Democracy at Risk: An Analysis of Electronic Voting Machines Security And Their Impact On Indian Democracy.

Ripima Narzary

Ph.D. Scholar, Gauhati University. ripimanarzary19@gmail.com

ABSTRACT

For more the two decades Elections in India are carried out by electronic voting (EVM) devices designed by two government-owned companies during the last two decades. These, recognised as EVMs in India, they are known for their simple architecture, ease of usage, and reliability, at the same time they have also been criticised for vulnerable and exploitative nature and repeated reporting of violations in elections. Despite this criticism, some elements design of the device were never officially disclosed and were not subject to a thorough objective protection review. In this paper we will discussed how EVM as machine base, are ease to serious attacks that might affect the result of the election and compromise the secrecy of the vote. We try to highlight the security reviews of EVM in this paper and its possibilities of violation which causes a great treat to any democratic country of the world.

Keywords:

EVM, Security, Design, Democracy, Human Factors, public Administration, E-governance.

Article Received: 18 October 2020, Revised: 3 November 2020, Accepted: 24 December 2020

INTRODUCTION:

In India voting is the most significant constitutional right of citizens. Voting is the very foundation pillar of any democratic country be it direct and indirect vote. Voting became constitutional right in India by the 1950 People's Act and fundamental rights under Article 19(1) (a). Voting is an obligation, just as it is freedom. Any citizens must cast his or her vote by 18 years of age under the universal adult franchise. The citizens of India shall elect their representatives, and a government shall be formed. India is the biggest democracy in the country. More votes were cast in recent national elections in 2019 than the whole population of the United States and Canada, and the vast majority of voters used paperless direct-recording electronic voting systems (DREs).

The electoral authorities of India insist that electronic voting machines usually referred to as EVMs, are entirely protected and used in India. E.g., in an August 2009 press release, the Election Commission of India, the country's highest electoral authority, asserted: "Today, once again, the Commission fully reaffirms its belief in the infallibility of EVMs." These areas ever absolutely tamper-proof.' "Chief Election Commissioner Navin B. Chawla has quoted in the media as saying the devices are “full “with no need to “technological change" as recently as April 26, 2010. To support these arguments, the architecture of EVMs, which is far more comfortable than most other DREs used internationally, and officials often cite various procedural protections.

Although EVM manufacturers firms and election commission of India have managed to hold the design of the EVMs confidential, for potential attackers, this represents just a small obstacle. There are about 1.5 million EVMs in operation globally, and only one of them would need access for offenders to corrupt the system and to create crime out of it. There are also many ways for manipulating and hacking Indian EVMs computers, with or without unethical election polling officer or insider in charge of conducting election. The type and size of possible manipulations can differ subject to the local setting and security environment, but neither the functionality of the devices nor their hidden nature makes them safe.

This research reveals in India, the EVMs that we used are unsafe along with manipulative and exploitative to several assaults. In many democratic country, such as Germany, Canada, California identical paperless DREs have been discontinued. The Indian election authorities should study the protection measures that are currently in effect immediately and check all EVMs for fraud signs. A different voting framework that ensures better protection and accountability could be implemented by India in the future.

Electronic Voting in India

In business with two government-owned firms, India's Electronics Corporation (ECIL) and Bharat Electronics Limited, India's Election Commission developed it is EVMs (BEL). Since the Indian government controls these businesses, they are not under the Election Commission's administrative jurisdiction. They are profit-seeking manufacturers aiming to sell EVMs internationally.

The first made in India EVMs machine is built by ECIL in the early 1980s. In some areas of the world, they were used but were never introduced nationally. These first-generation of Indian EVMs is based on Hitachi 6305 microcontrollers along with 64kb EEPROMs to store votes in external UV-erasable PROMs. Models of the second century were launched by both ECIL and BEL in 2000. The firmware was transferred into the CPU by these computers, and other aspects were upgraded. Beginning in 2004, they were eventually introduced in larger numbers and used worldwide. In 2006, the election commission recommended the manufacture of the third generation version for improved and fast up to date result.

