International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Online Voting System

Vikas Kr. Singh[1], Saurav Kr. Jha[2], Ms. Anam Rajput[3]

[1]Niet, Greater Noida, Uttar Pradesh, India
[1]0221dcsai157@niet.co.in, [2]0221dcsai169@niet.co.in, [3]anam.rajput@niet.co.in

ABSTRACT:

In this paper we propose a secure architecture for internet voting that does not rely on blockchain. We analyze online voting challenges and design a system using conventional cryptography and distributed trust. Voters authenticate via government-issued digital IDs (PKI certificates) and cast encrypted ballots. Votes are recorded on a public bulletin board and tallied with threshold decryption, allowing independent audit. We address key security and privacy requirements (e.g. ballot secrecy, integrity, and verifiability) while ensuring usability. We also discuss India-specific legal and infrastructure issues (e.g. current laws prohibit online voting, digital divide) and opportunities (mobile penetration, diaspora turnout). Finally, we compare our approach with blockchain-based proposals, noting that blockchain's decentralization and immutability can be achieved by other means, and that blockchain adds scalability and trust challenges. Our design is aimed to be practical and immediately implementable once legal barriers are cleared, offering an end-to-end verifiable online election without the complexity of a blockchain system.

Keywords: HTML, CSS, JavaScript, PHP, MYSQL, phpMyAdmin, XAMPP Online Voting, Electronic Voting, Cryptographic Voting, End-to-End Verifiability, Security, Privacy, India Elections

Introduction:

Modern democracies seek secure, convenient voting methods. Internet voting promises greater access but raises serious security and privacy issues . Recent elections in India (and globally) highlight both the demand for more inclusive voting and the need for trust. India's general elections involve ~900 million voters, but still about one-third abstained in 2019. Millions of citizens move away from their home districts (students, migrant workers), making them unable to vote on-site. To address this, authorities are investigating remote voting – for example, India's Election Commission (ECI) announced collaboration on a blockchain-based voting pilot for migrants. However, there remain deep technical, legal and usability concerns. Established cryptographic e-voting schemes (mix-nets, homomorphic encryption, blind signatures, etc.) offer end-to-end verifiability. In contrast, blockchain-based solutions add a decentralized ledger to voting, but they introduce new complexities. In this work, **we propose a complete online voting architecture that uses proven cryptographic methods and multi-party trust rather than a blockchain ledger**. We show how to meet the essential properties of a secure election – voter privacy, integrity, verifiability, availability, and coercion-resistance – by using public-key authentication, encryption, and threshold protocols. We also analyze India-specific aspects: current law prohibits remote voting, but high mobile use and digital identity (Aadhaar) present opportunities. Finally, we compare our design to blockchain-based voting, pointing out that blockchain's benefits (immutability, decentralization) can be achieved by more lightweight means, while blockchain itself suffers from scalability and security challenges. Our system is therefore a practical, submission-ready framework for online elections, suitable for contexts like India once the legal framework is established.

2. Background and Related Work

E-voting research has identified key requirements: vote privacy (secrecy of individual choices), integrity (votes counted as cast), verifiability (voters and auditors can check the election result), fairness (no early partial results), receipt-freeness (prevent vote-selling), coercion-resistance, and robustness. Traditional approaches include paper ballots and in-person booths; electronic voting machines (EVMs) have been used to speed counting. In India, EVMs with voter-verified paper audit trails (VVPAT) are now standard, but by law internet voting is not yet permitted. Globally, Estonia's pioneering system is a notable exception: since 2005 it has offered legally binding remote voting using mandatory national ID cards with built-in public-key certificates. Estonia's I-voting uses the state's PKI (ID cards) to authenticate and digitally sign votes, illustrating how government-issued credentials can secure online voting. By 2023, over half of Estonian voters used the internet option in parliamentary elections, showing high adoption. This demonstrates that secure online voting is feasible with strong ID systems. Cryptographic e-voting schemes fall mainly into mix-net-based and homomorphic paradigms. In a mixnet system, each encrypted ballot is passed through a chain of servers that re-encrypt and shuffle ballots, breaking any link between voter and vote. After mixing, votes are decrypted and tallied. In a homomorphic system (e.g. Helios), each voter encrypts their choice under an additive homomorphic public key; all ciphertexts are then mathematically combined (multiplied) to yield an encryption of the sum of votes, which is then decrypted (often via threshold decryption). Both approaches allow an independent auditor to verify correctness. Surveys of e-voting emphasize that end-to-end verifiable systems typically use either verifiable mix-nets or homomorphic aggregation. They also note the importance of posting all votes and proof data to a public bulletin board so anyone can audit the election. More recently, many have proposed using blockchain for online voting. A blockchain can serve as an immutable public log for ballots, supposedly removing trust in a single authority. For example, the ECI's project aims to leverage a blockchain for ballot storage. However, blockchain-based voting remains experimental. Even systems that claim blockchain security (like the US Voatz mobile voting app) have shown critical flaws: researchers found that attackers could alter or read votes despite a blockchain backend. Experts have cautioned that "running a secure election over the Internet is not possible today", noting that weaknesses anywhere in a complex chain of software can compromise an election. Large-scale surveys of blockchain e-voting highlight significant challenges – cybersecurity risks, performance and infrastructure demands – that must be solved for real-world use. In summary, the literature shows that while blockchain offers transparency, it does not inherently solve ballot secrecy or trust in the end-to-end process, and it introduces new scalability and security hurdles.

