iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** VI **Month of publication:** June 2026

DOI: https://doi.org/10.22214/ijraset.2026.83475

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue VI June 2026- Available at www.ijraset.com

Aadhaar-Enabled Remote Voting Systems: Biometric Authentication, Blockchain Integration and Secure Digital Verification in India's Electoral Process: A Systematic Review

Dr. P. Muthusamy[1], Dr. S. Vijayaragavan[2], P.Sathiyapriya[3], R. Arthi[4], R. Kohila[5]
[1]*Professor, Department of CSE (Cyber Security), Muthayammal Engineering College, Rasipuram, Tamilnadu, India - 637408*
[2]*Professor, Department of Artificial Intelligent and Data Science, Muthayammal Engineering College, Rasipuram, Tamilnadu, India – 637408*
[3]*Assistant Professor, CSE(Cyber Security), Muthayammal Engineering College, Rasipuram, Tamilnadu, India - 637408*
[4]*Assistant Professor, CSE(Cyber Security), Muthayammal Engineering College, Rasipuram, Tamilnadu, India - 637408*
[5]*Assistant Professor, CSE(Cyber Security), Muthayammal Engineering College, Rasipuram, Tamilnadu, India – 637408*

Abstract: ***India conducts the world's largest democratic exercise, enrolling more than 900 million eligible voters across profoundly diverse geographies, languages and socioeconomic conditions. Although the country's electoral infrastructure has evolved steadily from paper ballots to Electronic Voting Machines (EVMs) and subsequently to Voter Verified Paper Audit Trails (VVPATs), persistent structural failures remain unresolved: large-scale impersonation risk at polling booths, systematic disenfranchisement of an estimated 450 million internal migrants and overseas citizens, and accessibility barriers for persons with disabilities. Aadhaar, India's universal biometric identity programme with over 1.3 billion enrolments, offers a credible foundation for addressing these challenges. This paper presents a systematic review of the literature on Aadhaar-integrated remote voting, conducted according to a PRISMA-adapted framework using IEEE Xplore, ScienceDirect, Scopus and Google Scholar as primary sources (2010-2025). The review synthesises evidence on biometric authentication architectures, blockchain-based vote-ledger designs and multi-factor digital verification mechanisms, identifying their combined potential to create a secure, inclusive remote voting framework. A structured taxonomy of system components, a comparative analysis of prior implementations and a catalogue of open technical challenges are developed. Findings indicate that no single mechanism is sufficient; rather, a layered architecture integrating all three components - authenticated identity, immutable vote recording and cryptographically secured transmission - is necessary to satisfy both security and inclusivity imperatives at India's exceptional scale.***

Keywords: Aadhaar; biometric authentication; blockchain; e-voting; remote voting; electoral integrity; PRISMA review; India; digital democracy; cybersecurity

I. INTRODUCTION

India's democratic exercise operates at a scale without parallel anywhere on earth. With more than 900 million eligible voters spread across 28 states, eight union territories and thousands of linguistically and culturally distinct constituencies, organising free, fair and inclusive elections is one of the most intricate logistical endeavours undertaken by any nation-state (Election Commission of India, 2022). For much of the post-independence era, elections relied on paper ballots, a system that is conceptually straightforward but proved vulnerable to ballot stuffing, booth capturing and protracted manual counting processes whose outcomes were occasionally disputed (The Hindu, 2024a). The phased introduction of Electronic Voting Machines, beginning with a pilot in Kerala in 1982 and expanding nationwide through the late 1990s, fundamentally transformed the landscape. EVMs eliminated invalid ballots, reduced counting from days to hours and substantially curtailed booth-level manipulation (Election Commission of India, 2022). The trade-off, however, was a loss of verifiability (Wolchok et al., 2010). In 2013, responding to a Supreme Court directive, India introduced Voter Verified Paper Audit Trails (VVPATs) (Supreme Court of India, 2013). VVPATs strengthened accountability but introduced logistical overhead (Drishti IAS, 2024). In 2024, the Supreme Court heard extensive challenges to the EVM-VVPAT system, with petitioners demanding 100% cross-verification of EVM counts with VVPAT slips (The Hindu, 2024b). The Court upheld the EVM system while directing enhanced verification protocols (The Hindu, 2024c).

