E-Vote: A Secure, Accessible Online Voting System for Small-Scale Elections

1. Summary

E-Vote is a desktop-based online voting prototype designed to make digital elections secure, transparent, and inclusive. It addresses critical barriers to adoption, including identity fraud, cybersecurity threats, and accessibility limitations, by implementing multi-factor verification, resilient infrastructure, and inclusive design principles. The platform targets student elections, NGOs, local councils, and other small-scale democratic setups, enabling verified users to vote remotely while maintaining trust, transparency, and auditability.

---

2. Project Background and Motivation

Traditional paper-based voting systems remain the global standard despite their limitations, including restricted accessibility, human error, logistical inefficiencies, and high operational costs. Trust in electronic voting has been consistently low due to concerns over identity fraud, cybersecurity vulnerabilities, and usability for individuals with impairments or low digital literacy. Research shows that even with rapid technological adoption, voters and administrators hesitate to rely on online systems without demonstrable security and transparency measures.

Existing systems, such as Estonia's i-Voting platform, demonstrate that secure online voting is feasible at scale through cryptographic verification and digital ID integration. However, many current e-voting platforms fail to adequately address accessibility or risk modeling based on real-world vulnerabilities. E-Vote differentiates itself by combining research-led risk assessment with inclusive, user-centered design, ensuring the platform is secure, verifiable, and usable by individuals with diverse abilities. This approach creates a practical and trustworthy solution for small-scale elections while exploring secure system design, cloud-native infrastructure, and DevOps principles.

---

3. Aims and Objectives

Aim:

To design and prototype a secure, transparent, and accessible online voting system that allows

verified users to vote remotely while maintaining trust, security, and auditability.

Objectives:

1. Implement secure user authentication to prevent identity fraud.
2. Protect vote data and system integrity against cybersecurity threats.
3. Ensure the platform is accessible to users with impairments, low digital literacy, or mobility limitations.
4. Provide a transparent, verifiable voting process with real-time tallying and auditable logs.
5. Develop a proof-of-concept desktop application suitable for student elections, NGOs, and small-scale democratic setups.

---

4. Key Problem Areas and Challenges

A. Identity Fraud in Online Voting

Identity fraud represents the most direct threat to election integrity. Our research identified three critical categories:

1. **Impersonation (Traditional Identity Theft):**
   Attackers use stolen credentials or personal data to vote as legitimate users.
   Example: Phishing emails mimicking the election portal trick voters into disclosing credentials.
2. **Synthetic Identity Fraud:**
   Fraudsters register fake voters by combining real identifiers (e.g., valid SSNs) with fabricated names or addresses.
   Example: “Child SSN exploitation” or “deceased voter resurrection” schemes.
3. **Account Takeover:**
   Hackers gain access to real voter accounts through SIM-swapping, credential stuffing, or social engineering.
   Example: An attacker intercepts OTP codes after transferring a victim’s phone number.

Mitigation in E-Vote:

- Multi-factor authentication (OTP + password)
- Strong registration verification linked to official ID or institutional record
- Hash-chained audit logs to trace votes without revealing voter identity
- Automated anomaly detection (e.g., multiple logins from new devices)
- Restricted admin privileges to prevent insider manipulation

---

B. Cybersecurity Threats for Electronic Voting

Four main cybersecurity risks were identified from IEEE and government sources:

1. **Voter Registration Database Attacks:**
   Attackers could insert, delete, or modify records to enable fraud.
   Response: Mirrored, encrypted registration databases with immutable audit logs and restricted update permissions.
2. **System Availability Disruptions (DoS / Overload):**
   High traffic or malicious attacks could crash the system.
   Response: Distributed servers, load-balancing, real-time monitoring, and automated failover.
3. **Unauthorized Access and Vote Manipulation:**
   Compromised credentials or insider threats could alter votes.
   Response: Encrypt all data at rest and in transit, enforce least-privilege access, and implement cryptographic hash-chaining.
4. **Insider Abuse:**
   Election staff could alter or leak sensitive information.
   Response: Role-based access controls, logging of all admin actions, and independent verification of results.

