Research Journal of Information Technology 6(1): 8-13, 2015
ISSN: 2041-3106; e-ISSN: 2041-3114

Submitted: January 01, 2015 Accepted: January 15, 2015 Published: February 01, 2015

System Engineering for Democratic Process Leading to Next Generation EMS

[1]Innocent Kabandana, [2]A.N. Nanda Kumar and [3]S.J. Ravi
[1]Department of Computer Science and Engineering, Jain University Global Campus, Kanakapura,
[2]R.L. Jalappa Institute of Technology, Doddaballapur, Karnataka,
[3]Venus Technologies, Bangalore, India

Abstract: The main objective of this study is to know how a System engineering can play an important role in promoting the process of Election Management System. A voting system provides rules and regulations to ensure valid selection of leader by people. This survey describes System Engineering for Democratic process leading to the next generation Election Management System [EMS] using a Central servers for different options of election System. This Technology Survey Paper covers EVM Types, Hardware and Software EVMs, Voting problems, Advantages, Disadvantages, Attacks and our proposed EMS architecture with hi-tech feature set.

Keywords: Attacks in EVMs, EVM and EMS, hybrid EVMs, microcontroller based EVM, smart card based EVM, touch screen based EVM

INTRODUCTION

An electronic voting system (on-line voting, internet voting) is an election system which uses electronic ballot that would allow voters to transmit their secure and secret voted ballot to election officials. With the prosperity of internet over the years, inventers start to make the use of electronic voting in order to make the voting process more convenient and raise the participation of the civic society.

The implementation of electronic voting in local and national elections has the following benefits:

Mobility: E-voting would allow voters to cast their vote from any convenient location instead of going to the specific polling location.

Increased participation: Electronic voting increases the number of eligible citizens to cast their votes. An Internet based voting system might appeal to younger voters who are currently less likely to exercise their vote.

Increased efficiency and accuracy: E-voting assures to minimize some of the human errors inherent to the manual systems especially in the counting of votes. A computerised system is more efficient and allows for a quicker delivery of results.

Transparency: E-voting is expected to be more open to public scrutiny. They should be no cheating of the votes and any complain, an option of verification is provided.

E-voting requirements: The manual paper based voting process management in democratic elections follows the specific tasks:

The registration is concerned with the list of eligible voters.
The validation is to check the eligible voters and ensuring that only legitimate users can cast their votes.
The collection involves in gathering the ballots.
The tallying consists counting the votes.

The voting process is however performed within specific limitations that an electronically based voting system should conform to. In particular, the system must meet the following minimum requirements for a secure electronic voting scheme:

- Only eligible voters are able to vote.
- No voter is permitted to vote more than once.
- No one should be able to determine the value of anyone else's vote.
- No one can duplicate a vote.
- No one can alter another person's vote without being detected.
- Voters can verify that their vote has been counted.

Types of voting systems: Voting is a method by which groups of people make decisions. These decisions could be political, social or public. Voting can also be used to choose between difficult plans of actions or to decide who is best eligible to be awarded a prize. Voting can thus be defined as a process that allows a group of

Corresponding Author: Innocent Kabandana, Department of Computer Science and Engineering, Jain University Global Campus, Kanakapura, Karnataka, India

individuals to choose their leaders or representatives. Different types of voting systems may be identified by Ofori-Dwumfuo and Paatey (2011) and Prasath *et al*. (2014):

- Paper-based voting systems
- Direct-Recording Electronic (DRE) voting systems
- Public Network DRE voting systems (PNDRE)
- Precinct Count Voting Systems (PCVS)
- Central count voting systems

Paper-based Voting Systems (PVS): Sometimes called a "document ballot voting system". Paper based voting system is a system where votes are cast and counted by hand, using paper ballots. Some PVSs may allow voters to make selections by means of electronic input devices. With the initiation of electronic tabulation where paper cards or sheets could be marked by hand, but counted electronically.

DRE voting systems: The voting machine will be used to make the record votes by means of a ballot display provided with electronic optical or mechanical components which could be activated by the voter using the card. Also, data processing is achieved by the use of computer programs.

