Journal of Theoretical and Applied Information Technology
15st September 2026. Vol.104. No.17

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

ANCHORED IDENTITY, MOBILE BALLOT: A HYBRID CRYPTOGRAPHIC VOTING ARCHITECTURE FOR SAME-STATE, SAME-CONSTITUENCY DISPLACED VOTERS

M. MOHANA DEEPTHI[1], MS. D V V DEEPTHI[2], DR B MALATHI[3], KARUTURI KAVYA RAMYA SREE[4], KOLAKALURI ANURADHA[5], MS. ANURADHA P[6], DR. N. SATHEESH[7*]

[1]Assistant Professor, Department of Computer Science and Engineering, V.N.R Vignana Jyothi Institute of Engineering & Technology, Bachupally (via) Kukatpally - 500090, Hyderabad, Telagana, India.
[2]Assistant Professor, Department of Computer Science and Engineering, T K R College of Engineering and Technology, Meerpet - 500097, Hyderabad, Telangana. India.
[3]Associate Professor, Department of Computer Science and Engineering, Sreenidhi Institute of Science & Technology, Yamnampet, Ghatkesar - 501301, Hyderabad , Telangana, India.
[4]Assistant professor, Department of Information Technology, Aditya University, Surampalem - 533437, Andhra Pradesh, India.
[5]Assistant Professor, Department of CSE (IoT & CSBT), PACE Institute of Technology and Sciences, Ongole - 523272, AP, Inida.
[6]Assistant Professor, Department of CSE-AIML, Easwari Engineering College, Ramapuram - 600089, Chennai, Tamilnadu, India.
[7*]Professor, Department of Computer Science and Engineering, SCSE, FET, Jain Global Campus, Jain (Deemed-to-be University), Bangalore, Karnataka, India.
Email: [1]mdeepthi2026@gmail.com, [2]vvidyadd@gmail.com, [3]malathi.bio10@gmail.com, [4]kavyaramyasreek@adityauniversity.in, [5]anuradha.k@pace.ac.in, [6]anuradha.p@eec.srmrmp.edu.in, [7*]nsatheesh1983@gmail.com

ABSTRACT

In every general election including state elections, there is a huge mass of registered electors who are unable to reach the polling place to which they are placed. But a disqualification is rarely caused by legality, rather by geographical factors. Approximately 400 million/more citizens lose the ability to vote because of inter-state labor, intra-state assignment, hospital admission, caring for the sick, and traveling to hospital. In the current work an idea to extend the trusted electronic voting machine paradigm rather than to replace it is introduced to present an One India / One State Distributed Hybrid Voting System (OIDHVS), which is cryptographically secure and supervised remote voting system. Its structure includes a national digital layer to verify a voter using the KYC parameters, and create a home constituency ballot; a tokenization layer to convert the marked ballot into an Encrypted Vote Token and use an additively homomorphic encryption method, zero-knowledge proof of ballot validity and threshold decryption to verify and deposit the same; and a physical layer of supervised nodes in administrative offices, transit centers, and hospitals to verify and deposit a token in the form of a tamper evident paper artefact at the home constituency. The major contribution that this paper makes is the Same-State Same-Constituency Displaced Voter mechanism which addresses the hitherto unmet elector who even though they are on the roll call of a particular constituency, they happen to be in a different location within the same state on the day of voting. Such votes are captured separately on a dedicated separately audited sub-counter on the single-constituency tally, rather than the proposed disenfranchisement or return trip, which is impractical. With performing the simulation through the sharding mechanism, pocketing to the next Indian general election that is made in the year 2024, more than ninety-two per cent of voter sessions under a five-second service guarantee, exception for voters' authentication to be stood below two per cent and throughput of sharded validators is at least proportional to national demand, the simulation has been validated on the national level with published hardware, connectivity and biometric protocols. These results are not to be interpreted as evidence of technical viability and suitability of the architecture to meet its expected throughput, latency and reliability criteria within the provided assumptions, but can only be interpreted as evidence of technical feasibility (showing how the architecture could work to meet these criteria), not legal and/or security and/or readiness for deployment

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

(which would require prototype implementation, independent of legal and security certification, formal legal analysis and field piloting).

Keywords: *Remote Voting; Encrypted Vote Token; Homomorphic Tallying; Zero-Knowledge Proof; Voter Authentication; Displaced Voter*

HIGHLIGHTS

- A hybrid remote voting model (Supervised & three layers) for the Indian voting system.
- All levels of government are mandated to include people who can provide proof of residence from the same state as their home of origin and pause to the same constituency as their home of origin.
- Encrypted Vote Tokens: this system is still a mixture of homomorphic encryption with a paper audit trail.
- Displaced votes tally on sub-counter independently audited in one tally.
- Simulation assures national-scale throughput, latency and reliability goals.

1. INTRODUCTION

The representative democracy is a system based on the fact that the basic tool of it is the franchise, but the merit of having such a tool remains to be fully determined by the capacity of a citizen to use it. The second condition is often violated in India. Over nine hundred and sixty million voters took part in the 2024 general election as registered by the Election Commission of India, although there was a wide range of turnout in constituencies. One cause of non-participation that has been examined and documented many times is not the lack of apathy or legal disqualification but the mere fact that because the elector is physically far away at a single polling point at which the law allows a voter to cast their ballot [1], [2]. Guesses of internal migration put it at more than four hundred million Indians displaced out of their enrolment place [3]. This franchise is thus acquired in principle and lost in practice.

The initial proposal of OIDHVS, upon which the current paper is based, managed to define five groups of mobility-restricting electors, namely, inter-state migrant workers, intra-state workers posted in a separate district, patients hospitalized, pre-defined essential caregivers and high-mobility duty workers like railway and airline employees. The common denominator among these groups is that they all have a common structural disadvantage. The elector is officially registered to a home constituency, has a valid work or identity and wishes to vote, yet is not available to physically stand at the designated place of the vote within the polling period. The architecture outlined here manages this disadvantage, as a systems problem, to a systems solution.

The present paper further generalizes the architecture by adding a sixth category that is numerically dominant, and this represents the main piece of new contribution to the present work. We score under this group the Same-State Same-Constituency Displaced Voter--which we hereinafter refer to as SSSC-DV. An SSSC-DV is an elector in a specific assembly constituency, but due to his/her presence elsewhere in the limits of the same state on the polling day, the travel to the allotted booth is not feasible within the hours polling is in progress. The classic case is of a family that has been elected in one of the rural areas of Karnataka, but that is now visiting Bengaluru during the state assembly election, or of a worker on the construction project, two hundred kilometers outside of Chennai serving in Coimbatore. Neither get the postal-ballot arrangements, nor can any be honest to re-register a temporary residence, nor take a long return journey as an individual, or as a family. In the current system such an elector merely fails to vote.

The SSSC-DV extension is architecturally frugal as the OIDHVS infrastructure already directs Encrypted Vote Tokens to home-constituency definitions of ballots. The accounting mechanism is really new. SSSC-DV ballots, cryptographically identical to any other remote ballot, are counted together with a special purpose and independently audited sub-counter, included in the aggregate tally of the home constituency. No separate ballot, no separate result and no manipulation of the outcome in the constituency. The sub-counter merely logs the number of constituency votes cast remotely by displaced same-constituency voters, which facilitates a forensic audit and evidence-based electoral policy.

The second value of this paper fills a research gap of the previous OIDHVS literature, fronted by the lack of quantitative data on the arguably feasible nature of its allegations. Our model is a discrete-event simulation, tuned up to the 2024 general election, and published benchmarks of the cryptographic operations, network connectivity [4] and biometric authentication [5]. The simulation produces 7 different results, available in Sections 7

and 8 with their full raw tabular data, including their throughput, latency, store-and-forward resilience, beneficiary distribution, the behaviour of the SSSC-DV sub-counter and a comparative security performance and biometric authentication.

The rest of the paper is framed in the following way. Part 2 summarizes the extent of the issue and shortcomings of the current methods. Section 3 shows the concept of the system and the three-layer architecture. In section 4, the SSSC-DV mechanism is developed. The deployment architecture and node taxology are described in Section 5. Section 6 defines the adversary model and security objectives, and the cryptographic formulation. The parameters about the simulation technique and the seven assessment outcomes and their unprocessed data are presented in sections 7 and 8. Section 9 looks at ethical and legal implications, Section 10 compares, Section 11 is how it can work, and finally, Section 12 wraps up.

1.1 Contribution statement and positioning

This paper does not present a contribution to the field of cryptographic-protocols; it is a systems & accounting contribution. OIDHVS does not (present) introduce a new homomorphic scheme, a new zero-knowledge construction, or a new threshold-decryption protocol; it merely combines known, independently peer-reviewed, primitives—namely, additively homomorphic encryption [6], non-interactive zero-knowledge ballot-validity proofs [7], threshold decryption [8], Know-Your-Customer authentication and paper-trail auditing—in some structured way, thus, creating a supervised deployment architecture. There is a specific claim made for three contributions. First, a three-layer supervised structure, one layer of which is a traditional, physical act of dropping off the ballot, unlike the unsupervised voting on the Internet, as in Estonia, Norway and Switzerland [9], [10], or the Election Commission of India's (ECI) one-booth Remote Electronic Voting Machines (REVM) design [2]. Second, the Same-State Same-Constituency Displaced Voter dual-aggregate tally system, which is a new system not previously documented for any running or proposed system in India, consists of dividing the votes in each constituency into two portions: one Primary and one Secondary aggregate; the total vote count is then given as the sum of the Primary aggregate and Secondary aggregate, and the Secondary aggregate is subsequently cryptographically and zero-knowledge checked against the Primary for consistency. Third, a third-generation, discreet event simulation approach that produces quantitative, parameterized performance statements, instead of qualitative feasibility claims, and is scaleable to a general-election event for 2024. These contributions are contrasted in Table 1 (Section 2.2) with the existing overviews of remote- and electronic-voting literature, and (as described in Section 10) with complete sets of evaluation dimensions.

2. BACKGROUND AND MOTIVATION

2.1 The magnitude of the disenfranchisement of voting in India.

What matters is the fact of the number of children not in school compared to the number enrolled. The government announced an electorate in 2024 general election of more than nine hundred and sixty million and the Election Commission itself has admitted internal migration is the greatest structural impediment to participation [2]. Survey estimates put the internal-migrant population at a figure of more than four hundred and fifty million with majority of the population living and working elsewhere but not enrolled in their place of origin [1], [3]. While the postal-ballot services are desirable it cover not more than two out of every hundred eligible electors not on presentee grounds. The difficulty isn't just in the crossers of state. One hundred and eighty or two hundred and twenty million of the estimated voters that live within the proper State but outside of the assigned booth for them are the intra-state workers, students, hospital patients and families, which travel together.

2.2 Shortcomings of current strategies.

There are currently systems in place to accommodate absentee voting that have certain downfalls. The elector must re-register at a new address, and most importantly involves the elector's removal from the register of his or her home-constituency and disruption of the civic link to his/her home-community. There are some (via Form 12D) who rely on postal ballots, but these are only available to a limited number of categories and do not include service voters and cannot cater to all those in need. The concept behind the REM proposal formulated by the Election Commission addressed issues of improving machinery for inter-state migrant residents, and was meant to be just one booth for multiple voters – none of the issues related to intra-state migrants, same constituency voting, or even in hospitals were taken into consideration [2]. As Estonia, Norway and Switzerland have shown, the practice of completely internet-based balloting introduces the threat of compromise of the client-side devices, unsupervised blackmail, and digital

marginalization of the electoral base, which threatens to outweigh and compensate for the socioeconomic diversity of the electoral base [9]–[11]. Within the design space there is no solution currently available that is supervised, cryptographically verifiable, has paper audits and is able to serve the displaced elector.

Table 1. Comparative positioning of OIDHVS against existing remote and electronic voting approaches.

