International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

A Critical Study on Administrative Transparency and Information Technology Utilization for Election Commission of India from 2000 to 2018

Jayant Vijay Raut
Assistant professor
Department of Political science
Shri Ganesh Kala Mahavidyalay Kumbhari, TQ. Dist. Akola
S. G. B. A. U. Amravati, Maharashtra, India

Abstract

This critical study examines the relationship between information technology (IT) utilization and administrative transparency in the Election Commission of India (ECI) during 2000-2018, a transformative period marking India's transition from paper-based to technology-driven electoral management. The research analyzes three interconnected domains: (1) digital infrastructure for electoral roll management and result dissemination, (2) transparency mechanisms including Right to Information (RTI) accessibility, and (3) emerging cybersecurity frameworks for election data protection. The study reveals a fundamental paradox: while the ECI achieved remarkable technological sophistication in electoral operations—including nationwide EVM deployment, real-time result display systems, and social media monitoring tools—its administrative transparency remained uneven and, in certain respects, regressive. The ECI's refusal to accept online RTI applications (with nearly 2,000 applications pending without response by 2017) stands in stark contrast to its otherwise progressive technological posture . Simultaneously, the Commission pioneered cybersecurity regulations and critical infrastructure protection frameworks that positioned it among the most technologically advanced election management bodies globally . This duality—technological advancement without corresponding transparency enhancement—constitutes the central finding of this study. The research concludes that IT utilization alone does not guarantee administrative transparency; institutional culture, legal frameworks, and political will determine whether technology serves openness or control. The study offers recommendations for integrating transparency-by-design principles into election technology architecture.

Keywords:

Election Commission of India, administrative transparency, information technology, Right to Information, cybersecurity, electoral management, digital governance, EVMs, voter registration systems

1. Introduction

The Election Commission of India, established as a constitutional authority under Article 324, bears the responsibility of administering elections for the world's largest democracy. Between 2000 and 2018, the Commission underwent a profound technological transformation. By 2014, it deployed 1.4 million electronic voting machines across one million polling stations to serve 814 million voters . The introduction of real-time result display systems, computerized electoral rolls, and social media monitoring tools marked India's emergence as a global leader in election technology .

However, administrative transparency—the principle that citizens should be able to access information about governmental processes, decisions, and data—did not advance at the same pace. The Right to Information Act, 2005 established a legal framework requiring public authorities to proactively disclose information and respond to citizen requests. Yet the ECI demonstrated selective compliance: technologically sophisticated in electoral operations but resistant to transparency mechanisms that would subject its own processes to public scrutiny .

This study critically examines this disjuncture. It asks: To what extent did the ECI's IT utilization enhance administrative transparency between 2000 and 2018? Where did technology serve transparency, and where did it operate opaquely? What institutional, legal, or cultural factors explain this pattern?

The period 2000-2018 is analytically significant. It begins with the nationwide rollout of EVMs following political consensus and ends with the ECI's comprehensive cybersecurity framework ahead of the 2019 general elections. It encompasses the passage of the RTI Act (2005), the 2014 "social media election," and the Supreme Court's interventions on electoral transparency.

The study adopts a critical framework that distinguishes between *operational transparency* (public visibility of electoral processes) and *institutional transparency* (accessibility of the ECI's own administrative decisions and data). The findings suggest that the ECI successfully enhanced operational transparency through IT while simultaneously erecting barriers to institutional transparency—a pattern requiring explanation and remedy.

2. Definitions

Administrative Transparency: The principle that citizens and stakeholders should have access to information about governmental processes, decisions, data, and performance metrics. Within this study, transparency is disaggregated into: (a) *proactive disclosure* (information published without request), (b) *reactive disclosure* (information provided in response to specific requests), and (c) *process transparency* (visibility into how decisions are made).

Right to Information (RTI) Act, 2005: Indian legislation establishing a legal right for citizens to access information held by public authorities, with prescribed timelines (typically 30 days) and appeal mechanisms. Public authorities are required to appoint Public Information Officers (PIOs) and accept RTI applications.

RTI Online Portal: A centralized digital platform launched by the Department of Personnel and Training (DoPT) enabling citizens to file RTI applications electronically to any central public authority. By 2017, the portal processed applications for all central government departments—except the Election Commission.

Electoral Roll: The official list of eligible voters in a constituency. Prior to computerization, electoral rolls were maintained as paper documents, prone to errors, duplication, and fraudulent entries. Computerization began in 1998 with digitization of 620 million voter records .

Elector Photo Identity Card (EPIC): A photo identification card issued to registered voters to prevent impersonation. EPIC introduction was facilitated by National Informatics Centre (NIC) technology and represented a major anti-fraud measure .

Cyber Security Regulations (CSR): A framework launched by the ECI in March 2018 governing online behavior of election officers, data protection protocols, and security audit requirements. The ECI is "probably the first Constitutional authority in the country to have its own cyber security regulations" .

Critical Information Infrastructure (CII): A designation under Section 70 of the IT Act, 2000 for computer resources whose "incapacitation or destruction shall have debilitating impact on national security, economy, public health or safety." The ECI sought this designation for its election

infrastructure in 2018, following the US precedent of designating election systems as critical infrastructure after the 2016 cyberattacks .

Model Code of Conduct Media Monitoring Tool: An information retrieval system developed by C-DAC for the ECI to scan newspapers, television channels, and social media for potential violations of the Model Code of Conduct. The tool used Natural Language Processing (NLP) to identify keywords such as "liquor," "money exchange," and "booth capturing" .

Result Display System: An IT platform for disseminating real-time election results. First piloted in 2009, expanded after successful use in Delhi assembly elections (December 2013), and deployed nationwide for the 2014 Lok Sabha elections. The system involved five IT professionals per state commission and a 12-member central team .

3. Need for the Study

This study addresses three critical gaps in existing scholarship and public discourse.

First, the "technology means transparency" assumption remains unexamined. Much of the literature on e-governance and digital democracy assumes that technology adoption inherently increases transparency. The Indian Election Commission is frequently cited as a success story of technological modernization. However, this assumption requires critical scrutiny: IT can be used to obscure as readily as to reveal. The same digital systems that enable real-time result dissemination can also enable selective information disclosure. This study tests the technology-transparency hypothesis against empirical evidence from the Indian case.

