International Journal of Law and Public Policy
Vol. 1, Issue. 4, Dec 2025, pp. 24~34
ISSN: 3107-6017

Legal and Technological Safeguards for Digital Elections: A Comprehensive Framework

Lakshmi M P
Assistant Professor, SRM School of Law, India.

Article Info

Article History:

Received Sep 28, 2025
Revised Oct 30, 2025
Accepted Nov 29, 2025

Keywords:

Legislation against cybercrime
Blockchain
Safe online elections
Electronic voting systems

ABSTRACT

Election procedures in contemporary democracies have changed dramatically as a result of the quick adoption of digital technology, which present new chances for effectiveness, accessibility, and transparency. To maintain electoral integrity, however, the use of digital voting devices also presents serious ethical, security, and legal issues that need to be resolved. In order to guarantee safe, reliable, and resilient digital elections, this paper offers a thorough framework that combines legislative protections with cutting-edge technology precautions. It describes the essential legal frameworks needed to control digital electoral infrastructure, such as data protection laws, cybercrime statutes, certification requirements, and voter rights safeguards. The framework looks at crucial technology protections such end-to-end encryption, identity systems, blockchain-based verification, intrusion detection, and hazard mitigation methods in addition to these regulatory measures. The study highlights the necessity of comprehensive governance, ongoing system assessment, and open auditing to combat new cyberthreats and bolster public confidence by combining the two domains. The suggested framework offers election officials, technologists, and policymakers an organised method for creating and executing safe digital election ecosystems.

Corresponding Author:

Lakshmi M P,
Assistant Professor, SRM School of Law, India.
E-mail: lakshmim5@srmist.edu.in

1. INTRODUCTION

Since the start of the twenty-first century, a number of opportunities and difficulties have arisen as a result of the integration of technology and law, which has changed the fundamentals of legal systems all over the world. The effortless incorporation of technological advances into every area of our daily existence has not only transformed the way we engage, and conduct company, it has also required a fundamental overhaul of the integrity and resilience of the legal structures on which our cultures depend. Examining the quality of the legal norm in this new digital environment is crucial since the relationship of law and technology has caused a complicated interaction between judicial models, ethical considerations, and technological advancements. The nature of the legal norm, which has long been renowned for its uniformity, clarity, and dedication to basic concepts, is today confronting a variety of unprecedented issues inspired and intensified by the infinite pace of technological progress. Information technology is now a ubiquitous force that

impacts everything from the creation and enforcement of contracts to the commission and prosecution of crimes. The degree of adaptability, efficacy, and equity of the laws that govern the way we live to these unforeseen and ever-increasing changes represents an extremely difficult challenge for the intricate makeup of modern judicial systems, which frequently refer to ancient precedents. The study will use an interdisciplinary approach, incorporating elements from the social sciences, technology, ethics, and law, in order to accomplish this [1]. We seek to illustrate the advantages and disadvantages of the existing legal frameworks in addressing the quick advancement of information technology through instances, judicial trends, and comparative analysis. In addition, we will examine possible approaches and suggestions for improving the legal foundation's quality to guarantee that it continues to be efficient and equitable in a society that is becoming more and more reliant on technology.

