International Journal of Scientific Research in Science, Engineering and Technology

Print ISSN - 2395-1990
Online ISSN : 2394-4099

OPEN ACCESS

Available Online at : www.ijsrset.com
doi : https://doi.org/10.32628/IJSRSET

Biometric Voting System

Prasad Ramchandra Mavarkar[1], Jaychandra C[2], Vrashabh Naik[3], Krishna Talli[3], Shivanad Uttur[3], Parvati Nayak[3], Lakshmi Bhasme[3]

[1]Lecturer, Department of Electronics and Communications Engineering, Government Polytechnic College Rabakavi – Banahatti, Karnataka, India

[2]Lecturer, Department of Science, Government Polytechnic College Rabakavi – Banahatti, Karnataka, India

[3]Electronics and Communications Engineering, Government Polytechnic College Rabakavi – Banahatti, Karnataka, India

ARTICLEINFO

Article History:

Accepted: 25 March 2024
Published: 11 April 2024

Publication Issue :
Volume 11, Issue 2
March-April-2024
Page Number :
220-225

ABSTRACT

A biometric voting system abstract would outline the key features and principles of a voting system that utilizes biometric authentication methods, such as fingerprint or iris recognition, to ensure secure and accurate voter identification. It would emphasize the system's potential to enhance the integrity of elections by reducing fraud and ensuring each voter's unique identity. Additionally, the abstract might touch upon the technological aspects, security measures, and potential challenges associated with implementing a biometric voting system. The model proposed enables the voter to poll his vote in any of the polling station in his state or anywhere in the country. The voting terminals may be interconnected using IOT technology.

Keywords : Biometric Authentication, Fingerprint Recognition, Iris Scanning, Voter Identification, Election Integrity, Secure Voting, Fraud Prevention, Biometric Data Encryption, Voter Privacy, Technology Implementation, Electoral System, Authentication Accuracy, Voter Registration, Authentication Protocols, Election Security

I. INTRODUCTION

A biometric voting machine is an advanced electronic system designed to modernize and secure the voting process in elections. It integrates biometric technology, which involves the measurement and analysis of unique physical or behavioural characteristics, to verify the identity of voters. Common biometric modalities include fingerprint scanning, iris recognition, and facial recognition. The primary purpose of biometric voting machines is to enhance the security and accuracy of elections by ensuring that each vote is cast by a legitimate and eligible individual. Traditional voting methods, relying solely on paper ballots or electronic voting machines without biometric authentication, may be susceptible to issues such as voter impersonation and electoral fraud. Biometric voting machines work by capturing and

storing biometric data from registered voters during the voter registration process. On election day, voters present themselves at the polling station, and their biometric information is compared to the stored data to verify their identity. This process adds an extra layer of authentication, making it significantly more challenging for individuals to engage in fraudulent voting practices. The advantages of biometric voting machines include increased accuracy, reduced instances of voter impersonation, and enhanced transparency in the electoral process. These machines aim to mitigate concerns related to electoral fraud, ensuring the integrity of democratic elections. Additionally, the streamlined authentication process facilitated by biometric technology can contribute to faster and more efficient voting procedures. However, the implementation of biometric voting machines also raises privacy and data security concerns. It is crucial to establish robust safeguards to protect the collected biometric information and guarantee the confidentiality of voters' personal details. In summary, biometric voting machines represent a technological evolution in elections by leveraging biometric authentication methods. As with any technological advancement, careful consideration of privacy and security measures is essential to ensure the responsible and ethical use of biometric technology in the electoral process.

II. LITERATURE SURVEY:

A literature Survey during a project report is that section that suggests the numerous analyses and Studies made in the discipline of your interest and consequently the criteria and analysis cover various categoric including privacy, Security verification, integrity functionality and Examination Direct recording electronic voting machine. Online voting system is a web-based system that facilitates the running of elections and Survey online. online voting System provides the online registration from for the users before voting and makes the users to cast their vote online the system is to be developed with high security and were friendly. As information technology Evolves over time, the need for a better, faster, more convent and secure online voting is Essential requirement. The security is one of the main Concerns, such as authentication, confidential integrity and non-repetition. it is not an early task to achieve secure overing

Steps of voting process: -

1.first palling official will check your name on the voter list and check your ID proof
2.Second polling official will ink your finger, give you a slip & take your signature on a register
3.you will have to deposited the slip at the third polling official and show your inked finger and then proceed to the polling booth
4. Record your vote by pressing the ballot button opposite the Symbol of the candidate of your Choice on the Electronic voting machine (EVM); you will hear a beep Sound
5.check the Slip that appears in the transparent window of the VVPAT Machine. The slip with the candidate Serial No. name & Symbol shall be visible for 7 seconds before it drops in the Sealed VVPAT box
6.you can press NOTA, none of above, if you don't like ang on Candidate it's the last button the evm (Electrical voting Machine) Biometric voting systems.