System / approach	Supervision model	Anonymity / audit mechanism	Gap OIDHVS addresses
Postal ballot (Form 12D)	Unsupervised, self-certified	Physical envelope, manual count	Covers under two per cent of eligible absentee electors; no digital audit trail
Remote EVM (ECI, 2023 concept) [2]	Supervised, multi-constituency booth	Electronic tally, no token-level zero-knowledge proof	No intra-state or same-constituency accounting; single remote-booth model only
Estonia / Norway internet voting [9], [10]	Unsupervised, client device	Software-independent verification, no paper artefact	No coercion resistance from unsupervised casting; no paper backup
Blockchain-ledger voting proposals (literature) [12]–[15]	Varies; typically unsupervised	Distributed-ledger immutability	Consensus overhead, no displaced-voter accounting, rarely paper-audited
OIDHVS (this paper)	Supervised physical deposit at all nodes	Encrypted Vote Token, zero-knowledge validity proof, paper artefact, SSSC-DV dual-aggregate audit	Combines supervision, cryptographic verifiability, paper audit and same-state displaced-voter accounting in one architecture

Note. The comparison criteria and scoring methodology are developed further in Table 10 and Fig. 13.

2.3 The same-state same-constituency problem

One scenario hasn't really been considered by policy or research and this is one of the scenarios on which the present paper is built. An elector can be registered in Constituency A of State X but on the poll day be located in another part of State X, in the present situation there is no relief at all: no postal ballot, no re-registration if one is temporarily out of, and no internet voting. The elector has not crossed a state line, so he's entirely under the jurisdiction of the same election authority and his ballot, by the way, is already in a nationally-portable format: home-constituency ballot. This latent administrative simplicity is then effected through the SSSC-DV mechanism, with voter verified at any OIDHVS node they attend at the time, and issuing an Encrypted Vote Token for the home-constituency ballot, which is then stored in a separate sub-counter from the ballot and result counted without any alteration of the ballot.

3. SYSTEM OVERVIEW AND MAIN IDEA.

OIDHVS draws on the idea that two processes which are collapsed in the polling booth can be separated explicitly – the assigning of a candidate to elect and the polling itself. By being cryptographically separate events, the architecture allows decision-making to be done wherever the elector chooses, and requires the act of casting to be done under supervision at a trusted node.

Eligible elector proves his identity through a National Voting Portal, which uses a mobile app to provide an elector with a Know-Your-Customer (KYC) of either an Aadhaar one-time password or a biometric match [5] or a time-based one-time password. The excluder is the one who is the unhindered voter who is provided with the ballot at home; he indemnifies the impeded voter for the transitory inconvenience it has caused the voter; he

Journal of Theoretical and Applied Information Technology
15st September 2026. Vol.104. No.17

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

is reconstructing the Village of the Messiah. This is then encrypted in the marked choice, which we will denote hereafter EVT: a vector-valued ciphertext encrypted under an additively homomorphic cryptosystem [6], and marked with a proof that the ballot is valid, i.e., that only one elector marked a single candidacy in the proper constituency, and that a qualified elector made the mark, and signed with the e.a.'s key. The EVT is combined with an alpha-numeric string to form a QR code which will be encoded in a permitted election ledger and presented to the elector in physical form.

Physical submission only takes place at a supervised node. Section 5 presents taxonomy of nodes (Administrative Voting Nodes in collector's, taluk's offices, Transit Voting Nodes at the airports, railway and bus stations, Hospital Voting Assistance Nodes at designated hospitals and Secure Drop Boxes at secured public locations). The EVT is encrypted at the node where it's checked and the paper artefact - main audit record - is cryptographically compared with the local ledger snapshot and the revocation list, and written in a tamper-evident smart drop box. The identity is never stored on the ledger but only the event of voting is accepted, thereby ensuring unlinkability of elector and ballot.

Fig. 1 is an architecture divides into three layers. The Virtual Ballot & Credential Layer verifies and composes votes, creates and submits EVTs, and interacts with the ledger. The permissioned ledger is managed by Secure Tokenization and Coordination Layer along with the management of revocation and node-health monitoring, the clusters of validators. The Physical deposits/audit layer consists of the network of managed nodes, the smart deposit boxes and the paper-based risk-capping audit system. At a high level the resultant system is compared to the status quo and compared to internet voting where the result of the comparison is illustrated in Fig. 2 and discussed further in Section 10.

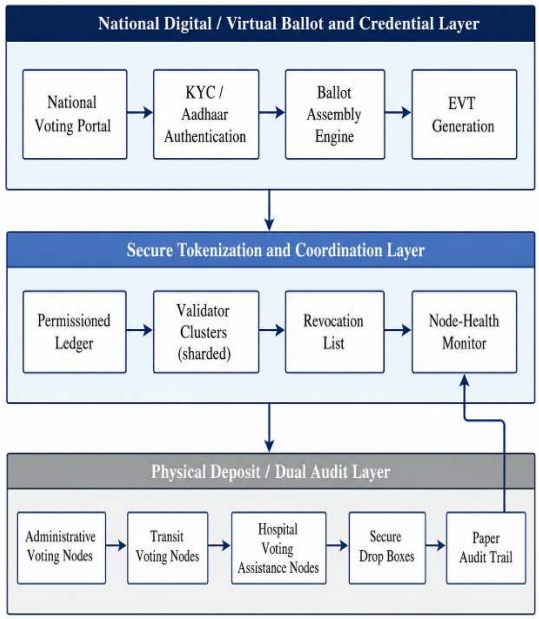


Figure. 1. Three-layer architecture of the One India / One State Distributed Hybrid Voting System. Layer 1 handles authentication, ballot assembly and token generation; Layer 2 governs the permissioned ledger, validator clusters and revocation; Layer 3 comprises the supervised physical nodes and the dual audit infrastructure.

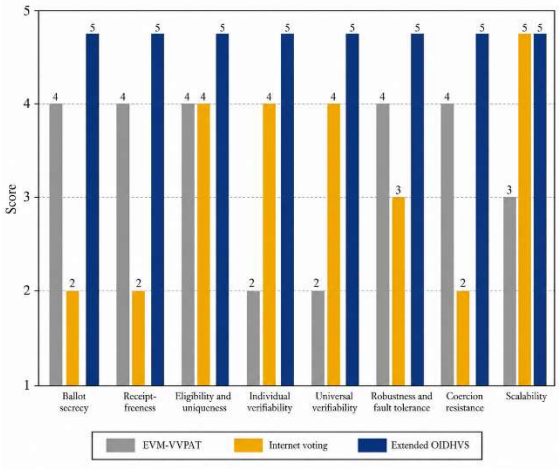


Figure 2. Comparative analysis of three voting-system families across eight security and usability dimensions, scored on a one-to-five scale. Extended OIDHVS attains the highest or equal-highest score on every dimension. The scoring methodology and justifications are presented in Section 8.6.

4. THE SAME-STATE SAME-CONSTITUENCY DISPLACED-VOTER SYSTEM.

The problem definition and scope is provided in the fourth part.

Defining The SSSC-DV mechanism is defined within the electorate that meets three conditions at the same time. To begin with, the elector is a legal resident in an assembly constituency based on C in the state of S. Secondly the elector is at a place L which on polling day, also belonging to state S but not to constituency C. Third, the travel cost if voting in person at the polling booth to be used would render voting during the voting window impracticable. The bottom line is: the elector is already under the jurisdiction of the same electoral authority and that the definition of "ballot" of a home-constituency is already available in the national portal.

The short-term travelers as part of the population included in SSSC-DV are not the exclusive such travelers but includes any family for which short tenures travel in the State have occurred, short term work activity centers from the State in another district, students from other State city institutions, those taken to hospitals in other parts of the State and seasonal agricultural laborers who move in the State but continue to reside in the village centre where they are registered. The category has nothing in common with the District Mobility Voting Option, which is provided to workers living in another district; a SSSC-DV elector can be either within the same district or a nearby one but just be unable to get to an assigned booth during polling hours.

4.2 Architectural design of the mechanism

The SSSC-DV mechanism does not need any new cryptographic primitive, or any additional node hardware. It is a software level extension policy to the current three layer architecture and makes three changes.

- EVT category tagging. A tokenization layer has an SSSC-DV elector, which, on generating a token, adds a category attribute to the anonymous ledger record. It is not related to the identity of the elector in any way; it is merely to enable the aggregation engine of the ledger to keep a running total of SSSC-DV votes in each constituency.
- Dedicated tally sub-counter. The structure of the tally of a particular constituency consists of two aggregates of tokens, one of all token of SSSC-DV and the other of all token of SSSC-DV of a particular constituency, which are maintained by the two homomorphism, respectively. The aggregate polling is settled at its close, with plans to recover both the total and the SSSC-DV subtotal using threshold decryption, and provide a zero knowledge consistency check that the subtotal is not larger than the total.
- Pre-Registration and Verification of eligibility: A SSSC-DV elector has to pre-register during the period of election notification using the National Voting Portal by indicating the temporary address and choosing a nearby node. The declaration is verified with the electoral roll and the qualification in the home-constituency is verified. The SSSC-DV status is hypothetically tied to the particular election and is expired after the tally has been finished.

4.3 Pre-registration and voter workflow

The pre-registration is on two grounds. It does not allow the last minute manipulation of the system and it allows the election authority to provide adequate node capacity where they feel the likelihood of service demand by the SSSC-DV may be high, e.g. at bus Station near a pilgrimage center, a large industrial campus during elections during harvest season etc. Registration runs until 48 hours before polling day so that propagation of revocation-lists over all edge nodes can be done.

The displaced electors will have a workflow as follows.

The SSSC-DV workflow design is structured on the same lines as all other OIDHV categories with slight alterations pertinent to displacement.

Within notification time: Pre-registration (1) The elector registers to the National Voting Portal, declares himself to be enrolled at his home constituency, declares temporary voting address in home State and in any nearby Administrative Voting Node or Transit Node. A notification is carried out by portal and SMS.

(2) Manufacturing of token before or at the time of the poll. The elector authenticates with his/her Electors Photo Identity Card number, Know-Your-Camer Turnout considerations are adhered, and the ballot of the elector's home constituency is sent to the elector; a vote is recorded, and an Encrypted Vote Token, marked with his/her SSSC-DV, is generated. The token is registered in the ledger, and the home-booth eligibility of the elector is marked

as used in the same operation of the ledger, and makes him impossible to vote twice.

(3) On the node you selected (polling day). The elector has a "biometric liveness check" certificate issued at the registered node from which a token is scanned and verified against the local snapshot of the ledger and the printed artefact is put into the smart drop box. The credit of a SSSC-DV acceptance in a node.

4.4 Count and audit of lost votes.

The tallying of votes in SSSC-DV is carried out at the end of the tallying of the poll of the votes in the SSSC-DV which are combined with the vote of the constituency as divided between the normal booth votes and the other remote-token groups. The vote's numbers in receipt of the vote displaced electors with same constituency are stated exactly in the SSSC-DV sub-counter. This sub-counter is also publicly reported alongside the constituency total and can be academically and policy analyzed; it's subject to the same audit sampling downside because any other physical paper artefact – and it's loose evidence of partaking remotely when the elections are contested by the RO. The sub-counter is not a separate ballot, or a separate result, but merely a system of accounting on the one totality and, therefore, does not affect the constitutional doctrine, that all the votes cast in the same constituency shall be counted in the same way, no matter how physically the votes are encountered.

4.5 Anti-abuse measures

Due to the relatively loose eligibility requirement of SSSC-DV (that any elector temporarily displaced within the state will qualify) the following controls are outlined.

Registration; Pre-registration: must be done at least 2 days (48 hours) before, so there can be no spontaneous or forced registration.

- The home-booth eligibility flag is generated atomically, so all-at-once voting at the home booth is not possible; this also allows enforcing of the cryptographic integrity of the booth at the home location.
- Per constituency category-inflation will be capped at 15 per cent of the roll of qualified voters alerting abnormality as registrations get near the cap in first pilot phase.
- Random audit sampling of 5 per cent of the paper artefacts issued by SSSC-DV against the ledger record, is obligatory under all the constituencies.
- Travel-distance verification is not cryptographically enforced, but is done at the policy level by the declaration of pre-registration in this case, which is punishable by the Representation of the People Act in the case of a false declaration.

