International Journal of Humanities, Commerce and Education
Volume 2 | Issue 5 | May 2026 (Special Issue) | ISSN: 3108-0456 (Online)
Available online at: https://ijhce.com/
DOI: https://doi.org/10.59828/ijhce.v2i5.67

Reimagining Digital Electoral Security through IKS: Ethical AI and Cyber Resilience for Viksit Bharat@2047

Swarnima Singh[1], Dr. Preeti Singh[2]

[1]Research Scholar, Department of Political Science, D.B.S. College, Kanpur Chhatrapati Shahuji Maharaj University, Kanpur, U.P. 208024

[1]Email: ashima.singh0608@gmail.com

[2]Associate Professor & Head, Department of Political Science, D.B.S. College, Kanpur

Received: 15 April 2026 | **Accepted:** 28 April 2026 | **Published:** 15 May 2026

Abstract

The rapid digitization of electoral processes in India has significantly enhanced administrative efficiency, transparency, and citizen participation. However, it has also generated critical challenges related to cybersecurity, data integrity, algorithmic bias, and digital manipulation, including misinformation, deepfakes, and vulnerabilities in electoral infrastructure. This paper reimagines digital electoral security through the integrative framework of Indian Knowledge Systems (IKS) and ethical Artificial Intelligence (AI), with the aim of strengthening cyber resilience in alignment with the vision of Viksit Bharat@2047.

Drawing upon foundational IKS principles such as dharma (ethical responsibility), nyaya (justice), and lokasangraha (collective welfare), the study develops a normative model for ethical digital governance. It argues that these indigenous philosophical constructs offer a culturally grounded approach to mitigating algorithmic bias, enhancing transparency, and fostering public trust in electoral systems. The research adopts an interdisciplinary methodology, combining political analysis, cybersecurity perspectives, and digital governance frameworks.

The paper further proposes a hybrid governance model that integrates IKS-based ethical reasoning with contemporary technological solutions such as AI accountability mechanisms, blockchain-enabled audit trails, and robust digital public infrastructure. It highlights the need for institutional reforms, policy innovation, and citizen-centric awareness to address emerging cyber threats effectively.

By bridging civilizational wisdom with technological innovation, this study contributes to the discourse on secure, inclusive, and ethically grounded democratic governance in India's digital age.

Keywords: *Digital Electoral Security; Ethical Artificial Intelligence; Cyber Resilience; Democratic Governance; Misinformation and Deepfakes*

1. Introduction

India's electoral democracy which is the world's largest democracy, has undergone a significant digital transformation since past two decades, evolving from paper ballots to ***Electronic Voting Machines (EVMs)***, ***Voter Verifiable Paper Audit Trails (VVPATs)***, and increasingly ***data driven*** and ***AI enabled campaigns***. This shift has accelerated post-2014 with initiatives like **Digital India**, has enhanced not only administrative efficiency boasting 97% voter registration accuracy and real-time turnout tracking in 2024 Lok Sabha polls, but also transparency and voter participation. Social media and apps like **cVIGIL** empowered citizen

engagement and oversight, reflecting a shift towards more participatory and technology driven electoral governance.

However, this transformation has also introduced a new set of complex challenges that pose risks to democratic integrity. The core problem lies in escalating **cyber threats**: ***misinformation surges*** (e.g., 2024 regional language fakes on EVM rigging), ***deepfakes*** of leaders and celebrities, and ***AI-amplified polarization*** stoking sectarian divides. Microsoft warned of foreign interference via GenAI; ECI issued advisories against manipulated content, but incidents persisted. Such developments have the potential to distort public opinion, influence voter behaviour, and undermine trust in democratic institutions. The growing sophistication of artificial intelligence tools has further intensified these concerns by enabling the creation and dissemination of highly convincing yet misleading content at scale. These dynamics highlight the emergence of a digital electoral ecosystem that is not only technologically advanced but also increasingly vulnerable to manipulation and cyber threats.

