Available at: www.researchpublications.org

Difficulties in Design of Electronic Election System

Dr. Vinod. M. Patil Head,
Associate Professor Department of Computer Science,
Shri Shivaji College of Arts, Commerce and Science
Akola-444001, MS, India
e-mail: vinmpatil2@yahoo.co.in

Sanjay Dhopte
Associate Professor
Department of Information Technology
Prof. Ram Meghe Institute of Technology and Research
Badnera 444601 Dist. Amravati , MS, India e-mail:
sanjaydhopte@gmail.com

Abstract: ***While designing of full electronic voting system, it confirms that it is totally unpractical for one system to solve simultaneously all the e-voting requirements and conditions. It is clear that there is a discrepancy between authentication and verification on one side and anonymity on the other part.. The other part of the design of electronic voting system make so simple that the traditional or manual voting system handles should also operate the e-election systems. The newly design an electronic voting system must satisfy eligibility, privacy, security and fairness. In the execution of e-election process voters have guaranty that their opinions recorded correctly after the voting completed and also the system reflect exactly that an election can be conducted on fairly and correctly without any particular party's intention.***

Keywords: ***Secrecy, security, accuracy, privacy, voter, poll worker etc***

I. INTRODUCTION

In the designing the electronic voting system by considering of all legal, political, social and technical aspects, it is very important to achieve the simultaneously voter's privacy and verification of voters votes. What an election authority should take a step for the purpose of verifying the validity of the ballots and voter's identity. Since the polling officer doesn't know about the information related to the voter and the ballot.

In the view of other side, that a voting system must be so robust, to tolerate any kind of attacks, viruses and wrong operations of the voters or poll officers and independent of scaling of voter's size. i.e. the election can conduct, any kind of small size, large size or medium size and also the multiple voting or choice base or preference basis voting systems. It must be easy to use and operate the system and that citizen can get the guarantee their votes will be recorded correctly in the final tally and expect that the result should be declared as soon as possible. The systems that adopted are satisfied all most all requirements of the election process if possible.

The design of electronic voting system makes so simple that those non electronic voting system to do the election process. An electronic voting system must satisfy eligibility, privacy, security and fairness. Eligibility means that only the valid voter can take part in the election process and the voters must show a proof of validity of their identities. In the real life, a voter can do it by showing his ID card or other information such as bio-matrix characteristics etc. However, in an electronic voting system, this information can be achieved by using bio–metric multipurpose identity card also.

In a public network like internet, it is very difficult to prove someone's legal identity. Since in open structure of network that the information passed can easily be caught and modified by attackers or hackers at any part of the network and at any time. On the other hand, polling authorities will not work efficiently and correctly and trustfully when they are under the influence of attack.

II. DESIGN ASPECTS:

There are some main problems to solved during design of electronic voting system.

- **Depending on trusted third party:**

In some voting system, the procedure of collecting ballots completely depends up on a trusted third party. In real life, it's a very difficult to find a completely trusted third party in a web. In some important elections situation, it will be very dangerous to establish the security of the whole system on a third party. In case the third party is controlled or under the influence by a certain attacker or political party, the voting system probably would be collapse.

- **Complexity of computing and communication technology:**

Considering to the point of designing of e-voting system or a algorithms the voting system becomes so complicated that decrease efficiency of the system but it's is become more and more secure as compare to the other voting systems. Consider the example; some scheme realizes an untappable channel by means of deniable encryption. However, research shows that 105 bits information in other channels must be passed only if passing 1 bit information in a logical untappable channel. That is the system will be very complicated if the scale of voting becomes larger.

III. Other important issues of EVS:

Other Important issue relating to the electronic voting system should be considering during the exhibiting of system.

a) Casting of Vote Anywhere:

In India, each voter has assigned a unique Identification UID and constitution where their name is registered on that electoral list and election authority prepares list of voters. In order to vote, the voters identity is authenticated to that constituency and consequently they can be authorized to vote to that constituency for the desire contesting candidates. (if they have not already done so). For the purpose of checking that the particular voter has already voted or not voted required a simple protocol just after a voter cast their vote. The arrangements are required to developed system that a public announcement of this are made in the bulletin board.

The new achievement of the e-election system is that a voter should not be binding to go to a particular polling

booth in order to vote; they should be able to go to any authorized voting booth across the nation.