Second, transparency in election management has received disproportionate attention to voting machines rather than administrative processes. Public and scholarly debate has focused extensively on EVM security and verifiability, but far less attention has been paid to the ECI's own transparency practices—how it responds to RTI requests, whether it proactively discloses information, and how it manages the digital data it collects from millions of citizens. This study shifts focus from the technology *of elections* to the transparency *of the election management institution*.

Third, the period 2000-2018 presents a paradox requiring explanation. The ECI simultaneously achieved remarkable technological sophistication (computerized electoral rolls, real-time results, media monitoring, cybersecurity frameworks) while demonstrating transparency resistance (refusal to accept online RTI applications, non-response to nearly 2,000 citizen requests, litigation over disclosure of electoral roll cleansing software) . Understanding this paradox is essential both for evaluating the ECI's performance and for informing election management in other democracies.

Fourth, the relationship between cybersecurity and transparency requires examination. The ECI's move to secure its cyber infrastructure in 2018—including classifying election data as "critical information infrastructure"—raises questions about the trade-off between security and transparency. While legitimate security concerns exist, such designations can also be used to justify withholding information from public scrutiny. This study examines how the ECI navigated this tension.

4. Aims

The study pursues four interconnected aims:

1. **To document and critically analyze the ECI's utilization of information technology** across key electoral functions between 2000 and 2018, including electoral roll management, voter identification, result dissemination, code of conduct monitoring, and cybersecurity.

2. **To evaluate the transparency implications of IT adoption**—distinguishing between operational transparency (public visibility of electoral processes) and institutional transparency (accessibility of ECI administrative data and decisions).
3. **To examine the ECI's compliance with and interpretation of the Right to Information Act, 2005,** including acceptance of online RTI applications, response rates, and proactive disclosure practices.
4. **To identify factors explaining the disjuncture between technological advancement and transparency enhancement,** including institutional culture, legal interpretations, political pressures, and legitimate security concerns.

5. Objectives

Objective Number	Objective Description
O1	Trace the evolution of IT utilization by the ECI from 2000 to 2018, identifying key technology adoption milestones and their administrative rationales
O2	Analyze the technological infrastructure for electoral roll computerization, including the role of National Informatics Centre (NIC) in digitizing 620 million voter records
O3	Examine the development and deployment of real-time result display systems (2009 pilot, 2013 Delhi expansion, 2014 national deployment)
O4	Evaluate the ECI's implementation of online RTI mechanisms, including training of officials and actual response rates
O5	Investigate the ECI's cybersecurity framework development (2017-2018), including appointment of CISO, regional training workshops, and critical infrastructure designation
O6	Analyze legal challenges to ECI technology use regarding transparency, including Telangana High Court cases on electoral roll cleansing software
O7	Assess the ECI's social media monitoring capabilities, including the C-DAC NLP tool for Model Code of Conduct enforcement
O8	Critically evaluate the transparency implications of the ECI's technology choices and data management practices

6. Hypothesis

The study advances three interconnected hypotheses:

H1 (Operational Transparency Hypothesis): The ECI's IT utilization significantly enhanced *operational* transparency—citizens gained real-time visibility into electoral processes, including voter registration status, polling station locations, and vote counting.

H2 (Institutional Transparency Hypothesis): The ECI's IT utilization did *not* significantly enhance *institutional* transparency—the Commission maintained or increased barriers to accessing its own administrative decisions, data, and internal processes, particularly through non-acceptance of online RTI applications and selective disclosure practices.

H3 (Security Justification Hypothesis): The ECI increasingly invoked cybersecurity concerns to justify transparency limitations, particularly after 2017, creating a framework where security and transparency were framed as trade-offs requiring resolution in favor of security.

7. Literature Search Strategy

The literature for this study was identified through a multi-pronged search strategy.

Academic Databases: Systematic searches were performed in Scopus, Web of Science, JSTOR, Google Scholar, and SSRN using Boolean operators: ("Election Commission of India" OR "ECI") AND ("transparency" OR "right to information" OR "RTI") AND ("information technology" OR "e-governance" OR "digital"). Additional searches focused on ("electoral roll" OR "voter registration") AND ("computerization" OR "digitization") AND ("India").

Legal Databases: Manupatra and SCC Online were searched for judgments pertaining to ECI transparency obligations, including Right to Information appeals and cases challenging electoral roll software.

Government and Institutional Sources: Election Commission of India annual reports (2000-2018), National Informatics Centre publications on electoral roll management, C-DAC documentation on media monitoring tools, PM India announcements on EVM procurement.

News Archives: The Hindu, Indian Express, Economic Times, and The Telegraph archives were searched for coverage of ECI technology initiatives, RTI controversies, and cybersecurity developments.

Civil Society Reports: Association for Democratic Reforms (ADR) publications on electoral transparency, FACTLY investigations on RTI online non-acceptance, and PRS Legislative Research analyses of election law amendments.

Inclusion Criteria: Sources were included if they: (a) addressed ECI technology deployment with specificity; (b) provided empirical data on transparency practices (RTI response rates, proactive disclosure); (c) offered legal analysis of transparency obligations; or (d) originated from authoritative institutional sources (ECI, NIC, C-DAC) or established news organizations.

8. Research Methodology

8.1 Research Design

This study employs a **qualitative critical case study design** with comparative temporal analysis. The single overarching case is "ECI administrative transparency and IT utilization 2000-2018." Temporal comparison examines: Phase 1 (2000-2005): pre-RTI Act technology adoption; Phase 2 (2005-2010): RTI implementation and early digital systems; Phase 3 (2010-2014): social media election and result display; Phase 4 (2014-2018): cybersecurity framework and transparency tensions.

8.2 Case Selection Rationale

The Election Commission of India is selected as a critical case for four reasons: (1) It is constitutionally mandated to conduct elections for the world's largest democracy, making its transparency practices globally significant; (2) It has been repeatedly cited as a model of electoral administration, meriting

critical examination; (3) It experienced rapid technology adoption during 2000-2018, enabling study of technology-transparency relationships; (4) It has been subject to sustained civil society scrutiny, generating rich documentary evidence on transparency practices.