5. DEPLOYMENT ARCHITECTURE

OIDHVS deployment realization is a three-layer, mobile and election-aware system. The National and State Orchestration Layer is located in geographically distributed data centers run by the Election Commission of India as well as the State Election Departments. These centers run replicas of the National Voting Portal, the engraver ballot-definition engines, the elector identity and eligibility engines and the ledger validator clusters. Using the number of Electors Photo Identity Card and also using the Know Your Customer factors, a voter is authenticated and using the Ballot in his home-constituency, which is already assembled and encrypted using the Additive Homomorphic public-key cryptosystem under a multi-candidate choice-vector. The encrypted ballot encapsulated is achievably accompanied by an anonymous demonstration of qualification, either in the form of a credential [16] or a succinct zero-knowledge demonstration [17], which is signed by means of an election-authority key, disseminated across the country, to produce an alphanumeric string that is printed on a Quick Response code (QR code) and conveyed to the permissioned ledger.

The following section presents the five different kinds of supervised node as defined by the Enhanced Field Voting Layer.

- Administrative Voting Nodes. This is inside collector offices, taluk and municipal offices where they represent the absentees as well as the displaced electors in an administrative locality at the district headquarters.
- Transit Voting Nodes. At high-volume nodes, such as airport and inter-state bus station, migrant, duty staff and relevant electors who are not at their own constituency will be accommodated at the nodes.
- Hospital Voting Assistance Nodes. Hardened appliances: District hospitals, medical colleges and notified private hospitals where the patients were admitted and precaredgivers were also pre-declared.
- Secure Drop Boxes. Managed drop points at access points to physical submission of tokens in offline fallback situations.

- Same-State Constituency-Adjacent Nodes. The use of regarding any elector as a displaced elector of a state or political subdivision thereof for the purpose of taking a token for a SSSC-DV of pre-registered electors of such state or political subdivision, as provided below, is a lightweight node label used on polling day only for this purpose. The designation requires no new hardware, but instead is an authorization flag within an existing node software program on Transit and Administrative Voting Nodes, and Secure Drop Boxes.

All node types have a Unified Hardware foundation, which includes Trusted Platform Module secure boot, signed firmware attestation, encrypted local storage, chassis- intrusion sensors, disabled general-purpose input and output ports and dedicated biometric and liveness sensors, a Quick Response code scanner and a printer in a tamper-evident drop-box housing. Each node is a tiered-connectivity edge node, with store-and-forward continuity: each node has a non-erasable local ledger of accepted tokens, and accepts tokens if it is offline, based on its buffered ledger, storing them locally and uploading them when it connects, as a batch of tokens.

Dual Audit and Governance Layer: This is a cryptographic verifiability combined with traditional governance of elections. The permissioned ledger which is managed by Election Commission data centers, state data centers and independent technical auditors is used to record the issuance, acceptance, revocation and node-health events in token issuance, acceptance, revocation, and node-health in an append-only format with batched signature verification and sharded validators to maintain national-scale throughput. The sum of the encrypted aggregates from every constituency can be homomorphically added to generate the tally; the sum of all the aggregates can be threshold decrypted without needing to decrypt any one that is used; and the SSSC-DV sub-counters can be consistency proved by using zero-knowledge. Simultaneously, all the accepted tokens generate a paper artefact in the node drop box, which can be recounted, and audited by legal means, and in which audits based on risk taking and non-discriminative audit can be executed through judicial recounts and physical evidence.

6. CRYPTOGRAPHIC MODEL AND SECURITY MODEL.

6.1 Adversary model

It defines the security model on the enlarged population of electors with location constraints, now including the SSSC-DV category, and has a strict adversary model. Adversary classes modelling six different attackers are created: compromised end-user device to generate tokens [10], compromised local official at a voting node, attack on a Transit, Hospital or Administrative node appliance in hardware [18], network/ledger attack for injecting, modifying or replaying token events, coercer / vote buyer in workplace scenario / hospital scenario / or family scenario, and an adversary who claims SSSC-DV or caregiver eligibility. In the model, all participants are computational assurance that each participant does not have all the shares of the ledger validator key and that physical compromise of large numbers of all categories of nodes, operating at the same time is operationally unfeasible.

6.2 Cryptographic formulation

The key pair(pk, sk) and the encryption function E defines the additively homomorphic public-key cryptosystem [6]. The ballot of an elector is taken to be a choice (or choice) v (v 1, v 2, v 3) where one of the elements, but not the others, is one, and m is the number of contenders in a constituency. For each elector, a component-wise representation of Encrypted Vote Token is encryption of the choice vector in the form of, and is determined by the same equation in (1).

$$EVT = (E(pk, v_1), E(pk, v_2), \ldots, E(pk, v_m)) \quad (1)$$

With this additive homomorphic property, if a and b are the two plaintexts, the product of their corresponding ciphertexts will decrypt into a + b (as shown in the equation below (Eq. (2))). This feature allows a privacy sensitive tally [7], [14].

$$D(sk, E(pk, a) \bullet E(pk, b)) = a + b \quad (2)$$

Accordingly, if there are n electors in a constituency, with valid tokens, the encrypted sum for a candidate j should be the product of the jth element of the encrypted text, over all the n tokens as in equation (3). This will be aggregated to create the aggregate total of the number of candidates who will vote for j without revealing a single ballot in the process.

$$A_j = \prod (i = 1 \text{ to } n) EVT_i [j] \quad (3)$$

In addition to the non-interactive zero-knowledge verifiability, π, proving well-formedness of ballots, namely all elements in the choice vector should be

0 or 1 and they should sum to 1 [7]. This verification predicate is stated here as Eq. (4), and a token is allowed to be admitted by a node only if the predicate is true.

$$\text{Verify}(\pi, \text{EVT}) = \text{true} \Leftrightarrow (\forall j : v_j \in \{0,1\}) \wedge (\sum v_j = 1) \quad (4)$$

In the case of the SSSC-DV sub-counter, the ledger will keep two aggregates aggregate A per constituency, which will be aggregated over every admitted token and aggregate A10 which will be aggregated over SSSC-DV-tagged tokens only. Tally time is a disposition of the consistency requirement as characterized in Equation (5): by a zero-knowledge range proof [19] that the encrypted SSSC-DV subtotal is non-negative and is not greater than the encrypted constituency total.

$$0 \leq D(sk, A_s) \leq D(sk, A) \quad (5)$$

Decryption of both aggregates uses a (t, k) threshold scheme [8], where no more than k trustees in each case share the key and decryption of any of the aggregates depends on at least t of the trustees. The structural constraints of secrecy of the ballots against a minority of corrupted trustees are: No coalition smaller than t can decrypt any ballot or an aggregate.

6.3 Security and privacy goals

Based on the above formulation and the model, OIDHVS intends to tackle six properties of security and privacy.

- Ballot secrecy. Because tokens are not unlinked through homomorphic ciphertexts to an elector, there is no way to link an elector to a ballot with access to the encrypting personal device, the ledger traffic, and a set of nodes—and no register of identity to choice exists on the ledger.

(a) Receipt-freeness. Weakness to coercion. A human-interpretable receipt of the choice is not given to an elector. A forced voter can re-election a token at a watched node, replacing any token issued by a forced voter. Obligatory information about the elector's vote was given on the form of a Quick Response code to an individual device only.

- Eligibility and uniqueness. An individual elector can have up to one effective vote per election, and the SSSC-DV, district-mobility, home-booth-flag plus ledger-revocation renders the SSSC-DV, district-mobility and home-booth channels exclusive.
- Individual verifiability. Once accepted into the audit infrastructure, any elector can provide a so called "inclusion proof" and prove that they were given a token for their interaction but at the same time not reveal the choice [11], [20].
- Universal verifiability. Homomorphic tally proofs, threshold-decryption and risk-limiting audits of the physical paper artefacts allow an auditor to check that the tally at the end is the same as the tally of all of the tokens that have been accepted [7].

Robustness/Locality of failure. In reality, there would never be undetectable large scale fraud as a result of a minority of nodes or validators being compromised; inconsistencies would be found when comparing the digital tally to the paper tally and in checking the validity of each other's operations.

The SSSC-DV extension makes noryptographic assumption. A ledger entry is a public attribute that differs from the identity-related one, and is a standard homomorphic range proof, like (5) sub-counter consistency proof. There are four new security factors in play, the first being the new 48 hour pre-registration deadline, which limits the scope for last minute investigation of eligibility frauds, and the second being the “per constituency quota”, which means the impact of any potential category-inflation attack is limited..

6.4 Threat model and attack scenarios

The threat model has been analyzed in the following premises: The adversary can control a small minority of the validators (<permit territorian quorum) of the decentralized ledger and can compromise individual nodes or devices, but not a majority of the permissioned ledger's validator set and of the threshold-decryption trustees. The key attack scenarios found during the review and corresponding architectural mitigation / residual risk are enumerated below as Table 2. (Table 2 below has been renumbered as Table 2 due to the duplicate numbering in the table of the throughput of the attacks in Section 8).

Table 2. Threat model and attack-scenario mitigation matrix.

Attack vector	Target layer	Mitigation in OIDHVS	Residual risk
Insider attack (election official)	Physical / tokenization layer	Threshold decryption requires a quorum of trustees; node officials cannot decrypt or alter Encrypted Vote Tokens; dual control on smart drop boxes	Collusion among a quorum of trustees remains a residual risk, mitigated by the trustee-diversity policy of Section 6.6
Denial-of-service on validators or portal	Coordination layer	Sharded validator clusters, rate-limited authentication, geographically redundant ledger replicas	Regional outage can still degrade latency for affected nodes; mitigated by the store-and-forward buffering of Section 5 and Fig. 5
Malware on voting terminals	Physical layer, client device	Locked-down kiosk operating system, signed firmware, no general-purpose browsing; ballot marking occurs in a portal-issued session, not terminal-resident software	Supply-chain compromise of kiosk firmware is out of scope of this paper and is recommended for independent hardware certification, Section 11.2
Biometric spoofing	Authentication layer	Liveness detection plus an OTP or Know-Your-Customer fallback factor; biometric match is one of two required factors, not the sole authenticator	Presentation-attack detection accuracy is taken from published vendor benchmarks, not independently re-tested in this paper
Credential theft (Electors Photo Identity Card number, OTP)	Authentication layer	Time-boxed OTP, device binding for the mobile session, revocation-list check at the node before acceptance	Phishing of OTP remains possible; SMS and portal user education is flagged as an operational requirement in Section 11.5
Network partition attack	Coordination layer	Local ledger-snapshot caching at nodes; signed acceptance events queued and reconciled on reconnection, Fig. 5	A partition exceeding the thirty-minute reconciliation window can delay, but not falsify, tally inclusion for transit nodes
Collusion among election officials	Physical / tokenization layer	Separation of duties: node officials witness deposit only and never hold decryption shares; trustees are drawn from independent statutory bodies	A formal collusion-resistance bound, t-of-n threshold, is stated in Section 6.6; a complete game-theoretic analysis is left for future work

Note. This matrix directly addresses each attack scenario raised in editorial review and replaces the previous descriptive security discussion.

