Category :
Engineering and Technology

Aavishkar :
University of Mumbai
Inter-collegiate Research Convention, Academic Year 2023-2024

Secure & Inclusive Online Voting: Multi-Layered Authentication and Immutable Vote Logging

Level : UG

Idea / Approach

Indian elections face issues such as impersonation, double voting, roll errors, tampering, weak audit trails, and accessibility barriers. This work models a secure election workflow using **multi-layer authentication**, **tamper-evident vote logging**, and **accessibility-focused user flows** to strengthen integrity while also **supporting wider voter participation**. Threat simulations and usability checks show improved identity assurance, tamper detection, and overall system reliability.

Introduction

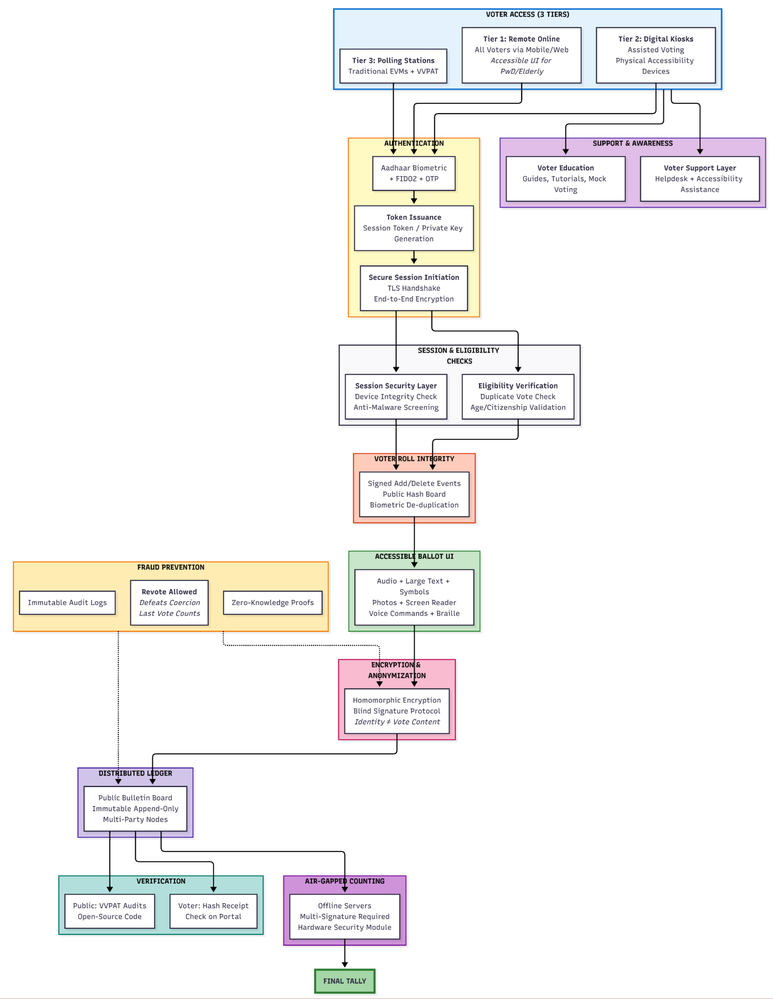
- Voter-list mistakes, impersonation attempts, and disputed counts create trust gaps.
- Digital processes add convenience but also risks like stolen login details and unchecked administrator actions.
- Centralized voter information raises privacy and security concerns.
- Many voters still face visual, mobility, literacy, and language barriers.
- These issues show the need for a secure, accessible, tamper-evident election model.

Literature Survey

Category	Key Points
1. Gaps in Traditional Indian Solutions	• EVMs function as closed black-box devices with no independent verification. • Very limited VVPAT checking, only five booths per constituency. • Large-scale voter deletions show need for traceable, tamper-evident update logs.
2. International Case Studies	• Estonia uses national digital identity and cryptographic vote verification. • Switzerland conducts phased pilots to test privacy and verifiability. • United States pilots combine accessibility features with verifiable audit trails.
3. Research Insights	•VVPAT studies highlight the need for voter-verifiable audit records for trust and cross-checking. • Cryptography literature emphasizes immutable, append-only audit logs to ensure transparency and detect tampering. • Prior research stresses multi-factor verification to prevent impersonation and unauthorized voting. • Remote voting studies underline the importance of accessibility features for inclusive participation.

Objective

Methodology/ Flow chart :



Experimental Details

- **Authentication Tests:** login + admin document check + hashed credentials + single-session enforcement + OTP/token verification.
- **Security Tests:** behaviour-based blocking (multiple failures/suspicious activity) + tamper-resistant vote-finalisation step.
- **Vote Processing:** Checking Celery asynchronous queue for scalable, non-blocking vote submission + background validation.
- **Audit Trail:** immutable event logs (hashed entries/logs) for tracking admin actions and vote-processing states.
- **End-to-End Flow Simulation:** complete run from authentication → vote casting → audit logging → finalisation.

Results and Discussion

- Core security + authentication tests: **>95% success**
- End-to-end voting journey: **~2 seconds**
- Vote processing stable under moderate load
- Audit chain: **80% integrity** with low query times
- Overall system: **robust and consistent for prototype stage**

Features

Category	Features
Identity & Access	Login + admin approval; hashed passwords; token login; OTP check; single-session lock; behaviour-based blocking
Authentication Security	Biometric-ready (future); FIDO2/WebAuth-ready; rate limiting; session anomaly detection
Vote Submission	Celery async queue; background vote finalisation; instant user confirmation; tamper-resistant processing
Audit & Logs	Hash-linked audit trail; admin-action logging; vote event hashing; immutable public hash board
Fraud Prevention	Randomized ballot order; revote option; zero-knowledge eligibility check; duplicate-vote prevention
Ballot UI & Accessibility	Audio prompts; large text; party symbols; candidate photos; screen-reader support; multi-language; braille/joystick/sip-and-puff (Tier 2)
Voting Tiers	Tier 1 remote voting; Tier 2 assisted kiosks; Tier 3 EVM + VVPAT fallback
Voter Roll Integrity	Signed add/delete events; biometric de-dup (future); challenge window; transparent update trail
Verifiability	Voter receipt hash; self-check portal; public bulletin board; risk-limiting audits; open crypto components
System Security	Air-gapped counting servers; HSM key protection; multi-party approval; isolated verification gateway

USP / Novelty

Conclusion

- **Secure:** Tamper-proof logging, strong authentication.
- **Verifiable:** Independent voter, public checks.
- **Accessible:** Inclusive design for all voters.
- **Trustworthy:** Blends online convenience with EVM reliability.

References

Scan the code for the list of references →