8.3 Data Sources

Data Type	Sources	Period
Technology deployment records	ECI annual reports, NIC publications, PM India announcements	2000-2018
RTI compliance data	DoPT RTI Online statistics, FACTLY investigations, RTI response letters	2015-2018
Legal judgments	Telangana High Court, Supreme Court of India	2010-2018
Media monitoring documentation	C-DAC technical publications, DNA coverage	2014
Cybersecurity framework	ECI Cyber Security Regulations, The Indian Express investigation	2017-2018
Electoral roll data	NIC Informatics editorial, ECI status papers	1998-2018

8.4 Analytical Framework

Data analysis proceeds through three phases:

Phase 1: Technology mapping. Each major IT system deployed by the ECI between 2000-2018 is identified and categorized by function (voter registration, identification, result dissemination, enforcement, security).

Phase 2: Transparency audit. For each technology, transparency implications are assessed across three dimensions: (a) Does it increase or decrease public visibility? (b) Does it facilitate or hinder citizen information access? (c) Are there transparency deficits introduced by the technology itself?

Phase 3: Institutional explanation. Patterns of transparency enhancement or restriction are analyzed for explanatory factors: institutional culture, legal interpretations, political pressures, security justifications, and resource constraints.

8.5 Limitations

The study acknowledges several limitations. First, access to internal ECI decision-making records is not available; analysis relies on published reports, legal proceedings, and investigative journalism. Second, the study period ends in 2018, excluding post-2019 developments. Third, the research does not include primary interviews with ECI officials, RTI applicants, or system developers. Fourth, quantitative analysis of RTI response rates is limited by incomplete data disclosure.

9. History of IT Utilization in Election Commission of India (1998-2018)

9.1 Pre-Computerization Era: Paper-Based Electoral Management (1950-1998)

For nearly five decades following independence, the Election Commission managed electoral rolls entirely through paper-based processes. Voter lists were maintained as physical registers, updated manually, and subject to errors, duplications, and fraudulent entries. Eligible voters were identified primarily through self-declaration, enabling impersonation. The scale of India's electorate made paper-based management increasingly unsustainable: by 1998, the voter list exceeded 620 million names .

9.2 Computerization of Electoral Rolls (1998-2000)

A transformative milestone occurred in 1998 when the National Informatics Centre (NIC) undertook the computerization of electoral rolls. This monumental task involved digitizing 620 million voter records—the largest such exercise globally . The digitization promised three transparency improvements: (a) reduction of errors and duplications through systematic data management; (b) faster updates and corrections; (c) easier public access to voter rolls.

The computerization facilitated the introduction of Elector Photo Identity Cards (EPIC), which began issuance around this period. EPICs provided visual identification to prevent impersonation, though their rollout was gradual and faced logistical challenges .

9.3 Electronic Voting Machine Rollout (2000-2004)

While EVMs themselves are not primarily transparency tools, their deployment during this period is relevant to the broader IT transformation narrative. Following political consensus in 1998, EVMs were used in 16 constituencies in 1999, expanded to 46 parliamentary constituencies in 1999, and deployed nationwide for the 2004 general elections . The 2001 state assembly elections in Tamil Nadu, Kerala, Puducherry, and West Bengal were the first to abandon paper ballots entirely .

The EVM rollout involved two public sector manufacturers: Bharat Electronics Limited (BEL) and Electronics Corporation of India Limited (ECIL). The Election Commission maintained that EVMs provided operational transparency through reduced fraud, though critics argued they created a "black box" problem .

9.4 Electoral Rolls Management System and EPIC Integration (2005-2010)

Following the computerization milestone, NIC developed the Electoral Rolls Management System, a comprehensive platform for preparation, revision, and maintenance of electoral rolls. This system streamlined updates and enabled systematic cleaning of duplicate entries .

The period also saw expanded EPIC issuance. However, full coverage remained elusive; by 2019, the Supreme Court was still hearing cases regarding Aadhaar linkage and voter list cleansing .

9.5 RTI Act Implementation and Early Digital Disclosure (2005-2010)

The Right to Information Act came into force in October 2005, requiring all public authorities—including the Election Commission—to appoint Public Information Officers, accept RTI applications, and proactively disclose information. The ECI complied with basic requirements, maintaining physical RTI application acceptance and publishing some information on its website.

However, transparency advocates noted that the ECI was not among the early adopters of the online RTI portal launched by the Department of Personnel and Training. This portal enabled citizens to file RTI applications electronically to any central public authority—but the ECI remained outside this system for years .

9.6 Result Display System: Pilot and Expansion (2009-2014)

The Election Commission's collaboration with the Press Information Bureau (PIB) on result dissemination began as a pilot project in 2009. At that time, results were available online for only a limited number of states. The system represented a significant operational transparency enhancement: citizens could follow vote counting in real-time rather than waiting for newspaper reports or television broadcasts .

The Delhi assembly elections of December 2013 proved pivotal. The result display system was deployed successfully, providing reliable real-time updates. Buoyed by this success, the ECI deployed the system nationwide for the 2014 Lok Sabha elections .

The technical architecture involved five IT professionals in each state commission who received vote count updates from returning officers. These professionals generated HTML of the results and transmitted them to the central ECI office, where a 12-member team managed the result display system in coordination with PIB. As V.N. Shukla, Director of IT at ECI, stated: "It was an extremely tiring and exhaustive process, but equally rewarding" .

9.7 Model Code of Conduct Media Monitoring (2014)

A significant innovation for the 2014 general elections was the development of an information retrieval system to monitor Model Code of Conduct violations. The ECI partnered with the Centre for Development of Advanced Computing (C-DAC) to create a tool that scanned news channels, newspapers, web portals, and social media platforms for suspected violations .

The system used Natural Language Processing (NLP) techniques and was "adept in recognising Indian languages." Keywords such as "liquor," "money exchange," "booth capturing," and other terms were fed into the system to trace relevant content. When suspected violations were identified, the tool generated reports in English and forwarded them to EC observers for assessment .

Prof. Rajat Moona, Director General of C-DAC, explained the rationale: "There are several incidents of violation of model code of conduct, which go unnoticed during the elections. So there needs to be a system, which will keep track on the identified textual-data from newspaper websites, political leaders and party websites and social media" . The system was piloted in Madhya Pradesh before national deployment.

9.8 Transparency Tensions: RTI Online Non-Acceptance (2015-2018)

Despite its technological sophistication in electoral operations, the ECI demonstrated significant resistance to online transparency mechanisms. As FACTLY reported in November 2017, the ECI refused to accept RTI applications filed through the RTI Online portal, despite having been included as a public authority on the portal and having trained its officials on the system .

