

Cyber Security Challenges for General Election in India

Author: Arun M. Ranvir

Affiliation: Scientist-F and Senior Director (IT)

NIC, MEITY, Amravati IN

E-mail: am.ranvir@nic.in

DOI: 10.26821/IJSHRE.10.12.2022.101208

ABSTRACT

Indian Constitution gives rights to the citizens for representation in house of people by means of Elections. Now a day's Digital Technologies are playing major role in conducting Elections in India. Securing Data and Information have become one of the biggest challenges and Cyber Security plays an important role in the field of Information and Communication Technology. The use of Digital Technologies needs to solve Security challenges associated with protecting Election Infrastructure. This paper presents various Cyber Security challenges encountered in Elections and appropriate measures to be deployed to overcome these Cyber security issues for conducting free and fair Elections during the entire Election process from Voter registration to Result declaration, etc.

Keywords: ECI, EVM, ICT, Cyber Security, Election, Data, Information, Digital, Systems, Framework

1. INTRODUCTION

India is the largest democratic country in the world, in democracy Government runs by the people for the people as per Direction and Control of Indian Constitution. As per the Indian Constitution voting is the fundamental right of all citizens over the age of eighteen years. Indian Constitution consists of Articles 324 that provides the power of superintendence, direction and control of Elections to Parliament, State legislatures, the office of President of India and the office of Vice-President of India shall be vested in the Election

Commission. The Election Commission prepares, maintains and periodically updates the Electoral Rolls, Organize the polling booths where voting takes place, counting of votes and the declaration of results [1]. Election Commission of India focuses more on use of Digital Technology in Election Process. These Technologies are now playing a major role in Conducting General Election in India. Digital Technology is being used in conducting Elections for decades for Electronic voting machines, Voters online Registration, the explosion of these new Technologies and increasing access to citizens and election machinery creates some issues of Cyber Security.

Internet is the fastest growing infrastructure in the world today and we are unable to safeguard our information so Cyber crimes are increasing day by day. Now a day Securing Data and Information have become one of the biggest challenges and Cyber Security plays an important role in the field of Information and Communication Technology. The act of protecting ICT systems and their contents has come to be known as Cyber Security. Cyber security can be an important tool in protecting privacy and preventing unauthorized surveillance and information sharing and intelligence gathering can be useful tools for effecting cyber security [2]. Privacy and data theft will be the top security issues that organizations need to focus. We live in a world where all information is in digital form [3]. Cybercrime includes Frameworks, Network and other Commutation Systems. Issues including sorts of

crimes especially those encompassing hacking, copyright infringement, child pornography. Cyber Crimes can be mainly divided into three major classifications: Cyber Crimes against persons, Cyber Crimes against property and Cyber Crimes against government [4].

Privacy and information protection can be the primary security behaviour which any company cares about continually. Cybercriminals will most frequently change the current malware signatures to take advantage of new technical faults. Cyber criminals are taking advantage of emerging Internet technology and millions and billions of active users to access a huge amount of people easily and effectively using these new technologies [5]. Highlights of the Check Point 2022 Cyber Security Report are Cyber attacks against corporate networks increased by 50% in 2021 compared to 2020, Education and Research was the most targeted sector with organizations facing an average of 1,605 weekly attacks and Software vendors experienced the largest year-over-year growth, with an increase of 146% [6]. The assurance of equitable security during an electoral process is essential to retaining the participants' confidence and commitment to an election. Consequently, Security is both integral to the goal of an election and an inseparable part of the electoral process. Security of an election is unique to the circumstances in which it is conducted. Election time threats and intimidation tactics have been identified as a major security issue as well as an all-pervasive challenge [7]. The Recent trends in Digital technologies need to solve these Cyber Security challenges associated with protecting Election Infrastructure.