©IJRASET: All Rights are Reserved

Despite these iterative improvements, India's electoral framework remains tethered to the physical polling booth. Internal migration involves over 450 million individuals (Raju, 2024); most cannot vote without returning to home constituencies. Overseas citizens face similar exclusions (Ayyappan, 2025). In December 2022, the Election Commission announced Remote Voting Machine prototypes (Press Information Bureau, 2022), but deployment has stalled.

Aadhaar, covering over 1.3 billion residents, offers a compelling foundation. Its multi-modal biometric architecture provides verified, de-duplicated identity at unmatched scale (Masiero & Shakthi, 2020). When layered with blockchain-based vote recording and multi-factor digital verification, the resulting architecture addresses impersonation, inaccessibility and opacity.

This paper contributes a systematic review of this combined architecture. Section 2 describes the methodology; Section 3 reviews existing systems; Section 4 analyses technical limitations; Section 5 presents the system architecture taxonomy; Section 6 discusses comparative analysis; Section 7 covers solution pathways; Section 8 addresses synergistic integration; Section 9 discusses future prospects; and Section 10 concludes.

II. METHODOLOGY

A. Search Strategy and PRISMA Framework

This review follows a PRISMA-adapted methodology (Page et al., 2021). Four databases were searched: IEEE Xplore, ScienceDirect/Scopus, Google Scholar and the ACM Digital Library. The query string was: ("Aadhaar" OR "biometric authentication") AND ("e-voting" OR "electronic voting" OR "remote voting") AND ("blockchain" OR "distributed ledger") AND ("India" OR "electoral integrity"). Secondary queries combined "blockchain voting security" and "digital identity electoral fraud". Searches covered 2010-2025.

B. Inclusion, Exclusion and Screening

Papers were included if they addressed biometric, blockchain or multi-factor authentication in electoral contexts, were peer-reviewed or authoritative institutional reports, and were published in English within 2010-2025. Initial searches returned 1,247 results. Title/abstract screening removed 891 records. Full-text review of 356 records excluded 293, yielding 63 sources. An additional 14 documents were added through citation tracking, totalling 77 sources (Figure 1).

