Quest Journals
Journal of Electronics and Communication Engineering Research
Volume 9 ~ Issue 3 (2023) pp: 26-31
ISSN(Online) : 2321-5941
www.questjournals.org

Research Paper

Novel Hybrid Biometric Electronic VotingSystem

[1]B. Ravi Babu, [2]K.K. Vanitha, [2]K. Vishnu Vardhan,
[2]N. Vamsa Vardhan Reddy, [2]M. Tejaswini, [2]S. Venkata Somasekhar
[1], Electronics and Communication Engineering, SiddharthInstitute of Engineering and Technology (SIETK), Puttur, Andhra Pradesh, India [2]Electronics and Communication Engineering, Siddharth Institute of Engineering andTechnology (SIETK), Puttur, Andhra Pradesh, India

Abstract: *Electronic voting machines (EVMs) were first utilized in the 20th century and are still in use today. Conventional electronic voting machines only have the ability to record a candidate's vote total. The polling officer personally verifies voters' identities before allowing them to cast ballots using the voter list. The poll worker uses indelible ink to detect fraudulent voters. These techniques call for more labor. In order to address these issues, we suggested a novel method based on the Internet of Things (IOT). Here, we're tying the Internet of Things to the voting machine. At first, the user enrolled their faces and their finger prints with an id. If a user's finger print is recognized later on during the voting process, the monitor will display their ID and the short names of each party. This party id must be entered by the user using switches. The party icon will then show up in the LCD. The total votes cast for each party will increase, as well as that party's vote total. If one of them matches, thevoter is permitted to cast a ballot because the system uses both biometric and video data. The server receives each party's vote total as well as voter identification information.*

Keywords: *Electronic voting machines, IOT, Voter verification, Biometric identification, Fraud prevention.*

R*eceived 12 Mar., 2023;* ***R****evised 25 Mar., 2023;* ***A****ccepted 28 Mar., 2023* © *The author(s) 2023.*
P*ublished with open access at* ***www.questjournals.org***

I. INTRODUCTION

Electronic voting machines (EVMs) were first utilized in the 20th century and are still in use today. Conventional electronic voting machines only have the ability to record a candidate's vote total. The polling officer personally verifies voters' identities before allowing them to cast ballots using the voter list. For the purpose of identifying a fake voter, poll workers employ indelible ink. Two units, the Control Unit and the Balloting Unit, make up an EVM. The Ballot Unit is placed inside the democratic compartment, while the Control Unit is kept with the Presiding Officer or a Polling Officer. The Polling Officer responsible for the Control Unit will press the Ballot Button rather than hand out a voting form paper. By pushing the blue catch on the Ballot Unit next to the up-and-comer and displaying the image of their choice, the voter will be given the ability to project their vote. The maker permanently identifies the working project of the regulator used in EVMs in silicon at the time of assembly. Once the program is created, no one can alter it. EVMs can accommodate amaximum of 64 competitive up-and-comers. If more competitors apply than there are spaces in a BU, which is limited to 16 newcomers, a second BU must be connected in a manner similar to the primary BU. In the rare event that the total number of applicants exceeds 32, a third BU is to be added, and if the total number of applicants exceeds 48, a fourth BU is to be added to accommodate for a maximum of 64 applications. The EVMs save a significant amount of time, money, paper, and labour because the cycle is faster and more reliable. The officer conducting the survey must complete a genuine cycle of citizen recognition. Citizens must present their Election Picture Identity Card (EPIC), which was provided by the Election Commission, in order to project votes using EVMs. These techniques call for more labour. In order to address these issues, we suggested a novel method based on the Internet of Things (IOT). Here, we're tying the Internet of Things to the voting machine. At first, the user enrolled their faces and their finger prints with an id. Once the user's Aadhar ID has been verified, he must then vote. If any of his fingerprints match, the monitor will display his ID and the brief names of each party. The user must utilize the keypad module to enter that party ID. The party icon will then show up on the monitor. The vote total for that party will increase, and the server should be updated with the total vote totals for all parties. If one of them matches, the voter is permitted to cast a ballot because the system uses both biometric and video data. The server receives each party's vote total as well as

voter identification information. Based on this information, the server thanks voters with an email and a message and compares the votes received by each party to identify the winner.

