Smart voting system using Face Recognition

Nandan Gowda S H[1], Jayam Haresh Tharun[2], Ashik B N[3], Deepak Lamani[4],

Priyadarshini J Patil A[5]

[1-4]Student, Dept. of Electronics and Communication Engineering, KSIT, Karnataka, India
[5]Asst. Professor, Dept. of Electronics and Communication Engineering, KSIT, Karnataka, India

---

Abstract - Elections are fundamental defining characteristics of any democracy that is being governed by the people expressing their choices or articulate opinions in the form of voting. Now the voting mechanism have evolved from leaps and bounds of simple hand written ballots to online voting systems. This project aims to build a smart voting system using face recognition technology that allows any voter in INDIA by going to their respective constituency from "**ANYWHERE IN INDIA**" to the nearest voting booth in the place of stay. This project is used to maintain High level biometric security. The voter details are stored in server database. Before entering the voting process the person should stand in front of the PC, the camera will read the image of the voter. After reading the details the microcontroller sends the details to the web application through the serial port. The web application software maintains the person database. In the "smart voting system" once a person casts his vote, the webpage gives the confirmation message that the vote is successfully registered and if a person's age is less than 18 years of age if he tries to vote once again using his face sample, the web page will display that he is not eligible to vote. The election commission can login and check the results of the Election after the voting process is completed, also it can reset the votes and update the candidate results every year.

1. INTRODUCTION

India is a Democratic country every citizen above 18 years of age is eligible to elect their leaders. When a person attends the age of 18 has the constructional right to voluntarily enrole for voter id given by the Indian Election Commission (IEC). Nowadays with the rise in population the need for checking the validity of the voters has become a problem. As the modern communications and Internet, today are almost accessible electronically, the computer technology users, brings the increasing need for electronic services and their security. This new technology refers to electronic voting systems where the election data is recorded, stored and processed primarily as digital information. Therefore, the necessity of designing a secure e-voting system is very important. Usually, mechanisms that ensure the security and privacy of an election can be time-consuming, expensive for election administrators, and inconvenient for voters.

2. PREVIOUS WORK

[1] In the paper ''SEVEP: Verifiable, secure and privacy preserving remote polling with untrusted computing devices" author "AMNA QURESHI", describes, designing a polling system that provides flexible polling, device fingerprint to allow multi-factor authentication for different devices used by the voter, zero-watermarking of polling code sheets, and generation of polling tags. More specifically, the main contributions of this paper are as follows:

Unlike most of the remote voting schemes, a 3layeredauthentication scheme is designed to provide access tone authenticated voter only. The proposed multi factor authentication scheme employs device fingerprinting to recognize the computing device that the voter is utilizing to login. Based on the results of the fingerprint the voter is required to input his/her authentication factors (possession, biometric) to establish his/her identity.

[2] In the paper "Secure and Hassle Free EVM through deep learning face recognition" author "Ishani Mondal", proposed a face recognition based on the features extracted by a convolutional neural network from the captured image of a voter. If the captured image's features match with those existing images stored in the database, the result is considered as positive and the voter is asked to cast vote for a political party. Once the vote has been casted, all the facial alignment details pertaining to the voter gets deleted from the system, so that if the same voter comes for voting, the system detects the maliciousness and prevents it instantly.

[3] In the paper "VOT-EL: Three Tier Secured State-Of-The-Art EVM Design Using Pragmatic Fingerprint Detection Annexed With NFC Enabled Voter -ID Card" author", Anooshmita Das", proposed design, the viability study of the emerging technology NFC, in conjunction with biometric is done. This technology allows communication between the NFC card and the device equipped with the reader when they are brought together within less than five centimeters apart in a very secured and reliable manner, which ebbed the complicacy and preventing from the malicious attacks or frauds. Once the user is verified, the person can proceed to the next level of biometric authentication. To make the system more stringent and robust, another layer of security is

reinforced through the use of biometric fingerprint identification as every individual has unique fingerprints. Biometrics is the science and technology that deals with analyzing the biological information or data. Biometric logistics operates by procuring fingerprints from an individual, then decoction of a feature set from the acquired data, and comparing this feature set with reference to the template set stored in the database. Using fingerprint matching is very reliable and popular biometric technique in personal identification process as it generates solemnity while stressing on building or cultivating voter confidence.