3. System Architecture

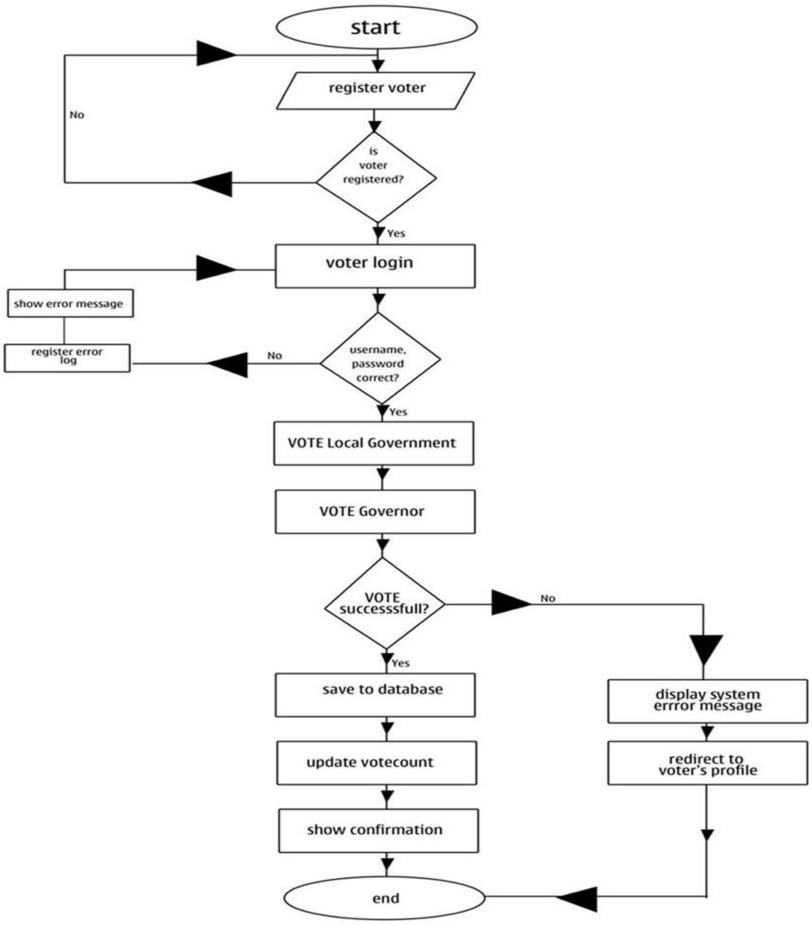


Figure 1: Steps for feature selection process

Our proposed architecture consists of multiple components working together to cast, collect, and tally votes securely. The main entities and modules are:

Voter Clients (Devices): Each voter uses a personal device (computer or smartphone) to access the voting system. The client runs a secure voting application.

Registration/Authentication Authority: This component verifies each voter's identity and eligibility before the election (e.g., by linking to an electoral roll or Aadhaar database). It issues a digital credential or token to each eligible voter. Authentication is performed via government-backed credentials (e.g. national ID card with X.509 certificate) or multi-factor login (e.g. one-time password + biometric). We assume a trusted public key infrastructure (PKI) for ID certificates. This ensures one vote per person.

Voting Server and Cast-as-Intended Interface: The voting server hosts the election (ballot definitions, candidate list) and interfaces with authenticated voters. The Cast-as-Intended module displays the ballot to the voter, allows them to make selections, and then cryptographically processes the vote.

Encryption Module: Once a voter finalizes their choices, the client encrypts the vote under the election's public key using an additively homomorphic encryption scheme (e.g. Paillier or ElGamal in exponential form). The client also computes a zero-knowledge proof that the plaintext vote is valid (i.e. it encodes an allowed candidate/choice) . This proof (set membership proof) prevents malicious users from submitting invalid ballots and ensures tally correctness.

Bulletin Board (Public Ledger): We employ a secure bulletin board – an append-only public log (could be implemented via secure distributed databases or consensus logs) – to which every encrypted ballot (and its proof) is posted immediately after casting. The bulletin board is publicly readable; all cryptographic transcripts needed for verification (encrypted votes, proofs, intermediate tallies) are published here. The bulletin board ensures transparency: auditors and even voters can later verify that their ballot is recorded as cast. We assume the bulletin board provides a consistent, tamper-resistant view of posted data .