The Election Commission of India using IT Systems to increase elections activities to reduce the elections expenses and to achieve goal of Transparency and faith of citizens in Election system. The Election Commission has undertaken the Computerisation of all electoral rolls throughout India which has lead to improvements in the accuracy and speed so that electoral roll can be updated. IT team of Election Commission has taken IT initiatives and developed no. of Election related application and Mobile app for conducting free and fair Elections in India. Election IT infrastructure being faced by Cyber Security

challenges which is required to be addressed and Cyber security solutions need to be deployed to conduct the Elections in India.

The remaining part of paper is organized as Section-2 Related Work, Section-3 Cyber Security Challenges in General Election, Section-4 Cyber Security Measures- Discussions and Section-5 Conclusion.

2. RELATED WORK

Privacy and security of the data and information are the top Security measures that any organizations to takes care of. Elections are being conducted in all Countries using recent Digital Technologies for Election Process from Elector enrolment to Result declarations, etc. Performed study of concept, methodology and Digital Technology for some of the recent ICT based Election systems for Cyber Security issues encountered and measures deployed to achieve a goal of free and fair elections.

Sanjay Kumar and Manpreet Singh proposed framework ensures secured identification and authentication processes for the voters and candidates through the use of fingerprint biometrics. The main phases of a voting system are registration, authentication, and accessibility, casting and counting. Fingerprint matching is one of the most popular and reliable biometric techniques used in automatic personal identification. In this paper, a framework for electronic voting system based on fingerprint biometric is proposed and implemented with the objective of eliminating bogus voting and vote repetition, less election expenditure, more transparency and fast results [8]. Fridrik P. Hjalmarsson, Gunnlaugur K. Hreidarsson introduced a block-chain based Electronic voting system that utilizes smart contracts to enable secure and cost efficient election while guaranteeing voters privacy. Author outlined the systems architecture, the design and a security analysis of the system. Election scheme allows individual voters to vote at a voting district of their choosing while guaranteeing that each individual voters vote is counted from the correct district which could potentially increase voter turnout. To successfully DDoS a distributed system such as proposed, the attacker must DDoS every single boot node in the

private network. The individual or institution would be immediately located if that would occur [9].

Ahmed Ben Ayed proposed Secure Block-chain based Electronic Voting System which is secure, reliable, and anonymous and will help increase the number of voters as well as the trust of people in their governments. To ensure that the system is secure, the block will contain the previous voter's information. The Block-chain is where the actual voting takes place. The Citizens vote sent to one of the nodes on the system and the node then adds the vote to the Block-chain. The voting system will have a node in each district to ensure the system is decentralized [10]. Dhinesh Kumar M., Santhosh. A., Aranganadhan N.S. and Praveenkumar D. proposed Embedded System based Voting Machine System using Wireless Technology. There are two types of problems with EVM which is currently in use Security Problems, one can change the program installed in the EVM and tamper the results after the polling and Illegal Voting (Rigging), which is faced in every electoral procedure. One candidate casts the votes of all the members or few amounts of members in the electoral list illegally. Its main advantage is that since fingerprints of every person is unique and hence this system completely reduces the chance of invalid votes. The system is highly reliable, tamper-proof and secures [11].

Scott Wolchok Eric, Wustrow J., Alex Halderman, Hari K. Prasad, Arun Kankipati, Sai Krishna Sakhamuri, Rop Gonggrijp and Vasavya Yagati presented a paper mentioning there have been two official technical evaluations of EVM security performed at the behest of the Election Commission. In their report the commission reiterated the belief that the machines were tamper-proof; however, they also recommended a small number of changes to enhance the security of the machines. These included the adoption of dynamic key coding of button presses from the ballot unit to protect against simplistic attacks on the cable and the addition of a real-time clock and time-stamped logging of every key press, even if invalid, to provide a record of any attempt to activate malicious logic by a secret knock. Some of these changes were adopted in third-generation EVMs, but they cannot prevent the attacks [12]. Holly Ann Garnett and Toby S. James presented a paper mentioning some cyber security threats such as

hacking compromising private information, such as voter registration rolls or election results. In recent years the Distributed denial of service attack, which floods a website or service in order to render it unusable for legitimate users, has become a threat to elections. Commentators and academics alike have warned about the potential for security breaches, threatening the privacy of an individual's vote, or erasing or amending election results. Thus, any implications of the use of technology for public perceptions of the transparency and impartiality of electoral management are key to electoral integrity [13].

