ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization *Volume 4, Special Issue 9, July 2015*

National Conference on Emerging Technology and Applied Sciences-2015 (NCETAS 2015)

On 21st & 22nd February, Organized by

Modern Institute of Engineering and Technology, Bandel, Hooghly-712123, West Bengal, India

On Some Design Issues of Electronic Voting Machine

Subendhu Bhattacharya [1], Suvendu Chattaraj [2]

U.G. Student, Department of Computer science & Engineering, Om Dayal Group of Institutions Uluberia, Howrah, West Bengal, India [1]

Assistant Professor, Department of Computer Science & Engineering, Om Dayal Group of Institutions Uluberia, Howrah, West Bengal, India [2]

ABSTRACT: Indian and other democratic countries elections are conducted through electronic voting machines (EVM). It is developed over the past two decades. EVM retainsall characteristics of voting by ballot papers, while making election process a lot more easier than manual counting of ballot papers. EVM is fast, also it's working is expected to be absolutely reliable. It saves lot of time and manpower. However there are many security loop holes and threats, which affect the results of the election. Several researchers team have concluded that EVM used in India are no longer tamper proof and are prone to internal and external attacks. Current work investigates such threats and proposes a solution for more secure and reliable voting.

KEYWORDS: Embedded system, Microcontroller, GSM Module, Frequency hop- ping, Embedded data encryption

I. INTRODUCTION

EVM have replaced ballot paper voting system in India since past two decade. EVM has advantage over polling by ballot papers, as it save considerable amount of time and it is more secure than manual counting of ballot papers. It's simplified design provides an easy environment of operation for the voters. It reduces the chances of error while counting the votes. The advantage of EVM are transparency, speed & simplicity. The EVM consists of two units that are inter-linked. Balloting Unit (BU) - which a voter uses to exercise his vote, and Control Unit (CU) - used by the polling officials. Balloting unit is a simple voting device which displays the candidates list, party names and symbols. The voters cast their vote by pressing the desired switch, corresponding to the name of each candidate. A single balloting unit holds names of 16 candidates, which may be extended by associating more BU, with the control unit.

Control unit controls the overall conduction of polling, functions such as display of total votes polled, counting at the end of the poll, and finally, declaration of results are accomplished by CU. This electronic CU gives all necessary information like count of total votes, candidate wise result etc. by pressing few buttons. EVM operates on a battery power source making it independent and totally reliable by maintaining total voting secrecy, without the use of ballot papers. However, since the past decade, many security loop holes and threats have crept into the EVM, making it vulnerable. Recently in general election of 2014, many news reporters and media have reported vulnerability of EVM used in India as major problem[1]. Similar voting machines are allowed in most states of USA with a paper backup[2],[3]. These machines have been found to be prone to dangers such as displaying fraud results and more importantly, lack of transparency and verification associated with it. Access to hardware of these machines, may allow one to replace the original display unit such that, fraud results are displayed and counted. Also the software burn't in the EVM is not secure due to lack of its technical design and architecture of the machine. Software may be manipulated to direct vote for candidate A to candidate B[4]. Current work investigates problems associated with EVM. The study includes vulnerable security loopholes in present EVM model and brings these threats to notice. A better solution to overcome these drawbacks of the present EVMs has been proposed, with the explanation of the methods which avoid security threats. Organisation of the paper is as follows. After a brief introduction, some back- ground along with challenges involved in the evolution of EVM, and also the detail of current EVM has been discussed in section-2. Detailed description of problems associated with EVM such as tampering of EVM before and after the counting session, vulnerability of the design and software burnt in it, has been discussed next. Proposed solution to mitigate these

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 4, Special Issue 9, July 2015

National Conference on Emerging Technology and Applied Sciences-2015 (NCETAS 2015)

On 21st & 22nd February, Organized by

Modern Institute of Engineering and Technology, Bandel, Hooghly-712123, West Bengal, India

problems, by sending the vote data wirelessly to a secure centralized server as and when vote is cast, by interfacing global system for mobile communications (GSM) module is discussed in section-4. Section-5 concludes the present discussion.

