Title

Secure Biometric E-Voting System

Advisor

Oluwafemi Samuel

Project Description

Project Overview

The use of technology in elections has become increasingly important worldwide. Electronic voting (e-voting) systems have the potential to improve accessibility, speed up vote counting, and reduce electoral fraud. One promising approach is to integrate biometric authentication, using unique human traits such as fingerprints or facial features to verify voters' identities.

This project explores the design and implementation of a secure e-voting system that balances voter authentication with anonymity and transparency. Students will research existing technologies and protocols, then propose and develop a prototype system demonstrating secure and verifiable voting.

Motivation

Traditional elections face challenges such as voter impersonation, ballot tampering, and slow vote counting. Biometric authentication can address voter verification challenges, while cryptographic protocols can help maintain the secrecy of votes. This project allows students to explore the intersection of computer security, biometrics, and human-computer interaction in a socially impactful context.

Research Questions

Students will have the freedom to investigate questions such as:

1. Which biometric modality (e.g., fingerprint, facial recognition, iris scan) is most suitable for an e-voting system in terms of accuracy, cost, and usability?
2. How can voter anonymity be maintained in a system that requires biometric authentication?
3. What mechanisms can ensure transparency and verifiability of election results without compromising voter privacy?

Student Scope and Flexibility

The project is intentionally open-ended, allowing students to make critical design decisions, including:

- Choice of biometric modality for authentication.
- Design of the voting interface (web, mobile, or desktop).
- Selection and implementation of anonymisation and cryptographic techniques.
- Methods for testing and demonstrating system security, usability, and reliability.

Technologies (suggestive)

1. Biometric Authentication:
    - Fingerprint, facial recognition, or iris recognition libraries/SDKs.
    - Template extraction and matching algorithms.

2. Frontend & Backend Development:
    - Web: HTML, CSS, JavaScript (React/Vue/Angular)
    - Backend: Python (Flask/Django), Node.js, or Java/C#
    - APIs for client-server communication.

3. Databases:
    - Relational (MySQL, PostgreSQL) or NoSQL (MongoDB)
    - Secure storage with encryption for sensitive data.

4. Cryptography & Security:
    - SSL/TLS, digital signatures, hashing
    - Protocols to maintain anonymity and verifiability (blind signatures, homomorphic encryption, zero-knowledge proofs).

Skills the student will develop and any prerequisites

- Biometric authentication and computer vision
- Software development and database management
- Critical analysis of security and privacy issues
- Research, experimentation, and academic reporting