PNDRE systems: Making use of electronic ballots and transmit vote data from the polling stations to the central server using a public network. The votes may be transmitted as individual ballots as they are cast, or periodically as batches of ballots, or as one single batch, at the end of voting

PCVS systems: Putting the ballots in a tabular form at a polling station. They provide mechanisms that store vote count electronically and transmit the results to a central location over public telecommunication networks.

CCVS: The system involves tabulation of ballots from multiple precincts at a central location. Voted ballots are safely stored temporarily at the polling station, then transmitted to a central counting location. In some cases CCVSs may produce printed reports on the vote count.

Classification of EVMs: Types of Voting Systems have been designed and widely used in different countries are listed below:

Hardware based EVMs (https://jhalderm.com/pub/papers/evm-ccs10.pdf):

- Microcontroller Based EVM
- Smart card based EVM
- Touch screen based EVM.

Microcontroller based EVM: Microcontroller Based EVM is a simplest EVM and the schematic representation of which is presented in Fig. 1. The components of the system are (Prasath *et al*., 2014; Diponkar and Sobuj, 2013):

- Voting unit
- Control unit
- Confirmation unit
- Display unit (LCD)
- Power supply unit

An EVM has been designed by a microcontroller for which the code is written in assembly language. Microcontroller based EVM will play an important role of controlling and executing different activities of electronic election process.

Smart card based EVM: Smart card will be issued to voters and poll officers. Voters will swipe smart card for Verification. Once verified, voters can cast their votes and poll officers will use the smart card for results tabulation. Figure 2 displays an example for Smart Card based EVM.

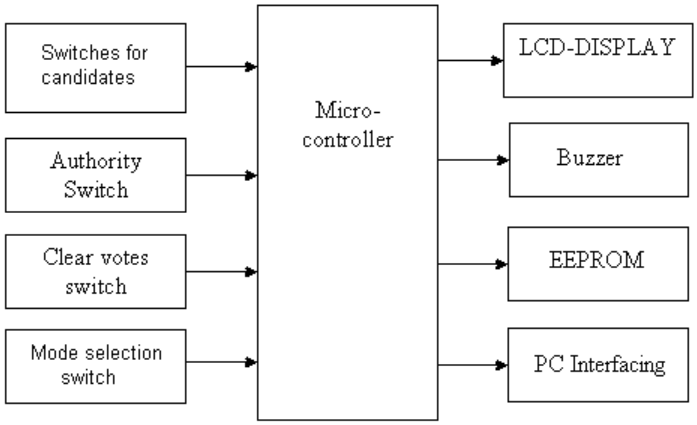

Fig. 1: Microcontroller based EVM (Prasath and Mekala, 2014)

Fig. 2: Smart card based EVM (www.verifiedvoting.org)

Touch screen base EVM: The Graphical User Interface (GUI) and touch screen provide easy access to the voters and poll officers. The candidate list will be displayed and the voter can touch the candidate name to access. By touching the candidates name on the screen, voters can cast their votes. Figure 3 exhibits a type/example of Touch Screen based EVM.

Software based EVMs (https://jhalderm.com/pub/papers/evm-ccs10.pdf): The software based EVM make use of some standard hardware products to implement voting system software and are illustrated in Fig. 4 and 5.

The different types of Software based EVMs are as follows:

- Mobile based voting system
- PC based voting system
- Internet based voting system

Mobile based EVM: Mobile voting software runs with a server and an app which uses password as authentication. Mobile voting can be of different types (Abdalla and Samani, 2013):

- Interactive Voice Response (IVR)
- Unstructured Supplementary Service Data (USSD)
- Short Message Service (SMS) and app

PC-based EVM:

- Firstly, software runs on the PC with voter data base and then, poll worker verifies the voter ID.
- Further, the voter can vote using the software in PC.

Internet Based EVM: The entire Internet transaction on the voter side can be resumed in four steps:

- Voter identification through his voting card number

Fig. 3: The diebold AccuVote-TS, a touch screen based EVM (Ariel *et al*., 2006)

Fig. 4: Mobile based EVM

Fig. 5: Personal computer (PC) based EVM

- Make a Vote
- Confirmation of the voter's choices and voter authentication
- Confirmation of the vote (date and time of the vote).

