VOLUME 4 | ISSUE 3

INTERNATIONAL JOURNAL OF ADVANCED LEGAL RESEARCH

CRITICAL ANALYSIS OF ELECTRONIC VOTING SYSTEM; SECURITY CONCERNS AND POLICY IMPLICATIONS IN INDIA

- Heeral Devpura & Yash Johari[1]

Abstract

In India, electoral processes predominantly rely on electronic voting machines (EVMs), developed over the past two decades by government-owned entities. These devices, commonly called EVMs in India, have been commended for their uncomplicated design, user-friendliness, and dependability. However, recent scrutiny has arisen due to widespread reports of electoral irregularities. Despite their positive attributes, certain specifics regarding the EVMs' design remain undisclosed to the public, and they have not undergone thorough, impartial security assessments. This paper presents a security analysis of a genuine Indian EVM procured from an undisclosed source. We provide an intricate overview of the machine's structure and functionality, assessing its security in light of pertinent electoral protocols. Our findings indicate that despite the machines' simplicity and limited software-trusted computing base, they are susceptible to severe attacks capable of manipulating election outcomes and compromising ballot secrecy. We illustrate two such attacks, utilising custom hardware, that are feasible for dishonest insiders or malevolent individuals with brief physical access to the machines. This case study underscores significant insights relevant to Indian elections and the broader realm of electronic voting security.

Research Methodology:

1. Literature Review: We greatly reviewed published works about e-voting systems used in India. This includes reading about security issues and policy frameworks. It helped them grasp the current situation and the problems they faced.

[1] Students at Amity University Rajasthan

2. Case Studies: Past e-voting efforts were examined, both those that succeeded and failed miserably. We looked at security measures, vulnerabilities found, and effects on election results.
3. Comparative Analysis: Next, we compare their findings to international best practices for e-voting security and policy-making. This helped them learn lessons and make recommendations that could work in India.

Introduction

India is the largest democracy in the world. Over the past 20 years, technological advances have revolutionised democratic processes. One area of ongoing debate is the use of electronic voting machines (EVMs). Unlike traditional pencil and paper voting systems, technology has the potential to empower voters, increase their voice, and hold governments accountable. Indian election authorities claim electronic voting machines (EVMs) are entirely secure. However, details of their design have remained a mystery, and EVMs have not been subject to rigorous independent security assessments. This paper will analyse the security measures around EVMs in India. The simplicity of EVMs' design may protect them from threats but also open them up to a unique set of hazardous attacks. Election insiders or criminals may attempt to manipulate the outcome of an election without being detected. Portable hardware devices may extract and alter the votes stored in the EVM's memory. Election results may be compromised. Ballot secrecy may be compromised.

This study confirms that India’s EVMs are tamper-resistant and vulnerable to various attacks. With the discontinuation of such paperless DRE systems in several countries, such as California[2], Florida[3], Ireland, Netherlands, and Germany, India’s electoral authorities must reconsider their current security protocols and conduct thorough inspections on all EVMs to protect against fraud. This study confirms that the electronic voting machines (EVMs) used in India are highly susceptible to several attacks. Similar paperless DREs have been discontinued in many countries, such as Florida, California, Ireland, and Germany. The Indian election authorities should review the security procedures currently in place and thoroughly inspect all EVMs for any evidence of fraud.

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

[3] A. Goodnough and C. Drew. Florida to shift voting system with paper trail. In The New York Times, Feb. 2, 2007

Overview of Electronic Voting System

Definition and Functionality:

Electronic Voting Systems (EVS) are computerised tools created to simplify the process of casting and counting votes electronically. These systems replace the traditional paper-based method with digital interfaces for voters to submit their choices. The key features typically include:

- Voter Authentication: Voters are verified through biometric checks, smart cards, or unique IDs.
- Ballot Display: Voters see digital ballots on a screen once authenticated. These ballots list the candidates or issues to vote on.
- Vote Casting: Voters make their selections by interacting with the digital interface, often by touching the screen or using input devices like keyboards or buttons.
- Vote Recording: The system securely records each vote to ensure accurate capture and counting.
- Vote Tabulation: The system automatically tallies the votes after voting closes, providing quick and precise results.

