Scientific Journal of Impact Factor (SJIF): 5.71

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 5, Issue 05, May -2018

DESIGN AND DEVELOPMENT OF SECURITY BASED VOTING SYSTEM FOR GOVERNMENT USING RASPBERRY PI

Prashantha N.C[1], Arpitha Y.C[2], Preethi raj B.K[3] , Ranjitha Dharmaraju[4] , Vinutha.T[5]

[1]*Assistant Professor, Department of ECE, BGSIT, Mandya.*
[2]*Student, Department of ECE, BGSIT, Mandya.*
[3]*Student Department of ECE, BGSIT ,Mandya.*
[4]*Student Department of ECE, BGSIT , Mandya.*
[5]*Student Department of ECE, BGSIT , Mandya.*

Abstract- *Voting process takes the significant part of democratic systems. In most of the developing countries, paper ballot method is still being used. Information technology also has offered significant advantages and facilities to improve the quality of voting process. Digital recording electronic systems are developed replacing paper ballots. Although this is a great advancement, this process is prone to tampering threats and electoral frauds. This paper presents a new voting process which makes use of Raspberry Pi which has improved reliability and transparency over currently used systems. This system employs biometric identifiers in pursuit of authenticity. Pre collected Details of all the voters in the country will be maintained as a central database by the government. This data is rechecked at the time of voting to ensure the identity of voters. Usage of Raspberry Pi for web casting the complete voting process and time to time display of polling percentage etc., details will tremendously affect the reliability of the process. Transparency and minimum usage of personnel is achieved at a cheaper cost and simpler process with this Raspberry Pi and its peripherals. The aim of this study is to design a secured electronic voting system using multimodal biometrics.*

Keywords- *digital recording, biometric identifiers, web casting.*

I. INTRODUCTION

Elections are a transformative tool for democratic governance. They are the means through which people voice their preferences and choose their representatives. Elections are unique. They change the fate of nations, influence participation and activism in politics, and deeply affect the lives and attitudes of citizens. Society deems the voting process so important that it must be 100percent reliable. Each vote is part of a larger process that stretches before, during and after an election: the Electoral Cycle. At present in most of the countries, election processes comprises of paper ballot system/digital recording electronic systems/even online voting system. Raspberry Pi is a credit card sized single board Computer. This board is cost effective when compared to an actual computer. This board uses power rating of 5V, 700m Aand it weighs not more than 50g. This board is like a computer in your pocket. This board contains many features like camera connector, Ethernet port, GPIO pins for interfacing sensors and switches, USB ports to connect to external devices(like keyboard, mouse, Wi-Fi adapter etc.,), HDMI port to interface to monitors (like LCD screens, projectors, TVs etc.) And an audio jack also available.

Biometrics is our most unique physical (and behavioural) features that can be practically sensed by Devices and interpreted by computers so that they may be used as proxies of our physical selves in the digital realm. Physical attributes may include face, fingerprints hand geometry, handwriting, iris, retina, and voice. Biometrics plays crucial role in today's security systems. Possession based (e.g.ID card) and knowledge-based (e.g. password) authentication methods can be easily misplaced, forgotten or easily copied whereas physiological biometrics cannot be manipulated. Biometric authentication is very convenient for user as this is very simple to use. Python is one of the most popular languages in the world and has been around for more than two decades. It is heavily used in academic environments and is a widely supported platform in modern applications, especially utilities, and desktop and Web applications.

II LITERATURE SURVEY

Paper-based Voting Systems (PVS) record, count, and produce a tabulation of the vote count from votes that are cast on paper cards or sheets. Some PVSs may allow voters to make selections by means of electronic input devices. Voter selections are, however, not independently recorded, stored or tabulated by such input devices.

Direct-recording Electronic (DRE) voting systems record votes by means of a ballot display provided with mechanical or electronic optical components which could be activated by the voter. Such systems record voting data and ballot images in computer memory components. Also, data processing is achieved by the use of computer programs.

Public network DRE voting systems (PNDRE: Make use of electronic ballots and transmit vote data from the polling stations to other locations over a public network. The votes may be transmitted as individual ballots as they are cast, or periodically as batches of ballots, or as one single batch, at the end of voting.

Precinct count voting systems (PCVS) put the ballots in a tabular form at a particular place, say, a polling station.

They provide mechanisms that store vote count electronically and transmit the results to a central location over public telecommunication networks.