There were about 1,393,235 EVMs in service in 2010 July, according to Election Commission figures. Of these, 492,000, with 243,500 from BEL and 185,700 from ECIL, were all third-generation version computer produced from 2006 to 2009. The rest 901,235 were second-generation versions computer produced between 2000 and 2005, with BEL manufacturing 440,146 and ECIL producing 490,206. (The first-generation machines are deemed too risky to use in national surveys because of their 15-year service life has expired, although some are still utilised in certain local and state election) There were 426,752,578 votes cast in the 2009 parliamentary election, with an average of 306 votes per system.

Election Procedures through EVM Operation

India's EVMs has two key components. Polling personnel monitoring unit collects and accumulates ballots and a polling unit collected and used by electors in the voting booth. These systems is linked by a 5.5 m wire, one end of which is attached to the ballot unit .A battery pack within the control unit controls the device.

EVM has 16 keys for members. It is sealed with a plastic masking tab within the device if any are unused. For a limit of 64 contestants, up to 4 ballot units may be connected together in this manner.

In a variety of public records, election procedures are defined. Staff set up the ballot machine before the referendum by adding a paper label that displays next to the campaign buttons the candidate name and party symbol. The poll staff holds a limited mock election on the morning of the election to verify the computer. By clicking the transparent button, they then set the totals vote count to zero, in which the control device monitor indicates that zero ballots have been cast. At any point, staff will verify this count by clicking the complete icon. To restrict entry and reset activities seals are then put on different control unit sections.

When an elector appears, staff check their name and report the voter's existence by collecting a signature or thumbprint. They mark ink to correct index finger of the elector to stop double voting. Next a polling officer presses the ballot button on the control unit to allow one vote. This allows the ballot device to shine with a green, ready light. The elector reaches the voting booth and pushes the button of choice to the candidate he supports. Next a red light glows besides the candidate party logo and the ready light goes out, and a loud beep is created by the control device to indicate that vote has been cast. The red light then turns off automatically. This process repeats itself with each elector.

At the conclusion of the poll, the polling officer then removes a cover on the control device and clicks the close switch, stopping extra votes from being approved by the EVM. The ballot machine is removed, and the control unit is placed into storage before the result count, which could occur weeks away.

The EVMs are sent to a counting center on the counting day. An election official opens a seal on the EVM in public view, and the result button is pressed. The EVMs monitor displays a series of result:

1) The number of candidates,

2) The overall number of votes,

3) The number of votes obtained by each nominee.

Officials manually record the totals from each computer and connect them together in order to determine the final score. The computers are then stored in storage before the next election.

Challenges for Electronic Voting in India

Indian EVMs should be built to run further complex environmental factors and operating restrictions than prior security assessments that examined other electronic voting systems. These criteria have influenced the new machines' basic configuration, and our protection review has been affected. The problems include, among others:

Cost The device's cost is a big problem, with well over a million EVMs in operation. Constructed from cheap commodity materials, the new EVMs cost only $200 for each group of devices, considerably fewer than Unites states EVMs machine but it doesnot go cheap with the Indian economy situation.

Lake of Electricity Several polling stations are situated in remote villages that does not have unreliable coverage for electricity. Thus, rather than only having a battery as a substitute, the EVMs run entirely from battery control.

Natural Disasters India's diverse atmosphere has excellent temperature extremes. Under these unfavorable circumstances, EVMs must run and be processed for lengthy periods in buildings without climate protection. The study of the Election Commission mentions more dangers arising from 'attacks by vermin, rats, fungi or technological hazards [that could lead to technical failure.'

Illiteracy Although many voters in India are well educated, many others are illiterate. In 2007, the country's literacy rate was 66 percent and just around 55 percent among women, so it must be the norm rather than the exception to deal with illiterate voters. Therefore, ballots display both graphical party icons and individual names, and without written instructions, the devices are intended to be used.

