RASPBERRY PI VOTING MACHINE USING GUI PYTHON

[1]Author: Vegesna Ananda Sita Raghu Rama Teja, M. Tech Scholar, Department Of Computer Science & Engineering, Vishnu Institute Of Technology, Bhimavaram, India

[2]Author: B CH S N L S Sai Baba, Assistant Professor, Department Of Computer Science &Engineering, Vishnu Institute Of Technology, Bhimavaram, India

Abstract: To ensure that everyone is able to exercise their right to vote, the "Vote from Anywhere" system employs cutting-edge technology. The voter enters their Aadhaar number onto a display linked to a Raspberry Pi. The voter is next required to scan his fingerprints, which are checked with those already stored in the Aadhaar database. Before an election, the administrator may log in with their user id and password to the online portal and add candidate information. The admin has the ability to modify and remove the candidates' data. Furthermore, we have implemented encryption methods to ensure that voting is conducted in a safe environment. So, in order to prevent people from voting for the same candidate more than once, the system receives a request to deactivate the user and an encrypted vote tally from each voter before sending both to a centralized database.

I. INTRODUCTION

A nation's democracy rests on the votes its citizens cast for its leaders. Despite its high level of security, this system has a number of problems, most of which arise during the lengthy verification procedure. Though there may be ways for political parties to intervene and for people to make mistakes, the situation currently has no optimal answers. The country might fall into the wrong hands if this issue is not resolved. This article presents a way for avoiding the need for extra security personnel and human resources throughout the verification process. Voting has evolved over the ages, using a variety of systems and procedures. After elections have been held, the results should be announced in a fashion that is acceptable to all parties involved, including those running for office and those casting ballots. Cultural values and political agendas shape the atmosphere of voting and election administration.

II. LITERATURE REVIEW

A. Voting using Iris Recognition Technology After capturing a photograph of an individual's eye, the iris may be identified by comparing it to previously acquired photos using an image processing method. When the voter's Aadhar information is verified, the system verifies that the voter is a qualified elector. The voter's eligibility to vote will be verified before the ballot is cast. Voters' blood groups may be readily examined thanks to the current Aadhar database, which has all the information about their Iris, fingerprints, and other characteristics like address. This method is both cost-effective and safe.

B: A Biometric Voting Machine. Fingerprints may be scanned into a database and stored using a sensor. The microcontroller's serial connection will be used to communicate with the web app when the biometric image has been read. If the voter's picture matches one already stored in the database or on the server, a confirmation message is sent to the voter's device and shown on the LCD. If there is no Matching, the same message as "Not Eligible" is shown on the LCD.

C. Intelligent Voting People above the age of 18 will have their information pulled from the Aadhar database. Voters will get their unique ID and password through the email address they used to register to vote in the first phase. In the second step, fingerprint data is used to verify the voter's identity before he or she is granted voting privileges. In the last step, the voter id is removed so that the voter cannot cast a second ballot. The voter's Aadhar number and other identifying information would be stored in a protected database for future use. There will be no lag in between the count updates.

D. A Trusted Blockchain-based Lottery Voting System. Voting data is recorded on the client and saved to the server. When casting a ballot, voters will be granted access to the website where their name and address will be recorded, as well as their assigned voting lot. A sensor captures a picture of the fingerprint, and that image is then cross-referenced against a database of fingerprints. Vote only if all voter information is correct. Voting data is captured and kept in blocks, or blocks of voting, for each voter.

E. CNN-based Multimodal Biometrics using face, iris, and palmprint photos all safely stored is the cutting-edge approach of multimodal biometrics. The use of Convolutional Neural Networks for picture feature extraction. Using CNN for multimodal Biometrics is a dated approach at best. Comparing the incoming picture to images already stored in a database, convolutional neural networks (CNNs) are used. Fingerprint image matching is another task that CNN does. The latest iteration of CNN makes use of two-layer fusions.

III.EXISTING SYSTEM

The verification procedure may be carried out in a number of ways. Biometric verification offers the highest level of safety compared to other methods. Unfortunately, none of these biometrics are utilized by the current systems. There is no way to guarantee safety with these methods. Furthermore, these strategies have not been properly adopted.