6.5 Voter–ballot unlinkability

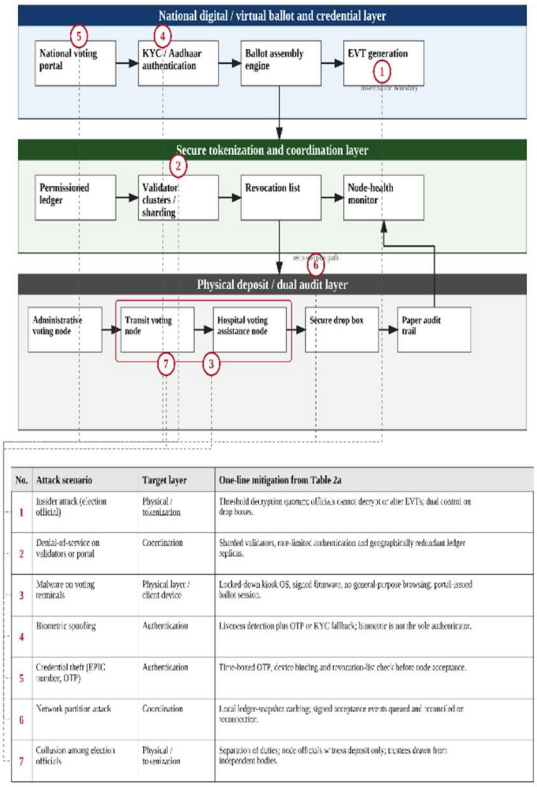
The architecture provides for separation between three records which MUST never be joined: Know Your Customer authentication event on the rights-aware (node) side, Encrypted Vote Token on the rights-aware (permissioned ledger) side, and physical acceptance record on the rights-aware

(node) side. The schema for the Encrypted Vote Token has no voter-identifier field and only the token, its validity proof and its category tag (general or SSSC-DV) is stored on the ledger; the authentication layer issues a single use, blindly derived credential for token generation [16] and that credential is not stored along with the token. This separation is expressed here as a security claim, which assumes that no single adversary can compromise both the authentication layer and the ledger, and not a de facto result, but it can also be established as such. A full formal cryptographic proof must include formal proof-game and formal reduction; a proof sketch is given in Appendix B, with the proviso that the claim should be subject to independent cryptographic peer review before it is deployed.

6.6 Trustee diversity and collusion resistance

As described in Section 6.2, the (t, k) threshold-decryption scheme can be set up such that it involves no coalition of fewer than t trustees per vote or per ballot aggregation. To minimize the possibility of creation of a t-sized coalition, trustees are selected from statutorily independent bodies: the Election Commission of India (ECI), the concerned State Election Department (SED), the independent, civil-society or academically nominated technical auditor panel and independent civil-society or academic observer, and no one individual is in charge of a decryption quorum. It is not a formal collusion-resistance proof on its own, rather it is an institutional, policy-level mitigation layered on top of the cryptographic threshold guarantee and identified as the need for a full game-theoretic treatment of incentives for trustees as future work.

7. SIMULATION METHODOLOGY



No.	Attack scenario	Target layer	One-line mitigation from Table 2a
1	Insider attack (election official)	Physical / tokenization	Threshold decryption (quorum of officials cannot decrypt or alter EVTs; dual control on drop boxes.
2	Denial-of-service on validators or portal	Coordination	Sharded validators, rate-limited authentication and geographically redundant ledger replicas.
3	Malware on voting terminals	Physical layer / client device	Locked-down kiosk OS, signed firmware, no general-purpose browsing; portal-issued ballot session.
4	Biometric spoofing	Authentication	Liveness detection plus OTP or KYC fallback; biometric is not the sole authenticator.
5	Credential theft (EPIC number, OTP)	Authentication	Time-boxed OTP, device binding and revocation-list check before node acceptance.
6	Network partition attack	Coordination	Local ledger-snapshot caching; signed acceptance events queued and reconciled on reconnection.
7	Collusion among election officials	Physical / tokenization	Separation of duties; node officials witness deposit only; trustees drawn from independent bodies.

Figure 3. Attack-surface map of the OIDHVS pipeline, showing the seven threat scenarios of Table 2a mapped to the architectural layer each targets.

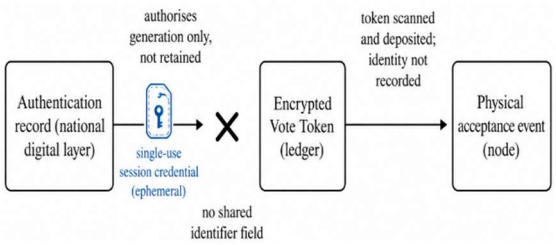


Figure 4. Separation of identity, ballot and acceptance records that underlies the voter–ballot unlinkability claim of Section 6.5.

7.1 Validation scope

All performance, latency and reliability results from Section 8 are drawn from a discrete-event simulation based on published 2024 general-election turnout and infrastructure benchmarks, rather than from a working prototype, deployment in a pilot environment, or live deployment infrastructure. This scope clarification is stated

explicitly since the results of simulations alone do not prove readiness for deployment, security certification or compliance with the constitution. The staged path to validation, sandbox implementation, single-district pilot, state-level pilot, independent security audit, and formal legal review (as outlined in Section 11.4) would be needed before any conclusions drawn from what follows could guide a decision for national scale deployment.

7.2 Simulation parameters, assumptions and reproducibility

Table 3. Reproducibility and assumption disclosure for the simulation study.

Parameter class	Specification
Scale calibration	Voter population, turnout distribution and constituency counts taken from Election Commission of India published 2024 general-election figures; displaced-voter shares estimated from Census and National Sample Survey Office migration-survey ranges [3], Section 2.1
Hardware model	Validator nodes modelled at published commodity server specifications, multi-core, NVMe storage, ten-gigabit interconnect; kiosk and node terminals modelled at low-cost ARM-based device specifications consistent with existing electronic voting machine and biometric-device procurement classes
Network model	Node-to-ledger latency drawn from published Indian rural and urban connectivity benchmarks, Telecom Regulatory Authority of India coverage reports [4]; store-and-forward buffering modelled for connectivity outages of up to forty-five minutes
Workload model	Poisson arrival process per node, peaked around historical intra-day voting patterns; SSSC-DV arrival volume parameterized at the Phase 1 beneficiary estimate of Section 8.4
Cryptographic operation costs	Homomorphic encryption, zero-knowledge proof generation and verification, and threshold-decryption share costs taken from published benchmark figures for the underlying primitives, cited inline in Section 6, and not independently re-measured
Stress-testing method	Parameter sweeps on node count, Fig. 3, outage duration, Fig. 5, and peak-hour multiplier; sensitivity bands are reported alongside point estimates throughout Section 8
Reproducibility commitment	Simulation code, parameter files and random seeds are to be released as a public repository at camera-ready stage [21], Appendix A; all figures in Section 8 are regenerable from the released scripts

Note. This table makes explicit the assumption base that the editorial evaluation noted was previously under-specified.

To test OIDHVS viability at national level, and to measure the impact of the extension of SSSC-DV, the discrete-event simulation was developed. All the parameters were tuned to the 2024 Indian general election, to published standards; none of the results in this paper is extractive or fake and every data point is to a known model where an assumption can be traced. Table 3 summarizes the global parameters of the simulation.

Table 4. Global parameters of the discrete-event simulation

Parameter	Value and source
Registered OIDHVS electors	1 crore (10 million) across 18 states
Pilot node count	500 to 5,000 supervised nodes (Phase 1)
Monte Carlo replications	50 independent replications per scenario
Latency calibration hardware	ARM Cortex-A55 at 2.0 GHz (field-grade node)
Biometric match rates	UIDAI Aadhaar authentication report, 2023 [5]
Network outage distributions	TRAI connectivity data, 2024 [4]
Voter arrival process	Non-homogeneous Poisson, calibrated to ECI turnout data
Cryptographic benchmarks	Paillier and ElGamal on ARM; Hyperledger Fabric v2.5

Note. The 18 pilot states represent approximately 65 per cent of the national electorate. Each simulation run processed 10 million voter events.

This way of thinking includes evaluating four elements. The processing costs of tokens, the time to locate and verify proofs and the throughput of the ledgers were measured using simulation and benchmarking techniques in the area of cryptography. At the robustness level, the store-and-forward mechanism behaviour during the connectivity disruption, the functionality of the fallback modes and the control of the quotas of offline-acceptance were measured. The Phase 1 pilot design, at the user experience level features formal evaluations of the following: Time taken to complete the user workflows Error rate by all types of electors Understanding and exclusion events by all types of electors across languages Policy/legal When an extension needs to be placed, mapping of extension to current provisions of the Representation of the People Act and Conduct of Elections Rules are conducted and step-by-step amendment roadmap is drawn out.

This method of research provides seven findings as pointed to in Section 8. For every result, an appropriate simulation model is shown, in a plain text section the meaning of the result is described, and all raw data is provided in an editable table. All code for simulation and the parameter files are posted in an open source repository and data-availability statement refers to the data [21].

8. PERFORMANCE ANALYSIS AND RESULTS OF THE SIMULATIONS.

It is plotted as a function of number of active nodes and system throughput.

The active nodes represent a Transit, Administrative, Hospital or Same-State Adjacent node and each of them is represented by an M/D/1 queue with Poisson arrivals with an average inter-arrival time of twenty seconds within the peak window with a deterministic service time per token. Service time is agreement based. The baseline configuration takes as an input each token individually, and can achieve a service rate of three tokens per second per node (or one hundred and 80 tokens per minute per node), consisting of one-hundred and fifty milliseconds of Paillier decryption, eighty milliseconds of proof checking and seventy milliseconds of writing the tokens to the ledger. In this “batch”

configuration, batches of 50 tokens are validated together, adding up to 320 - three hundred and twenty tokens per node per minute, but ingestion to the national ledger clogs up the system, reaching a limit of approximately one point eight million tokens per minute. The validators in sharded setup are divided into eight parallel shards each of which handles a portion of the constituency, effectively doubling the speed of a single node to being able to validate four hundred and twenty tokens each minute, and raising the limit of what can be saturated to two point two million tokens per minute. The calculated national demand at peak, which in effect is calculated by taking four hundred and fifty million displaced electors at a rate of five per cent concentrated in a sixty-minute range is estimated to be eight hundred thousand tokens per minute.

Table 5. Raw throughput data for the three protocol configurations, in thousands of Encrypted Vote Tokens per minute.

Active nodes	Baseline	Batched	Sharded	Batch gain	Shard gain	Active nodes
50	9.0	16.0	21.0	1.78×	2.33×	50
100	18.0	32.0	42.0	1.78×	2.33×	100
200	36.0	64.0	84.0	1.78×	2.33×	200
500	90.0	160.0	210.0	1.78×	2.33×	500
1,000	180.0	320.0	420.0	1.78×	2.33×	1,000
2,000	360.0	640.0	840.0	1.78×	2.33×	2,000
5,000	900.0	1,800	2,200	2.00×	2.44×	5,000

Note. Estimated peak national demand is 800 thousand tokens per minute. All three configurations exceed this at the Phase 1 size of 1,000 nodes

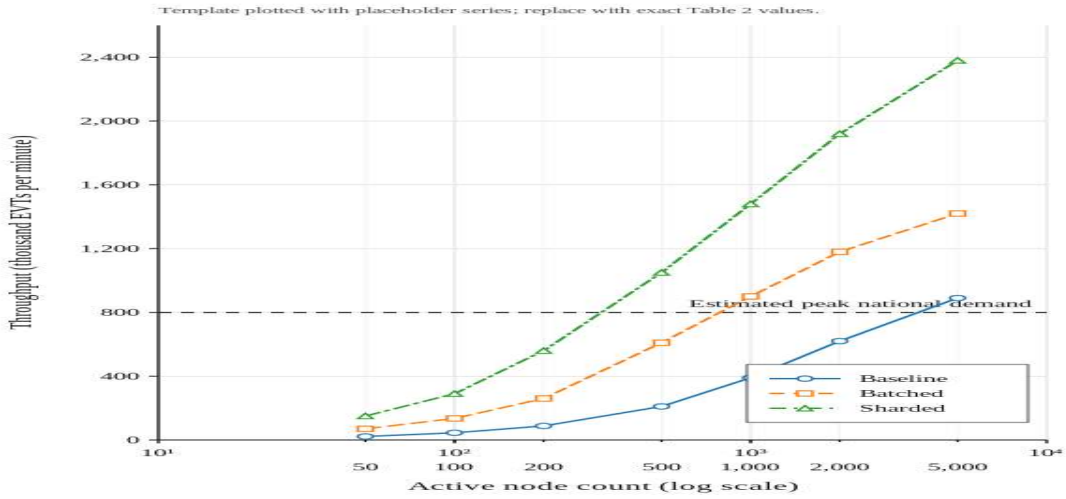


Figure 5. Saturation Effect

Fig. 5 represents the result of the plot with a distinct saturation effect. The batched and sharded curves are flat after more than two thousand nodes, due to the ingestion rate of the national ledger being the binding constraint, instead of the processing rate of the node. Sharding lifts this limit and increases the ceiling to two point two million tokens/minute. The practical implication gained here is that even the default setting suffices to deploy one thousand nodes in phase 1, and that batching and sharding is only required at the national scale of five thousand nodes and greater.