There are three main issues that are arising during the vote anywhere exhibiting system:

- Firstly, how do know that the voter has not already caste a vote at a particular polling station?
- Secondly, How to count the voters cast their vote only once in her / his constituency?
- Thirdly, how do generate the correct ballot (corresponding to that polling both) where this depends on the constituency for which the voter is registered to vote and independent of the polling booth where they went to vote?
- How the voters guarantee that the casting vote recorded correctly in the final tally.

b) Choice of Re-vote:

Facility of allowing a voter to change their choice and to re-cast a vote is one which often arises when voting can be done under the influence of any political party or under the pressure of any unwilling person before closing the election process. One could argue that allowing re-votes could hinder vote coercion in this situation.

This new required functionality for e-voting system:

- After a voter casting a vote then there is no way of accessing the ballot or contents of ballot until the voting process is closed. This mechanism is required to ensure that no one can add or remove votes during the voting process.
- No links are require to found between voter and the ballot in order to identify the identity of the voter to whom the particular voter cast their vote in his/her constituency.
- The voting process is required to so transparent that which assists verification of the fact that no votes are recorded before to start voting process and no unauthorized person already use the power of casting a vote in place of authorize citizen. Transparency means that, in order to meet the additional requirement of secrecy.

The e-election system should support re-voting provided that there is a mechanism to finding the ballot of a particular voter in the ballot box without disclosing the identity of voter and preserve the voter's privacy. Identify such ballot as being signed by authority.

Here apply the some technique in order to preserve the voter's privacy, by generate pseudonyms for each voters that cannot directly link to the voters registration or identity. Also cannot identify the voters by the election authority or any political party or anything else without the permission of voter and other groups form for the purpose of privacy. The group means consider the different groups related to the political party, related to the NGO or social groups or any individual verification and related to the election authority itself.

c) Casting of re-votes anywhere:

The requirements of interdependency between the Vote Anywhere and Re-vote, as both features must be need in e-election system. The main issues are whether being able to vote multiple times at different polling stations is functionally possible and, if so, continue an offer and only the last choice of vote should counted in the result as per the recorded time during the voting process.

The interdependency, in this case, is not avoidable in the classic sense of requirements. The feature interaction and analysis will show that the Revote feature can help in the process of designing a solution to the Vote Anywhere non-functional requirement that can cover a denial of service attack on the network and cannot compromise the voting system.

d) Quality of Service Requirements:

Most of the citizen complaint about the quality of service the issues raise with many voting systems including both traditional and electronic voting system around the world. A significant number of voters were in queue for more than an hour in order to cast a vote in the newly introduced electronic voting machines; and as a consequence some voters left without recording a vote. These problems arise due to a number of traditional voting booths being replaced by a single voting machine. However, it observed that no one thought to analyze whether the new electronic system offered the same quality of service as the traditional system. The most significant threat is being able to get quality of service requirements that is a denial of service, where users of the system are unable to execute core functionality and would prohibit anyone from recording a vote. If an e-voting system depends on components that are accessed across a network then a significant number of denial of service threat would arises and in such case if the network was not reliable then it will not resistant to attacks and hacking. However, it is also a concern in electronic voting system, where the network is a key component of e-voting system.

IV Parameter to consider:

The following parameter should be considered during construction of electronic voting system in order to optimize the system.

A. Voting system accuracy:

In democratic process, every voters expect that what so ever it may be the voting system, it must be 100% accurate. At the point of theoretically consideration, a computer-based system should be virtually 100% accurate and they are operated on binary system therefore failure rates will be very low. On the other side analog systems involving complex gear trains, card punches, optical sensing or human judgment are known to have significant error rates. Unfortunately, computer-based systems have not proven to be 100% accurate .

B. Voting system security:

Many national politicians, state politicians, computer experts and concerned citizens are clamoring for security of hardware and software of electronic voting systems.

Three things should consider about the security point of view:

1. The easiest ways to affect an entire election system is to buy or sale absentee ballots during execution of election process.
2. If election commission uses the one type of voting

system in entire election process than if causes one type of attack then that creates major havoc in entire system.

3. Finally it diver towards the little demand on absolute bullet proof security in the entire voting system.

C. Voting system trustworthiness:

It expects that the electronic election system must be sufficiently robust in order to withstand a variety of fraudulent behaviors and must be sufficiently transparent and comprehensible that voters and candidates can easily accept the results of an election. Actually absolute trustworthiness cannot be proven; it can merely be clear from a lack of negative data. Negative data can include objective information such as clearly recorded failures, and subjective information such as suspicious expected secrets and questionable behavior, motives or associations.