Characteristics, advantages and disadvantages of EVMs

Characteristics of EVMs: Valid elections via EVMs must meet each of the following characteristics (Abdalla and Samani, 2013):

Privacy: No other person should be able to tell how a voter voted. Even bulk statistics such as correlating vote with language should not be exposed. The only acceptable information disclosure is the final vote total or each precinct (Ghassan and Rani, 2007).

Lack of evidence: The voters should not be able show the proofs to anyone i.e., the way they voted. Together with the privacy condition, this prevents vote-selling and coercion. If there is no way to assure a third party of which way a vote has been cast, bribes and threats are ineffective.

Fraud-resistance: Each qualified voter should be able to vote exactly once and no other persons should be able to revote the same. The system must verify the identity of each potential voter and determine their status, but must not allow this information to become associated with their votes.

Low cost: The cost effectiveness for selecting voting systems is a major concern for developing counties. A lower-cost and high-secure system is often times more attractive than a higher-cost ones. If a system can't be implemented cheaply, it isn't useful.

Ease-of-use: Elections must serve the entire public. This includes people with various levels of technological familiarity, various languages and various physical capabilities. Any systemic bias in the error rates between these groups could unfairly alter the election results. Additionally, the poll workers running each voting stations should have minimal training and technical skills. Setting up and administrating the system must be simple.

Scalable: Large elections must serve millions of people. The system must scale to handle these elections as well as smaller precinct-specific ones.

Speed: As a result of exposure to computer-counted ballots, the American public now demands that at least preliminary results should be available within several hours of polls closing and any voting system that requiring lengthy counting time will not be acceptable.

Advantages of EVMs: The advocate of electronic voting claims that the convenience, mobility, tally speed, less cost and flexibility are the main advantages (Prasath *et al*., 2014). Those advantages are described as:

Convenience: With the well-designed software and system, the voters should simply use their voting equipment with the minimal time and skill to finish the voting process.

Tally speed: Once the voting time is over, the computer should immediately calculate the result of the election and it has to be much faster than the traditional ballot counting method operated manually.

Less cost: Compared to paper ballot voting, electronic voting saves money from reducing the personnel expense, expense for location management, human resource and administration fee. In the beginning, the investment expense of building up the electronic voting system would be very high. But after the system is build up, the total expenses can be reduced to be much lower than paper ballot system.

Flexibility: Electronic voting system must be designed to support a variety of ballot question formats and it should be used to collect public opinions on elections.

Voter participation: The participation of voters must increase due to the convenience, availability and mobility of the system and it should motivate people who are not interested in voting or unable to vote originally.

General disadvantages of EVMs are (Ghassan and Rani, 2007; Saltman, 1988):

- Lack of transparency
- Confidence, trust on voting system
- Audit of results
- Secrecy and security of the ballot
- Setup procedures for EVMs
- Tendered ballots
- Lack of education for voters on operating EVM
- Specialized IT skills
- Integrity and accuracy of source code
- Storage of equipment
- Environmental and energy considerations
- Consequences of Fraud
- Management Complexity
- Cost

EVM attacks (Wolchok, 2010; Slavik *et al*., 2006): Various components of the system could be subjected by an attack from a number of parties: malicious voters,

members of the polling station staff and outside hackers.
A major types of attacks are explained below:

Attack on the hard-drives capabilities: Machine's hard drives could be subjected to tampering by someone who has access to the physical machines prior or after the elections. In case of Diebold, the data on the hard-drive was encrypted by a single well-known company-wide key.

Attack on the network capabilities of the system: Variety of avenues here, one being producing a malicious voting station that would report the result to tabulation after the voting day.

Attacks on smart card, smart card voting station interface protocol: If properly designed, smart cards are powerful security instruments. In some cases (Diebold is the prime example), smart cards could be an entry point of an attack, because of lack of cryptography, there won't be a secure authentication of the smartcard to the voting station employed. i.e., the mechanism for the prevention of user to use his/her own smartcards to vote multiple times is unavailable.

Insert backdoors into code attacks: This could be done by someone from the poll crew or even someone who works for the company that produces DREs. Although, certification process allows code reviews, it's still conceivably possible to hide a piece of malicious code that is difficult to spot.

