Implementing Smart Voting Systems: Challenges and Opportunities

Sayyadanand Sarfaraj Patel[1]
Student, Dept. of Electronics and Telecommunication,
Rajgad Dnyanpeeth's SCSCOE,
Pune, India
srkfanadnan333@gmail.com

Pooja Santosh Mahamuni[2]
Student,Dept. of Electronics and Telecommunication,
Rajgad Dnyanpeeth's SCSCOE,
Pune, India
poojamahamuni364@gmail.com

Kiran Prakash Jujare[3]
Student, Dept. of Electronics and Telecommunication,
Rajgad Dnyanpeeth's SCSCOE,
Pune, India
kiranjujare2@gmail.com

Deepak Sampat Khaladkar[4]
Student Dept. of Electronics and Telecommunication,
Rajgad Dnyanpeeth's SCSCOE,
Pune, India
deepakkhaladkar5412@gmail.com

Rohit Sandip Birdawade[*5]
Student,Dept. of Computer Science Engineering,
Rajgad Dnyanpeeth's SCSCOE,
Pune, India
rohitbirdawade2875@gmail.com

Sanjay Bapuso Patil[6]
Principal,
Rajgad Dnyanpeeth's SCSCOE,
Pune, India
principal@rajgad.edu.in

***Abstract*—*This article offers a detailed explanation of the process for creating an innovative electronic voting system that utilizes the flexibility and efficiency of the Raspberry Pi. This method aims to improve voting security, transparency, and user-friendliness by employing digital technology and a mechanism called the Voter Verified Paper Audit Trail (VVPAT). The proposed system comprises several components, including a Raspberry Pi for control, candidate selection buttons, a camera for voter verification, red LEDs to indicate selected candidates, a 16x2 LCD for displaying the current state, and a buzzer to provide feedback to voters regarding their success. Individuals choose candidates by activating a GPIO button connected to a Raspberry Pi device. Following the casting process, every vote undergoes thorough verification using red LEDs that simulate the corresponding button presses. Implementing the Voter-Verified Paper Audit Trail (VVPAT) method is an excellent approach to address the challenges associated with digital tampering. This approach guarantees transparency and precision by producing a tangible vote record, facilitating future audits and verification. The camera can detect fraud using facial recognition or QR code verification when linked via USB. The 16x2 LCD screen displays confirmation messages, voting instructions, and feedback when voters cast their ballots. As an added convenience and to make voting more transparent, the system alerts the user by sounding a bell when a vote is successful. Thus, the voter receives immediate audio confirmation. This article discusses the design and integration of future voting systems, emphasizing creating secure, transparent, and efficient systems. After thorough evaluation and testing, the proposed solution has been proven to significantly improve the voting experience while maintaining the integrity of elections*.

Keywords*—*Electronic Voting System, Voter Verified Paper Audit Trail (VVPAT), Digital Technology, Transparent Electoral Processes, Secure Voting

I. INTRODUCTION

Nowadays, with more and more people questioning the legitimacy of election processes, people have been trying to find a way to vote that integrates the best of computerized voting and the reliability of paper ballots. Together, they form the basis of a voting mechanism we are exploring. The most noteworthy contribution to the state-of-the-art results from this attempt is an electronic voting system built on Raspberry Pi. Applying cutting-edge technological solutions, this initiative seeks to address the shortcomings of existing voting methods. It is quite significant within the realm of voting technology. Utilizing the flexibility, affordability, and widespread availability of Raspberry Pi, the movement seeks to establish a new voting system that is more open, honest, accessible, and transparent [8].

This effort was created in reaction to the problems linked to physical ballots and the first version of digital voting machines [9]. Although paper ballots are frequently employed as a safeguard against tampering, they include other drawbacks, such as the lengthy casting process and the possibility of human mistakes. Nevertheless, despite endeavors to improve the procedure, electronic voting techniques have encountered censure because of their vulnerability to cyber-attacks and software deficiencies. This dilemma has been resolved by introducing an innovative electronic voting system that integrates the most beneficial elements of traditional and digital voting methods. By incorporating additional hardware components such as cameras, LCD screens, buzzers, and LEDs, the already straightforward and secure voting procedure on the cost-effective and versatile Raspberry Pi is further enhanced.

