NIAS/CSS/ISSSP/U/RP/068/2019

THE SAFETY OF DIGITAL DEMOCRACY

Abhishek Sunil
P.M. Soundar Rajan

March 2019

National Institute of Advanced Studies
Indian Institute of Science Campus
Bangalore-560012

Executive Summary

One of the challenges prevailing in the present world is securing the safety of digital democracy. It is of utmost importance to carry out a free and fair election. In a diversified country like India, carrying out election has always been a difficult task. Like every election process in the world, Indian elections have also been under many threats such as physical tampering of the ballot box, booth capturing, etc. The emergence of technology in the election procedure has eradicated these threats. The credit of incorporating technology into Indian election process goes to the electronic voting machine of the country. The Indian voting machines are direct recording electronic voting machines with electromechanical buttons for voters and are non-networked, leaving little option for hacking. The EVM has been augmented with the voter verified paper Audit trail (VVPAT). However, the use of technology in the election process has introduced some other cyber vulnerabilities to the machine. When the concept of safety in the Indian democratic process emerge, the entire nation question the safety of electronic voting machine leaving aside the actual threats caused by fake news, information warfare, social botnets and big data. The fake news, social botnets, big data and information warfare manipulates the thought process of the voters or confuse them. There are theories in social psychology that explains, why the above threats can badly manipulate the decision making process of the voters, than tampering with internal state of machine.

The study shows that the accusations that the EVM being tampered are not valid. The casting of vote through Indian electronic voting machine is quiet safe and moving back to the ballot paper voting system is not a feasible idea to uphold the essence of free and fair election.

The safety of Digital Democracy

Abhishek Sunil[1]*, Prof. P.M Soundar Rajan*[2]

Key words: *Election process, Indian electronic voting machine, VVPAT, Cyber-threats to the machine, Administrative policy of Indian election, Fake news, Social botnets, Disinformation and Propaganda***,** *Heuristic processing ,Peripheral route to persuasion*

Introduction

In the contemporary world, technology has been incorporated into democratic process and system known as digital democracy or e-democracy.[3]This present world has been hit by digitalization, from registering a voter to casting a vote in the election booth. The best examples to be mentioned for the digitally democratic countries are India, USA, Brazil etc. Amalgamating the technology to the election process has reduced physical tampering of the ballot boxes and other physical threats. But this same technology has increased vulnerability of the election process to cyber-attacks. The mixing of technology to election process should be credited to the electronic voting machines(EVM). There are two kinds of EVMs across the globe, direct recording electronic voting machines (DR-EVM) and those electronic voting machines using optical scanners. When the voter presses a button on the DR-EVM his/her vote is recorded electronically in the machine's memory. EVMs used in countries like India, Venezuela and Brazil falls in this category. Whereas in the other type a voter marks his preference on a paper ballot which is then optically scanned by the machine and the counting is done electronically. Recording of votes in the DR-EVM is carried out through an electro-mechanical button or through a touch screen. These systems can be stand-alone or networked. Machines which are networked can transmit the recorded results to a central server. These results are then compiled quickly and displayed on a central website. Indian voting machines are direct recording electronic voting machines with electromechanical buttons for voters and are non-networked. Counting is carried out separately by each machine and the results are then

---

[1] Abhishek Sunil is a graduate in Bachelor of science in Physics, Mathematics, Electronics and currently pursuing his MA international studies from Christ (Deemed to be) University, Bengaluru.

[2]Prof. P.M Soundar Rajan is a visiting professor at international Strategic and Security Studies Programme, National Institute of Advanced Studies and formerly outstanding Scientist and Director, Defense Avionics Research Establishment.

[3] 'Defending Digital Democracy', *Belfer Center for Science and International Affairs,* n.d., https://www.belfercenter.org/project/defending-digital-democracy

compiled manually.[4]Despite all these advantages, EVMs and election process are still vulnerable.