Despite the presence of regulatory and institutional mechanisms, including guidelines and advisories issued by the **Election Commission of India (ECI)** and broader legal frameworks governing information technology and data protection, current responses remain largely reactive in nature. They tend to focus on compliance, content moderation, and post-facto regulation rather than proactive prevention, ethical design, and systemic resilience. Moreover, existing Western centric approaches may not fully account for India's unique socio-cultural context and democratic complexities. This creates a gap in the development of a holistic and context-sensitive framework for digital electoral security.

2. Research Objectives

In this context, there is a need to explore alternative and integrative approaches that combine technological innovation with ethical and philosophical grounding. Indian Knowledge Systems (IKS), rooted in longstanding traditions of ethical reasoning and governance, offer valuable normative insights that can inform contemporary policy challenges. Concepts such as *dharma* (ethical responsibility), *nyaya* (justice), and *lokasangraha* (collective welfare) provide a framework for understanding governance not merely as administrative control but as a moral and socially embedded practice. Integrating these principles with modern technological tools, particularly ethical Artificial Intelligence (AI) and cybersecurity mechanisms, can contribute to the development of more accountable, transparent, and resilient electoral systems.

This paper seeks to reimagine digital electoral security through such an integrative framework. It adopts an interdisciplinary approach, drawing upon political science, cybersecurity studies, and digital governance frameworks, with a contextual focus on electoral developments in India.

This research paper examines this central question:

"How can a framework combining Indian Knowledge Systems (IKS) and ethical Artificial Intelligence (AI) enable secure, resilient, and future-ready electoral governance in India?"

This paper is guided by two objectives:

1. To reimagine digital electoral security through the integration of Indian Knowledge Systems (Arthashastra's vigilance, Dharma's ethics) with ethical AI frameworks.
2. To develop a hybrid governance model combining ethical principles with technological solutions for resilient electoral systems.

By bridging ethical traditions with technological innovation, this study contributes to the development of a secure, inclusive, and future-ready electoral framework. In doing so, it aligns with the broader vision of Viksit Bharat@2047 by building a technologically advanced yet ethically grounded democratic system capable of addressing emerging challenges in India's digital age.

3. Review of literature

Past studies on digital electoral security can broadly be divided into **three interrelated themes**: 1. cyber threats in electoral processes, 2. ethical AI and digital governance, and 3. the emerging application of Indian Knowledge Systems (IKS). While each strand offers important insights, the literature remains fragmented, with limited efforts to integrate technological, ethical, and indigenous perspectives into a unified framework.

The first strand focuses on ***cyber threats and vulnerabilities in electoral systems***, particularly following the introduction of Electronic Voting Machines (EVMs) in India. Scholars have increasingly highlighted the rise of misinformation, deepfakes, and AI-driven manipulation in electoral contexts. Recent analyses document the growing circulation of digitally altered political content and coordinated disinformation campaigns, raising concerns about voter perception and electoral integrity **(Mabbu, 2025; Resolver, 2024).** Institutional responses, such as the Election Commission of India's (ECI) grievance redressal mechanisms and advisories, have attempted to address these challenges; however, they are often characterized as reactive and insufficient to counter the scale of emerging threats **(Alt News, 2025; CyberPeace, n.d.)**. Consequently, this body of literature remains largely techno-centric, focusing on vulnerabilities and responses without adequately addressing underlying ethical dimensions.

The second strand engages with ***ethical AI and digital governance frameworks***. Policy initiatives such as NITI Aayog's guidelines on Responsible AI emphasize principles of fairness, accountability, and transparency in the deployment of AI systems **(NITI Aayog, 2021)**. However, studies suggest that the application of these principles in electoral contexts remains limited, particularly in relation to issues such as algorithmic bias, voter profiling, and targeted political communication **(Friedrich Naumann Foundation, 2024)**. Scholars argue that existing regulatory frameworks, including data protection and IT laws, prioritize compliance and content moderation rather than proactive governance or ethical design **(Indic Pacific, 2025)**. As a result, current approaches are often seen as inadequate for addressing the rapidly evolving challenges posed by AI-driven electoral manipulation.

