`

JOURNAL OF MULTIDIMENSIONAL RESEARCH & REVIEW

JMRR Innovate*Share*Explore

Website: http://www.jmrr.org **Vol.2, Iss.3 Pages:51-57**

E-ILLEGAL VOTING DETECTOR

Dr G Arockia Sahaya Sheela[1], J Janet Hephzibah[2], M Monisha[3]
[1]Assistant Professor, [2,3]BSc Computer Science,
Holy Cross College, Trichy, Tamilnadu

Article Received: April 2021 Published: October 2021

Abstract

The E-Illegal Voting Detector is a security mechanism for prohibiting the frauds in voting system. The main objective of this proposed authenticating system is to implement the Aadhar card for voting and also eliminating Fraud cards for entries. The manual operation takes time for presiding officer or polling officer to check each and every voter and also causes illegal voting or fraud voting. To exterminate illegal voting, Aadhar card must be implemented to authenticate the biometric measures of the voter. So that, only an authenticated voter is allowed to vote in the ballot boxes.. Fingerprint electoral/voting system was enforced with the Arduino Technology. In the System the candidate can poll his/her vote early. The voters are allowed to enrollwith the link of biometric data in the UID database to the voting machine and also ensure that a person cast their vote only once. All the candidate information's are stored in the database and the voters' aadhaar card was linked to the database. From the details of a person can be retrieved and matched for every citizen. If anyone tried to vote for second time the detector will alert that "Already voted". This can be considered as best practice for the citizen's right to vote and remain strong in fair elections. The System won't permit the candidate to vote. Fingerprint ballot is user friendly. It's straightforward design for approved investigation properly.

Keywords: Arduino, Aadhar card, Thumb impression, Cloud

INTRODUCTION

In every democracy, the security of an election is a matter of national security. The computer security field has for a decade studied the possibilities of electronic voting system with the goal of minimizing the cost of having a national election, while fulfilling and increasing the security conditions of an election. At first glance, electrical voting machine is exhibited to avoid delay of time and much man power. And so many illegal voting took place. This electronic voting detector helps us to avoid those corruption in voting.

PROPOSED SYSTEM

The proposed system is a biometric e-voting system which has two main sections- 1) voter registration & 2) voting control and result calculation. Each user needs to register first as a voter through the system with biometric (fingerprint) verification. The information of the voter will be saved in a central database. Then during the election, digital ballot paper will be used instead of paper ballot paper and it will contain the list of candidates and their respective logos. A registered voter can cast only one vote by verifying his/her finger print. The process of voting system has been explained under the dataflow diagram.

LITERATURE SURVEY

Standard electoral systems, such as paper ballots, lever voting equipment, punched cards, GSM portable smart polling scheme, etc., have many drawbacks to address. Use biometric methods in [Nic, 16] to achieve safer and more versatile real-time applications. Since this system has immediate monitoring, we can get the results faster and earlier. Some specifications were described in [Naik, 15] depending on product design. Few are said to be the long-lasting battery control-unit, simpler and less costly components, etc., Then the control unit should be readily accessible also the device must readily handle. Voters need to have one of the switches, such as Aadhaar board, pan board, etc. There are two phases of tracking in [Sri, pok, Sai, 09]. First, to use this particular method, the hash code is created and use both hands ' hands and the hash password created has a 13-digit symbol that can be put as a barcode. To attain fingerprint value, the distinctive Points are calculated. The surveillance stage begins after the original stage above. Electors only have access to record efficiency games after inspecting for fingerprint. The voting phase begins after he has access to the EVM button to register their voting. The licensed repositories are discovered in EVM during the electoral processing &enrolment stage, which are continually evaluated. The electronic voting device biometrically guaranteed [Sal, Amar, Ravi, Sur, Mah, 16] explains how to incorporate the EVM with the bio-metric In [Nic, Jon, 14],[Rah, Huz, Bip, Shu, Abd, 17] the related concentrate is primarily on safety and security parts. These ideas prompted and provided the idea of using picture, eye and fingerprint authentication [Alv, Hal, 08] to consider to use Raspberry Pi 3 to produce experimental kiosk prototype. We used raspberry pi 3 in our execution and in reality, functionalities such as image capture characteristics are embedded with efficiency in elections that register the picture of people [Asl, Pop, Riv, 08],[Cha, 04].The concept behind the multimodal verification scheme to improve safe monitoring polling or voting and to attain zero tolerance for fraud and other crimes. This paper therefore gives priority. The primary goal and purpose of the suggested

Design is to have a safe, secure and intelligent polling machine with enjoyable, better thoughts for the comfort and comfort of the audience. "Bio-Metric Based Assistance and Security System Using Arduino" a biometric authentication scheme. Biometric methods enable a individual to be recognized immediately on the basis of physical or cognitive characteristics that relate to a certain individual. Each biometric characteristic has its boundaries and no biometric scheme is ideal so that a range of issues arise from biometric unimodal methods. Multimodal biometric devices are used to satisfy some of the listed inconveniences and constraints and to boost the amount of safety. This further section explains the main features of the multimodal biometric system: structure, fusion point, the methodology used to incorporate multiple verifiers and standardization techniques.

