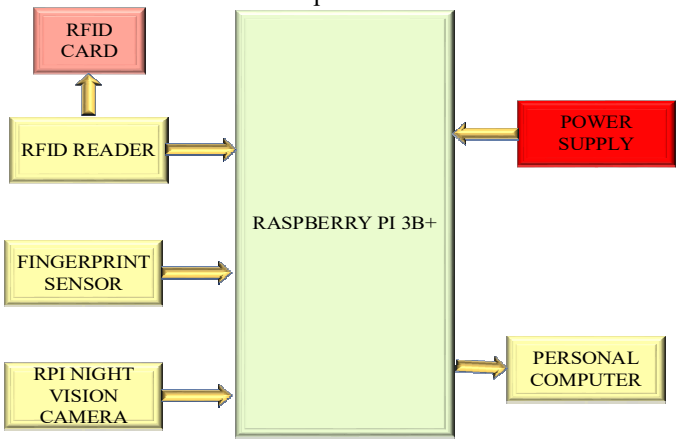

Fig. 1. System Block Diagram

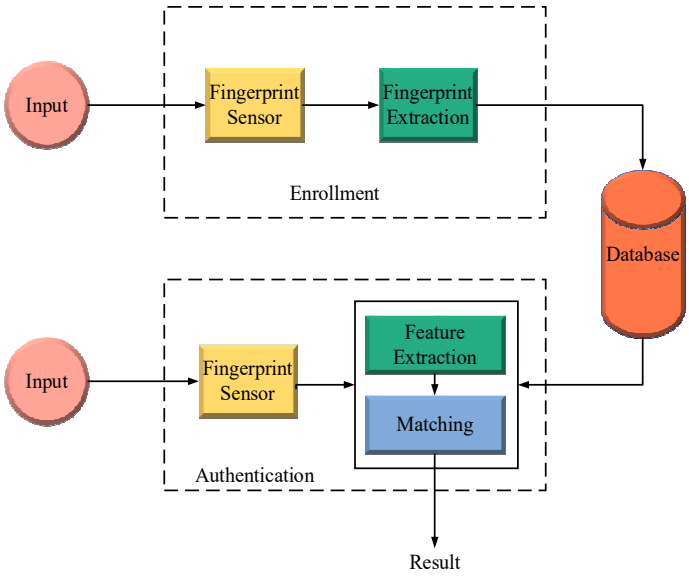

Fig. 2. Fingerprint Enrolment and Authentication

IV. RESULTS AND DISCUSSION

The conclusions of the research effort are presented and discussed in this section. The system accuracy and response time were determined, as well as the typical assessment metrics of the False Acceptance Rate (FAR) and False Rejection Rate (FRR). The method's machine reaction time and accuracy are also calculated, and the findings are presented in Tables 1 and 2. The Raspberry Pi 3B+, fingerprint sensor, iris recognition, RFID sensor and tag, and a laptop TTL USB module were chosen as the hardware components for the built system. Figure 3 depicts the developed electronic voting system.

