

¹POOJA V. SHELKE

**Department of Computer Science and Engineering, HVPM College of Engineering and Technology, Amravati, India
pvshelke94@gmail.com**

²POOJA D. POKALE

**Department of Computer Science and Engineering, HVPM College of Engineering and Technology, Amravati, India
poojapokale19@gmail.com**

³PROF. JAVERIYA I. SYED

**Department of Computer Science and Engineering, HVPM College of Engineering and Technology, Amravati, India
javeriyaisyed@gmail.com**

ABSTRACT: -In the era of technology, the voting machine, which is present today, is highly unsecured. Being in the age of computers we are compromising the security by option for electronic voting machine because in the present electronic voting machine is not intelligent that is it cannot determine the person came for the voting is eligible or not. That mean the whole control is kept in the hand of voting in charge officer. One more risk with the present voting machine is that anybody can increase the vote count, since the count is present in the voting itself.

Keywords: Eye retina scanning, E-voting, Machine, Iris technology.

1. INTRODUCTION

In India election has supreme weight age. So to make it secured and efficient in the vision of modern technology we are using “Global Wireless E-Voting”. Why we are looking for it? In the era of technology, the voting machine, which is present today, is highly unsecured. Being in the age of computers we are compromising the security by option for electronic voting machine because in the present electronic voting machine is not intelligent that is it cannot determine the person came for the voting is eligible or not. That mean the whole control is kept in the hand of voting in charge officer. One more risk with the present voting machine is that anybody can increase the vote count, since the count is present in the voting itself. In this the machine is made intelligent which can determine the eligibility of the voter by scanning the eye pattern and also the vote count is not kept into the same machine itself instead of it is store in the remote server by converting it into radio waves. Here there is no chance of increasing the vote count of machine. Even in case of damage to voting machine there will not be harm to continuity of the election process.

2. OVERVIEW

Electronic voting systems for electorates have been in use since the 1960s when punched card systems debuted. Their first widespread use was in the USA where 7 countries switched to this method for the 1964 presidential election. The newer optical scan voting systems allow a computer to count a voter's mark on a ballot. DRE voting machines which collect and tabulate votes in a single machine are used by all voters in all elections in Brazil and India, and also on a large scale in Venezuela and the United States.

They have been used on a large scale in the Netherlands but have been decommissioned after public concerns .Internet voting systems have gained popularity and have been used for government elections in the United Kingdom, Estonia and Switzerland as well as municipal elections in Canada and party primary elections in the United States and France.

3. PRESENT SYSTEM

Since now days voting system is replaced by electronic machine to carry out voting. Now in a present system each and

every section is given an electronic machine which stores the votes of the people how have voted for the particular candidate. Control of present system is given to the in charge officer. He only check for the eligibility of the candidates and allow for the voting. Finally we collect all the voting machine at a place and go for counting.

4. DISADVANTAGES OF PRESENT SYSTEM

1. After voting if any technical problems or damage occurs with the machines it may leads to the reelection.
2. The machine is not able to recognize the eligibility of a candidate, so the corrupted officers may misguide the people. The corrupted officers may increase the count of the voting.
3. This system is not a cost effective one.
Since we need security, in charge officers, secured place for counting and election place.
4. The person from any other region cannot vote in for a candidate of other region.
5. The voting take place where the machine is located.

5. PROPOSED METHOD

In this system it trying to keep counting of votes in to a remote secured system. In this system it uses an electronic circuit which enables the voter to vote and transfer this vote to the remote system by converting it to radio wave through the mobile towers. This machine can check the eligibility of the candidate by itself, so there is no question of corruption. Machine itself is automated to check the eligibility of the candidates. Here we need not to go for the reelection even if the machine is damaged. A person even can vote from a mobile system and also from Internet. We can vote from anywhere even though being a voter of another region.

6. EYE RETINA

1. Eye Retina Scanning: The eye retina machine is a simple web cam or device which can capture the images effectively. Each person's retina is unique. A retinal scan is performed by casting unperceived beam of low energy infrared light into a

person's eye as they look through the scanners eyepieces. This beam of light traces standard path on retina.