Documents obtained under the RTI Act revealed that in March 2016, Mr. S.K. Mishra from the ECI sent an email to the RTI-PMU regarding linking ECI with the RTI Online portal, nominating Mr. Tapas Kumar as nodal officer. In May 2016, 25 ECI officials were trained on the RTI Online portal, and they even suggested functional improvements .

Yet by September 2017, a total of **1,951 RTI applications** filed online to the ECI had received **no response whatsoever**. Additionally, **595 first appeals** filed online were also pending. The ECI continued to process paper RTI applications (approximately 150 per month) but ignored the online channel entirely, despite having integrated it .

The FACTLY investigation noted: "Nothing explains the reluctance of ECI... It is indeed an irony that such a progressive institution refuses to make it easy for citizens to exercise their Right to Information... Knowingly, the ECI is scuttling transparency" .

9.9 Legal Challenges to Electoral Roll Software (2018-2019)

The transparency of ECI's software systems was challenged in the Telangana High Court in March 2019. K. Srinivas, an IIT-Chennai engineering graduate, filed a Public Interest Litigation (PIL) arguing that the software used by the ECI to prepare and maintain electoral rolls was "neither transparent nor public." He sought disclosure of the source code, algorithms, and data audit logs .

The High Court dismissed the interim plea, noting that the petitioner's request was "contradictory to the very plank on which the main writ petition was founded"—specifically, the petitioner had also

argued that state governments sharing information with the ECI infringed privacy rights. The Court declined to order disclosure of source code or forensic audit, though it left the question to be examined at final disposal .

This case illustrates the tension between transparency demands and ECI's resistance to disclosing the inner workings of its software systems—a pattern mirroring the EVM source code non-disclosure controversy.

9.10 Cybersecurity Framework and Critical Infrastructure Designation (2017-2018)

From 2017 onward, the ECI initiated an unprecedented cybersecurity drive. The catalyst was global concern over election interference following allegations of Russian meddling in US and European elections. As an ECI official stated: "A cyber attack, irrespective of the actual damage caused, spreads misinformation and can delegitimise a democratic process. Hence, for the first time, cyber security is part of election planning" .

Key measures included:

Appointment of Chief Information Security Officer (CISO): A dedicated CISO was appointed at ECI headquarters in December 2017, along with Cyber Security Nodal Officers (CSNO) in each state .

Cyber Security Regulations (CSR): Launched in March 2018, these regulations guide officer online behavior, prohibit personal device use for protected information, and require electoral roll provision in non-editable formats. "ECI is probably the first Constitutional authority in the country to have its own cyber security regulations" .

Training Programs: Three regional workshops (north, south, central India) were conducted starting June 2018, training electoral registration officers, district election officers, and chief electoral officers in "cyber hygiene." Seven additional workshops including secure coding practices were planned .

Mandatory Security Audits: Annual third-party security audits of poll-related websites and applications became mandatory. Poll-bound states initiated security audits, SSL implementation, and disaster recovery plans .

Ghost Application Takedown: The ECI began identifying and removing applications that mimicked its logo and offered fraudulent electoral services .

Critical Information Infrastructure (CII) Designation: Perhaps most significantly, the ECI sought to have its election infrastructure recognized as "critical information infrastructure" under Section 70 of the IT Act. This designation would provide additional funding, resources, and higher punishment for unauthorized access. The US had designated election infrastructure as critical following the 2016 cyberattacks, setting a precedent .

9.11 VVPAT Procurement and Transparency Enhancement (2016-2018)

The introduction of Voter Verifiable Paper Audit Trail (VVPAT) systems represented a major transparency enhancement for EVM-based elections. Following the Supreme Court's 2013 directive, the ECI phased in VVPAT deployment. In July 2016, the Union Cabinet approved procurement of 550,000 Ballot Units and 545,000 Control Units, with allocation of Rs. 25 crore for R&D to reduce costs. VVPAT procurement was addressed in subsequent years .

The phasing out of obsolete EVMs procured during 2000-2005 was also approved, addressing concerns about aging hardware .

10. Strong Points of IT Utilization for Election Commission Transparency

10.1 Real-Time Result Dissemination

The result display system represents a genuine transparency achievement. For the first time in Indian electoral history, citizens could follow vote counting in real-time from any internet-connected device.

This compressed the information asymmetry between election officials and the public, reduced speculation and rumor, and enabled civil society to perform parallel vote tabulation. The system's reliability during the 2014 elections—when 1.4 million EVMs were counted simultaneously—demonstrated sophisticated IT management .

10.2 Computerized Electoral Rolls with Public Access

The digitization of 620 million voter records transformed electoral roll management. Citizens could now verify their registration status online, identify polling station locations, and request corrections electronically. This reduced the burden on election officials and empowered voters to ensure their inclusion. The Electoral Rolls Management System streamlined the revision process, enabling more frequent updates and reducing the window for fraudulent entries .

10.3 EPIC Integration Combating Impersonation

While not purely a transparency tool, the EPIC system—enabled by IT infrastructure—enhanced electoral integrity. Photo identification at polling stations created a verifiable link between voter identity and voter record. This made impersonation more difficult and provided a mechanism for challenging fraudulent votes .

10.4 Model Code of Conduct Monitoring

The C-DAC media monitoring tool represented an innovative application of natural language processing to electoral enforcement. By scanning millions of news articles, social media posts, and television transcripts for code of conduct keywords, the system enabled the ECI to detect violations that would otherwise go unnoticed. The tool's ability to recognize Indian languages was particularly significant given India's linguistic diversity .

For transparency purposes, this system creates a record of potential violations that can be audited. The reports generated are forwarded to EC observers, creating accountability for enforcement decisions.

10.5 Proactive Cybersecurity Framework

The ECI's development of comprehensive cybersecurity regulations positioned it as a leader among constitutional authorities. By appointing a CISO, training officers in cyber hygiene, and mandating third-party audits, the ECI demonstrated awareness of emerging threats. The designation of election infrastructure as critical information infrastructure—if approved—would provide resources for protection that smaller democracies cannot afford .

From a transparency perspective, the cybersecurity framework includes provisions that enhance accountability: mandatory audits, non-editable electoral roll formats, and prohibition of personal device use for official communication. These measures reduce the scope for unauthorized manipulation and create audit trails.

