International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 05 | May 2020 www.irjet.net p-ISSN: 2395-0072

A Three Tier Secure System for Online Voting

Sreeresmi T.S[1], Teena George[2], Asha Rose Thomas[3]

[1]*Assitant Professor, Dept. of CS Engineering, Adi Shankara Institute of Engineering & Technology, Kerala, India*
[2]*Assitant Professor, Dept. of CS Engineering, Adi Shankara Institute of Engineering & Technology, Kerala, India*
[3]*Assitant Professor, Dept. of CS Engineering, Adi Shankara Institute of Engineering & Technology, Kerala, India*

Abstract - *Conventional voting process can be overwhelming, time consuming and prone to security breaches and electoral fraud. Over the years technology related systems were developed to resolve some of these issues like Electronic based voting that is been actively used for voting in countries like India and so. However these systems were still prone to electoral frauds and voters has to make tremendous effort in order to cast their ballots. A Three Tier Secure System for Online Voting is a Web application where the user is recognized by his/her fingerprint pattern.. The system allows the voter to vote through their fingerprint which is used to uniquely identify the user because fingerprint minutiae features are different for each human being. This system allows persons who are abroad also to cast their vote whereas in the current scenario of voting system present in our society demands physical presence of person who intends to do voting at the polling booth. Also the system helps to generate accurate results faster with less human effort compared to current mode of election.*

***Key Words*: Ballot, EVS, Aadhar, fingerprint, Three Tier etc**

1. INTRODUCTION

Democracy principles depend upon the people decision, so to have vision we need to take correct decisions. This can be made by "Voting". In a democratic country "voting" is one of the fundamental duties as a responsible citizen of the country, but now people all around the country are not able to come and cast their vote during the election process. The manual voting system takes long time as there is a lot of paper work first and then human effort is also there behind the counting of votes. Manual voting consumes mostly a complete day which is surely a headache for the election conducting officers and staffs. The conventional voting mechanisms follow the issue of voter id and other details which generated manually. So there are chances of parallax errors. Moreover the electronic voting machine may be devised in such a way that people whatever and whomever they vote, will be converted into some other's party or candidates. It may be misused.

2. EXISTINGSYSTEM

The automated voting systems are developed before some years ago. The existing systems have only been approved in developed countries. That too, not in all developed countries. Because the securities has not been fully preserved. We moved onto automation mainly to rely on security. But, the existing systems failed to ensure.

Naturally, the belief of the election process is utmost important [1]. Election process has strong media coverage, particularly if something goes wrong. This system will increase the level of security and also the trust of voters. The problems of Maoist affected places for the voting has been addressed in [2] while [3] describe the genesis of Maoist violence and showed that public needs a more secure way of casting their vote. Online voting system definition given in [4] states that Online voting systems offers advantages compared to other voting processes. The question of who gets to count your vote was addressed in [5] while in [6] the voting security has been analysed. The same problem has also been addressed in [7] more abstractly to ponder over its perception and reality.

2.1 DISADVANTAGES OF EXISTING SYSTEM

(ELCTRONIC VOTING SYSTEM)

1) Expensive and Time consuming
2) Too much paper work
3) Errors during data entry
4) Machines are vulnerable to malicious programming.

Abroad people can't cast their vote since physical presence is required at polling booth

3. PROPOSED SYSTEM

The proposed system involves important tasks:

1) Working model architecture
2) Verification process
3) Verification schema
4) Processing and counting
5) Generating Reports

3.1 WORKING MODEL ARCHITECTURE

It includes the steps like:-

(i) Entering valid user credentials which is nothing but username and password

(ii) Accessing and reading of user fingerprint pattern via external device

(iii) Retrieval and verification of details from AADHAR database with current samples

(iv) OTP is being send to registered Email/ Mobile number

(v) Voting can be done

Initially the people who wish to do vote must register on the site. So as a part of giving three level securities, the person must create an account for himself/herself. The proposed system is much secure and efficient than the traditional voting systems. Manipulation of votes and delay of results can be avoided easily. A unique AADHAAR identity is the centre point of our proposed model. Meanwhile on account generation stage it willbe get successful only if the person is 18years or above of age as it is the eligibility criterion for voting. This filtration can be carried out by checking the date of-birth of the user along with an AADHAAR, another security parameter used. This first level process itself helps to reduce unwanted entries to the database.

3.2 FINGERPRINT RECOGNITION:-

An important component in fingerprint recognition is fingerprint matching algorithm. According to problem domain, fingerprint matching algorithms are classified into:

a) Fingerprint verification algorithm

b) Fingerprint Identification algorithm

a. Fingerprint verification algorithm: The purpose of this algorithm is to determine whether two fingerprint come from same finger or not.

b. Fingerprint Identification algorithm: The purpose of algorithm is to search a query fingerprint in a database looking for the fingerprints coming from the same finger.

