

Smart voting system using Face Recognition

Nandan Gowda S H¹, Jayam Haresh Tharun², Ashik B N³, Deepak Lamani⁴, K S Priyadarshini Patil A⁵

¹⁻⁴Student, Dept. of Electronics and Communication Engineering, KSIT, Karnataka, India

⁵Asst. 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’s age becomes 18 they have the constitutional right to voluntarily enroll for voter id given by the Indian election commission(IEC). Aadhar card is used as Voter ID so we don’t need separate card for voting.

Citizens who miss out to enroll their vote during the election time due to the negligence in voting because voter is not ready to travel such a distance. To avail constitutional voting right to every citizen, “Smart voting system” is best solution. Nowadays with the rise in population the need for checking the validity of the voters has become a problem. Nowadays as the modern communications and internet are accessible electronically. Usage of new technology in the voting process improve the election process. The new technology refers to electronic voting systems where the election data is recorded, stored and processed primarily as digital information. In the past usually information security was used mostly in military and government institutions. But now this type of security is growing every day. In computing e-services and information security it is necessary to ensure that data communications or documents are enough secure and privacy enabled. Advances in cryptographic techniques allow pretty good privacy on e-voting systems. Security is a heart of e-voting process. 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. LITERATURE SURVEY

[1] In “AMNA QURESHI” [1], this paper 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 3- layered authentication 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 “Ishani Mondal”, this Usually a face recognition module comprises of the following

In this paper we have 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 “Anooshmita Das”, In this 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 SeVEP, 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, SeVEP 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, SeVEP 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.

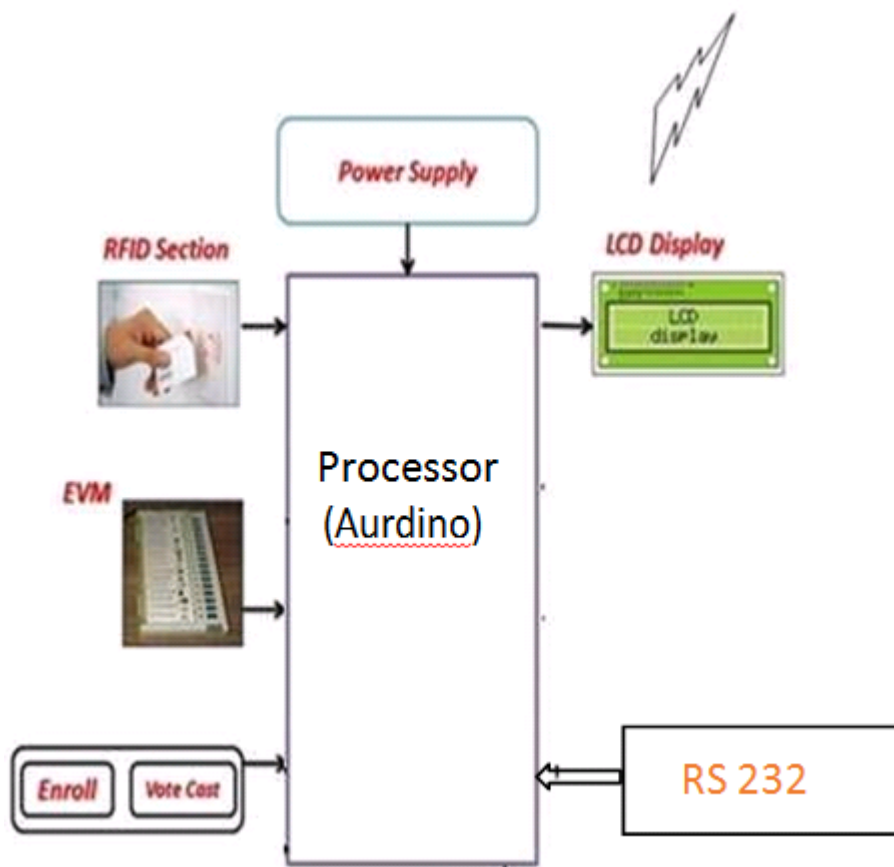
[5] In the paper “VOT-EL: Three Tier Secured State- Of-The-Art EVM” the authors Anooshmitha das and Manash Pratim dutt, Designed Using Pragmatic Fingerprint Detection Annexed with NFC Enabled Voter -ID Card The best solution to diminish corruption is to augment voting machines with a proper auditing 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 re- engage 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.

[7] In the paper “Towards Secure E-Voting Using Ethereum Blockchain”, the authors Ali Kaan Koç, Emre Yavuz, Umut Can Çabuk, Gökhan DalkÖlÖç succeeded in moving e-voting to the blockchain platform and we addressed some of the fundamental issues that legacy e-voting systems have, by using the power of the Ethereum network and the blockchain structure. As a result of our trials, the concept of blockchain and the security methodology which it uses, namely immutable hash chains, has become adaptable to polls and elections. This achievement may even pave the way for other blockchain applications that have impact on every aspect of human life. At this point, Ethereum and the smart contracts, which made one of the most revolutionary breakthroughs since the blockchain itself, helped to overturn the limited perception of blockchain as a cryptocurrency (coin), and turned it into a broader solution-base for many Internet-related issues of the modern world, and may enable the global use of blockchain. E-voting is still a controversial topic within both political and scientific circles. Despite the existence of a few very good examples, most of which are still in use; many more attempts were either failed to provide the security and privacy features of a traditional election or have serious usability and scalability issues. On the contrary, blockchain-based e-voting solutions, including the one we have implemented using the smart contracts and the Ethereum network, address (or may address with relevant modifications) almost all of the security concerns, like privacy of voters, integrity, verification and non-repudiation of

votes, and transparency of counting. Yet, there are also some properties that cannot be addressed solely using the blockchain, for example authentication of voters (on the personal level, not on the account level) requires additional mechanisms to be integrated, such as use of biometric factors. The prominence of distributed systems stands out especially when considering the mitigation of the risk that storing the registrations at a central location (office). This can always somehow allow officials to have the opportunity to physically access to the vote records, which could lead to corruptions and cheatings by the authorities.

3. BLOCK DIAGRAM



4. 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 three phase of authentication. First is through QR Code and second is Fingerprint and Third 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 QR code it is not possible due to QR 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 QR code. Also the proposed method provides the voter to vote from any region with in India to their Residential Constituency from the nearest Voting Booth with a secure voting process without neglecting to vote.

5. REFERENCES

- a. Ishani Mandal “Secure and Hassle Free EVM through deep learning face recognition”.16th Feb (2019) IEEE.
- b. Qureshi “SEVEP: Verifiable, secure and privacy- preserving remote polling with untrusted computing devices, “in Future Network Systems and Security Feb 22(2019) IEEE.

- c. 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
- d. 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.
- e. R. Murali Prasad and Polaiah Bojja- “Aadhar based Electronic Voting Machine using Arduino”, International Journal of Computer Applications. July 2017.
- f. G. Keerthana and P. Priyanka - “Impressive Smart Card Based Electronic Voting System”, International Journal of Research in Engineering and Technology, March 2017.
- g. 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
- h. 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.