IV PROPOSED SYSTEM

Candidates and voters would both be able to register and verify their identities with the use of a centralised database and a web-based voting platform. The Elections Commission is responsible for the Admin Login. To manage the Candidate Login Voters will be assigned a different ID and password for each candidate they choose to support, allowing them to vote for each candidate just once every Election. The Elections Commission, the Voters (who will be better informed to make informed choices), and the Candidates themselves will all benefit from this endeavour. Candidates may update their profiles in the programme with new information and uploaded documents, such as their most recent milestone. The administrator has the ability to review all Candidate information and documents, and only after successful verification will a Candidate ID and Password be produced. Candidates running for office in a certain region may be seen by Voters through the system's centralised database. The administrator has complete control of the platform and may alter or remove any information that is not directly related to the Election Rules.

The election mode, candidates, voting gui application, and viewing of results may all be set up using the implemented gui application.

The programme is written in Python and has a graphical user interface (GUI) in front of it; it communicates with a Raspberry Pi and a biometric device to ensure that a certain voter is registered in their zone and then lets them cast a ballot by choosing their preferred political party.

V. RASPBERRY PI 3

Model B of the Raspberry Pi 3 is the most basic version of the third-generation device. This device has a 64-bit, 1.2-gigahertz Broadcom BCM2837 processor. It contains a CSI camera connector and four USB 2 ports, making it ideal for use with a Raspberry Pi camera. There is a micro-SD card slot for installing software and transferring files. With these capabilities, the Raspberry Pi 3 may serve as an effective controller. This controller is used for image processing, which requires very high resolution. This processor can also communicate with the ATMEGA 329p. Pi also allows for far faster capture and verification of the acquired picture than is possible with other CPUs. Pi may function as a conventional computer. Pi uses the Python programming language.