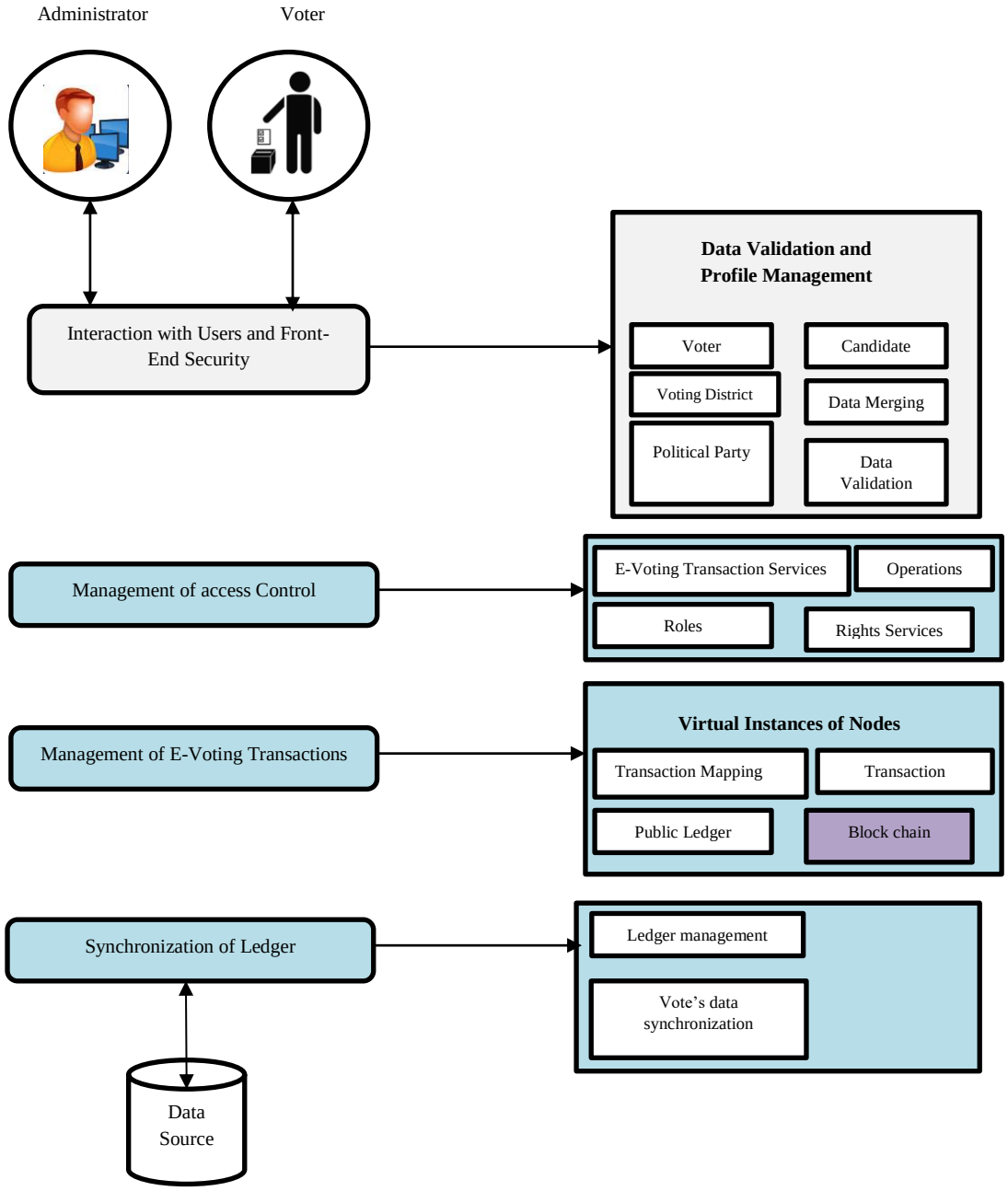

Figure 1. Architecture of the proposed e-voting system

The analysis covers a wide range of topics, such as the suitability of current legal models to deal with new technological issues [2], the function of legal experts in deciphering and implementing technological concepts, the consequences of technology-based legal reforms, and the protection of fundamental rights and moral principles in changing digital environments.

The VoteChain system's architecture, which was created to secure voting, is shown in Figure 1 [3]. Two essential elements that help voters and administrators manage elections are the User Interfaces (UI) and Front-End Security. Voter credentials are verified through secure techniques like username/password and One-Time Password (OTP) verification on the user interface (UI), which functions as the interaction portal. By guaranteeing adherence to system policies, this not only improves user experience but also safeguards the voting process. By defining and managing user roles, access control management makes sure that only those with the proper authorisation can carry out particular tasks. This module also starts the blockchain mining process and oversees the description of voting transactions.

By creating encrypted hashes and transaction IDs, the E-Voting Transactions Management Level guarantees the privacy of every vote. Additionally [4], it incorporates voter identities from the user interfaces and maps activities onto the blockchain. A mining technique that employs several virtual nodes enhances VoteChain's decentralised security and increases the system's resistance to manipulation.

