2016 IEEE International Conference on Advances in Electronics, Communication and Computer Technology (ICAECCT)
Rajarshi Shahu College of Engineering, Pune India. Dec 2-3, 2016

Raspberry Pi Voting System, A Reliable Technology for Transparency in Democracy

Patchava Vamsikrishna[#1], Sonti Dinesh Kumar[#2], Dinesh Bommisetty[#3], Akshat Tyagi[*4]
[#] Department of Electronics & Communication Engineering, RGUKT-Nuzvid, Andhra Pradesh, India
*Department of Computer Science & Engineering, Amity School of Engineering and Technology, Noida, India

[1]vamsi.patchava@gmail.com, [2]dineshkumar.sonti@gmail.com,
[3]dinesh.bommisetty@gmail.com, [4]akshat95tyagi@gmail.com

***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.**

***Index Terms*—Elections, Voting systems, Raspberry Pi, Biometric, Paper ballot, Electronic systems, finger prints, webcasting**

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 100 percent 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.

A. Paper Ballot

Paper ballot [1], [6] is commonly used simple voting system. This is widely used before the introduction of Electronic recording systems. Still even after the introduction of electronic systems, in many countries this paper ballot system is being used because of its simplicity. In paper ballot system, every voter is given a paper ballot to cast his vote. Paper ballot is a piece of paper containing all the contestant names along with their symbols printed on it. Voter has to simple put a mark using stamp beside the choice of his/her contestant's name on the paper ballot. This is a very simple process and cost effective as well. But this process has the disadvantages as this is a very long and time-consuming process. Paper ballots are easily prone to fraud like manipulation of paper ballot / ballot tampering. Paper ballot counting is also another time consuming process which may cause delay to the election results.

B. Electronic Recording System (ERS)

Electronic recording systems [12], [13] are introduced to make the voting system more effective and simpler. In these electronic recording systems, voters can cast their vote using electronic ballot [2]. Unlike paper ballot which is easy to manipulate, this system uses electronic ballot to cast votes. This system is more convenient and a minimal time and skill is sufficient to finish the voting process. One of the significant benefits of new digital recording electronic system [11] is the possibility for increased efficiency over paper ballot system. Electronic voting has the advantages over paper ballet system such as ability to reduce fraud, by eliminating the opportunity for ballot tampering. One thing to consider is that the success of electronic voting rests directly in the ability of the Electronic Machines to function in the way it is required at that moment.

C. Problems of ERS Vulnerability to Hacking

"Vendors and election jurisdictions generally state that they do not transmit election results from precincts via the Internet, but they may transmit them via a direct modem connection. However, even this approach may be subject to attack via the Internet, especially if encryption and verification are not sufficient.'' –as quoted by 'Congressional Research Service'. The above quote is a major disadvantage to be taken into account. Physical security to machines has to be taken care which otherwise is waste of time and money using the machine for election process. Designing a malicious ERS itself is a fraud that outputs an incorrect result which is not expected.

D. Online Voting System

The online voting system [10] is the latest technology used in elections. It uses internet to cast the vote and transmit it. This system is impressive at the point that voters can cast their vote from anywhere in the world which improves the polling percentage. The main problem with this system is security issue [5], [22], [25]. As this uses the public internet to cast the vote and transmit, it is more prone to hacking vulnerability. Technological advancements that might make the voting process more efficient [20] or convenient could also chip away at that integrity, which requires a voting system that is available, secure, and verifiable. Considering all the advantages and difficulties [21], a new system is designed in such a way that its functions will give optimistic solutions to almost all the problems of present systems that are currently being raised. This paper is proposed considering most of the common issues happening in under developed and developing countries only. The proposed system in this paper can stand as a best approach to conduct elections in these not so developed countries which have limited and not so distributed sources. Our approach uses Raspberry Pi board which serves in many ways at a cheaper cost. Biometric process used in our system along with Raspberry Pi is briefed below:

E. Raspberry Pi

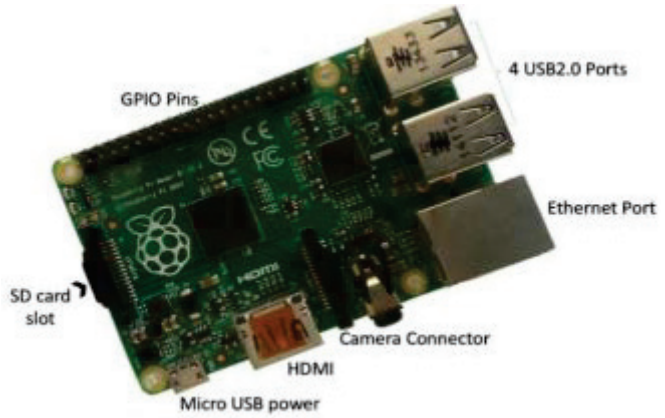

FIGURE 1.1: RASPBERRY PI BOARD

Raspberry Pi [7], [8], [9] 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, 700mA and it weighs not more than 50g. This board is like a computer in your pocket. This board being small in size gives advantages of ease in carrying, installation in any place. 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. By all these embedded on a single board, Raspberry Pi is not just limited to single use, it can be of wide use according to the application. Using Raspberry Pi multiple programs can be run at a time. Raspberry Pi board comes in three models A, B, B+. Raspberry Pi B+ model is used in this system. This model board comes with 512 MB RAM. It runs on ARM11 processor typically operates at 700MHz frequency. This model supports Linux based operating systems like Raspbian, Pidora, and Raspbmc etc. Latest model Raspberry Pi2 is released with 1GB RAM and it is going to support Windows10 operating system as well. With all these features, Raspberry Pi is not just limited to single use, it can be of wide use according to the application.

F. Biometric Process

"Biometrics are our most unique physical (and behavioral) 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." [24] Physical attributes may include face, fingerprints [2], [4], 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 [23] 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.

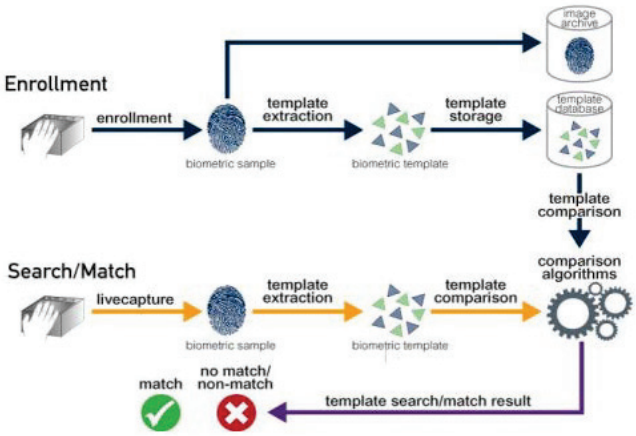

FIGURE 1.2: BIOMETRIC DETAILS ENROLMENT AND COMPARISON PROCESS [24]

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 rest of the paper is structured as follows. Section II explains the system design implementation. Section III deals with the algorithm of the program. Section IV shows the results. Section V discusses the challenges of this system. Section VI discusses the conclusion and future work.