II. LITERATURE REVIEW

A hybrid biometric electronic voting system that employs both fingerprint and iris recognition for voter authentication is proposed in the research article "A Secure and Robust Electronic Voting System Utilizing Hybrid Biometric Method" by G. Ananthi and S. Deepa. The method attempts to increase voting process security and accuracy while lowering the possibility of fraud. The proposed system's performance was evaluated through experiments by the authors, and the findings indicated that it had a high accuracy rate and could successfully thwart fraudulently voting.

A novel biometric electronic voting system using face and fingerprint recognition wasproposed by M. F. Talha and M. S. Hossain in a different research paper under the title "A Novel Biometric Electronic Voting System Using Face and Fingerprint Recognition." The system would use facial and fingerprint recognition to authenticate voters. For feature extraction and classification of the biometric data, the system uses machine learning methods. The results of the trials the authors ran to assess the effectiveness of the suggested method revealed that it had a high accuracy rate and could thwart attempts at fraudulent voting.

A biometric-based electronic voting system that uses fingerprint recognition for voter authentication is proposed in the research paper "Biometric Based Secure Electronic Voting System" by N. N. Singh and S. Srivastava. The voter's biometric information is accessed by the system using a smart card reader, and the fingerprint information is encrypted for protection. The results of the trials the authors ran to gauge how well the suggested system worked revealed that it had a high accuracy rate and could stop fraudulent voting.

In conclusion, the examined literature indicates that the security and accuracy of the voting process can be increased by using biometric-based electronic voting systems. The security of the system can be further increased by using hybrid biometric approaches, such as combining iris and fingerprint recognition or facial and fingerprint recognition. Additionally, the confidentiality and integrity of the biometric data can be guaranteed through the use of machine learning algorithms and encryption methods.

III. EXISTING SYSTEM

Electronic democratic machine (EVM), which was introduced in the 20th century, is widely used. Traditional electronic voting machines can only record the democratic results of each candidate. A polling officer physically identifies voters and counts their votes while using a citizen list. Surveying officials use permanent ink to identify dishonest citizens. Two units,the Control Unit and the Balloting Unit, make up an EVM. The Ballot Unit is placed inside the majority rule compartment, while the Control Unit is kept with the Presiding Officer or a Polling Officer. The poll worker in charge of the control unit will press the ballot buttonrather than hand out a paper with the democratic framework. By pressing the blue catch onthe ballot unit next to the contender and image of their choice, the voter will be able to cast a longer ballot. At the time of assembly by the manufacturer, the working task of the controller utilized in EVMs is permanently etched in silicon. The program cannot be changed once it has been generated by anyone. EVMs can support a restriction of 64 testing newcomers. Ifthe total number of competitors exceeds 16, there is only room for 16 up-and-comers in aBU; in this case, a second BU must be added in addition to the primary BU.

Drawbacks: A few issues with the current method have been discovered generally. These are the verification process itself takes longer because officials perform it by hand and it lacksthe ability to detect bogus votes.

IV. PROPOSED SYSTEM

In order to overcome the problems with the current strategy, a highly secure and intelligent electronic voting machine (EVM) system is proposed. To verify the voter's authenticity, the system uses both facial recognition and biometric (fingerprint) verification. Voters must scan their fingers on the biometric system before looking into a webcam to view their faces in order to cast a ballot. Once the voter's ID has been validated, this activates the biometric system and makes them eligible to cast a vote.