Central count voting systems (CCVS) Tabulate ballots from multiple precincts at a central location. Voted ballots are safely stored temporarily at the polling station. These ballots are then transported or transmitted to a central counting location. CCVSs may, in some cases, produce printed reports on the vote count.

III. PROPOSED SYSTEM

In our proposed system, we used finger print biometric for authentication purpose. Here is the brief description of how this biometric process works. First stage is the enrolment process in which biometrics (e.g. fingerprints) of the voters are collected and archived to generate templates for future comparisons. Here quality biometric samples from voters are recorded and archived. By using template extraction techniques biometric template is created and stored in database for future comparisons. This enrolment process has to be done before the elections are commenced. Second stage is matching/ Searching stage. In this stage, during times of authentication check person fingerprints are again captured and template is created. This biometric template is compared with the template database for matching. If the template matches with any of the template in the database, it gives a result “match”. Otherwise, gives a result “no match”. Result “match” implies the person is valid and can be allowed to next stage. “No match” implies person is not authorized / allowed.

Figure 1-Raspberry pi model

Biometrics is our most unique physical (and behavioural) features that can be practically sensed by devices and interpreted by computers so that they may be used as proxies of our physical selves in the digital realm. In this way we can bond digital data to our identity with permanency, consistency, unambiguity and retrieve that data using computers in a rapid and automated fashion. Physical attributes may include face, fingerprints, hand geometry, handwriting, iris, retina, and voice. Biometrics plays crucial role in today’s security systems. Possession based (e.g.ID card) and knowledge-based (e.g. password) authentication methods can be easily misplaced, forgotten or easily copied whereas physiological biometrics cannot be manipulated. Biometrics authentication is very convenient for user as this is very simple to use. Implementation and maintenance of biometric systems is also cost-effective and more secure process from business point of view.

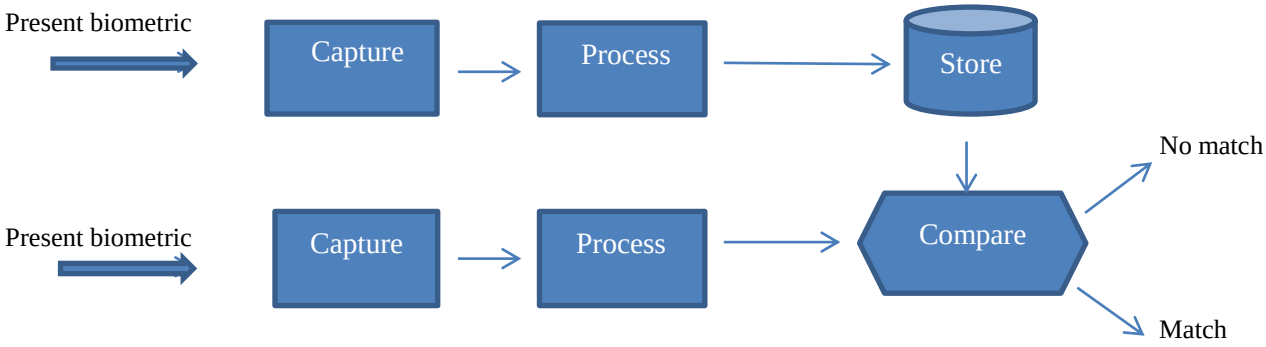

Figure 2: Biometric Details Enrolment and Comparison Process

In our proposed system, we used finger print biometric for authentication purpose. Here is the brief description of how this biometric process works. First stage is the enrolment process in which biometrics (e.g. fingerprints) of the voters are collected and archived to generate templates for future comparisons.
Here quality biometric samples from voters are recorded and archived. By using template extraction techniques biometric template is created and stored in database for future comparisons. This enrolment process has to be done before the elections are commenced. Second stage is matching/ Searching stage. In this stage during times of authentication check person fingerprints are again captured and template is created. This biometric template is compared with the template database for matching. If the template matches with any of the template in the database, it gives a result "match". Otherwise, gives a result "no match". Result "match" implies the person is valid and can be allowed to next stage. "No match" implies person is not authorized / allowed.
The election process follows some steps beginning with biometric authentication of voter till the voter casting his/her vote. This process is explained as an algorithm below:

1. The process of election initializes with biometric system. When the voter enters the polling booth he/she will be asked for biometric authentication which is fingerprint type here.

