The Electronic Voting Machine in India

Zachary Macke

A term project for CS:4980:0004 Spring 2020, Electronic Voting at the University of Iowa

This version is intended for public distribution

"To hold democratic, free and fair elections in India is an amazing and a daunting task. In the 2014 elections, 66.4 % from total eligible electorate of 834,101,479 cast their vote". [1] With a voting body over two and a half times the population of the United States handling an Indian election in any means seems logistically impossible let alone holding one electronically. However, India, the world's largest democracy, manages to hold elections exclusively electronically and see an increase in voter turnout and vote legitimacy as a byproduct.

Pre-Electronic Voting Machines (EVMs)

The problem with holding fair and legitimate elections in India is the sheer size of their voting population. This voting population is not only the largest in the world, but a large section of this population falls into marginalized groups such as illiterate adults, handicapped, elderly, women, scheduled castes, and tribes. These individuals, making up a large subsection of the eligible voters were simply not accounted for and sometimes not able to cast their vote.

This time period was pre-1990 and all Indian elections were being done through a paper ballot system that was begging to be replaced. A general election of this magnitude required a magnitude of resources to hold. An estimated 8-10,000 tons of paper were required for ballot making and recording purposes which is roughly 200,000 trees every election. On top of paper, an estimated 400,000 phials of indelible ink had to be produced as well. After the physical action of voting had been completed, roughly 2.5 million "strong boxes" or safe boxes were used to store the votes under heavy security until they could be counted. [2] However, raw material was not the only problem with a paper ballot election in India. India also had many issues with election fraud in a more violent sense. "Under the paper ballot system, polling booths would often be captured, and ballot boxes would be stuffed, resulting in an unusually high voter turnout." [3] This action of capturing booths and stuffing the ballot boxes was known as “booth capturing” and it was a major problem in marginalized areas. Criminal organizations on behalf of a candidate or political party would violently capture a polling station and literally stuff the ballot box with little to no opposition. With all of these factors compounding the Election Commission of India (ECI) decided to make the move to electronic machines for voting. [4]

The Creation - Electronic Voting Machines

With a number of known problems to solve India legalized the electronic voting machine (EVM) in 1988. T.N. Seshan was the 10th chief election commissioner of India from the 12th of December 1990 until 11th December 1996. As the Chief Election Commissioner, he was looking for solutions to the various election related problems, so he developed India’s first Electronic Voting Machine. As Seshan’s main concern was reducing election fraud the EVM’s contained a few security features in an attempt to prevent various forms of election fraud which were centered around the device’s memory. It had a “close button” which would store and secure the votes that had been cast into permanent nonmodifiable memory. This feature was also adapted to fight tampering with the device; if the device was opened or tampered with it would disable to the ability to cast or accept any more votes to memory. The ECI was also thinking about the transparency of the electronic voting machines, “. . . they created a database of thumb impressions and electronic voting signatures which was made open for inspection by polling agents, volunteers, and also outside observers.” [5]

The adoption of these voting machines wasn’t immediate as they need to be tested before enduring the general election. The EVM’s first trial was approved in 1998 after years of debate and used in 25 Legislative Assembly constituencies spread across three states of Madhya Pradesh, Rajasthan and Delhi. After that it was expanded in 1999 to 45 Parliamentary Constituencies and in February 2000 to 45 Assembly Constituencies of the Haryana Assembly elections. [6] After a few more trials India’s EVM was ready for its first large scale test. That test came during the 2004 general election as they made the EVM the sole method for casting votes and nearly 1.1 million were deployed.

Modern Electronic Voting Machines

The electronic voting machine deployed in the 2004 general election is extremely similar to the electronic voting machines used today. This is because the technology used in the EVM is quite simple and unchanging. From an outsider's perspective this idea of simple technology used over a long period of time seems like a security and or integrity issue. However, the simplicity of the Indian EVM is most of the beauty of it as it seems to rid the system of complexity and issue.

