ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 8, August 2015

System Engineering Based on Micro-Controller for Election Management System [EMS]

Innocent Kabandana[1], A.N. Nanda Kumar[2]

Department of Computer Science and Engineering, Jain University Global Campus, Kanakapura, Karnataka, India[1]

R. L. Jalappa Institute of Technology, Doddaballapur, Karnataka, India[2]

Abstract: Election is one of the indicators which is used by different countries to promote their democracy for allowing the eligible citizens to elect their efficient leaders to lead their political parties, institutions, and even their countries. In present era, the technology is growing amazingly and it is playing a significant role in Election System to minimize elevated expenses of manual and paper-based systems like, money spent on paper based voting, indelible ink, man power expenditure. The technologies have also been improved to reduce the possible errors which can happen in the process of election time, in voting and counting the votes as well as in publishing the votes. This paper describes the key components on security issues in the hardware and software of Electron Voting Machine (EVM), and significance of Rivest Shamir Adleman (RSA) algorithm to assure the security of the election systems. The main objective of this paper is to pronounce the primary role of E-Voting and its security in securing the voters privacy, integrity, reliability, simplicity, verifiability, coercion and accountability.

Keywords: EVM, Micro-controller, RSA algorithm, and EMS.

I. INTRODUCTION

Election:

Elections allow the public to choose their representatives and express their preferences for how they will be governed. Naturally, the integrity of the election process is fundamental to the integrity of democracy itself. The election system must be sufficiently robust to withstand a variety of fraudulent behaviours and must be sufficiently transparent and comprehensible so that voters and candidates can accept the results of an election.

In a democratic structure, freedom and democracy are often used interchangeably, but the two are not the same. Democracy is government by the people in which the supreme power is vested in the people and exercised directly by them or by their elected agents under a free electoral system.

In the phrase of Abraham Lincoln, “democracy is a government of the people, by the people, and for the people". Freedom is the right and capacity of people to determine their own actions, in a community which is able to provide for the full development of human potentiality. All democracies are the systems in which eligible citizens freely make political decisions by majority rule [6].

In a democratic society, majority rule must be united with guarantees of every human rights that, in turn, serve to protect the rights of minorities, whether ethnic, religious, or political, or simply the losers in the debate over a piece of controversial legislation.

The rights of minorities do not depend upon the goodwill of the majority and cannot be eliminated by majority vote. The rights of minorities are protected because democratic laws and institutions protect the rights of all citizens [4].

II. MANUAL/PAPER BASED VOTING VS E-VOTING SYSTEM

Manual/Paper based voting system: It is a way where the election commission will provide different sites and ID’s to eligible citizens which are to be used during the voting time with the physical presence of the voter. It also involves the registration of candidates who are participating in election with the required documents before the contest to ensure their candidature. On the voting day, the eligibility of the voters will be checked by polling officer with the help of issued ID. If the voter is eligible to vote, a ballot paper will be given to the voter to select a candidate on his/her choice using a paper. Then the voter is allowed to drop the ballot paper into ballot box available in polling station. Finally, the counting and publishing of the votes will be done manually.

During this tedious process, there is a possibility of some errors and problems which can be caused knowingly or unknowingly. Some of the problems are: managing many people on queue, increased number of polling stations and more time to vote, use of papers and indelible ink, probable ways to cheat, counting and results publishing time, as well as requirement of human resource.

E-Voting System: This is a technological system which will be used in election process and will facilitate the election commission to minimize various problems caused in manual election system. And this is a rapid system, the implementation of which is to full fill the user requirements. The election commission will provide the period of registration for the eligible citizens as well as the candidates and the registration will be done from any location using mobile or computers connected to the internet. Also, to reach the common man who is not

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 8, August 2015

equipped with the facilities, the government will provide a particular locations to register their voting.

A unique ID's and password will be generated to an individual voter which are to be used during the voting period. In the voting period the eligible voter will cast their votes from anywhere via internet and the votes will be gathered to the central server system. Further, the counting the votes will be done automatically within a short period of time and the result will be published with no errors.