2. Immediately after taking the template fingerprint from the voter using fingerprint machine, it is processed and sent to a database that is maintained by government.

3. The database maintained by government comprises of list of voters, corresponding voter details regarding polling and their fingerprint data. For the sake of security issues, this database is not distributed and is very confidential.

4. There it checks for a match and if the fingerprint match is not found in the database that may be because of any error, the voter will be provided an alternative method. If the match is found, the database returns a unique ID of the voter corresponding to that fingerprint.

5. The value will be returned to the database that is maintained in local polling booth. This database which is stored in Raspberry Pi device consists two tables, one with electoral list named as ELECTORAL DATABASE and the other with the list of names who already casted their votes named as CASTED DATABASE.

6. Raspberry Pi itself after taking the value from the central database will search for the unique ID in the electoral database. Search will tell whether the ID is found in the electoral database or not.
7. If found in database, the voter name with their details will be displayed on the monitor and he/she will be allowed to cast their vote. This will complete the voting process.

8. There occurs two occasions when the match is not found. One may be due to voter already voted and other may be due to the voter belonging to other polling station.

9. Considering the situation, the casted table is searched for the voter's ID. And if the ID is found in the casted table, it implies that the voter had already casted his/her vote. The voter is a fraud.

10. The voter's ID if not found in any of the tables i.e. in electoral table and casted table, then a request to find the identification of the voter will be sent to district database.

11. Finally it will return the details of the voter to which polling station he/she belongs to. This completes the voting process of a single person.

12. If it could not return any match, it indicates that the particular voter is not eligible to vote and controller refuses his identity.