[4] In the paper "Secure and Electronic polling system", the authors AMNA QURESHI, DAVID MEGÍAS, HELENA RIFÀ-POUS described Se-VEP, an electronic polling system for small to medium sized Internet based public opinion systems that provides privacy of vote, voter's anonymity, voter's authentication, auditability, poll integrity, security against coalition of malicious parties, double-voting prevention, fairness, and coercion resistance, and prevents malware infected voting device from manipulating the authenticated voter's voting choices. In addition, Se-VEP provides cast-as-intended verifiability based on cryptographic primitives, which are used to design a complex voting interaction between the voting device, the polling server, the code generator and six polling code generators during the polling phase. Compared to the other state-of-the-art e-voting systems, Se-VEP ensures voter's authenticity via multifactor authentication scheme, supports multiple voting, prevents double voting through a polling tag, offers verifiability in the presence of an untrusted voting device, requires less trust assumptions on involved entities, and offers computationally feasible solution for implementation on portable communication devices.

[5] In the paper "VOT-EL: Three Tier Secured StateOf-The-Art EVM" the authors Anooshmitha das and Manash Pratim dutt, Designed Using Pragmatic Fingerprint Detection Annexed with NFC Enabled Voter -ID Card The best solution to diminish corruption is to augment voting machines with a proper auditing trail. Auditing is one of ways to discover patch security holes to uncover specific vulnerabilities. This model guarantees that the voter is not a deceitful rogue. This designed proposal is ubiquitous for biometric capture and using NFC tag which adds security and privacy, is a small contribution towards conducting an unprejudiced and fair election. This model satisfies the democracy, anonymity (privacy), reliability, accuracy and usability criterion. This model shows potential to reengage all demographic age groups to participate in elections and cast their votes.

[6]In the paper "A Secure Verifiable Ranked Choice Online Voting System Based on Homomorphic Encryption", the authors Xuechao Yang, Xun Yi, Surya Nepal, Andrei Kelarev, and Fengling Han proposed a secure voter verifiable e voting system, which allows the voters to cast their ballots by assigning arbitrary numbers of points to different candidates. This means that the voters can assign equal points to different candidates, and they are also allowed to assign different points to different candidates. Our system incorporates the distributed ElGamal cryptosystem. Each cast ballot is encrypted before submission and remains encrypted at all times. The additive homomorphic property of the exponential ElGamal cryptosystem enables effective processing of the ciphertexts during these procedures. Furthermore, the eligibility of voters and their submissions can be verified by anyone without the contents of the ballots being revealed. The security and performance analysis not only confirm the feasibility of our online voting system for practical elections, but also demonstrate that it has achieved significant improvements over other systems considered previously. It is a limitation of our system is that we have to assume that at least one authority is honest, since otherwise the system is not secure. In future work, we plan to address this issue and potentially could consider further generalizations.

3. PROPOSED SYSTEM

This project aims to build an Aadhaar and Web based Voting System using Face Recognition. This project is used to maintain High level security. The voter details are stored in database in computer. Before entering the premises that person should swipe RFID card on to RFID reader, the RFID reader sends a character associated with the RFID card. After sending the character to the Arduino UNO, the Arduino UNO uploads the character to MAT Lab.After receiving the character from Arduino UNO the MAT Lab asks for face authentication if the character obtained from the MAT Lab and the Arduino UNO is same then he is valid person, he will be allowed to vote. In this project we can overcome the problem prevalent in the existing system, such as proxy votes, missing identity, security, high cost and helps people to vote from any booth to his respective constituency.

To overcome above stated problems we are proposing a voting system which is more secure, time saving and provide two level of authentication by electronic means based on individual Face pattern recognition of voters. The new system will use face pattern of the voter as authentication by which at the time of election if scanned face pattern data of the voter matches with that of saved in the system then he is allowed to vote otherwise he is rejected a reported as fake voter and law breaker.