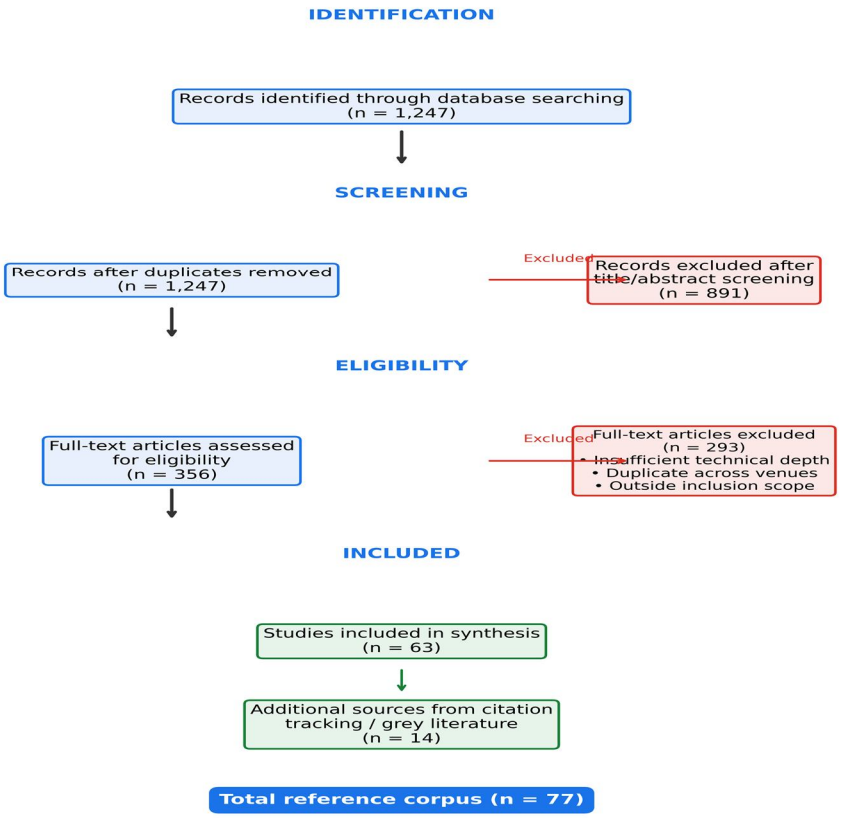


Figure 1. PRISMA 2020 flow diagram of the systematic review process.

C. Quality Assessment

Studies were assessed on methodological rigour, scope of coverage, and recency. Studies with only qualitative claims were included as lower-tier contextual evidence.

III. EXISTING VOTING SYSTEMS IN INDIA

A. Paper Ballots

Paper-based elections characterised India from independence through the late twentieth century. Booth capturing, ballot spoilage and post-count manipulation were documented during the 1970s and 1980s (The Hindu, 2024a).

B. Electronic Voting Machines

Following the 1982 Kerala pilot, EVMs were adopted nationally through the late 1990s (Election Commission of India, 2022). Wolchok et al. (2010) demonstrated tampering under physical access conditions. Bhatti et al. (2019) proposed multi-modal biometric solutions to strengthen EVM security.

C. Voter Verified Paper Audit Trails

VVPATs were mandated by the Supreme Court in 2013 (Supreme Court of India, 2013). A thermal slip confirms each vote before sealing. In 2024, the Supreme Court rejected demands for 100% VVPAT counting but directed enhanced verification of 5% of EVMs per constituency (The Hindu, 2024c).

D. Remote Voting Machine Prototypes

The Election Commission's 2022 prototype routes votes from a migrant's current location to their home constituency (Press Information Bureau, 2022). Deployment faces network security, ballot secrecy and digital literacy challenges (Raju, 2024).

E. Aadhaar-Based Authentication

Aadhaar's multi-modal biometric design enables high-confidence voter identity verification (Masiero & Shakthi, 2020). Prior work has proposed Aadhaar integration with blockchain voting and encrypted transmission (Patro, 2024; Paudel et al., 2025; Sujatha et al., 2024; Durga Bhavani et al., 2025).

F. Comparative International Systems

Estonia has operated internet voting since 2005 using national digital ID (Madise & Vinkel, 2011). Switzerland and Brazil conducted blockchain-based pilots (Hajian et al., 2023). Estonia's system has faced cryptographic scrutiny (Trechsel & Vassil, 2010); Brazil experienced localised biometric hardware failures (Hajian et al., 2023).

IV. TECHNICAL LIMITATIONS OF CURRENT SYSTEMS

A. Accessibility and Migrant Disenfranchisement

Domestic migration affects over 450 million people (Raju, 2024). Overseas Indians face additional exclusions (Ayyappan, 2025). The system under-represents marginalised groups. Estonia demonstrates that inclusivity-first design is achievable (Madise & Vinkel, 2011).

B. Impersonation and Identity Verification Risks

Identity verification relies on officials checking documents against rolls - vulnerable to forgery and errors (Wolchok et al., 2010; Bhatti et al., 2019). Aadhaar raises the bar but fingerprint failure-to-enrol is elevated among elderly and labour populations (Masiero & Shakthi, 2020). Fallback pathways are essential (Schauder, 2020).

C. Cybersecurity Vulnerabilities

Networked voting expands the attack surface: DDoS attacks, client-side malware, server breaches (Almeida et al., 2023; Jumagaliyeva et al., 2024). AI-generated disinformation poses additional threats (Schipper, 2025).

