GLOBAL WIRELESS E-VOTING

S.VINOTHINI

IT – Final Year

IFET College of Engineering, Villupuram

vinolathavino@gmail.com

ABSTRACT:

In the era of technology, the voting machine, which is present today, is highly unsecured. 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 machine itself. In proposed machine that is "Global Wireless E-Voting" 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. The overall concept of "Global Wireless E-Voting "is explained.

1. INTRODUCTION:

In India election has supreme weight age. So to make it secured and efficient in the vision of modern technology we are "Global Wireless E-Voting". Why we are looking for it?

2. 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 a 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.

3. DISADVANTAGES OF THE PRESENT SYSTEM:

After voting if any technical problems or damage occurs with the machines it may leads to the reflection. 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. During transportation of the machines the in charge person can change the status of machines and even may destroy.

This system is not a cost effective one. Since we need security, in charge officers, secured place for counting and election place. The person from any other region cannot vote in for a candidate of other region. The voting take place where the machine is located.

4. PROPOSED SYSTEM:

In our system we are trying to keep counting of votes in to a remote secured system. In this system we are using a electronic circuit which enable the voter to vote and transfer this vote to the remote system by converting it to radio wave through the mobile towers. Our 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.

5. 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.

6. EYE RETINA SCANNIG:

The eye retina machine be a simple web cam or device which can capture the images effectively. The capture image will be represented in the form of a matrix where each pixel represents 24-bit (RGB,8+8+8 format).

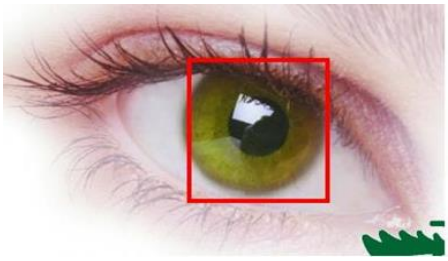

Fig:6.1 eye retina scanning

7. INTERFACE DEVICE;

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

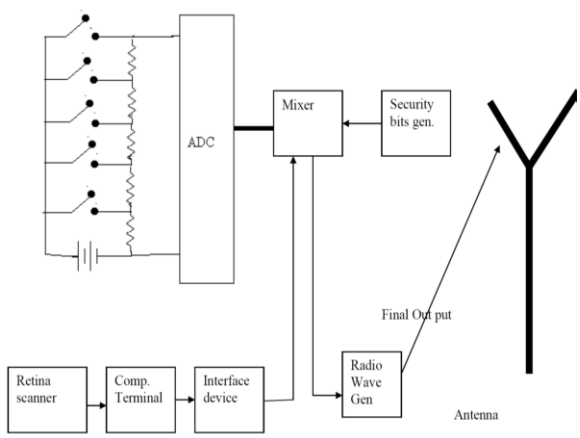

Fig: 7.1 block diagram

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 i.e. if the voter is not voted yet

then positive ack is send to the mobile tower and then to the corresponding voting machine. This ack is recognized by the receiver kept at the voter side and machine is made to scan next retina pattern and vote, otherwise if–ve ack then alert alarm is made to ring.

9. HURDLES IN THE PATH OF IMPLEMENTATION:

There are several more issues that we have to consider along the Implementation such as

- Security
- Efficiency

Another problem is that one may trap the radio waves in between and can determine the person and the vote. this may disclose the result of the election before the completion of the voting process. To avoid this problem we can go for applying the efficient and complex encryption algorithm so that the transparency of data can be hidden and the server side the encrypted data can be again decrypted and original data can retrieved this make the trapping of wave meaningless. The encryption algorithm can be termed as **Key Complex Algorithm,** which is as follows**,**

- First it finds the length of the string.
- Generate the random numbers equal to the length of the string.
- Add the corresponding Characters from the given string and random values.

E.g. KSHITIJ

Let this be the given words.

- Geographical Problems

9.1 SECURITY:

The radio waves of a mobile frequency consist of Retina pattern and vote can be generated by means of external source. That's why we need to provide some set of security to avoid this problem. One of the idea to solve this problem is CDMA (which will be explained later) and another technique is inserting security bits at regular interval of time during the transmission of radio waves (Ex.2 msec) .At the server side after the given interval (2 msec) security bits are checked (ex 1001) . In case of positive confirmation we can accept as valid vote, otherwise simply rejected.