II. SYSTEM DESIGN

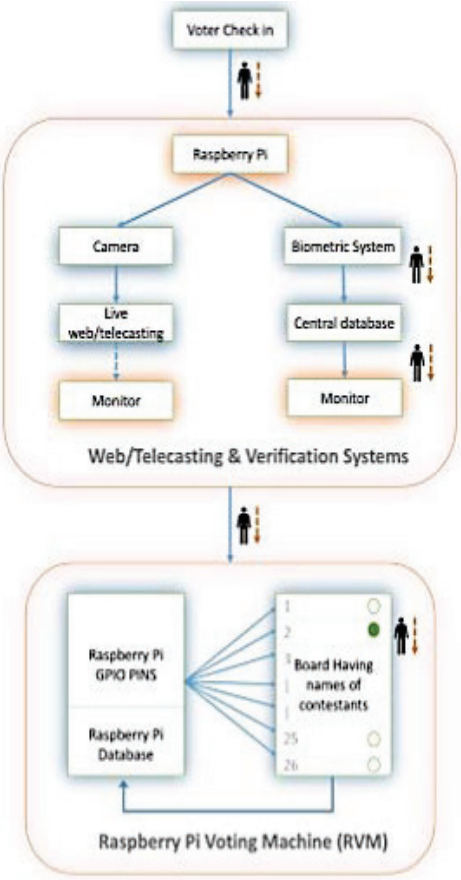

FIGURE 2.1: RASPBERRY PI SYSTEM VOTING DESIGN

There were many other electronic systems being used in voting process in several countries. Here we introduce Raspberry Pi for making the voting process more convenient and conformable to the resources of developing countries. Refer Fig 2.1. "Raspberry Pi Voting system" has been designed by considering and minimizing drawbacks of the technologies that are currently being used. Implementing this new system will reduce human resource and transform the entire process to a secured, simple and easy voting system. What makes this system feasible and simple? Undoubtedly the components! We used two Raspberry Pi boards for the whole system. These two are completely physically isolated from one other in order to perform their respective functions. First Raspberry Pi board is connected to internet [19] as it needs internet for sending biometric data and receiving results from central database. A camera, a biometric identifier and a monitor for officer in the polling station are the additional necessary components that are to be connected with first Raspberry Pi. A secondary monitor can also be connected to it so that the live webcasting can be displayed at the premises of the polling station itself. The second Raspberry Pi is not connected to internet as it is solely maintained to record ballots and maintain contestants database. As this is not connected to internet it is secured from external network threats. A box displaying contestants' names and buttons against their names is connected to the second Raspberry Pi. Based on the importance and care that should be given, RVS has been classified to below 4 categories.

A. Verification System

The voting system should only permit the voters who are eligible to cast the vote as per the electoral lists. At the same time, the system should not allow who is not eligible for voting. This system checks the validity of the voter and decides whether the voter is eligible to cast his vote. This validation process will comprise of biometric system which primarily concerned on checking of fingerprints [14] of voters. To accomplish this, a biometric identifier is connected to Raspberry Pi board which continuously checks for the best match with voters' fingerprints. This verification is designed to give accurate results and ensures the identity of voters. After successful identification, voter is eligible for voting and sent to next stage.

B. Web/Telecasting System

Unlike other government activities, election process needs to be very transparent in view of its vulnerable nature and great tendency for tampering of the whole system. Here system can be referred to the elements we use in the elections process. A common election process [3] involves coordination of broadly spread elements like working personnel, procedures and equipment. Tampering these systems can be in terms of physical damage, intentionally disabling the equipment and also can be hacking via intranet or internet. However a responsible authority for conducting elections cannot take a choice of giving any chances to attack and malfunctioning of the voting system. Thus, we use web cameras to continuously record and monitor this process and periodically report to higher authorities. This recording can be telecasted using large screens at public places in the interest of people.

C. Raspberry Pi Voting Machine

Advent of electronic technology gave us the chance of moving from manual paper ballot method to many electronic voting methods ages ago. This electronic way of conducting

elections dramatically decreased the human resource. Electronic voting machines are designed to record votes casted by voters. Considering the flaws of the presently used electronic systems, we introduced this Raspberry Pi Voting Machine (RVM) to serve better and simplify the votes recording process. There'll be a box containing names of the contestants and buttons against the names. These buttons are directly connected to Raspberry Pi GPIO [15] pins to record the responses given by the voters. Only one chance is given to each voter which is commonly known as one ballot per each voter. This system ensures that there's almost no scope for failures or interference by any means as it is not connected to any network during the process of voting. This proposed RVM is also made to run on batteries as this paper is targeted to those developing countries in which many areas may not have continuous power supply.