By guaranteeing that all votes are safely recorded on a blockchain using cryptographic hashes, the Ledger Synchronisation Level is in charge of maintaining the local application's synchronisation with the multichain ledger. Additionally, this level uses smart contracts to compute the vote results, which are then announced at the conclusion of the polling period.

Vote tallies, voter registration information, and transaction histories are all kept as permanent recordings on the blockchain. Accessing and querying this data is essential for transparency, audits, and real-time election monitoring. At the moment, Vote Chain uses simple blockchain queries to obtain block data, intelligent contract events, and transaction logs via APIs offered by Ethereum and other platforms. This protects voter privacy while enabling stakeholders to monitor election progress and confirm votes.

Objectives

1. To assess how citizens can use digital tools to improve democratic integrity and electoral participation.
2. To investigate issues arising from digital change, such as privacy problems, digital divides, misinformation, and cyber dangers.
3. To evaluate Election Commission and government programs to raise rural residents' understanding of digital issues.
4. To propose ideas for policymakers to avoid digital misuse before Indian elections and increase democratic resilience.

2. LITERATURE REVIEW

Understanding the possible advantages and inherent dangers of electronic voting has attracted a lot of scholarly attention due to the growing use of computer technology in electoral systems. Classical Direct Recording Electronic (DRE) devices, which were first praised for their effectiveness and accessibility, were the main subject of early research. However, studies quickly revealed serious flaws in terms of openness, susceptibility to manipulation, absence of verifiable

paper trails, and reliance on proprietary, closed-source applications [5]. These worries sparked a second wave of research focused on cryptographic voting methods, which sought to provide end-to-end verifiability by allowing voters and auditors to verify election results without jeopardising ballot confidentiality. Though issues with coercion resistance, scaling, and usability remained topics of scholarly discussion, systems like Helios, Prêt-à-Voter, and Security showed creative methods to voter confirmation and cryptographic proof production.

Blockchain technology becomes a potent instrument for decentralised, unchangeable record keeping in tandem with these advancements. Because of blockchain's immutability, distributed consensus procedures, and public auditability [6], researchers started looking at its applicability for securing electronic voting. The ability of distributed ledgers to remove single points of failure, increase resistance to manipulation, and offer immediate verification of election events was demonstrated by studies looking into blockchain-enabled e-voting platforms, such as Voatz, FollowMyVote, and educational prototypes. However, the literature also warns that blockchain-based systems are vulnerable to consensus-level attacks like 51% or collusion-based threats, as well as problems related to metadata leaks and transaction traceability. Additionally, voters and administrators may face additional usability issues due to blockchain's technological complexity.

Legal scholars have studied the institutional and legislative conditions required to protect digital elections in addition to technological study. Voter data processing is subject to stringent regulations under data protection regimes like the EU's GDPR and India's DPDP Act, while cybercrime laws outline offences pertaining to voting system intrusion, deceit, or disruption. Transparency, accountability, and software independent are emphasised in election technology certification requirements published by organisations like the Council of Europe and the U.S. Election Support Commission [7]. Despite these gains, numerous studies show that current legal frameworks frequently fall behind the speed at which technology is developing, creating gaps in operational governance, accountability, and oversight. Researchers stress how important it is to incorporate legal protections—from liability regimes to procedural controls—directly into the development and implementation of digital voting systems.

When considered collectively, the corpus of available literature reveals a recurring gap between legal control and technological advancement [8]. Although decentralised security models, blockchain architectures, and cryptographic techniques present promising answers to long-standing election security issues, they cannot be implemented successfully without thorough legal oversight that guarantees procedural fairness, transparency, auditability, and privacy protection. Unified models that integrate advanced technical processes, cyber governance concepts, and regulatory measures into a single cohesive framework are lacking in the current research scene. By putting forth an integrated legal-technological paradigm intended to improve the robustness, reliability, and integrity of digital election ecosystems, this study aims to close that gap.

3. METHODS AND MATERIAL

This study uses a qualitative analytical approach that combines technical assessment, exploratory system analysis, and documentary research [9]. Below is a summary of the materials and techniques used.

