Necessary Requirements to Developed an E-Election System Protocol Based on Legal, Social and Security Point of View

Vinod. M. Patil
Head
Department of Computer Science,
Shri Shivaji College, Akola-444001,, MS, India

ABSTRACT

Computers and computer networks technology play a major role in the field of research and developments stages of information and communications technology (ICT) in the globe. This can motivate and encourage to introducing an electronic election system or proposing an E-election protocol to implementing an e-election system. Any e-election protocol or application may be accepted on basis of reliable, secure and efficient and satisfies core requirement and some basic properties. These requirements are mandatory for any electronic voting systems. A Secure system should need these requirements for execution and acceptance by voters and political parties otherwise, it will not be an adequate solution to electoral system.

1. INTRODUCTION

Although a wide variety of e-election systems / schemes and protocols exist today but the basic structure of an election system are almost have same standard. Therefore, the general requirements used for the traditional paper-based voting system are also be applicable to the electronic election system in addition to the legal, social and security point of view.

2. Categories of Requirements:

In the electronic election system, to the purpose of modularization, divide a complete requirements of the system [138] into the following categories:

2.1 Electronic election system requirements:

Regarding Hardware, software, firmware and relating to any e-election equipments.

2.2 Administrative Requirements:

Relating to the responsible election authority, administrator and poll-workers etc.

2.3 Assurance of the compliance:

Related to the stages of developments of the system, processing and evaluation of the system and to assurance of the compliance as per the requirements time to time.

2.4 Securities Requirements:

Security regarding data and computer network that can used during transmission of data. Other related to data updating, modification , insertion ,deletion. Security against virus, data hacking, threads etc.

2.5 Functional requirements:

Regarding the behavior of the e-voting system and usability related to user-interfaces.

3. Basic requirements:

The following are the basic need to apply for electronic voting system in secure & reliable manner.

3.1 Authentication and registration:

Only authenticate citizen can vote on the election day, for that purpose only eligible vote's can registered their name in front of election authority with their proof of identification about that he / she belongs to that particular constituency including age proof, address proof, Nationally, domicile & much more as per demand of election authority (Election commission).

The election authority should compile a list of eligible voter prior to the elections. Eligible votes generate public / private key for signing a ballots and register a vote by sending it. Voter's identification and public key are placed on a registered voter electoral roll. Issuing a National ID cards to all eligible voters that contain digital signature which combines the digital identity of the holder and the real identity.

3.2 Eligibility:

Only eligible citizen can vote only once. To cheek the eligibility of voter, the authentication process can verity the eligibility and conform that he / she up till now cannot vote. If he/ she already casted a vote then discard he / she ID card.

The voter will be interacting with a polling booth at his predetermined constituency and produce his identity ID to the polling booth. The polling agent transmits ID proof to the election authority for verification. If voter ID is eligible, then the election authority sends token to the voter.

3.3 Confidentiality:

The voter's ballots should be kept confidential for voter's privacy and to avoid as opportunity of vote buying and extortion. If allowed to the remote voter that is by using own computer system like Laptop, Pam top, mobile or any other device, then there is a chances of vote buying or selling and much more possibility. The contesting candidates have guarantee about the casting of vote is in proper manner. Since all election process of casting votes, takes place in front of candidates or on the behalf of representative of candidates.

3.4 Uniqueness:

Every voter can vote only ones. That is no votes should be able to vote more than ones time during the election process.

3.5 Integrity:
Votes should not be able to be modified, forget or deleted after casting. If so happen then there must be detection; and there must be a possibility to repair the manipulation during the execution of election process.

3.6 Secrecy:
A fundamental objective of democratic elections is secrecy of the vote. It requires that only the voter knows his voting decision and nobody else is able to gain information about it, apart from what is leaked by the tally.

The concept of secrecy usually refers to keeping sensitive information confidential. In an election, however, the voter's identity may not be a secret because it could be published which voters actually voted, and the vote is not secret either (because tallying would not be possible otherwise). Election secrecy is refers to the link between voter and vote. It is thus also referred to as unlinkability.

3.7 Voters Privacy:
The content of ballot after the eligible votes can voted shall not know to the third party. A personnel vote remains anonymous. It is the inability to link a voter to a vote. Voter privacy must be preserved during the election as well as after the election for a long time.

Privacy is a vital requirement in e-voting protocols, as nobody can know voter's cast vote. So it should be impossible to reveal and prove the relationship between voter and his vote. This is the principle requirement for both paper based voting and e-voting.