The third strand of literature explores ***the relevance of Indian Knowledge Systems (IKS)*** in contemporary governance discourse. Drawing upon classical texts such as the *Arthashastra* and broader philosophical traditions, scholars have emphasized concepts such as *dharma*, *nyaya*, and *lokasangraha* as foundational principles for ethical governance **(RJPN, 2025; VIIRJ, 2025)**. Recent studies attempt to apply these principles to modern domains, including AI ethics, public policy, and digital governance, suggesting their potential to provide culturally grounded normative frameworks **(IJCRT, 2025; Journal of Political Science, 2026)**. However, the application of IKS to digital electoral security remains limited, with only preliminary attempts to link classical notions of vigilance and ethical duty to contemporary cyber challenges.

Taken together, the literature reveals a significant gap. While studies on cyber threats provide empirical insights and ethical AI scholarship offers normative guidance, there is little integration between these domains and indigenous knowledge frameworks. In particular, no comprehensive model currently exists that combines technological innovation with IKS-based ethical reasoning to address digital electoral vulnerabilities in a future-oriented manner. This paper seeks to bridge this gap by proposing an interdisciplinary framework that integrates ethical AI, cyber resilience, and Indian Knowledge Systems for strengthening electoral security in India.

4. Analytical Framework

This section develops an analytical framework for understanding and *strengthening digital electoral security through the integration of Indian Knowledge Systems (IKS) and ethical Artificial Intelligence (AI)*. The framework seeks to move beyond reactive approaches to electoral governance by proposing a proactive and

resilience-oriented model that combines ethical reasoning with technological innovation. Drawing conceptually from Kautilya's *Arthashastra* and contemporary principles of Responsible AI, the framework positions electoral security as a multidimensional system involving ethical, technological, and institutional components.At its core, the framework is based on the premise that technological solutions alone are insufficient to address the complexities of digital electoral threats. Instead, a ***hybrid model*** is required one that integrates normative ethical principles with operational technological mechanisms. In this regard, IKS provides a foundational ethical layer, while AI and cybersecurity tools function as applied instruments for implementation.

4.1. Conceptual Foundations of the Framework

The framework is built upon **three interrelated pillars**: 1) **ethical foundations derived from IKS, 2) principles of ethical AI, and 3) mechanisms of cyber resilience**.

First, Indian Knowledge Systems offer a rich normative basis for governance. Concepts such as *dharma* (ethical responsibility), *nyaya* (justice), and *lokasangraha* (collective welfare) provide a moral framework for decision-making and institutional conduct. In the context of digital electoral systems, *dharma* can be interpreted as the obligation of institutions to ensure fairness, truth, and accountability in the use of technology. Similarly, *nyaya* emphasizes justice and impartiality, which are critical in addressing algorithmic bias and ensuring equitable access to electoral processes. The idea of *lokasangraha* underscores inclusivity and collective well-being, highlighting the need to design digital infrastructures that are accessible and beneficial to all sections of society. Additionally, Kautilya's notion of *netra-drishti* (vigilance through intelligence networks) provides a useful analogy for contemporary cybersecurity practices. It emphasizes continuous monitoring, anticipation of threats, and strategic preparedness principles that are highly relevant in addressing modern cyber risks such as misinformation, deepfakes, and data breaches.

Second, the framework incorporates principles of ethical AI, particularly those outlined in policy initiatives such as **NITI Aayog's Responsible AI guidelines**. These include fairness, transparency, accountability, and non-discrimination. When combined with IKS principles, ethical AI can be operationalized more effectively. For instance, algorithmic auditing mechanisms can be seen as extensions of *dharma*, ensuring that AI systems function in a just and unbiased manner. Similarly, transparency measures align with *satya* (truth), helping to counter misinformation and build public trust.