Electronic voting scheme has arises many problems to implement that are because the digital data are copied exactly to the original one. It is possible that, multiple copies of eligible ballots will be sent to the voting authorization center by dishonest voters. It also possible to suffers from the tapping of the public communication networks by hackers. More serious problem in electronic voting system is participants can figure out who voted for whom from the public channel.

D. Distributed Trust:

In the e-voting process each procedure is supervised by multiple authorities, and the final result cannot be disclose without the cooperation of a given number of authorities. To identify the intermediate procedure or any attempt to undermine the procedure of election will require the corruption of a large number of authorities. In some process authorities and voters may overlap arbitrarily and thus, it is may possible for the voters themselves to ensure trustworthiness or have an active role in it.

E. Voting system usability:

Recent available advances in the different communication networks and cryptographic techniques have made possible to consider on-line voting system as a feasible alternative over conventional elections system. In response to this on-line electronic voting allows voters to participate in an election process from any where they are physically present at the moment of the voting process depending upon the availability of a wired or wireless Internet connection to the system servers.

F. Cost Reduction:

Considering to the economical point of view, this will be force to consider the economical study of the e-voting system. It is also known as study of economical feasibility of the electronic voting system. It is observed that if the voting scheme in real life is replaced with computerized voting, election expenses can be considerable reduced as compare to the traditional voting system. Since the traditional voting system require expenses are larger due to the physical equipment involvements, transportation, organization of election authority, poll workers, vehicle management to the polling booth etc. are very difficult to manage and cost of arrangement of this activity is also large. On the side if replace it by electronic election system the number of manmade activity will be considerably reduce due to utilization of existing infrastructures like communication network and computer resources.

G. Decrease of invalid votes:

Invalid votes can produce deliberately or unconsciously or by mistake. Deliberately producing invalid votes are presumably protested against politics in general, therefore they must be provided in online elections. Unconsciously produced invalid votes could be already identified at “feeding time“ with plausibility checks, so that the voting software could point out this mistake. This means a difference to traditional polling booths. Whether this kind of restricting the democratic “principle of equality” is tolerable has to be examined legally.

H. Lower election fraud in endangered countries:

The security of traditional elections will base on the confidence in persons and in the independence of election committees. For example, in the context of political polls in any polling station at any time there are several persons belonging to different parties, and the counting takes place at another location by other people. In endangered countries with young democracies the confidence in these mechanisms is lower, and a shift from organizational security precautions to technical ones (e.g. cryptographic coding) might be helpful. However, it is necessary to mention that the coexistent use of organizational and technical security precautions features a gradual character, i.e. the securest technology can always be annulled, if all organizational units involved cooperate corrupting.

V. E-election system methodology also covers the following points:

- **Aim Achievement:**

During the electronic voting process, the technological, procedural, and sociological goals of the upcoming experiments are defined can served to optimize the developments of the voting machine functions.

- **Advertising:**

The use of e-voting system and the goal of the experiment over e-voting system have been present to the voter by the Advertising by using media publication , video advertisements etc. As per the size of preparation, the phases of experiment are conduct in different ways.

- **Simulation of procedure:**

The e-voting machines have been made available to the voter in public places for experimentation purpose. The simulation require for special configuration of electronic voting machine that allows citizens to vote more than once. The ballot prepare for the simulation containing the candidate names and their symbol and that must be unique and could not match to any local and national party in order to participation.

- **Training of poling officers:**

Training is required for poll worker’s, officers and

election authority in order to the usage of the machines and on the procedures regulating the experiment. The method should arranged for the use of electronic elections with legal value. The experiment can be dividing into two parts: one part regarding the logistical constraints and other part to the qualitatively evaluate. Those are needed to find out the advantages and disadvantages of alternative ways of conducting the electronic elections process.

- **Trial of procedure:**

The e-voting systems and the procedures were carried out for the purpose of trial basis. The trial have been always to be conducted in parallel: one traditional elections process and other with the e-voting system installed in the polling booths where the voting is taking place that dedicated to personnel responsibility for managing the machines by voters. The polling officers of the electronic election system will be asked to follow the procedures like they were in a traditional election with legal value and voter will be asked to repeat the casting of vote.

- **Data Collection and Analysis:**

After applying electronic voting system on the experimental basis, the corresponding data are collected about:

(a) Voters' opinions about the e-voting system data collected through interviews at the polling booths.
(b) Information about the systems' performances and comments.
(c) Regarding the new procedures' adaption's
(d) Related to the view point of voters, weather the new method / system it is advantages or disadvantages and comments.
(f) The candidate's opinion about the electronic devices (Just information, which does not have any legal value).