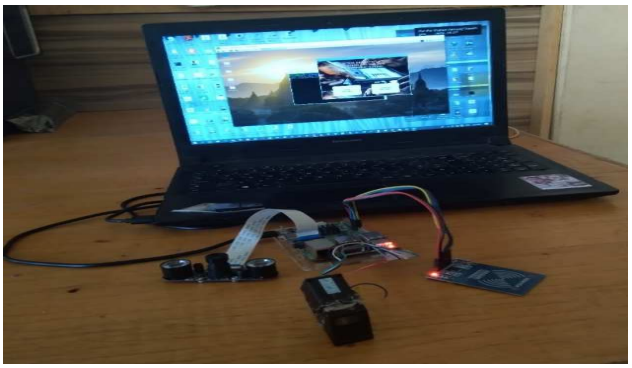

Fig. 3. The Developed Electronic Voting System

The developed system makes use of PyQT5 and MySQL to implement the voting system. MySQL is used to display machine tables that are made up of three databases: a voter database, an election database, and a party database. The ID, election title, station, date, parties, election form, election starting, and stopping times are all listed in the election table. The party's table includes categories for identification, titles, and elections, as well as names for each category. For voters, the system also displays the party database table. ID, Name, Age, LGA, State, REG Station, Station ID, Title, Pooling Unit Station, Date, Result, Parties, Start and Stop Time are all included in the table of voters. The database aids the system's data management; the administrator is given the ability to add, examine, edit, and delete voters for a certain candidate. Because each vote is linked to a specific voter and a specific polling unit, they can audit and verify that each cast vote is valid. The vote table displays the number of votes each contender received in each category.

A graphical user interface was built to allow users to engage with the electronic voting system. Figure 4 depicts the graphical user interface. It has capabilities allocated to the voter's manager, GUI, such as voter forms, biometrics enrollment (iris and fingerprints), editing, deleting, and viewing voters, as well as registering voters. During registration, each voter must provide biographical information as well as register their fingerprint. After clicking the add voting button, the registration page appears, followed by the view/edit ballot page, which displays a list of registered voters, and then clicking on each registered ballot provides editing space. After completing registration and providing identification, the user is directed to the voting page, where they can choose a candidate from a drop-

down menu and cast their vote by pressing the vote button. The user is notified whenever a successful vote is cast.

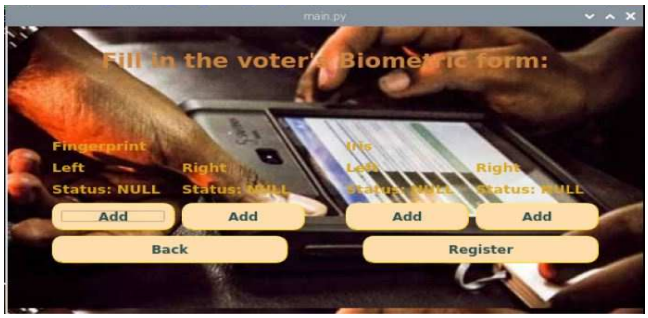

Fig. 4. Voter Biometric Page

The False Accept Rate, False Reject Rate, accuracy, and response time of the designed system were all used to assess its performance. The purpose of FAR is to check how well the system keeps unregistered users out of or correctly invalidates them, whereas FRR is used to see how well the system authenticates registered system users correctly. The accuracy of a measurement refers to how near it is to a specific value. It is taken into account the accuracy of fingerprint and iris recognition.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \times 100 \quad (1)$$

Where TP stands for true positive, TN for true negative, FP for false positive, and FN for false negative. When repeating a measurement, precision refers to how near the results are to each other.

$$\Pr ecision = \frac{TP}{TP + FP} \quad (2)$$

The throughput of a device is the quantity of data it can handle in a given length of time. The system's relevant efficiency measures include the speed with which such workloads may be completed and the time it takes to react, as well as the time required for a single interactive user request and response acceptance. False acceptance is the calculation of two different fingers that allows an unauthorized user to accept access.

$$\%FAR = \frac{FA}{N} \times 100 \quad (3)$$

Where percent FAR is for false acceptance rate percentage, FA stands for false acceptance rate number, and N stands for number of identification attempts. Rejection that is not true. When the device rejects a user whose fingerprint data has been stored with approved privileges, this error occurs.

$$\%FRR = \frac{FR}{N} \times 100 \quad (4)$$

In which case, percent FRR stands for false rejection rate percentage, FR stands for false rejection rate number, and N stands for number of identification attempts. There was a total of 15 unregistered fingerprints found on the device. Table 1 shows that a single fingerprint was incorrectly accepted from the total, giving the device a FAR of 2.22 percent. Unregistered and ineligible voters are excluded from the scheme. This quality ensures the dignity of the democratic process as well as the accuracy of the election results. Tables 2 and 3 show the results of twenty different registered users checking the device ten times each to determine the FRR. The worst result for a user was two incorrect rejections, while the greatest result was no rejection for a registered user. The FRR is ten percent in total. The most prevalent cause of erroneous rejection was discovered to be incorrect/incorrect finger location on the sensor. The appropriate location of the finger on the sensor may primarily confirm the recorded fingerprint.