10.6 EVM-VVPAT Integration Enhancing Verifiability

While the VVPAT system is primarily associated with EVM security, it represents a transparency enhancement for the voting process. Voters can visually verify their vote for seven seconds, creating a paper trail that can be audited. The Supreme Court's 2013 directive mandating VVPAT was a response to transparency demands, and the ECI's phased implementation demonstrated institutional responsiveness .

10.7 Swift Response to Global Cyber Threats

The ECI's October 2018 cybersecurity initiative demonstrated institutional learning from international events. Following allegations of Russian interference in US elections and concerns about election infrastructure vulnerabilities globally, the ECI proactively strengthened its defenses. The official statement—"A cyber attack, irrespective of the actual damage caused, spreads misinformation and

can delegitimise a democratic process"—showed sophisticated understanding of election security beyond technical concerns .

10.8 Transparency in EVM Challenges

Following allegations of EVM tampering after the 2017 Uttar Pradesh state elections, the ECI issued a public challenge: anyone who could demonstrate EVM tampering would be rewarded. While the challenge did not result in successful tampering demonstrations, the act of issuing it represented a transparency posture—an invitation to skepticism to prove itself .

10.9 Nodal Officer Structure for RTI

The ECI did appoint RTI nodal officers and participated in training sessions on the RTI Online portal. The nomination of Mr. Tapas Kumar as nodal officer and the training of 25 officials in May 2016 demonstrated institutional recognition of RTI obligations, even if implementation was incomplete .

10.10 Polling Personnel Management Systems

NIC's systems for drafting and deployment of polling personnel, randomization of EVMs, and appointment of sector and zonal magistrates improved operational transparency. These systems reduced discretion in personnel allocation, potentially reducing opportunities for partisan influence .

10.11 Live Webcasting from Polling Stations

NIC facilitated live webcasting and video streaming from polling stations, allowing ECI officials, political parties, and the public to observe polling processes remotely. This innovation enhanced trust by enabling real-time verification of polling station conduct .

10.12 Geographic Information Systems (GIS) for Election Management

NIC employed GIS for polling station rationalization and election data visualization. This provided spatial transparency—public visibility into where polling stations were located, how they were allocated, and what demographic patterns characterized constituencies .

11. Weak Points of IT Utilization for Election Commission Transparency

11.1 Systematic Non-Acceptance of Online RTI Applications

The most significant transparency failure is the ECI's refusal to accept RTI applications filed through the RTI Online portal. Despite being included as a public authority on the portal, despite training 25 officials on its use in May 2016, and despite approximately 1,951 online applications being filed by citizens expecting responses, the ECI simply did not respond to any of them. Additionally, 595 first appeals were pending without response .

This cannot be explained by technical incapacity—the ECI demonstrated sophisticated IT capabilities across multiple domains. The explanation appears to be institutional choice: the ECI preferred to restrict RTI access to the slower, more burdensome paper channel. This choice directly contravenes the spirit of the RTI Act, which aims to make information access "easy, inexpensive, and expeditious" . As FACTLY noted: "Knowingly, the ECI is scuttling transparency" .

11.2 Lack of Transparency in Electoral Roll Cleansing Software

The Telangana High Court case regarding electoral roll software revealed significant transparency deficits. The petitioner, an IIT graduate, argued that the software used to prepare and maintain electoral rolls was "neither transparent nor public," potentially enabling mass deletions of voters without accountability .

While the Court dismissed the interim plea, the underlying concern remains valid: citizens have no visibility into the algorithms and audit logs that determine whether they remain on the voter list. The ECI's refusal to disclose source code or provide data audit logs mirrors its position on EVM source code—security and proprietary concerns are invoked to justify opacity.

11.3 Selective Proactive Disclosure

While the ECI publishes substantial information on its website, the scope of proactive disclosure is limited. Comparative analysis with election commissions in other democracies (Canada, UK, Australia) reveals that the ECI discloses less information about its own internal decision-making, administrative expenditures, and technology procurement details. The distinction between *operational transparency* (how elections work) and *institutional transparency* (how the ECI works) is significant: the former is high, the latter low.

11.4 Delayed VVPAT Implementation

While VVPAT ultimately enhanced transparency, its implementation was delayed and resisted. The Supreme Court had to compel the ECI to introduce VVPAT in 2013, and full deployment took years. The ECI's initial resistance to VVPAT—citing cost and logistical challenges—suggested institutional preference for efficiency over verifiability .

11.5 EVM Source Code Non-Disclosure

The ECI's refusal to disclose EVM source code remains a persistent transparency concern. While security arguments for non-disclosure have some validity, the complete absence of independent source code review creates an opaque system. The German Constitutional Court's reasoning in discontinuing EVMs—that citizens cannot verify what they cannot inspect—applies equally to India .

11.6 Limited Scope of VVPAT Verification

Even with VVPAT deployed, the ECI limits manual verification to a small fraction (approximately 5%) of VVPAT slips. This means systematic manipulation affecting all machines would not be detected. Transparency advocates have consistently demanded expanded verification, which the ECI has resisted as "regressive" .

11.7 Lack of Transparency in EVM Storage and Custody

Between elections, EVMs remain in storage under ECI custody. The public has no visibility into storage conditions, access logs, or security protocols. While the ECI asserts that protocols are stringent, the opacity of storage arrangements creates space for suspicion—regardless of actual security.

11.8 Cybersecurity as Transparency Limitation Justification

The ECI's cybersecurity framework, while necessary, also provides new justifications for limiting transparency. Classification of election data as "critical information infrastructure" could be used to deny RTI requests on national security grounds. The prohibition on personal device use and non-editable electoral roll formats serve legitimate security purposes, but also reduce opportunities for independent verification.

The risk is that "security" becomes a catch-all justification for opacity, without independent scrutiny of whether claimed threats justify specific limitations.

11.9 Non-Transparent Procurement Processes

The procurement of EVMs, VVPATs, and other technology systems involves substantial public expenditure—Rs. 77007 per Ballot Unit and Rs. 93007 per Control Unit in 2016, with Rs. 25 crore allocated for R&D . However, procurement processes lack transparency. Competitive bidding is limited (BEL and ECIL are the sole suppliers), and contract details are not publicly disclosed. This creates potential for inefficiency and reduces public accountability for technology spending.

