Enhancing Democratic Integrity through Secure E-Voting: A Public-Private Partnership Model for Sri Lanka

Unit Code	CSG2344.3
Unit Name	Project Methods and Professionalism
Lecturer	Chandrasiri WEERASEKERA
Group Members	Hesandi DISSANAYAKE (10676483) Methuli JAYAWICKRAMA (10675813) Leshindri AGALAWATTA (10684165) Hirun KANAKKA HEWAGE (10676626) Janith GUNARATHNE (10676638) Yapa JAYASINGHE (10675273)

Table of Contents

1. Introduction

In Sri Lanka, the demand for efficient and trustworthy electronic voting, or "e-voting," has grown over time. Such modernization is necessary for the obvious difficulties that conventional voting presently faces, including how logistics and accessibility at polling stations have become crucial for all citizens, just like in many other countries. The electronic infrastructure for e-voting is mobile phones and online banking services, which are already embedded in more than 90% of Sri Lankans.

Thus, a safe electronic voting system is vital in gaining trust in the democratic process. The public construes that systems must be clear and verifiable, as well as be designed to make sure it cannot be manipulated or made to fail technically, for it to reflect the real outcome of the election. The challenge therefore is to have such a system which promises not only fairness and accuracy of votes but, above all, convinces people that their votes are secure.

Sri Lanka's public and commercial banks have proved their worth as reliable suppliers of genuine digital services through online banking services. Therefore, the e-voting system would have existing banking authentication technologies incorporated by the government as it collaborates with these banks. Such collaboration would ensure that top standards of election security and transparency are upheld, while facilitating a smooth, safe and easy-to-use e-voting system for Sri Lankan citizens.

2. Literature Review

2.1 Global Experiences with E-Voting

Numerous nations have experimented with and used electronic voting methods, with varying degrees of success (Smith, 2009). Being the first nation to introduce nationwide online voting in 2005, Estonia is a prime example (Masterson, 2024).

According to Smith (2009), the Estonian system is highly praised for its transparent election procedures, safe authentication methods utilizing national ID cards, and user-friendly interface.

E-voting for foreigners has been used in other nations, such Switzerland, indicating its potential to improve accessibility (Smith, 2009).

However, nations such as the United States and the Netherlands have been criticized for their lack of transparency and voting machines' susceptibility to manipulation, which has led to the discontinuation of electronic voting in some areas (Loeber, n.d.).

These incidents highlight how crucial it is to balance security, transparency, and accessibility when creating electronic voting systems.

2.2 Challenges of E-Voting Systems

Security, trust, and scalability are the main issues that e-voting systems must deal with (Schweitzer, 2019).

Because e-voting systems are susceptible to malware, hacking, and denial-of-service (DoS) assaults, cyber security is one of the biggest worries (Schweitzer, 2019).

Furthermore, there is a moral and technical dilemma in preserving voter anonymity while guaranteeing vote reliability (Dill, n.d.).

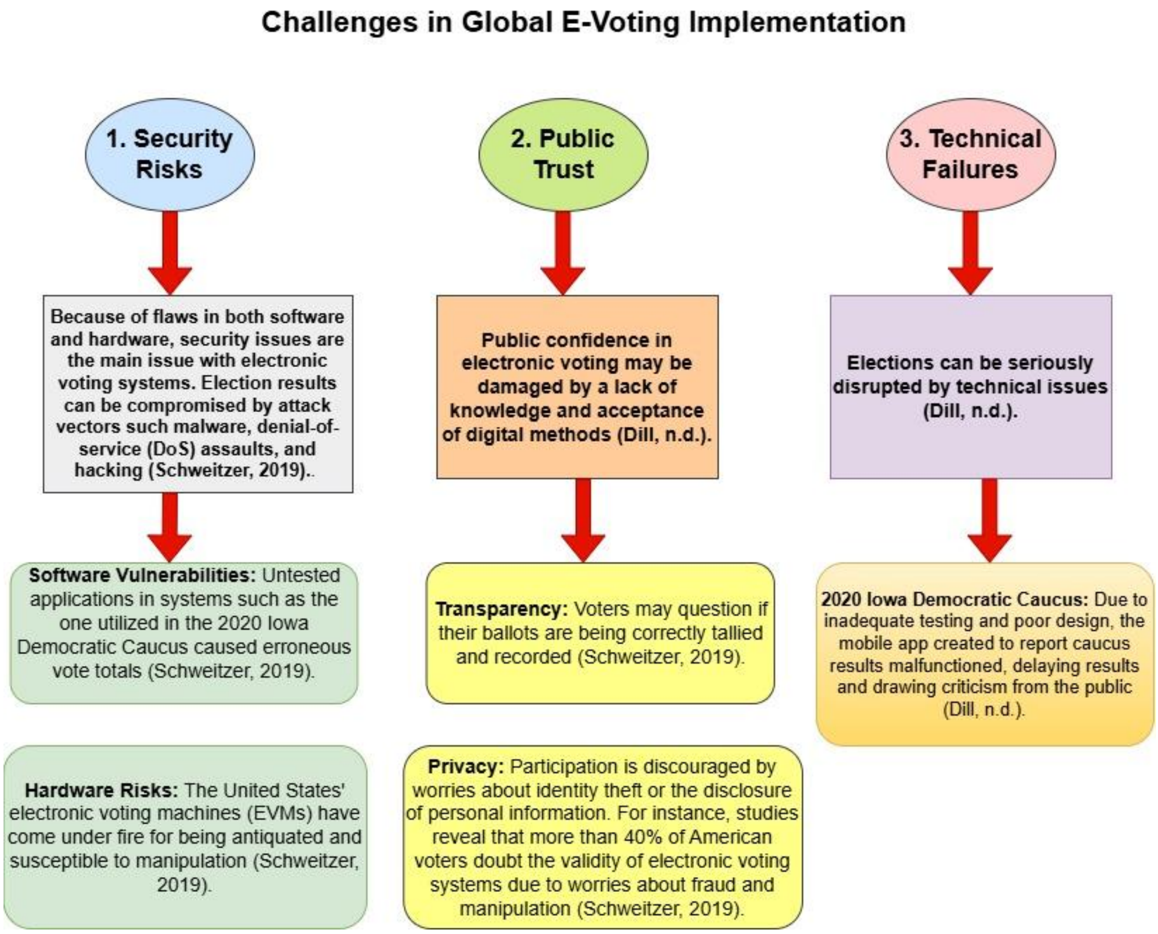
Lack of knowledge and transparency on safe recording and counting of votes might undermine confidence in electronic voting systems (Schweitzer, 2019).

Furthermore, the digital gap is still a significant problem, especially in areas where access to the internet and digital literacy are not equally distributed (Dill, n.d.).

To achieve successful implementation, these issues call for thorough testing, strong system design, and public education.

Figure 1.

Challenges in Global E-Voting Implementation



Because of flaws in both software and hardware, security issues are the main issue with electronic voting systems. Election results can be compromised by attack vectors such malware, denial-of-service (DoS) assaults, and hacking (Schweitzer, 2019)..

Software Vulnerabilities: Untested applications in systems such as the one utilized in the 2020 Iowa Democratic Caucus caused erroneous vote totals (Schweitzer, 2019).

Hardware Risks: The United States' electronic voting machines (EVMs) have come under fire for being antiquated and susceptible to manipulation (Schweitzer, 2019).

Public confidence in electronic voting may be damaged by a lack of knowledge and acceptance of digital methods (Dill, n.d.).

Transparency: Voters may question if their ballots are being correctly tallied and recorded (Schweitzer, 2019).

Privacy: Participation is discouraged by worries about identity theft or the disclosure of personal information. For instance, studies reveal that more than 40% of American voters doubt the validity of electronic voting systems due to worries about fraud and manipulation (Schweitzer, 2019).

Elections can be seriously disrupted by technical issues (Dill, n.d.).

2020 Iowa Democratic Caucus: Due to inadequate testing and poor design, the mobile app created to report caucus results malfunctioned, delaying results and drawing criticism from the public (Dill, n.d.).

Note. The above diagram depicts the main challenges of the global E-Voting Implementation.

(Diagram self- constructed)

2.3 Lessons from Previous Attempts

Important lessons can be learned from earlier attempts to install electronic voting systems.