C. Accessibility Barriers

Accessibility limitations prevent equitable participation for users with visual, auditory, motor, or cognitive impairments. Common issues include:

- Small or fixed font sizes, non-scalable text, or improperly responsive layouts
- Gesture-only or path-based interactions that exclude users with motor impairments
- Poor screen reader support, missing alt text, or confusing navigation order
- Inadequate alternatives for audio/video content, CAPTCHAs, or error handling

Mitigation in E-Vote:

- Follow WCAG AA guidelines for mobile and desktop accessibility, including contrast, focus order, alt text, and interactive element sizing
- Support for OS dynamic font scaling up to a reasonable percentage to ensure readability
- Single-finger or keyboard alternatives for complex gestures
- Multiple navigation options, clear confirmation buttons, and accessible 2FA inputs
- Captioned or text-based alternatives for any media content
- Conduct automated and manual accessibility testing using tools like BrowserStack Live, simulating different assistive technologies, screen readers, and device conditions to verify

inclusivity and usability for all users

---

5. System Overview and Features

Platform: Desktop-based (Windows, macOS, Linux)

Key Features:

Feature	Problem Area	Description	User Benefit
Multi-Factor Authentication	Identity Fraud	OTP + password login with strong registration verification	Ensures only legitimate users can vote
Secure Vote Casting	Cybersecurity	End-to-end encrypted vote submission with hash-chaining	Protects votes from tampering and maintains trust
Audit Logs & Real-Time Tallying	Cybersecurity	Immutable, time-stamped logs and transparent vote tally	Enables verifiable and transparent election audits
Distributed, Resilient Infrastructure	Cybersecurity	Load-balanced servers with automated failover	Maintains system availability during high traffic or attacks
Role-Based Admin Controls	Cybersecurity	Granular permissions and detailed logging	Prevents insider abuse and manipulation
Accessibility Support	Accessibility	Screen reader compatibility, keyboard navigation, scalable fonts, multiple	Ensures inclusive experience for all users, including those with disabilities

		navigation options	

Uniqueness:

Most online voting systems focus on blockchain or cryptographic complexity. E-Vote's innovation lies in balancing *practical security with inclusivity* — applying verifiable principles to a prototype that is usable, auditable, and realistic within small-scale election contexts.