II. BACKGROUND

Idea of EVM in India was emerged by the Chief Election Commissioner in 1977 and he advised E-voting to save time, expenditure on storage, transportation and security of ballot paper. In order to overcome these problems and errors in counting of ballot papers, electronic voting was recommended. Challenges was to develop a machine which would fit into the existing election procedure and appear familiar to the voter, and would be transparent and acceptable to all.

a) Evolution of EVM

The first Indian EVM's were developed in 1980. The first generation of EVMs were based on Hitachi 6305 microcontroller and used firmware stored in external ultraviolet (UV) - erasable PROM's along with 64 kb EEPROMs for storing votes.1st generation of EVM's were based on UV- erasable PROM's and were also risky to be used in national elections, because of their 15-year service life was expired. 2nd generation of EVM's are gradually developed and used nationwide beginning in 2004. These machines moved the firmware into the CPU and up- graded other components. In 2006, the developers developed a next generation machine by making further changes. These EVM consists of two main components Control Unit and Balloting Unit, whose functioning are discussed in previous section.

b)Detail Of EVM

The CU and BU are connected with a cable.The CU remains with the presiding officer and the BU is placed inside the voting compartment. Instead of giving ballot papers, the presiding officer operates the control unit of EVM. By this procedure a voter cast his vote by pressing another button on BU corresponding to the candidates name or symbol of their choice. Steps of casting and registering votes are as follows:

- Ready lamp glows GREEN when ballot button on CU is pressed by polling officer to enable voting. Turns off when voter has finished casting his vote.
- Candidates light turns RED when the voter pressed the candidates button.
- In ballot paper Screen candidates name, serial number and Symbol of contesting candidates is listed. The controller used in EVMs has its operating program frozen permanently in silicon chip at the time of manufacturing by the manufacturer. Details of CU and BU are depicted in Fig.1
-

III.PROBLEM DEFINITION

Many independent security analysis has been done by several research teams and their study includes video demonstrations of two attacks that the researchers carried on EVM, also descriptions of various other threats described as follows:-

Before voting- one evince threat was based on replacement of the actual display unit that displays candidate's total vote[5]. The study showed how 'display-unit' can be replaced with a fraud one which is pre- programmed to transfer a percentage of the votes in favour of a chosen candidate.

After voting- The 2nd evince threat was accessing memory where votes are stored by using a small on-clip unit (device). EVM's memory can be manipulated between the election and the public counting session by using a small on-clip device. [6]. EVM is a microcontroller based device, which uses a electrically programmable memory to store voting record.

This memory can be read and written by an peripheral on-clip interface. This on-clip interface is used to manipulate the data by swapping the vote from one candidate to another. EVM's can also be hacked with a bluetooth device[7]. Recently in 2014 election in Assam, Pune, West-Bengal etc. EVM was found to be triggered to vote for a particular candidate [8]. In order to mitigate these threats, the researchers suggest, moving to a voting system that provides greater transparency.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 4, Special Issue 9, July 2015

National Conference on Emerging Technology and Applied Sciences-2015 (NCETAS 2015)

On 21st & 22nd February, Organized by

Modern Institute of Engineering and Technology, Bandel, Hooghly-712123, West Bengal, India

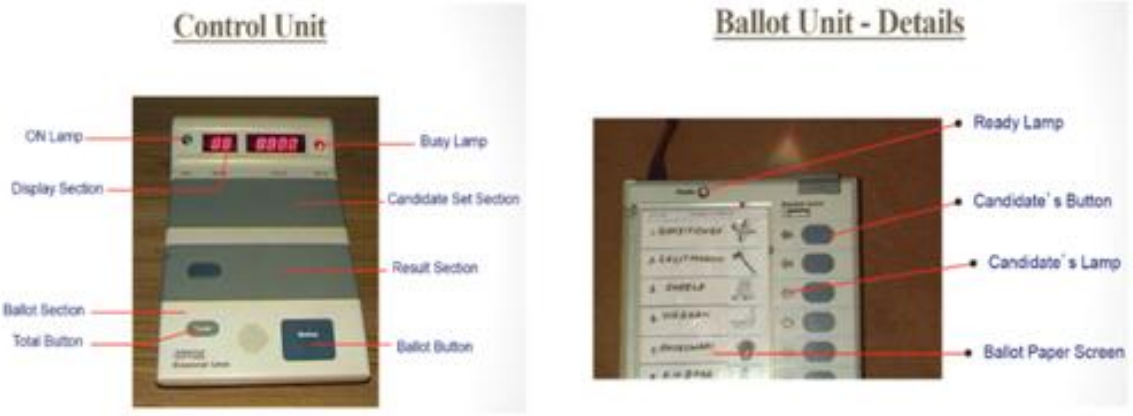

Fig. 1. Control Unit and Balloting unit details

IV. PROPOSED SOLUTION TO OVERCOME THE SAID PROBLEM

The complex hardware design of EVM has been a significant source of vulnerability. As we have seen that EVM's can be tampered with by substituting hardware components or by altering the internal state of the machine using malicious hardware devices. Simple design of machine cannot cure EVM's security problems. Furthermore, when design is simple, it is difficult to apply certain defences, such as cryptographic integrity and confidentiality protections. Simple and cheap hardware designs allow easy reverse engineering process for hardware tampering. For the convenience of voter's the external design of the balloting unit in proposed design has been kept unaltered. Since field programable gate array (FPGA) are less prone to external signals, entire circuit design is to be based on FPGA, and the BU & CU will be designed based on unibody structure respectively to avoid physical tampering of the machine. If anyone tries to open the body then entire EVM will get frozen.

