ISSN No. 0976-5697

Volume 2, No. 2, Mar-Apr 2011

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Internet Voting (e-voting) in Indian Environment

Sanjay N. Kandekar*
AES collage of computer science & Management
Narhe -Abemgoan,
Pune, India.
Sanjaykandekar2000@yahoo.co.in

Dr. Ashwinikumar P. Dhande
Professor and Head
Pune Institute of Computer Technology,
Pune, India
ashwpict@yahoo.com

Abstract: Voting may seem like simple activity – cast ballots, then count them. Complexity arises, however, because voters must be registered, and votes must be recorded in secrecy, transferred securely and counted accurately. Votes can be lost at every stage of the process. Two simple problems are to blame, first registration database error and second poor design of system (ballot or machine). In case of Indian election, electronic voting machine like DRE is used from 2004 election. This machine has its own merits & demerits. Voter cast their vote by going to the polling booth, where he or she has to press one button next to the candidate. But the voters which are 1000 and more kilometer away from their constituency relay on slow postal system. So can we send our vote to particular EVM (booth) in particular constituency by using internet? This is the main theme of this paper

***Keyword:*.** Internet voting, e-voting, Global e-voting, local e-voting, multimodal e-voting, E-VS, Security

I. INTRODUCTION

Through the centuries, different technologies have done their best. In ancient Greece, Egypt and Rome, marks were made for candidates on pieces of discarded pottery called ostraca [1][2][3]. This gave way to paper ballots dropped in sealed boxes. Other modern technologies are lever machines, punch-cards and marks-sense ballots (where each candidate's name is next to an empty oval or other shape that must be marked correctly to indicate the selection & scanner counts the votes automatically). New computerized voting machines promise even more efficiency and internet voting even mare convenience.

But in the rush to improve speed, scalability and confidential voting, accuracy has been sacrificed. Accuracy is how well the process translates voter intent into appropriately counted votes [2]. Following Table-1 summaries the benefit and drawback of method and suggest to improve them.

II. BACKGROUND

Before we discuss any machine or technique, we need to explain why voting is so difficult. A voting system has four required characteristics [1].

A. Accuracy:

The goal of any voting system is to establish the intent of each individual voter and translate those intents into a final tally. To the extent that a voting system fails to do this, it is undesirable. This characteristic also includes security. It should be impossible to change someone else's vote, stuff ballots, destroy votes or affect the accuracy of the final tally.

B. Anonymity :

Secret ballots are fundamental to democracy. Voting must be designed to facilitate voter anonymity.

C. Scalability:

Voting system need to be able to handle very large election.

D. Speed :

Voting system should produce result quickly.

III. PROBLEM WITH EMERGING TECHNOLOGY

As the technology advancing on each step more potential errors are coming, simply because no technology is perfect. For example – consider an optical-scan voting system. The voter fills in the ovals on a piece of paper, which is fed into optical scan-reader. The reader senses the filled - in ovals and tabulates the votes. This system has several steps and at each step error can occur. If the ballot is confusing, some voter fills the wrong oval. If a voter doesn't fill them in properly or if the reader is malfunctioning, the sensor won't sense the ovals properly, mistakes in tabulation – either in the machine or when machine totals get aggregated into larger totals also cause error. The error relates in modern system can be significant, some voting technology have a 5% error rate, which means one in twenty people who votes using the system don't have their votes counted[3].

The current debate centers on all computer voting system like EVM (Touch screen system called (DRE) direct record electronic machine used in USA & Europe) In these system the voter is presented with list of choices on a machine, he indicate his choice by pressing button. These machines are easy to use, produce final tallies immediately after polls close and can handle very complicated elections.

.