This voting system makes use of a biometric feature to authenticate users of the sputum fingerpaint recognition hand ware is integrated with the system so as to solve the problem of the Existing system The system operates in an identification mode and performs Capture fingerprints. Extracts the features and Stores in the database verifies the identity of the voter at login time by comparing the fingerprint that has been pre-stored in the database with the fingerprint being supplied at login provides an interface for the user to cast votes if a match is found

provides an interface for viewing the results of the Election System Design & flow. The Biometric voting system's architectural design is a diagram that defines the relationship between Major Structural Elements of the Software, the design patterns that Can be used to archived the. requirements defined for the System & the Constraints that affect the way in which architectural design Patterns can be applied Project Implementation

Steps of biometric voting System

1. Create your account Here in first database
* Name
* Phone number.
* Password. next click on create account

2.than we are going voting then only give your finger than it shows your all details.

3.than identified the all details next go to the) Wrong

Steps of biometric voting System

1. voter registration: Individuals register to vote by providing their biometric data such as a fingerprint, iris scans, or facial recognition data, along with other information identifying

2.Biometric Data Enrolment:

During registration, the voter's biometric data is captured using Specialized devices. This data is securely Stored in a database

3. voter verification: on Election Day or during Early voting, voters present themselves at a polling station. Their identify is verified by Matching their biometric data with the data Stored in the database

4. Issuance of Ballot: once the votes identify is confirmed they are issued a ballot to cast their vote

5.voting process: The vote casts their vote using the designated voting method

6. vote counting: After the voting periods Ends votes are tallied In a biometric system the biometric data may also be used to entire they Each person has only case and vote

7. Results compilation: The results from each Polling station are compiled to determine the overall outcome of the election

8. data security: - Throughout the process. Stringent Security measures are in place to porters the integrity of the biometric data & pane not tampering or unauthorized access

III. METHODOLOGY

A biometric voting system typically involves the use of unique physical or behavioural traits, such as fingerprints, iris patterns, or facial features, to verify a voter's identity. The methodology generally includes:

1. Registration: Voters enrol by providing their biometric data and other relevant information. This data is securely stored in a central database.

2. Verification: On election day, voters present themselves at the polling station. Their biometric data is matched against the stored records to confirm their identity.

3. Voting Process: Once verified, voters cast their ballots using traditional or electronic voting methods.

4. Biometric Data Security: Robust security measures are implemented to protect the stored biometric data from unauthorized access or tampering.

5. Real-time Authentication: The system ensures real-time authentication to prevent multiple voting attempts by the same individual.

6. Redundancy and Reliability: Implementing backup systems and ensuring the reliability of biometric devices are critical to the system's overall integrity.

7. Audit Trails: A comprehensive audit trail is maintained to track all interactions with the biometric voting system, providing transparency and accountability.

8. Privacy Protection: Strict measures are in place to safeguard voters' privacy and prevent misuse of their biometric information.

9. Accessibility: The system should be designed to accommodate individuals with disabilities, ensuring inclusivity in the voting process.

10. Training and Awareness: Training election officials and creating awareness among voters about the proper use of the biometric system are essential for its successful implementation.

Working of Arduino board

1. Microcontroller: The heart of the Arduino is a microcontroller (usually an AT mega series chip). This chip is responsible for executing the program (sketch) you write.
2. Digital and Analog Pins: The board has digital pins (for binary signals) and analogy pins (for analogy signals). These pins can be used to read inputs or send outputs to various components like sensors, LEDs, or motors.
3. Power Supply: Arduino boards can be powered through USB or an external power source. They usually operate at 5 volts.
4. USB Connection: The USB connection allows you to upload your code from your computer to the Arduino. It also provides power and can be used for serial communication.
5. Voltage Regulator: Ensures a stable and consistent voltage supply to the components connected to the board.
6. Clock Crystal: Provides the timing reference for the microcontroller's operation.
7. Reset Button: Pressing this button restarts the code execution on the Arduino.
8. LEDs: There are often built-in LEDs on the board, such as the power indicator and a pin 13 LED that can be controlled in your code.
9. Programming Interface: The Arduino IDE allows you to write code in a simplified C/C++ language, compile it, and upload it to the board.

Code working:

Creating a full-fledged biometric voting machine using Arduino would be quite complex and potentially controversial due to security and reliability concerns. However, I can provide you with a basic outline of what such a system might entail:

1. Hardware Setup: - Arduino board (e.g., Arduino Uno)- Biometric sensor (e.g., fingerprint scanner)- Keypad for voter input- LCD display for instructions and feedback- Push buttons for navigation and confirmation

2.Software:- Set up the Arduino IDE and necessary libraries for the biometric sensor.- Write code to initialize the components and establish communication with the biometric sensor, keypad, LCD, and buttons.- Implement functions for:- Enrolling new voters' fingerprints.- Verifying voters' fingerprints during the voting process.- Handling voter input and navigation through the voting process.- Recording votes securely and accurately.- Displaying appropriate messages and feedback on the LCD.- Implement security measures to ensure the integrity of the voting process, such as encryption of data and secure storage of votes.