Here all collected data are used to verify whether the aim had been achieved to fulfill the requirements and, if not, then what kind of changes are require to correct the procedure and corrective actions to introduce for the next cycle of developments and experiment.

VI. Adverse capability:

During execution of the electronic voting system the following different scenarios are understood with regard to the formal capabilities:

- The system has capable to access to public information.
- Communication about the election authority and voter :
  - A one-way communication channel from the voter to the enquiry.
  - A two-way communication channel between the voter and the a enquiry.
- Communication channel about other and each of the election authority:
  - A one-way communication channel from some / each of the election authorities to the a enquiry.
  - A two-way communication channel between some / each of the election authorities and the enquiry.
- Under control of communication channel to the enquiry:
  - The adversary become taps the existing communication channels.
  - Capability of the adversary to control the existing communication channels.
  - The adversary become trace out the IP addresses back to the identities of the senders.
- Adversary about the remote terminals:
  - The adversary can control the voting terminals remotely.
  - The adversary can monitor the voting terminal remotely.

VII . CONCLUSION:

In order to maintain the democratic environment in the nation the election process is play an important role. To achieve this it is necessary to develop a system for voters electronically in a secure and secreate manner by using electronic voting system (e-election). This lead to find a way to do the guarantee to fulfill all the requirements with a relative high degree of security and accuracy against the preserving the privacy of the voters. The design of electronic voting system is a task (difficulty) of covering all aspect that fulfill the necessary requirements along with traditional election process and accepted by all political party, contesting candidates social organization, election commission , faith by voters and government. This design of election process not useful for verification at every stage of election process but also useful after the elections.

VIII. RERENCES:

[1]. John C. Paolillo, SLIS and Informatics and David Heald, "Democratic Participation in the Discursive Management of Usenet", Proceedings of the 35th Hawaii International Conference on System Sciences – 2002, 0-7695-1435-9/02 , Computer Society, IEEE-2002.

[2]. Lina Wang, Jingli Guo, Min Luo, "A More Effective Voting Scheme based on Blind Signature", Computational Intelligence and Security, 2006 International Conference on Volume 2, 3-6 Nov. 2006 Page(s):1507 – 1510.

[3]. HyoungJun KIM, KyoungCheol KOO, KiShik PARK, "Implementation of a Workflow-based Web Application with an Electronic Signature Mechanism", Communication Technology Proceedings, 1998. ICCT '98. 1998 International Conference on Volume vol.2, 22-24 Oct. 1998 Page(s):5 pp. vol.2 .

[4]. Charles A. Gaston, "A Better Way to Vote", Proceedings of the 38th Hawaii International Conference on System Sciences – 2005, 0-7695-2268-8/05, IEEE,pp 1-6.

[5]. Gibson, J.P.; Lallet, E.; Raffy, J.-L.; "Analysis of a Distributed e-Voting System Architecture against Quality of Service Requirements", The Third International Conference on Software Engineering Advances, 2008. ICSEA '08, Page(s): 58 – 64.

[6]. Jared Karro and Jie Wang "Towards a Practical, Secure, and Very Large Scale Online Election", Computer Security Applications Conference, 1999. (ACSAC '99) Proceedings. 15th Annual 6-10 Dec. 1999 Page(s):161 – 169.

[7]. Schryen, G.; "Security aspects of Internet voting", System Sciences, 2004. Proceedings of the 37th Annual Hawaii International Conference on 5-8 Jan. 2004 Page(s):9 pp.

[8]. Langer, L.; Schmidt, A.; Buchmann, J.; Volkamer, M.; Stolfik, A.; "Towards a Framework on the Security Requirements for Electronic Voting Protocols" , First IEEE International Workshop on Requirements Engineering for e-Voting Systems (RE-VOTE), 2009 , Page(s): 61 – 68.

[9]. Aggelos Kiayias, Laurent Michel ,Alexander Russell , Narasimha Shashidhar, "Tampering with Special Purpose Trusted Computing Devices: A Case Study in Optical Scan E-Voting", 23rd Annual Computer Security Applications Conference 1063-9527/07, Computer Society, 2007 IEEE, pp 31-39.

[10]. Weldemariam, K.; Mattioli, A.; Villafiorita, A.; "Managing Requirements for E-Voting Systems: Issues and Approaches", First IEEE International Workshop on Requirements Engineering for e-Voting Systems (RE-VOTE), 2009 Page(s): 29 – 37.