The system response time is the time interval between the user's actions, the system's input, and the system's response to the input. It is concerned with the observed delay during system operation. Table 4 shows the system's measured response time for various scenarios. The degree of similarity between a measured value and its real or actual value is called accuracy. The fingerprint verification scheme has been determined to be accurate for both the verification of registered fingerprints and the invalidation of unregistered fingerprints. The results for system reaction time for fingerprint, iris, and accuracy of the system are presented in Tables 5 and 6.

Voting, voter registration, and verification all had response times of 0.3, 3, and 9 seconds, respectively. Voting verification takes longer than enrolling because there are too many processes between the bi-factor biometrics processes. Voting, voter registration, and verification have response times of 10, 15, and 20 minutes, respectively. The iris response time for voter identification is substantially longer than the fingerprint response time since the iris goes through additional processes. Before any voter can be recruited or checked, picture extraction, image localization, image segmentation, and pattern matching must all be completed. The overall system accuracy was 94 percent.

TABLE I. FAR FOR THE DEVELOPED SYSTEM

Matching Tries	Accepted	Rejected	FAR%
15	1	14	2

TABLE II. FALSE REJECTION RATE FOR THE DEVELOPED SYSTEM

Matching Attempts	False Rejection	FRR	FRR	True Acceptance Rate
10	1	0.1	10.0	90.0
10	2	0.2	20.0	80.0
10	1	0.1	10.0	90.0
10	1	0.1	10.0	90.0
10	2	0.2	20.0	80.0

978-1-6654-7978-3/22/$31.00 ©2022 IEEE

TABLE III. SYSTEM RESPONSE TIME FOR FINGERPRINTS VERIFICATION

Action	Response Time (s)
Voting	0.6
Voter's enrolment	3
Voter's verification	9

TABLE IV. SYSTEM RESPONSE FOR FINGERPRINT AND IRIS

ACTION	RESPONSE TIME (S) IRIS	RESPONSE TIME (S) FINGERPRINTS
Voting	10	0.6
Voters Enrolment	15	3
Voters Verification	20	9

TABLE V. ACCURACY OF THE FINGERPRINT AND IRIS VERIFICATION SYSTEM

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

V. CONCLUSION

The INEC employed a partial e-voting system with the use of a card reader for voter identification and verification in the 2015 and 2019 general elections in preparation for a full e-voting system in the 2023 general election. This good proposal, however, was marred by a failure in fingerprint identification and authentication, which prevented a considerable number of voters from voting. There was a false match the majority of the time. This is due to the continual shifting of the skin of the finger as a result of the vast majority of voters in this category's farming and tiresome work. This paper proposes a bi-factor biometric authentication approach for use in the voting system to address these issues. An accuracy of 94 percent was obtained as a result of the results. The Iris response time for voter enrolment and verification is 15s and 20s, respectively, while the fingerprint response time is 3s and 9s, respectively. Using one of two biometric methods will speed up the process of voter identification and authentication, reduce voting fraud, reduce voter disenfranchisement as a result of not being recognized by the card reader, reduce voting time, eliminate the manual voting system, and eliminate the use of incident forms, all of which encourage election rigging, resulting in a more robust, reliable, and efficient electronic voting system.

.

REFERENCES

[1] N. B. K. A. M. I. Z, "A Secure E-Voting System Using Biometric Fingerprint and Crypt-Watermark Methodology," *Paper presented at the International Conference Proceedings – Information Systems and Engineering,* 2018.