From the above discussions on existing Electronic Voting System it is observed that Recent Digital Technologies such as High speed internet, Mobile Phone, Mobile Apps, Biometric Technology, Block-chain, etc are being utilized for conducting elections Electronically. ICT and Digital Technologies playing crucial role in conducting Elections in efficient manner but deployment of new Digital Technologies in Elections comes with new Cyber Security issues. During Election process such as registration, authentication, accessibility, casting and counting some of the Cyber Security issues discussed are Secured identification and authentication, Distributed Denial of Service (DDoS), Web site Hacking, EVM and tamper the results, Illegal Voting (Rigging), Hacking and Compromising private information, etc. are encountered and some appropriate solutions are deployed to overcome the issues. In next section we will discuss these and some other Cyber security issues and Challenges encountered in Elections in more detail.

3. CYBER SECURITY CHALLENGES FOR GENERAL ELECTIONS

Digital Technologies such as Computers, Smart phones, Tablets, Laptop, Communication and Networking devices have a great impact on ways of Working, Communicating in General Elections. In last few years Election Commission of India focus on use of Digital Technology in Election Process. These Technologies are now playing a major role in Conducting General Election in India. The use of Digital Technologies in Elections has emerged as a

key issue in recent years with concerns about Database hacking, Information manipulation, and foreign technological interference leading to public concerns.

Election IT Infrastructure

Election IT infrastructure used to manage Elections for Voter registration, Votes counting and displaying of election results, Pre and Post-election reporting to ECI. Election IT Infrastructure includes the Electronic Voting Machines (EVMs), VVPATS, Voter database, Data Centers, Data Base Servers, Application Servers, Communication Devices, Network systems, Election Software's and Mobile Apps and other related IT systems, etc.

Election Stakeholders

Major stakeholders are Citizen, Elector, Voters, Candidates and Election Officers. Election Officers includes ECI officials, Chief Electoral Officer, District Election Officers, Returning Officers and Assistant Returning Officers.

Election IT Applications

Elections IT Applications which are implemented during Pre-Poll, During the Poll and Post Poll Election Process for successful conduct the General Elections. IT applications being used are cVIGIL, SUVIDHA, SUGAM, EMS, ERO Net, NVS, PDMS, CDMS, National Grievances Services Portal, ETPBS, etc.

Citizen, Electors access IT applications for Election related service such as Election enrolment, Deletion, Updating in Election roll, EPIC Card, Violations of Election Module of Conduct etc, upon receipt of request Concerned Election Officer take necessary action and inform accordingly the status of application through SMS. Candidates also request for Permissions for Election meeting, Rally, etc online, Election Officer approve or Reject application accordingly. Election Officers also use these Election related applications during entire Election purpose as per Instructions of ECI and RO handbook.

The main targets of hacking attacks against Election-related technology include voter registration technologies, voting, vote counting technologies, result transmission and aggregation technologies, websites for result publication and