Implementation in India:

In India, Electronic Voting Machines (EVMs) have been used since the late 1990s to conduct elections electronically. EVMs are standalone devices with simple functions that replace traditional paper ballots. Critical features of EVMs in India include:

- **User-friendly Interface:** EVMs in India have a straightforward interface with buttons representing different candidates or options. Voters press the button corresponding to their choice.
- **Tamper-resistant Design:** EVMs are designed to be tamper-resistant, with strict security measures to prevent unauthorised access or manipulation.
- **Battery-powered:** EVMs operate on batteries, making them usable even in areas with limited or no electricity supply.
- **Easy to Deploy:** EVMs are relatively easy to set up and transport, making them suitable for use across diverse geographic regions. Despite some controversies and

concerns about the security and integrity of EVMs, they have been widely utilised in Indian elections at various levels, including national, state, and local.

Advantages and Disadvantages:

Electronic voting systems can significantly speed up the process of voting, counting votes, and reporting results compared to manual methods. They can also help reduce errors in vote counting and minimise invalid or spoiled ballots. These systems can be designed to accommodate voters with disabilities, providing features like audio prompts, larger text, and other accessibility options. Over time, electronic voting systems may lead to cost savings by reducing the need for printing and distributing paper ballots and the workforce required for manual counting.

However, these systems also have some drawbacks. They are vulnerable to hacking, tampering, and cyber-attacks, raising concerns about votes' security and confidentiality. Additionally, not all voters may be comfortable or familiar with using electronic devices, which could potentially exclude specific demographics or communities.

Security Concerns with Electronic Voting Systems in India

What are the potential vulnerabilities of electronic voting systems in India?

Various researchers have studied electronic voting systems in India as a potential vulnerability. The vulnerability of electronic voting machines in India has been identified through collaborative studies. These machines are vulnerable to fraud and can be criticised for their lack of reliability. The absence of personal verification of the system's integrity is a potential vulnerability of electronic voting systems in India. The software source code used in electronic voting machines is not accessible to citizens, making it difficult for them to monitor the systems for any anomalies. Threat actors exploit technological gaps to compromise the democratic fabric, casting a shadow over the very essence of democracy. Hacking EVMs and disruptingvoter registration databases are other potential vulnerabilities that could jeopardise the integrity of the entire election process.

Moreover, Indian electronic voting machines use a simple embedded system architecture, considerably different from the complex voting machines used in the US and Europe. The vulnerabilities of the electoral process in India are evident, as political parties are raising allegations of fraud and EVM tampering after election results. Indian authorities have not permitted a severe and independent review of the security of electronic voting machines, which further highlights the potential security risks involved with electronic voting systems in India. Designing voting systems that provide transparency and security is a challenge in India and many other democracies, as the study demonstrated technical problems in India's electronic voting system, which has implications for voting technology beyond India.

How can cyber-attacks target electronic voting systems?

Electronic voting systems have become increasingly popular worldwide, but their potential for being targeted by cyberattacks has also grown. These systems are vulnerable to various types of attacks, putting the integrity of elections at risk. An attack involves substituting a small component with a look-alike that can be instructed to steal votes from a specific candidate.[4] This attack can be carried out by simply swapping out the original component with the fraudulent one, thereby manipulating election results. Another issue with electronic voting systems is that they can be attacked through almost every element, including vote-counting software programmed into "mask-programmed microcontrollers."