3.8 Voters anonymity:
Anonymity is requiring to perverse the voter's identity. In other words Anonymity ensures that a subject may use a resource or service without disclosing its user identity.

3.9 Accuracy:
Election system should record the votes correctly. A voter's vote can not be altered, duplicated, or remove after being recorded. Invalid vote are not tabulated in final tally and all casted votes should be counted. Any attack on the votes should be detected and uniqueness should be satisfied for accuracy.

3.10 Simplicity:
Voting mechanism should be user-friendly, easy and understood by any voter quickly without any special training. Also on the other side voter can finish voting process quickly, with minimum time, if require equipment on special skills. No need the help of third party or technical support at the time of casting a vote.

3.11 Mobility:
Voters are not restricted for physical location from any location they can cast their votes. On election day if voters are not presents to their constituency, even then it can cast their vote from any physical location to their constituency.

3.12 Soundness:
The dishonest voter cannot disrupt the voting process partially or completely during the election period.

3.13 Robustness:
Election system should work robustly without loss of any single vote / votes; even at extreme condition, it can face a numerous future including failures of voting machine and total loss of Internet communication. The voting process can be performed successfully regardless of partial future of the system. Any number of parties or even authorities cannot disrupt or influence the election process and final tally.

To have confidence in the election process and result, robustness should assure. However, there are numerous of ways for corruption such as registration authorities may cheat by allowing ineligible citizen to register; ineligible voter may register under the name of someone else. In addition, ballot boxes, ballots and vote counting machine may be compromise.

In order to satisfy robustness, system should be protected against any kind of active and passive attacks. Empty Ballot, Null Ballot, Abstaining voter requirements should also be fulfill for robustness.

3.14 Efficiency:
The eligible voter can cast a vote within time i.e. all components during voting period will be working properly and that are response to the voter so that votes are not require to wait to the other voter to complete their process. In all phases, registration, authentication and authorization, voting and tallying the processes should be done efficiently in a very short time. It is derived, to get the result as such as possible after the voting phase ends.

3.15 Scalability:
The geographically scattered area of constituency of election or number of contesting candidate in particular constituency or number of constituency (total number member of parliament / assembly) and number of votes in the election process will not drastically affect performance of voting system.

3.16 Fairness:
No partial tally is disclosed before the end of the voting period to ensure that all candidates are given a fair decision. Even the counter authority should not be able to have any idea about the intermediate result.

3.17 Uncoercibility:
No one should be able to determine how any individual voted and voters should not able to prove how they voted. Any coercer, even authorities should not be able to extract the value of vote or even should not be able to coerce a voter to cast his vote in any way in favour of it. Voter must be able to vote freely.

3.18 Directness:
Voters should cast their vote directly without any help of intermediates or any representatives during election process.

3.19 Freedom:
Voter is free to vote for any party or candidates as per his / her choice without under any influences or political pressure on it.

3.20 Verifiability and Auditerbility:

To verity, that all votes have been recorded correctly and accounted in the final tally and there should be reliable and demonstrably authentic election records. Verification involves being able to verity the transaction in full confidence at any time or at the time of voting. A receipt of our transaction is required that provides full confidence, at the time of voting, that our choice were accurately recorded. We must provide a record that your vote was recorded as per intention.

Voters can be sure that their votes are tabulated correctly, but voters are not required to verify their votes, in order to ensure election integrity. It is the provability that the final tally is correct.

Verifiability can divide into two types:

a) Individual verifiability.

b) Universal Verifiability

Individual Verifiability: The individual voter should be able to check that his vote is counted correctly.

Universal Verifiability: The final result published by election authority is correct weather match the all voter who cast the votes and who not cast the vote during the election period.

3.20 Convenience:

The voter should cast their vote easily, quickly, simply without the help of any skill or third person, or even any extra equipment and in a one session. User interfaces should be clear and easy to use and no particular computer knowledge should be necessary to cast a vote. System should not involve any type of misguide, misunderstood or ambiguous information about the computer operations.

3.21 Testability:

The election system working should be testable at any intermediate steps so that election officials have confidence that system work satisfactorily during the election process, without the prediction of any intermediate results.

3.22 Equality of Candidates:

The E-election system should give equal opportunity to the every candidate.

3.23 Open Source:

All source code should be allowed to be publicly open and verifiable. The security and reliability of the system must not rely on secrecy of its source code which cannot be guaranteed, only keys must be considered secret.