3.1 Sampling and Participants

Three groups of participants are the subject of the study:

(1) Voters using digital electoral tools;

(2) Election administrators in charge of managing digital systems;

(3) Tech specialists working on the creation of e-voting systems.

In order to ensure representation from rural and urban environments, different levels of computer literacy, and institutional players including Election Commission officials and technical employees, a purposive sample strategy was employed to select pertinent groups.

3.2 Method of Data Collection

Documents analysis of government documents, election standards, academic literature, technical papers of blockchain-based vote platforms, and legal regulations were used to gather data. Secondary data, such as instances of digital elections [10], publicly accessible Election Commission datasets, and system design documents for the Vote Chain model, provided further insights. To evaluate practical implementation qualities, technical tools like Truffle, Ganache, and MetaMask were looked at.

3.4 Analysis of Data

Thematic and comparative analytic techniques were used to examine the data. To find important regulatory trends, governance gaps, and conformity needs, legal materials were analysed. To assess system architecture, safety features, and potential vulnerabilities, technical sources were examined. Conceptual system analysis was used to evaluate the Vote Chain model's compliance with technological and legal protections [11]. In order to create an integrated framework that combined legal and technological aspects, the results of these investigations were triangulated.

3.5 Vote Chain: Block Organisation

Vote Chain is built on Distributed Ledger Technology (DLT), which guarantees a safe, transparent, and unchangeable voting environment. Every block has crucial elements that protect system integrity and vote confidentiality. Voter IDs are securely connected to encrypted votes stored on the blockchain and are assigned at random to preserve anonymity. Hash-based signatures created with the voter's private key are used to validate votes, guaranteeing validity without sacrificing confidentiality. While the SHA-256-based hashing linking system assures that any tampering efforts are instantly visible, timestamping maintains chronological fairness.

3.6 The Implementation Structure of Vote Chain

To provide safe, effective, and scalable system functionality, Vote Chain incorporates a number of development tools, such as NPM [12], Truffle, Ganache, MetaMask, VS Code, MongoDB, and Twilio. When these tools are used together, decentralised app creation, real-time authorisation, data storage, validation, and interaction with users are all made easier while adhering to blockchain security guidelines.

3.7 Smart Contracts and Vote Chain's Technical Architecture

The Ethereum blockchain is the foundation of the Vote Chain system, which provides a dependable and transparent online voting procedure. By requiring validated entities to stake their assets and using financial penalties to deter bad activity, the Casper Proof-of-Stake agreement process improves security. With MetaMask-enabled voting interfaces, Vote Chain allows for widespread involvement while providing flexibility and security through both entire nodes and service nodes. By automating voter registration, voting, and result computation, smart contracts promote transparency and reduce human error.

3.8 Vote Chain: Block Organisation

Voter ID is a unique number that is given to eligible voters at random. It preserves voter anonymity by enabling accurate identification without revealing personal information. The blockchain safely records the choice cast as the voter's choice, ensuring that each vote is cast and stored with the highest security measures. Vote validation is made possible while preserving the anonymity of the vote's contents by using the voter's secret key for signing the vote's hash.

The timestamp records the precise moment each block was sent, which helps to verify equality when multiple files have equal time stamps.

The digest (Hash) of the Last Blocks links each block to its predecessor using the SHA-256 technique to maintain the chain's impenetrability [13]. Any alteration to a block would be immediately identifiable due to the hole in the cryptography link.

3.9 The Implementation Structure of Vote Chain

Vote Chain is built using a range of tools and technologies, each of which makes a unique contribution to the creation and maintenance of the system's functionality. This section provides a more detailed description of the rationale behind each tool's selection as well as how they complement the Vote Chain scheme to ensure accessible, safe, and efficient electronic voting.

Node Package Management (NPM), a well-liked JavaScript package management system, makes it simpler to add and update third-party packages. By supplying the libraries and dependencies required for the Vote Chain application, it provides developers with easy access to a vast ecosystem of packages. This makes the development process easier because Vote Chain programmers can efficiently install and maintain cryptographic libraries, testing mechanisms, and necessary modules for the Ethereum network's integration.