This paper is divided into three parts, the first part talks about the possible threats to the voting machine in genral. The threats to machine mentioned in the article are considered to be the possible attacks. The reason why these attacks fall into this category is that machine can be tampered but these tampering can be performed only in labs. When it comes to the real election these kinds of attacks aren't possible due to many factors, that are discussed in the paper. The subsequent part focuses on the actual threat to the election such as fake news, social botnet, disinformation warfare and big data as a weapon. The integrity of the machine is always questioned when the safety of the democratic process is in doubt. The critics in India have questioned only the safety of the EVM, ignoring the actual threats. The rigging of the election process need not necessarily carried out by tampering the machine, it is always the actual threats, explained later in this paper, which spoiled the essence of free and fair election. The last part focus on how these actual attacks are preferred dominant over tampering of the machine. It is found that the actual attacks have worked badly in manipulating the votes than tampering of the machine, which is never recorded.

Indian electronic voting machines.

The election machinery body of India developed the country's EVMs in partnership with two government-owned companies Electronics Corporation of India Limited(ECIL) and Bharat Electronics Limited(BEL). There are three different generations of EVMs working in the election process.[5]

The electronic voting machines operate on a 7.5 volts battery. Its claimed to be tamperproof, error-free and easy to operate. Indian EVMs have four parts: a control unit, control unit display board, ballot unit and communication between ballot unit and control unit. There is a space assigned for display. In this space, contesting candidates name and symbols allotted to them can be placed. A sepia brown colored button is provided against the name of each candidate. By pressing this button, the voter can record his vote in favor of the candidate of his choice. Alongside of the said button, there is also a lamp for each candidate. This lamp will glow red

[4]S.Y. QURAISHI, An undocumented wonder: the making of the great Indian election, Use of technology in Indian election, New Delhi, Rupa publications India PVT ltd, 2014, p. 193-194.
[5] Status Paper on EVM: The journey of EVM in India,3rd Edition, New Delhi, 2018, p. 5-6,

when the vote is recorded. Simultaneously, a beep sound will also be heard. One ballot unit caters up to fifteen candidates. One control unit can record the votes polled for a maximum of 60 candidates. On the topmost portion of the control unit, there is a provision for displaying various information and data recorded in the machine, like the number of contesting candidates, the total number of votes polled, votes polled for each candidate etc. are recorded. This portion is called, the display section of the control unit.[6]

Possible Attacks

EVMs are found vulnerable to cyber threats and tampering of the machine. The following are the kinds of attack that can be done in an EVM which have been proven by a group scientist - Scott Wolchok, Eric Wustrow, J. Alex Halderman, Hari K. Prasad, Arun Kankipati, Sai Krishna Sakhamuri, Vasavya Yagati, Ron gonngrijp.[7]

1. ***Tampering with the software before CPU manufacture***

Extracting the firmware of an EVM or verifying its integrity is not possible as it is stored in the masked read-only memory, inside the microcontroller chips. This creates a difficulty in detecting if the software gets manipulated before it is placed into the CPUs. The CPU manufacturing is done by a Japanese company, Renesas. This company integrates the software into the CPU. The attack can be carried out only if the employer/employee or the company itself can be compromised. The employer of the company can replace a version consisting of a back door with less chance of being noticed.

2. ***Substituting a look-alike CPU***

This type of attack can be done when CPUs gets shipped to India for assembling into the control unit main board. Attackers will try to substitute a look-alike CPUs containing software that counts the votes dishonestly. The counterfeit chips are swapped from the real ones in the supply chain or by attackers with access to the assembled machines. These swapping can be done earlier to the assembly by corrupt employees or the courier which transport this. These attack

---

[6] Comprehensive Manual for Multi Post Electronic Voting Machines(Used in Rural Areas):Chapter-1, Kerala, State Election Commission, 2017, p.1-2.

[7] Scott Wolchok, et al., 'Security Analysis of India's Electronic Voting Machines', 17th ACM Conference on Computer and Communications Security (CCS '10), Illinois, Association For Computing Machinery, 2010, p.6-8

can also take place on the programmable logic devices in the ballot unit. The attacker can construct a look-alike chip consisting both a radio frequency receiver and a processor.

3. Substituting look-alike circuit boards

Swapping of a dishonest CPU with the real one is difficult as it needs desoldering and replacing the surface mounted chips. This difficulty can be overcome by replacing the entire mainboard with a dishonest one to manipulate the votes. Making a new board is found to be easy because of its simple design and functions. This procedure needs opening the control unit, exchanging out the snap-fitted board, and rewiring the cable to the display unit.