3.24 Reliability:

E-election system must ensure the reliability and security of the system without loss of any votes, even in the face of numerous failures including failures of voting machines and total loss communication or malfunctioning voting machines. These include the possibility of fraud or unauthorized intervention or possible breakdowns or denial of service attacks.

3.25 Manifold of Links:

The E-election system should be backed up and use a manifold of important components against the failure and attacks.

3.26 Transparency:

The whole voting process must be transparent. For that purpose Bulletin Board (BB) may be used to publicize the overall election process, to what going inside system in order to achieve the confidence of citizen over the system. The security and reliability of the system must not rely on the Secrecy of the network, which cannot be guaranteed.

3.27 Physical Recounting and Auditing:

The election data and result should be saved in both electronic and physical environments after the election ends without compromising the election integrity or votes privacy.

3.28 Technical Adequacy:

Technical infrastructure of hardware and software should be adequate. In such case, use of cryptographic technique should be effective not only for today but also for the near future.

3.29 Abstaining Votes:

The system should count all votes including the abstaining voters, in order to verify the final result at the time of tally. This can help to identify the eligible voters who have not voted.

3.30 Null Ballot:

The system should represent null voting, which means voter started voting process but not completed. Voter may decide, not to vote at any time before casting the ballot. Null voter should also be counted as null ballots and they cannot filled, catered, deleted, and invalidated or copied.

3.31 Empty Ballot:

The system should represent blank votes, which means none of the candidates is selected. Voter may change the choices from 'Vote' to 'blank Vote' and Vice versa before casting the ballot. Blank votes should also be counted as empty ballots and they cannot filled, deleted, copied, invalidated or altered.

3.32 Announcement of results:

After verifying the result electronically and physically, the result must be declared publicly and ready for recounting and auditing. The e-election system shall not allow the disclosure of the number of voter cast for any voting option unit after the closure of electronic ballot box. This information shall not be disclosed to the public unit after the end of the voting period.

3.33 Unlinkability:

During the executing of electronic election process, steps of operations should not link. This is known as unlinkability and it is the primary requirement to satisfy privacy in e-voting protocols.

The link between voter and vote can possibly be established between voter and plaintext or encrypted vote, and it may be provable or not. Thus, we distinguish the following levels of secrecy:

(a) Unlinkability of voter and vote / ballot. It is not possible to establish a link either between voter and vote or between voter and ballot.

(b) Unlinkability of voter and vote. It is not possible to establish a link between voter and vote.

(c) Improvable linkability of voter and ballot. It is possible to establish a link between voter and ballot, but the link is not provable to third parties.

(d) Improvable linkability of voter and vote. It is possible to establish a link between voter and vote, but the link is not provable to third parties.

3.34 Receipt-freeness:

A voter does not gain any information (a receipt) which can be used to prove to a coercer that he / she voted to particular candidates.

4. ADDITIONAL REQUIREMENTS

The following requirement is not mandatory, but they are desirable at the time of processing e-election system politically.

4.1 Feasibility Study:
The total cost of the e-election system should be less than the traditional cost of paper-based system.

4.2 Design Independence:
The design of e-election system should be independent from the operating system, development environment and technology to be adopted.

4.3 Authenticated Ballot Styles:
The empty ballot authenticated by election authority may be used in place of abstain vote during the election process or ballots may be signed by authority to prevent invalid votes.

4.4 Scalability of e-election system:
An e-election system should be capable to supports small, mid and large-scale elections at any time without any extra effort or skill. The election system must be sufficiently robust to withstand a variety of fault behaviors occurs during the system execution. The processing of election system should be satisfied such that voters, candidates and it political party can accept the result of election unanimously.

4.5 Recorrecting the choice:
The processing of the e-election system should be such that, the voters should be able to alter their choice at any point, before finalizing a casting of vote, without their previous choice being recorded. However, the e-election system shall prevent the changing of a vote after finalizing the casting of vote. No recording of vote or votes should be recorded after voting procedure has been completed. If the voter wish, then the voter should be able to break the intermediate procedure without vote being recorded. Each vote and absentee of vote must be recorded correctly. Every vote in electronic ballot box should be counted and counted only once. There shall be secure and reliable method to aggregate.

4.6 Flexibility:
Every device used during the e-election system equip with required format and must be compactable with a variety of standard platforms and technologies and allow for a variety of ballot question formats. And also may be accessible to voter with disabilities.