This project prioritizes transparency, accessibility, and security. To ensure the authenticity of the voting process, comprehensive digital and physical security measures have been implemented to prevent tampering. These methods involve the use of tamper-evident sealing and encryption. The implementation of Voter Verified Paper Audit Trail (VVPAT) technology improves security by allowing the verification of votes and simplifying the auditing process.

A thorough and all-encompassing methodology is necessary to implement such a system in different election scenarios. The program seeks to improve cyber resilience by employing open-source software, a modular design philosophy, and technologies that address technological obstacles. Furthermore, a thorough examination will be conducted[10].

Developing an electronic voting system based on Raspberry Pi aims to rethink the electoral landscape and make democratic processes more accessible, inclusive, and reliable. This attempt brings the possibilities of integrating paper ballots with electronic technology to light. This combination can usher in a new era of voting that is clear, easily accessible, and confidential.

II. LITERATURE SURVEY

As the 2000 presidential election in Florida unfolded, individuals worldwide started questioning whether using Internet Voting would solve all the problems. Shortly after,

individuals worldwide thoroughly analyzed their voting systems, searching for methods to enhance their functionality [1]. Politicians actively advocate for remote internet voting to enhance voter confidence, increase election turnout, and provide greater convenience. Nevertheless, as elucidated further in this document, distant internet voting will have a limited lifespan due to substantial societal and technological influences. This paper provides an overview of the current state of electronic voting, including various studies on Internet voting and electronic poll-site voting. It highlights the benefits of these methods, such as enhanced voter convenience, while addressing the concerns and grounds against their implementation.

"electronic voting" refers to voting in elections using electronic devices such as computers. Occasionally, this phrase is employed in a more limited sense to refer specifically to online voting. Electronic methods can be used for voter registration, tallying, and voting recording [2].

To avoid repeating the issues that impacted the US presidential elections in 2000, the Caltech/MIT Voting Technology Project [3] was established to create groundbreaking voting technology. The report analyzes the magnitude of the issues, their root causes, and the capacity of technology to mitigate them. The topic extensively addresses several aspects of "What is," including the procedures for conducting elections, the equipment utilized, the available voting locations, the options for early or absentee voting, and the financial resources allocated to elections. They propose using an innovation process to depart from traditional, uniform voting systems, introducing a new paradigm called "What could be" for voting technology. Based on the "A Modular Voting Architecture ("Frogs")" framework, the creation of a vote is separate from the actual casting of the vote. The "Frog" system ensures that votes are recorded in a way that cannot be changed, which is highly important. In this scenario, the computer responsible for generating the votes can be privately owned, but the device used for casting the votes must be open-source. It should be evaluated thoroughly to ensure its precision and security, and certification should be obtained accordingly. The study concludes by providing immediate and future recommendations for enhancing voting procedures.

In his work on "Electronic Voting", Rivest examines the challenge of establishing a secure platform for voting and explores the feasibility of issuing receipts to voters. In addition, he explores the subject of e-commerce and e-voting, discussing potential risks associated with automated, widespread attacks on home voting, the importance of using simple voting equipment, the need for audit trails, support for disabled voters, security issues with absentee ballots, and other related matters[4-7].

The "e-Voting Security Study" [11] thoroughly examines electronic voting methods. The book features insights and perspectives from prominent regional scholars and a concise overview of the area's latest academic and corporate advancements. This tool identifies weaknesses in voting systems, potential points of entry, and attack routes.

The detailed study on remote voting is built upon the contributions of Fujioka, Okamoto, and Ohta (FOO) [12]. The mathematical framework for a secure election is delineated, comprising an administrator, a counter, and voters who are interconnected anonymously. The blind voting technique discussed in this article has been effectively implemented in practical projects.

Sensus [13] utilizes blind signatures to guarantee that only authorized voters can submit their vote and that each vote is recorded only once while safeguarding the voter's privacy. It enables voters to autonomously and confidentially authenticate their ballots and contest the outcomes in case of any inaccuracies in the tallying process. The FOO architecture is enhanced by E-VOX [14] at MIT by utilizing Java, Netscape, and JDBC. This strategy continues to be utilized in education and research, as exemplified by its application during MIT's 1999 Undergraduate Association election. The paper titled "Multiple Administrators for Electronic Voting" [15] presents a method to reduce vote fabrication by distributing authority among multiple administrators.