Insert backdoors: Insertion of backdoors into Operating Systems (OS)/hardware, compiler/linker/ loader/and other developed software are not even analyzed by ITAs, this constitutes a conceivable vector of attack.

Our proposed EMS: Some of the problems in manual voting are: many people on queue, many polling stations and more time to vote, use of papers and indelible ink, easy to make errors and cheat, more time to count votes and publish the results, requirement of human resource. In E-Voting system, the problems are: hackers, security, network, electricity and lack of skills for the voters on the usage of EVMs, infrastructures, auditing the system and etc. Our proposed hybrid hi-tech EMS can overcome the above mentioned problems with an advantages of mobility, tally speed, low cost, flexibility, voter participation, immediate election results, maximum tamperproof features and convenience. The detailed explanation and schematic representation of our proposed EMS is as below.

Components of our EMS:
Hardware: Implementing a hardware based EVM using FPGA having three voting options:

- Manual voting
- Smart card voting
- Mobile voting

Software: Implementation of software based voting machine provides wide accessibility to the users via internet.

Centralization: Implementation of server based voting machine will help to connect all the hardware and software voting machine to central server via Wide Area Network (WAN). The results of voting will be tabulated, stored and displayed in central server.

An effective features of our EMS: The major attracting factor of our proposed EMS is the utilization of all types of voting systems like manual, smart card, mobile, internet voting along with centralized data base management in a single turn as the schematic representation of which is presented in Fig. 6. No other voting systems have integrated all types of voting in the