The vulnerability is that the system treats its components as trusted components. The attacker can manipulate the votes by replacing the circuit board in the ballot unit which dishonestly responds to the key presses or by replacing the display board in the control unit.

4. Substituting look-alike units

The problem with the Indian EVMs is that there is no practical way to verify whether the EVMs used are authentic or not. This lacking feature indeed helps the attacker to build identical looking but dishonest control units or ballot units and substitute them before the elections.

The same vulnerability mentioned in the above sub-section is a main threat to the EVM. The machine trusts the connection between the components. The attacker can perform the action by inserting a device between the ballot unit and control unit. By this, the attacker would be able to successfully intercept the key press signals and replace the votes.

5. Dishonest display attack

In this method, the real display board is replaced with a dishonest display board. In an election process, the votes received by each candidate is shown on the display board. A hidden microcontroller is placed under a dishonest display board that intercepts the vote total and substitute a fraudulent result. The dishonest display detects electrical signal from the control units when the EVM tries to display the election result, this controls the 7-segment led digits. The received information is used by the display unit to manipulate the real overall number of votes. In the last stage of this attack, it calculates and shows plausible but fraudulent vote counts for each candidate. To complete this process, attackers must communicate with the EVM to favor chosen candidate with predetermined margin in the election process. The communication signal is sent through many different ways such as Bluetooth.

6. Clip on memory manipulator attack

Dishonest display attack is done by replacing the real hardware unit with a dishonest look-alike component whereas clip on memory manipulator attack includes only the temporary application of new hardware. This device clips directly to the EEROM memory chips which are responsible for recording the votes inside the EVM. This attack provides two ways to manipulate the vote: stealing the vote and violating the ballot secrecy.

The real EVM is designed in a way, ballot stuffing is limited by the time constraint feature that takes twelve seconds to place a vote from the preceding votes, so in a minute, only five votes can be placed not more than that. But the clip on memory manipulator hardware bypasses this time constraint restriction, so the attacker could stuff the electronic ballot box with any number of votes. In India, sometimes counting of votes is done weeks after voting. so this attack can be done when EVMs are kept at safe rooms.

This hardware has a rotatory switch that selects the number from 0 to 9 and the attacker can use it to pick a favored candidate in any of the first nine ballot position. This way an attacker can steal the vote. When the switch is placed to positions 1–9, the clip-on device executes a vote-stealing program. The program runs in two phases: first, it reads the vote data and calculates how many votes to steal from each candidate; second, it rewrites the list of votes, stealing votes as calculated in the first phase. The stealing of votes takes only milliseconds per vote hence the entire attack can be done in several seconds.

Why these are the possible attacks?

The attacks mentioned above are possible but is not going to happen in the coming years as the election commission of India has laid down a strong administrative policy to tackle these threats. All these manipulation can be done if a huge number of employees get corrupted or the shipment company gets compromised. As the EVMs of India are stand alone and non-networked system, this feature eliminates the centralised hacking of the machine. The EVMs are randomised before transportation to the polling booths. The success rate of the these attacks are very less as the attacks need huge amount of investments and cannot be carried out in a large scale. As a reason attackers would prefer the other kinds of attack which manipulates the thought process of the voters and this method avoids the chance of getting caught and can be done easily. These attacks will be explained in the later sections of this paper.

The introduction of voter verified paper Audit trail(VVPAT) has further minimised chance of tampering the machine. VVPAT is a method that displays the feedback to the voters. It is an independent verification printer machine, which is connected to the electronic voting machine. It allows voters to verify whether their vote has gone to intended candidate. The machine works when the voter presses the button in the ballot unit. The ballot unit sends the signal to the VVPAT machine to print a paper slip. The printed paper slip consists of the name and symbol of the candidate, which voter has voted. It allows the voter to verify his/her choice. After displaying to the voter from a glass case in the VVPAT for seven seconds, the printed ballot slip will be cut and dropped into the drop box in the VVPAT machine and a beep sound is heard. VVPAT machine can be accessed only by the polling officers. This machine helps the voter to detect if the EVM is tampered.[8]

Administrative security

A strong administrative security to an extent can tackle cyber space vulnerabilities. The commission has clearly drafted the procedural checks and balances aimed at preventing any manipulation of EVM.