The authors of the paper entitled "An untraceable, universally verifiable voting scheme" [16] suggest a remote voting technique that uses blinded signatures to enhance the anonymity of the voter's ballot. The deliberate choice to sacrifice the absence of receipts in their system is a compromise to maintain its qualities of safeguarding privacy, ensuring that anybody can verify it, providing convenience, and ensuring that it cannot be tracked.

The E-Poll project [17] investigates using UMTS-based broadband mobile communications to provide the required capacity and security for the E-Poll network. Establishing a safe and private network enables the utilization of E-Poll kiosks in any location. The voter-recognition system relies on advanced smart cards that incorporate biometric fingerprint readers, ensuring flawless identification of voters. Individuals with disabilities can easily use an ergonomic kiosk.

The primary goal of the non-partisan and non-commercial FREE e-democracy project [18] is to create the GNU.FREE Internet Voting system and promote the adoption of Free Software.

The author presents a technique, described in [19], for secure electronic voting that relies on something other than uninterrupted network connectivity between polling stations and the vote tallying server. The system is built upon a network-deficient environment, specifically sporadically linked. It operates effectively even in the absence of a network.

Computer systems used in electronic voting must adhere to essential criteria for assurance, availability, reliability, confidentiality, and integrity, as specified in the document "Security Criteria for Electronic Voting" [20]. Upon careful examination of the feasibility of those requirements, it becomes evident that many of them could be more attainable with absolute assurance from an operational perspective.

The new hazards identified by Rubin in [21] are why incorporating state-of-the-art technology in voting may not be advantageous. The voting platform is exposed to substantial security concerns, including malicious payloads and delivery mechanisms such as attack programs, DNS server attacks, and automatic downloads of active content. Malicious threats in the communications infrastructure are a significant problem. In addition, he observes that social engineering and the utilization of specialized gadgets also possess security vulnerabilities.

The Raspberry Pi, a small computer equipped with image processing capabilities, is built upon the Electronic Voting Machine (EVM) [22], which oversees the entire voting system. Utilizing a camera to capture an image of a citizen's national ID card serves to authenticate the individual's eligibility to vote within that jurisdiction. Every qualified voter who has yet to vote will be allowed to do so. Each voting machine is equipped with an authentication module that necessitates fingerprints. After the user's identity is confirmed, a designated system obtains the fingerprints for voting. A centralized Raspberry Pi voting system is connected to each voting system for identification.

The Impressive Smart Card Based Electronic Voting System [23] presents a voting system that instills confidence in elections by employing fingerprint techniques and issuing a smart card to each user, ensuring variety in the voting system and alleviating the workload of the Indian election committee. Simultaneously, the election process results will be automatically disclosed to the general public. Using this technique, anyone can effortlessly vote at any designated polling location. This study handles and integrates tests and effects using the given data sets. This report thoroughly examined all conceivable guidelines.

A biometric fingerprint-based electronic voting machine that incorporates Aadhar card verification. The voting mechanism implemented by [24] utilizes biometric fingerprints in conjunction with Aadhar certification. The program stores the Aadhar number on a compact ARM7 microcontroller, which then verifies the number using the provided information. This technology will be employed to capture the unique patterns of ridges and furrows on the fingertips of individuals who are citizens of India. If an individual meets the criteria for voting eligibility, they have the right to cast their ballots.

The Smart Voting System [25] implements a voting mechanism that allows individuals who are Indian nationals and above the age of 18 to cast their vote despite not being obligated to visit their hometown on the designated day. The objective of implementing a voting system based on Aadhar is to enable individuals to cast their votes electronically in their present place of residence during electoral elections.

The Smart Voting System utilizing RFID [26] offers a Radio Frequency Identification (RFID) method that allows users to vote securely using their computer or mobile phone without going to the polls physically. This is accomplished through a two-step verification process that includes the recognition of a face and the authentication of the one-time password (OTP). RFID tags, rather than voter identification cards, are used in the offline unofficial voting system. Voters can view the election results at any moment thanks to this application, which may help prevent consequences that could lead to disruptive voting.

III. Proposed System

The block diagram of the proposed SEVM system is shown in Fig.1.

The proposed setup comprises a Raspberry Pi, the primary component powered by a battery. The purpose of the push button is to cast a vote for the candidate displayed on the Voter Verifiable Paper Audit Trail (VVPAT) equipment. The buttons are linked to the Raspberry Pi via GPIO pins. The camera is connected to the Raspberry Pi using a USB cable. Each button of the VVPAT machine is equipped with red LEDs. Upon pressing the button, an audible alarm will be activated to indicate to the voter whether their vote has been successfully registered. At the same time, a 16x2 LCD panel will display the current voting status.