The fact that the software in these machines is unknown and cannot be read out or verified adds to the vulnerability of electronic voting machines. Paperless voting systems have intrinsic security flaws and are vulnerable to cyber-attacks. Attackers can change the votes stored in electronic voting machines between the election and the public counting session using a pocket-sized device, altering the election outcome. Even electronic identification to access the voting machine can be vulnerable to cyber-attacks. Criminals can change election results by accessing paperless machines, even briefly. Furthermore, lack of transparency in electronic voting systems can make them susceptible to dishonest vote counting, and computers can be programmed to count votes honestly or dishonestly. In conclusion, electronic voting systems, particularly Direct Recording Electronic (DRE) machines, are fundamentally vulnerable to cyber-attacks and pose a significant threat to the integrity of elections worldwide.

[4] Cyber News #24 - Security in Electronic Voting Systems. (n.d.) retrieved March 25, 2024, from www.linkedin.com

What are the implications of security breaches in electronic voting systems for the Indian electoral process?

The Indian electoral process is essential to democracy, and its security should be paramount. However, as evidenced by past events, electronic voting systems used in Indian elections are susceptible to security breaches and attacks. For instance, hackers can manipulate EVM machines to vote for a particular party[5]. This vulnerability can lead to the modification of results, which could impact the election outcome and undermine the public's confidence in the electoral process. Therefore, it is crucial to implement improved security measures that utilise unclonable technology to secure EVM machine votes to protect democracy. One way to prevent fraudulent activities is by uniquely authenticating every individual and machine through voter ID chips and EVM machines. This approach ensures that everyone can only cast one vote, and machines cannot be tampered with or modified. However, using unsecured software in EVM machines is a common issue that needs to be addressed. As a result, the public and political parties do not trust EVMs completely, undermining the electoral process's credibility. In addition, misuse of EVMs has resulted in numerous cases being filed against them[6]. Severe penalties should be imposed on those guilty of election tampering to mitigate these concerns. It is important to note that security breaches in electronic voting systems have severe implications for the Indian electoral process. Therefore, it is necessary to enact and enforce cybersecurity laws to deter threat actors from attempting to manipulate election results[7]. Furthermore, the government should establish a legal framework that addresses election tampering. By implementing these measures, the Indian electoral process can be protected from cyber threats and ensure the integrity of democracy.

The critical analysis of electronic voting systems in India presented in this research paper highlights the security concerns and policy implications associated with these systems. The vulnerability of electronic voting machines has been identified as a potential threat to the integrity of the Indian electoral process. These machines' simple embedded system

[5] India's electronic voting machines are vulnerable to attack (w/ Video). (n.d.) retrieved March 25, 2024, from phys.org

[6] India’s electronic voting machines are vulnerable to attack | University of Michigan News. (n.d.) retrieved March 25, 2024, from news.umich.edu

[7] Security Problems in India's Electronic Voting System. (n.d.) retrieved March 25, 2024, from eecs.engin.umich.edu

architecture makes them susceptible to fraud, and researchers have criticised their lack of reliability. A potential vulnerability threat actors could exploit is the absence of personal verification of the system's integrity. Additionally, the software's source code used in electronic voting machines is not accessible to citizens, making it difficult for them to monitor the systems for any anomalies. The government must establish a legal framework that explicitly addresses election tampering to deter threat actors from attempting to manipulate election results. It is crucial to enact and enforce cybersecurity laws to ensure the security of electronic voting systems and prevent security breaches from having severe implications for the Indian electoral process. The results of this study emphasise the need for further research to address the limitations and gaps identified and suggest future research directions to ensure the integrity and security of electronic voting systems in India.

Existing Legal Framework:

Elections in India are governed by the Representation of the People Act, 1951, and the Conduct of Elections Rules, 1961. These laws provide the legal framework for using Electronic Voting Machines (EVMs) in elections. The Election Commission of India (ECI) is responsible for conducting elections and issuing guidelines for using EVMs. The ECI has established comprehensive procedures for storing, transporting, and deploying EVMs during elections. These procedures aim to ensure the security and integrity of the voting process. The ECI also conducts mock polls and randomises EVMs before elections to verify their functionality and authenticity. Additionally, the Information Technology Act of 2000 and its related rules have implications for electronic voting systems, addressing data security and privacy issues.