D. Database Management

Database is referred to data of voters. "Central database" maintains details of all the voters residing in the country. Details comprises of particular voter's unique ID to identify, personal details, photographs and most importantly biometric details of the voter. These details are in general not revealed to any other organization and so these are maintained in additional servers with promising security. This data is used for matching of the voters' details at the time of verification process. Apart from this database, at each polling station and district or zone level, a "local database" is maintained which gives his or her unique ID and personal details only for reference. This local database need not contain any confidential information like biometrics. These are the two main databases from which we collect information and the prime deciding factor for the voter whether eligible to vote or not. For reference, the local database is parted to two tables **1. Electoral table 2. Casted table**. After each ballot, these tables are updated so that voted person details are moved from electoral table to casted table. This table is maintained by Raspberry Pi I. At Raspberry Pi II which is used at RVM, a **Ballot table** is maintained to count and update the casted votes against the contestants.

III. ALGORITHM

A. Algorithm for Verification of Voter in RVS

The election process follows some steps beginning with biometric authentication of voter till the voter casting his/her vote. Refer Fig 3.1. 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.

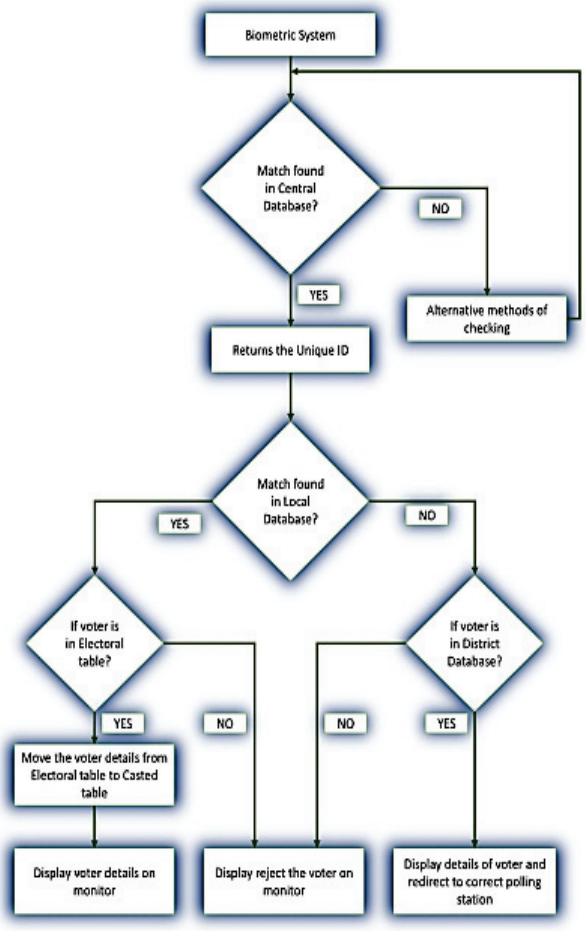

FIGURE 3.1: ALGORITHM FOR VERIFICATION OF VOTER VALIDITY IN RVS

B. Algorithm for RVS Working

After successful biometric authentication, the voter is sent to the "Raspberry Pi Voting Machine (RVM)" for casting the vote. A control manager is present for RVM functions like initialization of RVM to allow the voter. Refer the Fig 3.2.

Working model and the algorithm of the RVM is explained as follows:

1. After successful biometric authentication, valid voter comes to cast his vote in RVM. Now, Control Manager gives initialization signal by pressing the control switch of RVM. Control switch should be in adequate distance from RVM to ensure privacy of voter while voting.
2. On Initialization of RVM, GPIO pins of Raspberry Pi [17], [18] gets activated to input mode
3. In RVM, all the GPIO pins are connected to buttons present in line with all the contestants. In input mode, GPIO pins wait for any button to be pressed to receive input.
4. Voter casts his vote in RVM by pressing the button corresponding to the contestant name of his choice.
5. As soon as the voter presses any button, vote count of that contestant should be increased and updated in the database. This process can be explained as a separate sub process as follows:
   (1) In input mode, GPIO pins are all set to low level logic (0 Volts).
   (2) When voter presses any button, GPIO pin connected to corresponding button will be raised to high level logic (5 Volts) due to switching action of button.
   (3) Now, only one GPIO pin is in high level logic. Rest of the pins are in low level logic.
   (4) GPIO pin giving the value '1' (high level logic) is determined by Raspberry Pi with the help of coding.
   (5) Corresponding contestant name is also identified by using this pin¬ number, using input dictionary which consists of matching pin number with contestant name.