other online election-related services, institutional and private email accounts and communication systems and broader national infrastructure, including Government systems, power grid and communication links. Generic attacks often require little sophistication and limited resources and include Denial of Service (DoS) attacks, website breaches and malware and ransomware attacks. Website breaches involve defacing the appearance of websites or manipulating their content. Malware and ransomware attacks can have adverse impacts on elections by making essential systems and data inaccessible. Finally, insider attacks include intentional data and system breaches by users with access to election-related information systems [14]. Security vulnerabilities can be exploited to electronically disrupt voting or affect vote counts at polling locations or in instances of remote voting. DoS can be used to disrupt vote casting, vote tallying or election audits by preventing access to e-poll books, electronic voting systems, or electronic auditing systems. Malware, malicious software that includes worms, spyware, viruses, Trojan horses, and ransomware is perhaps the greatest threat to electronic voting [15]. Trends in Cyber Attacks of Elections are Targeted Phishing Attacks; Phishing is the most common way of stealing information in today's cyber world as users continue to fall for it. Digital Dictatorships and Information Warfare; New technologies might tempt various governments across the world to build unprecedented totalitarian regimes that will monitor and control everyone all the time and Use of Mobile Devices by Cyber Criminals; Mobiles allow quick getaways and ubiquity. Cybercriminals are developing customized applications to increase their anonymity to avoid the detection of their identity to make their tracking difficult [16].

Cyber Security Attack trends during Elections

While there are many different ways that an attacker can infiltrate an IT system of Election, many Cyber-attacks rely on similar techniques. Security vulnerabilities can be exploited to electronically disrupt voting or affect vote counts at polling locations or in instances of remote voting in Election Process.

Phishing attacks: Phishing is the most common way of stealing information in Cyber world. Phishing attacks are getting more sophisticated every day. It is attack wherein an attacker

impersonates to be a trusted contact and sends the victim fake mails to steal the information.

Digital Dictatorships and Information Warfare:

A citizen gains or losses social credit according to ones behaviour, actions and even thoughts. Citizens can now be tracked with every move and decision, scoring on what one buys, what one vote for and who you see.

Cybercrimes through Mobile phones: Mobiles allow quick getaways and ubiquity. Cybercriminals are developing customized applications to increase their anonymity to avoid detection by making it difficult to track them.

Denial-of-Service Attacks: Denial-of-service (DoS) attacks interrupt or slow access to Election Computer systems. DoS can be used to disrupt vote casting, vote tallying or election audits by preventing access to Electronic voting systems or Electronic auditing systems.

Malware: Malicious software that includes Worms, spyware, viruses, Trojan horses and Ransomware are the greatest threat to Electronic voting. Malware can be introduced at any point in the electronic path. Election Equipments are manipulated to slow its operation or compromise its operability. Malware can prevent voting by compromising or disrupting or by disabling vote-casting systems.

Stealing Voter information: Cyber threat actors may try to compromise or manipulate Voter registration

Website breaches

Attacks: Cyber threat actors often target Websites of Election Commission of India with DDoS, Phishing and Defacement. Official election result websites may also be vulnerable to hacking. Hackers can take over, deface or shut down official Election Web sites.

Email Compromise: Cyber threat actors use Phishing with which to target Government email systems. An email account can be compromised in a number of different ways to get the email account access.

Networks Attacks: Cyber threat actors use Phishing or Malware in their attempts to infiltrate Election system Networks that election office relies on for regular Election process.

Password Attack: A Password attack refers to any methods which are used to maliciously authenticate into password protected accounts. It is done with the help of software that expedites cracking or guessing passwords to get access to Election systems.

SQL injection: SQL injection is a cyber attack that injects malicious SQL code into an application, allowing the attacker to view or modify an Election database. These results in attacker being able to view edit and delete data from the databases. Attackers can also get administrative rights through SQL injection.

Other Classes of Attacks: There are other attacks from which Electronic systems may be disrupted. Malicious actors may obtain sensitive information such as User ID and Passwords by pretending to be a trustworthy entity in an Electronic communications system. Data Servers and Application may be breached to obtain administrator level credentials. Individuals who are having Web Portal and Mobile Apps access might physically access a system for viewing and editing the data.

Digital Technologies being used in Elections that creates Cyber Security issues which need to be monitored and controlled by Election Commission of India for the entire Election Process. Election Commission of India therefore needs to initiate additional Cyber Security measures for the long term to conduct free and fair Elections in India.