11.10 Lack of Public Access to Media Monitoring Data

The C-DAC media monitoring tool generates reports on potential code of conduct violations, but these reports are not publicly accessible. Citizens cannot verify whether reported violations were investigated appropriately or whether enforcement was even-handed. The tool serves internal ECI enforcement but does not generate public transparency.

11.11 Limited Accessibility of Digital Services

While the ECI has developed sophisticated digital services, accessibility remains uneven. Voters in rural areas, elderly voters, and voters with disabilities may face barriers accessing online services. The digital divide means that transparency enhancements benefiting urban, literate, tech-savvy citizens may not reach all voters equally.

11.12 No Independent Audit of ECI Transparency Practices

Unlike some election commissions that undergo independent transparency audits (e.g., by national audit offices or civil society organizations), the ECI has not established regular independent assessment of its transparency practices. Self-assessment is not a substitute for external verification.

12. Current Trends in ECI IT and Transparency (2000-2018)

[Note: While the study period ends in 2018, understanding contemporary trends provides context for evaluating the 2000-2018 period.]

12.1 Continued RTI Online Resistance

The pattern of RTI online non-acceptance documented in 2017 persisted beyond 2018. Subsequent investigations have confirmed that the ECI continues to process paper RTI applications while systematically ignoring online filings, despite repeated civil society appeals and despite the DoPT's mandate that all central public authorities accept online RTI applications.

12.2 Supreme Court Oversight of VVPAT Verification

Following the 2019 general elections, the Supreme Court has maintained active oversight of EVM-VVPAT verification. Opposition parties have continued demanding expanded verification, and the Court has sought ECI explanations. This judicial pressure may eventually force greater transparency.

12.3 Expansion of Cybersecurity Framework

Post-2018, the ECI has expanded its cybersecurity infrastructure. The cybersecurity regulations launched in 2018 have been refined, and third-party audits have become routine. The critical information infrastructure designation remains under consideration.

12.4 Mobile Voting Pilots

Recent pilots of mobile voting applications (using blockchain and facial recognition) raise new transparency questions. Unlike physical EVMs, mobile voting systems are inherently networked, creating new attack surfaces and transparency challenges.

12.5 AI in Campaign Monitoring

The ECI has begun exploring AI tools for campaign monitoring beyond the 2014 NLP system. Generative AI and deepfake detection pose new challenges for code of conduct enforcement, requiring continuous technological adaptation.

12.6 Continued Partisan Debates on EVM Transparency

Political parties have maintained their pattern of "convenient skepticism"—supporting EVMs when in power, questioning them when in opposition. This partisan dynamic prevents stable resolution of transparency demands.

12.7 International Comparative Developments

Globally, election transparency debates have intensified. The US designation of election infrastructure as critical (2017) set precedent that India followed. European countries continue to diverge, with some expanding e-voting and others discontinuing it.

13. Discussion

13.1 The Technology-Transparency Paradox

The central finding of this study is the disjuncture between the ECI's technological sophistication and its administrative opacity. The same institution that deployed real-time result display systems and NLP-based media monitoring refused to accept online RTI applications. The same Commission that invested in cybersecurity infrastructure resisted disclosing electoral roll software audit logs.

This paradox requires explanation. One interpretation is that technology serves *operational* efficiency but not *institutional* accountability. The ECI adopted technology that made elections run smoothly, reduced its administrative burden, and enhanced its public reputation. It did not adopt technology that would subject its own processes to external scrutiny. The distinction is not accidental—it reflects institutional priorities.

Another interpretation is that the ECI genuinely believes in transparency but faces legitimate security constraints. The RTI online portal may present cybersecurity risks that the ECI is not equipped to manage. Electoral roll software may contain proprietary elements that cannot be disclosed. EVM source code disclosure would create genuine vulnerabilities.

However, this security justification is undermined by the ECI's selective application. The RTI online portal is used by all other central government departments—if it is secure enough for the Ministry of Finance or the Home Ministry, why not for the ECI? The portal's security has been audited and approved. The ECI's rejection cannot be convincingly explained by security concerns.

13.2 Institutional Culture and Transparency Resistance

The ECI has historically viewed itself as an autonomous constitutional authority with minimal accountability obligations beyond those explicitly mandated. This institutional culture—developed over decades of defending electoral integrity against political pressures—may generate resistance to transparency that appears as external interference.

The ECI's transparency resistance may also reflect concern about administrative burden. Processing RTI applications (online or paper) requires resources. The ECI may calculate that limiting transparency reduces its workload, enabling focus on core electoral functions. However, this calculation is inconsistent with its willingness to invest in sophisticated IT systems for other purposes.

13.3 The RTI Online Case: A Transparency Failure

The non-acceptance of online RTI applications is the most indefensible transparency failure documented in this study. The facts are damning: the ECI trained officials on the portal, was included as a public authority, received 1,951 applications, and responded to none. First appeals (595 of them) also received no response .

This constitutes *systematic non-compliance* with the RTI Act, not mere administrative delay. The Act does not distinguish between online and paper applications; both are legally equivalent. By ignoring one channel entirely, the ECI violates citizens' legal rights.

The ECI's conduct is particularly troubling given its constitutional mandate to uphold democratic values. The right to information is fundamental to democratic accountability. An institution that denies this right—especially an election management body—undermines the democratic order it is charged with protecting.

13.4 Operational vs. Institutional Transparency

The distinction between operational and institutional transparency helps make sense of the ECI's pattern. Operational transparency—visibility into electoral processes—has been enhanced significantly. Citizens can verify registration, locate polling stations, and track results in real-time. This transparency serves the ECI's mission and enhances its reputation.

Institutional transparency—visibility into ECI's own decision-making, expenditures, software systems, and internal processes—has not been enhanced. The ECI resists revealing how it makes decisions, what

software algorithms do, or how procurement funds are spent. This transparency would subject the ECI to scrutiny, potentially revealing inefficiency or error.

The pattern suggests that the ECI adopts technology that serves its mission and enhances its public standing, while resisting technology that would make it accountable. This is not necessarily malicious—institutions naturally resist accountability mechanisms. But it is a transparency deficit requiring correction.

13.5 The Cybersecurity-Transparency Trade-Off

The ECI's cybersecurity framework, while necessary, creates new tensions with transparency. The designation of election data as "critical information infrastructure" could be used to deny RTI requests on national security grounds. The prohibition on personal device use and non-editable formats reduces opportunities for independent verification.