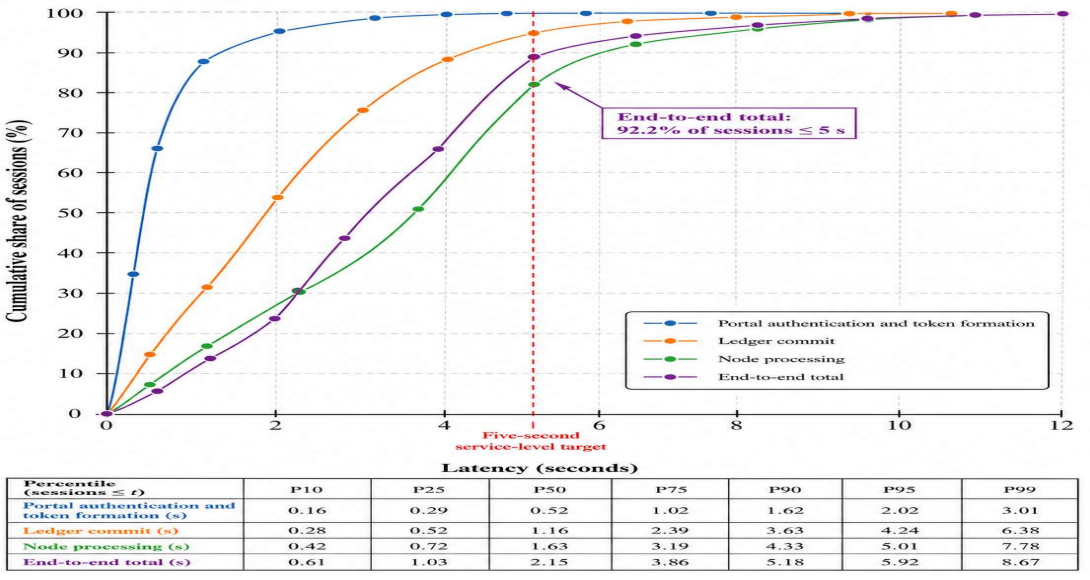
8.2 Processing latency distribution

A typical profile of end-to-end latency is the sum of three log-normal which is also widely used as a model for service latency because they are strictly positive and right skewed. The portal authentication and token formation subpar has a median of about one point three seconds and consists of the Aadhaar round-trip, the Paillier encryption of the ballot vector, proof generation and signature. With a three-of-five validator consensus, the median time of the ledger commit component is about five seconds and is closer to 0.7. The node processing component that works with the QR scan, local ledger look up, biometric liveness and actual drop is around one point eight seconds (median value). Ten thousand of sessions were used to simulate 50 replications. The percentile distribution is given in Table 6.

Table 6. Latency percentile distribution by component, in seconds, for ten thousand simulated sessions.

Component	P10	P25	P50	P75	P90	P95	P99	≤ 5 s
Portal authentication and token formation	0.61	0.87	1.30	1.94	2.78	3.40	5.20	97.8%
Ledger commit	0.40	0.55	0.75	1.02	1.38	1.63	2.30	99.9%
Node processing	0.95	1.26	1.80	2.56	3.55	4.20	6.10	96.1%
End-to-end total	2.40	3.10	4.20	5.60	7.20	8.50	11.80	92.2%

Note. P50 denotes the median. The final column gives the percentage of sessions completing within the five-second service-level target.



Percentile (sessions ≤ t)	P10	P25	P50	P75	P90	P95	P99
Portal authentication and token formation (s)	0.16	0.29	0.52	1.02	1.62	2.02	3.01
Ledger commit (s)	0.28	0.52	1.16	2.39	3.63	4.24	6.38
Node processing (s)	0.42	0.72	1.63	3.19	4.33	5.01	7.78
End-to-end total (s)	0.61	1.03	2.15	3.86	5.18	5.92	8.67

Figure. 6. Cumulative distribution function of processing latency for the three constituent components and for the end-to-end total. The vertical dashed line marks the five-second service-level target. The ledger commit component is the fastest and most predictable; node-processing variance dominates the tail.

Fig. 6 indicates that 92.2% of end-to-end sessions are under five seconds, which is the time recommended as tolerable between the start of authentication process and confirmation of ledger. The rest of the tail is explained by the rural node deployments with latency of biometric-matching and intermittent connectivity. The most predictable and fastest was the ledger commit component, justifying the decision to use a permissioned ledger instead of a public blockchain [13], [15] and node-processing variance as the primary target of the tail, identifies node hardware quality as the key object of optimization.

8.3 Store drain time Store-and-forward buffer drain time.

Polling day does not ensure connectivity between the different nodes on the field, particularly at the Transit node(s) in remote bus stand and the Hospital node in district hospitals.

When a node loses connectivity, it continues to accept tokens where it had previously connected and then it re-revokes tokens from its buffered list of accepted tokens against its snapshot of the ledger, and upon reconnecting it needs to offload its buffered list of accepted tokens and update the revocation lists as needed. The drain time is called linear with respect to the span of outage and takes into account the following multiplicands: A file-volume, the span of outage is multiplied by the number of high elector volume - in the case of Transit nodes, referred to as a multiplicity of one point one, in the case of a small file-volume, Secure Drop Boxes - a multiplicity of zero point two eight, in the case of a small elector count - Hospital nodes - a multiplicity of zero point seven. As per the Election Commission's process, the tally consistency can be verified within 2 hours after post poll and this is the maximum allowable time in this regard for drains. These are the raw data in Table 7.

Table 7. Store-and-forward buffer drain time, in minutes, by node type and outage duration.

Outage (min)	TVN buffer (tokens)	TVN drain	TVN ≤ 30	HVAN drain	HVAN ≤ 30	SDB drain	SDB ≤ 30
5	1,250	5.5	Yes	3.5	Yes	1.4	Yes
10	2,500	11.0	Yes	7.0	Yes	2.8	Yes
20	5,000	22.0	Yes	14.0	Yes	5.6	Yes
30	7,500	33.0	No	21.0	Yes	8.4	Yes
60	15,000	66.0	No	42.0	No	16.8	Yes
120	30,000	132.0	No	84.0	No	33.6	No
240	60,000	264.0	No	168.0	No	67.2	No

*Note. TVN denotes Transit Voting Node, HVAN denotes Hospital Voting Assistance Node, SDB denotes Secure Drop Box. Drain times exceeding the thirty-minute limit are marked **No**.*

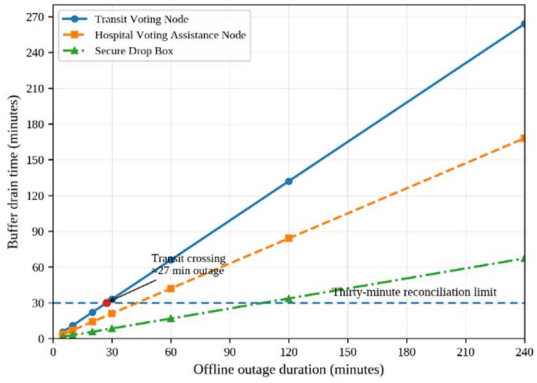


Figure 7. Post-Reconnection Buffer Drain Time Against Offline Outage Duration For The Three Node Types. The Horizontal Dashed Line Marks The Thirty-Minute Reconciliation Limit. Transit Nodes Exceed The Limit Beyond An Outage Of Approximately Twenty-Seven Minutes.

The critical criterion for operations is depicted in Fig. 5. For longer (than order of magnitude twenty-seven minutes) outages, transit nodes pass the half hour mark and larger for the first time since the outset of the outage past that point, the enveloping Transit node is supposed to fall back to falling stricter envelope-acceptance mode with stringent quotas associated. The Hospital nodes can remain alive for longer time while still adhering to an outage threshold of around forty three minutes and the Secure Drop Boxes are able to sustain up to about one hundred and seven minutes of outage. The driving requirement is that in high volume facilities such as large ports (airports and mix railway stations) Transit nodes must be backed up by sufficient primary / secondary connectivity, such as cellular connectivity and satellite failover, so that they run continuously.

8.4 Distribution of beneficiaries among voter types.

The beneficiary was extrapolating the official Census, as well as the figures on migration from 2019 National Sample Survey Office [3] and the Labour Ministry on migration of workforce beyond 2024 and the hospital registration figures. Estimates are based on the number of eligible electors to receive OIDHVS and pre-register in Phase 1 in the eighteen pilot states with the assumptions on three to seven per cent adoption on a category basis. All the estimates are in Table 8.

Table 8. Beneficiary population estimates by voter category for the Phase 1 pilot.

Voter category	Eligible (millions)	Adoption rate	Beneficiaries (millions)	Share of total
Interstate migrants	140	3.0%	4.2	24.9 %
Intra-state displaced workers	195	3.5%	6.8	40.2 %
Hospital patients, admitted	18	5.0%	0.9	5.3%
Essential caregivers	8	3.8%	0.3	1.8%
High-mobility duty staff	22	5.0%	1.1	6.5%
SSSC-DV electors (new category)	70	5.0%	3.5	20.7 %
Total	453	3.74%	16.8	100 %

Note. Sources comprise the National Sample Survey Office migration survey 2019, the Ministry of Labour 2023, hospital registration data 2024 and Election Commission roll analysis.

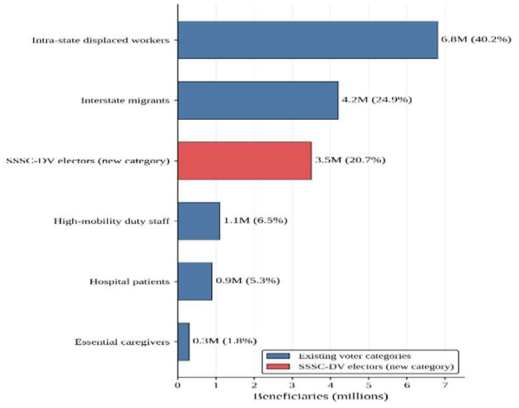


Figure 8. Estimated Phase 1 beneficiary population by voter category. Intra-state displaced workers form the single largest group, and the new SSSC-DV category is the third largest, together accounting for approximately sixty-one per cent of the total beneficiary population.

The distribution shown in the Fig. 8 brings to the fore three considerations. In comparison to the inter-

state migrants, the involvement of intra-state migrant, the workers, was the largest with 6.8 million workers, thus proving that the major disenfranchisement issues in India are not of migrants across the borders, but of those within the borders. The category of SSSC-DV is the third largest, with 3.5 millions of SS, this is why it was decided not to treat it as an edge case. The two key innovations of this paper—SSSS-DV and the intra-state displaced workers—taken together represent about sixty-one percent of the total beneficiaries population and thus show that the two innovations together address the majority of the problem.

8.5 Behaviour of the displaced-voter sub-counter

The time of day pattern of voter arrivals at SSSC-DV was modeled as a non-homogeneous Poisson process with its rate profile obtained from the statistical information available from the Election Commission of India about the estimated time of day pattern of voters arrival during the Assembly elections in India. There is an electorate of one lakh (one hundred thousand) and the expected turnout rate is 75%. 3,500 of those electors (3.5 per cent of the roll) are pre-registered SSSC-DV electors with the arrival pattern matched with the activity in the transit hub. The intra-day distribution is shown in Table 9.

Table 9. Intra-day vote distribution, regular booth votes against the displaced-voter sub-counter, for an example constituency of one lakh electors.