4. CYBER SECURITY MEASURES AND DISCUSSIONS

Digital Technologies includes Smart phones, Tablets, QR code Scanner, EVM, VVPAT, Web based Applications, Mobile Apps, Communication and Networking etc. is being increasingly used in the Election Process to deliver public services and Conduct Election in effective manner. Election Commission of India developed no of IT

Applications under IT Initiatives for better Elections in the India.

Cyber Security Measures

During Election process Secured identification and authentication, Phishing attacks, Malware, Distributed Denial of Service (DDoS), Web site Hacking, EVM and tamper the results, Hacking Websites and Stealing of Information, etc Cyber Security challenges are encountered and appropriate solutions need to be deployed to overcome these issues. Cyber Security challenges may be overcome by means of the adoption of the following measures during working with Election process:

Strong Password: Use complex passwords with a minimum length of 8 characters, using a combination of capital letters, small letters, numbers and special characters. Passwords need to change at least once in 45 days and Use multi-factor authentication.

Use of firewalls: Software and hardware Firewalls filter the traffic that enters in to the device. Windows and Mac OS have their default built-in firewalls such as Windows Firewall and Mac Firewall.

Email Scrutinize: Scrutinize your email as most phishing emails have significant errors like spelling mistakes and format changes from that of legitimate sources.

Software Updates: Application Software, Mobile Apps and others drivers need to be updated with latest patches. Also keep Operating System and BIOS firmware updated with the latest updates and patches.

Antivirus Software: Install enterprise Antivirus software on Desktops, laptops, etc. Ensure that the antivirus software is updated with the latest virus definitions, signatures and patches.

Backup of Data: Save Election data and files on the secondary drive e.g. Drive D:, Pen drive, etc as back up and maintain an offline backup of critical data.

Apps Download: Download Apps from official app stores of Google and Apple. Before downloading an App, need to check the popularity of the app and read the user reviews.

Data Encryption: While sending any important Election related Information or document over email or any Electronic medium, encrypt the data before transmission.

Virtual Private Network: Virtual Private Network (VPN) Token may be used for connecting any IT assets located in the Data Centers.

GPS, Bluetooth disabled: Keep the GPS, Bluetooth and other devices disabled on your Desktops and Mobile phones. They maybe enabled only when it is required.

URL Shortener Services: Be cautious while opening any URLs because many malwares and phishing sites abuse URL shortener services.

Suspicious Links: Observe caution while opening any links shared through SMS or social media, etc., such links may lead to a phishing or malware webpage, which may compromise system.

The growing use of Technology in the election process has made cyber security a crucial issue. Instances of the spread of fake news, manipulation of voter behaviour and hacking show how digital technology can be misused. These issues need to be addressed in the long term. The Election Commission (EC), tasked with maintaining the sanctity of India's electoral process, has taken several steps to ensure the inviolability of the technical infrastructure, which includes the Electronic Voting Machines (EVMs), Voter database, Voting software and IT systems. Reliability of EVMs: EVMs are stand-alone machines, which cannot be connected to any network; Individual machines can theoretically be tampered with, though there has been no evidence of this. Now with the mandatory use of the Voter Verifiable Paper Audit Trail machines, this doubt too will be eliminated. Specialized initiatives on cyber security: In 2017, the EC created the new post of Chief Information Security Officer whose job is to supervise various measures, such as conducting regular cyber security drills and ensuring various EC offices compliance with Cyber

security measures. Making election infrastructure as critical infrastructure: The next step for the EC is to redesignate its Election infrastructure as Critical Infrastructure under the Information Technology Act 2000 [17].

