International Journal of Engineering & Technology, 7 (4.19) (2018) 586-588

SPC

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Secured Voting System with Multimodal Biometric Technique using ANN

Payal Deora[1], Abhishek Kumar[2], Gayathri.M[3], Malathy.C[4]

[1,2]Student/CSE, [3]AP / CSE, [4]Professor, CSE,
[1,2,3,4]SRM Institute of Science and Technology, Chennai

Abstract

Free and fair elections play a major role to explicate a democratic government, but all too frequently, the actual mechanics of election has always been taken for granted in our country, the largest democracy in the world. The issue of security is very prominent in any system such as the current electoral voting system. There is no proper record of people who have already casted their vote. The voter Id card does not have any record of biometrics of the voter, so we cannot guarantee genuine voting hence creating chances of bogus voting. Therefore, we intend to aid in security of voting system by bringing advanced technologies of neural networks with multimodal biometrics (face recognition, fingerprint scan, retina scan etc). As these biometrics of a person is already recorded in their Aadhar card, so it can be used as database. At the time of voting, biometric information of a voter will be gathered and will be matched to the database obtained by Aadhar card so that the person can be identified correctly. The proposed new voting system with multimodal biometrics can help any democratic government in conducting smooth election by removing all the ambiguities and security issues of current scenario. ‘

1. Introduction

India is the largest democracy with parliamentary system of government which requires free and fair elections for the country to choose its representative. In the current voting system, positive identification of a person is made manually based on the voter card of the voter. The identified voter is than allowed to cast their vote through EVM. The identification is very ambiguous as it requires manual verification of the person. As the voter card can be easily duplicated, it creates a chance of fake voting. In this paper we propose a new method of voting which will remove all the ambiguities of the antiquated method. We tend to introduce voting using multimodal biometric techniques (i.e. face recognition, fingerprint scan, retina scan etc). This can be accomplished using Aadhar card of an individual as it contains all the biometric details of a person. The implementation of the model will be explained in the later sections.

2. Issues in Current System

➢ **Bogus Voting**: As it is very easy to duplicate voter card, fake voter are set unidentified which leads to bogus voting.
➢ **Vulnerability to Hacking**: EVM are not end to end encrypted which allows manipulation in counting of votes.
➢ **Humanistic Failure**: Manual identification increases the probability of errors cause by humans.
➢ **Sluggish Process**: Manual counting of votes casted is time consuming which delays the election result. Also offline voting requires lots of paperwork to be done.
➢ **Adroit Employees**: Loads of humans should be fully trained before getting employed for election duties so as to decrease human errors.
➢ **Susceptibility to fraud**: Due to lack of security, there are chances of stealing of votes hence altering election results.

3. Existing Research Work

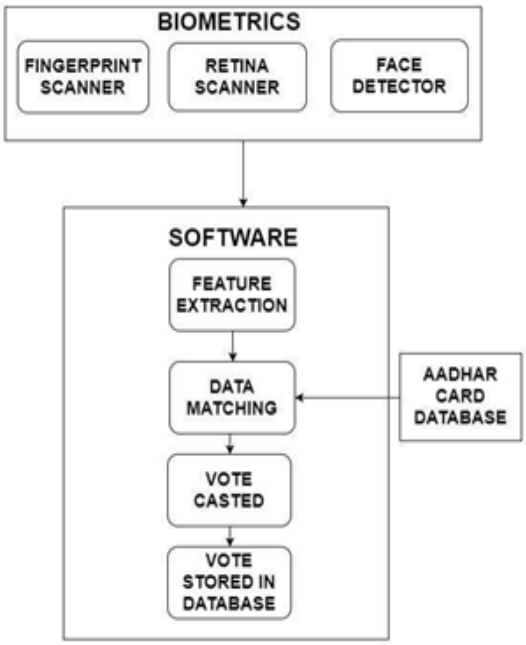
The paper [1] has proposed a model in which before the voting day they have to create a database of all the voters. Also it has been proposed to cross-check the result with manual voting which in turn is doubling the work. On the contrary our model is much simpler to use as we are using Aadhar card database and hence we need not build any extra database.
The paper [2] has proposed voting using Arduino which includes a lot of hardware and also there is no way to store the casted votes and there is no system to count the votes, hence the arduino based voting can not be implemented in the current voting system whereas our proposed system overcomes these drawbacks. Votes are encrypted and also there is a counting mechanism which reduces the human work and therefore
reducing humanistic errors.
The paper [3] has proposed a Model where the Voter has to register through Aadhaar Card Number, name, email, mobile number and other relevant details. Voter has to introduce himself through biometric data for the first-time login only. No such authentication details are required further. Voter has been provided a QR code by admin to login but this QR code is transferable, if secrecy of the “above mentioned” Code is kept open. On the contrary our model redirects to voting page directly after the successful biometric authentication processor.