However, critics have raised concerns about the adequacy of the existing legal framework in addressing emerging challenges such as cyber security threats and the need for greater transparency in electronic voting systems. There have been calls for amendments to existing laws to strengthen the legal safeguards and accountability mechanisms concerning electronic voting systems.

Need for Strengthening Security Measures:

Ensuring the(se)curity of electronic voting systems is crucial for maintaining the credibility of elections. In India, there is a pressing need to strengthen security measures related to Electronic Voting Machines (EVMs) to address concerns about potential tampering or hacking. Some key ways to enhance security include:

- **E2E Encryption:** Implementing robust encryption protocols to secure data transmission between EVMs and central servers, thereby protecting against interception and tampering.
- **Multi-factor Authentication:** Introducing multiple authentication streps to verify user identities accessing EVMs, preventing unauthorized access.
- **Regular Audits:** Conducting periodic security audits and vulnerability assessments of EVMs to identify and fix potential issues.
- **Physical Security:** Enhancing physical security measures like tamper-evident seals and secure storage facilities.
- **Independent Oversight:** Establishing independent oversight mechanisms, such as a dedicated election security committee or an independent audit agency, to monitor and evaluate the security of electronic voting systems.

By implementing these measures, the Indian government can bolster the security of electronic voting systems and instil greater confidence among voters and stakeholders in the integrity of the electoral process.

International Best Practices:

Several countries have started using electronic voting systems and have implemented good practices to ensure they are secure, transparent, and effective. Some critical international best practices that India could consider include:

1. Paper Trails: Implementing paper records alongside electronic voting systems so voters can check their choices and there is an extra layer of transparency and accountability.

2. Audits: Doing audits that sample paper ballots to verify the accuracy of electronic vote counts helps build confidence in the election results.

3. Open Software: Using open-source software for electronic voting systems so the code can be reviewed publicly, reducing the risk of hidden problems or backdoors.

4. Independent Checks: Subjecting electronic voting systems to independent certification by accredited third-party organisations.

5. Public Education and Awareness: Conducting public education campaigns to raise awareness among voters about electronic voting systems, their features, and the measures in place to ensure their security and integrity.

Successful Implementations:

- **Case Study: Bhind District, Madhya Pradesh[8]**

In the 2019 Lok Sabha elections, Bhind district in Madhya Pradesh witnessed a successful implementation of Electronic Voting Machines (EVMs) with Voter-Verified Paper Audit Trail (VVPAT) systems. VVPAT machines were used alongside EVMs to provide a physical paper trail of each vote cast electronically. This initiative aimed to enhance transparency and increase voter confidence in the electoral process. The implementation in Bhind district was notable for its smooth conduct, minimal technical glitches, and positive feedback from voters regarding the transparency and verifiability of the voting process.

Failures and Challenges:

- **Case Study: Controversy Surrounding EVMs in Uttarakhand[9]**

In the 2017 Uttarakhand state elections, Electronic Voting Machines (EVMs) were scrutinised due to allegations of tampering and malfunctioning. Several political parties raised concerns about discrepancies between the votes polled and votes counted in specific constituencies, leading to protests and demands for a return to paper ballots. While the Election Commission of India (ECI) dismissed these allegations and attributed the discrepancies to human errors and procedural lapses, the controversy highlighted the challenges associated with ensuring the security and integrity of electronic voting systems.

Lessons Learned:

- **Case Study: Goa's Approach to Ensuring EVM Security[10]**

In Goa, the state election commission took proactive measures to address concerns about the security of Electronic Voting Machines (EVMs) and enhance public confidence in the

[8] "Successful Mock Poll, Dry Run of EVMs, VVPAT Machines in Bhind." India Today, 2 April 2019.

[9] "EVM Row: Harish Rawat Files Complaint with CEC Over Alleged Tampering in Uttarakhand Assembly Polls." The Indian Express, 12 March 2017.