5.1FINGER PRINT SENSOR

In this Endeavor, the R305 fingerprint scanner module was implemented. The fingerprint may be taken, stored, and eventually matched against a database, all with the help of this equipment. The module connects to the Raspberry pi through two of its four external connections. The other two wires provide the biassing voltage and ground. As a secondary verification method, we employ a fingerprint sensor. The third and final mode of authentication, facial recognition, is performed only after fingerprint verification has been completed.
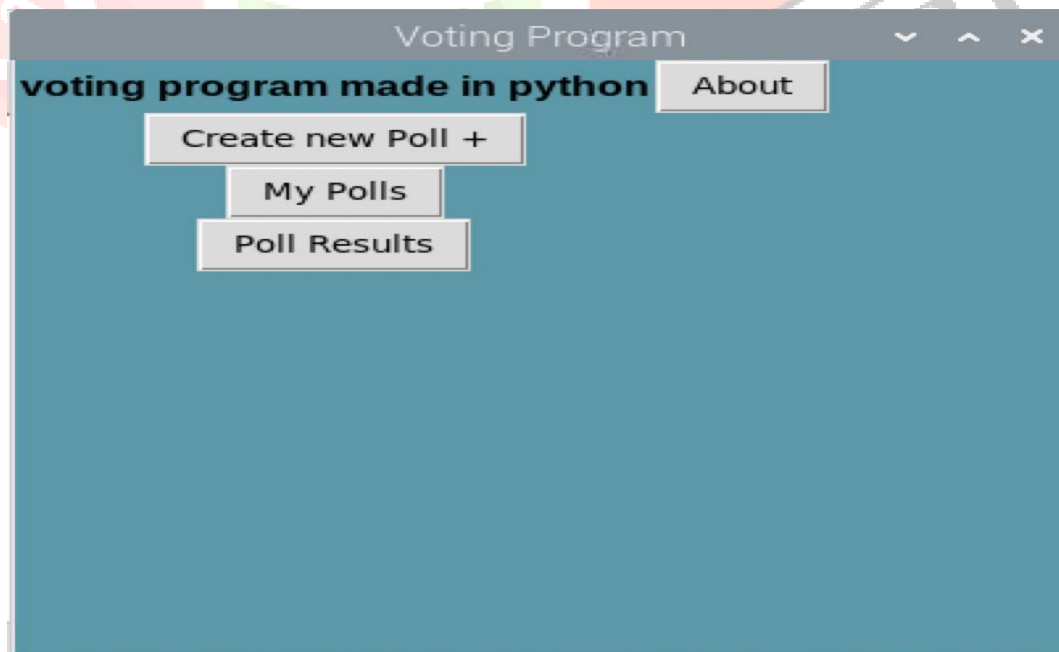
VI.RESULTS
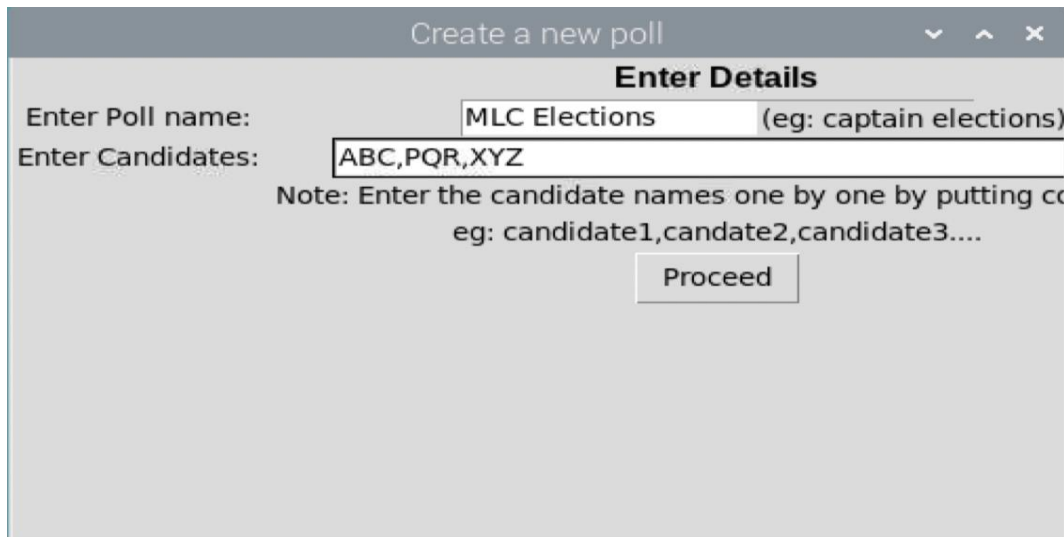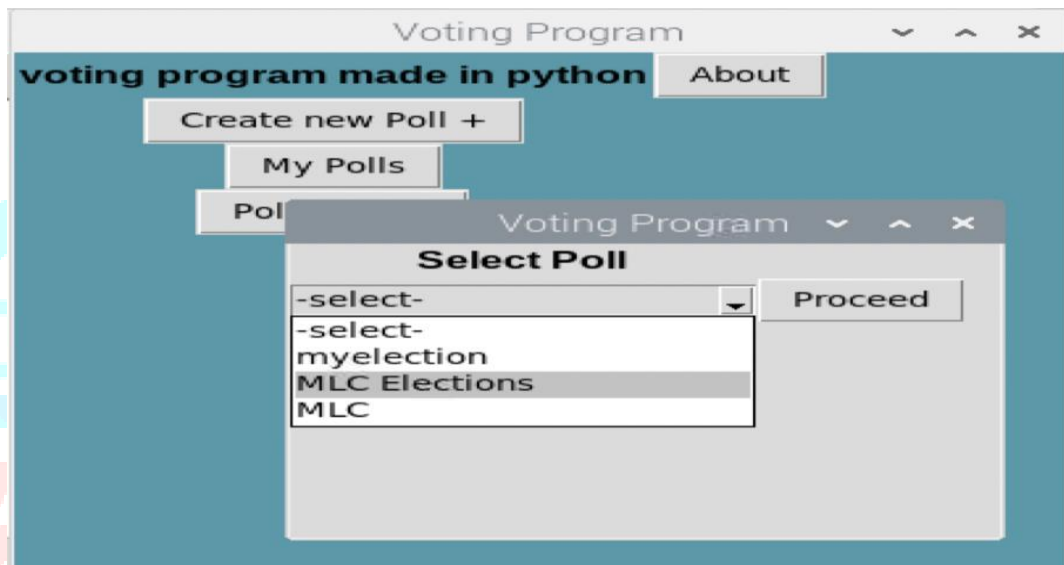