5. ISSUE RELATED TO LEGAL POINT OF VIEW:
During the E-election process, the following important issue must be consider by the Election Commission to fulfill all their tasks within the limits of the law: [6]

- Except the committee members nobody is to know any of the private keys of the committee until the opening of the ballot box.
- No committee member knows the private keys of any other committee members used for encrypting the votes until the opening of the ballot box.
- Any pre-defined quorum of the election committee can open the ballots.
- A group of members short of the quorum even by one member only shall have a non-realistic chance in deciphering what a valid quorum may decipher.
- No committee member is able to sabotage the process by supplying fake keys.[R8]

6. CONCLUSION
While converting the traditional voting system into the electronic voting system the requirements essential for the traditional voting system can also application to the e-election system. Also if the storage and communication media are electronic than problem arises regarding security and modification of the data that force towards the problem of faith of voters, governments, election commission and political parties.

In order to develop an electronic voting system protocol, need to satisfy near about all the requirements discuss above to achieve the faith of the voters regarding the formation of the democratic governments.

7. REFERENCES
[1] Yih-Chun Hu, Adrian Perrig, and David B. Johnson, "Wormhole Attacks in Wireless Networks", ieee journal on selected areas in communications, vol. 24, no. 2, February 2006, pp 370-380.

[2] 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.

[3] Yasinsac, A.; Bishop, M.; "Of Paper Trails and Voter Receipts" ,Hawaii International Conference on System Sciences, Proceedings of the 41st Annual 7-10 Jan. 2008 Page(s):487 – 487.

[4] Prosser, A.; Krimmer, R.; Kofler, R.; Unger, M.K.; "The Role of the Election Commission in Electronic Voting", System Sciences, 2005. HICSS '05,Proceedings of the 38th Annual Hawaii International Conference on 03-06 Jan. 2005 Page(s):1-6.

[5] 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.

[6] 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.

[7] Anane, R.; Freeland, R.; Theodoropoulos, G.;" e-Voting Requirements and Implementation", E-Commerce Technology and the 4th IEEE International Conference on Enterprise Computing, E-Commerce, and E-Services, 2007, Page(s): 382 – 392.

[8] 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.

[9] Alexandros Xenakis and Prof. Ann Macintosh, "Procedural Security in Electronic Voting", Proceedings of the 37th Hawaii International Conference on System Sciences – 2004, 0-7695-2056-1/04, 5-8 January, 2004 IEEE pp 1-8.

[10] Costas lambrinoudakis, dimitris gritzalis, sokratis katsikas, "Building a Reliable e-Voting System: Functional Requirements and Legal Constraints", Proceedings of the 13th International Workshop on Database and Expert Systems Applications (DEXA'02) ,1529-4188/02, 2002 IEEE,pp 435.

[11] Cansell, D.; Gibson, J.P.; Mery, D.; "Formal verification of tamper-evident storage for e-voting", Software Engineering and Formal Methods, 2007. SEFM 2007. Fifth IEEE International Conference on 10-14 Sept. 2007 Page(s):329 – 338.

[12] Villafiorita, A.; Weldemariam, K.; Tiella, R.; "Development, Formal Verification, and Evaluation of an E-Voting System With VVPAT"; Information Forensics and Security, IEEE Transactions on Volume: 4 , Issue: 4 , Part: 1, 2009 Page(s): 651 – 661.

[13] Thomas E. Carroll , Daniel Grosu "A Secure and Efficient Voter-Controlled Anonymous Election Scheme", Information Technology: Coding and Computing, 2005. ITCC 2005. International Conference on Volume 1, 4-6 April 2005 Page(s):721 - 726 Vol. 1.

[14] Robert Kofler, Robert Krimmer, Alexander Prosser, "Electronic Voting: Algorithmic and Implementation Issues", Proceedings of the 36th Hawaii International Conference on System Sciences (HICSS'03) , 2003. 6-9 Jan 2003 Page(s):7 pp.

[15] Melanie Volkamer, Margaret McGaley , "Requirements and Evaluation Procedures for e Voting", Availability, Reliability and Security, 2007. ARES 2007. The Second International Conference on 10-13 April 2007 Page(s):895 – 902.

[16] 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.

[17] Brian whitworth and robert j. Mcqueen, "Voting before discussing: Computer voting as social communication", Proceedings of the 32nd Hawaii International Conference on System Sciences – 1999 IEEE ,pp 1-12.