3.3 FEATURES

1. Increased number of voters as individual will find it easier and more convenient to vote, especially those abroad.

2. Less capital, less effort, and less labor intensive as the primary cost and effort will focus primarily on creating, managing and running a secure online portal.

3. The cases of vote miscounts shall also be solved since at the backend of this system resides a well-developed database using MYSQL that can provide the correct data once it's correctly queried.

4. Reduces time wasted in announcing election results.

5. Conducts free and fair elections.

3.4 CONSTRAINTS

1. Any windows operating system.

2. Interface is in English.

3. Administrator can access this system.

4. FLOW DIAGRAM

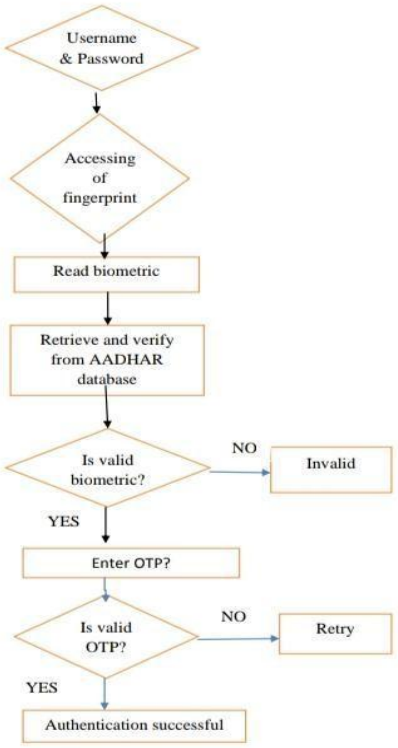

Fig -1: Flow diagram of online voting system

4.1 VERIFICATION PROCESS

When the user wants to login to the account user needs the password given at the time of registration to this website. After verifying whether the entered user name and password by the user are valid with respect to the database only the initial verification stage gets completed.

After login, along with the data filling process the fingerprint impression of the user must be given. After successful completion of the data filling process, all the data will be stored to corresponding database including the fingerprint. Later when the admin declare the date of election, user can see on which constituency which all candidates are standing for the election along with their symbol and photo. User can use the „vote tab" to do voting process. Now the system requires live fingerprint impression of the user. The first and the foremost thing to ensure proper voting are by accurately authenticating every voter. It is necessary to identify that every person coming to vote is unique otherwise it will violate the very principle of voting. Any person would be voting on behalf of others. Fingerprint matching ensures the authentication that the system requires. Use „capture finger" tab to scan your finger. The fingerprint device will be getting connected to the USB port of the system in use in prior. Now on scanning the scanned fingerprint impression will get to compare over the fingerprint stored on database. Only if the fingerprint matches only he/she can move to further steps. The user data's will be retrieved from database and the user can cross check and confirm its true in all sense.

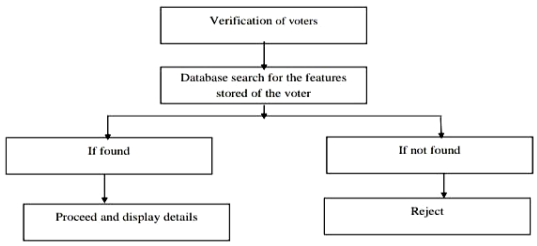

Fig-2: Verification process

4.2 VERIFICATION SCHEMA

For verification the person's fingerprint will be scanned at the client-side and matched one-to-one at the servers with the data extracted from the local database. This process puts less stress on the local database and improves data traffic. We use fingerprints for authentication because processing fingerprints is faster and better than other biometric data. Moreover AADHAR details would be insufficient to establish the true identity of a person since they can be easily faked but by using fingerprints it is ensured that such fake entries are blocked right at the very beginning.

After entering captcha in order to prevent machine malpractice click on confirmation. An OTP will be transferred to registered email address of the person. This OTP has to be given as such then only he/she can choose constituency, candidate and do vote steps. Even if the person tries to vote for more than one time the system has the ability to detect it avoids the same. Also the election result will be getting attached to mail of every user including the election count.