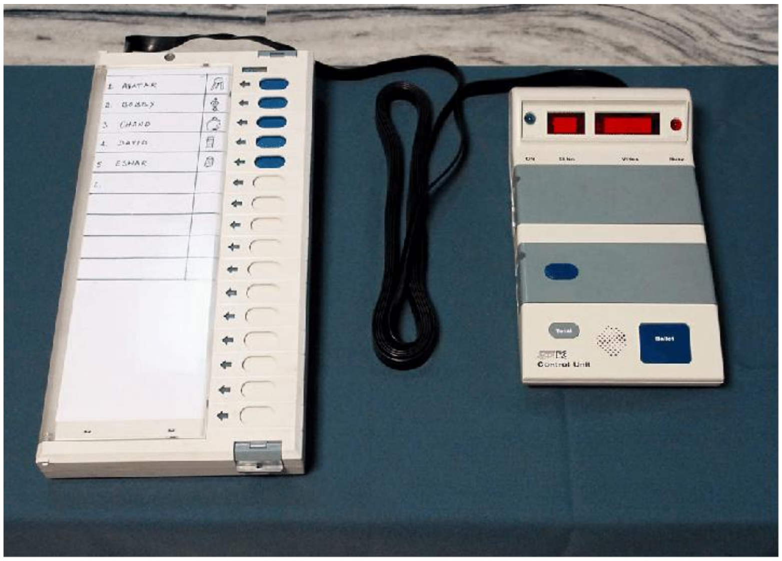

Figure 1.1, An Indian EVM, made up of a balloting unit (left) and control unit (right). [7]

The EVM runs on a normal battery as they do not require electricity. This seems somewhat odd for an EVM, but this is because of India's unique voting law and the rurality in some of the places where these devices travel. According to Indian voting law, "one should not have to travel more than 2 kilometers (about 1.25 miles) to vote" [8] meaning these machines, and their poll workers, must travel all over the country so everyone may have the opportunity cast their vote. On top of being extremely portable, they are very simple to operate and maintain.

There are two pieces to the EVM, a control unit and a balloting unit. These two are connected by a five-meter cable between the devices. [6] The balloting unit, is the ballot itself where individuals can mark their ballot and cast their vote. Here in the balloting unit is where a lot of accessibility work has been done to empower the marginalized voter. All candidates are arranged in alphabetical order and a corresponding symbol is placed next to each candidate's name. To cast your vote is as simple as pressing a button next to the name. This also keeps the vote anonymous as a polling worker can hold the control unit and stand over five meters away. Upon casting the vote, a gratifying long beep will be heard and there is reassurance that a vote has been made. If said voter is illiterate, the polling worker can explain the connection between each symbol and the candidate it stands for so they can still make an educated vote. [9] This symbol-oriented design is very important and an empowering innovation for India. The Atlantic states, "symbol-oriented design that makes voting more accessible to a country with 287 million illiterate adults and a multilingual electorate that speaks 22 officially-recognized languages and hundreds more unofficial ones." [10]

Each control unit can also hold 2000 votes at a time before the counts need to be tallied for said machine and the memory erased. Also, if either piece malfunctions, votes are stored in memory of the control unit until a replacement piece arrives making it easy to maintain. [9] They also have a built-in protection against the aforementioned "booth capturing" as they only register up to five votes per minute. All of this is available for only 10,500 rupees, which is roughly equivalent to $175 and is a massive price difference from the EVM's used in the United States and elsewhere. [10]

The final modification to the system came in 2012-2013 when the two-part system became a three-part one. One major problem with the dual part system was that it was too closed. There was very little to no auditability of the EVM and that led to major trust issues with politicians, especially loosing ones. So, between 2012-2013 the Voter Verifiable Paper Audit Trail (VVPAT) was added to the system to increase its auditability. What the VVPAT does is simple. Upon casting a vote, it helps the user easily verify whom they voted for by printing a small slip of paper containing a serial number, name, and symbol of the candidate whom the vote was cast for. This small slip of paper is present through a small screen for seven seconds and after it falls into a sealed box for auditing purposes. [3] One potential problem with this system is the violation of a "secret ballot" which could cause issues for individuals right to an anonymous vote. These audits aren't done for 100% of the total vote count though as no audit can be 100% done for a population of that size. On April 9th, 2019 the Supreme Court of India made it mandatory to include the VVPAT with all EVMs. However, the audit percentage only fell around 2% of EVMs, “i.e., 5 polling stations per constituency before certifying the final results.” [3]

Safety of Electronic Voting Machines

Device safety and security are some of the most important things when evaluating a voting machine. The Indian government has taken security quite seriously in regard to their machines and they own both companies federally which produce the EVMs. On top of this they are extremely confident in the devices’ ability to deter fraud. The ECI is on record many times touting the security of their devices stating that to intervene in the election through the EVM one would need quite high technical skills to tamper. However, tampering with one would require access to the physical device which are stored under strict security and can be monitored by a candidate and or their agents at all times, claiming it is impossible to gain physical access to a machine. [11] Also, because they only hold up to 2000 votes one would need hundreds to thousands of the millions of machines to make a difference in elections of such magnitude.