Extensive deliberation was devoted to the foundation of our electronic voting system, which is built upon Raspberry Pi. Multiple stages were employed in the development of the system, with each stage specifically aimed at addressing a distinct part of the process. The system's architecture, comprising the Raspberry Pi, LCD, LEDs, buzzer, and USB-connected camera, plays a crucial role in the design process and has a substantial impact. It is of utmost importance to prioritize the reliability, cost-effectiveness, and user-friendliness of the technology we select. Furthermore, it is imperative to develop a voting system that is not only secure but also simply accessible. Multiple measures have been taken to prevent tampering or illegally entering the voting equipment. These tactics include secure boot procedures, data encryption, and physical security safeguards. Regarding other concerns, we prioritize security and privacy above everything else.

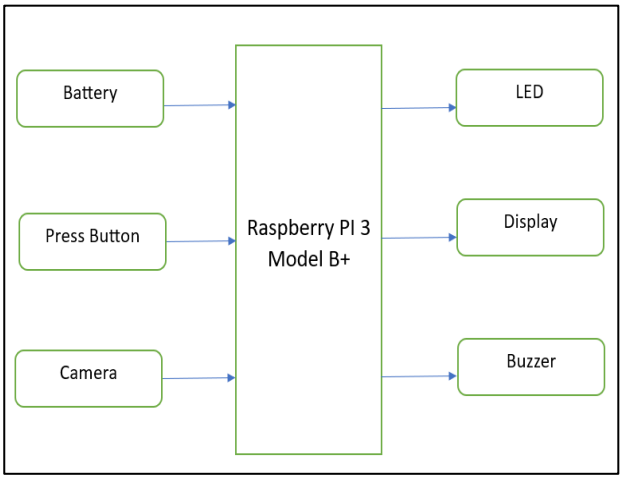

Fig. 1. Block diagram of proposed SEVM system

The initial stage of the development process is the design phase, which is subsequently followed by the programming of the Raspberry Pi. As a result, the hardware operates smoothly and offers a user-friendly LCD interface. Video voter verification and the production of Voter-Verified Paper Audit Trail (VVPAT) numbers are two effective technologies that can enhance the integrity of the voting process. When assembling hardware, it is crucial to collect and store all the separate components in a secure area. Usability testing involves conducting tests with multiple user groups at various stages of the testing process. This is done to guarantee that the system is easily accessible and user-friendly. Functional tests and vulnerabilities are also identified during security assessments, which are conducted to ensure that everything performs appropriately. The feedback from this phase enhances the dependability of the system and the user experience, which influences changes to the software and hardware.

Simulated pilot testing is the final process that must be completed before deployment. In this way, we can observe how the system operates during a genuine election and collect data on voter participation. This step is essential for determining any changes that may occur at the very last

minute and evaluating the system's capacity to expand and adapt to various election scenarios. Our project uses Raspberry Pi to modernize and enhance the electoral process. Every vote is counted accurately and securely using our cutting-edge electronic voting system, which is also safe and user-friendly. It is going to be done in this particular manner.

Agile methods will make the new voting procedure fluid, adaptive, and constantly enhanced. Agile is suitable for a changing process like voting due to its iterative development, stakeholder interaction, and rapid response.

The flowchart of the proposed system is shown in Fig.2.

