Global Wireless E-Voting system

[1]J.E.Nivetha, [2]K.Kiruthika
[1,2]Dept. of CSE, Panimalar Engineering College, Channai, Tamilnadu, India

Abstract
In the current system of technology, the voting machine is not much secured. The present electronic voting machine cannot able to determine whether the candidate is eligible or not and the whole control is kept in the hand of voting in charge officer. Another problem with the present voting machine is that anyone can change the vote count, because the vote count is kept their itself. In this new system "Thumbprint scanner as a candidate button in Global Wireless E-Voting system " grasp can instigator the relatedness of the punter by scanning the fingerprint pattern in candidate button itself and also the result is not kept their itself instead of it is store in the remote server by converting it into radio waves. Consequently there is no fortuitous to change the reckoning, and no chance to allow illegal voter to vote. When there is any problem in the voting machine there will not be harm to continuity of the election process and vote count.

Keywords
E-Voting, Scanner, Finger Print, Thumbprint, Machine

I. Introduction
The elections system has superlative weight age. Therefore it should be protected and competent in the apparition of modern technology we are "fingerprint scanner as a candidate button in Global wireless E-voting ".

A. Contemporary System
Contemporary voting system is undertaken by electronic machine to cast voting. During election each and every booth is given a voting machine which cans stores votes casted by candidate. Control of each booth is given in the hand of in charge officer. He test out the eligibility of the candidates and allow them to enter their votes. Finally all the voting machine gathers at one place and counting take place.

B. Disadvantages of The Present System
If any methodological problems or damage occurs with the machines during election it may results to the re-election. The machine is not so intellectual to distinguish the eligibility of a candidate, so the besmirched officers may misguide the candidate. The tainted officers may swell the count of the voting. During hauling of the machines the in charge person can change the rank of machines and even may demolish. This system is not so cost lavish. For election process we need protection, in charge officers, secured place for booth and counting. The individual from any other constituency cannot vote for a candidate of other region because of the fingerprint scanner. The voting takes place in booths only.

C. Proposed System
In this new system we are keeping counting of votes in to a far-flung secured system. we are using electronic circuit which records the votes and transfer votes to distant system as a radio wave through mobile towers. This new system can check the eligibility of the candidate using finger print scanner in the candidate button, therefore no corruption occurs. Machine itself is computerized to verify the eligibility of the candidates. By this method we need not go for the re-election even if the machine is smashed. A person even can vote from a mobile system and also from Internet.

D. Detail Diagram of the Voting Machine
The voting machine is in point of fact a device which produces the different voltages for different votes these voltages are nourished to the convertor which is then rehabilitated to digital bits then it can be converted to radio waves.

II. Fingerprint Scanning
An optical scanner shining a bright light over your fingerprint when people place their finger on candidate button to caste vote, at that time it takes effectively a digital photograph. If you've already photocopied your hand, you'll discern unerringly how this works. Instead of producing a grimy black photocopy, the image feeds into a scanner. The scanner uses a light-sensitive chip called a CCD (charge-coupled device) to produce a digital image.

Fig. 1: Optical Scanner

A. Interface Device
Through this kit we can convert the input digital signals such as (fingerprint pattern+ votes+ secure bits) to radio waves.

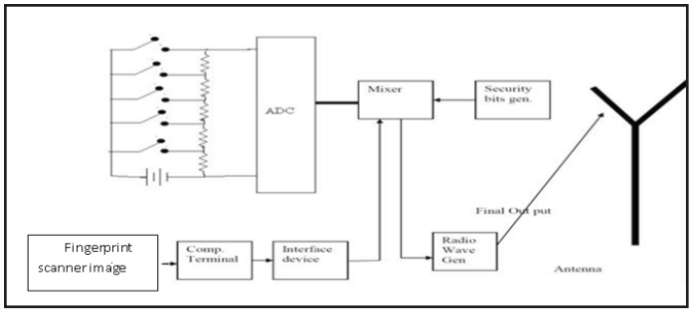


Fig. 2: Block Diagram

B. Working of Whole System
Whenever punters enter to voting sukkah then he will be inculcated to unswervingly enter his vote, so fingerprint scanner button which located as candidate button will scan his fingerprint and

voting machine register his vote. Therefore no illegal voter can enter some others vote, because the fingerprint scanner which is located as candidate button will recognize the illicit finger print which is not deposited already in the secluded system ie. He/she not belong to that area. Now the fingerprintpattern is converted to radio wave of mobile frequency range by an interfacing device. Through mobile tower waves are sending to remote system where the endorsement and voters ID is stored into a secured database.

The conventional data is first rehabilitated into digital configure from the radio waves through the interface device kept the server side, and then fingerprint pattern and votes are estranged. Next the fingerprint pattern is harmonized beside the obtainable database. If any contest is found then flag is check which indicates its voting status i.e. if the constituent is not nominated yet then positive acknowledgement is send to the mobile tower and then to the analogous ballot unit. This acknowledgement is renowned by the receiver kept at the person on the electoral roll side and machine is allow to get next fingerprint pattern and vote, otherwise if–ve acknowledgement then alert alarm is made to ring.