---

6. User Experience Design

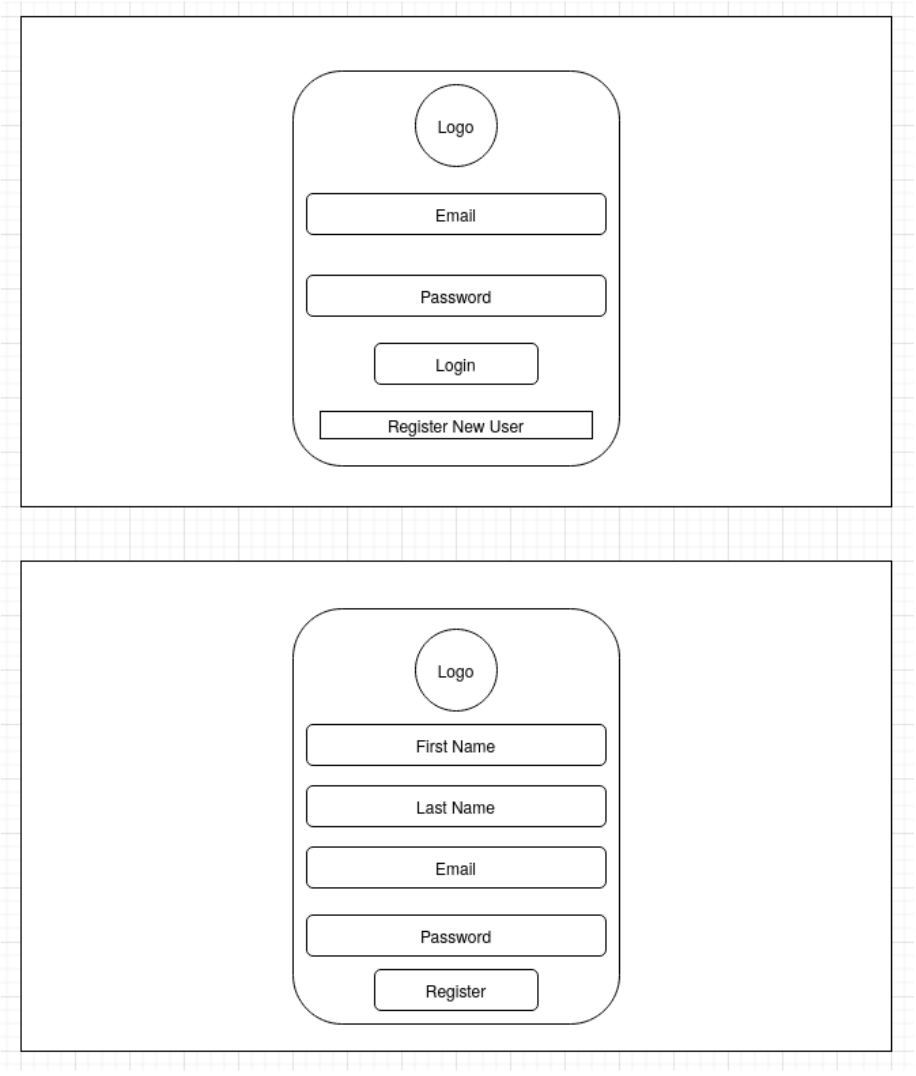

Figure 1: Login and Registration

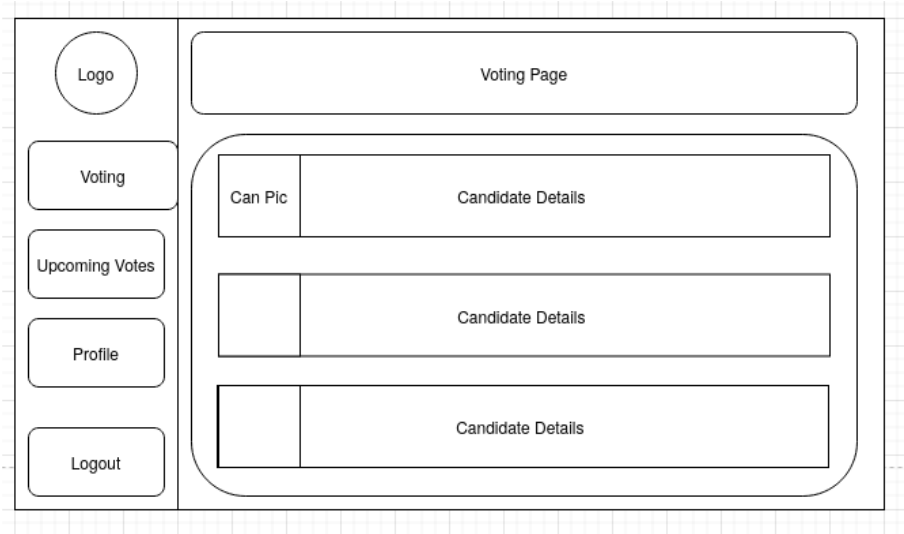

Figure 2: Dashboard

---

7. Expected Outcomes

By the end of the project, the team will deliver:

- A functional prototype of a secure online voting system.
- Demonstration of fraud prevention, accessibility, and verifiable logging mechanisms.
- Evaluation report detailing usability and trust perception among test users.

Success Criteria:

- All users can register, verify, and vote successfully within defined time windows.
- No duplicate or invalid votes recorded in audit logs.
- Simulated penetration tests confirm system resilience.
- Positive usability feedback from test participants, including those with limited technical experience.

Anticipated Impact:

E-Vote demonstrates that **digital elections can be both secure and inclusive**. It aims to serve as a model for small-scale democratic processes, offering institutions a credible, transparent foundation for digital participation — without requiring national-level infrastructure.

References

- Reddit discussion: "Is there any genuine reason to not allow online voting?"
- EU Commission (2019), Remote Voting Solutions: Access, Security, and Participation.
- Caltech Science Exchange (2024), Online Voting Risks and Benefits.
- Stanford CS181 Project (2006), Electronic Voting Systems.

- Estonian National Electoral Commission (i-Voting) [https://www.valimised.ee/en/internet-voting]
- Electronic voting system using Blockchain technology
- https://ieeexplore.ieee.org/document/11035902
- https://ieeexplore.ieee.org/document/9626247
- https://ieeexplore.ieee.org/document/10664114
- https://ieeexplore.ieee.org/document/9626247