Software Requirements Specification

for

E-VoteSecure - An Online Voting System

Version 1.0 approved

Prepared by Group InfoSec

04.10.2024

.

Table of Contents

Revision History

Name	Date	Reason For Changes	Version
InfoSec	04.10.2024	Initial Report	1.0

1. Introduction

1.1 Purpose

The purpose of this document is to outline the system requirements for an **Online Voting System** designed to conduct secure and transparent elections using electronic means. This system will allow voters to cast their votes remotely via mobile devices while ensuring the integrity, confidentiality, and anonymity of the election process. The system leverages unique National Identity Card (NIC) numbers and mobile apps registered to individual voters for secure access.

1.2 Document Conventions

This document follows the standard typographical conventions, with headings, subheadings, and bold text for emphasis. All the requirements are prioritised and structured hierarchically.

1.3 Intended Audience and Reading Suggestions

This document is intended for system developers, project managers, election officials, auditors, and security personnel. It is recommended to read the chapters most related to the individual's role, beginning with the general chapters.

1.4 Product Scope

The system will cater to eligible voters with unique NICs and registered mobile phones. It will be accessible via an app and will include features for secure authentication, vote casting, vote recording, real-time validation, and audits. Key components of the system include:

1. **Voter Registration Module**
2. **Voter Authentication and Verification**
3. **Secure Voting Interface**
4. **Encrypted Vote Transmission**
5. **Tamper-Proof Vote Storage**
6. **Audit Trails and Logs**
7. **Post-Election Audits and Results Certification**

1.5 References

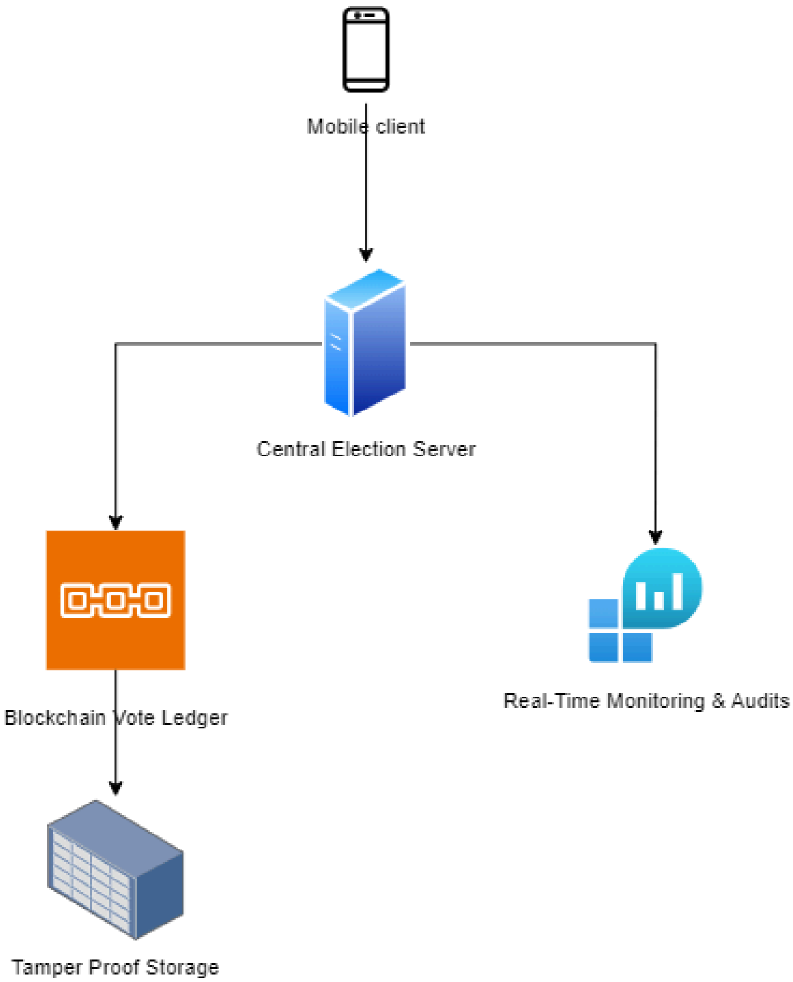
IEEE. IEEE Std 830-1998 IEEE Recommended Practice for Software Requirements Specifications. IEEE Computer Society, 1998.

2. Overall Description

2.1 Product Perspective

The Online Election System is a standalone product designed to facilitate secure, electronic voting for national, regional, and local elections. The system is not part of a larger product family but is a modern replacement for traditional manual election systems. This system leverages modern technology, including mobile devices, two-factor authentication, and blockchain-based vote storage, to provide a transparent and secure voting process.

The product interacts with various subsystems such as the National Identity Database for voter verification, secure mobile apps for voter interaction, and a blockchain-based ledger for vote storage. It integrates with government infrastructure to securely verify voters using their unique National Identity Card (NIC) numbers and registered mobile devices. The system's architecture also supports interconnectivity with legal bodies for auditing, certification, and dispute resolution.