Third, **cyber resilience** forms the technological backbone of the framework. This includes the use of secure digital infrastructures, encryption technologies, and audit mechanisms to protect electoral systems from external and internal threats. Emerging technologies such as blockchain can enhance transparency and immutability in electoral processes, while advancements in encryption can safeguard voter data against evolving cyber risks. Together, these elements contribute to a more secure and trustworthy electoral ecosystem.

4.2. Structure of the Hybrid Model

The analytical framework can be understood as a **three-layered model** that connects ethical principles, technological processes, and institutional mechanisms.

Building upon the conceptual foundations outlined above, the ***first layer*** operationalizes IKS principles by guiding institutional decision-making and ethical design in electoral technologies. It emphasizes the role of institutions, particularly the Election Commission, in upholding fairness, preventing manipulation, and ensuring transparency in electoral processes.

The ***second layer*** translates these ethical principles into practice through the deployment of accountable and transparent AI systems. This includes the use of AI tools for detecting misinformation, identifying deepfakes,

and monitoring digital campaign practices. Such systems must remain explainable and subject to institutional oversight, with mechanisms such as algorithmic audits and transparency dashboards ensuring accountability.

The ***third layer*** provides the technological backbone necessary to sustain electoral security. It includes secure voting systems, digital public infrastructure, and data protection mechanisms. Technologies such as blockchain can create verifiable audit trails, while decentralized and privacy-preserving systems enhance resilience and safeguard voter data without compromising transparency.

These three layers are interdependent and must function in coordination to ensure effective electoral security. Ethical principles guide technological design, while technological tools enable the practical realization of accountable and resilient governance.

4.3. Application to Electoral Developments in India

The relevance of this framework can be illustrated through developments in India's electoral processes over the past two decades. The introduction of EVMs and VVPAT systems marked a significant shift towards digitization, improving efficiency and reducing logistical challenges. However, concerns regarding security, transparency, and trust have persisted. In recent years, the rise of AI-driven misinformation and deepfake technologies has further complicated the electoral landscape. Instances of manipulated political content and coordinated disinformation campaigns have highlighted the limitations of existing regulatory mechanisms. While the Election Commission has introduced measures such as advisories and monitoring tools, these responses have largely been reactive.

The proposed framework offers a more proactive approach. By integrating ethical principles with technological tools, it enables early detection of threats, promotes transparency, and strengthens institutional accountability. For example, AI-based systems can be used to identify and flag manipulated content, while blockchain-based audit mechanisms can enhance trust in voting processes. At the same time, ethical guidelines derived from IKS can ensure that these technologies are used responsibly and inclusively.

4.4. Towards a Future-Ready Electoral System

Looking ahead, the framework provides a foundation for developing a future-ready electoral system in India. This involves not only strengthening existing technologies but also rethinking governance structures and policy approaches. In the **short term**, efforts can focus on enhancing regulatory frameworks and building institutional capacity for managing digital threats. In the **medium term**, the integration of digital public infrastructure and advanced AI systems can improve efficiency and resilience. In the **long term**, emerging technologies such as quantum-resistant encryption and decentralized governance models can further strengthen electoral security.

Importantly, the success of this framework depends on the alignment of technological innovation with ethical and societal values. By incorporating principles from Indian Knowledge Systems, the framework ensures that digital transformation is guided by a ***broader vision of justice, inclusivity, and collective welfare***.

4.5. Limitations of the Framework

While the proposed framework offers a comprehensive approach, it is not without limitations. Its application requires empirical validation and may face challenges related to institutional capacity, technological feasibility, and socio-cultural adaptation. Additionally, the integration of traditional ethical frameworks with modern technologies requires careful interpretation to avoid oversimplification or misapplication.