The paper [4] has proposed a model which is Biometrically authenticated using a Unimodal biometric system i.e. Fingerprints only. Unimodal biometric systems comprises of several limitations like: noisy data, spoof attacks, non-universality, intra-class variations, limited degrees of freedom, and high unprecedented error rates.
Most of these can be eliminated by deploying multimodal biometric systems. To Corroborate this various research works are going on, which is a proof of itself.
This paper discusses the various aspects that are plausible in multimodal biometric systems. Multimodal biometric systems capitalizes such integration strategies by blending together to put forward a condensed form.
The Paper [5] has proposed a system taking Vein Pattern as parameter, involves tedious and exhaustive trot. In this cumbersome method, in order to cross check the voter's authentication, Database for every voters needs to be prepared before voting date, which in turn is doubling the work. On the contrast our model is much simpler to use as we are using Aadhar card database and hence we need not build any extra database.

4. Biometrics

Biometric is a verification and identification system based on the physiological or behavioural characteristics of a human being. Finger-scan, Facial-scan, Iris-scan, Retina-scan, Hand-scan are considered as physiological characteristics whereas Voice-scan and signature-scan are considered as behavioural characteristics. In the biometric literature, these characteristics are referred to as traits, indicators, identifiers, modalities. Besides bolstering security, this system also enhances user convenience by alleviating the need to design and remember passwords.

5. Block Diagram of Proposed System

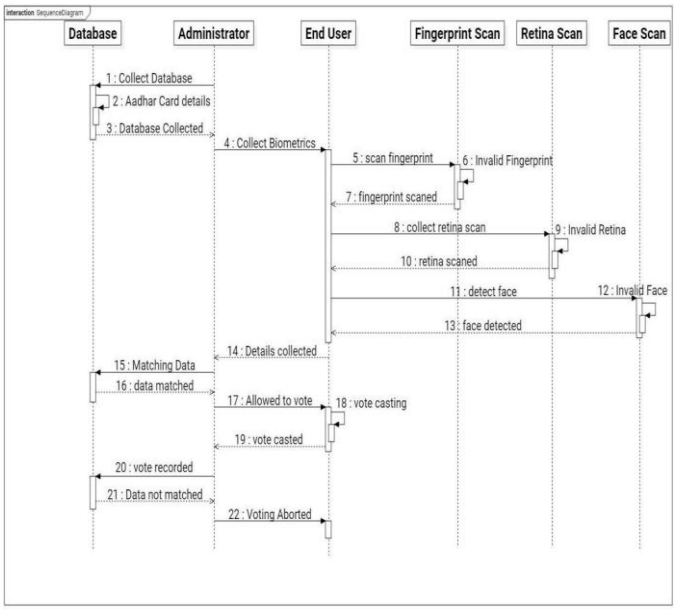


5.1. Components Used:

Biometric Device:
Biometric device is the first component used in this system. It is the scanner which will scan physical characteristics of the voter and will collect the data. This machine is now a days available in any store or online shopping malls at a very cheaper price.

All the three biometrics i.e. face, iris and fingerprint are sometimes scanned by single device otherwise maximum devices can scan face and finger at the same time and for iris scan different device can be used. The hardware components of the device includes platen referred to as scanner which is used to scan fingerprint. CCTV camera required to capture the image of face. Iris scan deployments require special devices that provide necessary infrared illumination**.**

System Architecture: Sequence Diagram of the System:



6.1 Methodology

Software is the main implementation part of the system through which all the process of voting has been done. All the features of the software are listed as follows.

- **Collect Database:**

As the voter will enter the environment to caste his vote he will be firstly providing his Id proof i.e. Aadhar card. Instead of entering 16-digitAadhar number, Aadhar card has an in built QR code which allows user to scan it and access the stored information. The stored biometric information will be extracted from the Aadhar card.

- **Collect biometrics:**

For ensuring that the person is genuine biometrics of the person has to be collected using the biometric device discussed above. There are five stages involved in scanning and matching of data:

1. Image acquisition: It is very important to acquire high quality image. Fingerprint quality varies from person to person. High resolution image required for facial and iris scan.

2. Image processing: After acquiring high quality image, it must be converted into usable format. Colour of the image is usually converted to black and white.