In E-Voting system, the possible problems are: hackers, security, network, electricity, and lack of skills for the voters on the usage of EVMs, infrastructures, auditing the system and etc. Based on advantages and disadvantages between manual system and E-voting system, we prefer to use E-voting System as the one with more advantages and less disadvantages.

Our objective in this paper is to propose the E-voting system with the minimum components and to satisfy the maximum customer needs during election process with lesser disadvantages.

Minimum requirements of E-voting system:

- Accessibility: System should be accessible from anywhere so that the voter can vote from his/her own location (i.e. home, office, school, etc.).
- Accuracy: All valid votes must be counted and assigned to their concerned candidates.
- Anonymity: The secrecy on votes and voters must be maintained to avoid any harassment or any incident on the voters from candidates.
- Authenticity: Only eligible citizens will be allowed to cast their votes according to their choices and nobody else can cast votes on their behalf.
- Availability: The system must have the high-availability during an election campaign.
- Democracy/uniqueness: The voter is allowed to vote only once i.e. no duplicate vote is allowed.
- Integrity: Once a voter cast his/her vote no alternation to this vote is permuted/allowed.
- Privacy: The system should ensure that none of the stakeholders i.e. organizers, administrators, voters etc. involved in the voting process can link any ballot to the voter who cast it, and that no voter can prove that he or she voted in a particular way.
- Reliability: The election system should make sure to work strongly to fulfil the voter and candidature requirements in terms of accessibility, security, secrecy, authenticity and accountability.
- Simplicity: The system should be user friendly i.e. should be equipped with easy operating system so that even a common man/uneducated people can access for voting.
- Verifiability: The voter should be assured that his/her vote has been counted by having an option of verification [2].

EVMs: EVMs are being used in Indian General and State Elections to implement electronic voting as a part of elections since from1999 to till date. The EVMs reduce the time in casting the vote and declaring the results compared to the paper ballot system [7].

Categories of Voting Systems have been designed & widely used in different countries like hardware based EVMs, smart card based EVMs [11] and touch screen based EVMs.

III. MICRO-CONTROLLER

The most benchmarks for choosing a microcontroller is that it must meet the task at efficiently and cost effectively. In analysing the needs of a microcontroller-based project, it is seen whether an 8-bit, 16-bit, 32-bit or 64-bit microcontroller can be able to handle the computing requirements of the task most effectively.

Microcontroller based EVM is a simplest EVM used in E-voting System with different components and the schematic representation of which is presented in figure 1 [3] [10]. The components of the system are:

- Confirmation Unit: This is a part of the system which will allow the voter to send the vote after making his/her choice of a candidate.
- Display Unit: LCD is a device which is used to show the results of the measuring instrument.
- Power Supply Unit: Power supply is a very important part of electronic circuit, this circuit requires a fixed +5V of current supply to fix the voltage needed to regulate the system.
- A voltage regulator generates a fixed output voltage of a pre-set magnitude that remains constant regardless of changes to its input voltage or load condition.
- Control Unit: A control unit in general is a central part of the system that controls its operation, which will be able to manage any number of complex systems with enough organizing capacity.
- Voting Unit: The voting unit will be available on the screen of the voting machine where the voter will be activating this unit after turning on the system.

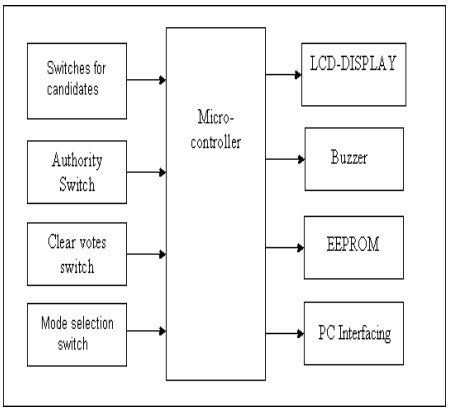

Figure 1: Schematic representation of Micro-controller based EVM [3].