5. Policy Analysis & Implications: Future Vision

This section examines the policy implications of the proposed hybrid framework by *analysing gaps* in existing regulatory mechanisms, particularly those of the **Election Commission of India (ECI)** and the **Digital Personal Data Protection (DPDP)** framework, while outlining a future-oriented roadmap. By integrating

Indian Knowledge Systems (IKS) with technological governance, the framework advances a more resilient and ethically grounded model of digital democracy.

5.1 Current Policy Framework

Recent policy interventions reflect growing awareness of digital electoral risks but remain limited in scope and effectiveness. The ECI's 2024 advisories mandate AI-generated content labelling and rapid takedown mechanisms; however, enforcement challenges persist, as evidenced by legal interventions and a rising number of deepfake-related complaints **(Business & Human Rights, 2024)**. Similarly, the DPDP framework emphasizes data protection through consent-based mechanisms and penalties, yet it largely prioritizes compliance over proactive ethical governance, contributing to continued public distrust **(PIB, 2025; McAfee)**. Judicial observations, including those related to VVPAT verification, reinforce confidence in technological systems while simultaneously highlighting the need for greater transparency and auditability.

5.2. Implications: Operational Reforms

The hybrid framework suggests a phased approach to policy reform:

- **Short-term (2026–2030):** Establish dedicated ECI units integrating IKS principles with AI-based monitoring systems. Platforms such as cVIGIL can be upgraded with advanced detection tools for misinformation and deepfakes. Ethical audit mechanisms (*nyaya*-based) can be introduced for political use of AI technologies.
- **Medium-term (2030–2040):** Develop a National Electoral Digital Public Infrastructure (DPI) integrating secure technologies such as blockchain-enabled audit systems and federated voter identification. Educational reforms under NEP can incorporate governance and cybersecurity modules inspired by classical texts.
- **Long-term (2047):** Strengthen technological sovereignty through advanced encryption systems and global digital cooperation frameworks. These developments can contribute to both electoral integrity and broader economic growth by enhancing trust in digital systems.

5.3 Broader Implications

The framework carries wider implications across multiple domains:

- **Democratic:** Enhances inclusivity and fairness in electoral participation, particularly for marginalized and rural populations.
- **Economic:** Strengthens trust in digital public infrastructure, supporting long-term economic growth.
- **Global:** Positions India as a contributor to global norms on ethical AI and digital governance.

5.4. Policy Recommendations

Based on the above analysis, the following policy recommendations are proposed:

- **Enact an IKS–AI Act (by 2026):** Mandate *nyaya*-based algorithmic audits and establish ethical AI sandboxes for electoral technologies.
- **Introduce an ECI *Rajadharma* Charter:** Integrate *netra*-based monitoring mechanisms through pilot implementations in platforms such as cVIGIL 2.0.
- **Establish a ₹1,000 crore Cyber–IKS Fund:** Support capacity building, particularly in rural areas, through digital literacy programs and *lokasangraha*-oriented awareness campaigns.
- **Develop a Federal Blockchain Electoral Stack:** Enable secure integration of VVPAT systems with digital public infrastructure (DPI) for enhanced transparency and auditability.
- **Promote Global Engagement:** Position India as a leader in shaping international norms by advocating IKS-informed cyber governance frameworks at multilateral platforms such as the United Nations.

5.5. Challenges

Key challenges include technological accessibility, digital literacy gaps, and institutional capacity. These can be addressed through inclusive policy design and awareness initiatives grounded in collective welfare principles.

6. Conclusion

This paper reimagines digital electoral security by integrating Indian Knowledge Systems (IKS) with ethical Artificial Intelligence (AI), addressing emerging vulnerabilities in India's electoral processes. It argues that contemporary challenges such as misinformation, deepfakes, and algorithmic manipulation cannot be effectively addressed through reactive regulatory frameworks alone. Instead, a proactive and ethically grounded approach is required. The study demonstrates that the fusion of IKS principles such as *dharma*, *nyaya*, and *netra-drishti* with ethical AI and cybersecurity mechanisms offers a viable pathway toward resilient and trustworthy electoral systems. By combining normative ethical foundations with technological innovation, the proposed framework enhances transparency, accountability, and inclusivity in digital governance. The analysis further suggests that such a hybrid model has the potential to significantly mitigate emerging threats while strengthening institutional trust.