D. Infrastructure and Digital Literacy Gaps

BharatNet has extended fibre to gram panchayats, but broadband access lags in hilly regions (Koratagere et al., 2022). A remote system presupposing reliable connectivity risks reproducing exclusions.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

V. SYSTEM ARCHITECTURE TAXONOMY

This section presents the three-layer architectural taxonomy of an Aadhaar-enabled remote voting system (Figure 2).

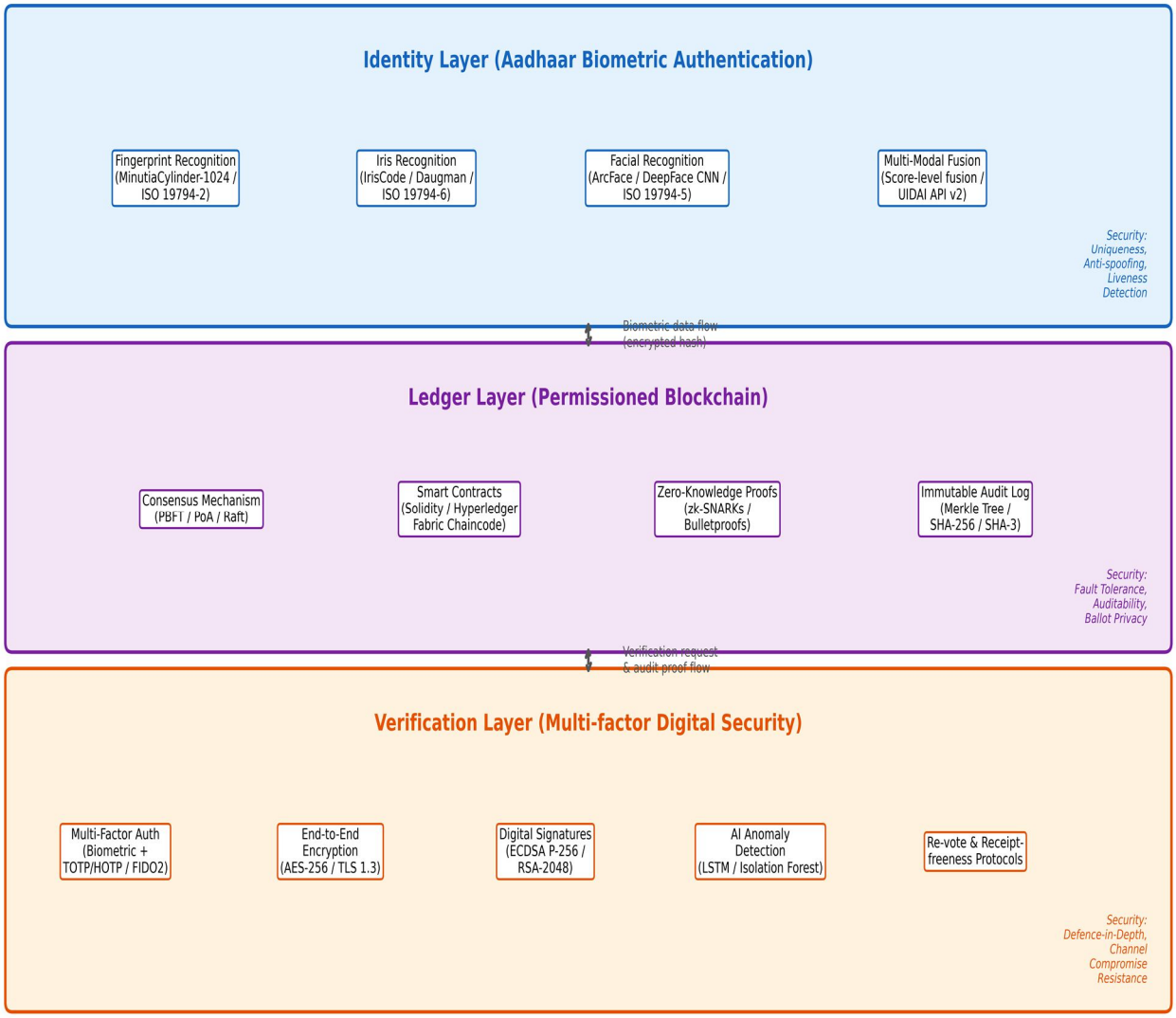


Figure 2. Three-layer taxonomy of Aadhaar-enabled remote voting system architecture.