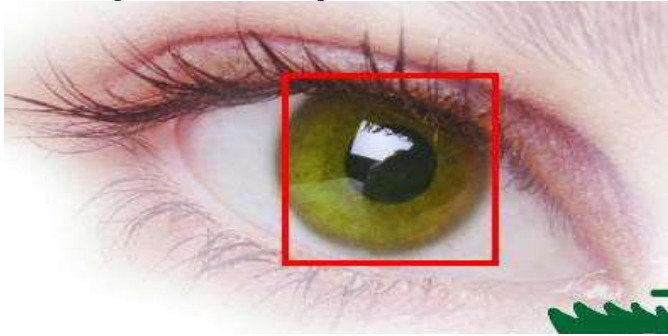


Figure 1: Eye Retina

2. Iris Recognition Technology: This technique is mostly useful for blind person. Iris recognition is the best of breed authentication process available today. Iris recognition simply involves taking picture of the iris; this picture is used for authentication. This technology is pattern dependant.

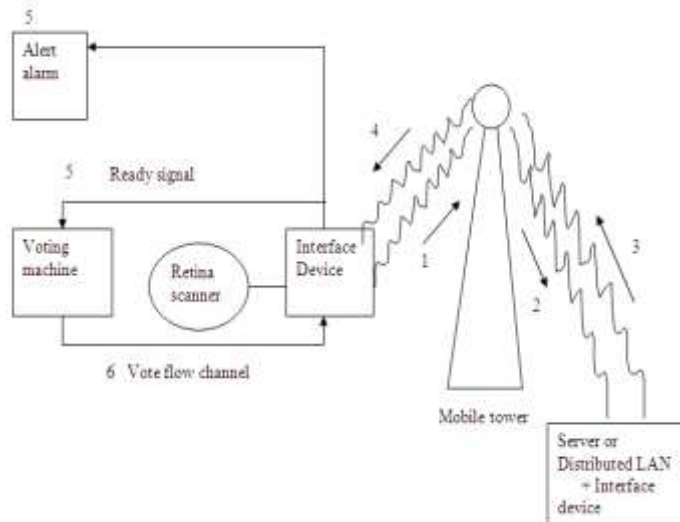


Figure 2: Block diagram of retina scanning

1. Radio waves representing scanned retina pattern and vote to Mobile tower.
2. Radio waves representing scanned retina pattern and vote to remote server.
3. Acknowledgement (+v or -v) from the server to mobile tower.
4. Acknowledgement (+v or -v) from mobile tower to Interface device.
5. Ready signal if retina is scanned properly to voting machine. And if -ve signal then alert alarm will be activated.
6. Accepted vote is made to flow to the interface device.

7. INTERFACE DEVICE

This is an electronic kit which converts the input digital signals such as (retina pattern votes+ secure bits) to radio waves.

8. WORKING OF WHOLE SYSTEM

Whenever voters enter to voting booth then he will be instructed to directly look at retina scanning machine at this time the machine scans the retina. Once retina scanning properly confirmed then it sent signal to the voting machine as to accept the vote it will be powered on .then voter is made to vote. Now the whole data including the retina pattern is sent to interfacing

device which is convert into radio waves of mobile frequency range and these radio waves are sent to mobile tower and then to the remote server, where the authentication and voters identification is stored into a secured database. The received data is first converted into digital format from the radio waves through the interface device kept the server side, and then retina pattern and vote separated. Next the retina pattern is matched against the existing database. If match is found then flag is check which indicates its voting status.

9. DETAIL DIAGRAM OF THE VOTING MACHINE

The voting machine is actually a device which generates the different voltages for different votes these voltages are fed to the (ADC) which is then converted to digital bits then can be converted to radio waves.

