International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 03 | Mar 2019 www.irjet.net p-ISSN: 2395-0072

DESIGN AND DEVELOPMENT OF SECURITY BASED VOTING SYSTEM

Mounisha A, Niraimathi D K, Niveditha S

Banupriya N, Assistant Professor

Department of Computer Science and Engineering
R.M.K Engineering College, Tamil nadu, India.

Abstract - *Voting Machines are used to define ballots; to cast and count votes; to report and display the election results; and to maintain and produce any audit trail information. The first Balloting Machines had been mechanical but it is more and more common to electronic voting machines(EVM). It is also important that false entry should not be made. So to avoid those, we are implementing secure methods of voting through biometric sensor. In this paper we use fingerprint sensor for providing access to the voter as well as making log if the person has voted or not.*

Key Words: ***Fingerprint recognition, Arduino, Electronic voting , Biometric, Security, Election***

1.INTRODUCTION

Elections are conducted according to the constitutional provisions and parliamentary legislation. The Election Commission of India is the league authority that is responsible for administering all the electoral process in India and ensure that they are free and honest. Elections in the Republic of India includes : General Elections (Lok sabha), State Assembly Elections, Rajya sabha Elections, Local Body Elections. Electronic Voting Systems have the ability to improve the traditional voting methods by giving additional convenience and flexibility to the voter. Electronic Voting Machines (EVM) are being used opposed to ballot bins to prevent fraud in elections. They are being used in General and State Elections of India . After the citizen votes his or her left index finger is marked with an indelible ink. This practice was instituted in 1962. Several digital voting methods had been proposed in the earlier days, but most of them have failed to provide voter authentication in an efficient and transparent way.

These EVM system fail to achieve security as false vote casting is highly possible by threatening the poll officers and forcing the genuine voters to cast illegal votes again. The intruders can also hack and change the votes of the people. Considering these problems and to overcome the consequences, we have proposed and implemented an automated biometric voting model along with the PHYVOS(Physical layer Voting System) that are Secure and fast for voting .

Instead of using the traditional voting system, we prefer PHYVOS for its faster and secure voting method. PHYVOS uses OFDM(Orthogonal Frequency Division Multiplexing) that makes use of subcarrier orthogonality for the faster voting without any delay and also maintaining its higher security level.

Biometrics is the technical word that is used for body measurements and calculations. It refers to metrics related to human characteristics. Biometrics authentication is used for identification and access control. Biometric identifiers are a kind of distinctive and measurable characteristics that are unique to individuals. There are different types of biometric authentication and identification methods. For this model we use the fingerprint recognition technique.

Our present voting process is complicated and time consuming process. The voter has to show his/her id card and undergo a lot of process for his/her verification. So to make this process faster and secure, we design and develop the voting system based on the fingerprint authentication of the voters with the Aadhar card database. Once the fingerprint of a voter is identified for the first time, it asks for the voter to cast vote and following that it freezes for a certain period of time for the next voter to cast their vote. This proposed machine sends a confirmation to the voter via GSM. The false vote or recasting of vote is not possible since it locks the voter's ability to cast their votes again. If tried, it makes an alert to the poll officer and their votes will not be updated in the Voting database.

We organize the paper as follows. In Section 2, we present the system model and architecture. System implementation steps are stated in Section 3. Finally, Section 4 concludes the paper with conclusion , acknowledgement and references.

1.1 EXISTING SYSTEM

Electronic voting machines provides voter a button for each choice that is aided by a cable to an electronic ballot box.

An EVM includes two devices--control unit and voting unit--and they are connected by a five-meter cable. when a voter presses a button for the candidate he/she wishes to vote for, the machine locks itself for a period of time for that particular candidate .Even though when one presses that button for any number of times or presses any other button, no vote can be recorded. So it is not possible to vote more than once. In this way, the EVM make certain the principle of "one individual, one vote". Even this system ensures this principle, the polling booth can be took over by the fraudulent.

Problems that could be encountered during the usual elections are as follows:

i. Incorrect validation of voters.
ii. Polling Booths could be captured.
iii. Altering the election results by getting access to machines by insiders and frauds to alter.
iv. The voters may find this as a boring event and time consuming one, resulting in to a small number of voters.
v. Deceitful election mechanism.
vi.
vii. Lack of transparency.

1.2 PROPOSED SYSTEM

The voter at the polling booth has to show his/her finger and they need to scan their finger on fingerprint module(Scanner). This module scan the voter's fingerprint and send to controller for matching with scanned fingerprint that is stored Virtually created view of Aadhar card database in system. If the fingerprint match with already stored voter the database, then he/she is valid for polling sections and voter is allowed to cast their vote. If not, a message is displayed on LCD along with the buzzer alert and the voter is not permitted to cast his/her vote.

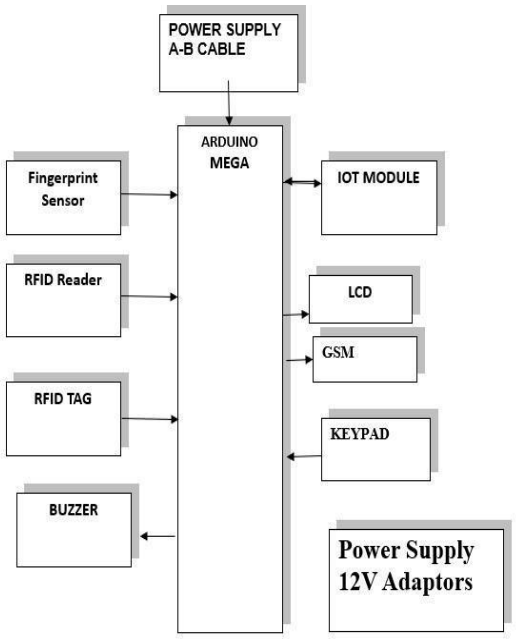
After the successful polling of their votes, GSM module sends confirmation message to voter registered mobile number.