Fig.1:Project Home Screen

Fig.2:Creating new Poll
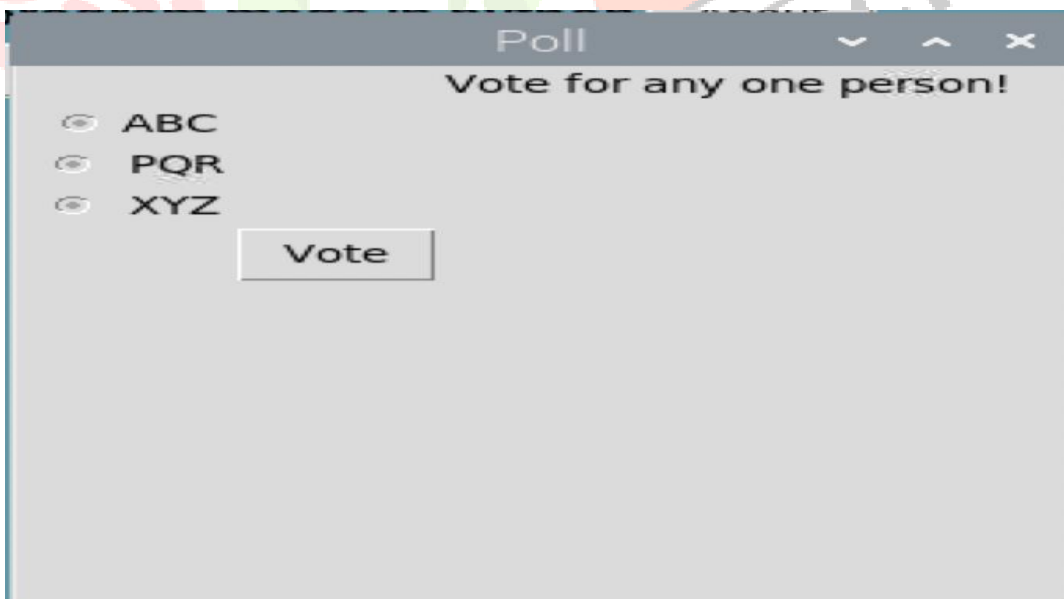

Fig.3: Voter selecting Poll

Fig.4: List of Candidates to Vote
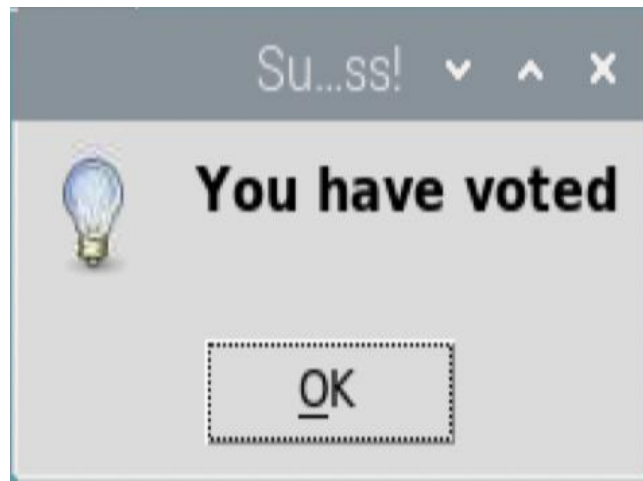
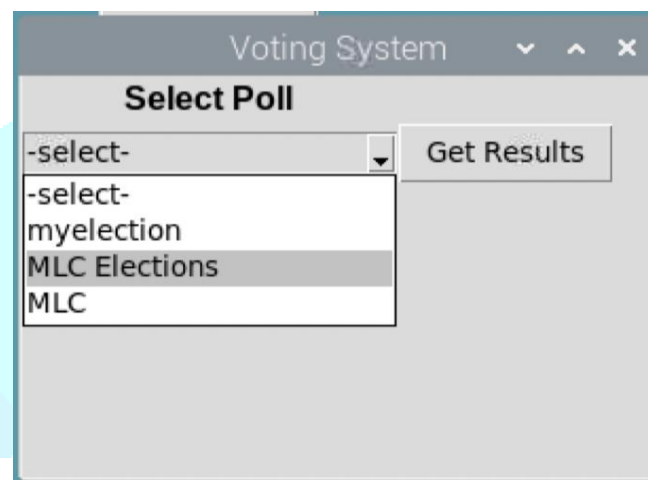**Fig.5: Conformation message after voting**