2.2 Product Functions

The Online Election System provides the following key functions to ensure a secure and transparent voting process:

- **Voter Registration and Verification:** Integration with the National Identity Database to verify the eligibility of voters using NIC numbers and mobile devices.
- **Two-Factor Authentication (2FA):** Voters authenticate using their NIC number and a second factor such as a PIN, biometric authentication, or a unique code sent to their mobile device.
- **Ballot Presentation:** Once authenticated, voters receive their ballot, tailored to their election district, allowing them to select candidates or options.
- **Vote Casting:** The system allows voters to cast their votes electronically, with the vote being encrypted and securely transmitted to the central election server.
- **Blockchain-Based Vote Storage:** Votes are stored in a tamper-proof blockchain ledger, ensuring that they cannot be altered once cast.
- **Audit Trails and Logging:** Every action, from voter authentication to vote submission, is logged securely to allow for post-election audits and verification.
- **Real-Time Monitoring:** Election officials can monitor the voting process in real-time to detect and address any irregularities.
- **Post-Election Audits:** The system supports independent audits and recounts to verify the accuracy of the results and ensure that the election process is carried out fairly.

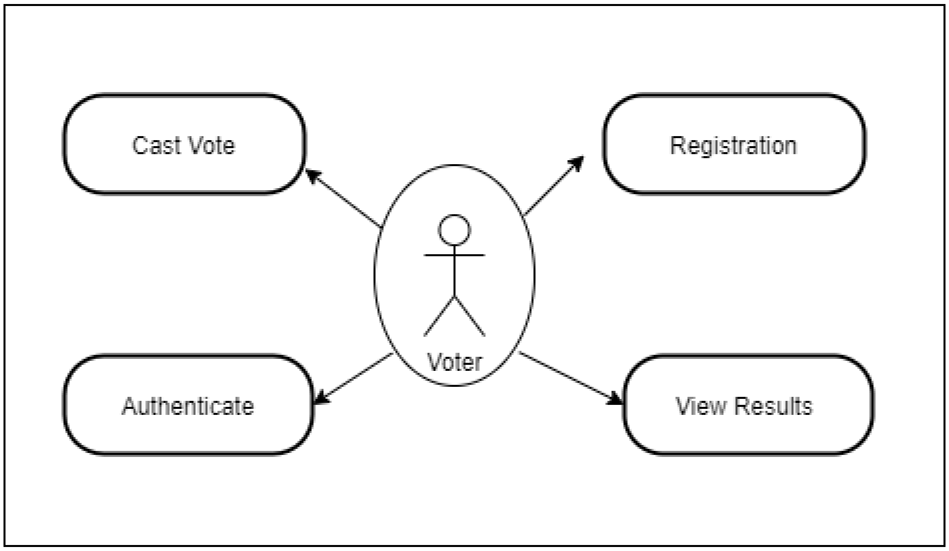
2.3 User Classes and Characteristics

In the Online Election System, we identify several distinct user classes based on their roles, technical expertise, and the level of access required within the system. These classes differ in their frequency of use, the subset of system features they access, and their privilege levels.

1. Voters

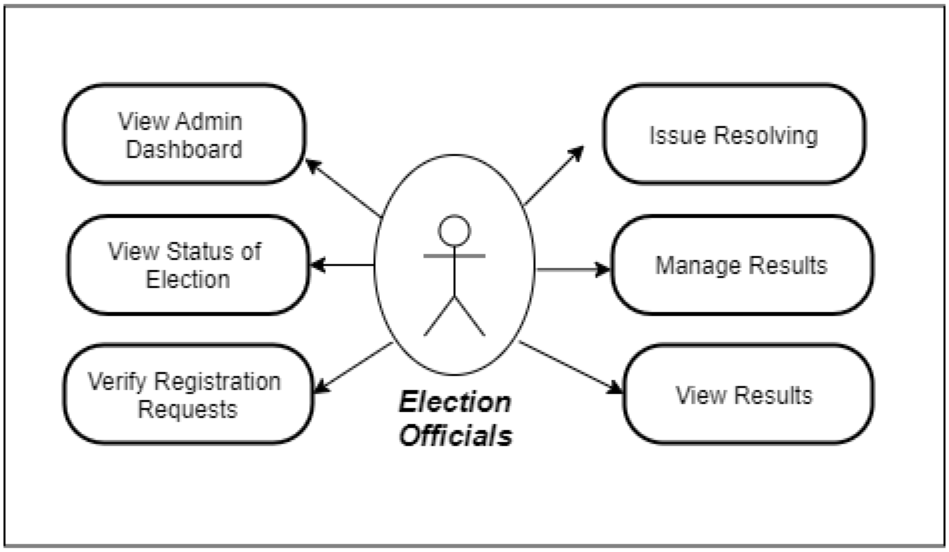
- **Frequency of Use:** Occasional (during election periods).
- **Technical Expertise:** Basic to intermediate. Voters are expected to know how to operate a mobile app, authenticate using their NIC, and cast their vote.
- **Security Level:** High priority is placed on maintaining voter anonymity and secure authentication.

- **Characteristics:**
  - Use the system to authenticate their identity and cast their vote.
  - Require easy-to-use interfaces with clear instructions.
  - Must receive prompt support for issues like forgotten passwords or lost devices.
- **Importance:** The most critical user class, as they are the primary participants in the election process.



2. Election Officials

- **Frequency of Use:** Frequent (before, during, and after election periods).
- **Technical Expertise:** Intermediate to advanced. Officials must be able to manage the backend systems, monitor voter registration, authenticate results, and manage the election process.
- **Security Level:** High. Election officials have access to sensitive election data and are responsible for managing the integrity of the system.
- **Characteristics:**
  - Oversees voter registration and monitors the voting process.
  - Manage audits, vote counting, and results certification.
  - Require access to system logs and real-time monitoring tools.
- **Importance:** Very important, as they ensure the election process is managed correctly and transparently.