EVMs are always stored in a secure room and guarded twenty four hours by the armed police. A prior notice is given to the political parties to be present while unlocking the secure room. Soon after unlocking the store rooms EVMs undergo rigours checking of which First Level checking (FLC) of the EVM is carried out by BEL and ECIL. FLC is done transparently in the presence of representatives of the political parties and the entire process of the checking is video graphed. In the process of FLC a mock polling is carried out and the sequential print out of the result is produced to representatives of the political parties. To avoid the further manipulation of the machines before the election, the EVMs are randomized twice using a computer software, first for the allocation of machines to assembly constituencies and second to polling stations in the presence of candidates or their representatives before they are distributed for use in individual polling stations. The randomization is carried out through EVM Tracking Software (ETS) by the DEO in the presence of the representatives of political parties/candidates and Central Observers deputed by the ECI for complete transparency. The lists of EVM containing the serial number of EVM allocated to a particular polling station are

[8] The Hindu Net Desk , 'All you need to know about VVPAT', The Hindu, 17 April 2017, https://www.thehindu.com/news/national/all-you-need-to-know-about-vvpat/article18077550.ece

provided to the political parties/candidates. The next step involved is candidate set, its done in the front of the candidates or their representative and in the front of the commission observer. Again a mock poll is conducted after the candidate setting. At the time of candidate set various compartments are sealed using multi-level threading as :

I. Thread seal is provided to the candidate set and power pack section of the control unit ,after the setting of contesting candidates and installing the battery respectively.
II. After fixing the ballot paper thread level seal for the ballot paper screen of the ballot unit.
III. Two thread seals for ballot paper cover of the balloting unit.

The second process of randomization of the control unit and ballot unit is done by the returning officers after the multi-level thread sealing. Later these control unit and ballot unit are stored in the secure room in the presence of the candidates or their representative and the commission's observer. The reopening of the strong room is again done in the presence of the candidates or their representative and the commission's observer on the day when polling parties are dispatched to their respective polling stations. Once again a mock poll is carried out on the actual poll day by presiding officer in the presence of candidates or their authorized agents. The presiding officer after the mock election seals the result section/ bottom compartment of the control units, green paper seal for the result section and thread level seal for inner door of the result section, bottom compartment and for the connector box for the cascading ballot unit. After the actual poll, the EVMs are sealed with paper seals and packed plastic boxes and the EVMs are stored, locked and sealed in the strong room in the presence of the candidates or the representatives. These representatives are allowed to guard the strong room till the counting begins. These rooms are under the surveillance of the police and CCTV. These rooms are opened only in the presence of respective people.[9]

The actual threat

The previous section of the paper focused on various methods of manipulation of the election using EVM. But in practicality this kind of attack isn't going to be successful. The deciding factor of any attack on the election to be successful, is the reach and the output of the attack.

[9] Status Paper on EVM: The journey of EVM in India,3rd Edition, New Delhi, 2018, p.17-18.

Attacking of EVM cannot be done in a large scale. So as a reason a favourable output can't be determined. Recent trends of attacks in political warfare are fake news, information warfare, hacking electoral web page. These attacks don't manipulate the input of the machine. It manipulates the thoughts of voters and the trust in a candidate.

Cyber-attacks and disinformation campaigns have become tools of yesterday's game. The present world have technological advances in artificial intelligence, automation and machine learning, combined with growing availability of big data have set a new platform for sophisticated, inexpensive and highly impactful political warfare.[10] There are serval attacks belonging to this categories but this paper focuses mainly on the fake news, social botnets, disinformation and propaganda, and big data.

Recent trends of attacks in political warfare

1. Fake News

Fake news is defined as that news article that are deliberately and verifiably false and would mislead readers. These kind of news are distorted signals uncorrelated with the truth. Fake news are produced in the market because it is cheaper to provide than the authentic signals because consumers cannot verify the authenticity of the distorted signals and these consumers enjoy the partisan news and they create "echo chambers" or "filter bubbles" where they would be insulated from contrary perspectives. Fake news may generate utility for some consumers, but it also imposes private and social costs by making it more difficult for consumers to infer the true state of the world-for example, by making it more difficult for voters to infer which electoral candidate they prefer.[11] A recent study from the Ohio state university " Fake news may have contributed to Trump's 2016 victory", according to the report fake news had substantial impact on the voting decisions of a strategically important set voters during the 2016 U.S election.[12]

---

[10] Alina Polyakova and P Spencer Boyer, ' The future of political warfare: Russia, the west Asia and the coming age of global digital competition', *The New Geopolitics, 2018, 10.*

[11] Allcott Hunt and Gentzkow Matthew, 'Social media and fake news in the 2016 election', *The journal of economic perspectives*, 2017, 212.