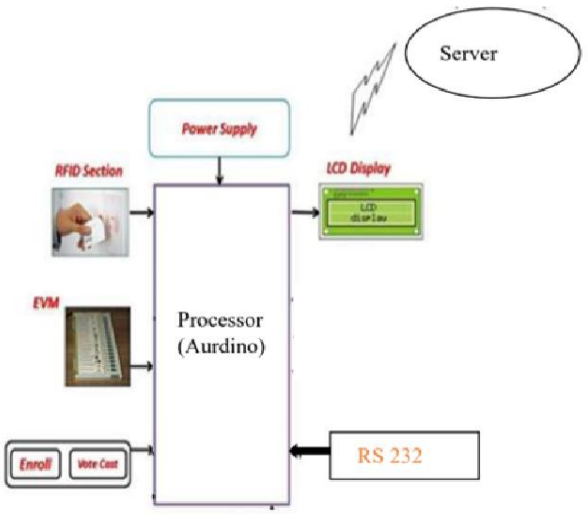

Fig 1: Block diagram of smart voting system

Face pattern properties of any individual are unique universally, which cannot be matched with anybody like fingerprint, iris, gaits, voice, face etc . The proposed approach is time saving and provides much better authentication from paper based authentication.

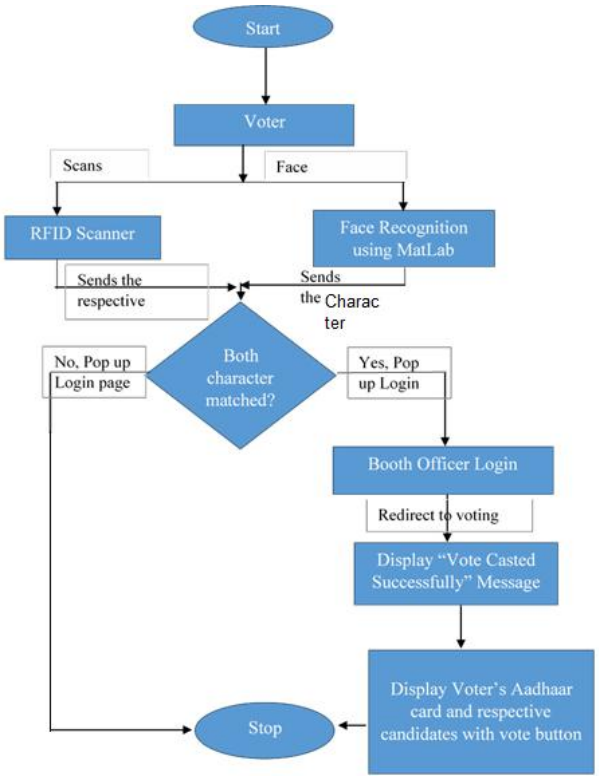

Fig 2: Flowchart for the proposed system

Once the voter enters the booth. He/She need go through first mode of authentication i.e, RFID reader, where he need to scan the his RFID card which sends the respective face which is stored in the data base to arduino and then allows second mode of authentication i.e, face recognition using matlab. The new system will use face pattern of the voter as authentication by which at the time of election if scanned face pattern data of the voter matches with that of saved in the system then he is allowed to vote otherwise he is rejected a reported as fake voter and law breaker. Once the face is matched then the login page with start button will be displayed indicating that the voter can proceed to vote. Once the vote is casted, The message 'vote casted successfully' will be displayed. If the user tries to vote for the second time, then the message 'already voted' will be displayed.

Description of Components

A. Arduino Uno

Each of the 14 digital pins on the Uno can be used as an input or output, using pin mode (), digital write (), and digital read () functions. They operate at 5 volts.

Each pin can provide or receive 20 mA as recommended operating condition. A maximum of 40mA is the value that must not be exceeded on any I/O pin to avoid permanent damage to the microcontroller. In our project, the Arduino is used as the main microcontroller for receiving the data from the RFID module and it also receives the face data using the mat lab and compares it with face of the user. If the data matches, then it allows the user to cast the vote.