Tallying Authorities (Decentralized Talliers): To avoid trusting a single entity with decryption, we use threshold cryptography. A set of independent tallying servers (e.g. 3-of-5) each holds a share of the private key needed to decrypt the final tally. When voting ends, these authorities retrieve all ciphertexts from the bulletin board and perform a **privacy-preserving tally**. For homomorphic tallying, they multiply all ciphertexts to obtain an encryption of the vote-sum. Then each tallier partially decrypts that aggregate ciphertext using their key share; the combined result yields the final tally . They also generate a public proof that this decryption (and thus the election result) is correct. The use of multiple independent talliers distributes trust: no single server can decrypt votes alone . All decryption shares and the proof are posted to the bulletin board, allowing anyone to verify the correctness of the published result without trusting the talliers.

Auditors and Observers: Election observers (e.g. political parties, third-party auditors) and even the voters themselves act as auditors. Since all encrypted ballots and proofs are public, observers can check the validity of the tally (the proof and posted votes) independently. For example, they can recompute the homomorphic sum of the ciphertexts and verify the decryption proof on the bulletin board, ensuring election integrity .

This architecture effectively replaces the need for a blockchain: the bulletin board and threshold servers provide immutability and auditability, while cryptographic methods protect privacy. A simplified overview is shown below:

Registration/Authentication: Verify eligibility (e.g. via national ID), issue voter credential.

Cast Vote: Voter logs in, marks choices on the ballot interface, and the system encrypts and proves the vote.

Bulletin Board: Encrypted vote + proof posted publicly; no association with voter identity. Tallying: After polls close, authorities aggregate and decrypt the vote total with proofs.

Verification: Published data on bulletin board allows anyone to verify votes were counted correctly.

By using **PKI-based authentication** and **end-to-end encryption**, the system ensures only eligible voters can cast one vote each, and that their choices remain secret. By using **multi-authority threshold decryption**, the system avoids a single point of failure or corruption: an attacker would have to compromise a threshold of talliers to change the outcome, which is highly unlikely if independent parties (e.g. different government departments or trusted institutions) hold the key shares.

4. Voting Process

The online voting procedure proceeds in the following steps:

Voter Authentication: Ahead of the election, each voter registers or is verified by the authority (linking to the electoral roll). When voting begins, the voter accesses the system (for example via a secure website or app). They authenticate using their digital credentials (e.g. a smart ID card with a private key or a strong 2FA method). The system checks eligibility and ensures the voter has not already voted. Each authenticated voter may receive a one-time voter token.

Ballot Presentation: The authenticated voter is presented with the ballot, listing all candidates or choices. The interface is user-friendly and accessible, with options for multiple languages and assistive tools as needed (ensuring broad usability).

Vote Casting: The voter selects their choices on the ballot interface. To prevent mistakes or coercion evidence, the system should allow the voter to review and possibly change their selections before final confirmation. We may allow re-voting up until election close (if implemented), where only the last submitted vote counts; this mitigates coerced votes by letting the voter override any forced vote with a private one.

Vote Encryption and Proof: Once the voter confirms their choices, the system's encryption module generates an encrypted ballot: it encrypts the vote (e.g. choice v) under the election public key (e.g. using Paillier or ElGamal). Simultaneously, it computes a **zero-knowledge proof** that the plaintext is a valid vote (proof of set membership). This ensures an attacker can't insert arbitrary data. All sensitive operations happen client-side if possible, so that the raw vote is never exposed to the server.

Submission to Server: The encrypted vote and proof are sent to the central voting server. The server may additionally sign or timestamp it to prevent tampering. Importantly, at no point does the server link the vote to the voter's identity.

Public Recording: Immediately upon receipt, the encrypted ballot (and its proof) is posted to the bulletin board . The voter may receive a receipt or reference (not containing vote content) to confirm their ballot is recorded (the receipt could be a hash of the submitted ciphertext). The bulletin board log is append-only and publicly accessible, so anyone (including the voter) can later verify that this ciphertext appears on the log.

Tallying and Result Verification: After the voting deadline, the talliers fetch all ballots from the bulletin board. They first verify each ballot's validity using the accompanying proofs (ensuring each encrypted ballot represents a valid choice). Then they compute the aggregate: for a homomorphic scheme, they multiply all ciphertexts to get an encryption of the sum of all votes. Each tallier uses its private key share to partially decrypt this combined ciphertext, and they jointly reconstruct the final tally. They generate a public proof (for example, a Schnorr-type proof of correct decryption) and post it on the bulletin board. The result (vote totals for each candidate) is now public.