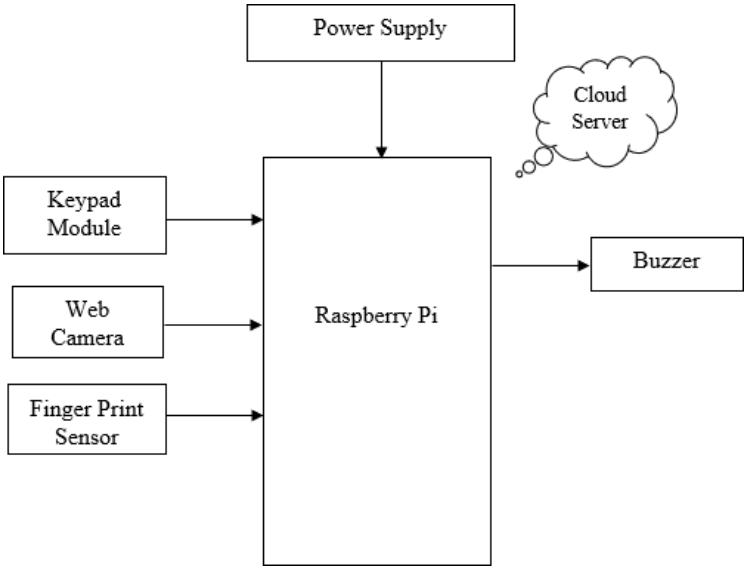

Fig. 1. Block Diagram of the proposed system

The proposed system has a number of benefits over the current method. The technology can decrease the need for human work, such as validating voter identities and applying indelible ink, by using biometric data to prevent fraudulent voting. The use of face recognition significantly strengthens the system's security because it can reliably identify the voter and thwart any impersonation efforts. Moreover, cameras and biometric voting devices increase voting efficiency by removing the need for poll workers to manually confirm each voter's identity. Voters' wait times may be cut down as a result, which will enhance their entire voting experience. Overall, the suggested system offers an approach to electronic voting that is safe, effective, and user-friendly. It has the ability to increase the accuracy and integrity of the voting process while making it more accessible to voters by using cutting- edge technologies like facial recognition and biometric verification.

Hardware Requirements:

Raspberry Pi: It is a small, single-board computer that can be used for various purposes, including home automation, gaming, and education. It is affordable and has a wide range of capabilities.

Fig 2. Raspberry Pi

The Raspberry Pi can act as the brain of the voting system, acting as a processor forall of the system's many parts. Also, it has an internet connection that enables data transmission and remote access.

Keypad Module: It is an input device that allows users to enter numeric or alphanumeric values. Keypad modules are commonly used in security systems, access control, and other applications that require user input.

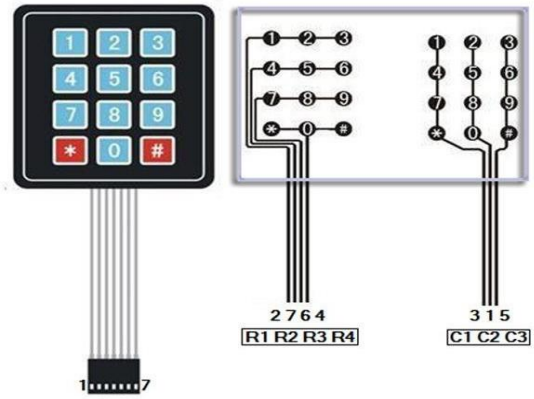

Fig 3. Keypad Module

Voters can cast their ballots and enter their voter identification numbers using the keypad module. Each vote must be cast for only one candidate, and the keypad can be designed to limit the amount of votes any person may make and keep track of the total number of votes cast.

Web Camera: It is a camera that can be connected to a computer or Raspberry Pi and used for video conferencing, surveillance, or other applications that require video input.

Fig 4. Web camera

During the voting process, the web camera can be utilised to record the voters'images, which can be used to confirm the voters' identities. To verify the accuracy of the voting process, the photos may also be saved for auditing purposes.

Buzzer: A buzzer or beeper is an audio signaling device, which may be mechanical, electromechanical, or piezoelectric. Typical uses of buzzers and beepers include alarm devices, timers and confirmation of user input such as a mouse click or keystroke. Buzzer is an integrated structure of electronic transducers, DC power supply, widely used in computers, printers, copiers, alarms, electronic toys, automotive electronic equipment, telephones, timersand other electronic products for sound devices.