The Truffle Framework is the primary development environment for creating decentralised apps (DApps) on the the Ethereum network. It offers comprehensive tools for developing, integrating, and putting into practice smart contracts. In Vote Chain, Truffle facilitates the development and testing of Solidity-based smart contracts. The platform also provides testing tools that allow developers to simulate various voting scenarios in order to ensure that the smart contracts operate as intended before deployment.

Ethereum uses Ganache as a local blockchain to replicate the blockchain environment. It makes it possible for developers to test each stage of the voting procedure in a controlled environment, including casting votes, confirming transactions, and maintaining data immutability. By eliminating the need to interact with the main Ethereum network during the development stage, testing becomes more efficient.

MetaMask, a plugin for the browser that functions as an Ethereum wallet, is used by Vote Chain users to control their voting activities [14]. MetaMask allows users to interact with the blockchain directly from their browser, sign transactions, and monitor their voting status. Thanks to this connection, voters may cast their ballots safely and have total control over transaction approvals and private information.

The Visual Studio Code (VS Code) is the primary development environment for the Vote Chain project. It provides developers with a robust code editor that makes version control, code linting, bugging, and support for extensions easier. These characteristics, which are essential for developing, testing, and deploying smart contracts and other components of the Vote Chain infrastructure, make Visual Studio Code an indispensable tool for the development team.

MongoDB is an open- source NoSQL database that holds crucial auxiliary data, such as voting records, login tokens, and registration details. While the Ethereum ledger safely keeps the crucial vote data, MongoDB enhances the system's scalability and agility by efficiently managing user sessions and logging login histories.

Twilio, a cloud-based connection provider that offers One-Time Passwords (OTPs) via email or SMS for voter authentication, is integrated into Vote Chain. This two-factor authentication method enhances security and prevents unauthorised access by restricting voting platform access to only registered voters.

Because these tools are used together, Vote Chain is built with longevity, efficacy, and safety in mind. The Ethereum blockchain, which provides security, transparency, and immutability, serves as the system's foundation. Meanwhile, Truffle and Ganache speed up the creation and testing of the decentralised application. MetaMask gives voters an intuitive interface, and MongoDB and Twilio offer crucial functionality for managing voter data and registration. Lastly, a robust development environment that supports the platform's continuous growth and scalability is produced using NPM and Visual Studio Code.

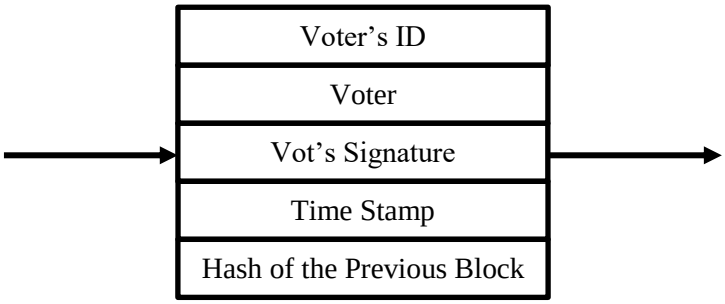

Figure 2. Voting Block

Vote Chain's blockchain framework, which ensures a secure, transparent, and immutable electronic voting process, is built on Distributed Ledger Technology (DLT). The anonymity and legitimacy of the voting process depend on each block on the blockchain. Each of these blocks contains several essential elements (see Figure 2) [15] that combine to provide a confirmed and tamper-resistant voting mechanism.

3.10 Vote Chain: Implementation, Smart Contracts, and Technical Architecture

The suggested Vote Chain system uses the Ethereum network, which is a blockchain that is open-source for distributed applications, to offer a secure and transparent way to vote. Candidates and citizens can register and participate in elections by integrating the Vote Chain with the bitcoin wallet MetaMask.