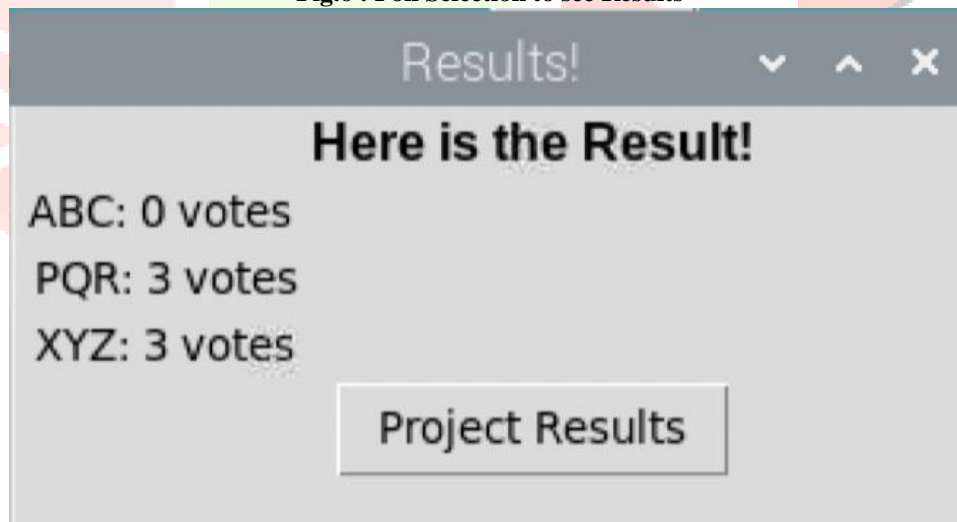**Fig.6 : Poll Selection to see Results**

Fig.7: Showing Results

CONCLUSIONS

A safe voting system based on biometrics is offered as a means of addressing the many problems with the existing voting system. There are a lot of great things about the suggested system. There is no need for a poll worker, paper ballots, or electronic voting machines with this approach; all that is needed is a way to authenticate the voter's identity online and provide them access to the voting machine. Every voter's voting pattern will be linked to their Card, preventing them from casting a ballot more than once. cause a database storage problem since the two finger patterns don't match. The criteria for democracy, privacy, anonymity, dependability, correctness, and usability are all met by this paradigm. This concept has promise for energizing voters across all age groups.

REFERENCES

[1] Samarth Agarwal, Afreen Haider, "Biometrics Based Secured Remote Electronic Voting System". IEEE Conference, Sep 2020.

[2] P.M.Benson Mansingh, T. Joby Titus, "Biometric voting system using RFID Linked with the Aadhar database" IEEE Journal, august 2020.

[3] S Jehovah Jireh Arputhamoni,Gnana Saravanan "Online Smart Voting System Using Biometrics Based Facial and Fingerprint Detection Image Processing "IEEE Conference,May 2021.

[4] Suresh Kumar, Tamil Selvan G M, "Block chain Based Secure Voting System Using Lot", IEEE Journal, Jan 2020.

[5] Hanzhuo Tan, Ajay Kumar, "Towards More Accurate Contactless Fingerprint Minutiae Extraction and Pose-Invariant Matching" IEEE Conference 2020.

[6] Chandra KeerthiPothina, AtlaInduReddy"Smart Voting System using Facial Detection"IEEE Journal, April 2020.

[7] Chengsheng, Yuan, Zhihua, Xia, "Fingerprint Liveness Detection using an improved CNN with image Scale Equalization" IEEE   Journal 2019.

[8] Anurag Chowdhury, Simon Kirchgasser, Andreas Uhl, Arun Ross "CNN Automatically Learn the Significance Of Minutiae Points for Fingerprint Matching?"IEEE Conference, Mar 2020