Initiatives taken by Government of India on Cyber Security

Government of India taken various steps to control and monitor Cyber security issues in Cyber Space. These initiatives are undertaken by Government of India to address Cyber security issues and improve their implementation at the National level. Some of the major initiatives undertaken by Government are as follows:

1. The Indian Computer Emergency Response Team (CERT-In)
2. National Critical Information Infrastructure Protection Center (NCIIPC)
3. Appointment of Chief Information Security Officers
4. National Cyber Security Policy, 2013
5. Cyber Surakshit Bharat

Election conducting bodies need to report suspicious emails or any Cyber Security incident to incident@cert-in.org.in and Adhere to the security advisories published by NIC-CERT.

Election Commission of India (ECI) Guidelines

The Commission has a vision that Elections that are completely free of crime and abuse of money based on a perfect electoral roll and with full participation of voters. The Election Commission of India recently released a document outlining Cyber Security General Guidelines for General Election 2019. Guide lines contains precautionary measures for Password Security, Email Security, Mobile Security, Data Storage Protection, Outsourced Staff, Desktops, Data Backup, Wi-Fi Security, Website Security are Password Complexity, Use of Gov/ NIC Email, Avoid Whats App for sensitive Official Documents/ Communications, Security of sensitive files, Sharing of information/data on need to know basis, Use of supported OS, Devise a data backup policy, Use WPA2 security, Use https for sensitive data interchange respectively. The Cyber Security Guidelines will be a stepping stone for all Election management bodies. One of the major initiatives

which ECI took was to revamp all old applications, reduced the number of applications and consolidated them into a manageable application [18]. Cyber Security Tips for ECI Officials are You Are a Target; Realize that you are an attractive target to hackers, Eight Characters Is Not Enough for Password, Lock It Up; Never leave your devices unattended, Practice Safe Clicking Always, be careful when clicking on attachments or links in email and Beware of Browsing; Sensitive browsing [19].

Cyber Security Measures, Initiatives taken by Government of India on Cyber Security and Election Commission of India (ECI) Guidelines discussed above will solve the Cyber Security Challenges/issues encountered in Election systems to some extent. Future work consists of Design of Security Framework for General Election in India based on Election Commission of India (ECI) Guidelines. Security framework help to reduce the Risk of vulnerability and Cyber Security issues in General Election by deployment of Digital Technologies. It also benefited from Accountability, Transparency, Accuracy, efficiency, etc. It improves the security measures and offer new possibilities of transparency. High level security measures will be deployed as all applications and Mobile app use Multi-Layer Authentication to avoid unauthorized access to the Election systems. Security Framework will be implemented effectively during the entire Election Process to ensure that Elections can take place in an orderly and fair manner.

5. CONCLUSION

The use of Digital Technologies in the Election Process has made Cyber Security a crucial issue. The increasing adoption and use of ICT has increased the attack surface and threat perception to Election IT infrastructure. The use of Digital Technologies needs to solve Security challenges associated with protecting Election Infrastructure. This paper presents various Cyber Security challenges and measures deployment to overcome Cyber security issues for conducting free and fair Elections during the entire Election process from Voter registration to Result declaration, etc. During Election process Secured identification and authentication, Phishing attacks, Malware, Distributed Denial of Service (DDoS), Web site

Hacking, EVM and tamper the results, Hacking Websites and Stealing of Information, etc Cyber Security challenges are encountered and appropriate solutions such as Strong Password, Use of firewalls, Email Scrutinize, Data Encryption, Virtual Private Network, Software Updates, Antivirus Software, etc need to be deployed to overcome these issues. Cyber Security Techniques/Measures, Initiatives taken by Government of India on Cyber Security and Election Commission of India (ECI) Guidelines discussed in this paper will solve the Cyber Security Challenges/issues encountered during working with Election systems to some extent. Future work consists of Design of Security Framework for Election System in India based on Election Commission of India (ECI) Guidelines. Security framework help to reduce the Risk of vulnerability and Cyber Security issues in General Election and improve the Security measures and offer new possibilities of transparency in General Elections of India.