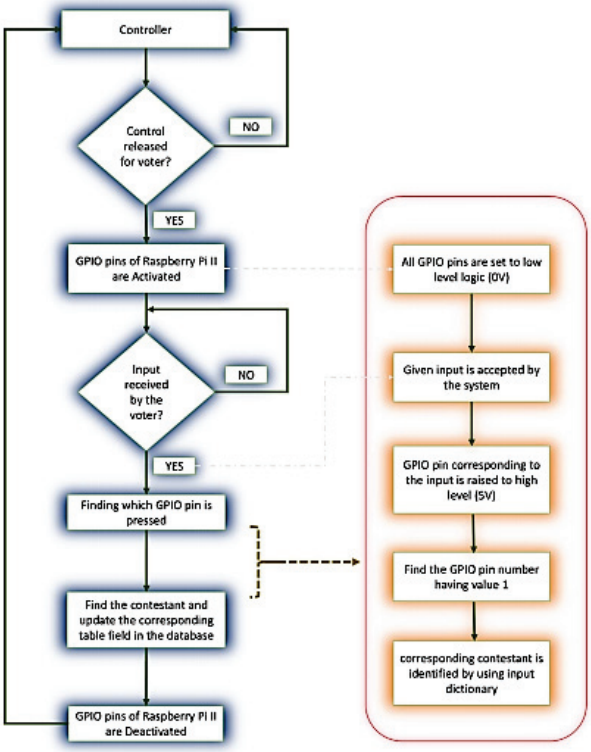

FIGURE 3.2: ALGORITHM FOR FUNCTIONING OF RASPBERRY PI VOTING MACHINE

6. After a voter casts his vote once, GPIO pins are deactivated. Even if voter tries to cast another vote, it won't be valid.
7. Deactivated GPIO pins are again activated only by initialization of RVM by Control Manager.

8. Control manager gives initialization when next valid voter comes from biometric check only and this process continues repeatedly till voting process terminates.

IV. RESULT

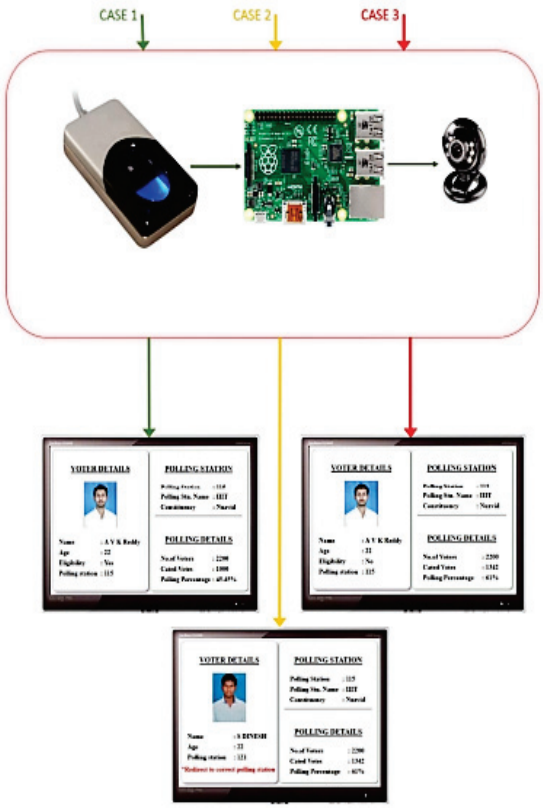

FIGURE 4.1: 3 CASES ARE SHOWN.

CASE1: VOTER CAME TO CAST VOTE AND SUCCEEDED IN VERIFICATION PROCESS.

CASE2: IF THE SAME VOTER CAME FOR SECOND TIME, NOT ELIGIBLE FOR CASTING HIS VOTE.