Application Unfamiliarity Some voters in India have very little technology exposure and could be frightened by electronic voting. 'sixty-year-old kausal Topon, for instance, impoverished tribal Oraon, which extracts firewood from the forest outside the Palamau Tiger Reserve, a Maoist hotbed 35 km from the town of Daltonganj," said, "I am afraid of the voting machine," before it came to my village."Mangal Jha, "a tribal and marginal farmhand in Palamau district's Chatarpur block," says he is “more frightened of the EVMs than the Maoists" because of technical illiteracy . In order to deter more threatening voters like these, India's EVMs encourage the elector to press only a single Key.

Booth Capture Earlier booth capture was a significant challenge against paper voting, a less than a discreet method of electoral manipulation seen mainly in India, in which party loyalists Will caste the vote on behalf of others several times by the use of force and also steal the ballot box to stop the winning of opposition candidates.

With times improved policy nowadays very few hazard can be seen but the electronic voting machines are still intended to deter with the restriction of the number of registering votes to five per minute.

Official Security Reviews of Indian EVMs

Two technical expert committee of Election commission of India EVM security official test were carried out. First was undertaken in 1990 in reaction to the "apprehensions expressed by political party leaders" regarding protecting the devices before implementing EVMs on a national scale. The research was carried out by team consisting of C. P.V. Indiresan, Rao Kasarbada, and S. Sampath, neither of them appeared to have previous information security experience. The committee had little access to the source code for the EVM; instead, it focused on the manufacturers' presentations and demos. Their report described two possible attacks: replacing the whole machine with a fake one and installing a computer between the cable of the ballot unit and the control unit. Through checking the computer, all threats, the study says, can be overcome. In the conclusion of the study they reported that EVM is tamper-proof."

A second 'Expert Committee' report was undertaken by the Election Commission in 2006 to examine improvements to third-generation EVMs. The committee representatives this time were A.K. D.T. and Agarwala Shahani, P.V. with. Indiresan's chair serving. All three were associated with IIT Delhi, but none claimed to have previous information security experience, like the first committee. Like pervious participants do not had access to the EVM source code and focused on the manufacturers' reports, exhibits, and site tours. The Commission repeated in its study the conviction computers are “tamper-proof"; But it proposed limited range to improve the safety level of the machines. This report placed the introduction of "dynamic key coding" from device of button presses to defend against simple cable attacks, with implementation of a real-time clock and time-stamped recording to each keypress including , false keypress, recording every effort by a "secret knock" to trigger malicious logic. Some of these enhancements have been applied in third generation EVMs, but threats cannot be avoided.

Reports of Irregularities

There have been several accusations and press accounts of electoral fraud concerning Indian EVMs in recent years. As there has never been a lawsuit involving EVM bribery, and there has never been a post-election inquiry to seek to ascertain the causes, the credibility of these claims is difficult to establish. However, in India, they are presenting a disturbing impression of electoral peace.

Rao thoroughly surveyed accounts of malfunctions. For example, he says that there was recorded EVM glitches in about 16 parliamentary districts around nation in the 2009 parliamentary election. It is documented that when the elector pushed a key of their nominee, a green light blinks for other keypress which they did not vote , which led to a direct assault on the EVM wire, Rao also comments on reports by influential lawmakers that engineers contacted them in 2009 promising to use this tool to rig elections.

Despite these events, the Election Commission's experts had given some criticism regarding protection of the EVMs attacking on the fairness and dignity of the Commission itself. In an interview, P.V. Indiresan, who chaired the 2006 technical examination of the Election Commission, went so far as to equate concerns about the protection of the EVMs with "asking Sita to prove her virginity by having Agni pariksha [fire trial]".

Vulnerability Analysis of Indian EVM

Earlier Security reviews of Indian EVM has suggested that ambiguity be avoided and the trustworthy computer base scale reduced. Based on this, India's EVMs may seem technically superior to many other DREs deployed. As mentioned in the previous section, the EVMs use a basic embedded device architecture. In contrast, DREs depend on commodity operating systems and run election software comprising thousands of code lines; the EVM software is lightweight, consisting of only a few thousand guidelines directly running on the hardware.