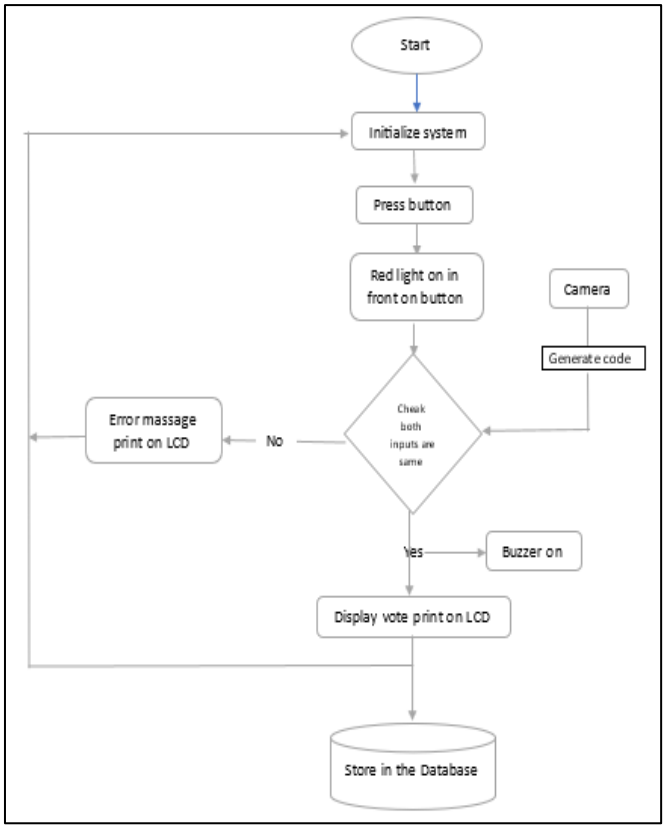

Fig. 2. Flowchart of the system

The steps required are as follows:

Step 1: Image Capture and Conversion.

- Image Capture: When a voter presses a button on the EVM machine, the light will glow, and a sensing device captures an image of the EVM's current state.
- Image Processing: Process the captured image to isolate the relevant information, such as the pressed button or the region of interest.
- Binary Conversion: Convert the processed image data into HSV color space. The Hue saturation and intensity values for red color are chosen and converted to the image into binary. Count the number of white pixels in the button's region of interest. If the count exceeds the threshold value set by the user, it indicates that the particular light is glowing.

Step 2: Button Press Conversion

- When the button is pressed, the particular GPIO pin of the Raspberry Pi goes high. The raspberry treats the particular button that is pressed.

Step 3: Compare the camera signal and button output

- The system would check the signal from the button and camera to authenticate that the correct vote has been cast. For example, if the button 1 is pressed, the particular GPIO assigned to that button becomes HIGH. Also, the light nearer to button 1 glows. The camera system checks whether the color of a particular region is red or not. If the signal of both the inputs matches, then the vote is recorded else, giving a system error.

Step 4: Database Storage

- Database Integration: Implementing a database to store voting data securely.

Step 5: Reset the process

- Reset the camera and verification kit to get another vote.

IV. Hardware and Software Specification

1) Hardware Requirement

A. Microcontroller or Processor: RASPBERRY Pi 3B+

The sample image of the Raspberry Pi 3B+ model is shown in Fig. 3.

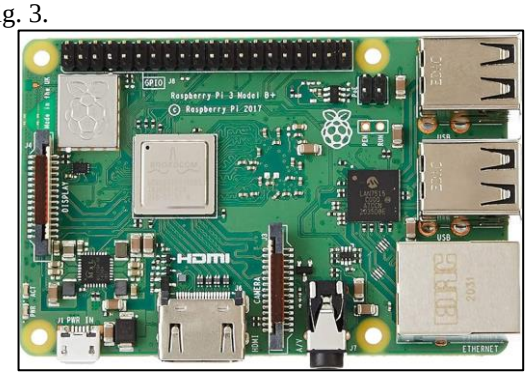

Fig. 3. Raspberry Pi 3B+ model

The Raspberry Pi Foundation has launched an enhanced iteration of the Raspberry Pi 3 edition B, known as the Raspberry Pi 3 Model B Plus(+), in response to the remarkable triumph of the previous edition. This upgraded edition boasts several advanced features, including faster Ethernet with a speed of 300 Mbps, a powerful 64-bit quad-core processor, a durable aluminum heatsink, dual-band wireless LAN operating at both 2.4GHz and 5GHz frequencies, and the added functionality of Power over Ethernet (PoE) through an extra PoE HAT.

It has fast 300Mbit/s ethernet, Bluetooth 4.2, dual-band 802.11 b/g/n/ac wireless LAN, and 1GB of random-access memory. The Pi 3 B+ is an upgraded version of the original Pi that includes Gigabit and PoE-capable Ethernet and enhanced safeguards to prevent the 64-bit processor from overheating. The new B+ board's footprint is identical to that of the original B model and the Raspberry Pi 2. You may use it to improve current projects or even in most cases.

Apps and computations will operate more quickly and smoothly on the new B+ model's improved board

components. An intriguing 64-bit quad-core CPU, which is at least 10% quicker than the previous generation, is also featured in the B+. Better heat control is another feature it offers.