6. ACKNOWLEDGMENTS

Author was working as a Nodal Officer for Computerization of Election process for General Elections to Parliament and Assembly for Amravati District. I would like to thanks Mr. Sailesh Naval District Election Officer for his guidance and motivation during entire Election Process. I would like to thanks Mr. K. P. Pariselvan SIO and Mrs. Meera Joshi ASIO for their guidance and motivation. I would like to thanks Mr. Manish Fulzele ADIO and Mr. Yogesh Umak for their support in Elections.

7. REFERENCES

1. Official Portal of Election Commission of India, <https://eci.gov.in>
2. Y. Poornima, Y.Naveena and Mr.V.Harsha Vardhan, "Cyber Security Issues and Challenges in India", International Journal of Scientific & Engineering Research, Volume 8, Issue 5, May-2017
3. Ravi Sharma, "Study of Latest Emerging Trends on Cyber Security and its challenges to Society", International Journal of Scientific & Engineering Research, Volume 3, Issue 6, June-2012
4. Aaditi Singh, "A Study on Emerging Issues of Cyber Attacks & Security: In India", IJARIE-ISSN(O)-2395-4396, Vol-7 Issue-1 2021
5. Dr. Prof. Rajasekharaiah K.M. , Chhaya S. Dule and Sudarshan E., "Cyber Security Challenges and its Emerging Trends on Latest Technologies", ICRAEM 2020, IOP Conf. Series: Materials Science and Engineering 981 (2020)
6. Check Point Research, "Cyber Security Report 2022" , <https://resources.checkpoint.com>
7. Chanchal Kumar, "Electoral Violence, Threats and Security: Problems and Prospects for Indian Democracy", American Journal of Social Science Research Vol. 1, No. 1, 2015
8. Sanjay Kumar and Manpreet Singh, "Design A Secure Electronic Voting System Using Fingerprint Technique", IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 4, No 1, July 2013
9. Fridrik P. Hjalmarsson, Gunnlaugur K. Hreidarsson, "Block chain-Based E-Voting System" 2018 IEEE 11th International Conference on Cloud Computing (CLOUD), July 2018
10. Ahmed Ben Ayed, "A Conceptual Secure Block chain- Based Electronic Voting System", International Journal of Network Security & Its Applications (IJNSA) Vol.9, No.3, May 2017
11. Dhinesh Kumar M., Santhosh. A., Aranganadhan N.S. and Praveenkumar D., "Embedded System based Voting Machine System using Wireless Technology", International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering Vol. 4, Issue 2, February 2016
12. Scott Wolchok Eric, Wustrow J., Alex Halderman, Hari K. Prasad, Arun Kankipati, Sai Krishna Sakhamuri, Rop Gonggrijp and Vasavya Yagati, "Security Analysis of India's Electronic Voting Machines", CCS '10: Proceedings of the 17th ACM conference on Computer and communications security, October 2010
13. Holly Ann Garnett and Toby S. James, "Cyber Elections in the Digital Age: Threats and Opportunities of Technology for Electoral Integrity", Election Law Journal, Volume 19, Number 2, 2020

14. Sam van der Staak and Peter Wolf, “Cyber Security in Elections” , Models of Interagency Collaboration, IDEA, 2019 International Institute for Democracy and Electoral Assistance
15. Ensuring the Integrity of Elections, National Academies of Sciences, Engineering, and Medicine. 2018. Securing the Vote: Protecting American Democracy. Washington, DC: The National Academies Press.
16. Samaya Dharmaraj, “Indian Election Commission releases new Cyber Security Guidelines”, <https://opengovasia.com>, October 3, 2019
17. Sameer Patil, “ The Cyber Security Imperative for India’s Elections”, Gateway House, 18 April 2019
18. Chief Information Security Officer, “Cyber Security General Guidelines for General Election 2019” Election Commission of India
19. Chief Information Security Officer, “ECI Cyber Bulletin, Election Commission of India, October 2019”