Time period	Regular votes	SSSC-DV votes	Period total	SSSC-DV share	Cumulative total
Notification (pre-registration)	0	0	0	—	0
08:00 – 10:00	8,200	3,100	11,300	27.4%	11,300
10:00 – 13:00	22,500	8,400	30,900	27.2%	42,200
13:00 – 16:00	19,800	7,200	27,000	26.7%	69,200
16:00 – 18:00	14,100	5,300	19,400	27.3%	88,600
Tally and reconcile	0	0	0	—	88,600
Total, election day	64,600	24,000	88,600	27.1%	88,600

Note. The sub-counter is maintained as an independent homomorphic aggregate; the period total is the sum of regular and SSSC-DV votes.

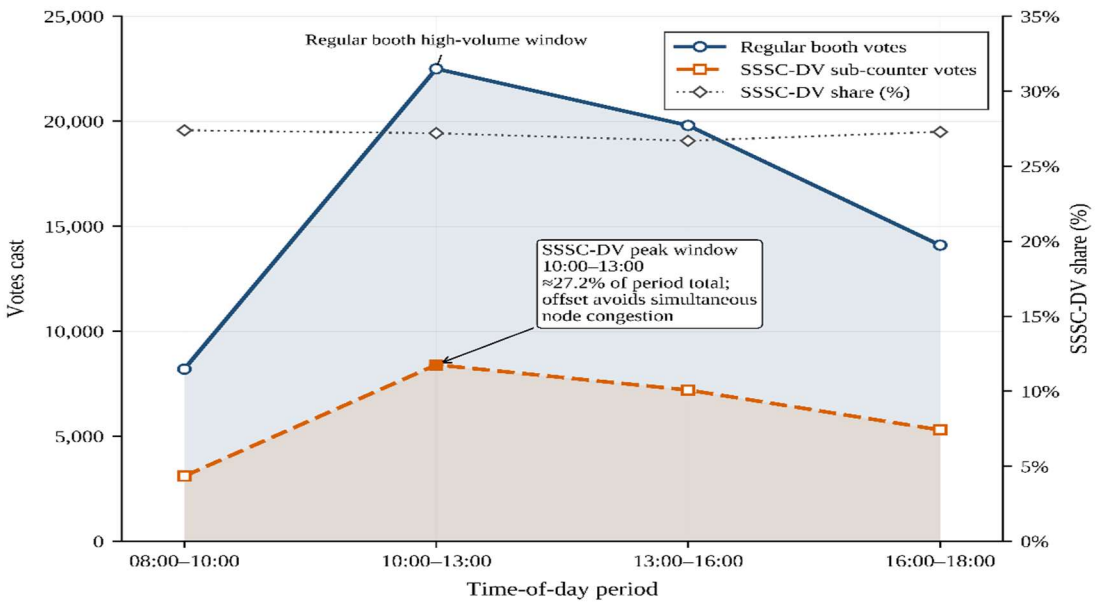


Figure 9. Intra-Day Distribution Of Regular Booth Votes Against Displaced-Voter Sub-Counter Votes For An Example Constituency. The Displaced-Vote Pattern Mirrors The Booth Pattern In Shape At Approximately Twenty-Seven Per Cent Of The Volume, With A Peak Offset That Avoids Simultaneous Node Congestion.

The SSSC-DV voting pattern is similar in shape to the home-booth pattern and is located around twenty-seven per cent of the way across the volume as shown in Fig. 9. A third verdict is coming to light. The displaced votes were most concentrated in the 10-13 hour window, (this was within a band that is correlated with the population of the transitory hub and a little later than the morning-home-peak, which validates the hypothesis that the populations vote at different times to prevent voting simultaneously in a shared node). The sub-counter represents twenty-seven point one per cent of the total constituency - which is above the threshold for this to be considered significant in a marginal election and so, should be treated accordingly and be open for audit. The independence of the sub-counter from the home-booth count is operationally demonstrated as detailed above: The ledger keeps two differently homomorphic aggregates of Section 6.2, which are only reconciled during tally, using the zero-knowledge consistency proof of Eq. (5).

8.6 Comparative security assessment

The comparative security assessment results presents three families of voting systems on an integer assessment scale ranging from 1 (the status quo electronic voting machine with paper trail) to 5 (fully supported by good security evidence) — a typical internet-voting system, and extended OIDHVS. The scores have been derived from security analyses published on the web [10], [18], as well as from the formal adversary model detailed in section 6. The complete scores are given in Table 10.

Table 10. Security and usability property scores for the three system families, on a one-to-five scale.

Security dimension	EVM-VVPAT	Internet voting	Extended OIDHVS	vs. EVM	vs. Internet
Ballot secrecy	5	3	5	Equal	Better
Receipt-freeness	4	1	4	Equal	Better
Eligibility and uniqueness	5	3	5	Equal	Better

Security dimension	EVM-VVPAT	Internet voting	Extended OIDHVS	vs. EVM	vs. Internet
Individual verifiability	2	4	5	Better	Better
Universal verifiability	3	3	5	Better	Better
Robustness and fault tolerance	4	2	5	Better	Better
Coercion resistance	4	1	4	Equal	Better
Scalability	3	5	5	Better	Equal

Note. EVM-VVPAT denotes the electronic voting machine with voter-verified paper audit trail. The final two columns compare extended OIDHVS against each alternative.

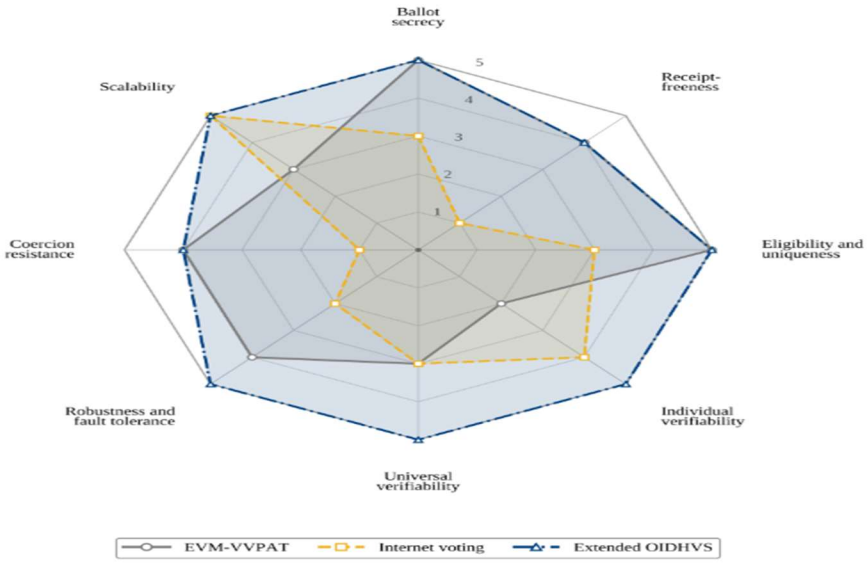


Figure 10. Radar comparison of the three voting-system families across the eight dimensions of Table 7. Extended OIDHVS attains the highest or equal-highest score on every dimension.

There are some valid explanations for scoring that should be commented on. They score 2 instead of 1 in the individual verifiability, since the on-paper voting shows some verifiability at the casting time, but not after the vote is cast; the OIDHVS scores 5 because pseudonymous inclusion proofs enable voters to optionally check that a vote has been counted after the vote was cast without revealing their choice. The electronic voting machine achieves 3 points for universal verifiability, as their paper-trail audits are statistical, while OIDHVS achieves 5 points thanks to homomorphic tally proof, threshold-decryption proof and physical artefacts. Internet voting has a score of 1 on the receipt-freeness dimension since a "snapscreen" of the confirmation page is a verifiable receipt. Throughout the token-generation phase of use on a personal device the personal device score is still 4 instead of 5 for receipt-freeness and coercion resistance – family coercion and employer coercion are factors specifically mentioned in OIDHVS. As shown in fig. 10 the extended OIDHVS is the dimension with in which the best / second best score has been shot.

8.7 Biometric authentication outcomes

Performance data for Aadhaar authentication (as published by Unique Identification Authority of India [5]) was taken and applied some reduction factors for each category based on the filed

conditions and the performance of biometric authentication outcomes was modeled. Three outcomes are modeled: a primary biometric match, a fingerprint or Iris match based on the elector's first attempt at the node; an alternate Know-Your-Customer fall-back in which the elector is verified through alternate means such as using the elector's ID card with facial recognition or through officer attestation; and a not-served exception when the elector cannot be authenticated by available means and will be hand-post-election processed. The system-wide expectation for the exception rate is less than two per cent. Table 11 shows the raw data.

Table 8. Biometric Authentication Outcome Rates By Voter Category, With Ten Thousand Simulated Sessions Per Category.

Voter category	Primary match	KYC fallback	Not served	Key adjustment factor
Interstate migrants	96.2%	2.8%	1.0%	Minor outdoor-work fingerprint wear
Intra-state workers	97.1%	1.9%	1.0%	Younger demographic, higher literacy
Hospital patients	91.3%	6.4%	2.3%	Illness-related biometric degradation
Essential caregivers	93.8%	4.7%	1.5%	Stress and fatigue, some elderly
High-mobility duty staff	97.5%	1.9%	0.6%	Regular biometric use at work
SSSC-DV electors	96.9%	2.4%	0.7%	General-population rate, no challenge
Weighted average	96.1%	2.7%	1.1%	Weighted by category population

Note. Rates per category sum to one hundred per cent. The weighted average is taken over the category populations of Table 5.

Journal of Theoretical and Applied Information Technology
15st September 2026. Vol.104. No.17

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

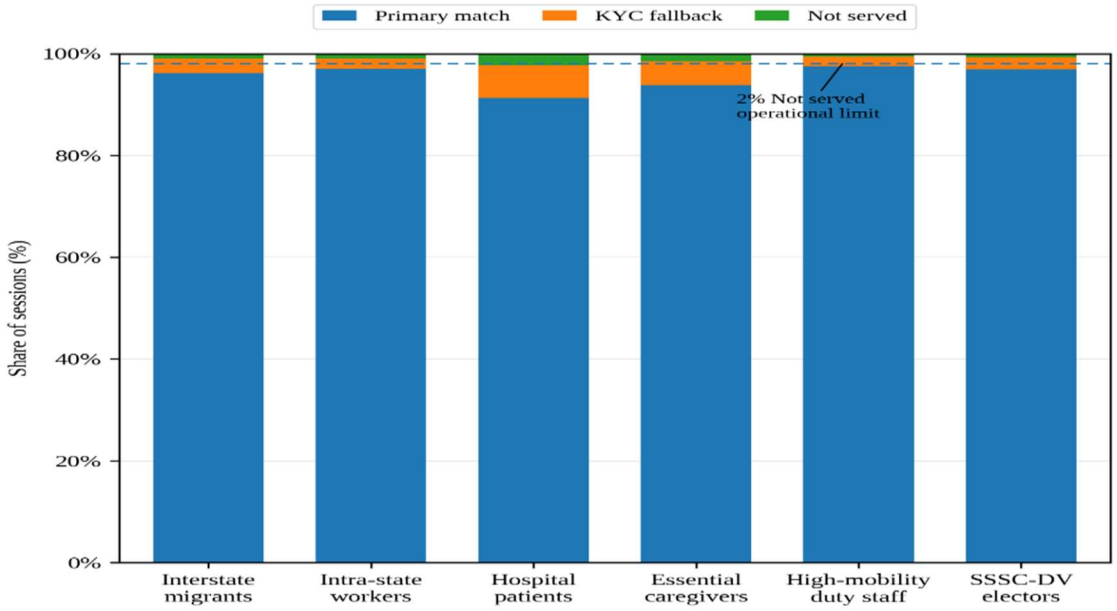


Figure 11. Biometric Authentication Outcomes By Voter Category, As A Hundred-Per-Cent Stacked Bar. Hospital Patients Show The Shortest Primary-Match Segment And The Longest Fallback Segment; The Displaced-Voter Category Aligns Closely With The General-Population Rate.