Concerns about vote tampering and insufficient auditing procedures led the Netherlands to abandon electronic voting, emphasizing the necessity of reliable audit trails (Loeber, n.d.).

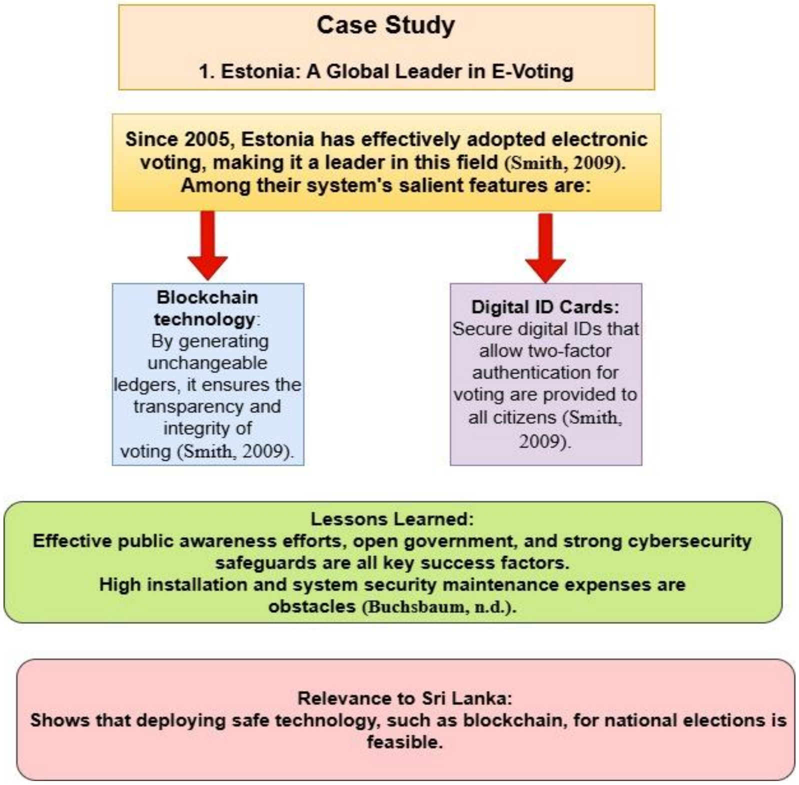
Even in environments with limited resources, India's experience with electronic voting machines (EVMs) highlights the value of simplicity in design to guarantee dependability and use (Smith, 2009).

Stakeholder confidence in the system is crucial, as evidenced by Norway's decision to end its e-voting experiments due to security and public trust problems (“E-Voting Experiments End in Norway amid Security Fears,” 2014).

According to these principles, e-voting systems need to put security, openness, and inclusivity first while building public confidence by thorough testing, transparent communication, and continuous development.

Figure 2.

Case study of a successful E-Voting Implementation



Case Study

1. Estonia: A Global Leader in E-Voting

Since 2005, Estonia has effectively adopted electronic voting, making it a leader in this field (Smith, 2009). Among their system's salient features are:

Blockchain technology: By generating unchangeable ledgers, it ensures the transparency and integrity of voting (Smith, 2009).

Digital ID Cards: Secure digital IDs that allow two-factor authentication for voting are provided to all citizens (Smith, 2009).

Lessons Learned:
Effective public awareness efforts, open government, and strong cybersecurity safeguards are all key success factors.
High installation and system security maintenance expenses are obstacles (Buchsbaum, n.d.).

Relevance to Sri Lanka:
Shows that deploying safe technology, such as blockchain, for national elections is feasible.

Note. The above diagram depicts a case study of successful E-Voting implementation of Estonia and the lessons that can be learned from it.

(Diagram self- constructed)

3. Scope of work

The above system aims to allow Sri Lankan citizens to cast their votes away through a mobile banking application and ensure secure, reliable, and accessible e- voting. It should also take care of ensuring voter authenticity, integrity of data, and compliance.

The six months project (Jan-June 2025) will involve planning, system design, development, testing, training, public awareness and deployment in order to meet the stringent deadline for the Federal election which is the key milestone of this project, ensuring timely progress and readiness for the election in August 2025.

Key tasks involved are voter authentication using multi-factor authentication, encryption and audit trails where voting will be done with own devices or at bank branches registered in the e-voting system.

This project will deliver detailed proposal, system deployment, and public education to ensure broad adoption, trust and successful completion of the e-voting process. Key deliverables, Inclusions and Exclusions for the E-voting project are listed down below.

Overall, this project portrays an innovative approach to enhance the democratic system in Sri Lanka by introducing a secure and accessible e-voting system for parliamentary elections.

3.1 Key Deliverables

1. **System Architecture and Documentation**

Creating a comprehensive design documentation including system components, security features and audit capabilities.

2. **Operational E-Voting System**

Fully operational and secure e-voting system integrated with participation banks’ applications.

3. **Public-Private Partnership Agreements**

Finalizing the agreements between the Election Commission and the participating banks including the respective roles and responsibilities as well as the compensation.

4. **Pilot Testing Report**

Results from pilot testing, such as reliability checks and troubleshooting, have been published.

5. **Voter Outreach Plan**

A comprehensive plan for nationwide voter education and engagement campaigns.

6. **Training Manuals and Workshops**

Training materials and workshops for bank staff to ensure efficient voter assistance during the election.

7. System Rollout Plan

Step-by-step plan for the e-voting system.

8. Risk management and Contingency Plan

Addressing potential risks like malfunctions in the system, cybersecurity issues, and access to voters.

9. Final Project Report

A report summarizing the challenges, project's development, outcomes and recommendations for future elections.

***Table 1**. Inclusions and exclusions.*

Inclusions	Exclusions
Development of E-Voting System	International Bank Involvement
Integration with Banking Infrastructure	Provision of Devices
Verifications and Authentication	Standalone Voting Applications
Security Measures	Polling Booths or Non-Bank Voting Locations
Public Awareness Campaign	Independent Authentication Services
Voting Facilities at Bank Branches	Election Day Logistics Beyond Banks
Stakeholder Coordination	
Compliance and Legal Adherence	
Pilot Testing and Training	
Budget Allocation	

4. Proposed Trusted Electronic Solution

4.1 Integration with Banking Apps

Leveraging Trusted Platforms

The foundation of the electronic voting system is the incorporation of the platform into the current mobile banking applications of six reputable Sri Lankan banks: three state banks (Bank of Ceylon, People's Bank, and National Savings Bank) and three private banks (Commercial Bank of Ceylon, HNB, and Sampath Bank). Because of their extensive use and track record of managing sensitive financial data with dependability, these banks have gained the trust of the public. Their applications offer the ideal platform for safe electronic voting (Nayanajith, D. A. G. 2021).

Seamless User Experience

A dedicated e-voting module will be integrated into each bank's app, ensuring a consistent and intuitive interface for all users. This module will guide users through the voting process, from authentication to vote confirmation, with clear instructions in Sinhala, Tamil, and English. The simplicity of the design aims to minimize barriers to entry, especially for first-time users (Hosman, L. 2008).

Enhanced Accessibility

- **BYOD Approach-** Voters with personal devices can access the system from anywhere, promoting convenience and reducing logistical overheads.
- **Branch Based Voting-** Citizens without devices or internet access can cast their vote at designated bank branches equipped with secure e-voting terminals (Hettiarachchi, N., & Lakmal, H. 2023).

Cost-Effective Infrastructure

The solution lowers development and operating expenses while upholding high security and reliability standards by leveraging the institutions' current infrastructure. In addition to saving a substantial amount of public money, this approach guarantees quick implementation within the allotted six months.

4.2 Authentication and Verification Methods

Two-Factor Authentication (2FA)

Two-Factor Authentication (2FA) is the foundation for safe access to the electronic voting system. It combines two distinct forms of verification to confirm a voter's identity:

- **Step 1: Primary Identification**
  The voter provides their **National Identity Card (NIC)** or **Voter ID number**, which is cross referenced with the **Election Commission's voter database** in real-time. This ensures that only eligible voters are granted access.