3. System Administrators

- **Frequency of Use:** Continuous.
- **Technical Expertise:** Advanced. Administrators are responsible for maintaining the system, ensuring its security, and fixing any technical issues.
- **Security Level:** Highest. Administrators have full access to system configuration, security settings, and data storage, including encryption mechanisms.
- **Characteristics:**
  - Ensure system uptime and performance.
  - Responsible for system security, including encryption of data and secure communications.
  - Perform system audits and respond to potential security threats.
- **Importance:** Critical, as they maintain the security and stability of the entire system.

4. Auditors (Independent/Third-Party)

- **Frequency of Use:** Post-election.
- **Technical Expertise:** Intermediate to advanced. Auditors need to access system logs, audit trails, and the blockchain ledger to verify the accuracy of results.
- **Security Level:** Medium to high. Auditors must have access to detailed logs but should not have access to modify election data.
- **Characteristics:**
  - Conduct independent audits to verify that votes were counted accurately and the system was not tampered with.
  - Review audit trails, system logs, and the blockchain ledger to validate election integrity.
- **Importance:** Important, as they provide independent verification of election integrity

5. Help Desk/Support Staff

- **Frequency of Use:** Continuous during election periods.
- **Technical Expertise:** Basic to intermediate. Support staff assist voters and election officials in resolving issues related to system access, authentication, and technical troubleshooting.
- **Security Level:** Medium. They do not have access to sensitive election data but must ensure secure handling of voter identity issues.
- **Characteristics:**
  - Provide support to voters and officials via hotlines or help desks.
  - Assist with resetting accounts, troubleshooting device issues, and other technical problems.
- **Importance:** Supportive, as they ensure smooth operation during voting periods by helping resolve issues quickly.

2.4 User Class Prioritization

- **Voters** - Critical, as they are the primary users of the system.
- **Election Officials** - Vital for the proper execution and management of the election.
- **System Administrators** - Essential for maintaining system security and functionality.
- **Auditors** - Necessary for validating and certifying election results.
- **Help Desk/Support Staff** - Important for resolving user issues during the voting process.

Each user class has distinct requirements based on their role in the election system, and their needs must be addressed to ensure a smooth, secure, and fair election process.

2.5 Operating Environment

The Online Election System will operate across multiple platforms and environments, ensuring compatibility with both voter devices and the election management infrastructure. Below is a description of the operating environments for each component of the system:

1. Voter Devices (Mobile Environment)

- **Hardware Platform:**
  Mobile devices, including smartphones and tablets.

- **Operating Systems Supported:**
  - **iOS:** Version 12.0 or later
  - **Android:** Version 8.0 (Oreo) or late

- **Required Applications:**
    - The official election app will be developed for both iOS and Android platforms. This app must peacefully coexist with other apps running on the voter's device, ensuring no conflicts with personal applications.
    - The app will require access to device features such as biometric authentication (fingerprint/face recognition), a camera, and internet connectivity (Wi-Fi or mobile data).

- **Network Connectivity:**
    - Internet connection via 3G/4G/5G or Wi-Fi for real-time interaction with the election server.

- **Security Requirements:**
    - Secure boot and device encryption must be enabled on supported devices to ensure protection against tampering.
    - The system will require the latest security patches and updates from the operating system for optimal security.

2. Central Election Server

- **Hardware Platform:**
  High-performance servers or cloud infrastructure capable of handling large volumes of secure data transactions during election periods.

- **Operating Systems Supported:**
    - **Linux (Ubuntu or CentOS):** Preferred for high security and stability. The version must be one of the long-term support (LTS) versions for security and performance benefits.
    - **Windows Server 2019 or later** (if required for certain administrative tools or compatibility reasons).

- **Required Software Components:**
    - **Blockchain Platform:** The server will operate a distributed ledger technology such as Hyperledger Fabric or Ethereum to securely store votes and ensure immutability.
    - **Database Systems:** A secure relational database (e.g., PostgreSQL or MySQL) for storing non-vote-related data, such as voter registration logs and audit trails.
    - **Web Application Frameworks:** Node.js, Django, or a similar framework to manage server-side logic for voter verification, vote submission, and real-time monitoring.

- **Network Configuration:**
  - Encrypted communications using TLS 1.2 or later. Servers will operate in a Virtual Private Cloud (VPC) environment to isolate the election infrastructure from public networks.
  - DDoS protection and advanced firewall settings will be required to protect the system from cyberattacks during peak election periods.

3. Blockchain and Auditing Systems

- **Hardware Platform:**
  Blockchain nodes will operate on distributed servers, either on-premise or using cloud providers such as AWS, Microsoft Azure, or Google Cloud.

- **Operating Systems Supported:**
  - **Linux:** Preferred for running blockchain nodes due to its stability and security.

- **Blockchain Network Configuration:**
  - The blockchain ledger will use a distributed network of nodes to ensure high availability and fault tolerance.
  - Encrypted peer-to-peer communications between nodes will ensure that data integrity is maintained across the network.