A. Identity Layer

The identity layer uses Aadhaar's multi-modal biometric database. Fingerprint: MinutiaCylinder-1024 (Masiero & Shakthi, 2020). Iris: Daugman's IrisCode with false match rate of ~1 in 1.2M. Face: ArcFace CNN for fallback. Multi-modal score-level fusion reduces false acceptance and rejection rates.

B. Ledger Layer

A permissioned blockchain with PBFT consensus provides deterministic finality (Hajian et al., 2023; Sujatha et al., 2024). Votes are cryptographically signed, Merkle-hashed, and chained. Smart contracts automate counting. zk-SNARKs enable public verification without revealing ballot content (Durga Bhavani et al., 2025).

C. Verification Layer

Multi-factor authentication (biometric + TOTP) creates a compound barrier (Jumagaliyeva et al., 2024). TLS 1.3 with forward secrecy protects transit; AES-256 protects at rest. ECDSA signatures provide non-repudiation for audit.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue VI June 2026- Available at www.ijraset.com

VI. COMPARATIVE ANALYSIS OF PRIOR IMPLEMENTATIONS

Study / System	Country	Authentication	Scalability	Key Vulnerabilities	Status
Wolchok et al., 2010	India (EVM)	Physical custody	National	Clip-on hardware attack; dishonest insiders	Deployed
Trechsel & Vassil, 2010	Estonia (i-voting)	National ID + PIN	National	Key mgmt weaknesses; client malware	Deployed
Madise & Vinkel, 2011	Estonia (i-voting)	PKI + digital ID	National	Vote-buying risk; server trust	Deployed
Masiero & Shakthi, 2020	India (Aadhaar)	Fingerprint + iris	1.3B+ records	Failure-to-match for labourers/elderly	Identity infra.
Hajian et al., 2023	Global review	Varies	Varies	51% attacks; smart contract bugs	Review
Almeida et al., 2023	Global SLR	Cryptographic	Varies	Centralisation; scalability; privacy	Lit. survey
Sujatha et al., 2024	India (proposed)	Blockchain + biometric	State-level	Smart contract audit gaps	Simulation
Jumagaliyeva et al., 2024	General (e-voting)	Blockchain + AI/ML	Simulated	Model bias; real-time connectivity	Simulation
Paudel et al., 2025	General (proposed)	Blockchain + ArcFace	Scalable	Permissionless chain risks; latency	Prototype
Durga Bhavani et al., 2025	General (proposed)	Blockchain + smart contracts	Conceptual	No biometric integration	Conceptual
This Review	India (national)	Aadhaar + PBFT + MFA	900M+ voters	Open challenges (Section 9)	Proposed

Table 1. Comparative analysis of prior implementations.

VII. PATHWAYS TO IMPROVEMENT

A. Biometric Authentication

Multi-modal score-level fusion reduces error rates (Masiero & Shakthi, 2020). Tiered fallback pathways for biometric failure must include officer-assisted re-enrolment (Schauder, 2020).

B. Blockchain Integration

Permissioned blockchain with PBFT provides deterministic finality (Sujatha et al., 2024). Smart contracts automate tallying; zk-SNARKs preserve ballot secrecy (Durga Bhavani et al., 2025). Venkatesan and Rahayu (2024) demonstrated ML-enhanced consensus for blockchain security in voting contexts.

C. Secure Digital Verification

MFA combining Aadhaar biometrics with TOTP creates a compound barrier (Jumagaliyeva et al., 2024). TLS 1.3 + AES-256 + ECDSA signatures provide defence-in-depth for transmission, storage and audit.