13. Same process is applicable to all other voters who are willing to cast their vote.

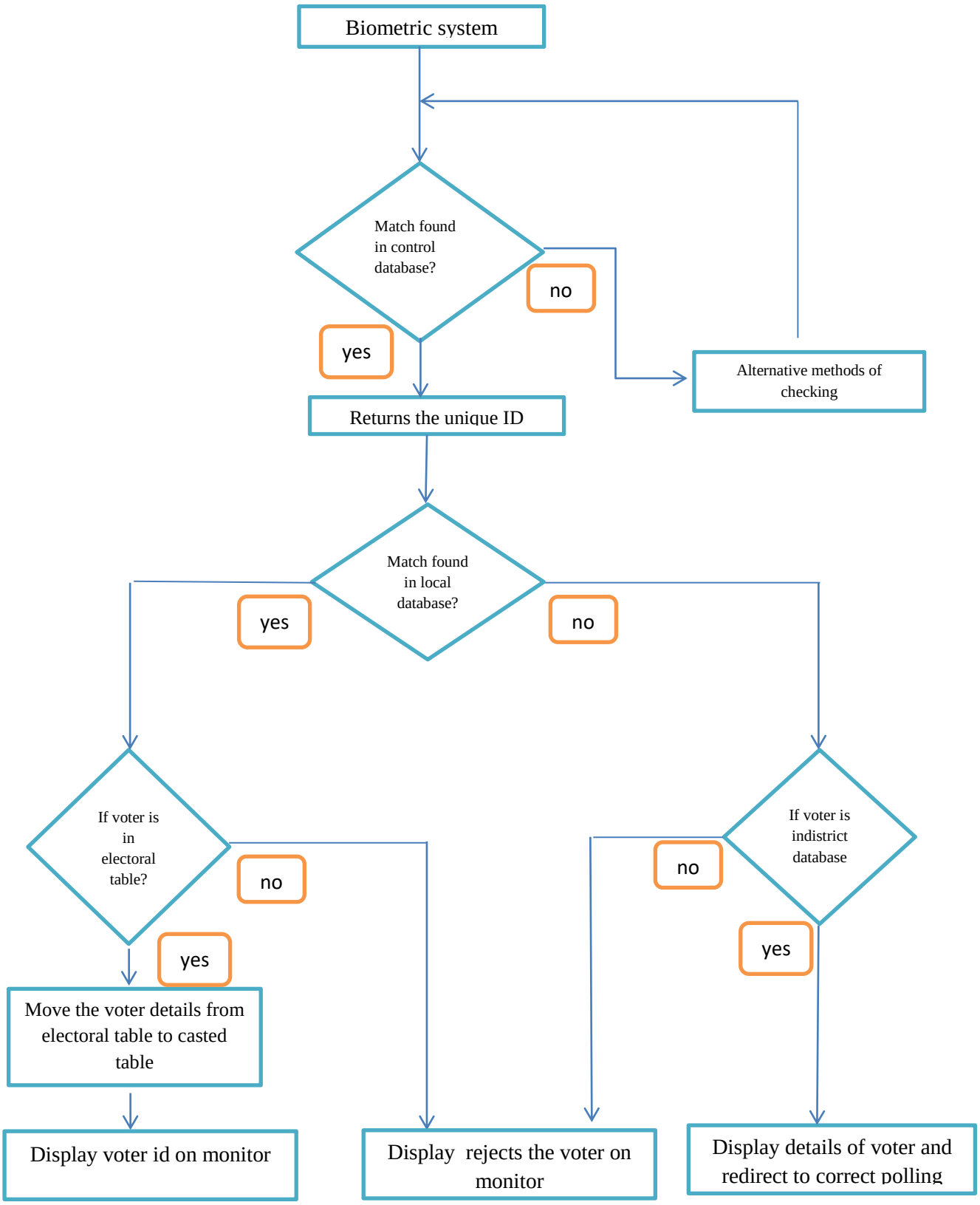

Figure 3: Raspberry Pi System Voting Design

IV. RESULT

The Raspberry Pi Voting System is designed with a motto improves reliability, efficiency and transparency in election process. Considering the problems of already existing system, this system is developed in such a way to overcome them. With the implementation of this system in election process, surprising results can be obtained. It follows a simple procedure, consumes minimal man power, can save a lot of time, less prone to frauds and manipulations compared to already existing systems. We aimed at extending this system to an advanced model in future in such a way to maximize the polling percentage. The people who work in distant places from home towns are the ones who may not use their right to vote. If these people cast their vote that can drastically change the result. We thought of designing this system so that any voter can utilize his/her vote from any workplace.