If the voter is trying to cast the vote again, it is considered as a false vote. This is prevented by the proposed system.

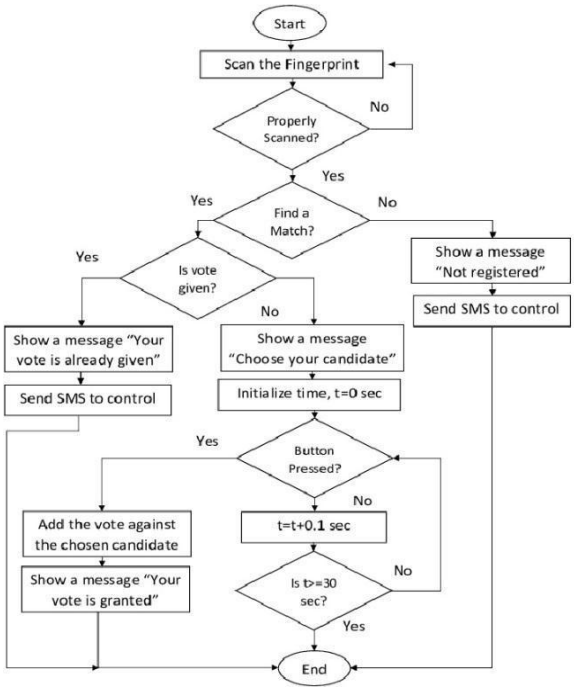
i. The buzzer in the system makes a alert so that the poll officer comes to know about the condition and the it do not consider the recast of the vote by a same voter(i.e Entry of the false vote is not uploaded into the Voting database).

2. SYSTEM DESIGN AND IMPLEMENTATION

1.DESIGN:



2.FLOW DIAGRAM:



There are few steps for the implementation of this process.they are the following:

- Valid Voter list
- Validation of a Voter
- Voting Process
- Confirmation

A. Valid Voter list:

For this particular list, we get the details of voter from aadhar card database that is made accessible by the Government.Since they are not secure to use specifically, We virtualize the view such that the voter's name, date of birth, enlisted unique number,fingerprints can be utilized.. This voter's information will be stored in the system under proper authentication.

B. Validation of a Voter:

At the time of Election, the election booth can start by the respective poll officer. The voters are checked in the following levels:

- Level-1: Using date of birth
- Level-2:Fingerprint match
- Level-3:Whether the person is trying to recast the vote.

The level-1 and level-2 check are done simultaneously. At the point when the fingerprint of the voter is filtered, the database that we have in our framework checks for impression coordinate and furthermore checks whether the voter is legitimate or not(above 18 or not).

The level-3 check is that if a voter attempts to recast his vote for the second time(not at his first time), then system gives an alert. Regardless of whether the survey officer and the polling stalls are caught and the voter is endeavoring to recast his/her vote once more, the framework won't refresh the votes.Hence, "One Person, One Vote" is achieved.

C. Voting Process:

At the point when the individual is viewed as legitimate, the ballot framework invites them and they are permitted to make their choice to the ideal competitor.

D. Confirmation:

After the completion of voting process, the LCD displays a message "Successfully Voted".GSM module sends a confirmation message to the voter's registered mobile number

.

CONCLUSION

This proposed system gives the best solution to the problems related to the Indian voting system . But they are susceptible to security attacks. Confidential biometric data may be leaked due to insecure network connectivity, system or machine hacking. Complete implementation is not a smooth venture; it involves political, financial and regional issues. Illiteracy is the main hurdle in this project to come true because this is not easy for them to work with the proposed machine interface.

ACKNOWLEDGEMENT

We are substantially obligated to our college "R.M.K Engineering College, Chennai" that has provided a healthy surroundings to transport us to perform our pursuits and desires. We would love to express our honest thanks to our guide Prof. N.Banupriya for the guidance, aid and help she has furnished in completing this paper. We are lucid to bring devout honest Gratitude to our dignitary professor for her encouragement and support to us, which made contributions to the successful finishing of this paper.

REFERENCES

1. "Analysis and Management of the Impacts of a High Penetration of Photovoltaic Systems in an Electricity Distribution Network", S. J. Lewis
2. "Security Analysis of India's Electronic Voting Machines" Scott Wolchok, Eric Wustrow, J. Alex Halderman
3. "Prototyping of Indian Electronic Voting Machine" Tushar Puri, Jaspreet Singh, Hemant Kaushal International Journal of Engineering Research and Development (May 2017)
4. "Secret Suffrage in Remote Electronic Voting Systems" Adrià Rodríguez-Pérez
5. "Election Voting Machine - A Review Sanket M. Gawade, Ninad S. Mandavkar, Sanket S. Mane, Chinmayee N. Manjarekar" International Journal of Engineering Trends and Technology (IJETT) – August 2017
6. "Verifiable Classroom Voting in Practice" Feng Hao, Dylan Clarke, and Brian Randell

7. "Secure Physical Layer Voting" Nirnimesh Ghose, Bocan Hu, Yan Zhang, and Loukas Lazos