[12] Richard Gunther, A Paul Beck and C Erik Nisbet,' fake news may have contributed to trump's 2016 victory', *ohio state university*, 2018.

The reason for fake news gaining importance is weak barrier to entry in the media industry and ease in setting up of a website. This web content can easily monetized through advertising platform. Fake news cannot completely convince the voters but it can confuse the voters.

2. Social botnets

A botnet is a network of internet-connected devices, which may include PCs, servers, mobile devices that are intentionally infected with a common type of malware by cyber criminals to perform automated tasks on the internet without the actual knowledge of the users.[1314] These social botnets automatically run accounts on social media. The usage of botnets was noticed during the US presidential election. One of the five tweets regarding the presidential election was posted by Twitter botnets. The Elections in Europe are another victim which saw the usage of botnets, these botnets retweeted or shared news on social media. Social botnets are used as an amplifiers for fake news, disinformation created by the media outlets. The social botnets enhance the visibility of stories and indirectly make certain groups popular on social media by inflating follower number.[15]

3. Disinformation and Propaganda

Disinformation and propaganda are tactics that created an impact on election outcomes. These tactics are not new, but carrying out these techniques through the internet came into existence since past few years. These are used to spread the false information of their opponents using internet fora and social media in order to shape public opinion. The technique is utilised by creators of fake news, by taking a complex case, remove some important facts, transform the whole story and then promote it under an attention-grabbing headline. The spread of news around the social media is done by social bots and amplifiers.[16]

---

[13] Margaret Rouse, *Search Security,* n.d., https://searchsecurity.techtarget.com/definition/botnet
[14] *Get Safe Online*, n.d., https://www.getsafeonline.org/online-safety-and-security/what-are-botnets/
[15] Marie Baezner and Patrice Robinn, 'Hotspot Analysis: Cyber and Information Warfare in elections in Europe', *ETH Zürich* , 2017, p.08.
[16] Marie Baezner and Patrice Robinn, 'Hotspot Analysis: Cyber and Information Warfare in elections in Europe', *ETH Zürich* , 2017, p.08.

4. Big data as a weapon

Big data is an evolving term that describes a large volume of structured, semi-structured, unstructured data that has the potential to be mined for information and used in machine learning projects and other advanced analytics applications.[17]

The threats hidden in the data collection are broader than social media sector. The entire industry of data brokers has emerged to meet growing demand by collecting and selling individual's personal data. The big data miners assemble information from public records, web browsing histories, online purchases and other web sources. They use this information to analyse the individual's taste, political attitude and other personal attributes. The information compiled is very valuable to the political campaigners, to attract the votes, to create echo chambers and filter-bubbles. The big data helps the fake news and political advertisements to reach the specified interest groups, thus, by limiting the reach of any contrary information. In recent times, Artificial Intelligence(AI) and Big Data technology used by the companies decide which content and advertisements to appear on user's display screen- search results, news feed and timelines. Social media companies can manipulate their algorithms for disinformation campaigns to reach the users effectively.

This kind of tool was used in the campaign of U.S- 2016 election. A firm, Cambridge Analytica has claimed to create personal profiles on two hundred million Americans. The company excavated the individual's data to micro-target in the 2016 United States election. The same pattern was found in the United Kingdom during the Brexit referendum.[18]

Why do the above mention attacks work better?