DOI 10.17148/IJARCCE.2015.4803

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 8, August 2015

Based on the output signal from switches the micro controller selects the mode of operation. In voting mode micro controllers fetches the data from display mode to memory location block, to indicate one key is pressed. In counting mode, micro controllers get data from memory location and then send it to the Liquid Crystal Display (LCD). Then, entering ID card information into the system will allow the voter to cast vote if all the requirements of voter for voting are fulfilled.

Software design: Software should be compatible with micro-controller. This will determine how casted votes are handled by the system. The interfacing between various blocks is also integrated with this. Also there will be some encryption for the voter ID numbers which will be printed on the paper record [5].

Another type of EVM is software based voting systems where we use mobile based voting system, Pc based voting system and internet based voting system. The compatibility of hardware and software in EVMs tools will allow the voters to vote using some of those available options. To maintain the security of our implemented voting system some algorithms will be used. Those algorithms are:

RSA ALGORITHM: RSA is a cryptosystem for public-key encryption, and is widely used for securing sensitive data, particularly when being sent over an insecure network such as internet. It will be using public key cryptography also known as asymmetric cryptography where a message will be accessible to everyone and private key cryptography known as symmetric cryptography where the message will be secret means not accessible to everyone.

The challenges of today's technology are the hackers and eavesdrops where the solutions will be to encrypt the plaintext from the sender, and the receiver will be decrypting the message using his/her private key where the third party cannot be able to guess this key when trying to decrypt the encrypted message.

In RSA cryptography, both the public and the private key can encrypt a message, the opposite key from the one used to encrypt a message is used to decrypt it. RSA algorithm provides a method of assuring the confidentiality, integrity, authenticity and non-repeatability of electronic communication and data storage. This method will be used in election process where the eligible voter will be provided a secret key to be used to cast his/her vote.

Steps to be followed in RSA algorithm for public and private key:

1. Choose a pair of very large prime p and q;
2. Calculate n=p*q, where n is a modulus of public and private key;
3. Calculate φ (phi)= (p-1)*(q-1) where φ is mathematical constant and it must not share a factor with e (e is public exponent between 3 and n-1);
4. Compute the private exponent d from e, p and q;
5. Output (n, e) as a public and (n, d) as a private key.

The sender will encrypt a message using a primary key as follow:

The cipher text (c) =Encrypt (m) =m^e mod n

where m is a plain text (i.e. normal text)

The receiver will decrypt the encrypted message to get the plain text.

m=Decrypt (c) =c^d mod n

The relationship between the exponents' e and d ensures that encryption and decryption are inverse, and decryption operation gives the original message which is m.

If somebody does not know the private key (d, n) or its equivalent the prime factors p and q, it is very hard to know the value of m from c mean that n and e can be known publically without compromising security, which is the main requirements for a public-key cryptosystem. As the encryption and decryption operations are inverses and will work on the same set of inputs this means that the operation can be employed in reverse order to obtain a voter ID scheme by applying Diffie and Hellman's model [6].

The message can be digitally signed by applying the decryption operation to it i.e. by exponentiation it to the d^{th} power.

s=VOTERID (m) =m^d mod n.

The digital signature can be verified by applying the encryption operation to it then comparing the result with recovering the message.

m= VERIFY (s)= s^e mod n.

The plain text m is generally some function of the message for instance a formatted one way hash of the message [1].

In this paper an algorithm is proposed for RSA method for implementing a public-key cryptosystem using two public key and some mathematical relation. This two public keys are sent separately, this makes the attacker not to get much knowledge about the key and unable to decrypt the message. The proposed RSA is used for system that needs high security but with less speed.

HOMOMORPHIC ECRYPTION ALGORITHM (HEA): HEA is used to encrypt all the votes and perform the calculation of the votes without revealing any information about them. Current research focuses on designing and building "electronic voting protocols" such

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 8, August 2015

as zero knowledge authentication protocol, based on Diffie-Hellman key exchange algorithm, to ensure a mutual authentication between the election authority server and the voters [8].

General disadvantages of EVMs are:

- 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
- Confidence, trust on voting system
- Audit of results
- Secrecy and security of the ballot
- Setup procedures for EVMs
- Tendered ballots
- Management complexity
- Cost
- Lack of transparency [9].

