E- Voting System for Handicapped People Using Biometrics Security

Kirti Jain

Ambedkar Institute of Advanced Communications Technologies and Research Delhi, India
E-mail: kirti27jain@gmail.com

Abstract—*With the rapid growth of networks attacks and corruption in the economy results with the demand of secure voting to all the citizens so, that all citizens including handicapped people will also able to vote. In the present scenario, this is the worth coming challenge that there is no vote casting system available for physically challenged citizens. Current research on online voting will use only fingerprinting technology for biometrics. But this technique is not much effective for physically handicapped people who are not in the position to give fingerprint impression due to some disability reasons. The online voting system model is developed with multiple psychological biometrics scanning techniques. Effective electronic voting system is developed to fulfill the demand of physically challenged citizens such that reliable, robust and secure system is developed. In this article, we are going to propose the new online voting system with multiple Biometrics scanning which is suitable for physically challenged and non-physically challenged citizens.*

Keywords: *Physically challenged, voting, fingerprint,iris, retina.*

1. INTRODUCTION

The motive of presenting this paper is to propose an online voting model for physically handicapped people and more specifically this E-based voting systems supports multiple psychological biometrics security, allowing them to participate in an election from any location that provides internet access. The proposed model of voting should ask about the physically challenged citizens about their disability and the model will scan accordingly. Online Voting opens up new possibilities in order to bring a unique experience to the Voting process. E-Voting is about improving voter convenience and accessibility, improving accuracy and the security of the voting process and the rapid feedback of Election or Ballot Results. This e- Voting is ideal in the circumstances where there are say, in excess of 1,500 eligible voters. There are lot of advantages of this online voting model because this model will help to vote all the citizens of the country especially emphasis is given to physically challenged people.

In second section the existing systems are explained. In third section the proposed procedure along with flow diagram and algorithm is described. In section 4 and 5 the proposed architecture components with their working and biometric techniques used in proposed system are explained.

2. EXISTING VOTE CASTING SYSTEMS

2.1 Direct Recording Electronic [2] :

Direct Recording Electronic voting systems completely eliminate paper ballots from the voting process. Voters prove their identity and thereafter given a smartcard, that allows them to approach a voting terminal, enter the token, and then vote for the candidates of their choice. When their selection is complete, DRE systems will typically present a summary of the voter's selections, giving them a final chance to make changes. Subsequent to this, the ballot is cast and the voter is free to leave. The most fundamental problem with such a voting system is that the entire election hinges on the correctness, robustness, and security of the voting terminal and the software installed within each of the voting terminal. Also the complexity of resources involved does not reduce to a greater extent as there is a necessity to install this DRE system in each of the voting terminal.

2.2 The Idea of Gujarat e-voting system [3]

It is a well-established e-voting system. The main advantages of this system rest in the fact of non-traceability of the votes and voters authenticity being well established. The main intension, with which this system is proposed, is to reduce and minimize the cost incurred to the government to conduct an election. The main drawback that this system encounters is that the non-availability of the personal computers/laptop by any individual necessitates the set up of an e-pooling booth which might not reduce the cost of conducting an election in big deal. Also the assumption of existence of internet connection by any individual in the home draws the crowd towards the e-voting booth.

3. PROPOSED PROCEDURE FOR VOTE CASTING

The proposed electronic voting model provide support both the physically challenged and non-physically challenged citizens. This model uses the concept of multiple physiological biometrics security to check the authenticity, integrity of the users who cast the vote. This system also eliminates the possible "security gaps" in the administrative workflow may

result in deteriorating the overall security level of the system, even if the voting protocol implemented by the system succeeds to fully comply with the security requirements set for voting.

The following requirements of our E- voting model. [4]

- Only authorized voters can vote.
- No one can vote more than once.
- No one can determine for whom anyone else voted.
- No one other than the voter should be able to know who he voted for while he votes.
- Every voter can make sure his/ her vote has been taken into account.