Table- 1 Existing Voting Technologies

TECHNOLOGY	Hand-counted Paper ballots	Lever machines	Punch cards	Mark-sense ballots	Electronic machines	Internet voting, phone messaging, Interactive TV
COMMENTS	Used in India before 2004.	First used in 1892 in Lockport ,N.Y.	First used in 1964 in Fulton and De Kalb counties, Georgia.	First used in 1962 in California.	First use in 1976.	Internet voting first used in 2000 primary Phoenix, Ariz.
ADVANTAGES	Simple. Lowest residual rate.	Over-votes are impossible. Guarantees secrecy of votes.	Removes human error of tallying. Compact machines.	With in-precinct scanning, has lowest residuals of any mechanical method. Easier than punching holes. Voter can read candidate's right on ballot.	Over-votes are impossible. No human errors of tallying. Easy for people with physical disabilities to use. Good feedback.	Vote from home. People with physical disabilities can use their own special-needs setup. No human errors in tallying.
DISADVANTA GES	Recounts differ from original count by twice as much as machine counted voters do. Persistent allegations of votes being altered, added, lost and so on.	Bulky, massive machines. Defective odometers: common. Misreading of odometers Voting falloff on lower races. (for Senate, state office, for example)	Hard to punch holes correctly Often punch wrong hole. Ballot design troubles. Card-reader jam frequently	Ballot readers are slower harder to calibrate and more prone to jamming than card readers. Bulky ballot. Ballot easy to spoil.	User interface often poor. Concerns about malicious software. Concerns about computer obsolescence.	Concerns about malicious software, network problems and hackers.
WAY TO IMPROVE	Count by mechanical scanner Treat paper with light ,heat or coating to make vote indelible.	Check and service before each election. Monitor odometers with video cameras. Improve labeling of groups of levers forming a race. Adjustable height of machines.	Optical way to check ballot while in booth might help.	Use an in-precinct scanner to catch problems and give the voter a chance to vote. Use DRE to mark ballot. "Fill in the shape" version better than "connect the arrow" version.	Test ballots. Consider closed systems. Test system, including on day of elections.	Use special Web browser. System on a CD. New approaches to security needed, such as multiple software agents.

IV. SECURITY

Software can be 'hacked'. That is someone can in deliberately introduce an error that modifies the result in favor of his preferred candidate. This is more dangerous when we connect voting machine or system to the internet. The threat is that the computer code could be modified. Its, much easier to modify a software system than hardware system and it is much easier to make these modifications undetectable. A software problem whether accidental or intentional can affect many thousands machines and skew the result of an entire election [6] [7].

To prepare for a fraud free voting day requires that every effort be made to create voting machine or system that do not harbor malicious code. The computer science research community is constantly debating the question of how to make provably secure software [8].

Computer security experts have devised many approaches to keep computer reliable enough for other purposes such as financial transactions. Financial software transfer huge money every day is extensively tested and holds up well under concerted attacks. The same security techniques can be applied to voting system. The best future schemes might include computer agents that check one another and creates internal audits to validate every step of the voting process.

A. E-Voting

If you want to vote on internet for particular constituency or EVM or booth, we cannot use EVMs because we cannot connect them directly to the internet (no provision is made in EVM for internet) so we can design the remote voting application using the web [9]. This application called Internet voting or e-voting. To vote online, one has to use the voters pin printed on the card. All the equipments relative to e voting is connected to a specific network and separated from it by a firewall. Direct access to the database server containing the e-Ballot box is impossible. The system will use two types of server internet/application & data base sever. At slightest sign of failure a signal is transmitted to the operator who takes necessary action [10]. The monitoring system also checks the e-voting home-page; any modification attempt will trigger an alarm. The number of votes received is compared with number of entries an electrol- roll any discrepancies will set up an alarm [11].

B. Need of Project

Many countries are currently working an e-voting solution or mobile phone voting system.

[a] Peoples are called 2/3 times a year to vote and internet –voting is easy for them.

[b] About 6.9 % Indian population has internet access at home or office or internet cafe

[c] Millions of Indian lives abroad.
[d] Existing EVMs are not developed for remote voting.

C. Prerequisite for Democratic Ballot on Internet

[a] The votes cannot be intercepted, modified or diverted.
[b] Nobody will have access to the votes before the official opening of the e-Ballot box.
[c] Only registered voters will have access to the e-voting application.
[d] Each voter will be able to vote only once using whatever voting method he/she has chosen.
[e] The secrecy of the vote will be guaranteed there will never be a link between vote & voter.
[f] The e-voting site will resist any attack.
[g] Voter will be protected against any attempt of identity theft.
[h] The number of cast ballots will be equal to the number of received ballots. It could be proved that a given voter has cast a ballot.
[i] The system will not accept any vote outside the voting period.

I. Procedural Security Measure [a] e-ballot box opening (server side) is open to any citizen & Monitored by representatives. [b] e-ballot box is locked by two keys password defined by representatives. [c] Testing e-ballot box.

II. Technical Security Measure [a]. A ballot is encrypted by randomly mixing alphanumerical characters. [b] When the ballot is returned to the voter for confirmation of choice and to add his ID features. [c] Voters identity & ballots use kept in two distinct files. [d] Before opening the content of e-Ballot box is shaken by applying an algorithm.

