International Journal on Emerging Technologies (Special Issue NCETST-2017) **8**(1): 403-405(2017)
(Published by Research Trend, Website: www.researchtrend.net*)*

ISSN No. (Print) : 0975-8364
ISSN No. (Online) : 2249-3255

E- Voting: An analysis of Security Issues in EVM

Vishwa Bhaskar Rao[1] and Mohit Giri Goswami[2]
[1]Assistant Professor, Department of Computer Applications, Invertis University Bareilly, (U.P.), INDIA
[2]Assistant Professor, Amrapali Institute of Technology and Sciences, Haldwani, (U.K.), INDIA

ABSTRACT: Voting in India is a constitutional right. Voting is the heart of democracy. Voting is a fundamental right under the Representation of People Act 1950 and fundamental rights in India under Article 19(1)(a). Indian democracy is built on the foundation of voting. Voting is a responsibility as it is a right. Every citizen must cast his or her vote if one is a citizen over 18 years of age. The citizens of India elect their representatives and these representatives form a government. A voter has right to know that his or her vote is recorded or counted accurately through EVM or not.
This Paper represents introduction of EVM, and evaluation of traditional voting process to E-voting process. Electronic voting machine is already used in developed countries but in India it is a burning issue and security is major concern, so this paper also focus on the security issues of EVM.

Keywords: Electronic Voting Machine

I. INTRODUCTION

Electronic Voting machine is a electronic device, which is used to store votes in place of earlier voting system. It can be easily used by the polls personnel and voters. The electronic voting machines (EVMs) used in Indian elections are internationally known as Direct Recording, which record votes directly in electronic memory.

The electronics Corporation of India Limited (ECIL) and Bharat Electronics Limited (BEL) developed the EVMs and the foreign companies in US and Japan supplying microcontrollers. These companies are owned by the Indian government. ECIL developed the first Indian EVMs in 1980s.

In 1984, the Supreme Court of India held that the use of electronic voting machines in elections was "illegal" as the Representation of People (RP) Act, 1951 did not permit use of voting machines in elections. Later, the R.P. Act was amended in 1989 incorporating Section 61A. However, the amendment says voting machines "may be adopted in such constituency or constituencies as the Election Commission may, having regard to the circumstances of each case, specify." Violating the provisions of the R.P Act, the Election Commission has conducted 2004 and 2009 nationwide general elections only using electronic voting machines. Many legal experts say that going by the 1984 judgment of the Supreme Court, parliamentary elections of 2004 and 2009 may be held illegal.

EVMs manufactured in 1989-90 were used on experimental basis for the first time in 16 Assembly Constituencies in the States of Madhya Pradesh (5), Rajasthan (5) and NCT of Delhi (6) at the General Elections to the respective Legislative Assemblies held in November, 1998.

EVM system

In India, an Electronic Voting Machine consists of two Units – a Control Unit and a Balloting Unit – joined by a five-meter cable (Fig. 1). The Control Unit is with the Presiding Officer or a Polling Officer and the Balloting Unit is placed inside the voting compartment. Instead of issuing a ballot paper, the Polling Officer in-charge of the Control Unit will press the Ballot Button. This will enable the voter to cast his vote by pressing the blue button on the Balloting Unit against the candidate and symbol of his choice [1].

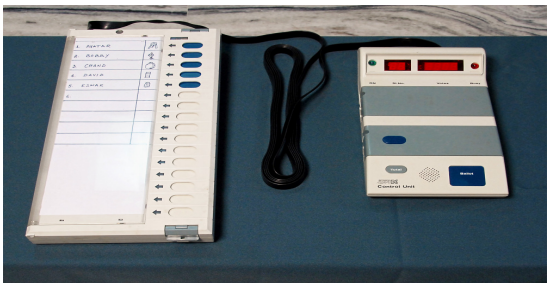

Fig. 1. Electronic Voting Machine.

EVMs run on an ordinary 6 volt alkaline battery manufactured by Bharat Electronics Ltd., Bangalore and Electronic Corporation of India Ltd., Hyderabad. Therefore, even in areas with no power connections, EVMs can be used.

EVMs can record a maximum of 3840 votes. As normally the total number of electors in a polling station will not exceed 1500, the capacity of EVMs is more than sufficient (fig 2).

EVMs can cater to a maximum of 64 candidates. There is provision for 16 candidates in a Balloting Unit. If the total number of candidates exceeds 16, a second Balloting Unit can be linked parallel to the first Balloting Unit. Similarly, if the total number of candidates exceeds 32, a third Balloting Unit can be attached and if the total number of candidates exceeds 48, a fourth Balloting Unit can be attached to cater to a maximum of 64 candidates [2].

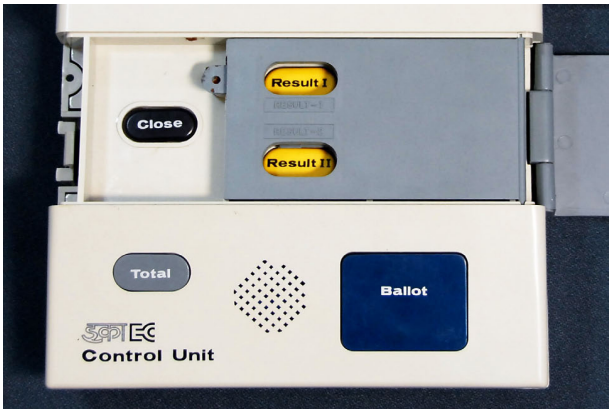

Fig. 2. Counting Vote.