A variety of forms in this segment that attackers might tamper with the EVMs. Moreover, though the voting program is entirely error-free, the assaults are likely to carry out proceed to impact election result for the EVMs existence. Most importantly, it is reported that while the simplistic EVM architecture allows such software-based attacks less possible than in other DREs, it allows physical tampering attacks more.

Manipulation of Software before CPU Manufacture

Inside microcontroller chips, the EVM firmware is contained in masked read-only memory, and there is no framework to retrieving it and checking its reliability. It indicates the updates would be tough to spot if the program was changed until it was built into the CPUs.

The maker, Renesas, a Japanese corporation, incorporates the program into the CPU. (CPUs manufactured by Microchip, an American company, are used by other EVM models.) Considering the designer in charge of the compilation of the source code and distributing to creator of the CPU. With little risk of being detected, they might replace a version featuring a back entrance. This reality alone is going to be a powerful lure for fraud.

Similarly, before turning it into the chips, the chipmakers' workers may alter the compiled software image. Although manipulating source code, in the sense of academic science, reverse engineering firmware with such low complexity is not challenging and has been achieved for various voting schemes.

Substituting Look-Alike CPUs

These CPUs are delivered to India after the firmware is attach into the CPUs by international chipmakers installed into the control center's mainboards. Attackers may attempt to replace software-containing look-alike CPUs that dishonestly count the votes. In addition to the firmware, the CPUs are a commodity item, so it would be easy to procure and program similar hardware. By building a cryptographic framework for detecting the original CPUs, such as a challenge answer protocol based on a secret found in the original firmware, the EVM programmers may have rendered such attacks more difficult. As they did not, this assault will only involve developing new applications with almost similar features to the first, a process that, due to the fundamental nature of the EVMs, is surprisingly straightforward.

The actual chips could be substituted during the transaction with dishonest ones and the hackers get access inside the integrated computers. They could be exchanged before assembly by dishonest workers at the chip manufacture company or the transaction company delivering them. Customs members in the exporting nations, maybe at the behest of international security services, may even have the ability to exchange chips.

The program logic devices in the ballot unit could be attacked in such an attack and the core CPU used in the control unit. A well-funded competitor might create exact replica of the original chip kit comprising a radio receiver as well as a processor.

Substituting Look-Alike Circuit Boards

After producing the control panel's mainboard, exchanging in a deceptive CPU will entail jumbling and removing the surface-attached device, requiring maybe 10 minutes for a professional worker with sufficient equipment. However, attackers can find it faster to create a deceptive mainboard that is electrically compatible and replace it with the original. Due to the basic nature and purpose of this part, building a new board is reasonably straightforward. Replacing it will only entail the control unit to be opened, the snap-fitted board to be switched out, and the cable to the monitor unit reconnected.

The scheme often regards its instruments for input and output as trustworthy modules. By swapping the circuit board in the ballot unit with fake one reacts to push button incidents, or swapping the display board in the control unit with one that records incorrect voting totals, an intruder may steal votes. To capture the main press signals and substitute them with votes for other parties, an intruder might attempt to install a gadget between the ballot unit and the control unit. These attacks are easy since the EVMs architecture does not have any way to dictate one another.

Substituting Look-Alike Units

There is no realistic way for voters and polling officers to check that the EVMs which use is genuine, so intruders can attempt to create similar yet fake control units or ballot units to replace them before polling date . Since the units are tested to have no efficient means of checking the validity of the units they are matched with, it will cause the perpetrator to adjust election outcomes by swapping any unit with a deceptive one.

Tampering with Machine State

Although any part of the device are genuine , by explicitly accessing or modifying the computer's internal state in ways not imagined by its creators, attackers may always try to exploit the system. For, e.g., an intruder might explicitly rewrite the EEPROM chips that stores votes by adding external hardware to the circuit board of the control device. This is made simpler because the computers are built to connect the CPU to the memory chips using a simple I2C serial interface and because the simple software architecture does not try to encrypt or authenticate the data held there cryptographically.