V. INTERNET VOTING SCHEME

It has four Stages [a]. To be recognized as a citizen being entitled to vote, the voter gives his card number. He has five attempts to do so. When recognized as an authorized voter the connection is made with secure server & the voter is sent an e- ballot. [b] He / She votes. [c] The system submits a recapitulation of his choices .The voter confirms or alters his choice. [d] The system confirms it has recorded the vote.

I would like to suggest two models - [i] Local e-voting model [ii] Global e-voting model **Figure2.**

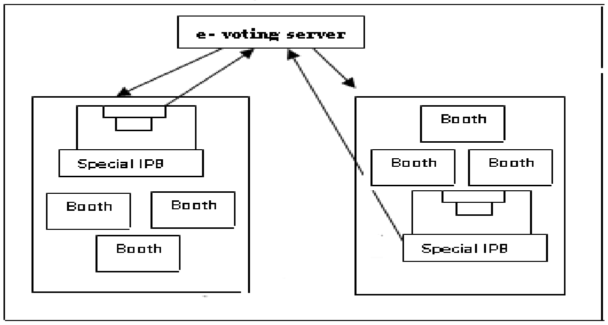

Figure.2 Local E-Voting

A. Indian E-Voting Schemes

The above mentioned information not necessary true for Indian election. Because we can not connect the existing EVM with web. And connection with EVM is not required because we can develop voting application on net itself called online voting application. Even there is no need to change exiting system , instead we can put 90:10 approach ,in which 90% EVM will records the votes directly at booths and 10% vote will cast on internet (i.e. by developing e-voting application)

[ii] Local E-Voting Model

The above fig.2 shows, how actually Local e-voting model could be done using local model, in which only registered voter outside their constituency or city or village or EVM can vote on internet. But they cannot use voting application at home or office. But they have to come at Internet pooling booth (IPB), where officers will check his/her identity and voter can use his Pin for voting.

I. Global E-Voting Model

Local model is only for voters those are living in India, but what about that voter who is abroad? For this we can suggest global model which act like common internet site or application and globally we can access it within stipulated time interval. Here we need to give importance to the security majors. Here we can divide application in two files internet program (front end) & registration database (back end), with appropriate firewall protection, auditor agents and other security major [13][14][15]. Using this model we can vote, provided that you should be registered voter of particular constituency. For identification personal identification number is enough. But we can use more sophisticated technology like **iris recognition** or **thumb impression**. The e-voting application will open for one or two minutes and after successful voting it will not open again for same voter.

VI. MULTIMODAL BIOMETRIC SYSTEM FOR LPB

Both Local Polling Booth and Global Polling Booth are possible in India. But LPB model is appropriate for polling on internet. We have to concentrate on two things mainly. Internet Security and Identity verification of voters.

As we already discussed probable major for internet security so that we can keep ‘hackers’ away and software agents will check the anomalies on the server. Another important thing is that how to identify the registered voters. Personal Identification Number (PIN) is adequate but it is not sufficient in Indian environment, because voter will sale their PIN to the parties who is giving them money. To prevent this we can design very sophisticated technology called multi-model Biometrics system for identity verification. This system can use three traits (iris, finger-print and signature) for each individual registered voter [16][17]. The final decision is made by combining results of these traits and comparing this result with already stored template records (database) of registered voter. Combining techniques for iris, finger print and signature is called fusion. See **fig.3**.

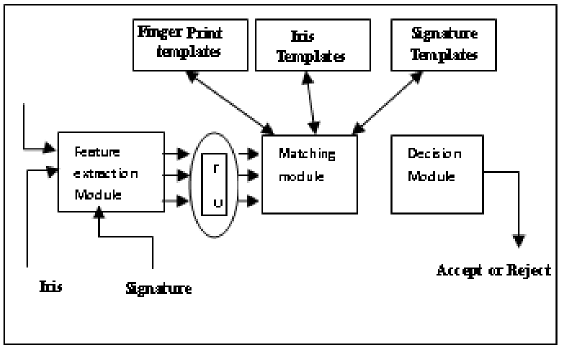

Figure: 3

Biometrics means life measurement; unique physiological characteristics are used to identify an individual. For example Face, Finger-prints, Hand-Geometry, Hand-writing, Iris, Retinal vein, Voice etc. Biometrics technologies are becoming the highly secure identification and personal verification solution. As level of security on polling booth increases, the needs for highly secure identification become important. Multi-Biometric system uses multiple sensors for data acquisition. These sensor capture different biometric traits and such system are expected to be more reliable due to the presence of multiple pieces of evidence. Multi-modal system also provides anti-spoofing measure by making it difficult for an intruder to spoof multiple biometric traits simultaneously.