3.1 Flow Diagram for Vote Casting System

The effective electronic voting system is developed to fulfill the demand of citizens such that reliable, robust and secure system is developed. We proposed the new online voting system with multiple Biometrics scanning for physically handicapped people. The algorithm of the proposed model (see Fig. 1). The flow diagram of the proposed model is that scan the voter –id of the candidate then it will ask for the candidate about the physical disability.
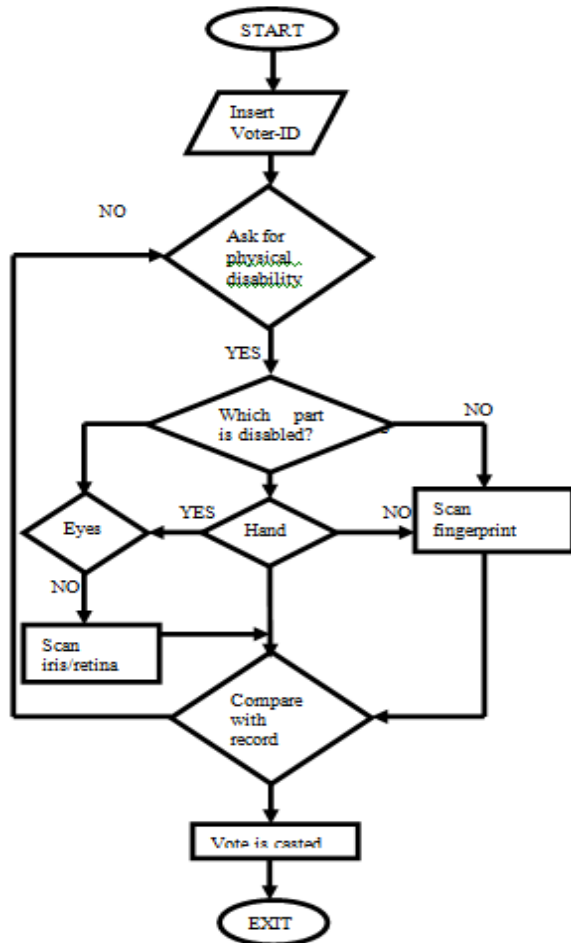
Fig. 1: Flow Chart of Proposed Model

If the candidate is physically challenged then only the area of physical disability is asked and if there is disability in hands then the system will scan the iris/retina as this comes under the physiological biometrics scanning and if the candidate do not have eyes then he/she will give the fingerprint sample as both iris/retina and fingerprint are comes under physiological biometrics.

3.2 Algorithm for Vote Casting

The algorithm of the proposed model has some steps which are explained in the following steps (See Fig. 2)

STEP 1: Input the voter-id/Aadhar Card.
STEP 2: Let category='Y' OR 'N'.
STEP 3: for (i=1;i<=n;i++)
{
If(category='Y')
{
Scan the biometrics details
}
Else
{
Scan the fingerprint impression
}
STEP 4: The Biometrics matching is done from the input_template to the stored_ template.
STEP 5: If (input_template == stored_template)
Then
Cast the vote and EXIT the system.
Otherwise go to step 1
Y category is for physically challenged people.
N category is for non-physically challenged people.
n is the number of registered authorized users

Fig. 2:Algorithm of the model

4. PROPOSED ARCHITECTURE COMPONENTS AND THEIR WORKING

The architecture of the system contains two modules front end and the back end .The front end interface is displayed to the user side and it has various options for all the citizens both the modules are interconnected to each other in order to provide the authentic electronic voting process. This system does not provide access to the un-authorized voters. [1]

4.1 The Front-End Server

The Front End component has Voter-ID/Aadhar Terminal, Ask for Physical Disability, Biometric recognition. The voter-ID /Aadhar card is inserted which in is interfaced to function with an LCD Display for its effective implementation. It has been designed in the way that a smart card is inserted into the terminal, then the computation on the smart card is being done to validate with the help of the central warehouse of smart card numbers obtained again from the back-end server and

thus the system will ask about the disability and then done the biometrics of the user according to the category of the user.

4.2 The Back-End Server

The Back End component used along with the Smart card /Aadhar card recognizing terminal is used to verify the biometrics impression of smart card holder against their respective smart card numbers from the configured entity at the election terminal. The design procedure of the module includes the verification of the biometrics Impression of the user using the cryptographic algorithm generates the message digest to verify the integrity and authenticity of data stored in the warehouse containing the biometrics impression against the smart card issued. So both the validity and authenticity of the user is completed only at this module. The central server has primary data repository for biometric matching and secondary data repository which store the message digest of VID and biometrics the secondary data repository is synchronized with the primary data repository to store the digest of vote cast by voter and their VID & smart card. This synchronization would be helpful in likely estimation process to retrieve the vote cast during the result declaration phase by comparing with the digest stored against the voter's Smart card Number and VID Digest from primary repository. The database is distributed to avoid the load on the server during the election process. The servers are given access only with the concern of the election commission authorities.

5. VARIOUS BIOMETRICS TECHNIQUE USED FOR VOTE CASTING

The biometrics techniques are of two type's behavioral and psychological biometrics. The behavioral biometrics change after some time so it is not stable .The psychological biometrics is a stable technique which cannot change with time. We are using the psychological biometrics techniques in this voting model to ensure the robustness, reliability and correctness of the system.

5.1 Iris/retina Recognition

This technique involve capturing a high quality picture of the iris or retina, using a digital camera and uses near infrared light. Iris recognition utilizes the iris muscle to perform verification. Retinal recognition uses the unique pattern of blood vessels on an individual's retina at the back of the eye.

Iris patterns are described by an IrisCode using phase information collected in the phasors. The phase characteristic of an iris can be described using 256 bytes of data using a polar coordinate system. Also included in the description of the iris are control bytes that are used to exclude eyelashes, reflection(s), and other unwanted data.