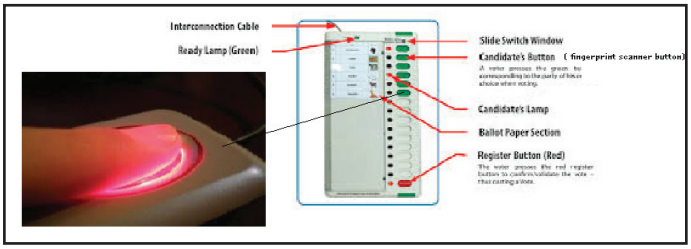


Fig. 3: Radio Wave From Finger Print

C. Hurdles in the Path of Performance

There are numerous is problem that we have to consider along the accomplishment such as

- Security
- Efficiency

Another problem is that one may ambush the radio waves in between and can determine the voter and the vote. This may unveil the result of the election prior to the finishing point of the voting process. To steer clear of this dilemma we can go for rub in the efficient and complex encryption system so that the lucidity of data can be concealed and the attendant side the scrambled data can be again decrypted and original data can retrieved this make the trap of beckon futile. The encryption algorithm can be termed as Key ComplexAlgorithm, which is as follows,

- Primarily it finds the length of the string.
- Spawn the random numbers equal to the length of the string.
- Add the consequent Characters from the given string and random values.

E.g. SHITI

Let this be the given words. Geographical problems

III. Security

The radio waves of a mobile frequency consist of fingerprint pattern and vote can be generated by means of peripheral source. That's why we need to provide some set of sanctuary to shun this predicament. One of the idea to solve this problem is CDMA (which will be explained later)and another modus operandi is inserting defense bits at customary hiatus of time during the transmission of radio waves (Ex.1 msec) At the server side after the given hiatus (1 msec)sanctuary bits are plaid (ex 1001) . In case of encouragingsanction we can accept as convincing vote, otherwise simply redundant.The length of the given string is 5. So let us generate the 5 random numbers .Let numbers be

A) 12 34 4 11 9 .

The ASCII values for SHITI are

S H I T I

B) 83 72 73 84 73

Add corresponding A) and B) values as

12+83 34+72 4+73 11+84 9+73

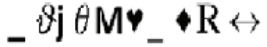
95 106 77 95 82

The analogous ASCII characters for these are

_ j M _R

The analogous characters for random values

at last put into code data as



The ensuing 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 uncomplicated.

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

IV. Efficiency

Whenever the data which is sent from the constituent (client) side, it is in the bulky quantity, this adjournments a bit a voting system and the statistics that is conventional at server side is in the Multiple access mode i.e. more than one client is sending the data. To triumph over this problem the following

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

As an alternative of using solitary server PC we will go for disseminated Operating system environment with multiple servers. This makes the job allotment and dispensation faster which leads to hasty responds in occasion of Multiple Access Environment.

CDMA Tecniques:

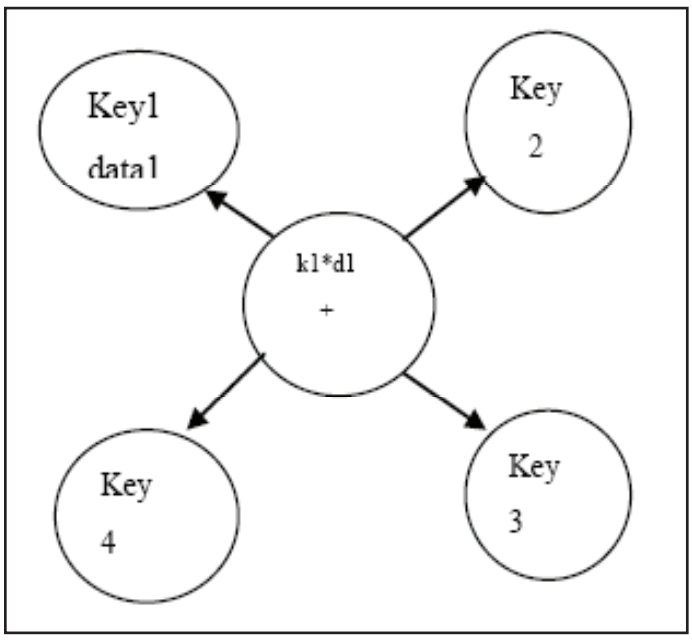


Fig. 4: Efficiency Key Value

To unravel the concurrency problem in case of multiple access environments we will use CDMA technique Key values are orthogonal to each other i.e. k1*k2=0 and k1*k1=1 i.e. if any tries to decipher the information with any supplementary key the data will be gone astray as the data will be in the form d1*k1.If you try to decode with K2 then magnitude will be as d1*k1*k2=0. This will evaporate the data. And if correct deciphering key i.e. k1 is used then interpreting will be d1*k1*k1=d1. This decodes the data fittingly. As per the scheming concurrency for multiple accesses the information from all the nodes is customary as k1*d1+k2*d2+k3*d3+k4*d4. In this case if you want the data subsequent to the second node then simply multiply the whole equation with the k2. This will give d2 as (k1*d1+K2*d2+k3*d3…)*K2=d2. So by this we can spectacle that any records of nodes are allowed to propel the data, the waitron will consent all the files and which ever has to be mined will be just burgeoned with corresponding key. This gets the corresponding data. Hence this is the impression of multiple accesses.

V. Geographical Problems

This is the crisis concerning the area where technological amenities like mobile pylon or Internet overhaul is not in audience. In this circumstances will convert the vote and fingerprint pattern into the electrical information and pass it through the electrical conductors awaiting we can reach the area where the practical amenities like internet or mobile tower is available, and if only internet competence is available is then we can adapt this electrical evidence to digital means and with these data using workstationsallied to internet we can pass the vote and fingerprint pattern. Here the fingerprint scanner will incarcerate image.

VI. Future Enhancements

This project can be superior to work over the mobiles that is selection is made possible through the cell phone through SMS. This machine can be made secret ballot through the internet.

VII. Conclusion

By this way the machine can be used for any level voting tenacity. The machine affords high level of fortification, endorsement, steadfastness, and sleaze - free mechanism. By this new way we can get result within minute after a achievement of voting. Bare minimum manpower exploitation, hence method is blunder free. By this way one can vote his own vote.

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.