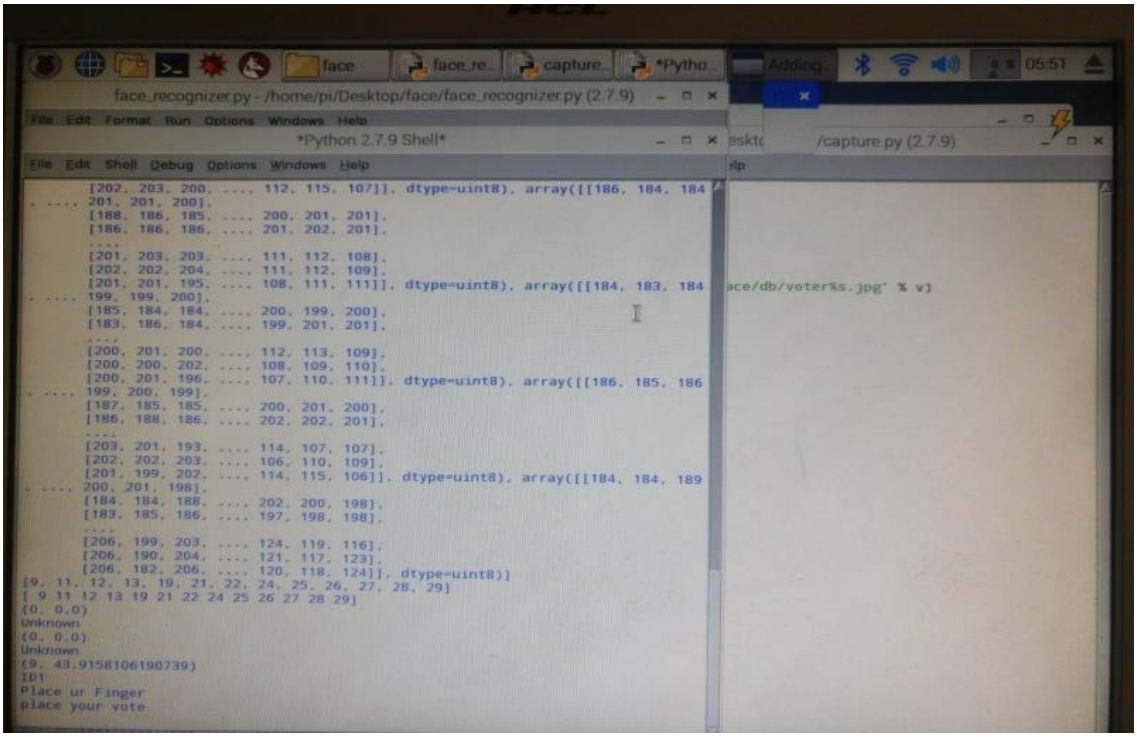

Figure 4: Voting commands of the program

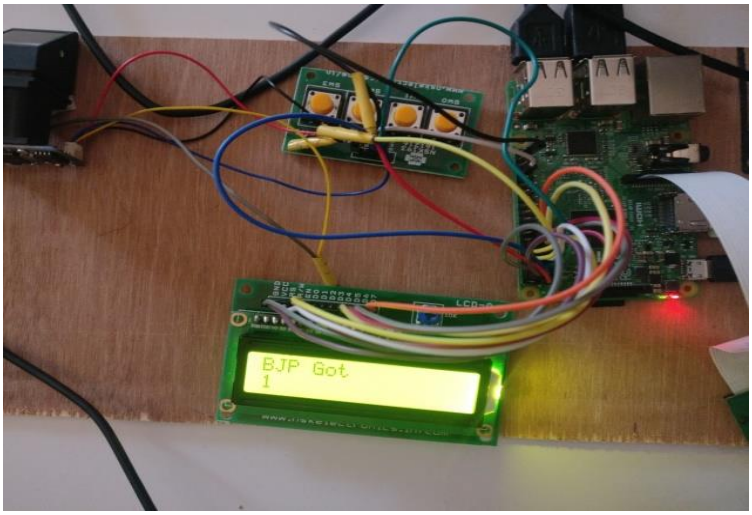

Figure 5: Proposed Voting system

V. CONCLUSION

For over a century, fingerprints have been one of the most highly used methods for human recognition; automated biometric systems have only been available in recent years. This work is successfully implemented and evaluated. The arrived results were significant and more comparable. It proves the fact that the fingerprint image enhancement step will certainly improve the verification performance of the fingerprint based recognition system. Because fingerprints have a

generally broad acceptance with the general public, law enforcement and the forensic science community, they will continue to be used with many governments,, legacy systems and will be utilized in new systems for evolving applications that require a reliable biometric. Thus the advent of this biometric voting system would enable hosting of fair elections in India. This will preclude the illegal practices like rigging. The citizens can be sure that they alone can choose their leaders, thus exercising their right in the democracy.

VI. REFERENCES

[1] Chaum D., "Secret-ballot receipts: True voter-verifiable elections", IEEE Security and Privacy, 2(1):38-47, 2004.J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.

[2] Ashok Kumar D., Ummal Sariba Begum T., "A Novel design of Electronic Voting System Using Fingerprint", International Journal of Innovative Technology & Creative Engineering (ISSN:2045- 8711),Vol.1,No.1. pp: 12 19, January 2011. R. Nicole, "Title of paper with only first word capitalized," J. Name Stand. Abbrev., in press.

[3] Tigran Antonyan, Seda Davtyan, Sotirios Kentros, Aggelos Kiayias, Laurent Michel, Nicolas Nicolaou, Alexander Russell, and Alexander A. Shvartsman, "State-Wide Elections, Optical Scan Voting Systems, and the Pursuit of Integrity", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, Vol.4, NO.4, pp. 597-610, December, 2009

[4] Ye Wang, Member, IEEE, Shantanu Rane, Member, IEEE, Stark C. Draper, Member, IEEE, and Prakash Ishwar, Senior Member, IEEE, "A Theoretical Analysis of Authentication, Privacy and Reusability Across Secure Biometric Systems", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 7, NO. 6, pp: 1825 1840 DECEMBER 2012.

[5] J. Bannet, D. W. Price, A. Rudys, J. Singer, and D. S. Wallach, "Hack-avote: Security issues with electronic voting systems," IEEE Security Privacy, vol. 2, no. 1, pp. 32–37, Jan./Feb. 2004.

[6] P. S. Herrnson, R. G. Niemi, M. J. Hanmer, and B. B. Bederson, "Voting Technology: The Not-So-Simple Act of Casting a Ballot. Washington", DC: Brookings Institution Press, 2008, ISBN 0-8157-3563-4.

[7] Gareth Mitchell, The Raspberry Pi single-board computer will revolutionize computer science teaching [For & Against], Vol.7, NO.3, pp. 26, 2012.