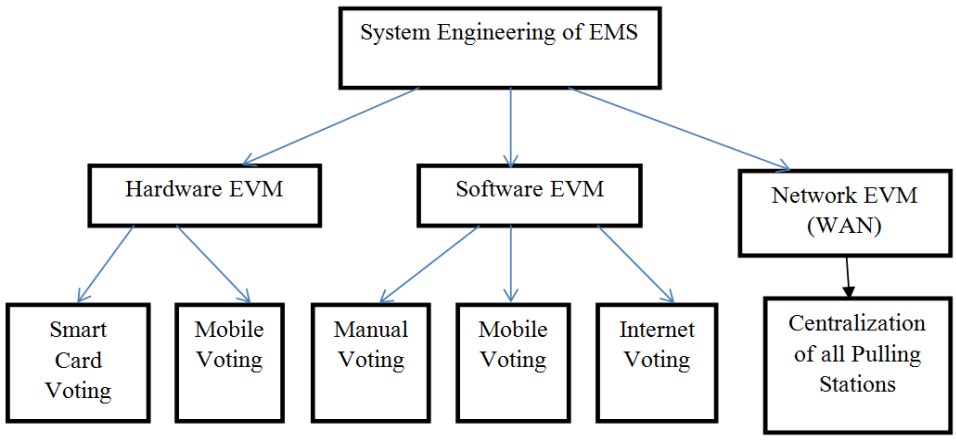

Fig. 6: System engineering of proposed EMS

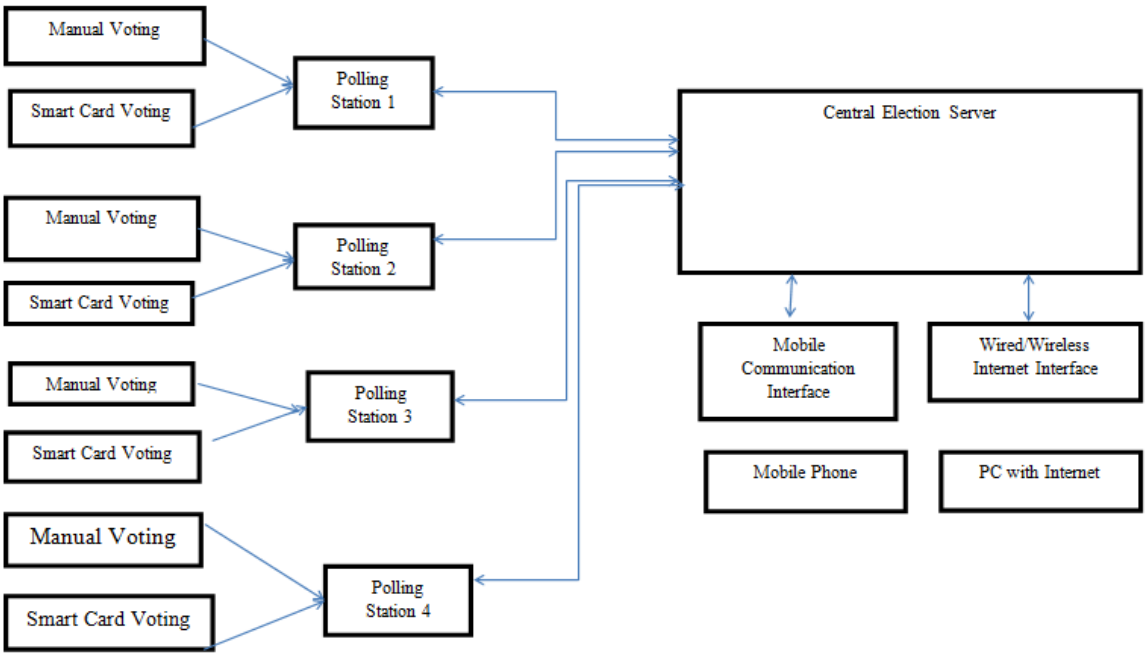

Fig. 7: Proposed system engineering block diagram EMS

same system and the system will be designed, implemented and tested for the integration.

Figure 7 indicate the proposed system engineering block diagram of EMS, which will be having all those different voting options and explains how the casted votes will be stored and tabulated to the central voting server through WAN and also the automatic display of the results at the end of the election.

CONCLUSION

After in depth survey of the technology and system engineering study, we found a strong need for Election Management System with completeness and obedience voting protocol. Voter's final ballot must be secret and he/she cannot prove the contents of his/her final ballot to anyone. In the other way, voter needs ability to verify that their votes are cast and counted as intended.

The citizen eligible for voting is provided with various technology options to use one of them, like manual, mobile, smart card and internet voting which will be running in parallel and integrated to the central server through WAN. Proper implementation of e-voting and its solutions can increase the security of the ballot, speed up the processing of results and make voting easier. Election results can be declared immediately after polling is over. Our research is a serious attempt towards building a reliable hybrid hi-tech EMS.

REFERENCES

Abdalla, A.A. and T. Samani, 2013. The technical feasibility and security of e-voting. In. Arab J. Inform. Technol., 10(4): 397.

Ariel, J.F., J. Alex Halderman and W.F. Edward, 2006. Security analysis of the diebold Accuvote-TS voting machine. Proceedings of the USENIX Workshop on Accurate Electronic Voting Technology (EVT'07), pp: 2.

Diponkar, P. and K.R. Sobuj, 2013. A preview on microcontroller based electronic voting machine. Int. J. Inform. Electr. Eng., 3(2).

Ghassan, Z.Q. and T. Rani, 2007. Electronic voting systems: Requirements, design and implementation. Comp. Stand. Inter., 29(3): 376-386.

Ofori-Dwumfuo, G.O. and E. Paatey, 2011. The design of an electronic voting system. Res. J. Inform. Technol., 3(2): 91-98.

Prasath, S.V. and R. Mekala M.E., 2014. A literature survey on micro-controller based smart electronic voting machine system. Int. J. Adv. Res. Electr. Commun. Eng., 3(12): 1756-1761.

Saltman, R.G., 1988. Accuracy, Integrity and Security in Computerized Vote Tallying. Institute for Computer Sciences and Technology, National Bureau of Standard, Gaithersberg, MD.

Slavik, K., A.K. Agarwala, D.T. Shahani and P.V. Indiresan, 2006. Security flaws of existing electronic voting systems. Report of the Expert Committee for Evaluation of the Upgraded Electronic Voting Machine (EVM).

Wolchok, S., E. Wustrow, J.A. Halderman, H.K. Prasad, A. Kankipati, S.K. Sakhamuri, V. Yagati and R. Gonggrijp, 2010. Security analysis of India's electronic voting machines. Proceedings of the 17th ACM Conference on Computer and Communications Security (CCS '10), pp: 1-14.