There are theories in social psychology that substantiate why the above mentioned attacks are efficient in manipulating the decision process of the voters. One such theory is heuristic processing and the other one is peripheral route to persuasion which explains why the readers believe the fake news, disinformation and propaganda to be factually true. Both the theories claim that the brain forms mental shortcuts such as "expert's statement need to be trusted" , the idea that "if it makes me feel good, I am in favour of it", to process the information. The fake

---

[17] Margaret Rouse, Bridget Botelho and Stephen J Bigelow, 'Big Data', *Search data management*, November 2018, https://searchdatamanagement.techtarget.com/definition/big-data,

[18] Alina Polyakova and P Spencer Boyer, ' The future of political warfare: Russia, the west Asia and the coming age of global digital competition', *The New Geopolitics,* 2018, p .10

news are structured in a manner that the piece of information is from an expert source, making the reader to presume the information to be factually true. Social botnet and bigdata helps the disinformation and propaganda to form a filter bubble or an echo chamber on the user, by providing only those information which makes the user to feel good , so the user automatically is in favour of it. Another strategy used by the cyber criminals is to make the people to believe that the information is from a valid source. In this strategy, the people process the information as valid even though it is factually wrong.

Heuristic processing and peripheral route to persuasion explain this type of processing works when we lack the ability or capacity to process the information more carefully or when the motivation to perform cognitive work is low. This is why persuasion of the reader becomes easy.[19]

The tactics and tools like fake news, social botnets, disinformation and propaganda don't work individually. It always works together to achieve the main objective. These techniques provide a sheer volume of information to the voters which make them difficult to focus on. Big data and artificial intelligence badly assist these tactics to work. These allow them for micro-targeting of communication so that the processed data what people receive, is limited to a filter bubble of the like-minded. [20]

In a technologically advanced world, most of the population depend heavily on the internet as a source of news. A survey by Hunt Allcott and Matthew Gentzkow claims that 14 percent of American adults viewed social media as their most important source of election news[21]. They don't question the authenticity of the news, suspect that is from an incredible source and conclude the received information to be factually true. The acceptance of the news psychologically enables them to re-transmit with the rest of the population, so that the friends, family, group of people are up to date with present news. This action makes furthermore readers believe the news is from a reliable source, due to the fact that it has been shared by many.

---

[19] Robert A Baron and Nyla R Branscombe, *Social Psychology*: *The Cognitive Process Underlying Persuasion,* South Asia, Pearson India Education Services Pvt Ltd, 2015, p.158.

[20] Joseph S. Nye, 'Is fake news here to stay ?', *Project Syndicate*, December 2018, https://www.project-syndicate.org/commentary/fake-news-part-of-the-background-by-joseph-s--nye-2018-12

[21] Allcott Hunt and Gentzkow Matthew, 'Social media and fake news in the 2016 election', The journal of economic perspectives, 2017, 212

The noxious of the above-mentioned attack is that the victim don't realise it has been infected and can't hold these attackers responsible for the infection. The reason why these attacks aren't visible is because it doesn't alter the internal state of the machine, only infects the decision process of voters. Contaminated information doesn't necessarily persuade the voters but it can make the decision making complex .

The allegations made by many political parties regarding the hacking of EVM could have been true had there been a strong administrative policy not in existence. Hijacking and hacking of few machines are possible, but it cannot be carried out on a large scale as there are millions of EVM in India. These factors make Indian EVM to be the safest machine to carry out a free and fair election.

Indian EVMs are found to be superior to other EVM models in the world. Even though being superior in the model it is still vulnerable to attacks. If the election commission of India improves the security of EVM a little then there will be no doubt regarding the fairness of the democratic process. It is not the EVMs rather it is the actual threat mentioned above which is creating havoc in the democratic process. The election commission of India should work with social media companies to arrive at a proper timely solution to prevent the democratic system getting poisoned.

Conclusion.

There are claims by Indian political leaders to move back to the ancient technique of voting system known as ballot paper system. The ballot paper system has more threats and vulnerabilities in conducting an election efficiently. The return of the ballot paper system brings back the threat like booth capturing, ballot stuffing etc. In order to avert these threats and to carry out a free and fair election, using of the Indian electronic voting machine is the optimal option.

The strong administrative and technical security makes the Indian EVM and election process to be superior and safer. The Indian voting machines are direct recording electronic voting machines with electromechanical buttons for voters and are non-networked, leaving little option for hacking. The last resort of attack on the machine is, tampering of the internal state of the EVM. This is strongly countered by the administrative policy of the election. Getting back to the ballot paper system is not a feasible and sensible idea.

There exist, a higher threat which lies in the election campaign process, the manipulation of the decision processing of the voter. The election commission and respective authorities should arrive on immediate countermeasures to tackle the actual threats mentioned in the paper. Free and Fair elections are a prerequisite for an increasingly for any democracy.