The challenge is to balance legitimate security needs with transparency requirements. The ECI's current approach appears to prioritize security over transparency, with limited independent oversight of that trade-off. The absence of a statutory framework governing when security can override transparency leaves the ECI with excessive discretion.

13.6 Legal and Judicial Oversight

The courts have played an ambivalent role in ECI transparency. The Supreme Court compelled VVPAT introduction, enhancing verifiability. However, the Telangana High Court declined to order disclosure of electoral roll software source code, deferring to ECI expertise . Judicial deference to the ECI has limits: courts recognize the Commission's specialized competence but also enforce statutory transparency obligations.

The RTI Act's non-compliance has not been litigated effectively. No major case has compelled the ECI to accept online RTI applications. This may reflect the difficulty of enforcing transparency obligations against a powerful constitutional authority.

13.7 Comparative Perspective

Comparing the ECI with election commissions in other democracies reveals distinctive patterns. The Election Commission of India is more technologically advanced than most but less transparent about its own operations than some. The UK Electoral Commission publishes detailed expenditure data and undergoes independent audit. The Canadian Elections Act mandates proactive disclosure of a wide range of information. The ECI lags on these dimensions.

However, India's scale creates unique challenges. No other election commission manages an electorate of 900 million. The ECI's technology investments are enormous, and transparency mechanisms that work for smaller democracies may not scale. This is a legitimate consideration, but it does not justify non-acceptance of online RTI applications—a mechanism that scales easily.

14. Results

14.1 Technology Adoption Outcomes

Result 1.1 (Electoral Roll Computerization): By 2018, all 620 million voter records had been digitized through NIC's Electoral Rolls Management System. Online voter registration verification became available nationwide .

Result 1.2 (Result Display System): The real-time result display system was deployed nationwide for the 2014 general elections, providing hourly updates to millions of citizens. The system involved 5 IT professionals per state commission and a 12-member central team .

Result 1.3 (Media Monitoring): The C-DAC NLP-based media monitoring tool was deployed for the 2014 general elections, scanning multiple Indian languages for code of conduct violations .

Result 1.4 (Cybersecurity Framework): By October 2018, the ECI had appointed a CISO, established CSNOs in each state, launched cybersecurity regulations, mandated third-party audits, and trained officers through regional workshops .

Result 1.5 (EVMs and VVPATs): By 2018, EVMs were used nationwide, with VVPATs deployed in phases following the 2013 Supreme Court directive. Procurement of 550,000 Ballot Units and 545,000 Control Units was approved in 2016 .

14.2 Transparency Outcomes

Result 2.1 (RTI Online Compliance): As of September 2017, 1,951 online RTI applications and 595 first appeals filed to the ECI had received no response. The ECI continued to accept paper applications but systematically ignored the online channel .

Result 2.2 (Proactive Disclosure): The ECI proactively discloses operational information (voter registration, polling stations, results) but limited institutional information (internal decisions, expenditures, software specifications).

Result 2.3 (Legal Challenges): The Telangana High Court declined to order disclosure of electoral roll software source code in March 2019, deferring to ECI on the interim application .

Result 2.4 (Operational vs. Institutional Transparency): Operational transparency (visibility into electoral processes) was significantly enhanced; institutional transparency (visibility into ECI's own operations) was not enhanced and in some respects (online RTI) regressed.

14.3 Hypothesis Testing Summary

Hypothesis	Finding	Supported?
H1(Operational Transparency)	IT utilization significantly enhanced operational transparency—real-time results, voter registration verification, polling station location	Yes
H2(Institutional Transparency)	IT utilization did not enhance institutional transparency; ECI resisted online RTI and software disclosure	Yes
H3(Security Justification)	ECI increasingly invoked cybersecurity to justify transparency limitations after 2017	Partially supported

15. Conclusion

This critical study has examined the relationship between information technology utilization and administrative transparency in the Election Commission of India from 2000 to 2018. The findings reveal a fundamental paradox: the ECI achieved remarkable technological sophistication in electoral operations while simultaneously demonstrating resistance to transparency mechanisms that would subject its own processes to public scrutiny.

The ECI's achievements in operational transparency are genuine and significant. Citizens can verify their voter registration online, locate polling stations, and track election results in real-time. The result display system deployed for the 2014 elections represented a major advance in public access to electoral information. The media monitoring tool enabled enforcement of the Model Code of Conduct at scale. The cybersecurity framework positioned India as a leader in election protection.

However, these achievements are undermined by systematic transparency deficits. The ECI's refusal to accept online RTI applications—with nearly 2,000 citizen requests ignored—constitutes a violation of legal rights and a betrayal of democratic principles. The resistance to disclosing electoral roll software

audit logs and EVM source code creates opacity that fuels suspicion rather than trust. The invocation of cybersecurity to justify transparency limitations—while sometimes legitimate—risks becoming a catch-all excuse for opacity.

The central lesson of this study is that technology alone does not guarantee transparency. IT can be used to reveal or to obscure, depending on institutional choices, legal frameworks, and political will. The ECI's pattern—enhancing operational transparency while resisting institutional transparency—reflects institutional priorities and culture. Technology serves those priorities; it does not autonomously produce transparency.

Looking forward, three reforms are essential. First, the ECI must accept online RTI applications and respond within statutory timelines. No legitimate justification exists for treating online and paper applications differently. Second, the ECI should adopt "transparency by design" principles, embedding auditability and public disclosure into software systems from the outset. Third, independent oversight of ECI transparency practices—through parliamentary committee, national audit office, or civil society audit—should be established.

The Election Commission of India remains one of the world's most capable election management bodies. Its technological achievements are globally recognized. But administrative transparency is not a luxury—it is a democratic necessity. The ECI must extend the same technological sophistication that serves electoral efficiency to the project of its own accountability.

16. Suggestions and Recommendations

Based on the findings of this study, the following recommendations are offered.

16.1 Recommendations for the Election Commission

Recommendation 1: Accept and respond to online RTI applications immediately. The ECI has no legitimate justification for ignoring the RTI Online portal. It should publicize that online applications are accepted, assign dedicated personnel to process them, and report response rates transparently.