- **Step 2: Secondary Verification**
  following preliminary verification, a **One-Time Password (OTP)** is sent to the voter's registered mobile number or email. This OTP is unique to the session and expires after a short duration, making it nearly impossible for unauthorized parties to gain access (Gichubi, P. M., Maake, B., & Chweya, R. 2024**).**

Biometric Verification

Biometric authentication adds an advanced layer of security, ensuring that votes are cast only by the rightful individual.

- **Mobile Device Authentication**
  Voters using smartphones equipped with biometric capabilities (e.g., fingerprint scanners or facial recognition) will be subject to a verification process before to being able to use the voting platform. This process leverages the device's built-in security features, minimizing the risk of spoofing.

- **Branch-Based Biometric Verification**
  For voters who choose to cast their vote at a bank branch, biometric devices compliant with **Election Commission standards** will be used. Fingerprint scanners and iris recognition systems will confirm the voter's identity on site.

Block chain-Enabled Audit Trails

Block chain technology ensures that every vote is recorded in an unchangeable and transparent manner.

- **Voter Verification Process**
  after casting their vote, the voter receives a cryptographic receipt that confirms their vote has been registered. This receipt cannot be reverse-engineered to reveal the vote's content, ensuring anonymity while maintaining verifiability (Daramola, O., & Thebus, D. 2020, May).

- **Real-Time Integration**
  Block chain nodes are hosted by banks and the Election Commission, ensuring distributed trust and eliminating single points of failure.

4.3 Security Measures

Security is the foundation of any trusted e-voting system. The proposed solution incorporates state of the art security measures to protect against cyber-attacks, fraud, and system failures.

1. Data Encryption

- **End-to-End Encryption (E2EE)**
  All communications between the voter's device and the system servers are encrypted using **Advanced Encryption Standard (AES-256)** (Bai, W., Pearson, M., Kelley, P. G., & Mazurek, M. L. 2020, September).

- **Encrypted Storage**
  Votes stored on the block chain and backend servers are encrypted to prevent unauthorized access.

2. Architecture of Decentralized Systems

A decentralized architecture ensures high availability and system resilience:

- **Distributed Nodes**

  Voting data is stored across nodes managed by participating banks and the Election Commission.

- **Fault Tolerance**
  The system is designed to continue functioning even if one or more nodes fail. (Van Eijk, N., Fahy, R., Van Til, H., Nooren, P., Stokking, H., & Gelevert, H. 2015).

3. Fraud Detection and Prevention

Duplicate Vote Detection

The system tracks and deactivates voter credentials immediately after a vote is cast, preventing duplicate voting.

Anomaly Detection Algorithms

Advanced machine learning models monitor system activity in real time, flagging irregular behaviors such as:

- Multiple login attempts from the same IP address.
- Sudden surges in voting activity from specific locations.

4. Regular Security Audits and Penetration Testing

- **Pre-Deployment Testing-**Independent cyber security firms will conduct penetration tests to identify and rectify vulnerabilities.
- **Post-Deployment Monitoring-**A Security Operations Center **(SOC)** will provide 24/7 monitoring during the election period, ensuring swift responses to threats.

5. Disaster Recovery and Business Continuity

To ensure that the system remains operational under adverse conditions:

- **Real-Time Backups**
  Voting data is continuously backed up to secure cloud servers.
- **Failover Systems**
  Redundant systems are in place to restore functionality within minutes in case of server or network disruptions.

6. Voter Privacy and Anonymity

The system adheres to strict privacy protocols:

- No personally identifiable information (PII) is linked to individual votes.
- Cryptographic methods ensure that voters can verify their participation without exposing vote details.

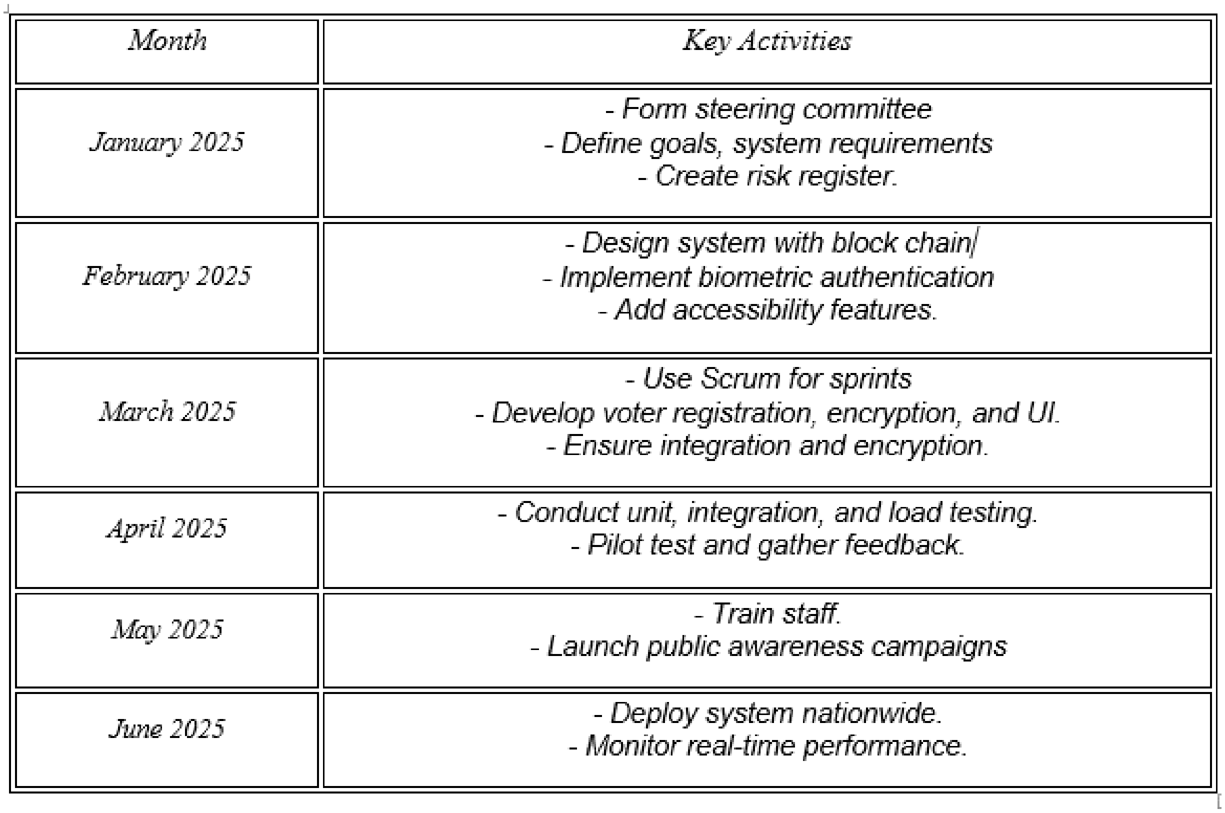
5. Project Management Approach

The proposed e-voting project for Sri Lanka marks a transformative step toward modernizing elections using digital technology. By integrating voting capabilities into existing banking apps, the initiative aims to make the process more secure, inclusive, and efficient. Achieving these goals will require meticulous planning, compliance with regulations, and strong collaboration among key stakeholders.

5.1. Timeline and Milestones

The project will span six months, from January to June 2025, targeting readiness for the national elections in August 2025. The timeline is structured around critical milestones to ensure systematic progress.