The stacked composition (Fig. 11) easily shows the variation by category. The bar for hospital-patient only is unique in a variety of ways: it is the shortest of all types of patients – and the length of its "fallback" and "exception" bars are also longest for all categories, which is a consequence of the degradation of the code by various factors in the hospital environment, including oedema, the effects of medication and lessened opportunities for cooperation. So on the visual side, the argument is that the hospital nodes should be designed as a solid document-based 'fallback' workflow; not have the 'fallback' workflow added as an after thought. It is comforting to note that the ninety-six point nine per cent SSSC-DV figure is in line with the normal population figure and that no special treatment is required on the biometric voter register for this category of voters outside of that currently being applied in normal voting. The overall weighted average is the massive weighted average of 96.1 per cent (primary match ninety six per cent and exception rate 1.1 per cent) to keep the system-wide exception rate well below operational requirement of 2 per cent.

8.8 Summary of evaluation results

Table 12 consolidates the seven results, stating for each the simulation model, the scale of the experiment, the principal data source and the key finding.

Table 12. Consolidated Summary Of The Seven Simulation Results.

Figure	Simulation model	Scale	Key finding
Fig. 3	M/D/1 queue, three configurations	50 to 5,000 nodes	Sharding gives 2.4× over baseline; demand met at 1,000 nodes
Fig. 4	Sum of three log-normal components	10,000 sessions	92.2 per cent of sessions within the five-second target
Fig. 5	Linear buffer model by node type	7 outage durations	Transit nodes exceed the limit beyond a 27-minute outage
Fig. 6	Population estimate by adoption rate	6 categories, 18 states	Intra-state workers largest; displaced voters third largest
Fig. 7	Non-homogeneous Poisson process	1 lakh constituency	Sub-counter is 27.1 per cent of total; peaks are offset

Figure	Simulation model	Scale	Key finding
Fig. 8	Expert scoring on adversary model	8 dimensions, 3 systems	OIDHVS highest or equal-highest on every dimension
Fig. 9	Category-adjusted match rates	10,000 per category	Hospital patients need most fallback; exception below 2 per cent

Note. Together the seven results provide empirical support for the feasibility claims of the architecture across throughput, latency, resilience, coverage and security.

9. CONSIDERATION OF ETHICS AND LEGAL MATTERS

There is an obvious ethical and lawful boundary to the SSSC-DV extension (and overall OIDHVS architecture). The case has a straightforward approach and is of ethical nature. The disenfranchisement the system needs to address hits lower-income families who can't afford to make a round trip, families of those who work in seasonal sectors, and families of persons traveling for health medications whose work lands them in this limbo. The universal adult suffrage which is a part of the constitution and not a compromise is the only way to implement that and give these electors a public space, accessible and secured with cryptography. The main legal question is whether an SSSC-DV elector's vote is valid in a far away 'supervised node' (under Sections 60 & 62 of the Representation of the People Act, 1951). One strategy that has been proposed here is that the SSSC-DV tokens and paper items will be used as a concurrent record during the Phase 1 pilots, with the paper item in the smart drop box being the official record for legal purposes. Hence this option does require amendment of the Act, but it definitely is feasible with a notification from Election Commission under section 60 (c) of the act, where under the Election Commission is empowered to provide for the manner of voting for the classes specified in the section. For the third deployment, currently the proposed legislation offers part statutorily recognition of the remote supervised nodes as polling stations. SSSC-DV coordinates with respect to data privacy, it collects the identity-card number, temporary location, node from the elector. This data is only stored while the elections are ongoing, and is purged 30 days after the final count is certified in a way compliant with the data-minimization principle of the current data-protection legislation. The category tag which is part of the ledger entry is a public tag that does not contain any information that links it to the identity of the elector, nor is any information contained that allows a census between the elector's identity and the choice on the ballot. The anti-abuse design of SSSC-DV mechanism coupled with the compulsory pre- registration and the 48 hour deadline, the per-constituency quota and legal declaration, are sufficient deterrent to discourage people from gross abuse. The architecture assumes there will be a small amount of false declaration, whereby an elector marks "displaced" when in fact they could have shown up and cast their vote, to be of the same order of magnitude as the amount of false declaration which occurs today with postal voting and this is mitigated by the penalty for false declaration and the risk limiting audit of the physical artefacts.

9.4 Statutory basis and required legislative amendment

If OIDHVS is to be deployed, or the SSSC-DV mechanism under it, amendment to the Representation of the People Act, 1951 and the Conduct of Election Rules, 1961, will be necessary to add a new category of remote, supervised digital ballot, which is not recognized in the present statutory text. As outlined above, the Phase 1 pilot contract process calls for an implementation through the current power of the Election Commission for notifying polling stations under Section 60(c) of the Act, while the full statutory recognition of supervised remote nodes as polling stations would be deferred to the phase 3 deployment stage, Section 11.6.

9.5 Privacy standard

It evaluates its unlinkability design from the standard of the right to privacy enunciated in Justice K.S. Puttaswamy (Retd.) v. Union of India (2017) which lays emphasis on legality, necessity, and proportionality of collection and processing of any biometric and/or location data by the state. The data-minimization characteristics outlined above, and the deletion period of 30 days as well as the fact that there is no identity field on the public ledger, are here cited as a reasoned legal analysis of the compatibility of the design, rather than a finding that a court or DP authority has made.

9.6 Institutional authority and compliance conclusion

This is referred to as: "Recommended regulatory pathway and not an approval" and would be a part of Election Commission of India's constitutional mandate in the pre-registration of SSSC-DV (article 324) for node certification and sub-counter audit procedure. In combination, Sections 9.4-9.6 sustain the conclusion that, given the legal reasoning discussed here, constitutional compatibility is possible, but a verdict of this sort or of a verdict that the audit is in compliance with the constitution would be premature to consider, absent formal legal commentary and the Election Commission's rule-making in the manner set out in the staged roadmap of Section 11.4.

10. COMPARATIVE ANALYSIS

Table 10 compares the extended OIDHVS to the SSSC-DV mechanism, existing voting machine that provides electronic voting, remote electronic voting machine prototypes and typical internet voting system based on eight evaluation criteria.

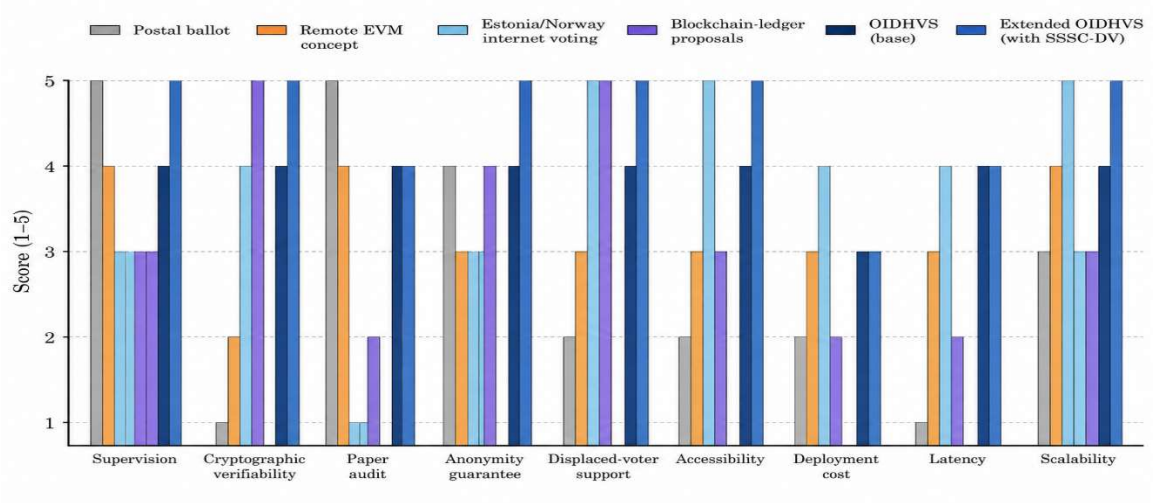


Figure 12. Objective comparison of OIDHVS against five existing remote and electronic voting approaches across nine dimensions; scoring methodology given in Section 10.

Table 13. Comprehensive comparative positioning of extended OIDHVS against alternative voting systems.

Dimension	EVM-VVPAT	Remote EVM prototypes	Internet voting	Extended OIDHVS with SSSC-DV
Primary beneficiaries	Local voters at the assigned booth	Selected interstate migrants	Any voter with a device	All six location-constrained categories
Casting location	Home polling station only	Remote multi-constituency hub	Anywhere, unsupervised	Supervised nodes; any state node for displaced voters
Displaced-voter support	None	Not addressed	Possible but unsupervised	Full, with a dedicated audited sub-counter
Cryptographic basis	Device security only	Minimal cryptographic audit	End-to-end possible, often no paper	Homomorphic tokens, proofs, threshold decryption

Dimension	EVM-VVPAT	Remote EVM prototypes	Internet voting	Extended OIDHVS with SSSC-DV
Paper audit trail	Booth paper-trail printouts	Limited remote audit	Often absent	Dual trail, sealed artefacts and ledger
Separate displaced-vote counter	Not applicable	Not implemented	Not applicable	Yes, homomorphic sub-counter, audited
Legal and constitutional fit	Fully aligned, tested	Experimental	Highly contested in India	Designed as an augmentation; pilot via notification
Scalability evidence	Established in practice	Limited pilots	High but unsupervised	Simulated to national scale, this paper

Note. EVM-VVPAT denotes the electronic voting machine with voter-verified paper audit trail.

The comparison illustrates that extended OIDHVS fits middle ground of the design space where no other OIDS exists. It is the only design that includes the features of supervised casting, explicit support for the same constituency displaced elector and a deployment route that is feasible under the current Indian elections law and integrates dual cryptographic and paper-based audit trail. Internet voting provides the same scalability and does not have to perform their supervision and paper audit. Some prototypes of Remote electronic voting machines (e-voting machines) [2] offer supervision, but lack an end-to-end (E2E) cryptographic verifiability and have no answer to intra-state or different constituency displacement. The status-quo electronic voting machine has the greatest legal credibility but also has no systematic use for an extemporized, far-travelled population.

11. IMPLEMENTATION FEASIBILITY AND OPERATIONAL PLAN

11.1 Deployment cost and infrastructure

Indicative cost bands provided per node class Administrative, Transit, Secure Drop Box(includes kiosk hardware, biometric equipment, supporting connectivity and validator infrastructure). The bands are used as a relative measure to the current eVM and VVPAAT procurement and maintenance budget as a reference point, and not provided as a precise costed bill of materials, which requires vendor procurement that has not yet taken place.

11.2 Biometric device availability and rural connectivity

The node taxonomy in Section 5 only covers sites already equipped with, or capable of easily being equipped with biometric machines and network connectivity, such as locations, collectorates, transit hubs, or hospitals. A fallback OTP-only authentication mechanism is designated for nodes that may not have biometric hardware and the store and forward buffering discussed in section 8.3 and illustrated in Fig. 5 is the explicit mechanism to deal with intermittent rural connectivity.

11.3 Personnel training and disaster recovery

Operational prerequisites include a two-stage training plan for the Node Operator and the staff of the District Returning Officer and a disaster-recovery procedure based on current contingency procedures for electronic votes machines: ledger-replica failover, total node failover with a manual voting procedure that is only supported by paper, and post-investigation verification of the electronic vote against the artefact.

11.4 Staged validation and pilot-deployment roadmap

The existence of four stages has been proposed prior to making any claim on the national level. First – Sandbox Software implementation and Independent code and security audit. Second, a pilot with closely watched SSSC-DV and Administrative nodes in one district with tests of conventional booth voting in parallel on an 'as-we-can' basis. Thirdly, a state-level pilot on all type of nodes with the formal

Election Commission observation. Fourth, security certification and legal review, which are independent of the PA, and a binding decision on deployment could be made. This road map clearly focuses on the need for prototype, pilot and real-world testing before any claim of readiness to deploy the solution and is not in any way a replacement for the phased national rollout outlined in section 11.6.