CASE3: VOTER BELONGING TO DIFFERENT POLLING STATION

V. CHALLENGES

Every system has got its own advantages and some real time challenges to face with. Some worst scenarios can cause interruption to the system's processes. Though the proposed voting system (RVS) has a pragmatic design, it may not give its hundred percent performances in some sensitive scenarios. This system is designed mainly to serve the purpose of underdeveloped and developing countries. As this system requires continuous power supply, few underdeveloped countries may fail to provide this. In such cases, as an alternative this system can be run on battery power. Failure in biometric fingerprint authentication may arise in few special cases. This can be solved by using alternatives like iris/face recognition which seeks for separate equipment. While authenticating the fingerprint template, if the data is transmitted through an unsecure channel there might be a chance of hacking and manipulating this data by third party. In such situation, the data that is transmitted should undergo high-level encryption and decryption techniques.

VI. CONCLUSION AND FUTURE WORK

The Raspberry Pi Voting System is designed with a motto to improve 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.

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-a-vote: 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.

[8] Chris Edwards, "Not-so-humble raspberry pi gets big ideas", vol.8, NO.3, pp. 30-33, 2013.

[9] Charles Severence, “Eben Upton: Raspberry Pi”, vol.46, NO.10, pp. 14-16, 2013.

[10] W. A. Arbaugh, “The real risk of digital voting?,”, vol. 37, no. 12, pp. 124–125, 2004.

[11] Tadayoshi Kohno, Adam Stubblefield, Aviel D. Rubin, and Dan S. Wallach, “ Analysis of an Electronic voting System”, In Proc. IEEE Symposium on Security and Privacy, May , 2004

[12] D. Ashok Kumar, T. Ummal Sariba Begum, “Electronic Voting Machine – A Review”, in proc. of the International Conference on Pattern Recognition, Informatics and Medical Engineering, March 21-23, 2012.

[13] T. Kohno, A. Stubblefield, A. D. Rubin, and D. S. Wallach, “Analysis of an electronic voting system,” in proc. of IEEE Symp. Security and Privacy, 2004, p. 27.

[14] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, Handbook of Fingerprint Recognition. New York, NY, USA: Springer-Verlag, 2009.

[15] Matt Richardson and Shawn Wallace, Getting Started with Raspberry Pi, United States of America: O’Reilly Media, 2013.

[16] Donald Norris, Raspberry Pi for the Evil Genius. McGraw-Hill Education, 2014, pp. 1-51.

[17] Maik Schmidt, Raspberry Pi, A Quick Start Guide. Pragmatic Programmers, LLC, 2012, pp. 1-47.

[18] Peter Membrey and David Hows, Learn Raspberry Pi with Linux. New York City: Apress, 2012, pp. 1-149.

[19] Eben Upton and Gareth Halfacree, Raspberry Pi User Guide. A John Wiley and Sons Ltd., 2012.

[20] Do Electronic Voting Machines Improve the Voting Process?[Online].Available:http://votingmachines.procon.org/view.resource.php?resourceID=000265.

[21] Why we don’t have online voting (and won’t for a long while) [Online].Available:http://worldmag.com/2014/11/why_we_don_t_have_online_voting_and_won_t_for_a _long_while

[22] What challenges remain for online voting [Online]. Available: http://politics.stackexchange.com/questions/17/what-challenges-remain-for-onlinevoting

[23] What is Biometrics? [Online]. Available: http://www.cse.iitk.ac.in/users/biometrics/pages/what_is_biom_more.htm.

[24] What Are Biometrics? - White Paper [Online]. Available: http://www.aware.com/biometrics/whitepapers/wab_biometric-processes.html

[25] J. Kelsey, “Strategies for software attacks on voting machines,” in Developing an Analysis of Threats to Voting Systems. Gaithers-burg, MD: National Institute of Standards and Technology[Online].Available:http://vote.nist.gov/threats/papers/stategies_for_soft-ware_attacks.pdf

[26] RPi Hub [Online], Available: http://www.elinux.org/RPi_Hub

[27] Python Software Foundation [Online], Available: https://pypi.python.org/pypi

[28] Raspberry Pi [Online], Available: http://en.wikipedia.org/wiki/Raspberry_Pi

[29] Raspberry Pi Foundation [Online], Available: http://www.raspberry.org