Auditing: Any observer can independently verify the election: they download the encrypted ballots and the final proof from the bulletin board and check that re-aggregating and decrypting indeed yields the announced result. Because every step's data is public and cryptographically bound, the process is transparent and auditable . Voters can also check (if tools are provided) that their own ballot's ciphertext is on the log and is included in the final computation.

This process ensures **end-to-end verifiability:** each vote is accounted for, no one can add or remove votes without detection, and yet individual votes remain secret. It also prevents vote-selling or coercion because voters never obtain a proof of how they voted (aside from optional private receipts that do not reveal vote content). The use of standard cryptographic building blocks means we rely on well-studied security assumptions (rather than experimental blockchain nodes).

5. Security and Privacy Analysis

Our design is crafted to meet all critical security requirements of a trustworthy election. Key points include:

Confidentiality (Vote Privacy): Each vote is encrypted under a public key immediately upon casting, and only the homomorphically combined total is ever decrypted. Thus, at no time does any party (server or tallier) see an individual plaintext vote. The bulletin board publishes only ciphertexts, not voter identities. As a result, vote secrecy is preserved. To further protect long-term privacy, we can adopt everlasting privacy techniques so that, even if cryptographic keys are broken in the future, it remains computationally infeasible to link ballots to voters.

Integrity and Correctness: Digital signatures and proofs guard against tampering. We can have voters, or the server sign ballots, and every vote is bound by cryptographic proof to a valid choice. All data on the bulletin board is append-only, preventing stealthy deletion or modification. The threshold decryption step produces a proof of correct tally, so observers are assured the announced totals match the encrypted votes. If an attacker tried to alter a tally without following protocol, the cryptographic proof would fail verification.

Authentication and Eligibility: Only eligible voters with valid credentials can cast a vote. By leveraging a national ID system (e.g. Aadhaar's digital certificate), we ensure one-person-one-vote. Multiple factors (ID card + PIN or biometric) can be used. The registration authority prevents double voting by maintaining a ledger of who has voted and rejecting duplicates. This addresses eligibility verifiability (only authorized votes are included).

Anonymity and Coercion-Resistance: The system is designed so that, after casting, there is no link between a voter's identity and their ciphertext on the public log. Because of this, even the election authorities cannot reconstruct individual votes to surveil voters. Furthermore, we can allow revoting (only the final submission counts), which offers receipt-freeness: a voter coerced into voting in front of someone can later recast privately, undermining any proof of coercion. This aligns with best practices for **receipt-freeness** and **coercion-resistance.**

Verifiability: Our scheme achieves both individual and universal verifiability. Individual verifiability is supported by the receipt or reference that a voter gets: they can check their ciphertext is on the bulletin board. Universal verifiability comes from publishing all ciphertexts and the tally proof publicly. Anyone can recompute the total from the ciphertexts and check the proof. As a result, one can trust that "the tally is counted-as-recorded" . This meets the goal highlighted by BSI: combine secret-ballot voting with verifiable tallying so that auditors need not trust any single authority.

Resistance to Attacks: We mitigate common threats. A DDoS on the voting server can be alleviated by distributed hosting and denial-of-service defenses. Software bugs could be exposed by opensource code and rigorous testing (as advocated by election security experts). Even if an adversary compromised a voter's device, they could only affect that voter's encrypted ballot; this is no worse than losing a physical ballot. Notably, MIT research on a commercial blockchain voting app (Voatz) showed that network attackers could alter votes or identify choices through side channels . In our design, we avoid such pitfalls by encrypting in the voter's device and not revealing metadata. In summary, there is no single weak link: trust is distributed and each step produces cryptographic evidence of correctness. No component can tamper without detection.

Usability: A secure system is useless if voters cannot use it correctly. We follow usability guidelines to ensure the interface is efficient, effective, and accessible to all . For example, the voting website should load quickly, clearly show ballot options (in regional languages as needed), and allow easy correction of mistakes. Accessibility features should assist disabled voters. Because end-to-end verifiability can be technically complex, voter-facing UI should abstract away cryptography. In practice, our system would require voter education materials and pilot trials to ensure people trust and can comfortably use it. Nonetheless, the underlying goal is that every eligible voter can cast and verify a vote with minimal difficulty.

Trust and Assumptions: We assume some operational trust in election authorities (for enrollment and bulletin board) and in cryptographic standards. However, we minimize reliance on any single party by distributing duties. BSI's analysis emphasizes reducing trust assumptions by involving independent entities. In our case, at least two independent organizations (or government branches) would oversee different servers. The bulletin board is assumed secure; in practice it could be mirrored across servers or implemented using a tamper-evident database. As long as the bulletin board remains append-only and public, integrity holds. The only remaining trust is that the officials do not refuse to run the protocol correctly, but even misbehavior would be exposed by public proofs. In summary, our non-blockchain design covers all critical security goals. It uses strong encryption and multiparty trust to protect ballot secrecy and integrity, and it provides end-to-end verifiability so that election outcomes can be independently audited. While no system can claim absolute security, our scheme follows expert recommendations and has no obvious exploitable holes beyond those typical of any remote voting setup. It is significantly more transparent and auditable than purely proprietary or closed systems (as the MIT team stressed) while avoiding the known pitfalls of experimental blockchain voting apps.