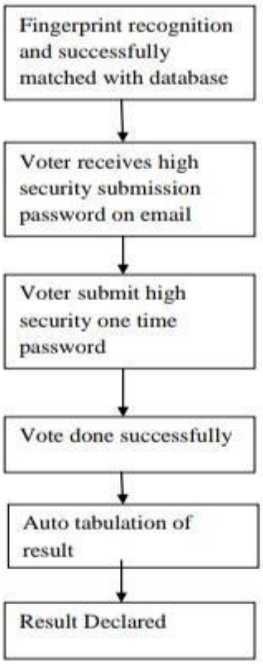

Fig 3: Verification Schema

4.3 PROCESSING AND COUNTING

Immediate and fast declaration of result also saves time and increase faith among voters for correcting counting than the existing. In the proposed framework, we have tried to build a secure online voting system that if free from unauthorized access while casting votes by the voters. The server aspects of the proposed system have such distribution of authority that server does not enable to manipulate the votes. It is expected that the proposed online voting system will increase the transparency and reliability of the existing electoral system.

4.5 GENERATING REPORTS

Whenever a voter casts a vote in favour of the candidate of choice, the vote count of that candidate gets incremented in the local database. The votes from all the local databases are summed up to get the final figure that the candidate has received. Thus this system provides instantaneous results and prevents unnecessary use of manpower and wastage of time. Since this is an electronic system and uses digital data it has several advantages. Statistics can be generated from the obtained data for e.g. we could answer how many people have voted from a certain region, how many females voted, which age group voted the most, the highest turnouts, comparisons from previous years, etc. all that was not possible from traditional voting methods not even from EVMs. It would provide important insights into the election results and help improve the system even further.

5. HARDWARE COMPONENTS

1) Biometric Module: Biometrics concentration comes on Fingerprint scanner. For this Morpho USB- MSO-1300 E3 Biometric Fingerprint Scanner is used

2) Technical Features: Low maintenance, Ergonomic, lightweight, and durable design. This device captures flat fingerprint images with Ambient light rejection. It has large active platen area 10 frames/second image captures and fully featured with auto capture, adjustable brightness, contrast, and gain functions. It provides live fingerprint detection

3) Specifications: The specifications of the MSO-1300 E3 fingerprint sensor is shown

Fig- 4: MSO-1300 E3 fingerprint sensor

Table -1: Specifications of MSO-1300 E3 fingerprint sensor

Item Model Number	MSO1300 E3
Platen Area	1.02 - 0.75 In. (26 - 19 Mm)
Active platen area	0.96 X 0.64 In(480 x 320 pixels)
Grey scale	**8-bit**
Weight	**220gm**
Dimension	6.5 x 3.5 x 1.5 cm
Material	Aluminium casing
Resolution	500ppi,10 frames/second
System requirements	Windows 2000, XP and above.

6. CONCLUSIONS AND FUTURE WORKS

Online Voting Systems have many advantages over the traditional voting system since they are very outdated. Some of these advantages in our system are three tier security, increases percentage of voters(persons staying outside, physically disabled people can also actively do vote) less cost, faster generation of results, easy accessibility, better accuracy, reduces man power to a great extent than previous voting methods and lowers the risk of human and mechanical errors. The system enables the user to cast vote from any part of the world if he/she is a particular citizen having valid AADHAAR and election card. And also focuses to reduce proxy vote and in booth capturing situation this system helps us. Due to easy and secure voting the voting percentage also increase drastically.

As a future work, we can implement this system as an application (software) in your android, iPhone, windows mobile platforms. Also this system can be modified by introducing Iris scanner beyond existing security measures to ensure high level of security for election.

ACKNOWLEDGEMENT

This is to acknowledge and thank all the group members who played role in shaping this paper. Without their constant guidance and assistance this report would not have been completed. Their guidance, coordination and reviewing this task could not be completed alone.

REFERENCES

[1] Tadayoshi Kohno, Adam Stubblefield, AvielD.Rubin, Dan S. Wallach, “Analysis of an Electronic Voting System”, Johns HopkinsUniversity Information Security Institute, Technical Report, TR-2003-19, July 23, 2003.

[2] http://newindianexpress.com/states/andhra_pradesh/ Maoist strike-fear-make-off-with-poll-papers-in-agency/2013/07/ 15/ article1684243. ECE.

[3] Executive Summary of "Genesis and Spread of Maoist Violence and Appropriate State Strategy to Handle it", Bureau of Police Research and Development, Ministry of Home Affairs, New Delhi

[4] http://en.wikipedia.org/wiki/Electronic_ voting

[5] David L. Dill, Bruce Schneier, and Barbara Simons, “Voting and technology: Who gets to count your vote?” Communications of the ACM, vol. 46(8), Aug. 2003, pp.29-31

[6] David Jefferson, Aviel D. Rubin, Barbara Simons, and David Wagner, “Analyzing Internet voting security”, Communications of the ACM, vol. 47(10), Oct. 2004, pp. 5964

[7] David Evans and Nathanael Paul, “Election security: Perception and reality”, IEEE Security & Privacy, vol. 2(1), Jan. 2004, pp. 24- 31