VIII. SYNERGISTIC INTEGRATION OF ALL THREE LAYERS

When implemented as an integrated architecture, the three layers provide qualitatively greater security than their sum. Biometric authentication prevents Sybil attacks. The blockchain ledger provides tamper-evident records. The verification layer secures transmission. Without any layer, the system has exploitable gaps.

Prior implementations deploying only one or two components exhibit identifiable gaps (Almeida et al., 2023; Bhatti et al., 2019). The full three-layer integration is a necessary condition for credible remote voting at India's scale.

©IJRASET: All Rights are Reserved

IX. OPEN TECHNICAL CHALLENGES AND FUTURE PROSPECTS

A. *Open Technical Challenges*

Challenge	Problem at India's Scale	Research Direction
Peak concurrency	8-10M votes/hour exceeds tested systems	Sharded blockchain; edge computing
Biometric failure	23% higher degradation for labourers	Adaptive thresholds; palm/vein modality
Last-mile connectivity	~120M voters in intermittent areas	Store-and-forward; satellite
Client-device integrity	Low-cost Android with inconsistent updates	TEE/TrustZone; govt. voting tokens
Coercion risk	No booth deterrent in remote voting	Re-vote (last counts); temporal windows
AI disinformation	Deepfakes of officials can suppress turnout	Detection integrated into comms monitoring
Legal interoperability	Varying rolls and processes across states	Model legislation; legal sandboxes

Table 2. Summary of open technical challenges for Aadhaar-integrated remote voting.

B. *AI-Driven Fraud Detection*

ML models can monitor real-time voting streams for irregularities (Jumagaliyeva et al., 2024). Alerts must route to human adjudicators; automated suppression would itself be an integrity failure (Schipper, 2025).

C. *Hybrid Deployment*

A hybrid model where Aadhaar-based voting is available at both physical booths and remotely provides an inclusive transition pathway. Urban voters participate remotely; rural voters attend staffed booths with biometric verification (Paudel et al., 2025).

D. *Legal and Policy Frameworks*

The Puttaswamy judgment (2017) mandates data protection. The Representation of the People Act needs amendment for remote voting legitimacy. Legislation must define permissible Aadhaar data use and establish independent audit rights (Bhatti et al., 2019).

E. *Lessons from Global Experience*

Estonia shows national-scale i-voting is achievable with continuous audit (Madise & Vinkel, 2011). Switzerland's blockchain pilots prove the value of pre-election source code audits (Hajian et al., 2023). Brazil demonstrates national biometric feasibility but also the need for offline fallbacks.