Transparency in the voting process is ensured by the Central Election Commission (CEC), which is in charge of the system. Voters cast their ballots via Vote Chain using two different types of nodes: Full Nodes, that are directly connected to the blockchain of Ethereum and provide greater security, and Service Nodes, which are accessible via wallets or cloud services and provide a more straightforward Vote Chain interaction. A key element of Vote Chain is the Casper agreement mechanism, which employs a Proof-of-Stake (PoS) protocol. PoS allows validators to "stake" cryptocurrency as collateral. Validators are selected to propose or validate fresh blocks based on their committed assets, significantly enhancing system security while also lowering energy consumption. Validators who act dishonestly run the risk of losing their promised assets, which

discourages such activity. VoteChain protects the voting process from fraud and manipulation by ensuring that actions are securely authenticated.

4. IMPLEMENTATION AND EXPERIMENTAL RESULTS

4.1 India's Election Landscape's Digital Transformation

From early wireless-based campaigning to AI-driven political initiatives, India's electoral processes have experienced a substantial technical transformation. Campaign outreach, voter participation, and political communication have changed as a result of the increasing adoption of mobile phones, the growth of social networking sites, and recent developments in artificial intelligence. Big data, algorithm targeting, WhatsApp platforms [16], and AI-generated content—such as voice clones, deepfakes, and multilingual automated messages—are all being used by political parties more frequently to sway public opinion and rally voters. These developments increase electoral reach, but they also bring with them concerns related to digital inequality, disinformation, and manipulation.

Over the span of three decades, India's electoral landscape has significantly changed due to the incorporation of modern technology. The widespread usage of phones in the 1990s marked the beginning of this transition, which continued with the first "mass mobile phone" elections in Uttar Pradesh in 2007, the introduction of virtual reality in 2014, and the current AI-driven period in 2024. Social media's influence increased during the 2014 elections, and artificial intelligence was introduced in 2024, completely changing election dynamics and campaign tactics. Two important themes came together during the 16th National Elections: the growing number of young voters and the growing influence of technology.

In order to further Prime Minister Narendra Modi's campaign, the Bharatiya Janata Party (BJP) carefully used big data as well as technology, hiring more than 100 young tech experts. Similar to U.S. President Obama's campaign, data-driven research was used to improve ads, maximise fundraising efforts, and create micro-targeted plans. Leaders and voters were directly connected through digital projects like "Chai peCharcha" and 3D rallies, which facilitated conversations about security, governance, and agricultural challenges. Due to the app's extensive use in voter mobilisation, organisation, and accurate information delivery, the 2019 General Elections were dubbed "WhatsApp elections." Given that more than 40% of Indians use smartphones, political parties used apps like WhatsApp to interact with people and plan campaigns. With technology driving outreach and participation, this signalled the start of an era of change in politics.