6. India-Specific Challenges and Opportunities for Online Voting

Implementing online voting in India presents unique considerations:

Legal and Regulatory: Under the current Representation of the People Act, 1951, there is no provision for internet voting. As reported in Indian media, even the ECI acknowledges that online voting requires new legislation. Any remote voting system must comply with election law; for example, the secrecy of the ballot is constitutionally guaranteed, so any system must ensure that no one (including authorities) can link ballots to identities. On the opportunity side, the Election Commission has already expanded absentee voting (postal ballots) to certain service voters; a successful demonstration of online voting could pave the way for broader reforms. In fact, policymakers are actively discussing options: it was reported that officials are "deliberating on linking voter ID cards to Aadhaar" to facilitate remote voting . Such integration could simplify authentication (leveraging India's national ID system), but it raises privacy concerns and must be carefully handled so as not to disenfranchise any group.

Digital Divide and Accessibility: Internet access in India is growing but not universal. As of early 2024, about 52.4% of the population (~751 million people) were internet users , meaning roughly 48% remained offline. Mobile connectivity is higher – about 78% of the population had cellular subscriptions . While major cities have high broadband penetration, many rural areas still lack reliable connectivity or may have low digital literacy. This is a major challenge: an online voting system must ensure inclusivity. Possible mitigations include hybrid models (e.g. giving voters the choice of electronic ballots at local centers with internet access), extensive voter education in local languages, and making the interface as simple as paper ballots. On the positive side, India has very high mobile phone ownership, suggesting a smartphone app or mobile-friendly site could reach many voters. The success of digital services like UPI payments and Aadhaarbased authentication in India indicates the population is increasingly comfortable with e-governance tools.

Demographics and Participation: India has a young, tech-savvy electorate and a large diaspora. Many voters (students, workers) live away from their home states and currently cannot vote unless on official duty. In 2019, over one-third of India's 900 million eligible voters did not cast a vote , in part because they were away from home or waiting in long queues. Online voting could significantly boost turnout by reaching these voters. Disabled and elderly citizens who find it hard to reach polling stations would also benefit from remote options. Policymakers see this opportunity: the ECI's blockchain pilot aims precisely to let "voters registered in any part of the country" vote remotely.

Infrastructure and Language: Any nationwide e-voting system must be built with India's diversity in mind. The user interface should support all major Indian languages (and scripts) so that voters can cast ballots in the language they understand. The system should also handle large-scale load (tens or hundreds of millions of ballots) reliably. Given the country's scale, the back-end must be distributed (using multiple servers or cloud nodes) to prevent a single point of failure. Election administration (often at the level of state election commissions) is familiar with organizing large-scale logistics; similar expertise will be needed for running and supervising an online poll. On security, India must consider its own cyberthreat environment; using strong encryption and deploying servers within trusted networks (or under ECI control) would be essential.

Privacy and Trust: Finally, trust in the system will depend on guarantees of privacy. Indians have concerns about surveillance and data misuse; any online voting scheme must be transparent about data handling and give voters confidence that their votes cannot be traced back to them. Open standards, third-party audits, and legal oversight can help build that trust. For example, we might legally mandate that after voting, personal identifiers are irreversibly separated from ballots.

In summary, India's challenges include legal barriers, incomplete internet coverage , and diverse languages. However, there are strong opportunities: high mobile usage, a drive for digital empowerment, and a very large electorate that could gain from greater access. If these challenges are addressed, online voting could modernize Indian elections and increase participation.

7. Conclusion

We have outlined a complete architecture for a secure online voting system that **does not use blockchain**. By leveraging traditional PKI-based authentication and advanced cryptographic protocols (encryption, threshold decryption, zero-knowledge proofs), our design achieves end-to-end verifiability and strong security guarantees. Every vote is encrypted and auditable; a public bulletin board records all ballots and proofs; and distributed talliers compute the result with publicly checkable proofs. We have also examined India-specific factors: the need for legal reform , the technical challenges of scale and diversity, and the potential benefits of higher turnout and mobile access. In comparison to blockchain-based proposals, our system delivers similar integrity and transparency with a simpler trust model and better scalability. No online voting solution is risk-free, but by adhering to established security principles and involving multiple independent authorities, our approach minimizes the trust placed in any single component. We believe this framework could form the basis for pilot projects or legislative proposals. If deployed carefully, it can expand democratic participation (especially for overseas and disabled voters) while maintaining the secret-ballot integrity at the heart of Indian elections. We recommend that policymakers consider such cryptographic e-voting solutions as a complement to, or pilot alongside, the EVM-based system currently in use. With further development and legal support, online voting without blockchain can be a secure and effective option for future elections. References

RESULTS AND DISCUSSION

Online voting systems present several opportunities and challenges that must be carefully considered. One of the primary concerns is related to security. Such systems remain susceptible to various cyber threats, including hacking attempts, malware infections, and denial-of-service attacks, all of which can jeopardize the confidentiality and integrity of election results.