Fig 5. Buzzer

Fingerprint Sensor Module: It is a device that can read fingerprints and be used for biometric authentication or identification. Fingerprint sensor modules are commonly used in security systems, access control, and other applications that require user identification.

Fig 6. Finger Print Sensor

The voters' identities can be verified using the fingerprint sensor. By matching fingerprints to those in the database, it is possible to programme the system to only permit registered voters to cast ballots. This assures that each voter can only cast one vote and eliminates the potential of voter fraud.

Software Requirements:

NOOBS Software: It is an easy-to-use installer for Raspberry Pi operating systems. It allows users to install multiple operating systems and select the one they want to use at startup. We can use the NOOBS programme to install the Raspbian operating system, which is a free and open-source Debian-based Linux distribution, for the Novel Hybrid Biometric Electronic Voting System. The essential libraries for the voting system's components can then beinstalled when the Raspbian operating system has been set up.

Python3 IDE: It is an integrated development environment for the Python programming language. It provides a text editor, debugger, and other tools to help developers write, test, and debug Python code. Python 3 can be used to create code that interacts with the keypad module, allowing voters to enter their ID numbers and cast their ballots. Python 3 can also be used to connect to the web camera and take pictures of the voters that can be used to confirm their identities. Python 3 can also be used to give feedback to voters during the voting process and present instructions to them on the LCD panel. Additionally, we can utilise Python 3 to communicate with the fingerprint sensor and confirm the identity of the voters.

V. CONCLUSION

The suggested approach of fusing the Internet of Things with electronic voting equipment can offer a more effective and secure voting process. A more effective and secure voting procedure may result from the merging of IoT technology and electronic voting machines. In order to prevent fraudulent voting and minimize the need for human work, biometric data, such as facial recognition and fingerprint scanning, can be

used in conjunction with video data. The security and privacy of the data the system collects must be guaranteed, though. The incorporation of IoT can boost the reliability, effectiveness, and security of electronic voting with careful planning and precautions.

References

[1]. Secured Electronic Voting Machine Using Biometric Technique with Unique IdentityNumber and IOT, 2020

[2]. A Review of Face Recognition System Using Raspberry Pi in the Field of IoT ArihantKumar Jain, Richa Sharma, Anima Sharma, 2018

[3]. A Review paper on biometrics implementation based on internet of things using raspberrypi Trupti Rajendra Ingale, 2017

[4]. A literature survey on micro-controller based smart electronic voting machine system

[5]. S.V. Prasath, R. Mekala M.E. (Ph.D.), 2014

[6]. P. S. Pandey, P. Ranjan, M. K. Aghwariya, "The Real-Time Hardware Design andSimulation of Thermoelectric Refrigerator System Based on Peltier Effect" ICICCD 2016DOI 10.1007/978-981-10-1708-7_66, vol. 7, pp. 581- 589, (2016). International Journal on Human and Smart Device Interaction Vol. 2, No. 1 (2015) 6 Copyright ©2015 GV School Publication

[7]. G. Rani, P. S. Pandey, M. K. Aghwariya, P. Ranjan, "LASER as a Medium for Data" Transmission Proceeding of International conference on ICARE MIT-2016, Organized byDepartment of Mechanical Engineering, M.J.P. Rohilkhand University, Bareilly-. ISBN No.: 978-93-82972-19-8, pp. 9-11, December (2016).

[8]. P. Ranjan, G. S. Tomar, R. Gowri, "Metamaterial Loaded Shorted Post Circular Patch Antenna" International Journal of Signal Processing Image Processing and Pattern Recognition (IJSIP) SERSC Publication, ISSN 2005-4254, vol. 9, no.10, pp. 217-226, (2016).

[9]. K. Ghatak, K. Thyagarajan, "Optical Electronic", Cambridge University Press, 20 July (1989).

[10]. N.Q. Ngo, "A new approach for the design of wideband digital differentiator and integrator", IEEE Transactions on Circuits Systems. II: Express briefs, vol. 53, no. 9, pp. 936-940, (2006).