Recommendation 2: Publish annual transparency reports. The ECI should publish annual reports detailing: number of RTI applications received (online and paper), average response times, appeals filed and outcomes, proactive disclosures made, and information requests denied with reasons.

Recommendation 3: Establish transparency-by-design principles for software systems. All electoral software should be designed with auditability and public disclosure as requirements. Data audit logs should be retained and made available for independent inspection under appropriate confidentiality arrangements.

Recommendation 4: Create an independent transparency advisory committee. This committee—comprising civil society representatives, technical experts, and retired judges—should review ECI transparency practices, receive complaints, and recommend improvements.

Recommendation 5: Disclose electoral roll software audit logs. The ECI should provide independent auditors access to electoral roll software audit logs to verify that deletions and modifications follow legal procedures. Summary findings should be published.

Recommendation 6: Expand VVPAT verification incrementally. While 100% verification may be impractical, the ECI should increase verification rates and accept independent observation of verification processes.

Recommendation 7: Clarify cybersecurity-transparency trade-offs publicly. When security concerns justify transparency limitations, the ECI should document the specific threat, the proportionality of the response, and the duration of the limitation. These justifications should be subject to independent review.

16.2 Recommendations for Policymakers and Legislators

Recommendation 8: Amend the RTI Act to mandate online acceptance. The RTI Act should be amended to explicitly require all public authorities to accept applications through the central online portal, with penalties for non-compliance.

Recommendation 9: Establish parliamentary oversight of ECI transparency. A Parliamentary Committee on Electoral Transparency should review ECI compliance with transparency obligations and recommend statutory reforms.

Recommendation 10: Enact legislation on election technology transparency. A comprehensive Election Technology Transparency Act should require source code escrow, independent security audits with public summaries, and mandatory disclosure of audit logs.

16.3 Recommendations for the Supreme Court

Recommendation 11: Clarify ECI transparency obligations. The Supreme Court should issue guidance on the scope of ECI transparency obligations under the RTI Act, addressing whether security classifications can override disclosure requirements and what procedural protections apply.

Recommendation 12: Establish transparency audit mechanism. The Court should consider appointing a commission to audit ECI transparency practices and report on compliance with statutory obligations.

16.4 Recommendations for Civil Society

Recommendation 13: Litigate RTI online non-acceptance. Civil society organizations should file strategic litigation compelling ECI acceptance of online RTI applications, seeking mandamus and penalties for non-compliance.

Recommendation 14: Conduct independent transparency assessments. Organizations like ADR and FACTLY should publish regular transparency scorecards evaluating ECI performance across multiple dimensions.

Recommendation 15: Develop citizen education on RTI rights. Many citizens remain unaware that online RTI applications to ECI are not processed. Civil society should educate applicants to use paper channels or alternative strategies.

17. Future Scope

This study opens several avenues for future research.

Future Scope 1: Post-2018 Transparency Developments. Researchers should extend the analysis to cover the 2019 and 2018 general elections, examining: (a) whether the ECI eventually accepted online RTI applications; (b) how cybersecurity frameworks evolved; (c) whether judicial oversight compelled greater transparency.

Future Scope 2: Comparative Analysis of Election Commissions. Comparative research should examine transparency practices across election commissions in major democracies (India, US, UK, Canada, Australia, Brazil), identifying institutional, legal, and cultural factors associated with greater transparency.

Future Scope 3: RTI Non-Compliance Patterns. Systematic research on RTI non-compliance across Indian public authorities—not just the ECI—would reveal whether the ECI's pattern is exceptional or typical.

Future Scope 4: Transparency Implications of Emerging Technologies. Blockchain voting, mobile voting applications, and AI-based monitoring systems raise new transparency questions. Research should address these prospectively, before technologies are deployed at scale.

Future Scope 5: Citizen Perceptions of ECI Transparency. Survey research on voter trust in ECI transparency, awareness of RTI rights, and experiences with information requests would complement institutional analysis.

Future Scope 6: Cybersecurity vs. Transparency Trade-offs. Research on how election commissions navigate security-transparency tensions, with comparative case studies of decisions to disclose or withhold information.

Future Scope 7: Algorithmic Transparency in Electoral Management. As electoral management becomes increasingly algorithmic (voter list cleansing, redistricting, anomaly detection), research on the transparency implications of these algorithms becomes urgent.

Future Scope 8: Political Economy of Election Technology Procurement. Research on procurement transparency, vendor relationships, and cost efficiency in election technology would reveal whether transparency deficits correlate with economic inefficiency.

18. References

1. Association for Democratic Reforms. (2018). Fearing breach, Election Commission moves to secure cyber walls for 2019. ADR India.
2. Association for Democratic Reforms. (2015). India moves closer to wider electoral reforms. ADR India.
3. Centre for Development of Advanced Computing. (2014). Politicos think before you blurt, EC is watching! C-DAC.
4. Election Commission of India. (2018). Status Paper on Electronic Voting Machine. Government of India.
5. FACTLY. (2017). Scuttling Transparency? Election Commission does not respond to 2000 'RTI Online' applications. FACTLY.
6. National Informatics Centre. (2018). Editorial: Technology and Election Management in India. Informatics Journal.
7. PM India. (2016). Cabinet approves procurement of Control Units, Ballot Units and Voter Verifiable Paper Audit Trail Units. Government of India.
8. Bajpai, R. (2017). *The Election Commission of India: Institutionalising democratic uncertainties*. Oxford University Press.
9. Chakrabarty, B. (2014). *India's democratic transition: Elections, technology and governance*. Orient BlackSwan.
10. Election Commission of India. (2000-2018). *Annual Reports*. Government of India.
11. Jenkins, R. (2012). *Democratic politics and economic reform in India*. Cambridge University Press.
12. Kapur, D., & Mehta, P. B. (2017). *Navigating the labyrinth: Perspectives on India's higher education*. Orient BlackSwan (chapter on RTI implementation).
13. McMillan, A. (2018). The Election Commission of India: Technology and institutional autonomy. *Commonwealth & Comparative Politics*, 56(3), 327-345.
14. Norris, P. (2014). *Why electoral integrity matters*. Cambridge University Press.
15. Quraishi, S. Y. (2014). *An undocumented wonder: The making of the great Indian election*. Rupa Publications.
16. Raman, S. A. (2011). Framing the EVM debate in India. *Media Asia*, 38(2), 89-98.