- **Auditing Tools:**
  - **Blockchain Explorers:** To allow auditors to verify transactions (votes) and ensure the blockchain has not been tampered with. These tools must support secure querying and validation of vote records.
  - **Log Management Systems:** Centralized logging tools (e.g., ELK Stack or Splunk) to collect and analyze audit trails. These systems will run in secure, isolated environments to prevent unauthorized access.

4. Election Management Consoles (Admin Environment)

- **Hardware Platform:**
  Desktop or laptop computers used by election officials and administrators.
- **Operating Systems Supported:**
  - **Windows 10 or later** (for admin tools)
  - **Linux distributions** (for backend management and development purposes)
- **Required Software Components:**
  - **Secure Web Browsers:** Chrome, Firefox, or Edge (latest versions) for accessing administrative dashboards and monitoring tools.
  - **Management Tools:** Tools such as SSH, VPN clients, and web-based management consoles for system administrators to monitor and manage the election infrastructure securely.
- **Security Considerations:**
  - Two-factor authentication (2FA) and role-based access control (RBAC) for all administrative tools and consoles.
  - Regularly updated antivirus software and security patches.

2.6 Design and Implementation Constraints

The following design and implementation constraints apply to the development of the Online Election System for Sri Lanka. These constraints reflect local legal, regulatory, technical, and infrastructural considerations and will limit the options available to developers. All constraints must be factored into the system's architecture and design.

1. Regulatory and Legal Compliance (Sri Lanka Context)

- **Data Protection Regulations:** The system must comply with **Sri Lanka's Data Protection Act** and any other applicable national privacy and data protection laws. This includes ensuring that voter data is stored securely and handled in a manner that respects privacy rights.
- **Election Laws:** The system must adhere to the **Election Commission of Sri Lanka's** rules and guidelines. This includes regulations concerning voter registration, vote counting, and audits. The system's design must allow for legal challenges, recounts, or election disputes as per local election laws.
- **Accessibility Requirements:** The system must meet accessibility requirements that cater to the needs of all Sri Lankan citizens, including those with disabilities. Compliance with local guidelines on accessibility must be ensured.

2. Security Considerations (Sri Lanka Context)

- **Encryption Standards:** All communications between voter devices and servers must be encrypted using AES-256 encryption or higher. **Sri Lanka CERT|CC** recommendations on encryption and cybersecurity standards should be followed.
- **National ID Integration:** Sri Lanka uses the **National Identity Card (NIC)** system for voter identification. The system must securely integrate with this database for voter authentication, ensuring that only eligible voters are allowed to cast their votes.
- **Tamper Resistance:** Blockchain technology will be used to store votes immutably. Sri Lanka's Election Commission and cybersecurity bodies must approve all security measures.

3. Hardware Limitations (Sri Lanka Context)

- **Mobile Device Compatibility:** The system must support a wide variety of mobile devices prevalent in Sri Lanka, including lower-end smartphones that may have limited processing power and storage. The system must run smoothly on devices with older versions of Android and iOS, as many voters may not have access to the latest technology.
- **Election Server Infrastructure:** The election servers must be located in secure data centers within Sri Lanka to comply with data sovereignty requirements. Servers must be capable of scaling to handle large volumes of simultaneous connections during peak voting periods.

4. Integration with Sri Lanka's National Systems

- **NIC Verification:** The system must integrate with the **Department for Registration of Persons (DRP)** database to verify voter identities via NIC numbers. Secure APIs provided by the DRP must be utilized, and all data transfers must be encrypted and comply with DRP protocols.
- **Telecommunications Integration:** Given that Sri Lanka has a well-developed telecommunications network, the system will integrate with local mobile carriers (e.g., Dialog, Mobitel, SLT) to send two-factor authentication (2FA) codes via SMS. These providers must follow national telecommunications regulations when handling voter data.

5. Communication Protocols (Sri Lanka Context)

- **Network Communication:** All data exchanged between the election system components must be encrypted using **TLS 1.2 or later** to ensure secure communication channels. Servers hosting the election system must be equipped with firewalls and DDoS protection, in line with guidelines from **Sri Lanka CERT|CC**.

- **Latency Considerations:** Internet connectivity in some rural areas of Sri Lanka may experience latency issues. The system must be designed to handle intermittent connections and ensure that votes are transmitted reliably, even in low-bandwidth scenarios.

6. Performance and Scalability (Sri Lanka Context)

- **Scalability Requirements:** The system must handle a large number of voters concurrently, particularly during peak voting hours. The system should be designed with the ability to scale horizontally, utilizing either local data centers or cloud infrastructure.
- **Blockchain Performance:** The blockchain ledger used for vote storage must be capable of processing transactions quickly enough to avoid delays in vote recording. High-speed consensus algorithms that balance security and performance are critical.

7. Programming and Development Standards (Sri Lanka Context)

- **Development Languages:** The system will primarily be developed using industry-standard programming languages such as **Java, Python, or Node.js** for the server side, with **Swift and Kotlin** used for mobile app development. The programming languages must support secure coding practices.
- **Coding Standards:** All code must adhere to the secure coding guidelines provided by **Sri Lanka CERT|CC**. Regular code reviews and security audits must be conducted to ensure the system meets local and international cybersecurity standards.
- **Version Control: Git** will be used for version control, ensuring that all changes to the code are tracked and auditable. This allows for rollback and security patching if necessary.