3. Distinctive Patterns: Core distinctive features such as swirls, loops, arches for fingerprint, nose shape, cheekbone etc for facial and rings, furrows, corona etc for iris of person are identified for matching.

4. Template Creation: After the feature extraction process, a template associating all the features is generated. This template cannot be used to obtain original image.

5. Template Matching: Various algorithms are applied for the matching of features. If the features obtained from the voter gets matched with the database in the Aadhar card above the threshold then the person is declared genuine and hence he is allowed to vote.

➢**Vote Casting:**

After the biometric details of the person are matched with the details stored in the database, voter will be able to see all the parties on the screen and will be allowed to vote. The voter can click the button of the favoured party.

Every party will be associated with a variable count which will indicate the number of votes casted to that particular party i.e. the number of times the button of the party is clicked. Initially the count of each party will be zero as the button of the party is not yet pressed. As and when the voter presses the button of the voted party the variable count of that party will get incremented by one and count of other parties will remain the same. So simultaneously the count of the associated party will increase when the button associated with that party has been clicked.

When the button is clicked, the number of times that particular button is clicked will be incremented in the database indicating that vote has been casted to that party.

This count will be end to end encrypted and hence there is no chance of fraud. At the end of the elections, the count of all the parties will be decrypted. The party which has the maximum count will win. For eg if count of a party 'X' is 10,000 means 10,000 votes has been casted to the party 'X'.

There will be no manual counting of votes. This system will help automatic counting of votes, based on how many times button of a particular party has been clicked.

7. Advantages of Proposed System

➢ **Increased Security:** Other security measures i.e. the passwords and the pins can be easily guessed as many users uses very obvious sequence for building them. In contrast biometric information of an individual cannot be stolen or shared, hence increasing the level of security then the traditional methods.

Successful login leads to biometric verification and the redirected to the voting page. unauthenticated suspicious activity signals criminal offenses (encircling the particular) and the same is sent to security personnel to alert. If a person is forced to cast his vote as per someone's' will, not his own, the model leads to generation of SOS signal automatically.

As the votes are fully encrypted even in case of Extreme condition (like Booth Capturing) a single data/datum to be altered is arduous.

➢ **Uniqueness:** Every individual has its unique physical characteristics, therefore satisfying the uniqueness property in biometric system.

➢ **Increased Convenience:** Majority of users chooses universal password so that they do not forget multiple passwords, but it increases the risk to security. On the other hand, physical characteristics of a human can never be forgotten. Hence biometric system eliminates the problem of mugging multiple passwords, scanning of QR provides all the prerequisite user credentials, resulting in increased convenience.

8. Conclusion

Effective Implementation of "Secured Voting system with Multimodal Biometric technique using ANN" in totality is to provide a platform which is online, highly secured, transparent and easy (Fit for democratic mind. Nothing called "professional knowledge" is required to have a better and clear picture, Simple and highly enthusiastic as per our growing society.)

Safety and security of each and every procedure is of prime concern. All the above are in accordance with integrity sovereignty and fraternity of any democratic country.

References

[1] NighatAyub, Masood Ahmad World Academy of Science, Engineering and Technology "Usability and biometric authentication of electronic voting system" In International Journal of Computer and Systems Engineering

[2] Dr. S. Karthikeyan, J. Nithya "Secured Electronic Voting Machine Using Biometric" in International Journal of Scientific Research in Computer Science, Engineering and Information Technology © 2017 IJSRCSEIT | Volume 2 | Issue 2 | ISSN:2456-3307586

[3] Madhuri Mahajan, Yogeshwari Pawar, Madhuri Wagh, Prof.PuspenduBiswas, Sagar Alai, Prof. Shital More"M-Vote (Online Voting System)" inVolume 2, Issue 10, October 2017 ISSN(online): 2456-0006 International Journal of Science Technology Management and Research.

[4] S. Karthikeyan, J. Nithya "Biometric Secured Electronic Voting Machine with Embedded Security" in International Journal of Scientific Research in Science and Technology (IJSRST) | Volume 3 | Issue 1 | Print ISSN: 2395-6011 | Online ISSN: 2395-602X

[5] P.Santhosh Selvam, S.Surya Prakash L.Balaji "Advanced E-Voting System Using Finger Vein Sensor" in Asian Journal of Applied Science and Technology (AJAST) Volume 1, Issue 3, Pages 304-306, April 2017

[6] Biometrics (Identity Verification in a Networked World), Authors: Samir Nanavati,MichaelThieme, Raj Nanavati Wiley India Pvt. Ltd.