B. LCD Display

A LCD is a flat-panel display or other electronically modulated optical device that uses the light modulating properties of liquid crystals. Liquid crystals do not emit light directly, instead using a backlight or reflector to produce images in color or monochrome. The options for selecting automatic and manual mode of the meter is made available on this LCD Display. Once the RFID reads the data, the LCD will display the user data.

C. RFID

The RFID technology is a means of gathering data about a certain item without the need of touching or seeing the data carrier, through the use of inductive coupling or electromagnetic waves. The data carrier is a microchip attached to an antenna (together called transponder or tag), the latter enabling the chip to transmit information to a reader (or transceiver) within a given range, which can forward the information to a host computer. One important feature enabling RFID for tracking objects is its capability to provide unique identification. An RFID system has four basic

components: A tag which is composed of a semiconductor chip and an antenna. An interrogator (sometimes called a read/write device), which is composed of an antenna, a RF electronics module, and a control electronics module. It is used for first mode of authentication. The voters are provided RFID cards which has unique code for authentication.

D. Power Supply Unit

The circuit needs two different voltages, +5V & +12V, to work. These dual voltages are supplied by this specially designed power supply. The power supply, unsung hero of every electronic circuit, plays very important role in smooth running of the connected circuit. The main object of this 'power supply' is, as the name itself implies, to deliver the required amount of stabilized and pure power to the circuit. The stabilization of DC output is achieved by using the three terminal voltage regulator IC. This regulator IC comes in two flavours : 78xx for positive voltage output and 79xx for negative voltage output is as shown in Fig.3.12. For example, 7812 gives +12V output and 7912 gives -12V stabilized output. These regulator ICs have in-built short-circuit protection and auto-thermal cut- out provisions. If the load current is very high the IC needs 'heat sink' to dissipate the internally generated power.

4. RESULT

The proposed system allows the voter to vote from anywhere using RFID and face authentication. Here the voter no need to go for a particular to vote for particular candidate. By visiting nearest booth the voter can vote to his own constituency rather than visiting the constituency. This system avoids voting multiple times by the same voter and thus helps to avoid malpractice.