Table 2. *Timeline of the project.*



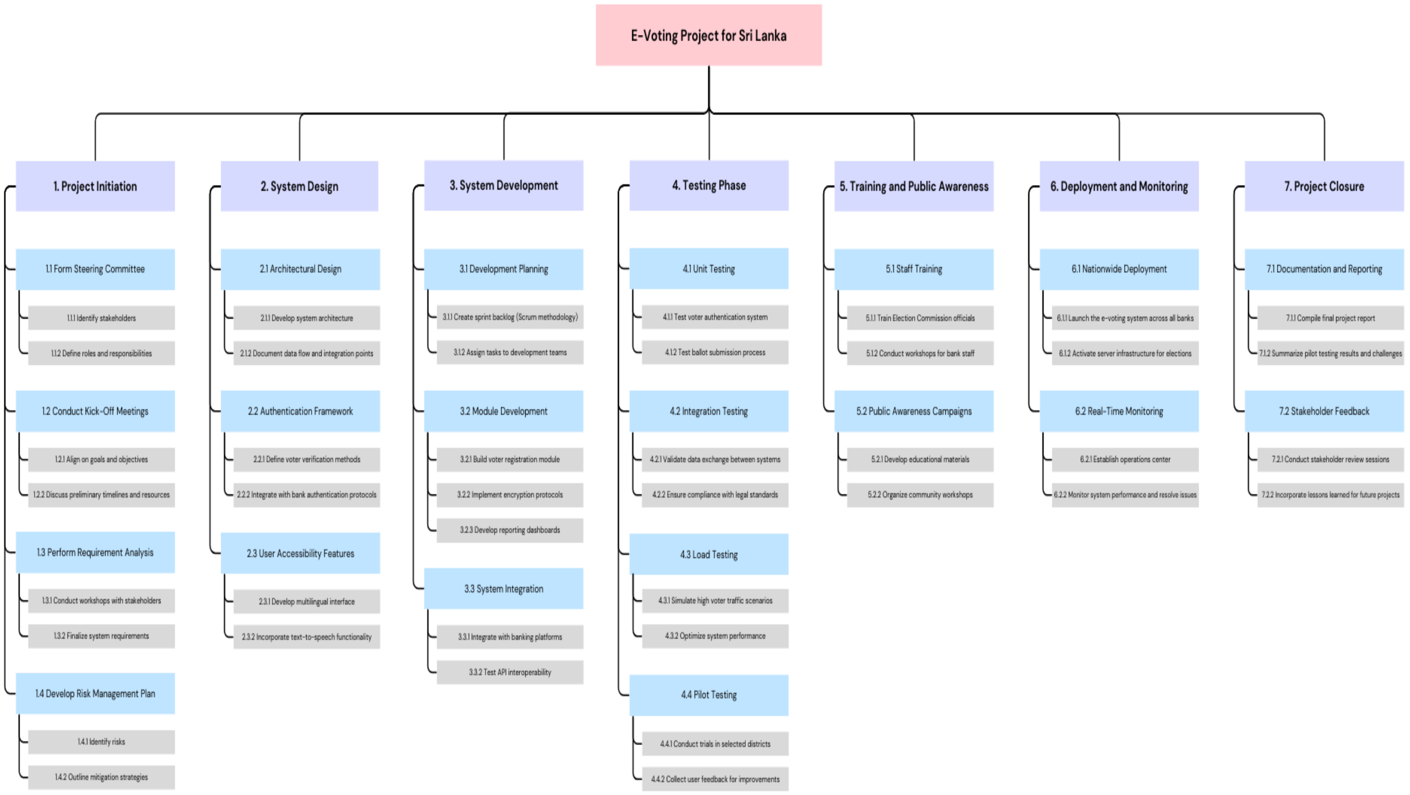
Month	*Key Activities*
January 2025	*- Form steering committee* *- Define goals, system requirements* *- Create risk register.*
February 2025	*- Design system with block chain* *- Implement biometric authentication* *- Add accessibility features.*
March 2025	*- Use Scrum for sprints* *- Develop voter registration, encryption, and UI.* *- Ensure integration and encryption.*
April 2025	*- Conduct unit, integration, and load testing.* *- Pilot test and gather feedback.*
May 2025	*- Train staff.* *- Launch public awareness campaigns*
June 2025	*- Deploy system nationwide.* *- Monitor real-time performance.*

5.2. Methodology

The Scrum framework has been chosen for its flexibility and iterative approach, which are crucial for a dynamic project like e-voting. Scrum enables continuous feedback and quick adaptation to changing requirements, ensuring the system meets user needs and regulatory standards.

Figure 3.

Work Breakdown Structure for the E-Voting Project


E-Voting Project for Sri Lanka
1. Project Initiation
1.1 Form Steering Committee
1.1.1 Identify stakeholders
1.1.2 Define roles and responsibilities
1.2 Conduct Kick-Off Meetings
1.2.1 Align on goals and objectives
1.2.2 Discuss preliminary timelines and resources
1.3 Perform Requirement Analysis
1.3.1 Conduct workshops with stakeholders
1.3.2 Finalize system requirements
1.4 Develop Risk Management Plan
1.4.1 Identify risks
1.4.2 Outline mitigation strategies
2. System Design
2.1 Architectural Design
2.1.1 Develop system architecture
2.1.2 Document data flow and integration points
2.2 Authentication Framework
2.2.1 Define voter verification methods
2.2.2 Integrate with bank authentication protocols
2.3 User Accessibility Features
2.3.1 Develop multilingual interface
2.3.2 Incorporate text-to-speech functionality
3. System Development
3.1 Development Planning
3.1.1 Create sprint backlog (Scrum methodology)
3.1.2 Assign tasks to development teams
3.2 Module Development
3.2.1 Build voter registration module
3.2.2 Implement encryption protocols
3.2.3 Develop reporting dashboards
3.3 System Integration
3.3.1 Integrate with banking platforms
3.3.2 Test API interoperability
4. Testing Phase
4.1 Unit Testing
4.1.1 Test voter authentication system
4.1.2 Test ballot submission process
4.2 Integration Testing
4.2.1 Validate data exchange between systems
4.2.2 Ensure compliance with legal standards
4.3 Load Testing
4.3.1 Simulate high voter traffic scenarios
4.3.2 Optimize system performance
4.4 Pilot Testing
4.4.1 Conduct trials in selected districts
4.4.2 Collect user feedback for improvements
5. Training and Public Awareness
5.1 Staff Training
5.1.1 Train Election Commission officials
5.1.2 Conduct workshops for bank staff
5.2 Public Awareness Campaigns
5.2.1 Develop educational materials
5.2.2 Organize community workshops
6. Deployment and Monitoring
6.1 Nationwide Deployment
6.1.1 Launch the e-voting system across all banks
6.1.2 Activate server infrastructure for elections
6.2 Real-Time Monitoring
6.2.1 Establish operations center
6.2.2 Monitor system performance and resolve issues
7. Project Closure
7.1 Documentation and Reporting
7.1.1 Compile final project report
7.1.2 Summarize pilot testing results and challenges
7.2 Stakeholder Feedback
7.2.1 Conduct stakeholder review sessions
7.2.2 Incorporate lessons learned for future projects

Note. The Work Breakdown Structure of the E-Voting Project. (Diagram self- constructed)

Sprint Planning- The project will be broken down into small, manageable sprints, each focusing on specific deliverables like voter authentication, encryption protocols, or reporting dashboards.

Daily Stand-ups- Teams will hold brief daily meetings to track progress, address challenges, and ensure alignment.

Stakeholder Engagement- Sprint reviews and retrospectives will provide opportunities for stakeholders, including banks, the Election Commission, and technical teams, to offer feedback and adjust plans.

Incremental Deliverables- Each sprint will produce a functional component of the system, allowing for continuous validation and improvement throughout the project.

Risk Management- Scrum's iterative approach ensures early identification and resolution of potential issues, minimizing delays or disruptions.

5.3. Stakeholder Roles and Responsibilities

The project's success depends on clear roles and effective collaboration among all stakeholders:

Banks

- Integrate e-voting features into their apps, ensuring security and user-friendliness.
- Promote the system through marketing campaigns to encourage voter participation.
- Safeguard voter data with advanced cyber security measures (Alwi et al., 2019).

Election Commission

- Ensure legal compliance and monitor the system's performance during the elections (Commonwealth Secretariat, 2020).
- Provide real-time oversight and transparent reporting on election outcomes.