Current work proposes that, every single EVM is to be linked with a centralized server as and when it is switched on through a GSM module. This enables the vote data to be transferred to a server, placed in the chief election commissioner's (CEC) office for reducing the possibilities of data manipulation. When a voter cast their vote by pressing the switch allotted for their favorable candidate, balloting unit gets locked and buzzer blows. Again to reactivate the BU, activate-switch is to be pressed by presiding officer who operates the CU. In CU, a microcontroller is used which will process the entire voting operation. The GSM module interfaced with the microcontroller board in CU, sends the vote data to the centralized server to avoid data theft before and after the election. If the vote data is sent to the secure centralized server through secure channel, as and when vote is cast, data theft can be minimized.

Before sending the vote data to the centralized server, all the vote data is to be encrypted by embedded Advanced Encryption Standard (AES)[9],[10],[11], to protect it from hackers and persons who operates the centralized server. Based on proposed design of control unit, 1 GSM module and 1 thermal printer will be interfaced with a microcontroller board (system on chip). With respect to subscriber identity module (SIM) number their vote data is sent and saved in server. As the vote data is sent wirelessly using a GSM module, there are possibilities that propagated signal may get trapped. To avoid signal trapping frequency hopping technique may be availed. A database management system in server will store the data in a tabular fashion with respect to sim number, and once the decryption key is entered by the chief election commissioner, all data gets decrypted and counting starts. Also a thermal printer is interfaced with microcontroller will produce a printout of name, symbol, serial number of the candidate who entertains vote. This will give a public satisfaction and transparency to all voters for the verification of their vote. Every candidate shall have a respective serial number.

The algorithm to cast one vote confirming the current design is described as follows:

Start do

{ 1. Initialise the control unit & balloting unit to
take new vote.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization *Volume 4, Special Issue 9, July 2015*

National Conference on Emerging Technology and Applied Sciences-2015 (NCETAS 2015)

On 21st & 22nd February, Organized by

Modern Institute of Engineering and Technology, Bandel, Hooghly-712123, West Bengal, India

2. Display in control unit L.C.D 'Ready to Vote'.
3. Read signal sent from control unit to balloting unit as in the case of existing EVM design.
4. Voter will cast their vote through balloting unit.
5. Serial number of candidate is sent from balloting unit to control unit.
6. Display in control unit L.C.D 'Voted Successfully'.
7. Receive serial number in control unit from balloting unit.
8. Print out of serial number of respective party from thermal printer.
9. Encrypt the serial number in control unit through embedded AES program .
10. Send the encrypted data with the EVM Id through GSM Module to centralised server.

} while no more voting

End.