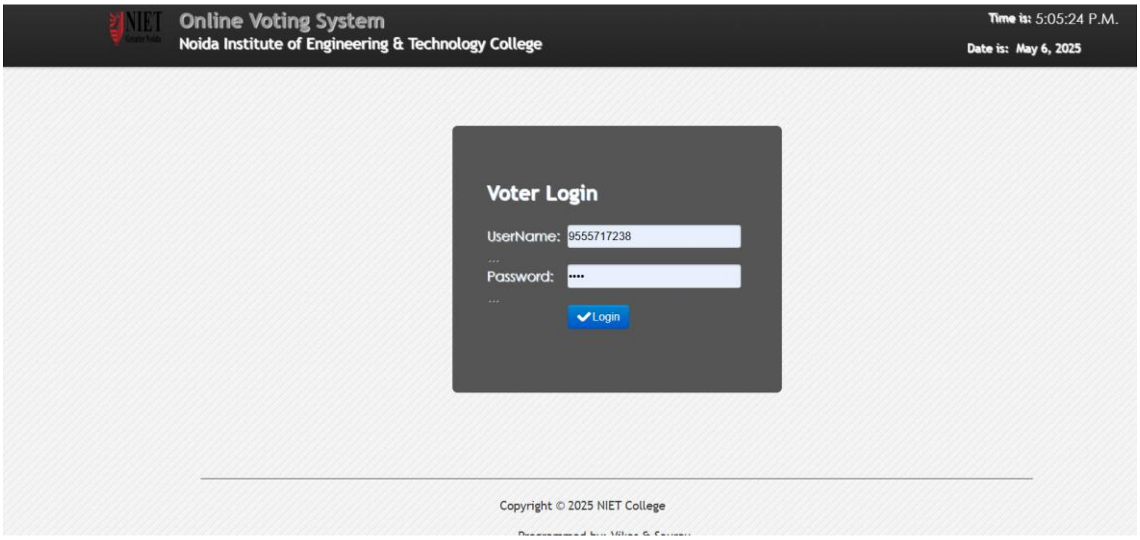
User perception plays a critical role in the success of online voting platforms. Studies indicate that voters are more likely to engage with an online voting system when they perceive it to be secure, reliable, and easy to use. Therefore, user experience design and transparent communication regarding system security are key factors in fostering voter confidence.

Online voting also offers the potential to enhance accessibility for specific groups, such as individuals with physical disabilities, citizens living in remote areas, or those with limited mobility. However, it can simultaneously introduce new barriers for individuals lacking internet access or the necessary digital literacy to navigate online platforms. Addressing this digital divide remains an essential consideration in system deployment.

Voter trust and confidence are foundational to the perceived legitimacy of any electoral process. It has been demonstrated that online voting systems designed with transparency, auditability, and accountability mechanisms can improve public trust in the process. Features such as end-to-end verifiability and publicly auditable logs are recommended to strengthen voter confidence.

In terms of efficiency, online voting can streamline certain aspects of the election process by automating vote counting and result tabulation. This can lead to cost savings over time and reduce human error. However, it is important to acknowledge that the initial development and ongoing maintenance of secure online voting platforms require substantial investment and technical expertise.