8. Data Storage and Privacy (Sri Lanka Context)

- **Data Sovereignty:** Voter data must be stored within Sri Lanka to comply with the country's data sovereignty laws. Data storage must occur on servers hosted in secure facilities within Sri Lanka.
- **Anonymity Constraints:** The system must ensure voter anonymity as required by Sri Lanka's election laws. Voter identity and votes must be separated to prevent any potential linking of votes to specific individuals.

9. Auditability (Sri Lanka Context)

- **Audit Trails:** The system must generate immutable logs for key processes such as voter authentication, vote casting, and vote counting. These logs will be available to the **Sri Lankan Election Commission** for audit and review.

- **Third-Party Audits:** The system must support independent audits conducted by authorized entities such as **Sri Lanka's Election Commission** or external auditors. These audits must verify the accuracy and integrity of the system without compromising voter anonymity.

10. User Experience Constraints (Sri Lanka Context)

- **Multilingual Support:** The system must support multiple languages used in Sri Lanka, including **Sinhala, Tamil, and English**, to ensure accessibility for all voters. All user interfaces, notifications, and instructions must be translated accurately.
- **Low Bandwidth Functionality:** Given that internet connectivity may vary across Sri Lanka, the system must be optimized for low bandwidth usage. The mobile app must support offline vote storage, with votes securely submitted when the device reconnects to the internet.

2.7 User Documentation

The following documents will be provided with the Online Election System to ensure the users will get a thorough understanding and smooth operation for all user classes.

1. **User Manuals**
   a. Voter Manual: includes step-by-step voter registration, authentication, and vote-casting instructions. It also covers troubleshooting for common issues such as OTP failures or login problems.
   b. Election Official Manual: Guides officials on managing voter records, monitoring elections, and generating results.
   c. Administrator Manual: Detailed instructions for system administrators on setting up, maintaining, and securing the system.

2. **Online Help**
   - Integrated help is available within the system to assist users with specific tasks. This can be accessed through a dedicated "Help" button.

3. **Quick Reference Guides**
   - This includes short guides, highlighting critical tasks for each user class. (e.g., voters, officials, administrators)

4. **Training Videos**
   - Video tutorials demonstrating key functionalities, such as the registration process, vote casting, and post-election auditing.

All documents will be provided in Sinhala, Tamil, and English to cater for all users in Sri Lanka. Documentations will provided as PDFs, HTML links, and videos in MP4.

2.8 Assumptions and Dependencies

The Online Election System relies on several assumptions and dependencies for successful implementation.

1. **National Identity Database Access**
    - This system assumes reliable access to Sri Lanka's National Identity Database for voter verification. Any downtime in the servers could disrupt voter registration and authentication.

2. **Telecommunication Services**
    - OTP-based means working with local telecom providers for successful implementation. This system seems to have the potential for interruptions that can be occasioned by service interruptions and/or regulatory changes.

3. **Regulatory Compliance**
    - The system development is dependent on the existing local election laws and data protection legal requirements. Any of these may lead to changes in the system.

4. **Blockchain and Database Platform**
    - Based on third-party solutions such as Hyperledger Fabric and PostgreSQL, the system is designed. Problems in compatibility or update of these platforms may destabilize the system.

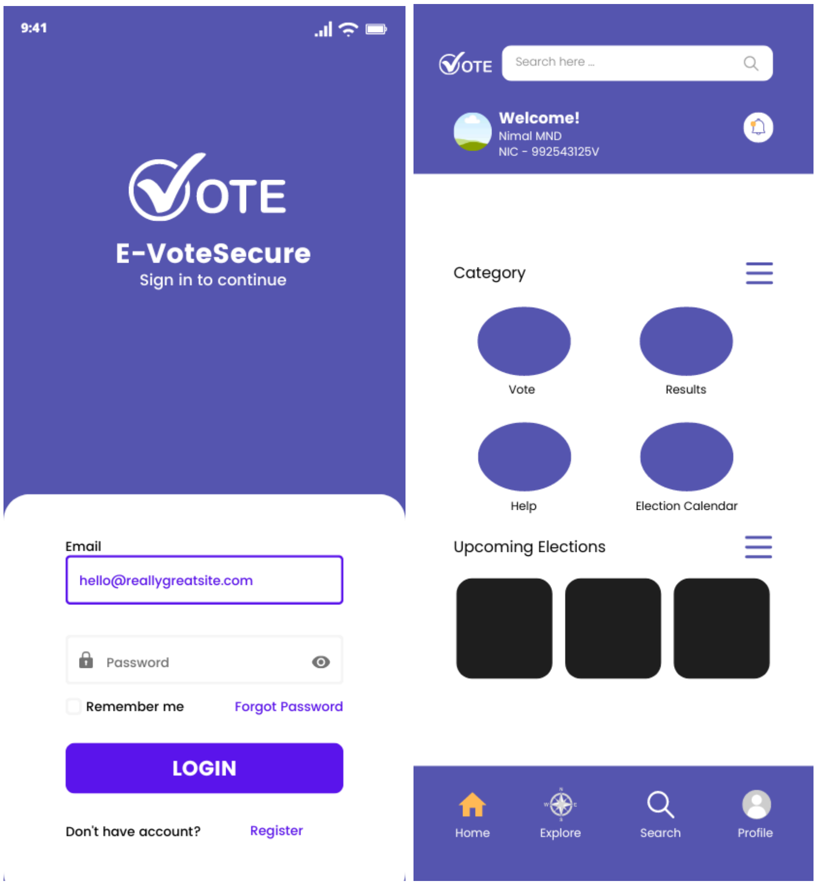
5. **Hardware and Network Infrastructure**
    - Adequate infrastructure is assumed for running servers, maintaining blockchain nodes, and ensuring low-latency communication.