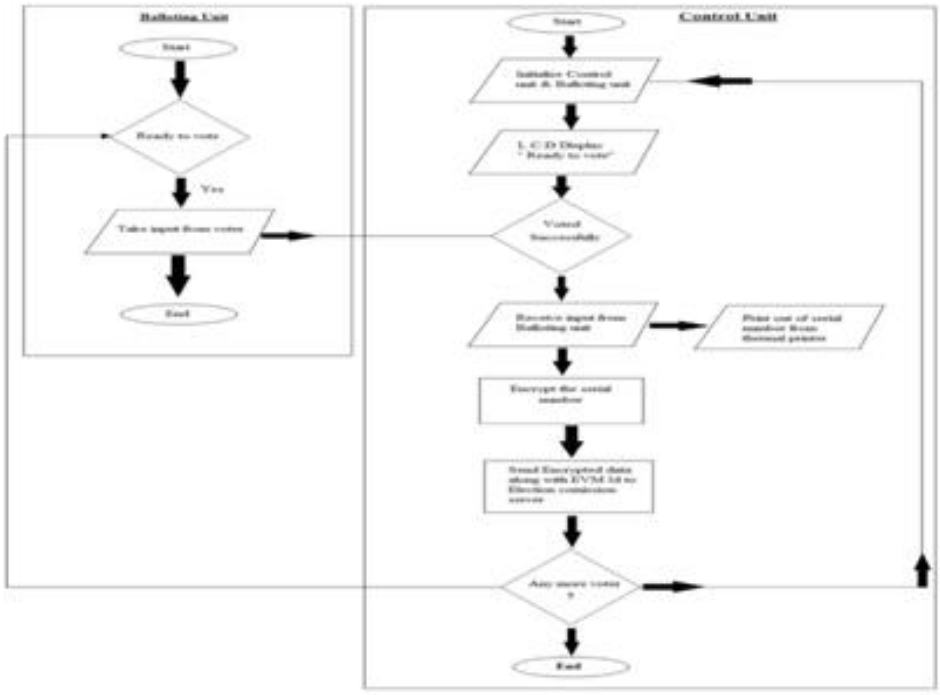

Fig. 2. Flow chart to show the entire data flow of upgraded EVM

As an when EVM is power-on, both balloting unit and control unit gets initialised. Display in control unit shows “Ready to vote”. Voter vote for their favourite candidate and serial number is generated. The thermal printer prints out the se- rial number of the candidate for whom the vote is casted. Then the serial number gets encrypted through embedded (AES) program and sent wirelessly through GSM Module. If there is any more voter then entire process gets repeated, as depicted in Fig.2. The circuit diagram of the balloting unit and its interfacing with microcontroller is shown in Fig.3. An L.C.D is interfaced to show when the balloting unit is ready to take vote and finally the total vote count of respective candidates.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization *Volume 4, Special Issue 9, July 2015*

National Conference on Emerging Technology and Applied Sciences-2015 (NCETAS 2015)

On 21st & 22nd February, Organized by

Modern Institute of Engineering and Technology, Bandel, Hooghly-712123, West Bengal, India

Fig.4 shows the block diagram of operation of proposed EVM. As and when a voter caste vote, a serial number of the candidate for whom the vote is casted is generated and processed through microcontroller to print the serial number of the candidate along with the symbol of that party. Once the printing process is done the serial number gets encrypted and is sent through the GSM module to destination server. Then L.C.D in CU displays "Voted Successfully"and when it gets ready to take new vote, L.C.D in CU displays "Ready to vote". This process continues till the last voter caste the vote. The use case diagram is shown In Fig.5 use of EVM by chief election commissioner, candidate, presiding officer and voter is explained.

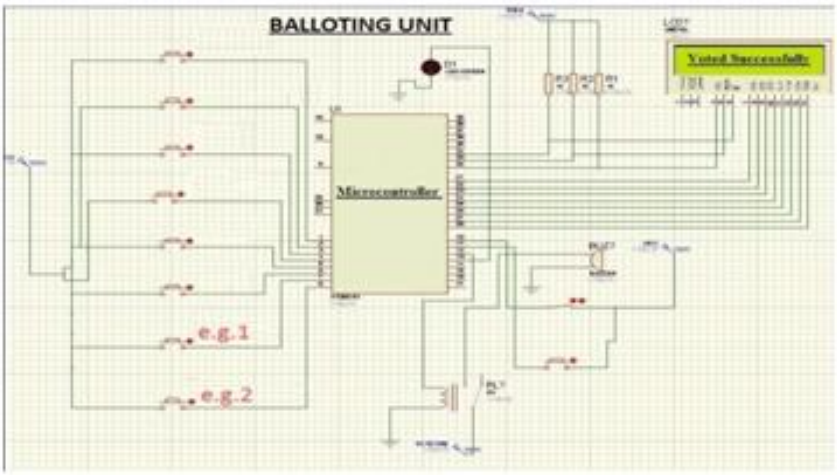

Fig. 3. Circuit Diagram of operation of EVM

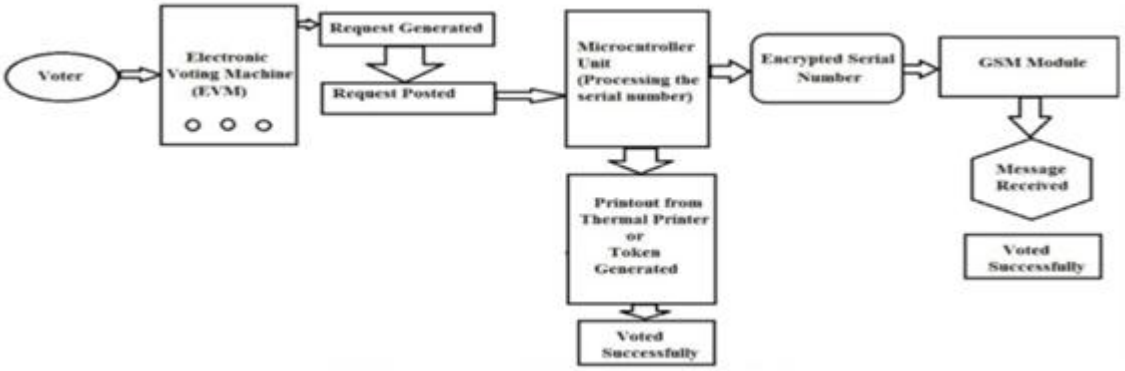

Fig. 4. Block Diagram of operation of EVM

The usability of proposed design is manifold.