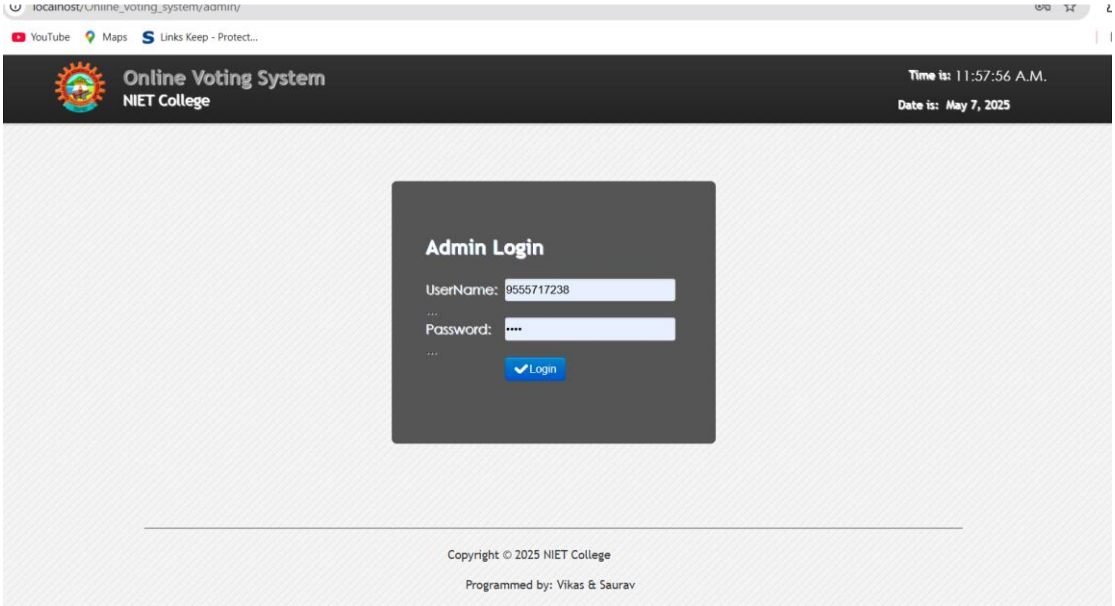
Additionally, advanced identity verification techniques, such as facial recognition, can further enhance system security. As illustrated in Figures 5 and 6, the system prompts users to verify their identity through facial recognition prior to casting their vote. This feature adds an additional layer of authentication, helping to ensure that only eligible voters participate in the election.



UserName: 9555717238

Password: ••••

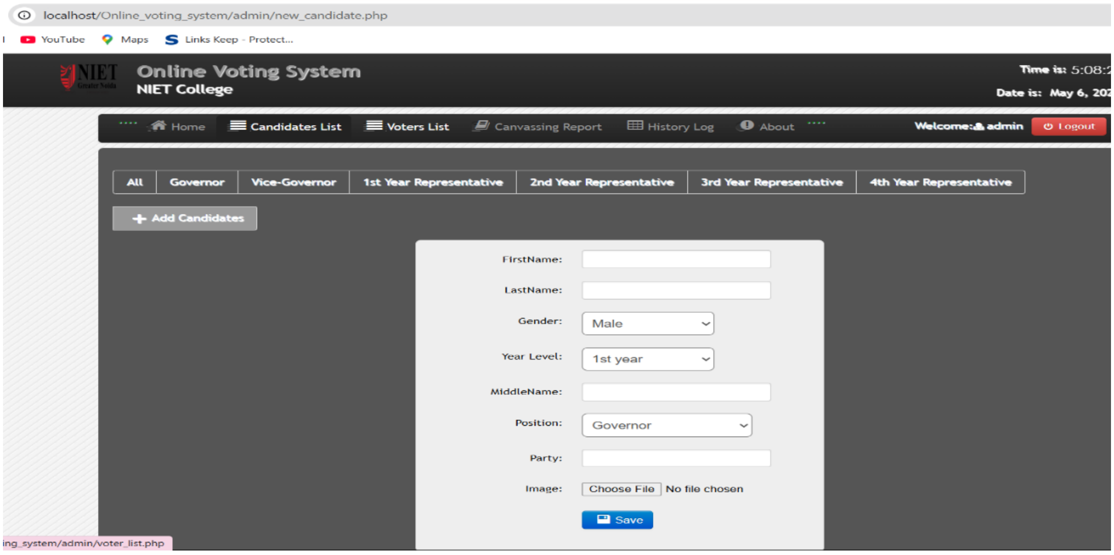
Figure 1: Voter Login phase.



UserName: 9555717238

Password: ••••

Figure 2: Admin Login phase.



FirstName:

LastName:

Gender: Male

Year Level: 1st year

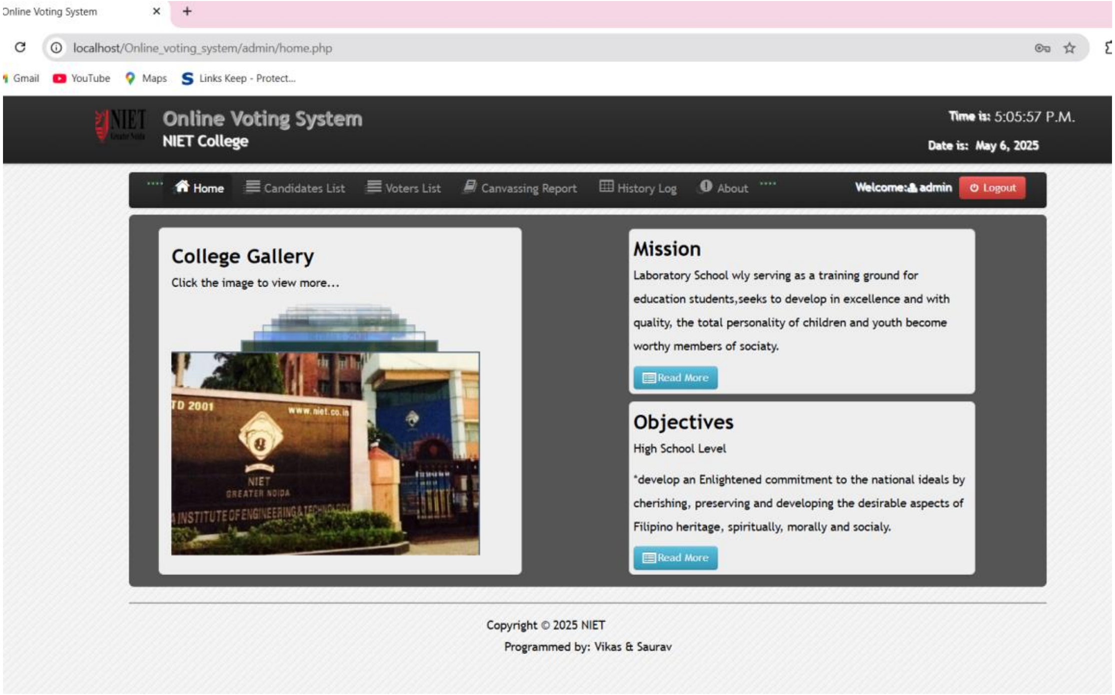
MiddleName:

Position: Governor

Party:

Image: No file chosen

Figure 3: Candidate Registration phase.



Online Voting System
NIET College

Time is: 5:05:57 P.M.
Date is: May 6, 2025

College Gallery

Click the image to view more...

Mission

Laboratory School wly serving as a training ground for education students,seeks to develop in excellence and with quality, the total personality of children and youth become worthy members of sociaty.

Objectives

High School Level

"develop an Enlightened commitment to the national ideals by cherishing, preserving and developing the desirable aspects of Filipino heritage, spiritually, morally and socialy.

Copyright © 2025 NIET
Programmed by: Vikas & Saurav

Figure 4: Home Page.

REFERENCES

[1] Times of India, “Outstation voters’ bat for online voting on lines of online banking,” Nagpur News, April 30, 2024.
[2] Y.-X. Kho, S.-H. Heng, and J.-J. Chin, “A Review of Cryptographic Electronic Voting,” Symmetry, vol. 14, no. 5, article 858, 2022.
[3] F. Moser, V. Cortier, and J. Müller, A Study of Mechanisms for End-to-End Verifiable Online Voting, Bundesamt für Sicherheit in der Informationstechnik (BSI), 2024.
[4] A. Abazorius, “MIT researchers identify security vulnerabilities in voting app,” MIT News, Feb. 13, 2020.
[5] SSL.com, “X.509 Certificates, PKI, and Online Voting in Elections,” Apr. 29, 2020.
[6] M. Hunt, “India to develop blockchain voting system,” Global Government Forum, Feb. 17, 2020.
[7] H. O. Ohize et al., “Blockchain for securing electronic voting systems: a survey of architectures, trends, solutions, and challenges,” Cluster Computing, vol. 28, art. no. 132, 2025.
[8] K. Kemp, Digital 2024: India, DataReportal, 2024.
11
A Review of Cryptographic Electronic Voting
https://www.mdpi.com/2073-8994/14/5/858
A Study of Mechanisms for End-to-End Verifiable Online Voting
https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Studies/Cryptography/End-to-End-Verifiable_OnlineVoting.pdf?__blob=publicationFile&v=4
Online Voting: Outstation voters bat for online voting on lines of online banking | Nagpur News - Times of India
https://timesofindia.indiatimes.com/city/nagpur/outstation-voters-bat-for-online-voting-on-lines-of-online-banking/articleshow/109707834.cms
Digital 2024: India — DataReportal – Global Digital Insights
https://datareportal.com/reports/digital-2024-india
India to develop blockchain voting system - Global Government Forum
https://www.globalgovernmentforum.com/india-to-develop-blockchain-voting-system/
Blockchain for securing electronic voting systems: a survey of architectures, trends, solutions, and challenges | Cluster Computing
https://link.springer.com/article/10.1007/s10586-024-04709-8
MIT researchers identify security vulnerabilities in voting app | MIT News | Massachusetts Institute of Technology
https://news.mit.edu/2020/voting-voatz-app-hack-issues-0213
X.509 Certificates, PKI, and Online Voting in Elections - SSL.com
https://www.ssl.com/article/x509-certificates-pki-online-voting-electronic-voting-elections/

Electronic voting in Estonia - Wikipedia
https://en.wikipedia.org/wiki/Electronic_voting_in_Estonia