IV. OUR PROPOSED EMS

Our proposed EMS will solve the above mentioned problems with the different advantages in terms of speed, cost, tally flexibility, mobility, voter participation, automatic election results, maximum tamperproof features and convenience.

Our EMS will have the following Components:

Hardware: Implementing a hardware based EVM using microcontroller will have three voting options like manual voting, mobile voting and smart card voting.

Software: Implementation of software based voting machine will provide wide accessibility to the users using internet.

Centralization: Implementation of server based voting machine will help to connect all the hardware and software voting machines to central server through 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 system. No other voting systems have integrated all types of voting in the same system and the system will be designed, implemented and tested for the reliability.

EMS performs all administrative tasks related to the chosen election configuration, such as:

- Contests and jurisdiction specification
- Polling stations
- Candidate registration
- Ballot generation
- Results collection
- Results tabulation
- Winner proclamation
- Election results publication

All election information set up by EMS can be used later by other devices during the course of the electoral event. EMS also establishes the configuration files for each voting machine being deployed, and finally contributes to the creation of reports and legal documents with the evaluation results of the system's performance [5].

The different electronic tools and options will be provided to an eligible voter and he can use one of them to join polling stations with their smart cards to cast their votes, and immediately after voting the votes will go to the central election server, where each polling station will be having its own code number and the eligible citizens voted from different polling station in the end there will be individual and global results from all polling stations including the votes for those who used their mobile phones, computers etc.

Any voting system should respect the real time for starting and closing voting time i.e. the system should be able to start and end voting time automatically. After the results publication, if there is any complain for any candidate about his result, verification and audit has to be done by the concerned team(s).

V. CONCLUSION

Our proposed EMS will provide the different options to the voters based on their choices. Those options are manual voting, smart card voting, mobile voting and internet voting. All the voting options will be connected to the Centralized Server System. Measure securities have to be provided to the voting system and the system should full fill the minimum user requirements and the election system will motivate the majority of citizens eligible to cast their vote using high secured systems.

RSA and HEA will play an important role in the security measures of EVMs. Otherwise the system cannot be strong enough to be useful for any election system. E-voting system will minimize the costs to the Government, maintain integrity of digital ballot against security vulnerabilities. The citizen eligible for voting is provided various technology options like mobile, internet and computers connected to the internet instead of using paper based voting system.

After the election, the votes will be tabulated, stored and counted automatically by the central server system & ballot boxes need not be transported. Election results can be declared immediately once polling is over.

REFERENCES

1. Amare Anagaw Ayele, Dr. Vuda Sreenivasarao, "A Modified RSA Encryption Technique Based on Multiple public keys ",International Journal of Innovative Research in Computer and Communication Engineering, June 2013

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 8, August 2015

2. Anil Pandit, R. C. Gangwar, "Issues and Challenges in Electronic Voting and Direct Recording Electronic Voting Systems", *IJARCSSE*, January 2015.
3. Diponkar Paul, Sobuj Kumar Ray, "A Preview on Microcontroller Based Electronic Voting Machine", International Journal of Information and Electronics Engineering, March 2013
4. http://www.beyondintractability.org/essay/human-rights-protect
5. http://www.smartmatic.com/voting/software/detail/electoral-management-system-ems/
6. Okediran Oladotun O., Ladoke Akintola, "Towards Remote Electronic Voting Systems", Computer Engineering and Intelligent Systems, No.4, 2011.
7. PRESS INFORMATION BUREAU GOVERNMENT OF INDIA, "EVM – Electronic Voting Machine", General Elections-2014.
8. Prof. Dr. Hala Helmy Zayed, Monira Monir Haroon Khater, " Secure E-Voting System ", 2011.
9. R. G. Saltman, "Security Properties for Electronic Voting, Accuracy, integrity, and security in computerized votetallying", 1988.
10. S.V.Prasath, R.Mekala M.E. (PH.D.), "A Literature Survey On Micro-controller Base Smart Electronic Voting Machine System", IJARECE, December 2014.
11. https://jhalderm.com