6. **Device Compatibility**
    - The system assumes voter devices have the required specifications.

3. External Interface Requirements

3.1 User Interfaces

1. **Voter Interface:** Portable application that will enable easy login using NIC, casting and confirming votes.



Email: hello@reallygreatsite.com

Welcome!
Nimal MND
NIC - 992543125V

sample voter interfaces

2. **Election Officials Interface:** Election and voter management system that can be accessed through the web browser.

3. **Administrator Interfaces:** Command-line and web-based tools for configuration and management of a computing system.

3.2 Hardware Interfaces

- Voter devices (smartphones/tablets) must have biometric sensors, an internet connection, and correct OS versions.
- Another requirement that has to be met by the election servers is that they must support the blockchain nodes and data storage with greater security.

3.3 Software Interfaces

- Integration with:
  - National Identity Database for Voter Verification
  - SMS gateways for OTP-based authentication
  - Blockchain platform for vote storage

3.4 Communications Interfaces

- Only encrypted data can be transferred over the network via TLS 1.2 and above.
- The normal HTTP/HTTPS convention is used for communicating with the server.
- Exchange formats of data between the components in an encrypted format such as JSON.

4. System Features

The Online Election System is designed to provide a secure and transparent electronic voting process through the implementation of several key features.

4.1 Secure Voter Authentication

4.1.1 Description and Priority

The Secure Voter Authentication feature ensures that only eligible voters can access the voting system and cast their votes. Authentication is done via two-factor authentication (2FA), combining the voter’s NIC (National Identity Card) number with a secondary authentication method (e.g., biometric authentication or a one-time password sent via SMS). This feature is of **High** priority due to its critical role in ensuring election security and voter identity verification.

- **Benefit:** 9 (Prevents voter fraud and ensures only legitimate votes are cast)
- **Penalty:** 8 (Failure to authenticate voters correctly could compromise the entire election)
- **Cost:** 5 (Development and integration with national identity databases and telecommunications)
- **Risk:** 7 (Risk of identity theft, unauthorized access, or system abuse

4.1.2 Stimulus/Response Sequences

- **Stimulus:** The voter opens the mobile app and selects the option to begin the voting process.
  - **Response:** The system prompts the voter to enter their NIC number.

- **Stimulus:** The voter enters their NIC number and confirms.
  - **Response:** The system validates the NIC number against the National Identity Database.

- **Stimulus:** Upon successful validation, the voter is prompted to provide biometric authentication (fingerprint or facial recognition) or enter a one-time password (OTP) sent to their registered mobile phone.
  - **Response:** The system verifies the biometric data or OTP.

- **Stimulus:** Authentication is successful.
  - **Response:** The system grants the voter access to the voting interface.

4.1.3 Functional Requirements

Requirement	Description
REQ-1	The system must verify the voter’s NIC against the National Identity Database to ensure eligibility.
REQ-2	The system must support two-factor authentication, either through biometric authentication or a one-time password (OTP) sent via SMS
REQ-3	The system must lock out a user after three consecutive failed authentication attempts and notify election officials of a potential security issue.
REQ-4	The system must allow for secure re-authentication if a session times out, without revealing previously entered vote selections
REQ-5	In the case of biometric failures or OTP delivery issues, the system must provide voters with a secure fallback option to complete authentication (e.g., manual verification by election officials).

4.2 Vote Casting and Submission

4.2.1 Description and Priority

The Vote Casting and Submission feature allows authenticated voters to select their candidates on an electronic ballot and securely submit their votes to the election server. This feature is of **High** priority because it is the core function of the voting system and directly impacts the election's integrity.

- **Benefit:** 9 (Essential for the execution of the election)
- **Penalty:** 9 (Failure to securely cast and submit votes would invalidate the election results)
- **Cost:** 6 (Implementation of secure vote submission protocols, including encryption)
- **Risk:** 8 (Potential security risks during transmission and storage of votes)

4.2.2 Stimulus/Response Sequences

- **Stimulus:** The voter completes the authentication process and is presented with the appropriate ballot for their election district.
  - **Response:** The system displays the ballot with candidate options.
- **Stimulus:** The voter selects their choices on the ballot and confirms the selection.
  - **Response:** The system prompts the voter to review their selections before final submission.
- **Stimulus:** The voter confirms their selections and chooses to submit the ballot.
  - **Response:** The system encrypts the vote and transmits it to the central election server.
- **Stimulus:** The vote is successfully transmitted.
  - **Response:** The system provides the voter with a confirmation that their vote has been recorded.

4.2.3 Functional Requirements

Requirement	**Description**
REQ-1	The system must present the voter with the correct ballot based on their election district and NIC verification.
REQ-2	The system must allow the voter to review and change their ballot selections before final submission.
REQ-3	The system must encrypt all vote data on the voter’s device before transmitting it to the central election server.
REQ-4	The system must confirm successful vote transmission to the voter and provide an auditable transaction ID without revealing the content of the vote.
REQ-5	In the event of a failed vote submission due to network issues or system errors, the system must allow the voter to retry the submission securely without losing their selections.