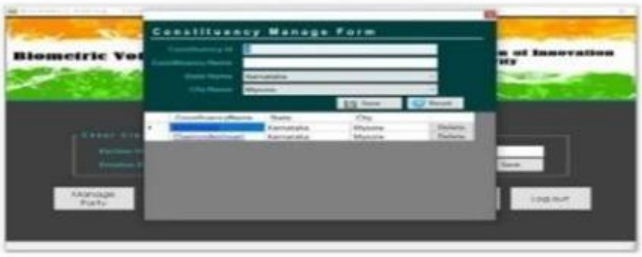
3. User Interface: - Design a user- friendly interface for voters to interact with the machine. - Display instructions and prompts on the LCD Use the keypad and buttons for voter input and navigation.- Provide feedback to voters about the success or failure of their actions.

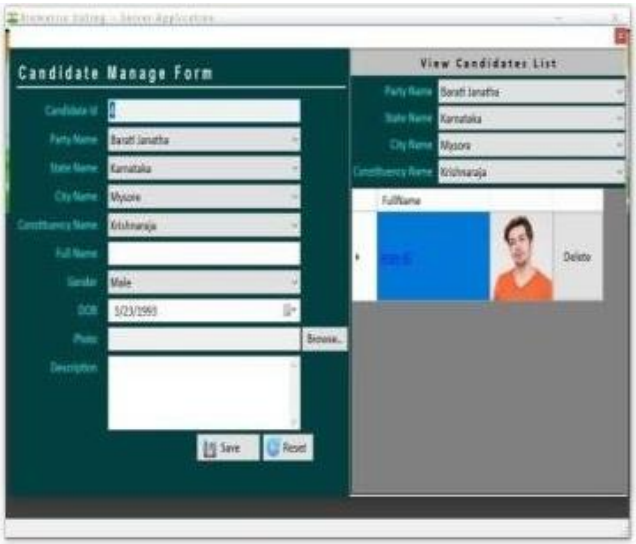
4.Testing and Deployment: - Test the system extensively to ensure reliability, accuracy, and security. - Conduct trials with a small group of users to gather feedback and identify any issues Address any issues or concerns raised during testing Deploy the voting machine in a controlled environment, such as a mock election or demonstration, before considering real-world use.

5. Regulatory and Ethical Considerations: - Ensure compliance with relevant laws and regulations governing voting systems Address ethical concerns related to privacy, security, and fairness in the voting process Consider the implications of using biometric data for voter identification and authentication. Remember, developing a biometric voting machine is a significant undertaking that requires careful consideration of technical, legal, and ethical factors. It's essential to prioritize accuracy, security, and

transparency to maintain the integrity of the democratic process.

IV. RESULT





V. CONCLUSION

In conclusion, the implementation of a biometric voting system holds the potential to enhance electoral integrity by providing a secure and efficient means of verifying voter identities. Despite the benefits, careful attention must be given to addressing technical challenges, ensuring accessibility, and safeguarding privacy to maintain public trust and uphold democratic principles. Ongoing scrutiny and iterative improvements are essential for the successful integration of biometric voting systems into electoral processes.

VI. REFERENCES

[1]. F. Thompson, B. K. Alese, O. S. Adewale and O. S. Falaki – Proceedings of the International Conference on Software Engineering and Intelligent Systems 2010, July 5th9th, Ota, Nigeria. pp. 168, 2010

[2]. Akinyemi Aminat E. – "Biometrics Based E-Voting System", April 2014. A 2012/2013 Computer Science Department Final Year Project, University of Ibadan

[3]. Alaguvel R., Gnanavel G., Jagadhambal K. – "Biometrics using Electronic Voting System with Embedded Security", pp. 1065, 2013

[4]. Alina, K. – "Comparison of Various Biometric Methods", Interactive Multimedia Systems, Electronic and Computer Science, University of Southampton. pp 2, 2010

[5]. Altun A.A, Kocer H.E, Allah Verdi, – "Genetic algorithm based feature selection level fusion using fingerprint and iris biometrics", International Journal Pattern Recognition

[6]. Artificial Intelligence. (IJPRAI), 22(3): 585-600, November 2008.

[7]. Bolle, R., Connell, J., et al. Guide to Biometrics, Springer. 2003

[8]. Davide Balzarotti, Greg Banks, Marco Cova, Viktoria Felmetsger, Richard Kemmerer, William Robertson, Fredrik Valeur, and

Giovanni Vigna “An Experience in Testing the Security of Real-world Electronic Voting Systems” pp. 5, 2010

[9]. Kashif H.M., Dileep Kumar and Syed Muhammad Usman, “Next Generation A Secure EVoting System Based On Biometric Fingerprint Method” 2011 International Conference on Information and Intelligent Computing IPCSIT vol.18 (2011) pp .26-27

[10]. Krimmer, R., Triessnig, S. and Volkamer, M., “The Development of Remote E-Voting around the World: A Review of Roads and Directions”. Springer Lecture Notes in Computer Science, Volume 4896/2007, pp. 1-15, 2007