Technical Experts

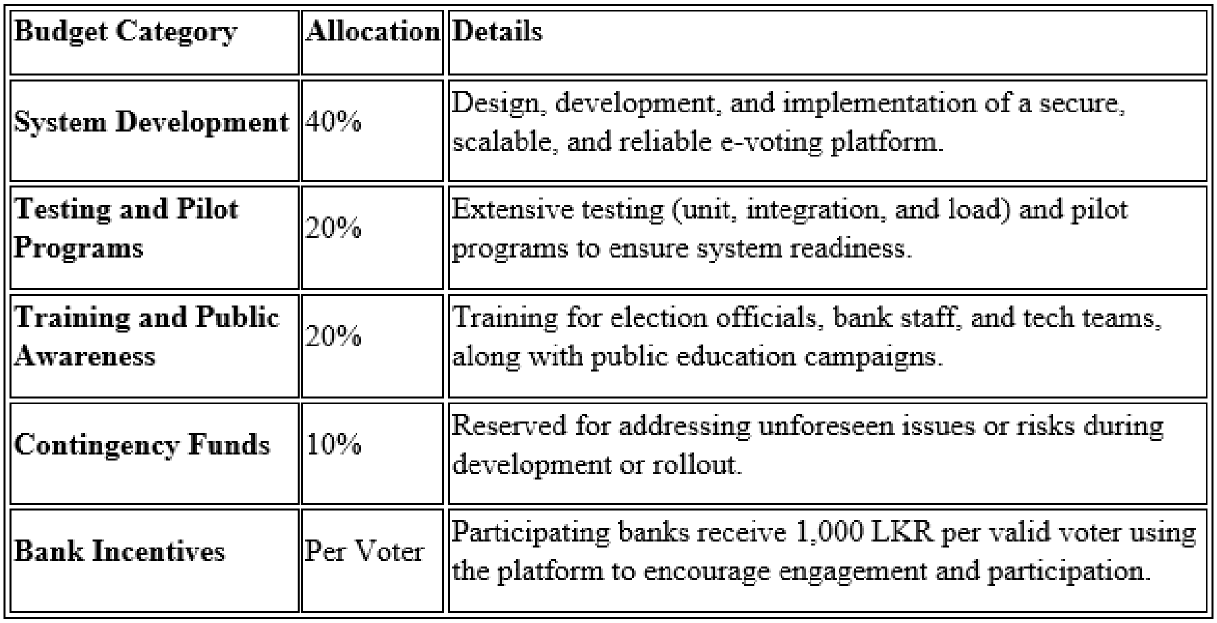
- Design, develop, and maintain the system using cutting-edge technologies like block chain and biometric authentication.
- Conduct regular tests to identify vulnerabilities and enhance security.

5.4. Budgetary Considerations

The overall budget for the project is set at 33 billion LKR, carefully distributed across key areas to ensure the project's goals are met effectively and efficiently.

Cost Breakdown:

***Table** 3. Budget considerations of the project.*



Budget Category	Allocation	Details
System Development	40%	Design, development, and implementation of a secure, scalable, and reliable e-voting platform.
Testing and Pilot Programs	20%	Extensive testing (unit, integration, and load) and pilot programs to ensure system readiness.
Training and Public Awareness	20%	Training for election officials, bank staff, and tech teams, along with public education campaigns.
Contingency Funds	10%	Reserved for addressing unforeseen issues or risks during development or rollout.
Bank Incentives	Per Voter	Participating banks receive 1,000 LKR per valid voter using the platform to encourage engagement and participation.

6. Analysis of Past Lessons Learned

6.1 Failures in Prior E-Voting Systems

1. Security breaches

- Many e-voting systems have been vulnerable to hacking, phishing and malware attacks.
- For recent example, last year Ecuadoreans faced difficulties in their national elections due to cyber-attack and many were unable to access the voting system before polls closed (Amrita, 2023)

2. Authentication Issues

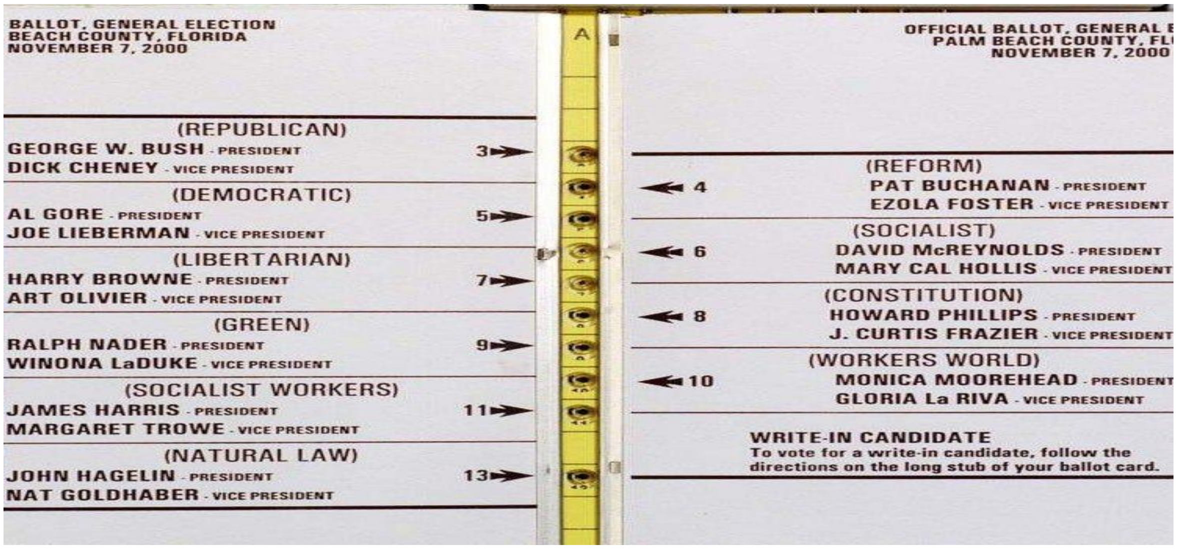
- Non-standardized authentication methods led to unauthorized voting or multiple votes from the same person.
- In Estonian i-Voting System found weaknesses in their system's authentication. Estonian government use to authorized citizens by their national Ids with one cryptographic key but they identified malicious actors exploit credentials and cast multiple votes (Ehin et al., 2022).

3. **Scalability & Reliability Problems**

- There happened several delays or crashes because the system was unable to handle large amounts of voters.
- Real world scenario in 2019 Australia NSW State elections voting system went down leaving approximately 30,000 voters unable to cast their votes because the lack of capacity in their system(Stilgherrian, 2021).

4. **User Accessibility**

- Voting became difficult or impossible for less tech-educated people due to poor user interface design.
- 2000 presidential election at the US in Florida the “butterfly ballot” was poorly designed and it causing voter confusion and misvotes(Mestel, 2020).



BALLOT, GENERAL ELECTION
BEACH COUNTY, FLORIDA
NOVEMBER 7, 2000

(REPUBLICAN)
GEORGE W. BUSH - PRESIDENT
DICK CHENEY - VICE PRESIDENT 3 →

(DEMOCRATIC)
AL GORE - PRESIDENT
JOE LIEBERMAN - VICE PRESIDENT 5 →

(LIBERTARIAN)
HARRY BROWNE - PRESIDENT
ART OLIVIER - VICE PRESIDENT 7 →

(GREEN)
RALPH NADER - PRESIDENT
WINONA LaDUKE - VICE PRESIDENT 9 →

(SOCIALIST WORKERS)
JAMES HARRIS - PRESIDENT
MARGARET TROWE - VICE PRESIDENT 11 →

(NATURAL LAW)
JOHN HAGELIN - PRESIDENT
NAT GOLDHABER - VICE PRESIDENT 13 →

A

OFFICIAL BALLOT, GENERAL E
PALM BEACH COUNTY, FL
NOVEMBER 7, 2000

← 4 (REFORM)
PAT BUCHANAN - PRESIDENT
EZOLA FOSTER - VICE PRESIDENT

← 6 (SOCIALIST)
DAVID McREYNOLDS - PRESIDENT
MARY CAL HOLLIS - VICE PRESIDENT

← 8 (CONSTITUTION)
HOWARD PHILLIPS - PRESIDENT
J. CURTIS FRAZIER - VICE PRESIDENT

← 10 (WORKERS WORLD)
MONICA MOOREHEAD - PRESIDENT
GLORIA La RIVA - VICE PRESIDENT

WRITE-IN CANDIDATE
To vote for a write-in candidate, follow the directions on the long stub of your ballot card.

Figure 4: Note. Communications, D. B. (2012, November 26). *Palm Beach ballot | David Berman Communications*. https://davidberman.com/consistent-clear-ballot-design-makes-for-better-democracy/ballot/

5. **Weak encryption protocols**

- The electoral process's integrity was jeopardized because of inadequate encryption using during data transfer.
- In 2021 during South Africa's 2018 municipal elections concerns which relied on weak encryption during the transmission of votes. The system was not as secure as intended, and there were reports of tampering and vote manipulation, (Limukani, 2022).