4.3 Post-Election Auditing and Verification

4.3.1 Description and Priority

The Post-Election Auditing and Verification feature ensures that votes are counted accurately and that the election process is transparent and accountable. Audits are conducted through blockchain verification and independent audits by third-party organizations. This feature is of **High** priority because it guarantees the integrity of the election results.

- **Benefit:** 9 (Ensures transparency and accuracy of election results)
- **Penalty:** 7 (Failure to conduct proper audits may lead to disputes or lack of trust in the results)
- **Cost:** 5 (Costs associated with implementing blockchain verification and auditing tools)
- **Risk:** 6 (Risk of incomplete audits or verification failureStimulus/Response Sequences

4.3.2 Stimulus/Response Sequences

- **Stimulus:** The election ends, and the system initiates an audit of all votes stored in the blockchain ledger.
  - **Response:** The system begins the verification process, ensuring each vote has been recorded accurately and has not been tampered with.

- **Stimulus:** Independent auditors access the system to verify vote records.
  - **Response:** The system provides auditors with read-only access to the blockchain ledger and vote logs for verification.

- **Stimulus:** The auditors complete their verification process.
  - **Response:** The system generates an audit report and submits it to the election commission for certification.

4.3.3 Functional Requirements

Requirement	Description
REQ-1	The system must generate an immutable audit trail of all voter actions, vote submissions, and system interactions.
REQ-2	The system must use blockchain technology to ensure that all votes are stored securely and cannot be altered post-submission.
REQ-3	The system must allow independent third-party auditors to access vote records without compromising voter anonymity or altering the data.
REQ-4	The system must generate comprehensive audit reports for certification by the election commission, including details on vote counts, discrepancies, and system performance.
REQ-5	In the event of discrepancies or issues found during audits, the system must support recounts or other forms of verification to resolve election disputes.

5. Other Nonfunctional Requirements

5.1 Performance Requirements

The Online Election System must meet the following performance benchmarks to ensure smooth operation under various conditions:

- **Voter Authentication:** The system must complete voter authentication, including NIC validation and 2FA, within 5 seconds under normal network conditions. This includes database checks and biometric or OTP verification.
- **Vote Submission:** The vote casting and encryption process must take no longer than 2 seconds on the voter's device, and vote transmission to the central server must be completed within 3 seconds, provided network conditions are stable.
- **Scalability:** The system must handle up to 1 million simultaneous users without degradation of performance. During peak voting periods, response times for any system function (e.g., authentication, vote submission) should not exceed 5 seconds.
- **Blockchain Transaction Speed:** Blockchain transactions (i.e., recording votes) must be completed within 1 second per transaction to ensure real-time vote counting and auditing.
- **Latency Tolerance:** The system must be able to tolerate up to 500 milliseconds of latency for users in rural or remote areas of Sri Lanka, ensuring that votes are still securely transmitted without significant delays.

5.2 Safety Requirements

The system must ensure that no voter, vote, or administrator can cause harm or loss due to system failures or misuse:

- **Data Loss Prevention:** Redundant systems must be in place to prevent data loss during network outages or system crashes. Votes must be securely cached on the voter's device and re-submitted once connectivity is restored, ensuring no loss of votes during submission.
- **Emergency Shutdown:** In the case of a critical system failure or cybersecurity incident, the system must provide a safe shutdown mechanism that prevents data corruption or loss of vote integrity.
- **Tamper Alerts:** The system must monitor for any tampering attempts (e.g., unauthorized access, corrupted votes) and alert election officials immediately to take action. Such alerts must trigger automated locking of the system until the issue is resolved.
- **Disaster Recovery:** The system must support disaster recovery protocols, including backup systems that can restore voting services within 1 hour in case of significant infrastructure failures (e.g., server crashes, or data center issues).
- **Compliance with Local Safety Standards:** The system must comply with Sri Lanka's safety regulations for digital products, including any requirements from local cybersecurity authorities such as **Sri Lanka CERT|CC**.

5.3 Security Requirements

The system must meet stringent security requirements to ensure voter privacy, vote integrity, and overall election security:

- **End-to-End Encryption:** All data transmissions between the voter's device and the election server must be encrypted using AES-256 encryption to prevent unauthorized access.
- **Two-Factor Authentication (2FA):** Voters and administrators must authenticate using NIC verification and a secondary authentication method (biometric or OTP). The system must enforce strong password policies and secure handling of biometric data.
- **Blockchain Security:** All votes must be stored in an immutable blockchain ledger. The system must prevent unauthorized modifications to the blockchain and support cryptographic integrity checks for all votes.
- **Access Control:** Role-based access control (RBAC) must be implemented to restrict access to different parts of the system. Only authorized election officials should have access to sensitive data and system management tools.
- **Data Protection Compliance:** The system must comply with **Sri Lanka's Data Protection Act**, ensuring that all personal data, including voter identities, is protected in line with local privacy laws.
- **Intrusion Detection:** The system must incorporate real-time intrusion detection systems (IDS) to monitor for unauthorized access or cyberattacks. Any detected intrusions must trigger immediate lockdowns and notification to administrators.