[10] "Ahead of Assembly Elections, Goa EC Undertakes Demonstration of EVMs." The Times of India, 28 December 2016.

electoral process. The commission conducted extensive public demonstrations and awareness campaigns to educate voters about the functioning of EVMs and the measures in place to prevent tampering or manipulation. Additionally, the commission collaborated with technical experts and civil society organisations to conduct independent audits and verifications of EVMs, thereby fostering transparency and accountability in the electoral process.

Case Studies from Other Countries:

- **Case Study: Estonia's Internet Voting System**[11]

Estonia is well-known for its advanced online voting system. This system allows eligible voters to cast their ballots through the Internet. The system was implemented in 2005 and has been used in several national elections. Estonian voters have widely accepted this system. The online voting system uses strong encryption and authentication measures to ensure the remote votes' security and integrity. Despite initial concerns about the security of online voting, Estonia's system has been praised for its transparency, accessibility, and convenience.

- **Case Study: Norway's Use of Scannable Paper Ballots**[12]

Norway utilises a hybrid voting system that combines electronic counting of scannable paper ballots with manual verification. In this voting system, voters mark their choices on paper ballots. Electronic machines then scan these ballots to count the votes. The scanned ballots are kept safely, allowing for manual recounts if needed. This method ensures the voting process is accurate and transparent while benefiting from the efficiency of electronic vote tabulation.

Lessons Learned and Best Practices:

Lesson Learned: Transparency and Trust Building

Estonia has shown that being open and building trust iscritical to successfully using electronic voting. Sharing details about how the system works, having outside experts check its security, and working with different groups can help people feel confident in the election process.

[11] Vinkel, Priit. "Overview of the Estonian Internet Voting System." IEEE Security & Privacy, vol. 15, no. 4, 2017, pp. 45-51.

[12] Institute for Democracy and Electoral Assistance (International IDEA). "Voter Registration and Electoral Systems: Norway." International Institute for Democracy and Electoral Assistance, 2018.

Best Practice: Multi-layered Security Measures

The best approach is to have multiple layers of security, like encryption, authentication, and records of what happened. Norway combines electronic counting with manual checks, an excellent way to be efficient and accurate when voting.

Lesson learned: Ensuring reliable voting Systems.

Continuous Evaluation and Improvement Continuously evaluating and improving electronic voting systems is crucial for addressing new challenges and maintaining public trust. Regular audits, reviews, and updates to security protocols help identify vulnerabilities and strengthen voting systems against evolving threats.

Best practice: Engaging the Public

Education and Participation Informing and engaging the public about electronic voting systems is vital for promoting understanding and acceptance among voters. Estonia's experience shows the importance of providing comprehensive information and support to voters, including guidance on securely using online voting platforms.

Recommendations for Improving Electronic Voting Systems in India

- **Ensuring security measures:** To improve electronic voting systems in India, it is crucial to prioritise enhancing security measures. This will safeguard against potential threats and ensure the integrity of the electoral process. Several recommendations can be made:

Implementing robust encryption protocols and multi-factor authentication mechanisms will secure data transmission and authenticate users accessing electronic voting machines (EVMs). This will help prevent unauthorised access and tampering with the voting process.

Secondly, conducting regular security audits and vulnerability assessments of EVMs is essential. This will identify and address potential security weaknesses. Independent third-party audits should be carried out to verify compliance with security standards and assess the effectiveness of security measures.

Furthermore, enhancing physical security measures, such as tamper-evident seals and secure storage facilities for EVMs, will mitigate the risk of physical tampering and unauthorised access. Furthermore, establishing dedicated election security committees or independent audit agencies tasked with overseeing the security of electronic voting systems and ensuring adherence to best practices and standards would strengthen accountability and oversight in the electoral process.