6.2 Risk Mitigation Strategies

1. **Avoid From Security Breaches**

- Regular Security Audits - To find possible vulnerabilities, carry out in-depth penetration tests and evaluations of vulnerabilities.
- Multi-Layer Security - Avoiding cyber-attacks, put intrusion detection systems (IDS), firewalls, and sophisticated anti-malware software into e-voting system.
- Incident Response Plan – Address any security incidents quickly, create and update a thorough plan on a regular basis.

2. **Strong Authentication Techniques**

- Two-Factor Authentication (2FA) - Cryptographic keys and secondary layer of authentication is needed, to avoid multiple votes by using biometrics or one-time passwords.
- Dynamic Credentials - Reduce the misuse or unwanted access, utilize time-sensitive cryptographic credentials.

3. **More Scalability, Reliability & Accessibility**

- Load Testing – load testing is assess the system's ability to manage high traffic capacity during elections.
- Cloud-Based Infrastructure - To adapt to the growing voter traffic, using scalable cloud solutions .Also setting up backup servers and offline voting choices.
- User-Friendly Interface - Create simple, well-documented interfaces, icons and provide multilingual functionality for a wider audience
- Educational Campaigns - Running video tutorials and demo platforms such as television, social media for the voters used to the e-voting process.

4. **Make Strong Encryption Policies**

- Use Strong Encryption Standards - For a fully secure data transmitting solution, using end-to-end encryption techniques with modern standards with AES-256 or RSA-4096.
- Quantum-Resilient Technology - Embrace post-quantum cryptography protocols to counter quantum computing threats.
- Regular third-party audits - Have external auditors to review encryption protocols frequently.

Risk Register

Table 4. *Risk register of the project.*

Risk ID	Risk Description	Likelihood	Impact	Mitigation Strategies	Risk owner
R1	Security breaches (hacking, phishing)	High	Critical	Maintain an incident response strategy, apply multi-layer protection (firewalls, antivirus software, and intrusion detection systems), and conduct routine security audits.	IT Security Team
R2	Authentication issues	Medium	High	Make use of dynamic credentials, two-factor authentication (2FA), and regular updates to national ID cryptography systems.	Election Commission
R3	Scalability and reliability problems	Medium	High	To guarantee system availability, do load testing, put cloud-based infrastructure into place, and create backup plans.	System Development Team
R4	User accessibility challenges	Medium	Medium	Create intuitive user interfaces, carry out usability testing, launch awareness campaigns, and provide support at polling places.	UX Design Team
R5	Weak encryption protocols	Medium	High	Adopt quantum-resilient technology, use AES-256/RSA-4096 encryption, and carry out frequent third-party encryption audits.	IT Security Team

7. Recommendations

7.1 Utilize existing banking infrastructure

Collaborate with at least six well-reputed Sri Lankan banks (3 public and 3 private) and utilize their secure mobile banking applications as the mode of e-voting. This would build upon the trust in and use of online banking services, assuring the voter of safety and reliability in the entire process.

7.2 It is possible to implement two-factor authentication

Incorporate the already available two-factor authentication systems used by banks for the transactional validation of voters. This makes sure that only eligible voters access the system, and each eligible voter casts only one vote. So, it stops forging votes and keeps the election process intact.

7.3 Conduct a complete public awareness campaign

Encompassing Public Awareness Campaign to teach people more about how to access the e-voting system through their banks. The e-voting system should be free for use and of incomparable reference security features, with all benefits-including-e-voting highlighted. Such particulars should further center on those demographics that may not be as familiar with technology, such as older voters and voters living in rural areas.

7.4 Continuous Security Monitoring

The system should be continuously monitored for any threats or anomalies after it goes live. Banks and Election Commission should form a joint team on security operations to respond to possible future cyber security incidents in a real-time basis to ensure the elections go on without interruptions.

7.5 Thorough Testing and Verification

Before the complete deployment of the system, rigorous testing and auditing have to be carried out to prove its compliance with set standards related to security, reliability, and performance. A continuous schedule of audits should be aligned to find resulting vulnerabilities and exposures. The audits must have an independent third-party oversight with the goal of building public confidence in the system.

8. Conclusion

There is nothing like that in Sri Lanka regarding the development and modernization of the electoral processes regarding accessibility and security. This report has proposed a trusted solution that harnesses the already set banking infrastructure within the country, based on collaboration between the government and the banks, to deliver a secure and user-friendly system. With the experiences from previous messy situations, the model attaches itself to established technologies like two-factor authentication and decentralized voting. Success would be ensured through extensive scrutiny, public education, and security monitoring. It would strengthen democracy by providing a safe means for citizens to cast their ballots in the upcoming 2025 national elections.

References

Alwi, N. H., Malik, S., & Khan, R. (2019). Biometric authentication in mobile banking. *Journal of Information Security and Applications, 46*, 102-111.

Amrita. (2023, August 22). Alleged cyberattacks mar online voting in Ecuador | Digital Watch Observatory. *Digital Watch Observatory*. https://dig.watch/updates/alleged-cyberattacks-mar-online-voting-in-ecuador

Bai, W., Pearson, M., Kelley, P. G., & Mazurek, M. L. (2020, September). Improving non-experts' understanding of end-to-end encryption: An exploratory study. In *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)* (pp. 210-219). IEEE. https://ieeexplore.ieee.org/abstract/document/9229664/

Beck, K., Beedle, M., Bennekum, A. V., et al. (2001). Manifesto for agile software development. Retrieved from https://agilemanifesto.org

Buchsbaum, T. (n.d.). E-voting: International developments and lessons learnt. https://subs.emis.de/LNI/Proceedings/Proceedings47/Proceeding.GI.47-4.pdf

Commonwealth Secretariat. (2020). *Handbook on Commonwealth electoral law*. London: Commonwealth Secretariat.

Daramola, O., & Thebus, D. (2020, May). Architecture-centric evaluation of blockchain-based smart contract e-voting for national elections. *Informatics, 7*(2), 16. MDPI. https://www.mdpi.com/2227-9709/7/2/16

Dill, D. (n.d.). Electronic voting: An overview of the problem. https://www.acm.org/binaries/content/assets/public-policy/usacm/e-voting/testimony/dill.pdf

Ehin, P., Solvak, M., Willemson, J., & Vinkel, P. (2022). Internet voting in Estonia 2005–2019: Evidence from eleven elections. *Government Information Quarterly, 39*(4), 101718. https://doi.org/10.1016/j.giq.2022.101718

E-voting experiments end in Norway amid security fears. (2014, June 27). *BBC News*. https://www.bbc.com/news/technology-28055678

Gichubi, P. M., Maake, B., & Chweya, R. (2024). Cybersecurity framework for Kenyan universities in conformity with ISO/IEC 27001: 2022 standard. *Open Access Library Journal, 11*(8), 1-16. https://www.scirp.org/journal/paperinformation?paperid=135674

Harrison, F., & Lock, D. (2017). *Advanced project management: A structured approach* (5th ed.). Routledge.

Hettiarachchi, N., & Lakmal, H. (2023). The public value of e-government in Sri Lanka: A literature review. *JETIR, 10*(1). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4552455

Hosman, L. (2008). A pilot takes off: Examining sustainability and scalability in the context of a Sri Lankan public-private partnership telecenter project. https://aisel.aisnet.org/acis2008/28/

Kumar, S., Agrawal, A., & Sharma, A. (2020). End-to-end encryption in e-voting systems. *Journal of Cybersecurity, 12*(2), 56-67.

Loeber, L. (n.d.). E-voting in the Netherlands; from general acceptance to general doubt in two years. Retrieved December 21, 2024, from https://cs.emis.de/LNI/Proceedings/Proceedings131/gi-proc-131-002.pdf

Masterson, V. (2024, April 4). What is e-voting? Who's using it and is it safe? *World Economic Forum*. https://www.weforum.org/stories/2024/04/what-is-electronic-voting/

Mathe, L. (2022). The adoption of digital technology for South Africa's 2021 municipal elections, and prospects for the future. *Digital Policy Studies, 1*(1), 13-26. https://doi.org/10.36615/dps.v1i1.1252

Mestel, S. (2020, December 15). How bad ballot design can sway the result of an election. *The Guardian*. https://www.theguardian.com/us-news/2019/nov/19/bad-ballot-design-2020-democracy-america

Mishra, D., & Mishra, A. (2020). Contingency planning in agile projects. *Journal of Software Engineering, 9*(4), 212-220.