5.4 Software Quality Attributes

- **Availability:** The system must have 99.9% uptime during the election period, with minimal scheduled maintenance. Downtime must not exceed 1 hour during critical periods, and system redundancy must ensure availability even during infrastructure failures.
- **Reliability:** The system must ensure reliable operation even under high user loads, with no more than 0.1% error rates for vote submissions or user authentication.
- **Usability:** The system must be user-friendly for both voters and administrators, with intuitive interfaces and clear instructions in **Sinhala, Tamil, and English**. The voter app must guide users through the process with a minimal learning curve, prioritizing ease of use.
- **Interoperability:** The system must be compatible with external systems such as the National Identity Database and mobile network providers for SMS/OTP functionality. It must also integrate with third-party auditing tools for post-election verification.
- **Maintainability:** The system must be designed for easy maintenance and upgrades. Modular code structure and thorough documentation must enable efficient system updates, including security patches.
- **Testability:** All system components must be designed to facilitate automated testing, including unit tests, integration tests, and performance tests. The system must undergo thorough testing before each election to ensure smooth operation.
- **Scalability:** The system must be scalable both vertically (improving server capacity) and horizontally (adding additional nodes) to accommodate varying voter loads, with a seamless transition to higher capacity during peak voting hours.

5.5 Business Rules

- **Voter Eligibility:** Only voters verified via their NIC in Sri Lanka's National Identity Database are allowed to vote. Each voter can cast only one vote, and voter fraud (e.g., duplicate votes, impersonation) must be prevented at all costs.
- **Role-Based Access:** Only authorized election officials can perform sensitive tasks such as result certification, system management, and audit initiation. Auditors have read-only access to logs and blockchain records, while administrators have full system control.
- **Vote Anonymity:** Once a vote is cast, it must be separated from any identifiable voter information. The system must ensure that no election official or system administrator can link a vote back to the voter who cast it.
- **Audit Transparency:** Election officials and third-party auditors must have access to audit logs and blockchain vote records to verify the election's integrity. Auditors must be able to perform their duties without interfering with the election process.
- **Session Management:** Each voter session is limited to one vote. After a vote is successfully cast and confirmed, the voter session must automatically terminate, and no further voting actions can be taken by that voter.

6. Other Requirements

Appendix A: Glossary

- **NIC**: National Identity Card, a unique identification number assigned to every citizen in Sri Lanka.
- **2FA**: Two-factor authentication, a security process requiring two distinct forms of identification.
- **OTP**: One-Time Password, a temporary password used for single login sessions.
- **Blockchai**n: A decentralized ledger technology used to store vote data securely.
- **TLS**: Transport Layer Security, a cryptographic protocol designed to provide secure communications.
- **AES-256**: Advanced Encryption Standard, a symmetric encryption algorithm used to secure data.
- **WCAG**: Web Content Accessibility Guidelines, a set of standards for ensuring web accessibility.
- **RBAC**: Role-Based Access Control, a system for managing access rights based on users' roles within an organization.
- **Sri Lanka CERT|CC**: Sri Lanka Computer Emergency Readiness Team Coordination Centre, responsible for managing cybersecurity and related initiatives.
- **Secure Boot:** A security procedure that a device can only boot with firmware that has been tested and approved by the manufacturer and to prevent unauthorized modification of firmware or boot loader.
- **Encryption**: The act of converting data into a form, which cannot be accessed by any unauthorized personnel. It retains the privacy of data by converting the written text into enciphered form by programs such as AES-256.
- **VPC**: Virtual Private Cloud which is a private cloud within a public cloud where the customer has control to manage resources over a virtual network.
- **VPN**: A Virtual Private Network is a technology that creates a secure channel over the internet or other insecure network for communication and protects data from cloning.
- **DDoS**: Distributed Denial of Service, a cyber attack whereby many systems send high amounts of traffic to the target network or server as a means to render it unavailable to users.
- **SSH**: SSH, which is the short form of Secure Shell and is a network protocol which facilitates safe access and management of other systems through a network.
- **TLS**: The Transport Layer Security, a protocol created for protecting information that passes over a network by providing safe encryption of messages and their content.

Appendix B: To Be Determined List

The following items are still to be determined and require further clarification:

1. **Telecommunication Provider Requirements**: Additional guidelines and directives given by individual mobile service providers such as Dialog, Mobitel, and SLT for delivering SMSes and handling one-time passwords, during the election period.
2. **Blockchain Consensus Algorithm:** The last procedure in the generation of the blockchain is the choice of the consensus forming mechanism to be employed (such as Proof of Stake, Practical Byzantine Fault Tolerance) that has to be done through the optimal/very good performance and security equation.
3. **Audit Trail Access:** The last call on how third-party auditors can gain access and certify the content of the blockchain while preserving the voters' identity.
4. **Data Center Location:** Decision of where the election infrastructure will reside in the data center(s), within compliance with national laws of data sovereignty.
5. **Mobile Device Compatibility Specifications:** Confirmation of minimum specifications for the mobile device which will operate the voting app for the benefit of rural people who use older devices.
6. **Regulatory Approval for Blockchain Use:** The Sri Lankan Election Commission and specific cybersecurity offices for the innovative application of blockchain for votes and vote tallies Archival.
7. **Election Commission API Access:** Signing off of APIs to query the voter data and specific data on an election

7. Team Members

Index Number	Name
200193U	C.M. Gunasekara
200401J	Muaadh M.N.M
200406E	Muthuthanthrige N.R