One of the two government manufactures, the Electronic Corporation of India Limited, has further touted the safety of their product. On more than one account they’ve stated their manufactured EVMs and VVPATs are “un-hackable and tamperproof”. These aren’t just open-ended claims. The company stated, “programming is done at a secure manufacturing facility and not with chip manufactures”. Apart from the chip manufacturing the former Chairman Managing Director (CMD) of the ECIL said, “EVMs are standalone machines and are not connected to any network. The machine has no internet interface, so the question of hacking externally doesn't arise” at the Institute of Electronic and Telecommunications Engineers in Hyderabad. [12]

Though these claims are strong, they have stood up to the test of time and finding evidence of election fraud at the fault of the device is rare. Most notably, in the 2014 general election there were claims against the integrity of the machine but ultimately, they did not hold up in court. However, these claims aren’t new. The machines have withstood seven court appearances and each time claims that the machines were insecure fell. [13] A study was done by the Brookings Institute to investigate the impact of the machines on fraud and democracy in 2017. They found that the EVM had an inverse effect on fraud compared to the traditional paper balloting system. Along with a decrease in fraud as a whole they found that the EVM was strengthening the weaker, marginalized groups mentioned earlier as it provided them a fair and safe opportunity to cast their vote. [14]

Because these claims of legitimacy and security come from the government, who are the sole manufactures of the devices, it is hard to fully trust their claims. An analysis of device security has been done by the Individuals at the University of Michigan and Hyderabad. They were performing these tests for many reasons. First, was the lack of official audits done on the EVM; they note, “It is difficult to assess the credibility of these charges [election irregularities], since there has apparently never been a prosecution related to EVM fraud, and there has never been a post-election audit to attempt to understand the causes.” Second, there was reports in the 2009 parliamentary election of EVM malfunction, specifically when a voter would press a button for a specific candidate, the light would blink for a separate candidate. This signaled that the voter had cast the vote for the wrong candidate, one that was not their choice, and no action was taken. [15]

In their vulnerability analysis they found ways that a possible attacker could manipulate the EVM in malicious ways, which directly counter the claims of security and safety made by the Indian government. There were five methods [15] of attack mentioned:

1. Tampering with Software before CPU Manufacture
    a. Because the EVM firmware is stored in ROM inside the microcontroller chips, there was no way of extracting and verifying the contents. This tampering is made possible as the software integrated onto the CPU is done by an outside entity, a Japanese Company, Renesas.
2. Substituting a Look-Alike CPU
    a. Once the software is integrated with the CPU it is then shipped to the Indian chip manufacturer which leaves the possibility of shipping a fraudulent CPU to said manufacturer which presents a hole in security.

3. Substituting Look-Alike Circuit Boards
    a. Swapping a CPU on an already manufactured board would be a challenge as it requires soldering, and when there are over a million EVM's this is not feasible. However, one could manufacture a "dishonest board" and make a complete swap. This is possible due to the simplicity of the EVM's board.
4. Substituting Look-Alike Units
    a. They mention, "Voters and poll workers have no practical way to verify that the EVMs they use are authentic." Meaning, it would be practical to make a complete swap of the EVM itself for a replica which could act maliciously.
5. Tampering with Machine State
    a. It is possible to attach hardware to the EVM's circuit board and then directly read and write the EEPROM chips that record votes.

The group concluded, "Despite elaborate safeguards, India's EVMs are vulnerable to serious attacks. Dishonest insiders or criminals with physical access to the machines can insert malicious hardware that can steal votes for the lifetime of the machines." This conclusion was shocking as the Indian government speaks so highly of the devices. These claims of vulnerability are also not out of reach for attackers with malicious intent. On top of this, what is most concerning is the government will not hear claims fraud as they would like to believe they have constructed the perfect machine to conduct electronic voting.