PROPOSED METHODOLOGY

In this phase, it has two methods of enrolment and authentication. The enrolment method manages the entry method to enrol the voter in this phase the enrolment mode yield will be deposited in the scheme database. The second phase, which is the authentication method, addresses the method of reviewing the voter’s status by adding the users multimodal biometrics and matching them with the databases; if the scheme discovered any comparable biometrics in the database, then the voters is entitled to register his ballot. The user's vote will be counted and stored in the database. The voter can inspect the election outcome by pressing the outcome key at the start of the polling cycle.

DATA FLOW DIAGRAM

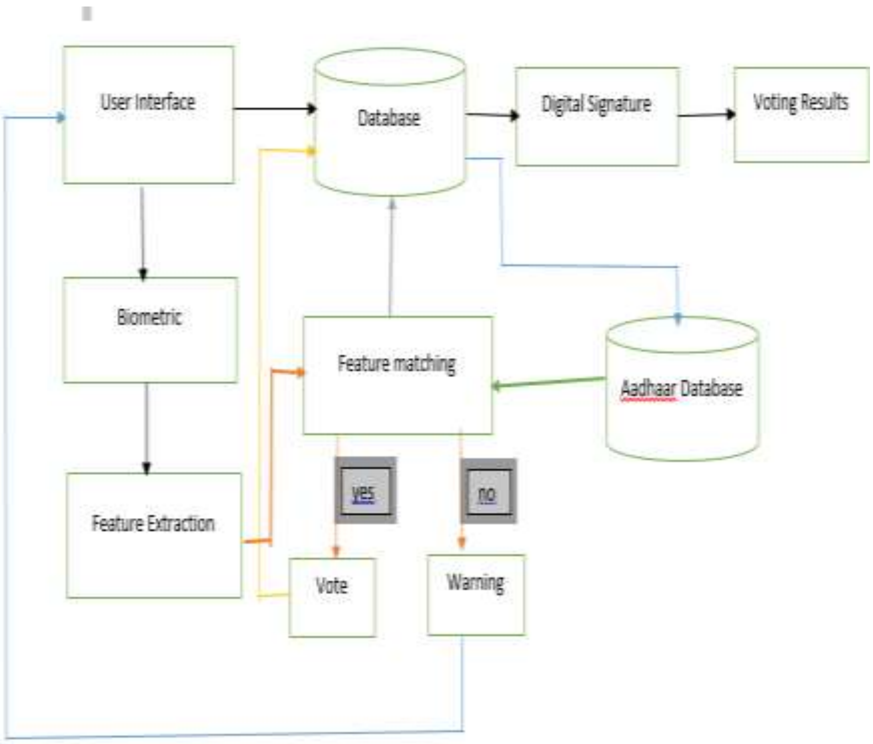

Fig 1 Data Flow Diagram for UI Registration

1. **EVM**

   Electronic Voting is the standard means of conducting elections using Electronic Voting Machines, sometimes called "**EVMs**" in India. The use of EVMs and electronic voting was developed and tested by the state-owned Electronics Corporation of India and Bharat Electronics in the 1990s. They were introduced in Indian elections between 1998 and 2001, in a phased manner. The electronic voting machines have been used in all general and state assembly elections of India since 2004.

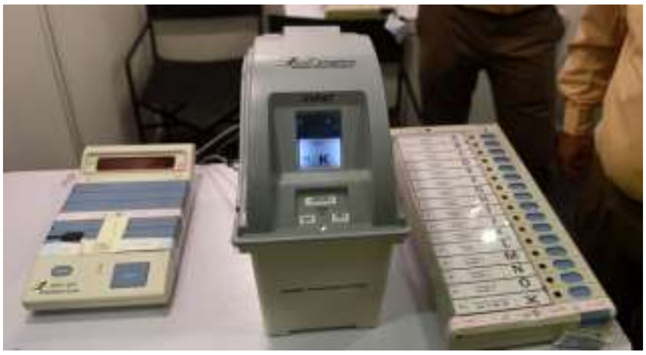

Fig 2 Electronic Voting Machine [2]

2. **Cloud Database**

   Cloud computing is the on-demand availability of computer system resource, which is majorly used for data storage and computer power without user.

3. **Biometric**

   Biometrics is the technical term for body measurements and calculations. It refers to metrics related to human characteristics. Biometrics authentication is used in computer science as a form of identification and access control. It is also used to identify individuals in groups that are under surveillance.

Fig 3 Biometric machine [4]

4. **Signature palette**

   An **electronic signature**, or **e-signature**, refers to data in electronic form, which is logically associated with other data in electronic form and which is used by the signatory to sign. This type of signature provides the same legal standing as a handwritten signature as long as it adheres to the requirements of the specific regulation it was created under.