Nayanajith, D. A. G. (2021). Perceived trust of e-services, perceived usefulness and adoption of e-banking amongst the students of University of Kelaniya: A relational study. *Journal of Business Research and Insights*, 7(1). http://journals.sjp.ac.lk/index.php/vjm/article/view/4917

Project Management Institute (PMI). (2021). *A guide to the project management body of knowledge (PMBOK® Guide)* (7th ed.). PMI.

Schweitzer, E. J. (2019). Digital divide | society. In *Encyclopædia Britannica*. https://www.britannica.com/topic/digital-divide

Smith, R. (2009). International experiences of electronic voting and their implications for New South Wales: A report prepared for the New South Wales Electoral Commission. https://elections.nsw.gov.au/getmedia/3542227f-7959-43b7-87c4-c61ac51063fe/international-experiences-of-electronic-voting-and-their-implications-for-new-south-wales-report-2009.pdf

Stilgherrian. (2021, December 6). No surprise: NSW iVote fails during local council elections. *ZDNET*. https://www.zdnet.com/article/no-surprise-nsw-ivote-fails-during-local-council-elections/

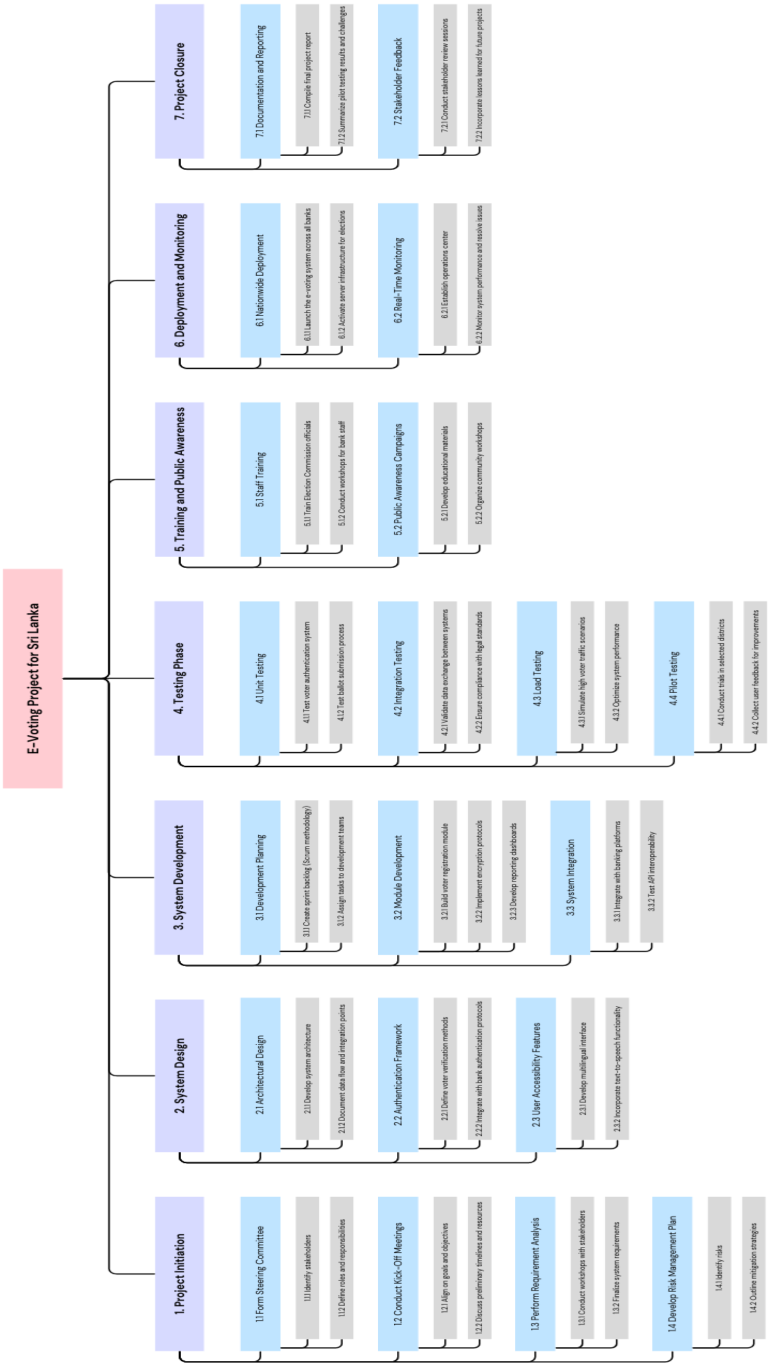
Swoboda, C. (2020, March 25). People, not technology, failed in the 2020 Iowa caucuses. *Forbes*. https://www.forbes.com/sites/chuckswoboda/2020/03/22/people-not-technology-failed-in-the-2020-iowa-caucuses/

Van Eijk, N., Fahy, R., Van Til, H., Nooren, P., Stokking, H., & Gelevert, H. (2015). *Digital platforms: An analytical framework for identifying and evaluating policy options*. TNO. https://dare.uva.nl/document/2/173306

Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). Blockchain challenges and opportunities: A survey. *International Journal of Web and Grid Services, 13*(2), 177-203.