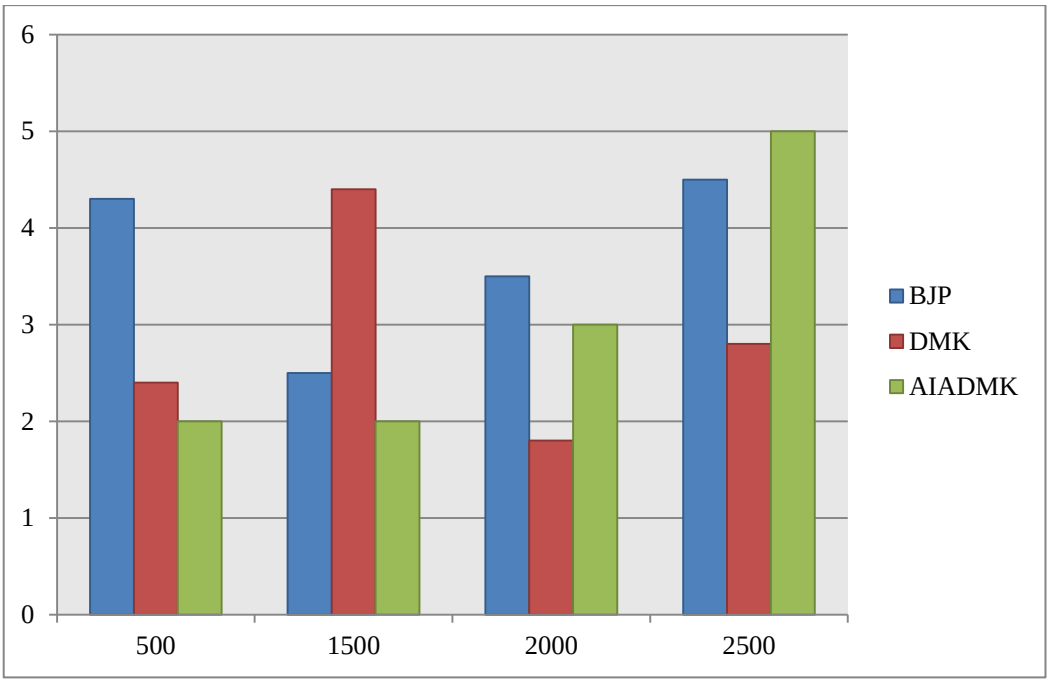

Figure 3. Amount spent by politician parties on Google ads

On the one other hand in Figure 3, the Indian National Congress (INC) used the "GharGhar Congress" app to monitor ground activity while deploying a ground-based team with data dockets to provide tailored messaging to voters via social media. In contrast, the BJP appointed approximately 9, 00,000 "Cell Phone Pramukh," one for every polling place. Amit Shah, the party president at the time, created a "booth action plan" that required state units to compile a list of smartphone users at every polling place. The Delhi war room of the party assimilated this data. After identifying important cell phone contacts, leaders—including MPs and office bearers—formed three WhatsApp groups, each with 256 members, for each polling place. In order to provide focused campaign materials on topics like the party's welfare programs, Modi's character, triple talaq, and the Ram temple, the central war room and the BJP's IT department worked with reputable businesses.

Nodal contacts at voting places disseminated these materials in their WhatsApp groups after they were sent to the voting war room extension in each state. By constantly interacting with PM Narendra Modi's fans on X (previously Twitter), the BJP effectively seized on his broad popularity and increased his online influence. Rahul Gandhi, the INC president at the time, on the other hand, did not employ a similar tactic to interact with voters on social networking sites despite receiving greater attention for his post. This difference in strategy let the BJP dominate the political discourse on X. AI in the 2024 Lok Sabha Elections: From Deep Fakes to Voice Clones A paradigm change occurred during the 2024 Lok Sabha Elections as both the BJP and INC used AI to improve their campaigns. Voice clones, AI-generated videos, customised audio messages in various Indian languages, robotic calls to voters in a candidate's voice, deepfakes, and AI-generated music and memes were all examples of AI-generated material.

The voter's emotional connection to their leaders was exploited by the hyper-realistic AI-generated content. AI was used by the BJP, which has become the pioneer in implementing cutting-edge technology, to translate PM Narendra Modi's talks into other regional languages, expanding their audience and portraying the leader as approachable by all societal groups. In order to support their current leaders, parties like Dravida Munnetra Kazagham (DMK) used voice clones and deepfakes to bring back prominent politicians like M. Karunanidhi. Arvind Kejriwal also used the

AI speech clones to campaign while incarcerated. Parties also employed deepfakes, propaganda photos, and AI parody films to intensify their meme wars.

5. CONCLUSION

Election systems are now more transparent, accessible, and efficient because to digitalisation, yet issues with digital disparities, false information, security, and regulatory gaps still exist. Although tools like C-Vigil and the "Know Your Candidate" app increase openness, their restricted disclosure policies and operational opacity expose accountability flaws. While there are many advantages to artificial intelligence, such as quick verification, managing massive voter datasets, and voter participation via automated platforms, there are also risks, such as the spread of deepfakes, political manipulation, and false information. There are serious issues with the lack of a thorough legislative framework governing the use of AI in elections. Coordinated efforts between legislators, engineers, and legal authorities will be necessary for effective governance in order to prevent the advancement of digital tools from undermining democratic integrity.

Digitalisation and online voter registration have revolutionised the election process by improving accessibility and transparency, yet issues like the digital divide and false information still exist, particularly in remote places with poor connectivity. By giving voters comprehensive information on political candidates, such as their financial holdings, liabilities, and criminal histories, the "Know Your Candidate" (KYC) app aims to empower voters. This program boosts openness and encourages accountability, allowing voters to make educated decisions and select politicians who uphold integrity, thus fostering a more honest and fair political process. In the absence of particular legislation controlling AI use in the nation, the Election Commission of India (ECI) performs a significant role.