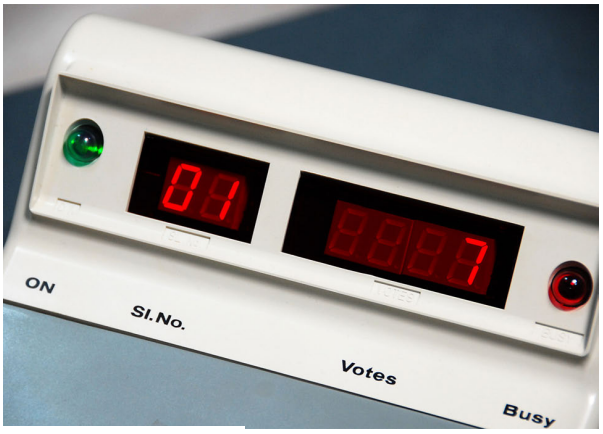

Fig. 3. Counting Vote.

Election Process

The general process of electronic voting on the most common EVMs models as

- On the first step the voter checks the voter's ID with poll workers. The polling personnel and the agents verify the name and identify the voter. To stop duplicate voting they take signature or thumbs print of the voter and, mark the voter's right index finger with indelible ink.
- Next step, the voter enters the polling booth, to allow one vote a poll worker presses the BALLOT button on the control unit, a green READY light to glow on the ballot unit. The voter presses the button of his or her choice for the candidate. The control unit emits a loud beep to indicate that the vote has been cast., the ready light turns off, a red light button glows and The red light then turns off automatically. This process repeats for each voter.
- At the end of the poll, the presiding officer removes a plastic cap on the control unit and presses the CLOSE button, which stop the EVM from accepting further votes. The ballot unit is disconnected and the control unit is placed in storage until the public count.
- On the counting day, at counting centre, an election official breaks a seal of the control unit and presses the RESULT button. The sequence of outputs displays on the control unit i.e. the number of candidates, the total votes, and the number of votes received by each candidate.
- To determine the results of the election, the Counting officials manually record the totals from each machine and add them together. The machines are then placed in storage for the next election.

Security Requirements

The security requirements that electronic voting system must satisfy are –

- **Eligibility** means only eligible voters can cast their votes during election period.
- **Authentication** makes sure that the one who votes is the right one and no one else.
- **Voter's privacy** enable's voters to vote in a highly private way in which their personal information and voting process information are protected and can't be known by others
- **Robustness** means that electronic voting system should be protected against any attacks, fraud and disruption.
- Finally, **fairness** in announcing voting results only at the end of allowable voting period**.**

Advantages of EVM-

In India, the use of Electronic Voting Machines (EVMs) has made drastic change in Indian election

process. As compare to traditional voting procedure, the simple operational procedure of electronic voting machine is the most valuable feature. It removes booth capturing, invalid votes, duplicate votes, and makes easy and faster counting process.

Disadvantages of EVM-

- Dr. Alex Halderman, professor of computer science in the University of Michigan says, "EVMs used in the West require software attacks as they are sophisticated voting machines and their hardware cannot be replaced cheaply. In contrast, the Indian EVMs can easily be replaced either in part or as wholesale units." EVMs manufacturers can perform fraud not only by using generic microcontroller but they replace mother board also (contains the microcontroller).

  These manipulations are undetected. The BEL and ECIL (EVMs manufacturers) have shared the top secret EVM software program to copy it onto the microcontrollers used in EVMs with two foreign companies, Microchip(USA) and Renesas (Japan).Whereas it can be done in India by manufacturers. Other than this when they handover the microcontroller chip, the code was unreadable by the Indian EVM manufacturers, and this software not even made available with election commission for some security reason. With such facts the software and as well as hardware both are not safe and secure.
- Apart from replacing hardware parts and software sharing, Indian EVMs can be manipulated using fraud display board by replacing real display in control unit which shows the fraud vote count result at the time of counting.
- Unlike the fraud display there is a device which attached directly to the EEPROM memory card inside the control unit. In India counting of votes takes some weeks after voting so insider or criminal can use the clip-on device to change the votes recorded in EVM.
- Due to the lack physical security of machine the Dishonest insider can use any hardware to steal votes
- The Government at the time of election may hire any manufacturer or company for manufacturing EVMs according to the needs of the political party in power. An EVM can be tampered during manufacturing stage, that too during the manufacturing of the Chip. After tampering the EVM, it's difficult to detect it by a third party.
- The votes that are cast using the electronic voting machines are stored in a safe storage or space in the computer machine memory. The time gap between election and the counting of votes is a risk to possible hacking and manipulation.
- There are so many issues which comes in newspaper and news channel that the EVMs result is not fair in the election of 2014 and also in election of 2017.

II. COUNTRIES REJECTED EVMS

Several developed countries in the world rejected electronic voting machines because they are easily manipulate, not secure and not error free for election in democratic society. In India all the EVMs do not produce paper trails, which is its major disadvantage. Developed nations like the United Kingdom, France, Japan and Singapore have so far stuck to voting on paper ballots, owing to their simplicity, verifiability and voter confidence in the system.

The countries Ireland, Italy, California, Germany, Netherland, Finland rejected EVMs because they don't trust on EVM machines and think that E-voting is unconstitutional.

III. CONCLUSION

In this paper, we introduce the existence and the working process of electronic voting machine. On study of various security features of EVM we discuss the advantages and disadvantages of the electronic voting machine and conclude that EVMs are not secure, and this is not the best choice for corruption prone election that exist in India.

REFERENCES

[1]. Election voting machine – Election commission of India http://eci.nic.in/eci_main1/evm.aspx

[2]. Hari k Prasad, J. Alex Halderman, Rop Gonggrijp, (2010) Security Analysis of India's Electronic Voting Machines

[3]. Sanjay kumar, Manpreet singh, march(2012). Security enhancement of E-voting system.

[4]. Anooshmita Das, (2015).Usability of electronic voting system in India and innovatory approach.