Appendix

Appendix A: Work Breakdown Structure for the E-Voting Project

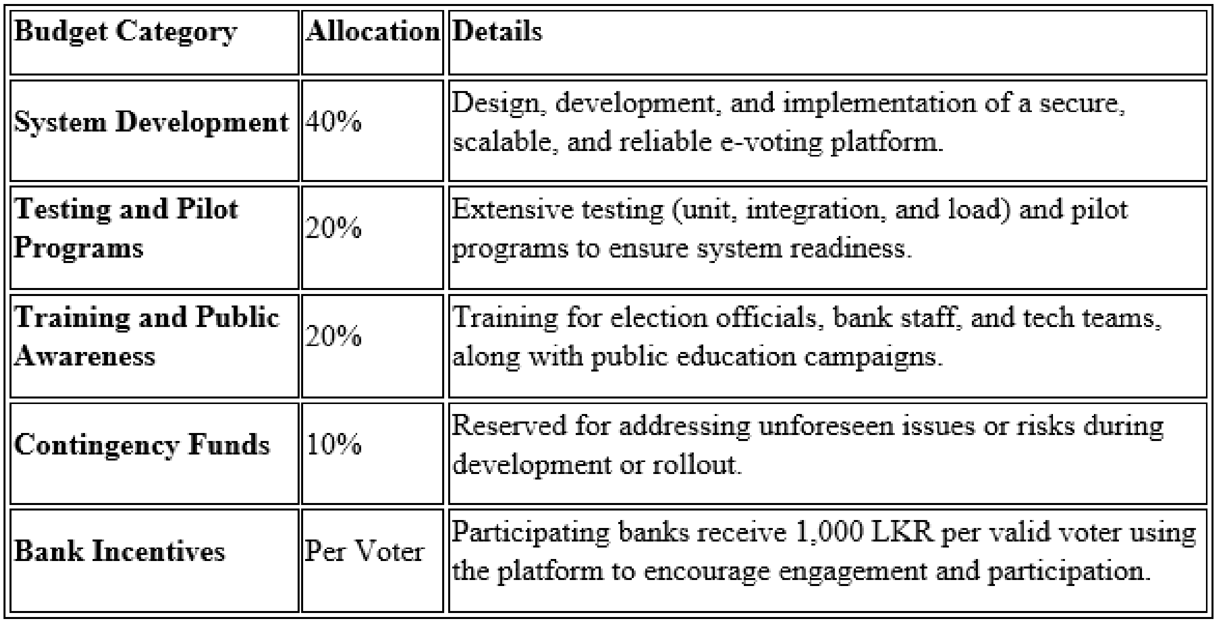

E-Voting Project for Sri Lanka
1. Project Initiation
1.1 Form Steering Committee
1.1.1 Identify stakeholders
1.1.2 Define roles and responsibilities
1.2 Conduct Kick-Off Meetings
1.2.1 Align on goals and objectives
1.2.2 Discuss preliminary timelines and resources
1.3 Perform Requirement Analysis
1.3.1 Conduct workshops with stakeholders
1.3.2 Finalize system requirements
1.4 Develop Risk Management Plan
1.4.1 Identify risks
1.4.2 Outline mitigation strategies
2. System Design
2.1 Architectural Design
2.1.1 Develop system architecture
2.1.2 Document data flow and integration points
2.2 Authentication Framework
2.2.1 Define voter verification methods
2.2.2 Integrate with bank authentication protocols
2.3 User Accessibility Features
2.3.1 Develop multilingual interface
2.3.2 Incorporate text-to-speech functionality
3. System Development
3.1 Development Planning
3.1.1 Create sprint backlog (Scrum methodology)
3.1.2 Assign tasks to development teams
3.2 Module Development
3.2.1 Build voter registration module
3.2.2 Implement encryption protocols
3.2.3 Develop reporting dashboards
3.3 System Integration
3.3.1 Integrate with banking platforms
3.3.2 Test API interoperability
4. Testing Phase
4.1 Unit Testing
4.1.1 Test voter authentication system
4.1.2 Test ballot submission process
4.2 Integration Testing
4.2.1 Validate data exchange between systems
4.2.2 Ensure compliance with legal standards
4.3 Load Testing
4.3.1 Simulate high voter traffic scenarios
4.3.2 Optimize system performance
4.4 Pilot Testing
4.4.1 Conduct trials in selected districts
4.4.2 Collect user feedback for improvements
5. Training and Public Awareness
5.1 Staff Training
5.1.1 Train Election Commission officials
5.1.2 Conduct workshops for bank staff
5.2 Public Awareness Campaigns
5.2.1 Develop educational materials
5.2.2 Organize community workshops
6. Deployment and Monitoring
6.1 Nationwide Deployment
6.1.1 Launch the e-voting system across all banks
6.1.2 Activate server infrastructure for elections
6.2 Real-Time Monitoring
6.2.1 Establish operations center
6.2.2 Monitor system performance and resolve issues
7. Project Closure
7.1 Documentation and Reporting
7.1.1 Compile final project report
7.1.2 Summarize pilot testing results and challenges
7.2 Stakeholder Feedback
7.2.1 Conduct stakeholder review sessions
7.2.2 Incorporate lessons learned for future projects

This diagram outlines the breakdown of tasks and deliverables for the successful implementation of the e-voting project in Sri Lanka.

Appendix B: Risk Register

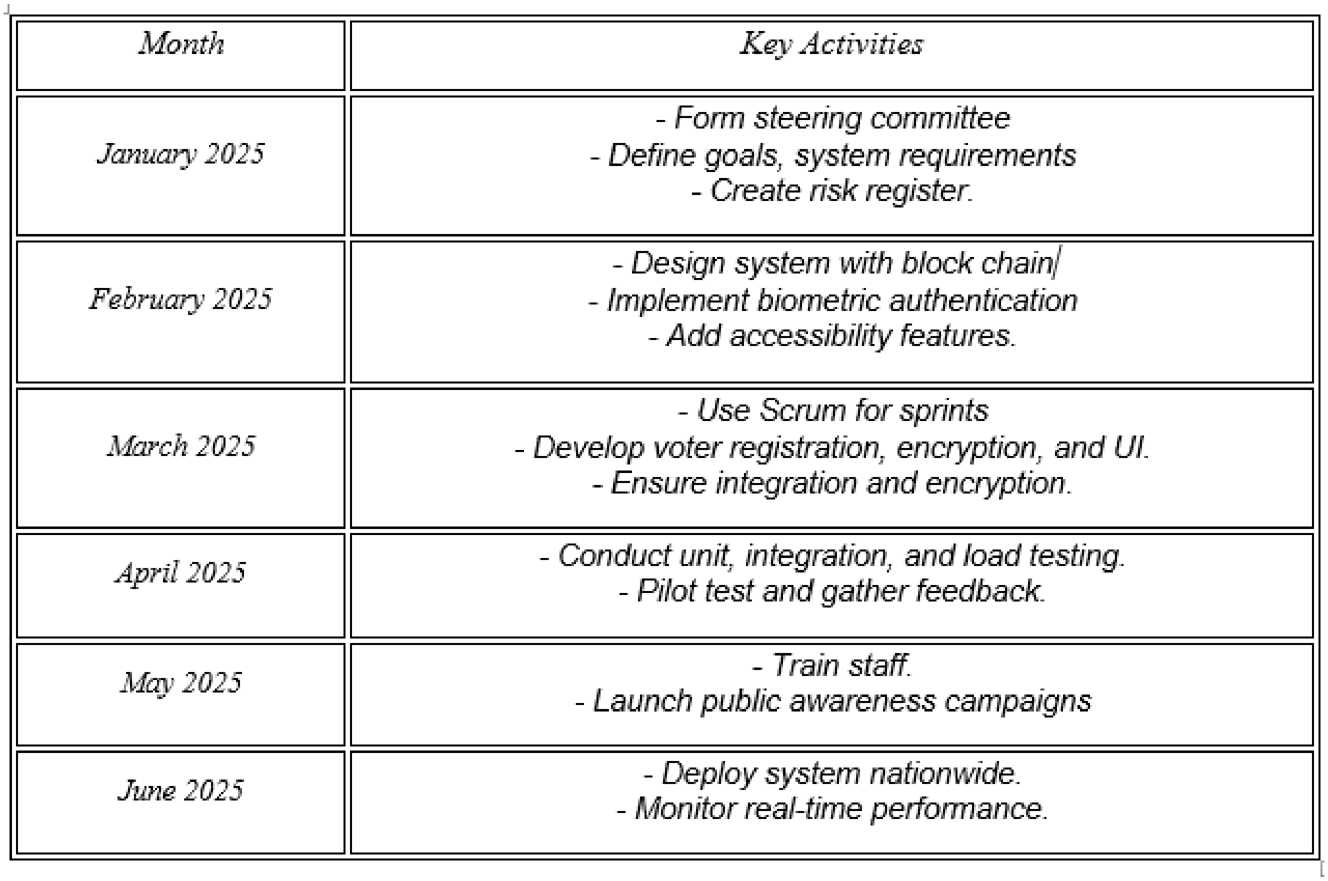
Risk ID	Risk Description	Likelihood	Impact	Mitigation Strategies	Risk owner
R1	Security breaches (hacking, phishing)	High	Critical	Maintain an incident response strategy, apply multi-layer protection (firewalls, antivirus software, and intrusion detection systems), and conduct routine security audits.	IT Security Team
R2	Authentication issues	Medium	High	Make use of dynamic credentials, two-factor authentication (2FA), and regular updates to national ID cryptography systems.	Election Commission
R3	Scalability and reliability problems	Medium	High	To guarantee system availability, do load testing, put cloud-based infrastructure into place, and create backup plans.	System Development Team
R4	User accessibility challenges	Medium	Medium	Create intuitive user interfaces, carry out usability testing, launch awareness campaigns, and provide support at polling places.	UX Design Team
R5	Weak encryption protocols	Medium	High	Adopt quantum-resilient technology, use AES-256/RSA-4096 encryption, and carry out frequent third-party encryption audits.	IT Security Team

Appendix C: Budget Allocation Details



Budget Category	Allocation	Details
System Development	40%	Design, development, and implementation of a secure, scalable, and reliable e-voting platform.
Testing and Pilot Programs	20%	Extensive testing (unit, integration, and load) and pilot programs to ensure system readiness.
Training and Public Awareness	20%	Training for election officials, bank staff, and tech teams, along with public education campaigns.
Contingency Funds	10%	Reserved for addressing unforeseen issues or risks during development or rollout.
Bank Incentives	Per Voter	Participating banks receive 1,000 LKR per valid voter using the platform to encourage engagement and participation.

Appendix D: Timeline Summary



Month	Key Activities
January 2025	- Form steering committee - Define goals, system requirements - Create risk register.
February 2025	- Design system with block chain - Implement biometric authentication - Add accessibility features.
March 2025	- Use Scrum for sprints - Develop voter registration, encryption, and UI. - Ensure integration and encryption.
April 2025	- Conduct unit, integration, and load testing. - Pilot test and gather feedback.
May 2025	- Train staff. - Launch public awareness campaigns
June 2025	- Deploy system nationwide. - Monitor real-time performance.