To perform the recognition, two IrisCodes are compared. The amount of difference between two IrisCodes — Hamming Distance (HD) — is used as a test of statistical

independence between the two IrisCodes. If the HD indicates that less than one-third of the bytes in the IrisCodes are different, the IrisCode fails the test of statistical significance, indicating that the IrisCodes are from the same iris. Therefore, the key concept to iris recognition is failure of the test of statistical independence.

5.2 Fingerprint Recognition

A fingerprint is the pattern of ridges and furrows on the surface of a fingertip. Ridges and valleys are often run in parallel and sometimes they bifurcate and sometimes they terminate. When fingerprint image is analyzed at global level, the fingerprint pattern exhibits one or more regions where ridge lines assume distinctive shapes. These shapes are characterized by high curvature, terminations, bifurcations, cross-over etc. These regions are called singular regions or singularities. These singularities may be classified into three topologies; loop, delta and whorl. At local level, there are other important features known as minutiae can be found in the fingerprint patterns. Minutiae mean small details and this refers to the various ways that the ridges can be discontinuous. A ridge can suddenly come to an end which is called termination or it can divide into two ridges which is called bifurcations. [6]

Some types of fingerprint are [8]:

a) Arches - Only represent five percent of the fingerprint patterns encountered. There no core or delta formations.
b) Loops - Constitute between 60-70 percent of the patterns found in fingers and have one delta formation and a core.
c) Whorls - Constitute between 25-35 percent of the patterns found in fingers and have two delta formations and a core.
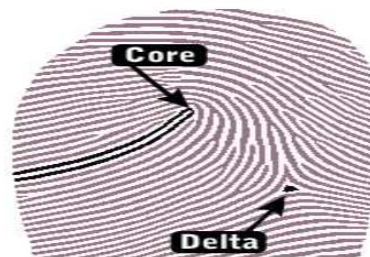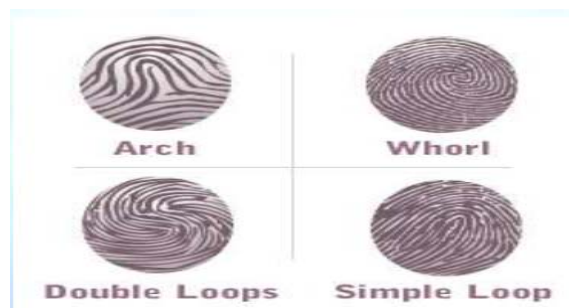

Fig. 2: Showing core and delta

Fig. 3: Types of fingerprint

6. CONCLUSION

We have tried to propose the model helps in maintaining the authentication, non-traceability and integrity of casted vote and security with confidentiality also being enforced. The current system is suitable for holding elections for computer literate only with fingerprinting impression. Gradually, as people become more educated and computers and internet become great part of our everyday lives, the whole electoral process of the nation can be brought online.

The proposed system is capable of denying access to any illegal voter/s, preventing multiple votes by the same voter, and blocking their vote .Moreover, the proposed voting system caters for the needs of the physically challenged voters by providing multiple biometrics scanning

7. FUTURE WORK

The proposed model will be implemented by developing the web interface using the web development languages and mobile online voting module is implemented for senior citizen users so that the time and resources of the users and pooling officers will be saved .The mobile voting system reduces the paper overhead and corruption in the democratic country.

REFERENCES

[1] S. Sridharan , "Implementation of Authenticated and Secure Online Voting System" in 4th ICCCNT July , 2013.

[2] A. D. Rubin. "Security considerations for remote electronic voting" Communications of the ACM, 45(12):39–44, Dec. 2002.

[3] Voting, "Gujarat online voting model system". Available: http://sec.gujarat.gov.in/e-voting-system.htm.

[4] S. Saini , Dr. J. Dhar ."An eavesdropping proof secure online voting model", International Conference on Computer Science and Software Engineering , 2008.

[5] C.Lambrinoudakis, S. Kokolakis, M. Karyda, V.Tsoumas, D. Gritzalis, S. Katsikas "Electronic Voting Systems: Security Implications of the Administrative Workflow", IEEE Proceedings of the 14th International Workshop on Database and Expert Systems Applications (DEXA'03), 2003.

[6] L. Paul, A. M.N ," Authentication for Online Voting Using Steganography and Biometrics" , International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 1, Issue 10, December 2012.

[7] D.Krishna, T.Hemalatha, G.Dhana Mani Shankar, K.Bala Krishna, V.Bala Subhramanyam " Aadhar Based Electronic Voting System And Providing Authentication", IJESAT , Volume-4 ,Mar-Apr 2014.

[8] A.Wagadre, B.B. Thorat, S. Sharma"Online Voting System Using Biometric Security", International Journal of Enhanced Research in Management & Computer Applications, ISSN: 2319-7471 Vol. 2, Issue 5, May-2013.