Specifications: -

- Device: Broadcom BCM2837 Quad Core A53 (ARM v8) 32-bit system on a chip
- One gigabyte of LPDDR2 SDRAM
- Bluetooth: BLE chip from Cypress EIA 802.11ac 2.4Ghz/5.0Ghz
- Port: USB 2.0 Gigabit Ethernet (up to 300 Mbps)
- US plug: four 2.0 connectors
- Video Output: 1 × full-size HDMI GPIO Header 40-pin
- Video: Composite video, 4 Pole stereo output, MIPI CSI camera port, and MIPI DSI display port
- Multimedia: 1080p30, H.264, MPEG-4 decode. Encode with H.264 (1080p30). Visuals using OpenGL ES 1.1 and 2.0 APIs.
- There is a microSD card slot for storing data and operating systems.
- Power: POE-enabled USB port for 5.1V/2.5A dc
- Data Entry Camera and button interface

B.Camera

It is easy to carry about due to its small size. It is a plug-and-play gadget with a maximum resolution of 640 x 480 and supports 300k pixels. It also has a USB 2.0 port for easy operation. The USB cable is retractable, making it very convenient to use. The sample image of the USB camera is shown in Fig. 4

Fig. 4. USB Camera

Specifications: -

- The format supports a resolution of up to 640×480 pixels, with compatibility for 300k pixels and VGA/YUY2 files.
- This product complies with CE and Rohs regulations and has been authorized to use Windows and Vista operating systems.
- The USB cable can be conveniently retracted for storage.
- Photographs with a high resolution and precise color representation.
- This device is compatible with a USB 2.0 High-speed Sensor and does not require any driver installation. It may be easily connected and used without any additional setup.
- Size: 40mm × 15mm x 30mm; designed for use with Raspberry Pi and PC.

C. Output Display: 16X2 LCD, Buzzer, LED

A simple alphanumeric display with two lines and sixteen characters. Green backdrop with black writing. This uses the widely used HD44780 parallel interface chipset. It can get the code for the interface for free. Interfacing with this LCD panel requires at least six general-purpose I/O pins. Comes with an LED light. Operates in both 4-bit and 8-bit modes. The sample image of the LCd is shown in Fig.5.

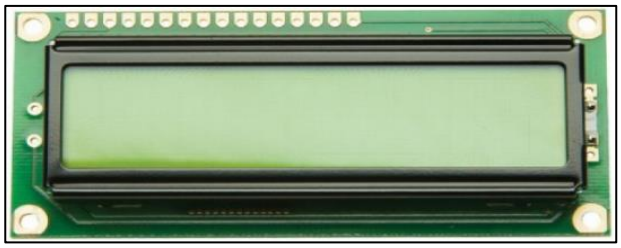

Fig. 5. LCD

Specifications: -

- There are two lines, each containing 16 characters.
- The HD44780 comparable LCD controller/driver features a green backlight, a 5x7 dot matrix character display, and a cursor. This interface is designed for use with either 4-bit or 8-bit microprocessors, specifically those incorporated into the system. It is a standard sort of interface.
- Compatible with a diverse range of microcontrollers

D. Memory: SD card of a minimum of 16 GB

The sample image of the memory card is shown in Fig.6.

Fig. 6. Memory: SD card

This project used a memory card of 16 GB is used to install the Raspbian OS.

E. Power Supply: 5V, 2A micro-USB charger

The Raspberry Pi is powered with a 5V micro-USB charger. The sample image of the power supply is shown in Fig. 7.

Fig. 7. Power Supply

2) Software Requirements

- OS: Raspbian
- Language: Python
- Image processing Library: OpenCV

V. RESULT AND ANALYSIS

Detailed explanations of the outcomes of the proposed system can be found in this section. As seen in Fig. 8, the Smart Electronic Voting Machines (SEVM) hardware has been proposed. Push buttons, a camera, and a Raspberry Pi 3B+ model are the components that are used to construct the system.