Apps like C-Vigil improve electronic access to the ECI, but their operations are still opaque and do not provide the type of complaints or how they were resolved. While AI has the potential to change information transmission and attain an 80% correct voter validation rate, it also has hazards. With the capacity to oversee voter data for almost 900 million voters while educating voters more successfully through educational websites and chatbots, it can greatly increase access to political procedures. On the other hand, unrestrained AI use raises questions about the dissemination of both true and false information, which could threaten societal institutions and cause political upheaval. The problem is how government officials will control and categorise content as deceptive or fraudulent in the face of swift technical progress.

REFERENCES

[1] Rekbi, R. (2024). LEGAL FRAMEWORKS IN THE ERA OF DIGITAL TECHNOLOGY. *Russian Law Journal*, *12*(2), 2814-2825.

[2] Polotnianko, O. (2024). The use of modern information technologies during elections in developed countries. *Visegrad Journal on Human Rights*, (6), 84-90.

[3] Chaturvedi, S. (2025). The Digital Transformation of Indian Elections: Opportunities and Challenges for Democratic Integrity. *IJSAT-International Journal on Science and Technology*, *16*(1).

[4] Fyneroad, Z. I., & Akeuseph, O. (2024). Sovereignty in the Digital Age: Examining Foreign Interference in US Elections through the Lens of International and Domestic Law. *Issue 6 Int'l JL Mgmt. & Human.*, *7*, 9.

[5] Olaniyi, O. O. (2024). Ballots and padlocks: Building digital trust and security in democracy through information governance strategies and blockchain technologies. *Available at SSRN 4759942*.

[6] Asimakopoulos, G., Antonopoulou, H., Giotopoulos, K., & Halkiopoulos, C. (2025). Impact of information and communication technologies on democratic processes and citizen participation. *Societies*, *15*(2), 40.

[7] Babikian, J. (2023). Securing Rights: Legal Frameworks for Privacy and Data Protection in the Digital Era. *Law Research Journal*, *1*(2), 91-101.

[8] Gauja, A. (2021). Digital democracy: Big technology and the regulation of politics. *University of New South Wales Law Journal, The*, *44*(3), 959-982.

[9] Dad, N., & Khan, S. (2023). Reconstructing elections in a digital world. *South African Journal of International Affairs*, *30*(3), 473-496.

[10] Mustafa, G., Rafiq, W., Jhamat, N., Arshad, Z., & Rana, F. A. (2025). Blockchain-based governance models in e-government: a comprehensive framework for legal, technical, ethical and security considerations. *International Journal of Law and Management*, *67*(1), 37-55.

[11] Gorwa, R. (2021). Elections, institutions, and the regulatory politics of platform governance: The case of the German NetzDG. *Telecommunications Policy*, *45*(6), 102145.

[12] Hajian Berenjestanaki, M., Barzegar, H. R., El Ioini, N., & Pahl, C. (2023). Blockchain-based e-voting systems: a technology review. *Electronics*, *13*(1), 17.

[13] Dowling, M. E. (2022). Foreign interference and digital democracy: is digital era governance putting Australia at risk?. *Australian Journal of Political Science*, *57*(2), 113-128.

[14] Ndubuisi, A. F. (2022). Cross-border jurisdiction challenges in prosecuting cybercrime syndicates targeting national financial and electoral systems. *International Journal of Engineering Technology Research & Management (IJETRM)*, *6*(11), 243-261.

[15] Hossain Faruk, M. J., Alam, F., Islam, M., & Rahman, A. (2024). Transforming online voting: a novel system utilizing blockchain and biometric verification for enhanced security, privacy, and transparency. *Cluster Computing*, *27*(4), 4015-4034.

[16] Shandilya, S. K., Datta, A., Kartik, Y., & Nagar, A. (2024). Navigating the regulatory landscape. In *Digital Resilience: Navigating Disruption and Safeguarding Data Privacy* (pp. 127-240). Cham: Springer Nature Switzerland.