[2] B. A. Oke, O. Mikail, A. Aboaba, and A. Diran, "Securing electronic voting system using crystographic technique," *ATBU Journal of Science, Technology and Education,* vol. 7, no. 1, pp. 88-105, 2019.

[3] M. Alhasnawi and A. Alkhalid, "Secure online voting using steganography and biometrics," *International Journal of Current Engineering and Technology,* vol. 7, no. 3, pp. 1097-1104, 2017.

[4] C. S. P. N. Narayanan, Piyush Gulati, G. Raj Bharath, S.Nivash "Design of Highly Secured Biometric Voting System.," *International Journal of Engineering and Advanced Technology (IJEAT),* vol. 8, no. (5S3), pp. 111-114, 2019.

[5] M. Wagner, D. Johann, and S. Kritzinger, "Voting at 16: Turnout and the quality of vote choice," *Electoral studies,* vol. 31, no. 2, pp. 372-383, 2012.

[6] B. Umar, O. Olaniyi, L. Ajao, D. Maliki, and I. Okeke, "Development of A Fingerprint Biometric Authentication System for Secure Electronic Voting Machines," *Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, and Control,* pp. 115-126, 2019.

[7] B. M. Haque, G. O. Ahmed, D. Sukruthi, K. V. G. Achary, and C. M. Naidu, "Fingerprint and RFID Based Electronic Voting System Linked with Aadhar for Rigging Free Election," *International Journal of Advance Research in Electrical, Electroinc and Instrumentation Engineering,* 2016.

[8] H. Hussien and H. Aboelnaga, "Design of a secured e-voting system," in *2013 International Conference on Computer Applications Technology (ICCAT)*, 2013, pp. 1-5: IEEE.

[9] D. Petcu and D. A. Stoichescu, "A hybrid mobile biometric-based e-voting system," in *2015 9th International Symposium on Advanced Topics in Electrical Engineering (ATEE)*, 2015, pp. 37-42: IEEE.

[10] O. A. Numbering, "Development of Antirigging Voting System Using Biometrics Based," 2015.

[11] F. I. Hazzaa, S. Kadry, and O. K. Zein, "Web-Based Voting System Using Fingerprint: Design and Implementation," *International Journal of Computer Applications in Engineering Sciences ISSN,* pp. 2231-4946, 2012.

[12] M. P. Ranjan, A. A. Badoni, S. Bahukhandi, and N. Saini, "Design of RFID based Electronic Voting Machine," 2015.

[13] P. K. Saravanan.N, Nandhini.C "Iris Based E-Voting System Using Aadhar Database. ," *International Journal of Scientific & Engineering Research,* vol. 8, no. 4, pp. 62-64, 2017.

[14] P. Tamilarasu, S. Aadhithyan, K. Gowthaman, and V. Hariprakash, "Fingerprint based electronic voting machine," *International Journal of Current Engineering and Scientific Research (IJCESR),* vol. 5, no. 2, pp. 67-70, 2018.

[15] K. J. K.Krisheswari, P.Kannan "Smart Voting System Using Android," *International Journal for Research Trends and Innovation,* vol. 3, no. 5, pp. 210-215.

[16] P. R. Pashine, D. P. Ninave, M. R. Kelapure, S. L. Raut, R. S. Rangari, and K. O. Hajari, "A Remotely Secure E-Voting and Social Governance System Using Android Platform," *International Journal of Engineering Trends and Technology (IJETT)–Volume,* vol. 9, 2014.

[17] D. G. Nair, V. Binu, and G. S. Kumar, "An improved e-voting scheme using secret sharing based secure multi-party computation," *arXiv preprint arXiv:1502.07469,* 2015.

[18] G. R. Nadar Rajkani Paulraj, M.Rajesh, S.V.Kiruthika, I.Jasmine " Smart Voting Machine Based on Finger Prints and Face Recognition," *International Journal of Engineering Research & Technology (IJERT),* vol. 5, no. 9, pp. 1-4, 2017.

978-1-6654-7978-3/22/$31.00 ©2022 IEEE