- **Strengthening Auditability and Verification:**

It improves electronic voting systems and verification mechanisms in India's audit ability. This would enhance transparency and trust in the electoral process. Introducing paper audit trials (PATs) alongsideelectronic voting machines (EVMs) would allow voters to verify their choices. This would provide an additional layer of transparency and accountability, as the re would be a physical record of each vote cast electronically. This could be used for manual verification and recounts if necessary. Furthermore, implementing risk-limiting audits would provide assurance about the integrity of election results. The audits involvethe statistical sampling of paperballots to verify the accuracy of chronic alleys. The audits should be conducted independently by third-party organisations to ensure impartiality and credibility. Additionally, improving education and awareness about thesuitability and verificationprocesses would power voters to participate more actively in monitoring and validating the electoral process, thereby fostering trust and confidence in electronic voting systems.

- **Addressing Accessibility and Usability:**

Making voting accessible and easy to use ensures everyone can participate fully in elections. To improve the accessibility and usability of electronic voting systems in India, here are some recommendations: Creating user-friendly interfaces with clear instructions would simplify voting for all voters, including those with limited digital skills or disabilities. Offering options like audio prompts, larger text, and adjustable contrast would help voters with visual or hearing impairments. Providing assistive technologies such as braille keypads and sip-and-puff devices at polling stations would allow voters with disabilities to cast their votes independently and privately.

Comprehensive accessibility assessments and consultations with disability rights groups can help identify and address any barriers preventing people with disabilities from fully participating in electronic voting systems. This ensures that the needs of all voters are effectively accommodated. Additionally, establishing dedicated support services and training programs for election officials and polling staff can help them better assist voters with disabilities or special needs. This will enhance inclusivity and ensure equitable access to the voting process. By implementing these recommendations, India can improve the security, auditability, accessibility, and usability of electronic voting systems. This will strengthen the democratic principles of transparency, integrity, and inclusivity in the electoral process.

Conclusion and suggestions

Examining electronic voting systems in India reveals strengths and areas needing improvement. The current legal framework provides a foundation for using Electronic Voting Machines (EVMs) but may require updates to address emerging challenges like cybersecurity threats and transparency concerns. Successful implementations, like in Bhind district, showcase the potential of electronic voting to enhance efficiency and transparency in the electoral process. However, as seen in Uttarakhand, controversies and challenges underscore the need for ongoing vigilance and improvement. Recommendations for improving electronic voting systems in India include enhancing security measures, strengthening auditability and verification processes, and addressing accessibility and usability concerns.

These recommendations aim to make the electoral process more reliable, inclusive, and trustworthy. This ensures that all eligible voters can participate effectively and securely. Implementing these recommendations requires coordination among government agencies, election authorities, technical experts, civil society groups, and other stakeholders.

The implications for future research in this field are significant. More studies are needed to explore new technologies and best practices for securing electronic voting systems against emerging threats. Research into the usability and accessibility of electronic voting interfaces can inform the design of more inclusive voting solutions that accommodate diverse voter needs. Additionally, investigations into public perceptions, attitudes, and trust levels towards electronic voting systems can provide insights into strategies for enhancing voter confidence and acceptance.

Going ahead, researchers must concentrate on evaluating electronic voting practices worldwide. They should analyse legal rules, rollout plans, and results in different nations. Comparing systems can offer critical lessons for improving voting processes globally. Policymakers and election officials can gain insights by examining various approaches. Continued research and teamwork are vital. They help advance electronic voting and secure democratic elections in India and everywhere. Ensuring integrity, safety, and accessibility for voters is crucial. Elections must be fair and open to all.

Lengthy, in-depth studies comparing many countries' electronic voting methods are needed. Legal frameworks for voter security and system oversight vary greatly. Implementation strategies like public education campaigns and voting machine upgrades impact success. Outcomes like voter turnout, issues encountered, and confidence in results differ too. This comparative analysis provides a wealth of knowledge. Learning from different nations' experiences is invaluable for enhancing electoral processes worldwide.

Furthermore, collaboration among researchers, government bodies, and election authorities is essential.