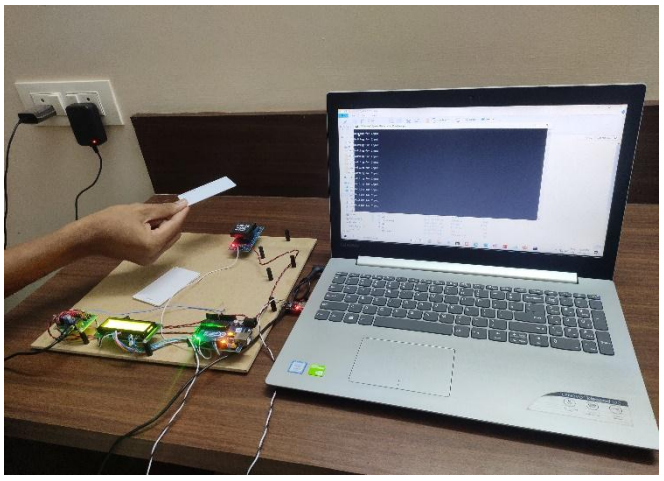

Fig 3: RFID Authentication

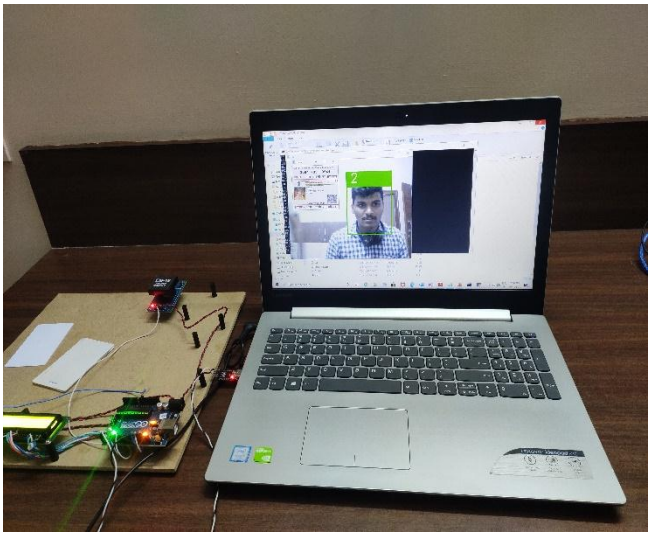

Fig 4: Face Authentication

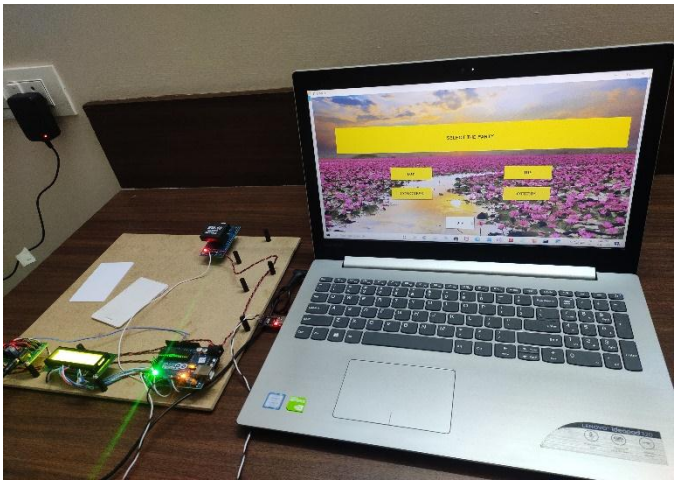

Fig 5:Party details display

5. CONCLUSIONS

The proposed method is to develop a secure internet voting system based on face recognition which tried to overcome all the drawback occurs in traditional or current voting system. The proposed system has many strong features like correctness, verifiability, convenience etc. For this system no requirement of an election officer, paper ballot or any electronic voting machine only the internet connection and Face scanners are required one can vote from anywhere securely.

The proposed system provides two phase of authentication. First is through RFID and second is Face Recognition. In this system no voter can vote twice because the voter Facial patterns will be linked to their Aadhaar Card. So that any user tries to vote twice with some other person's RFID card it is not possible due to RFID linked to the Aadhaar card and the respective Facial Patterns stored in data storage will not be matched with the Voter trying to voting with some other person's RFID.

6. REFERENCES

1. AMNA Qureshi ‘‘SEVEP: Verifiable, secure and privacy preserving remote polling with untrusted computing devices,” in Future Network Systems and Security Feb 22(2019)IEEE.

2. Ishani Mandal “Secure and Hassle Free EVM through deep learning face recognition”.16th Feb(2019)IEEE.

3. Annoshmitha Das “VOT-EL: Three Tier Secured State-Of-The-Art EVM Design Using Pragmatic Fingerprint Detection Annexed with NFC Enabled Voter -ID Card”(2016)IEEE

4. Shekhar Mishra and Y. Roja Peter - “Electronic Voting Machine using Biometric Finger Print with Aadhar Card Authentication” , International Journal of Engg. Science and Computing ,March 2018.

5. R. Murali Prasad and Polaiah Bojja- “Aadhar based Electronic Voting Machine using Arduino”, International Journal of Computer Applications. July 2017.

6. G. Keerthana and P. Priyanka - “Impressive Smart Card Based Electronic Voting System”, International Journal of Research in Engineering and Technology , March 2017.

7. Trupti Umakant Pavshere and S.V.More – “A Survey on Secured E-Voting System Using Biometric”, International Journal of Advanced Research in Science, Engineering and Technology, March 2016

8. Firas I. Hazzaa, Seifedine Kadry and Oussama Kassem Zein - “Web-Based Voting System Using Fingerprint Design and Implementation”, International Journal of Computer Applications In Engineering Sciences.