The length of the given string is 7. So let us generate the 7 random numbers .Let numbers be

A) 8 12 34 4 11 9 26 .

The ASCII values for KSHITIJ are

K S H I T I J

B) 75 83 72 73 84 73 74

Add corresponding A) and B) values as

8+75 12+83 34+72 4+73 11+84 9+73 26+74

83 95 106 77 95 82 100

The corresponding ASCII characters for these are

S _ j M _ R d

The corresponding characters for random values

ℵ ϑ θ ♥ ♦ ↔ ψ

Finally encrypted data as

S ℵ _ ϑ j θ M ♥ _ ♦ R ↔ d ψ

The final encrypted data is formed in such a way that the random data at the even place and rest at odd place. This makes Decryption very easy.

Simply subtract the character at even place from odd place character.

9.2 EFFICIENCY:

Whenever the data which is sent from the voter (client) side, it is in the large amount, this delays a bit a voting system and the data that is received at server side is in the multiple access mode i.e. more than one client is sending the data. To overcome this problem the following

Applying compression Algorithms at the Client and server side so those to decrease the data transfer. Compression technique such as JPEG compression or any other Compression.

Instead of using single server PC we will go for distributed Operating system environment with multiple servers. This makes the job sharing and processing faster which leads to fast responds in case of Multiple Access Environment.

To solve the concurrency problem in case of Multiple access environment we will use **CDMA** technique which is as follow

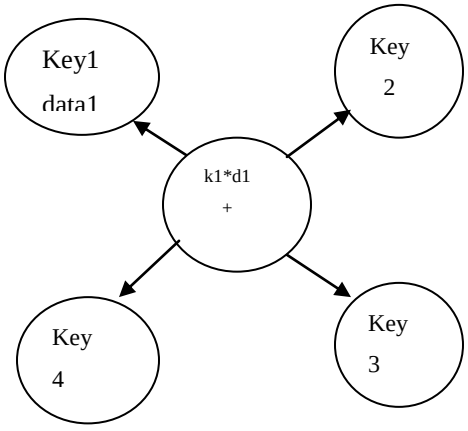

Fig: efficiency key value

Here the key values are orthogonal to each other i.e. k1*k2=0 and k1*k1=1 i.e. if any tries to decode the information with any other key the data will be vanished as the data will be in the form d1*k1.If you try to decode with K2 then effect will be as d1*k1*k2=0. This will vanish the data. And if correct decoding key i.e k1 is used then decoding will be d1*k1*k1=d1. This decodes the data correctly. As per the controlling concurrency for multiple access the data from all the nodes is accepted as k1*d1+k2*d2+k3*d3+k4*d4. In this case if you want the data corresponding to the second node then simply multiply the whole equation with the k2. This will give d2 as (k1*d1+K2*d2+k3*d3+k4*d4)*K2=d2. So by this we can show that any numbers of nodes are allowed to send the data, the server will accept all the data and which ever has to be extracted will be just multiplied with corresponding key. This gets the corresponding data. Hence the concept of Multiple access.

9.3 GEOGRAPHICAL PROBLEMS:

This is the problem regarding the area where technical facilities like mobile tower or Internet service is not present. In this case will convert the vote and retina pattern into the electrical information and pass it through the electrical conductors until we can reach the area where the technical facilities like internet or mobile tower is available, and if only internet facility is available is then we can convert this electrical information to digital means and with these data using computers connected to internet we can pass the vote and retina pattern. Here the eye scanner will be web cam.

10. 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.

11. 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 with in minute after a completion of voting. Minimum manpower Utilization, hence mechanism is error free.

12. REFERENCES:

1. David Chaum. Secret-ballot receipts: True voter-verifiable elections, 2004.

2. R. Mercuri. Explanation of voter-verified ballot systems. ACM Software EngineeringNotes (SIGSOFT), 27(5). Also at http://catless.ncl.ac.uk/Risks/22.17.html.

3. A. PRosser, 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.