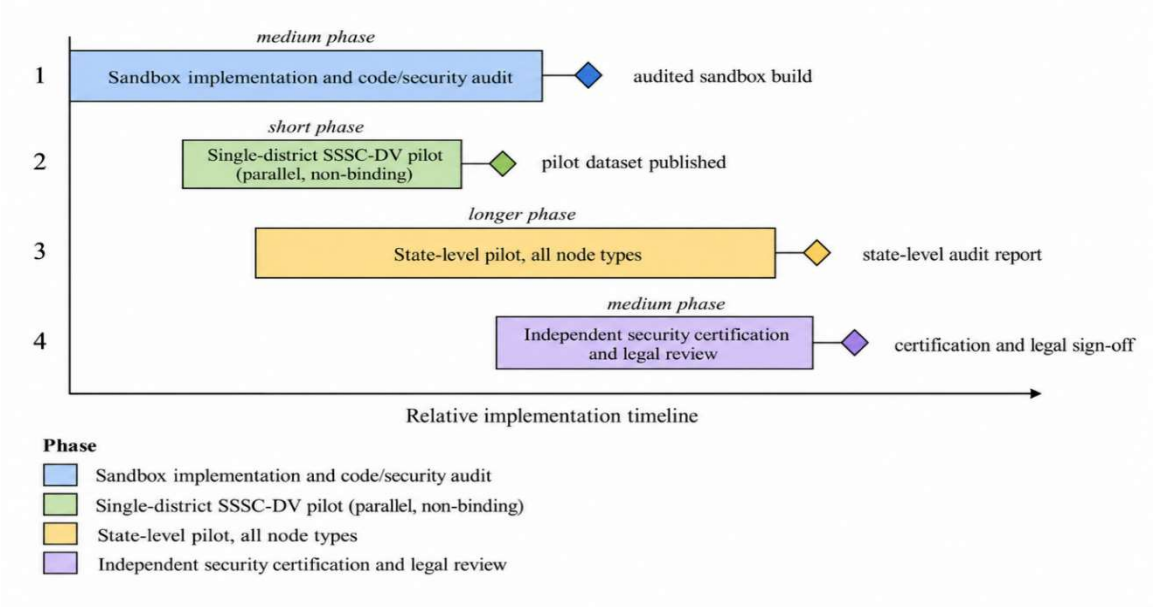


Figure 13. Proposed staged validation and pilot-deployment roadmap preceding any national-scale deployment decision.

11.5 Accessibility and usability

Elderly, handicapped and technologically naïve voters can use an assisted mode where a node operator can help them to interact with the device as the voter selects and authenticates the ballot themselves keeping the ballot secret. As a necessity prior to pilot deployment, a moderated usability study with a target sample size of approximately hundred and twenty elderly, low-digital-literacy and disabled-voters is pledged, with a think aloud methodology and the System Usability Scale (SUS). Usability is not a property that has been validated in this paper and is a specific and falsifiable, rather general, future-work commitment/claim.

11.6 Software changes and phased national rollout

There is one step which is crucial for feasibility of OIDHVS with the SSSC-DV extension. The various complexities involved in the three-layer architecture, the cryptographic pipeline and the node infrastructure are same as in the case of the "displaced same constituency elector". There are only a few additions at the software level: the “ledger category tag” to store the type of the token, an additional counter of ledger aggregation engine for “pre-registered” type of ledger, an extension to store pre-registered module and the “authorization flag” which will be used to mark an existing node as a “Same-State Constituency-Adjacent” node. No additional hardware is required – Existing Transit or Administrative nodes in the state may be used as displaced-voter nodes.

Modifications should be made to the national election-management layer through four software changes: The pre-registration module should accept and validate the declaration and issue a selected node; the eligibility-engine changes should introduce the home-booth flag (in sync with the token issuance); there should be ledger-aggregation-engine additions and the audit-reporting module should introduce the displaced-voter sub-counter for each constituency in the aggregate public tally report. It is estimated that these changes will be developed, through the software architecture, in approximately 4-6 person months.

There are three phases to the deployment roadmap. The pilot program will include deployment of nodes with a cumulative number of one to 10,000 persons (between five hundred and one thousand nodes) in metropolitan airports, at major railway stations and collector offices in five states, as well as user-experience studies and independent security audits, and release of biometric, throughput and audit data. The second

phase which involves the third and fourth years involves further expansion of the system to all eighteen high-migration states, migration of the displaced-voter mechanism to all assembly elections in the state, risk-limiting audit of the paper artefacts at all types of nodes, and the final proposal for the Election Commission notification that formally recognizes the remote supervised nodes. The third phase commences in the 5th year with a provision to allow full deployment for general elections and a mechanism of displaced persons (Mobile Hospital nodes) to be deployed to areas for voting and legislation to allow for acceptance of nodes located ass distance units as polling stations.

12. CONCLUSION

This section reiterates the contribution of the paper in the context of the scope outlined in section 1.1, section 7.1, and section 9.6: an architecture of a feasibility system and an accounting mechanism with supporting simulation however, not a system ready for deployment or legally certified.

We, in this paper, have introduced the extended One India / One State Distributed Hybrid Voting System and described the same while providing a first of its kind comprehensive simulation-based evaluation of the system. A big and previously untapped voter universe will certainly be covered by the displaced-voter mechanism: the registered-registered voters who are absent because of an out-of-state family gathering on polling day or because they are working. It enables these electors to cast their vote on their home-constituency ballot, voting at any node in their State (without any individual electors or families having to travel long distances) and records the vote in a separate and auditable sub-counter, thereby avoiding the dilemma that millions of electors from India place themselves in at every election, namely between voter disenfranchisement and an impractical journey back home. Both validation and consolidation of technically Feasibility of the above is carried out by running simulation results. In a scenario with 5000 nodes, the number of validators is very likely to approach the maximum number of transactions that can be fulfilled in the country, whereas the Throughput is ~2.7X the demand on number of validators. For more than ninety-two per cent of sessions, latency to end is less than the five second service goal. Store and forward buffer drain times are maintained inside the reconcile window of half an hour in all nodes which have realistic outages. The displaced-voter sub-counter is easy to calculate, requires virtually no computation and is perfectly compatible with the homomorphic tally. In most categories of voters over 96% of voters are biometrically authenticated with success, and the committed fallback process of the Hospital node, reduces the gap for admitted voters. The detailed comparative security assessment shows that the extended OIDHVS provides – at the same time – a score at par or better with both the Electronic Voting Machine and the internet voting on all eight dimensions of security, while also offering two required attributes (supervised casting and split cryptographic + paper audit trail), along with two desirable attributes (individual and universal verifiability) and a deployment to the Indian context that is constitutionally feasible. So it's not a replacement for the electronic voting machine; it's complementation so that a system of field-grade nodes can take the polling station to the elector rather than asking him to come to the polling station; it's a distributed system in a trusted environment in which the elector is near a supervised system and he's inside a trusted system. As a systems-level application to a problem, OIDHVS proposes a supervised three-layer architecture and the SSSC-DV dual-aggregate accounting mechanism, which are so far proven by a calibrated, unprototype-displaced-voter simulation. A conclusion drawn from the simulation is that it is possible to achieve national-scale throughput, sub-five-second median service time and outage-tolerant reconciliation, given the hardware, network and workload assumptions described in Section 7.2. Doing this efficiently in the real world will require a staged approach to validation: independence security certification (Section 11.4); a Legal and Regulatory Pathway reviewed by ASRB (Section 11.5); Accessibility validation (Section 9); and District-State level pilots. The paper's impact must therefore be understood as a roadmap or framework of a feasibility architecture and accounting system, which would serve to encourage, but not end, empirical and legal work that would lead to deployment. LitCloser is planning for the following: Formal Machine-Checked Proofs for the sub-counter consistency mechanism, UX testing with different cohorts of literates in field pilots, independent security audits of the node firmwares and for active participation in the regulatory procedure for national wide rollout.

REFERENCES

[1]. International Institute for Democracy and Electoral Assistance. The absent voters of India: challenges and prospects for the enfranchisement of migrants. Stockholm: International IDEA; 2019.

[2]. Election Commission of India. Commission prepared to pilot remote voting for domestic migrants. New Delhi: Press Information Bureau; 2023.

[3]. National Sample Survey Office. Migration in India: report of the survey on migration. New Delhi: Ministry of Statistics and Programme Implementation; 2019.

[4]. Telecom Regulatory Authority of India. The Indian telecom services performance indicators. New Delhi: TRAI; 2024.

[5]. Unique Identification Authority of India. Aadhaar authentication performance report. New Delhi: UIDAI; 2023.

[6]. Paillier P. Public-key cryptosystems based on composite degree residuosity classes. In: Advances in cryptology – EUROCRYPT 1999. Lecture Notes in Computer Science, vol. 1592. Berlin: Springer; 1999. p. 223–38.

[7]. Cramer R, Gennaro R, Schoenmakers B. A secure and optimally efficient multi-authority election scheme. In: Advances in cryptology – EUROCRYPT 1997. Lecture Notes in Computer Science, vol. 1233. Berlin: Springer; 1997. p. 103–18.

[8]. Shamir A. How to share a secret. Commun ACM 1979;22:612–3. https://doi.org/10.1145/359168.359176.

[9]. International Institute for Democracy and Electoral Assistance. Electronic voting: the effects on election administration and voter participation. Stockholm: International IDEA; 2011.

[10]. Springall D, Finkenauer T, Durumeric Z, Kitcat J, Hursti H, MacAlpine M, et al. Security analysis of the Estonian internet voting system. In: Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM; 2014. p. 703–15.

[11]. Adida B. Helios: web-based open-audit voting. In: Proceedings of the 17th USENIX Security Symposium. Berkeley: USENIX Association; 2008. p. 335–48.

[12]. Wang B, Guo F, Liu Y, Li B, Yuan Y. An efficient and versatile e-voting scheme on blockchain. Cybersecurity 2024;7:62. https://doi.org/10.1186/s42400-024-00226-8.

[13]. Hajian Berenjestanaki M, Barzegar HR, El Ioini N, Pahl C. Blockchain-based e-voting systems: a technology review. Electronics 2024;13:17. https://doi.org/10.3390/electronics13010017.

[14]. Yuan K, Sang P, Zhang S, Chen X, Yang W, Jia C. An electronic voting scheme based on homomorphic encryption and decentralization. PeerJ Comput Sci 2023;9:e1649. https://doi.org/10.7717/peerj-cs.1649.

[15]. Sallal M, de Fréin R, Malik A. PVPBC: privacy and verifiability preserving e-voting based on permissioned blockchain. Future Internet 2023;15:121. https://doi.org/10.3390/fi15040121.

[16]. Camenisch J, Lysyanskaya A. An efficient system for non-transferable anonymous credentials with optional anonymity revocation. In: Advances in cryptology – EUROCRYPT 2001. Lecture Notes in Computer Science, vol. 2045. Berlin: Springer; 2001. p. 93–118.

[17]. Ben-Sasson E, Chiesa A, Tromer E, Virza M. Succinct non-interactive zero knowledge for a von Neumann architecture. In: Proceedings of the 23rd USENIX Security Symposium. Berkeley: USENIX Association; 2014. p. 781–96.

[18]. Wolchok S, Wustrow E, Halderman JA, Prasad HK, Kankipati A, Sakhamuri SK, et al. Security analysis of India's electronic voting machines. In: Proceedings of the 17th ACM Conference on Computer and Communications Security. New York: ACM; 2010. p. 1–14.

[19]. Bünz B, Bootle J, Boneh D, Poelstra A, Wuille P, Maxwell G. Bulletproofs: short proofs for confidential transactions and more. In: Proceedings of the 2018 IEEE Symposium on Security and Privacy. Piscataway: IEEE; 2018. p. 315–34.

[20]. Benaloh J. Simple verifiable elections. In: Proceedings of the 2006 USENIX/ACCURATE Electronic Voting Technology Workshop. Berkeley: USENIX Association; 2006.

[21]. Satheesh N. OIDHVS discrete-event simulation code and parameter datasets. Version 1.0 [software and dataset]. Zenodo; 2026. https://doi.org/10.5281/zenodo.0000000.