Summary

In conclusion, the Indian EVM is not only an astonishing, simple piece of hardware, but it is a piece of technology that is empowering an entire class of individuals which had lost their democratic right to vote. The Indian EVM also does this for only a fraction the cost of other modern voting machines. It has done this while claiming an amazing track record of security and reliability which makes it, what I believe, the best version of an EVM we have seen. However, this track record of security and reliability seem hollow as they are not open to investigating claims of fraud or attack. If one is to believe the touts of security and reliability, then the Indian EVM does its job consistently and very well. This is sometimes all that is required within technology to create innovation. However, I believe the EVM could be much more secure and stand as a much stronger figurehead for electronic voting machines if government was more willing to accept possibilities of vulnerability and fraud. Regardless, the story of India's EVM is one that can serve as strong foundation for the future of electronic voting technology and governments can look to it as a starting point in developing their own.

Sources

[1] Herstatt M., Herstatt C. (2017) India’s Electronic Voting Machines: Social Construction of a Controversy Surrounding a Frugal Innovation. In: Herstatt C., Tiwari R. (eds) Lead Market India. India Studies in Business and Economics. Springer, Cham

[2] Kumar, S., & Walia, E. (2011). Analysis of Electronic Voting System in Various Countries. International Journal on Computer Science and Engineering, 3(5), 1825–1830.

[3] Ravi, S. (2019, December 05). How electronic voting machines have improved India's democracy. https://www.brookings.edu/blog/techtank/2019/12/06/how-electronic-voting-machines-have-improved-indias-democracy/

[4] Arvind Verma (2009), "Situational Prevention and Elections in India", International Journal of Criminal Justice Sciences, Pp. 86–89.

[5] Somanathan, M. (2019, May 02). India's electoral democracy: How EVMs curb electoral fraud. https://www.brookings.edu/blog/up-front/2019/04/05/indias-electoral-democracy-how-evms-curb-electoral-fraud/

[6] History of EVM. (n.d.). https://eci.gov.in/voter/history-of-evm/

[7] Herstatt, Maximilian & Herstatt, Cornelius. (2014). India’s Electronic Voting Machines (EVMs): Social construction of a "frugal" innovation.

[8] Frayer, L., & Khan, F. (2019, April 11). Polls Open In The World's Largest Democracy: Fun Facts On India's Election. https://www.npr.org/2019/04/11/712107668/polls-have-opened-in-the-worlds-largest-democracy-fun-facts-on-india-s-election

[9] Online, E. (2020, February 03). What are EVM's? https://economictimes.indiatimes.com/news/elections/lok-sabha/india/what-are-evms/articleshow/68807699.cms?from=mdr

[10] Ford, M. (2014, June 16). Indian Democracy Runs on Briefcase-Sized Voting Machines. https://www.theatlantic.com/international/archive/2014/04/indian-democracy-runs-on-briefcase-sized-voting-machines/360554/

[11] Lakshman, N. (2016, December 14). Hot debate over Electronic Voting Machines. https://www.thehindu.com/news/international/Hot-debate-over-Electronic-Voting-Machines/article16126892.ece

[12] Reddy, S., & Tnn. (n.d.). EVMs foolproof, can't be tampered with, says former ECIL chairman: Hyderabad News - Times of India.

https://timesofindia.indiatimes.com/city/hyderabad/evms-foolproof-cant-be-tampered-with-says-former-ecil-chairman/articleshow/69125520.cms

[13] Biswas, S. (2019, January 25). India election 2019: Are fears of a mass hack credible? https://www.bbc.com/news/world-asia-india-46987319

[14] Debnath, S., Kapoor, M., & Ravi, S. (2017). The Impact of Electronic Voting Machines on Electoral Frauds, Democracy, and Development. SSRN Electronic Journal. doi:10.2139/ssrn.3041197

[15] Scott Wolchok, Eric Wustrow, J. Alex Halderman, Hari K. Prasad, Arun Kankipati, Sai Krishna Sakhamuri, Vasavya Yagati, and Rop Gonggrijp. 2010. Security analysis of India's electronic voting machines. In Proceedings of the 17th ACM conference on Computer and communications security (CCS '10). Association for Computing Machinery, New York, NY, USA, 1–14. DOI:https://doi.org/10.1145/1866307.1866309