CONCLUSIONS

EVMs manufactured in India are weak and exploitative to severe threats, providing extensive protection. Dishonest insiders or other offenders may install malicious devices with physical access to the computers that can alter the election results. Intruders with direct access before polling and counting can randomly adjust voting totals and discover which nominee has been chosen by each elector.

These challenges are profoundly ingrained. The architecture of the EVMs in India is solely focused on the physical protection of the devices and the honesty of electoral insiders. The technology hoped that threats on the ballot box and dishonesty would be more complicated in the counting process. Nevertheless, we find that such assaults remain plausible, despite becoming theoretically harder to recognize.

It is doubtful that easy upgrades to the current EVMs or election processes will solve these problems. The primary issue cannot be fixed by merely rendering the assaults that we have seen to be more difficult: India's EVMs do not provide accountability, so electors and election officials have no cause to ensure the devices function genuine.

India needs to reconsider carefully, for creating a healthy and open method of voting that is acceptable to its national principles and specifications. The usage of a voter-verifiable paper audit trail (VVPAT), which incorporates an electronic record held in a DRE with a paper voting record that can be audited by hand, is one alternative that has been implemented in other countries. Current EVMs do not have functionality that can be modified. However, a VVPAT could be inserted by interposing the cable between the control unit and the ballot machine. Another method is precinct-count optical scan (PCOS) voting, where electors fill out paper ballots at the polling station that are checked by a voting computer before being deposited in a ballot box. It will entail messing with both paper documents and electronic records to target one of these processes, regular checks are done to guarantee that both sets of record are similar and agree. A third alternative is to revert to clear ballots on paper. Simple paper ballots have a substantial degree of clarity considering many of their documented flaws, meaning bribery that does arise would be more likely to be observed.

When the devices were first deployed in the 1980s, the usage of EVMs in India was seemed like a smart idea. However, since then, technical knowledge of electronic voting security and hijacking the system has improved significantly, and other technologically sophisticated countries have introduced and then discarded voting in the EVM style. Now that we have a clear idea of what technologies can and cannot do, all potential innovations to the still concrete challenges posed by election, workers need to fix the concerns and shield them from view.

REFERENCES

[1] A.K. Agarwala, D. T. Shahani, and P. V. Indiresan. Report of the expert committee for evaluation of the upgraded electronic voting machine (EVM). Sept. 2006. http://www.scribd.com/doc/6794194/ Expert-Committee-Report-on-EVM, pages 2–20.

[2] R. Anderson and M. Kuhn. Tamper resistance: A cautionary note. In Proc. Second USENIX Workshop on Electronic Commerce, Oakland, CA, 1996.

[3] W. Appel. Certification of December 1, 2008. http://citp.princeton.edu/voting/advantage/ seals/ appel-dec08-certif.pdf.

[4] W. Appel, M. Ginsburg, H. Hursti, B. W. Kernighan, C. D. Richards, G. Tan, and P. Venetis. The New Jersey voting-machine lawsuit and the AVC Advantage DRE voting machine. In Proc. Electronic Voting Technology Workshop/Workshop on Trustworthy Elections (EVT/WOTE), Montr'eal, Canada, Aug. 2009.

[5] Aviv, P. Cerny', S. Clark, E. Cronin, G. Shah, M. Sherr, and M. Blaze. Security evaluation of ES&S voting machines and election management system. In Proc. USENIX/ACCURATE Electronic Voting Technology Workshop (EVT), San Jose, CA, July 2008.

[6] D. Bowen. “Top-to-Bottom” Review (TTBR) of voting machines certified for use in California. California Secretary of State, Aug. 2007.

[7] J. Brunner. Evaluation & Validation of Election-Related Equipment, Standards & Testing (EVEREST). Ohio Secretary of State, Dec. 2007.