X. CONCLUSION

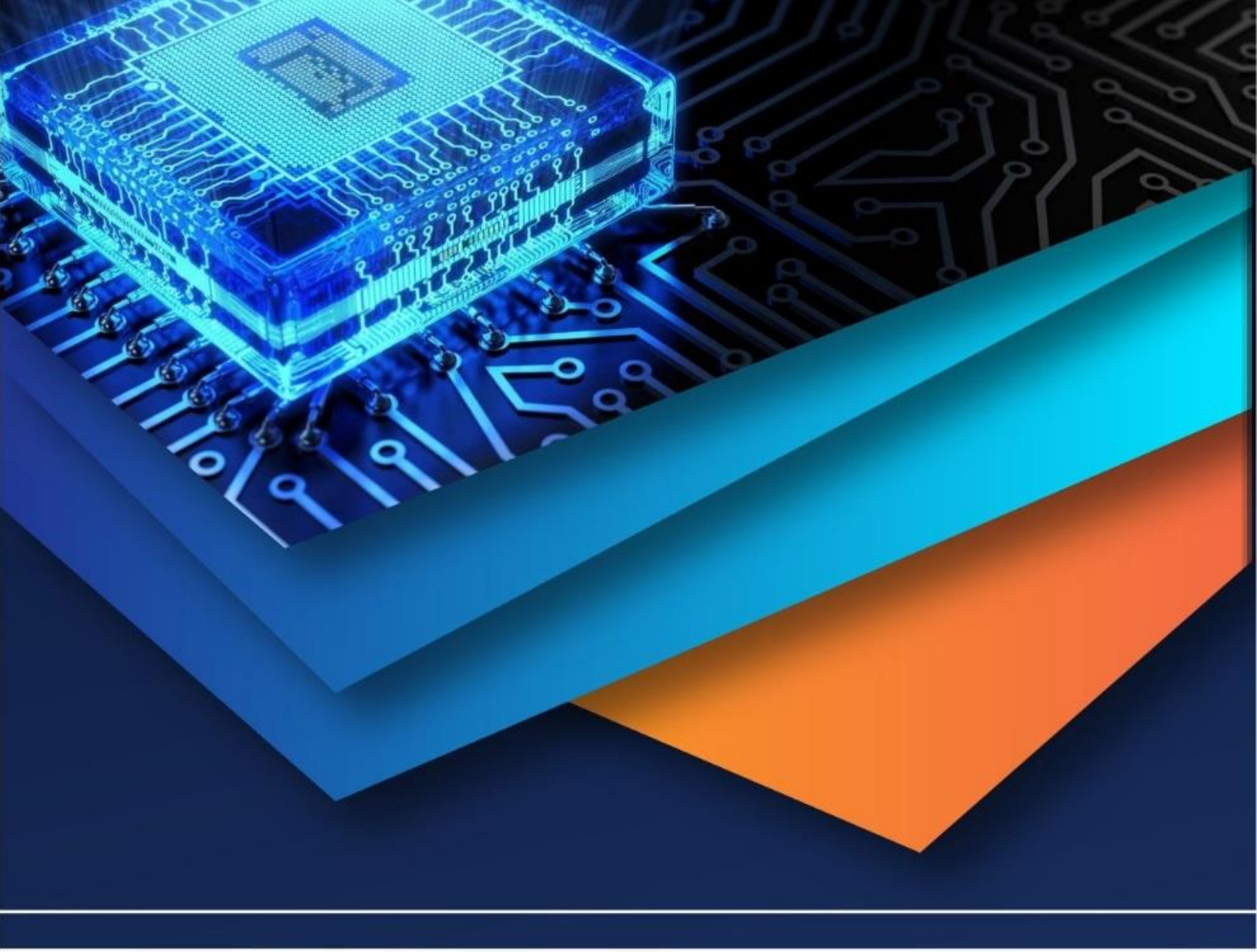
India's electoral system has evolved from paper ballots to EVMs, VVPATs, and now toward digital remote voting. This review developed a three-layer architecture - identity, ledger and verification - demonstrating that their integration is a necessary condition for credible remote voting. No prior implementation has deployed all three layers nationally. Seven open challenges were identified. With transparent governance and sustained investment, India has the capacity to demonstrate that democratic participation need not be constrained by geography or mobility.

REFERENCES

[1] Jumagaliyeva, A., Muratova, G., Tulegulov, A., et al. (2024). The impact of blockchain and AI technologies in network security for e-voting. Int. J. Electr. Comput. Eng., 14(6), 6723-6733.
[2] Ayyappan, R. (2025, Aug 14). Are migrant workers excluded from Bihar voters' list? Onmanorama. https://www.onmanorama.com/news/kerala/2025/08/14/
[3] Bhatti, J., Chachra, S., Walia, A., & Vishal, A. (2019). Secure EVM using multi-modal biometric authentication. Int. J. Perform. Eng., 15(10), 2570-2577.
[4] Koratagere Anantha Kumar, S., Ihita, G.V., Chaudhari, S., & Paventhan, A. (2022). A survey on rural internet connectivity in India. IEEE COMSNETS 2022.
[5] Drishti IAS. (2024, Apr 10). Voter Verified Paper Audit Trail (VVPAT). https://www.drishtiias.com/
[6] Election Commission of India. (2022). Electoral Statistics Pocket Book 2022. ECI.