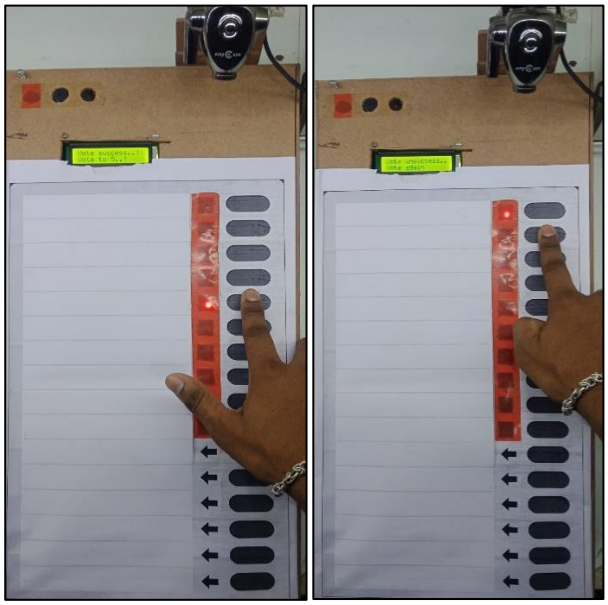

Fig. 8. Proposed system hardware

Test cases of the proposed system are tabulated in Table I

TABLE 1. TEST CASES

Case	Light indication	Actual Vote	Sound Status
Press button 1	Light of Candidate 2 ON	Vote for candidate 2	Buzzer ON
Press button 2	Light of Candidate 2 ON	Vote for candidate 2	Buzzer OFF
Press button 3	Light of Candidate 3 ON	Vote for candidate 3	Buzzer OFF
Press button 4	Light of Candidate 4 ON	Vote for candidate 4	Buzzer OFF
Press button 5	Light of Candidate 5 ON	Vote for candidate 5	Buzzer OFF
Press button 6	Light of Candidate 6 ON	Vote for Candidate 6	Buzzer OFF

Table 1 .outlines a series of test cases devised to assess the functionality and reliability of the electronic voting system. Each test case simulates a specific scenario where a voter selects a candidate by pressing a corresponding button, and the system's response, including light indication, recorded vote, and sound status, is evaluated. In the "Light Indication" column, the expected behavior of the LED lights on the VVPAT machine is described. As soon as the voter presses the button, the light corresponding to their choice of candidate should light up, visually confirming their choice. This visual feedback significantly improves transparency and enables voters to verify the accurate recording of their decisions.

The selection of the candidate is contingent upon the button clicked in the "Actual Vote" column. The objective of the voting process is to ensure the system accurately records and tabulates voter input votes. The accuracy of the voting process can be guaranteed by directly comparing the actual vote count with the desired outcome. The specific operating information of the buzzer connected to the system can be observed in the "Sound Status" column. The buzzer may be triggered instantly upon the voter's button press to validate their vote. This auditory verification can aid voters in verifying their vote, especially persons with visual disabilities.

To evaluate the accuracy and reliability of the electronic voting system, it is essential to meticulously carry out each test scenario and compare its actual performance with the expected results stated in the table. The purpose of these test cases is to verify the security of the voting process, guarantee that voters receive clear and reliable visual and aural feedback, and verify the system's capability to record their votes accurately. Thorough testing can identify and address possible issues, guaranteeing that the system is efficient and reliable during voting scenarios.

VI. CONCLUSION

Electronic voting machines (EVMs) with integrated cameras and push-button inputs can update voting procedures. One can achieve this by integrating digital interfaces, push buttons, and video systems to enhance the efficiency and effectiveness of voting on SEVM activities. By employing the camera feature to capture and document the votes cast by candidates, there is a possibility of enhancing accountability and the overall security of the process. However, it is imperative to establish rigorous security protocols to prevent unauthorized access and tampering, ensuring optimal functionality of the system. When creating a system everyone can use, it is crucial to consider several factors, such as accessibility, user interface design, and thorough testing methods. When used correctly, Secure Electronic Voting Machines (SEVMs) can enhance the ease of voting and the security and transparency of the voting process.

REFERENCES

[1] "Voting After Florida: No Easy Answers," Lorrie Faith Cranor, December 2000, http://lorrie.cranor.org/.

[2] "Electronic Voting," Encyclopedia of Computers and Computer History, prepared by Lorrie Faith Cranor and edited by Raul Rojas, published by Fitzroy Dearborn, 2001.

[3] "Voting – What is, What Could be," Caltech/MIT Voting Technology Project (VTP) Report, July 2001.

[4] "A Modular Voting Architecture ("Frogs")," Shuki Bruck, David Jefferson, and Ronald L. Rivest, August 2001.