[8] Bundesverfassungsgericht (German Constitutional Court). Judgment [...] 2 BvC 3/07, 2 BvC 4/07, official English translation. Mar. 3, 2009. http://www.bverfg.de/ entscheidungen/rs20090303 2bvc000307en.html.

[9] K. Butler, W. Enck, H. Hursti, S. McLaughlin, P. Traynor, and P. McDaniel. Systemic issues in the Hart InterCivic and Premier voting systems: Reflections on Project EVEREST. In Proc. EVT, San Jose, CA, July 2008.

[10] J. A. Calandrino, A. J. Feldman, J. A. Halderman, D. Wagner, H. Yu, and W. P. Zeller. Source code review of the Diebold voting system. Part of California TTBR, Aug. 2007.

[11] J. A. Calandrino, J. A. Halderman, and E. W. Felten. Machine-assisted election auditing. In Proc. EVT, Boston, MA, Aug. 2007.

[12] Castelluccia, A. Francillon, D. Perito, and C. Soriente. On the difficulty of software-based attestation of embedded devices. In Proc. 16th ACM Conference on Computer and Communications Security (CCS), Chicago, IL, pages 400–409, Nov. 2009.

[13] M. Chatterjee. Tribal voters in Jharkhand reckon with EVM technology. In Indo-Asian News Service, Nov. 20, 2009.

[14] Chaum. Secret-ballot receipts: True voter-verifiable elections. IEEE Security & Privacy, 2(1):38–47, Jan. 2004.

[15] Chaum, A. Essex, R. Carback, J. Clark, S. Popoveniuc, A. Sherman, and P. Vora. Scantegrity: End-to-end voter-verifiable optical-scan voting. In IEEE Security & Privacy, 6(3):40–46, May 2008.

[16] Chaum, P. Y. A. Ryan, and S. A. Schneider. A practical, voter-verifiable election scheme. University of Newcastle upon Tyne, Technical Report CS-TR-880, Dec. 2004.

[17] S. Checkoway, A. J. Feldman, B. Kantor, J. A. Halderman, E. W. Felten, and H. Shacham.

[18] Election Commission of India. Election laws. http://eci.nic.in/eci main/ElectoralLaws/electoral law.asp.

[19] Election Commission of India. Protocol for first level checking of EVMs before elections. Oct. 12, 2007. http://eci.nic.in/eci main/CurrentElections/ ECI Instructions/ins 121007g.pdf.

[20] Election Commission of India. Handbook for presiding officers. 2008. http://eci.nic.in/eci main/ElectoralLaws/ HandBooks/Handbook for Presiding Officers.pdf.

[21] Election Commission of India. Handbook for candidates. 2009. http://eci.nic.in/eci main/ElectoralLaws/HandBooks/ Handbook for Candidates.pdf.

[22] Election Commission of India. Handbook for returning officers. 2009. http://eci.nic.in/eci main/ElectoralLaws/ HandBooks/Handbook for Returning Officers.pdf.

[23] Election Commission of India. Schedule for general elections, 2009. Mar. 2009.

[24] Election Commission of India. Information under RTI on EVMs. July 2009. No. RTI/2009-EMS/39.

[25] Election Commission of India. Electronic voting machines– Regarding. Aug. 8, 2009. No. PN/ECI/41/2009.

[26] Election Commission of India. The Commission’s reply to Sh. V. V. Rao. Mar. 29, 2010. http://eci.nic.in/eci main/recent/reply sh.VVRao.pdf.

[27] J. Feldman, J. A. Halderman, and E. W. Felten. Security analysis of the Diebold AccuVote-TS voting machine. In Proc. EVT, Boston, MA, Aug. 2007.

[28] R. Kasarbada, P. V. Indiresan, and S. Sampath. Report of the expert committee for the technical evaluation of the electronic voting machine. Apr. 1990. http://www.scribd.com/doc/6794194/ Expert-Committee-Report-on-EVM, pages 21–37.