Fig 4 Signature Palette [9]

The voters will enter the polling booth with their voter board and aadhaar board to cross check their identity. After the checking process the voter's will print their impression in the biometric system. That ensures the voter and displays their details. Then they are allowed to pole. Further process is handled by the voter to select the candidate. The final process of the voting is the digital signature. This final detection is to confirm the voting process.

RESULT ANALYSIS

This system uses the cloud or Aadhaar repository as its backend. By using this database, the data of the voter will be deposited on the personal computer. Multimodal biometric testing could also be an honourable option for e-voting applications where you can provide appropriate input and instruction to customers and where the scheme works in a regulated setting. The scheme guarantees an individual's authentication by adding Aadhaar amount and registration is verified by calculating the voter's era, thus rendering the current electoral machines useless. Performance is measurements depending on the spatial resemblance of the F-measure (SSIM) and precision of identification. The votes for the candidates will be automatically updated for each individual.

ADVANTAGES

No one can vote illegally through this system. The machine will indicate if any unauthorized person is detected. The system will be locked when the unauthorized person enters. The time delay of counting the votes will be reduced as the count of votes are updated. As the end of the process, the signature verifies and stores the vote in the system.

DISADVANTAGES

The storage and the cost will be expensive according to the population. If the machine got locked it takes some time to unlock to the regular process.

RESULTS AND DISCUSSIONS

The implemented prototype of the system was tested for various constraints and loopholes but the result was quite satisfying. There is no way a user can register or vote falsely. All information regarding the voting process is stored in the database. As the Aadhar card is linked with the database the biometric system will recognise the false vote and will alert the commission. As the result he/she can’t vote twice.

CONCLUSION

The proposed voting system had many advantages over the traditional voting method. This system provides additional security by allowing voters to enrol once only by providing unique identification along with biometric data such as finger printing and digital signature. This scheme prevents illegal polling and illegal behaviour during the contest, which is the main problem in the tradition. The benefits of this scheme are quicker production, enhanced accessibility, higher precision, and decreased probability of private, physical and mechanical mistakes. A database composed of information such as era, people's biometrics should be changed every moment before voting. Information on set ballots can be sent to the elector through the communication system. Developing a set of metrics to recognize unauthorized client practices and recognizing false clients with an effective classifier is a motivational element.

REFERENCES

1. Nicholas Weaver. (2016). Secure the Vote Today. Available at:https://www.lawfareblog.com/ secure-vote-today.
2. Naik, Devendra Vijay. "Smart wireless authenticating voting machine." In 2015 International Conference on Communications and Signal Processing (ICCSP), pp. 0785-0788. IEEE, 2015.
3. Srinivasan, .Pokumaran and G. Sainarayan, “Improved Background Subtraction Techniques for Security in Video Application”, Anti-counterfeiting Security and Identification in Communication, pp. 114-117, 2009.
4. Saleem Ulla Shariff, C Amaranatha, Ravi AnandJadhav, Dr. K Suresh Babu, MaheboobHussain, “Face and Bio-Metric Based Attendance and Security System using RFID and Arduino”, 4th National Conference on Networking Embedded and Wireless Systems NEWS-2016 International Journal of Electrical Electronics & Computer Science Engineering Special Issue, pp. 84-89.
5. Nicole J. Goodman ; Jon H. Pammett, “The patchwork of internet voting in Canada”, 2014 6th International Conference on Electronic Voting: Verifying the Vote (EVOTE), Pages: 1 – 6.
6. RahilRezwan,HuzaifaAhmed,M. R. N. Biplob,S. M. Shuvo,Md. Abdur Rahman, “Biometrically secured electronic voting machine”, 2017 IEEE Region 10 Humanitarian Technology Conference (R10-HTC) DOI: 10.1109/R10- HTC.2017.8289010
7. Alvarez, R.M. and T.E. Hall. 2008. Electronic elections: the perils and promises of digital democracy. Princeton University Press.
8. Aslam, J.A., R.A. Popa and R. L. Rivest. 2008. On Auditing Elections When Precincts Have Different Sizes. Proceedings, 2008 USENIX/ACCURATE Electronic Voting Technology Workshop.
9. D. Chaum, "Secret-ballot receipts: True voter-verifiable elections", IEEE Security and Privacy, vol. 2, no. 1, pp. 38-47, 2004.

10. H. C. Lee, A. Banerjee, Y. M. Fang, B. J. Lee and C. T. King, "Design of a multifunctional wireless sensor for in-situ monitoring of debris flows", IEEE Trans. Instrum. Meas., vol. 59, no. 11, pp. 2958-2967, Nov. 2010.

Cite this article:

Dr G Arockia Sahaya Sheela, J Janet Hephzibah, M Monisha, “E-Illegal Voting Detector”, Journal of Multidimensional Research and Review (JMRR), Vol.2, Iss.3, pp.51-57, 2021