Multimodal system can operate in one of the two modes, Serial or Parallel mode. In serial mode the output of one modality is used to narrow down the number of possible identities before next modality is used. Therefore multiple traits do not have to be acquired simultaneously and decision could be made before acquiring all the traits. In parallel mode of operation, the Information from multiple modalities is used simultaneously in order to perform recognition.

The Levels of fusion proposed for multimodal system are categorized into three system architecture [18][19]

Fusion at Feature extraction

Fusion at Matching Score Level

Fusion at Decision Level

But for LPB, we can design system in which, voter either use his/her finger print or iris or signature or will uses all above techniques. Separately FEM extracts information from different sensors which is then compared with template (database) with the help of matching module. In decision module final decision is made i.e. whether accept or reject. See Fig.3.

Following points summarizes the details of traits used in LPB.

Fingerprint verification: The input image is enhances to bring out obscure information based on Gobar filtering and matching is done by combination of reference point and minutiae matching algorithm

.**Iris Recognition:** The input mage is localized by finding the papillary and outer iris boundary and is matched using combination of Harr Wavelet and circular Mdlin Operator

Signature Verification: Consist of Global and local feature of signature image and is matched using Euclidean Distance**.**

VII. CONCLUSION

Present system of voting in India is good and less problematic. But about 7 to 10 percentage of educated and highly qualified registered voter unable to cast their vote because of they are away from the constituency. **This system is using bimodal biometrics for identification of voters and internet technology for remote voting.** If we develop system for them defiantly percentage of overall voting will increases. Voting is major right in India and every citizens(registered) should vote. I hope my remedy for e-voting will work, but more research is a needed for security and accuracy.

VIII. REFERENCES

[1] Bruce Schneier (November 9, 2004) “What’s wrong with electronic voting machine?”

[2] Alan Agresti & Bret “Misvotes ,undervotes & overvotes” Statistical science

[3] Rebecca Mercuri “A Better Ballot Box ?” in IEEE spectrum. Voting Machines – scientific American

[4] Robert Hensler (2003) “The Geneva Internet voting system “

[5] Alexander, K. (2001) "Ten Things I Want People to Know about Voting Technology"

[6] Boutin, P. (2004) "Is E-Voting Safe?" PC World magazine, 6:1-6. Task Force. National Press Club, Washington, DC

[7] Chevalier, M. (2004) "Evoting project, State Chancellery of Geneva, Swiss" http://www.ge.ch/evoting.

[8] Mercuri, R. (2000) "Voting Automation (Early and Often?), Inside Risks" Communications of the ACM, vol.43, n.11.

[9] Mercuri, R., Neumann, P.G (2003) "Verification for Electronic Balloting Systems" Secure Electronic Voting (Ed. Gritzalis, D.A.), pp. 31-42. Kluwer,Boston.

[10] Neumann, P.G. (1993) "Security Criteria for Electronic Voting" Proceedings of the 16th National Computer Security Conference, September1993.

[11] Phillips, D.M. & Jefferson, D. (2000) "Is Internet voting Safe?" VIP Report, [online], http://www.votingintegrity.org

[12] Riera, A. Brown, P. (2003) “Bringing Confidence to Electronic Voting” The Electronic Journal of e-Government Volume 1 Issue 1, pp 43-50, available online at www.ejeg.com

[13] Riera, A. Ortega, J. Brown, P. (2003) "Advanced Security to Enable Trustworthy Electronic Voting" Proceedings of the 3rd European conference on e-government, Dublin, Ireland, p.p. 377-384.

[14] Rubin, A. (2001) "Security Consideration for remote electronic voting over the Internet" AT&T labs – Florham Park, NJ, http://avirubin.com/evoting.security.html

[15] Schryen, G. (2004). “Security Aspects of Internet Voting”, Proceedings of the 37th Hawaii International Conference on System Sciences (HICSS 37), January 2004.

[16] D. Chaum. Secret-ballot receipts: True voter-verifiable elections. IEEE Security and Privacy, 2(1):38– 47, 2004.

[17] Compuware Corporation. Direct Recording Electronic (DRE) Technical Security Assessment Report, Nov. 2003.

http://www.sos.state.oh.us/sos/hava/files/compuware.pdf

[18] A. Ross and A. K. Jain, "Information fusion in biometrics," Pattern Recognition Letters, vol. 24, pp. 2115–2125, Sep 2003.

[19] Y. Sutcu, Q. Li, and N. Memon, "Secure Biometric Templates from Fingerprint-Face Features," in Proceedings of CVPR Workshop on Biometrics, Minneapolis, USA, June 2007.