[5] "Comments of Professor Ronald L. Rivest," Caltech/MIT VTP Press Conference, July 16, 2001, http://theory.lcs.mit.edu/~rivest/publications.html.

[6] "Testimony was given before the US House Committee on Administration," Ronald L. Rivest, May 24, 2001, http://theory.lcs.mit.edu/~rivest/publications.html.

[7] "Electronic Voting," Ronald L. Rivest, Technical Report, Laboratory for Computer Science, Massachusetts Institute of Technology.

[8] "Report of the National Workshop on Internet Voting: Issues and Research Agendas," Internet Policy Institute, sponsored by the National Science Foundation, Conducted in cooperation with the University of Maryland and hosted by the Freedom Forum, March 2001.

[9] "A Report on the Feasibility of Internet Voting," California Internet Voting Task Force, January 2000.

[10] "Appendix A: Technical Committee Recommendations," California Internet Voting Task Force, January 2000.

[11] "e-Voting Security Study," E-Democracy Consultation, U. K. Cabinet Office, http://www.edemocracy.gov.uk/library/papers/study.pdf.

[12] "A Practical Secret Voting Scheme for Large Scale Elections," A. Fujioka, T. Okamoto, and K. Ohta, Advances in Cryptology - AUSCRYPT '92.

[13] "Sensus: A Security-Conscious Electronic Polling System for the Internet," Lorrie F. Cranor and Ron K. Cytron, Proceedings of the Hawai'i International Conference on System Sciences, January 7-10, 1997, Wailea, Hawai'i, USA.

[14] "Secure Electronic Voting Over the World Wide Web," Master's Thesis, Department of Electrical Engineering and Computer Science, Massachusetts Institute of Technology, May 1999.

[15] "Multiple Administrators for Electronic Voting," Bachelor's Thesis, Department of Electrical Engineering and Computer Science, Massachusetts Institute of Technology, May 1999.

[16] "An Untraceable, Universally Verifiable Voting Scheme," Professor Philip Klein, Seminar in Cryptology, December 12, 1995.

[17] http://www.e-poll-project.net/

[18] http://www.free-project.org/

[19] "Secure Voting Using Disconnected, Distributed Polling Devices," David Clausen, Daryl Puryear, and Adrian Rodriguez, Department of Computer Science, Stanford University.

[20] "Security Criteria for Electronic Voting," Peter G. Neumann, 16th National Computer Security Conference, Baltimore, Maryland, September 20-23, 1993.

[21] "Security Considerations for Remote Electronic Voting," Aviel D. Rubin, Communications of the ACM, Vol. 45, No. 12, December 2002.

[22] Md. Maminul Islam, Md. Sharif Uddin Azad, Md. Asfaqul Alam, Nazmul Hassan, "Raspberry Pi and image processing based Electronic Voting Machine (EVM)," 2014 International Journal of Scientific & Engineering Research, Volume 5, Issue 1, pp. 1506- 1510, January 2014.

[23] G. Keerthana, P. Priyanka, K. Alise Jenifer, R. Rajadharashini, Aruna Devi. P, "Impressive Smart Card Based Electronic Voting System", 2015 IJRET: International Journal of Research in Engineering and Technology, Volume 4, Issue 3, pp. 284-288, March 2015.

[24] Shekhar Mishra, Y. Roja Peter, Zaheed Ahmed Khan, M. Renuka, Abdul Wasay, S.V. Altaf, "Electronic Voting Machine using Biometric Finger Print with Aadhar Card Authentication," 2017 International Journal of Engineering Science and Computing, Volume 7, Issue 3, pp. 5897-5899, March-2017

[25] Gowtham R, Harsha K N, Manjunatha B, Girish H S, Nithya Kumari R, "Smart Voting System," 2019 International Journal of Engineering Research & Technology (IJERT), Volume 8 Issue 4, pp. 294-296, April-2019.

[26] Ganesh Prabhu S., Nizarahammed A., Prabu.S, Raghul S., R. R. Thirrunavukkarasu, P. Jayarajan, "Smart Online Voting System," 2021 7th International Conference on Advanced Computing and Communication Systems (ICACCS), pp. 632-643, 2021.

Journal of Microelectronics and Solid-State Devices (JOMSSD)

ISSN: 2455-3336
Volume-11
Issue-2
Year-2024

Research Article

Date of Receive- 1st-July-2024
Date of Acceptance- 16th-July-2024
Date of Publication- 28th-July-2024