In the context of India's long-term developmental vision, this approach contributes to the creation of a future-ready electoral system supported by robust digital public infrastructure and adaptive governance mechanisms. Ultimately, aligning technological advancement with ethical and civilizational values enables the evolution of a secure, inclusive, and sovereign democratic framework capable of addressing the complexities of the digital age.

References

[1]. Business & Human Rights Resource Centre. (2024, May 7). *India: Election Commission issues guidelines to parties on responsible social media amid elections, addressing deepfake video complaints.* https://www.business-humanrights.org/en/latest-news/india-election-commission-issues_guidelines-for-responsible-social-media-use/

[2]. CEO Delhi. (n.d.). *Theme 10 - EVM & VVPAT* [Training material]. https://ceodelhi.gov.in/PDFFolders/TrgMaterial/EVM_VVPAT.pdf

[3]. CyberPeace Foundation. (n.d.). *Role of cyber security in Viksit Bharat 2047*. https://cyberpeace.org/resources/blogs/role-of-cyber-security-in-viksit-bharat-2047

[4]. Drishti IAS. (2025, August 18). *Transformative reforms for Viksit Bharat@2047*. https://www.drishtiias.com/daily-updates/daily-news-analysis/transformative-reforms-for-viksit-bharat-2047

[5]. ET Edge Insights. (2026, January 15). *Security automation as an infrastructure mandate for Viksit Bharat.* https://etedge-insights.com/featured-insights/security-automation-as-an-infrastructure-mandate-for-viksit-bharat/

[6]. Friedrich Naumann Foundation. (2024). *Generative AI and its influence on India's 2024 elections* [Policy paper]. https://www.freiheit.org/sites/default/files/2025-01/a4_policy-paper_ai-on-indias-2024-electons_en-4

[7]. Indic Pacific Legal Research LLP. (2025, October 31). *Advisory on ethical use of social media and deepfakes in elections*. https://www.indicpacific.com/india-ai-regulation-101-landscape/advisory-on-ethical-use-of-social-media-and-deepfakes-in-election/

[8]. International Journal of Information Security & Cybercrime. (2026, March 16). *Digital transformation of Indian democracy: Electoral reforms and technology.*

https://www.ijisrt.com/assets/upload/files/IJISRT26MAR631

[9]. Mabbu, S. (2025). AI-driven cybersecurity and its legal challenges in India. *International Journal for Multidisciplinary Research*. https://www.ijfmr.com/papers/2025/6/64239

[10]. NDTV. (2024, April 19). *Explained: How EVMs record your vote, and how VVPAT verifies it*. https://www.ndtv.com/india-news/evm-vvpat-lok-sabha-election-2024-as-india-votes-today-a-look-at-how-evm-and-vvpat-polling-machi/

[11]. Press Information Bureau. (2017, March 30). *EVM challenge by Election Commission of India.* https://www.pib.gov.in/PressReleasePage.aspx?PRID=1490341

[12]. Reuters. (2024, June 5). *How India conducted the world's largest election.* https://www.reuters.com/graphics/INDIA-ELECTIONS/gdpzmqgrmvw/

[13]. Supreme Court of India. (2024). *SC upholds EVM and VVPAT system*. Drishti IAS. https://www.drishtiias.com/daily-updates/daily-news-analysis/sc-upholds-evm-and-vvpat-system-1

Cite this Article:

Singh, S., & Singh, P. (2026). Reimagining digital electoral security through IKS: Ethical AI and cyber resilience for Viksit Bharat@2047. International Journal of Humanities, Commerce and Education, 2(5), 52–59.

Journal URL: *https://ijhce.com/* ***DOI****: https://doi.org/10.59828/ijhce.v2i5.67*