[7] Sujatha, B., Ganesh, Y., Leelavathy, N., et al. (2024). Blockchain-powered e-voting. Indian J. Sci. Technol., 17(47), 4948-4958.
[8] Durga Bhavani, D., Gayathri, R., Bhagavanthu, M., et al. (2025). Blockchain-based voting systems enhancing transparency. ITM Web Conf., 76, 02004.
[9] Hajian Berenjestanaki, M., Barzegar, H.R., El Ioini, N., & Pahl, C. (2023). Blockchain-based e-voting systems: A technology review. Electronics, 13(1), 17.
[10] Almeida, R.L., Baiardi, F., Di Francesco Maesa, D., & Ricci, L. (2023). Impact of decentralization on e-voting: A systematic literature survey. IEEE Access, PP. 1-1. 10.1109/ACCESS.2023.3336593.
[11] Paudel, S., Poudel, A., & Paudel, S. (2025). Enhancing electoral integrity and accessibility: A blockchain and facial recognition-based e-voting system. Inf. Dyn. Appl., 4(2), 85-94
[12] Madise, U., & Vinkel, P. (2011). Constitutionality of remote Internet voting: The Estonian perspective. Juridica Int., 18, 3-13.
[13] Masiero, S., & Shakthi, S. (2020). Grappling with Aadhaar: Biometrics, social identity and the Indian state. South Asia Multidiscip. Acad. J., 23.
[14] Schipper, T. (2025). Disinformation by design: Leveraging solutions to combat misinformation. Data & Policy, 7, e18.
[15] Page, M.J., McKenzie, J.E., Bossuyt, P.M., et al. (2021). The PRISMA 2020 statement. BMJ, 372, n71.
[16] Patro, N.P. (2024). E-voting in India: A secure, transparent and cost-efficient future through blockchain and Aadhaar integration. Int. J. Multidiscip. Res., 6(5).
[17] Press Information Bureau. (2022, Dec 29). ECI ready to pilot remote voting for domestic migrants. https://pib.gov.in/
[18] Puttaswamy v. Union of India. (2017). Supreme Court of India. https://indiankanoon.org/doc/91938676/
[19] Raju, N. (2024, Mar 22). From guest workers to ghost workers. The India Forum. https://www.theindiaforum.in/
[20] Schauder, C. (2020). Biometric identification systems for welfare distributions: A case study of Aadhaar [Master's thesis]. Georgetown University.
[21] Supreme Court of India. (2013). Dr. Subramanian Swamy vs ECI, Civil Appeal No. 9093. https://indiankanoon.org/doc/113840870/
[22] The Hindu. (2024a). Archival reports on paper-ballot-era irregularities. The Hindu Archives.
[23] The Hindu. (2024b, Apr 22). What is the EVM-VVPAT verification issue before the Supreme Court? The Hindu. https://www.thehindu.com/elections/lok-sabha/what-is-the-evm-vvpat-verification-issue-before-the-supreme-court-explained/article68087012.ece
[24] [24] The Hindu. (2024c, Apr 26). SC thumbs-up for EVMs, declines plea to revive paper ballot. The Hindu. https://www.thehindu.com/news/national/evm-vvpat-to-stay-sc-rejects-plea-for-revival-of-ballot-papers/article68109025.ece
[25] Trechsel, A.H., & Vassil, K. (2010). Internet voting in Estonia. Estonian Natl. Electoral Comm. https://www.vvk.ee/public/dok/Report_E-voting_in_Estonia_2005-2009.pdf
[26] Venkatesan, K., & Rahayu, S.B. (2024). Blockchain security enhancement: Hybrid consensus and ML. Sci. Rep., 14, 1149.
[27] Wolchok, S., Wustrow, E., Halderman, J.A., et al. (2010). Security analysis of India's EVMs. ACM CCS 2010, 1-14.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)