Project Proposal Document

Designing Secure Vote-Transfer Mechanisms for E-Voting Systems

Team Members:

A. Krishi Prashant Shah - krishah@ucdavis.edu
B. Saurav Mohanty - samohanty@ucdavis.edu
C. Urmil Jatin Chandarana - uchandar@ucdavis.edu

Literature Review: Foundations for a Secure E-Voting System

We begin by reviewing the prior research on secure e-voting to ensure that our proposed solution is grounded in proven research. Each of the team members was responsible for identifying a key paper in this area, and based on that, an analysis of the following four key areas has been made:

1. The essential security requirements of an e-voting system.
2. Different system architectures and technologies currently in use, including blockchain.
3. How these systems work in maintaining security and integrity.
4. Major weaknesses and vulnerabilities which yet need to be overcome.

Core Security and System Requirements

Research points out the tough set of security requirements that every trustworthy e-voting system must satisfy.

A. Basic Requirements: An appropriate electronic voting system has to meet some critical areas: authentication, data privacy, data integrity, transparency, and verifiability.
B. Ballot Secrecy: Voter anonymity must be protected to prevent coercion or the act of vote-buying. This directly leads to the first goal of our project: votes should be secret.
C. Integrity and Trust: Transparency of and ability to verify election outcomes are essential in fostering public confidence in an election. Closed, proprietary systems like the Voatz app have thus been criticized as “threats to electoral integrity” since they cannot be independently inspected.
D. Auditability: While verifiable audit trails are important for proving system integrity-a key concern of our second project goal-research into voting systems still finds that traditional paper backups are often far more reliable than purely electronic systems, such as Direct Recording Electronic, or DRE, systems.

Requirements	Description
Anonymity	A vote should not be associated with a voter.
Auditability and accuracy	Voting processes should be able to be checked, audited, and certifiable by autonomous agents.
Democracy/singularity	Every voter should be allowed to vote only once.
Vote privacy	There is no way to prove the voter by his/her casted vote.
Robustness and integrity	It should be impossible to change or eliminate votes after they have been cast.
Voter verifiability	Everyone should be able to independently confirm that all the votes have been tallied accurately.
Verifiable participation/authenticity	Only those voters who have the right to cast a vote are verified by the system.
Transparency and fairness	Voting systems should be transparent and rely on the accuracy, precision, and protection of voter security.
Availability and mobility	Voting systems should be permanently accessible during the election period. Voting systems should not restrict the voting location.
Accessibility and reassurance	Voting systems should be available for people with disabilities or special conditions without requiring specific equipment or abilities.
Recoverability and identification	Electoral systems can detect flaws, defects, and attacks and restore voting data to their previous state.

Potential System Architectures and Technologies

We explored several system architectures, focusing in particular on blockchain as a basis that can potentially ensure secure e-voting.

- ➔ As a Base Layer, blockchain-based systems are well-liked due to their decentralization and immutability in facilitating data integrity and transparency.
- ➔ Tamper-Proof: Smart contracts and blockchain are designed to make votes unmanipulatable; votes would be verifiably authentic, per se, which is in line with our integrity ambition in the project.
- ➔ Implementation Matters: Yet, as the Security Analysis of Voatz paper illustrates, security really depends on how something is implemented. While Voatz employed a permissioned blockchain and mixnet, researchers still determined that the system was "unlikely to protect against server-side attacks." This points out that blockchain alone isn't adequate to guarantee security; careful design and implementation are critical.

Key Vulnerabilities Identified

Our review identified several major vulnerabilities directly impacting our project goals:

- ➔ Network-level threats, impacting privacy: Even when encrypted, an attacker can still carry out traffic analysis based on packet timing and size; this might reveal to the attacker when someone voted or whether their vote was accepted.
- ➔ Client-Side Threats (Affecting Privacy & Integrity): Malware on a voter's device can intercept or modify a vote before it is sent, resulting in fraudulent ballots — as shown in the Voatz analysis.
- ➔ System-Level Threats Affecting Integrity & Availability:
  - ◆ Lack of Verifiability: Proprietary, closed systems block independent auditing; thus, it is impossible to show proof of election integrity publicly.
  - ◆ Limited Scalability: Most blockchain systems are not designed to handle the transaction volumes created during national elections and might crash or be unavailable.

Fundamental Design Countermeasures

These risks point to the need for our system design to put in place the following countermeasures:

- ➔ Defending Against Traffic Analysis-Supports Goal 3: Resilience: Encryption is not enough. We must pad packets to make the packets containing data all the same size and equalize timestamps to hide voting times.
- ➔ Ensure End-to-End Verifiability: This system must be transparent and publicly auditable to avoid the "black-box" issues identified in Voatz, enabling anyone to verify that votes are recorded as cast.
- ➔ Engineering for Scalability - Performance bottlenecks in the blockchain should be tested using scaling solutions such as sharding, high-throughput consensus algorithms, and optimized transactions to ensure stable operations during periods of peak voting.

Bibliography

- **Paper 1:** Belousova, A., Marchiori, F., & Conti, M. (2025). *Inference Attacks on Encrypted Online Voting via Traffic Analysis* . arXiv:2509.15694v1.
- **Paper 2:** Specter, M. A., Koppel, J., & Weitzner, D. (n.d.). *The Ballot is Busted Before the Blockchain: A Security Analysis of Voatz, the First Internet Voting Application Used in U.S. Federal Elections*. MIT.
- **Paper 3:** Jafar, U., Ab Aziz, M. J., Shukur, Z., & Hussain, H. A. (2022). A Systematic Literature Review and Meta-Analysis on Scalable Blockchain-Based Electronic Voting Systems. *Sensors*, *22*(19), 7585 . https://doi.org/10.3390/s22197585