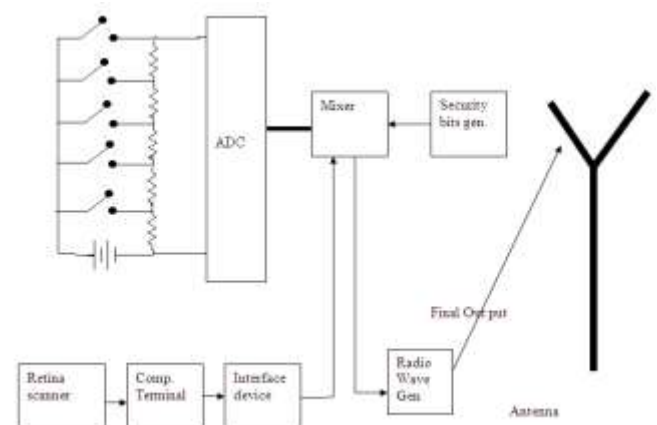


Figure 2: Block diagram of the Client Side Circuit

10. CONCLUSION

Thus this machine can be used for any level voting purpose. The machine provides high level of security, authentication, reliability, and corruption -free mechanism. By this we can get result within minute after a completion of voting. Minimum manpower Utilization, hence mechanism is error free.

11. FUTURE ENHANCEMENTS

This project can be enhanced to work over the mobiles that is voting is made possible through the mobile through SMS. This machine can be made vote through the internet.

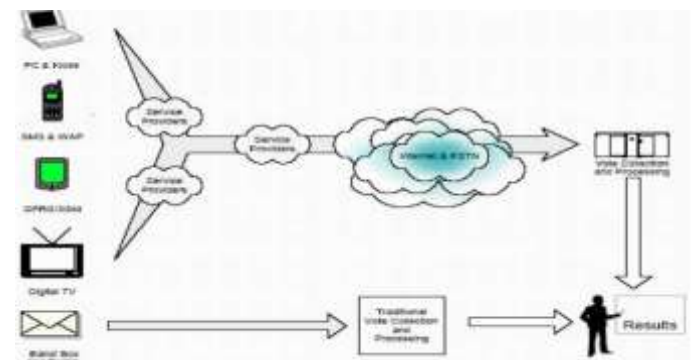


Figure 3: Future view

12. REFERENCES

- [1] David Chaum. Secret-ballot receipts: True voter-verifiable elections, 2004.
- [2] R. Mercuri Explanation of voter-verified ballot systems. ACM Software Engineering Notes (SIGSOFT), 27(5).
- [3] A. P Rosser, R. Kofler, R. Krimmer, and M. K. Unger. Security assets in e-voting. In the International Workshop on Electronic Voting in Europe, 2004.
- [4] B. Var Acker. Remote e-voting and coercion: a risk-assessment model and solutions. In the International Workshop on Electronic Voting in Europe, 2004.
- [5] T. Kohno, A. Stubblefield, A.D. Rubin, and D.S. Wallach. Analysis of an electronic voting system, 2004.
- [6] Buchsbaum, T. "E-voting: International development and lessons learnt". Proceedings of electronic voting in European Technology in 2004.
- [7] Zissis, D; Lekkas "Securing E-government and e-voting with an open cloud computing architecture" April 2011.
- [8] Schneier, Bruce. "An Incredibly Insecure voting machine", 3 December 2015.
- [9] Feldmen, Halterman and Felten. "Security analysis of the Diebold AccuVote-TS Voting machine" 3 December 2015.
- [10] Schneier, Bruce. "What's wrong with Electronic voting machines?" 3 December 2015.



Pooja D. Pokale Pursuing her B.E. in computer Science and Engineering from Shri Hanuman Vyayam Prasarak Mandal's College of Engineering and Technology, Amravati, Maharashtra, India. Her area of interest is Networking.



Javeriya I. Syed working as a Assistant Professor in computer Science and Engineering from Shri Hanuman Vyayam Prasarak Mandal's College of Engineering and Technology, Amravati, Maharashtra, India. Her area of interest is Networking.

13. AUTHOR PROFILE



Pooja V. Shelke Pursuing her B.E. in computer Science and Engineering from Shri Hanuman Vyayam Prasarak Mandal's College of Engineering and Technology, Amravati, Maharashtra, India. Her area of interest is Networking.