V. CONCLUSION

Current work discusses a design of EVM which allow entire voting system to be centralised and more secure. Since present EVMs accessible to fraud people. In proposed design of EVM the risk of tampering vote data is minimised by encryption of all vote data and sending it wirelessly to a centralised server. Extra expenditure to protect EVM after election, and the money spend on the security will be saved along with considerable amount of time. Three step verifications of result is proposed which includes printout of candidate's serial number from thermal printer, internal memory storage, result stored in the server. Since centralized server is used, in future there will be an option for online voting, and sms voting.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization *Volume 4, Special Issue 9, July 2015*

National Conference on Emerging Technology and Applied Sciences-2015 (NCETAS 2015)

On 21st & 22nd February, Organized by

Modern Institute of Engineering and Technology, Bandel, Hooghly-712123, West Bengal, India

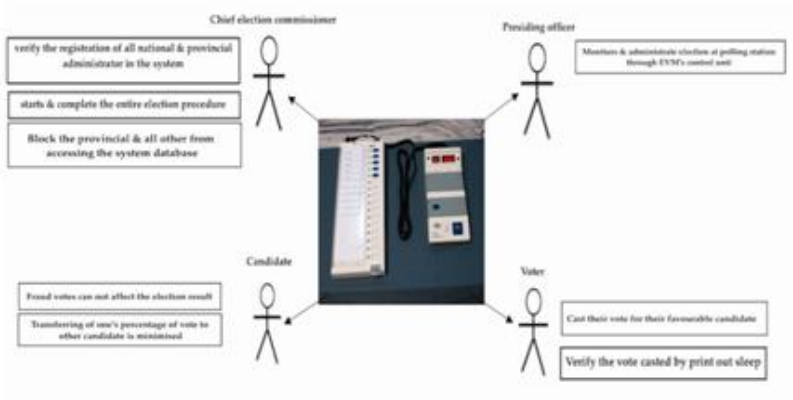

Fig. 5. Use case diagram of proposed election system

Implementation of such system and rigorous testing is yet to be done. In present scenario implementing online voting across the country is difficult due to lack of massive computer literates. Current design is based on microcontroller and FPGA. However using of crypto- processors may produce more secure electronic voting machine as such processors are more secured. Embedded encryption program can be developed further to increase the level of security. Also such issues may be topics of further research.

REFERENCES

[1]Defective Pune EVM 'transfers'all votes to Congress. http://timesofindia.indiatimes.com/news/Defective-Pune-EVM-transfers-all-votes-toCongress/articleshow/33852397.cms
[2]http://thevotingnews.com/tag/voter-verified-paper-audit-trail/
3]http://usatoday30.usatoday.com/news/opinion/editorials/story/2012-09-19/electronic-voting-fraud-security/57809062/1
[4] J.AlexHalderman,HariK.PrasadRopGonggrijpConductedtheresearchonIndias EVM and Concluded Indian EVMs are vulnerable to fraud.17th ACM Conference on Computer and Communications Security
http://indiaevm.org/authors.html
[5] This Is The Link Of The Video Which Demonstrate Attacks Before Voting And After Voting On Electronic Voting Machine http://youtu.be/apkSkb6Ak3I
[6] Electronic Voting Machine, Chapter 39, Reference handbook, Election Com- mission of India". Pib.nic.in. Retrieved 2010-09-01. Used in Hazaribagh District. http://pib.nic.in/elections2009/
[7] An EVM that 'votes'only for BJP stuns poll Staff in Assam http://timesofindia.indiatimes.com/india/AnEVM-that votes-only-for-BJP-stuns- poll-staff- in-Assam/articleshow/33153231.cms
[8] http://arxiv.org/pdf/1408.0733.pdf
[9] http://www.embedded.com/design/configurable-systems/4024599/Encrypting-data-with-the-Blowfish-algorithm
[10] http://brainstorms.in/?p=309
[11] http://grietinfo.in/projects/mini/eee/doc-a.17evm.pdf