[11]. Xiangdong Li, Michael Carlisle, Andis C. Kwan, Lin Leung, Amara Enemuo and Michael Anshel, "An Elementary Electronic Voting Protocol Using RFID", Proceedings of the 2007 IEEE Workshop on Information Assurance United States Military Academy, West Point, NY 20-22 l-4244-1304-4/07, 2007 IEEEJune 2007, pp 234-238.

[12]. Antonyan, T.; Davtyan, S.; Kentros, S.; Kiayias, A.; Michel, L.; Nicolaou, N.;Russell, A.; Shvartsman, A.A.; "State-Wide Elections, Optical Scan Voting Systems, and the Pursuit of Integrity " , Information Forensics and Security, IEEE Journals , Transactions on Volume: 4 , Issue: 4 , Part: 1, Page(s): 597 – 610.

[13]. Fauzia, N.; Dey, T.; Bhuiyan, I.; Rahman,M.S.;"An efficient implementation of electronic election system ", IEEE, 10th international conference on Computer and information technology, 2007. ICCIT- 2007, Page(s): 1 – 6.

[14]. Weldemariam, K.; Villafiorita, A.; Mattioli, A.; "Experiments and data analysis of electronic voting system" , Fourth IEEE International Conference on Risks and Security of Internet and Systems (CRiSIS), 2009, Page(s): 105 – 112.

[15]. Seo-Il Kang and Im-Yeong Lee, "A Study on the Electronic Voting System using blind Signature for Anonymity", Hybrid Information Technology, 2006. ICHIT'06. Vol 2. International Conference on Volume 2, Nov. 2006 Page(s): 660 – 663.

[16]. Athanassios Kosmopoulos ,"Aspects of regulatory and legal implementations on e-Voting ",s. wang et al.(Eds):ER workshop 2004. LNCS 3289, pp. 589-600, 2004.

[17]. J W Bryans, B Littlewood, P Y A Ryan, L Strigini, " E-voting: Dependability Requirements and Design for Dependability", Availability, Reliability and Security, 2006. ARES 2006. The First International Conference on 20-22 April 2006 Page(s):8 pp.

[18]. Kiayias, A.; Korman, M.; Walluck, D.; "An Internet Voting System Supporting User Privacy", Computer Security Applications Conference, 2006. ACSAC '06. 22nd Annual Dec. 2006 Page(s):165 – 174.

[19]. Anthony Watson, Vincent Cordonnier , "Information Technology Improves Most of the Democratic Voting Processes " Professor, Edith Cowan University - Perth, Australia , Professor, UniversitC des Sciences et Technologies de Lille – France , 1529-4188/01, 2001 IEEE ,page 388-393.

[20]. Jared Karro and Jie Wang "Towards a Practical, Secure, and Very Large Scale Online Election", Computer Security Applications Conference, 1999. (ACSAC '99) Proceedings. 15th Annual 6-10 Dec. 1999 Page(s):161 – 169.

[21]. Tadayoshi Kohno, Adam Stubblefield, Aviel D. Rubin, Dan S. Wallach, "Analysis of an Electronic Voting System", Security and Privacy, 2004. Proceedings. 2004 IEEE Symposium on 9-12 May
2004 Page(s):27 – 40.

[22]. Lorrie Faith Cranor, Ron K. Cytron, "Sensus: A Security-Conscious Electronic Polling System for the Internet", Public Policy Research AT&T Labs Research, 1060-3425197, 1997 IEEE, pp 561-570.

[23]. Alam, M.R.; Masum, M.; Rahman, M.; Rahman, A.; "Design and implementation of microprocessor based electronic voting system", IEEE 11th International Conference on Computer and Information Technology, 2008. ICCIT 2008, Page(s): 264 – 269.

[24]. Cottin, N.; Mignot, B.; Wack, M., "Authentication and enterprise secured data storage", Emerging Technologies and Factory Automation, 2001. Proceedings. 2001 8th IEEE International Conference on Volume 2, 15-18 Oct. 2001, pp 245 – 252.

[25]. Chai Wah Wu, "Multimedia "On the design of content-based multimedia authentication systems", 10.1109/TMM.2002.802018, IEEE Transactions on Volume 4, Issue 3, Sept. 2002 pp 385 – 393.

[26]. Won Jay Song; Byung Ha Ahn ,"Secure transmission of the prescription order communication system based on the internet and the public-key infrastructure using master smart cards in the 2-way type terminal ", System Sciences, 2002. HICSS. Proceedings of the 35th Annual Hawaii International Conference on 7-10 Jan 2002 IEEE CNF pp :2035 - 2042.