CHAMPTEK®

Champtek Incorporated

Bio-Voting System

Index

1. Introduction

CHAMPTEK is a versatile election application that captures biometric and biographic data. It can be customized to meet various needs, from small-scale handheld devices to large-scale desktop systems. CHAMPTEK supports multiple features like scanning, photo capture, fingerprint capture, and signature capture. It also includes advanced biometric features like image processing and template generation.

The Comprehensive Election Management System (CEMS) is a robust and integrated software solution designed to streamline and secure the entire electoral process. This system encompasses three key components: Voter Registration Software (VRS), Candidate Nomination Capture System (CNC), and Accreditation Management System (AMS).

The VRS module is responsible for managing the voter registration process, including capturing voter details, processing applications, and generating voter cards. It integrates GIS mapping for efficient polling station identification and provides features for voter updates, transfers, and objections.

The CNC module facilitates the candidate nomination process, capturing details of presidential, parliamentary, and local candidates. It includes modules for pre-nomination, supporter and agent registration, and final nomination. The system ensures compliance with nomination rules and generates necessary reports.

The AMS module manages the accreditation process for individuals and organizations involved in the election. It handles application submission, verification, and card generation. It also provides features for tracking accredited individuals and organizations, ensuring security and access control.

The CEMS is designed to be user-friendly, efficient, and secure. It utilizes biometric authentication, data encryption, and robust security measures to protect sensitive information. The system also includes features for data backup, restoration, and reporting, ensuring data integrity and accessibility.

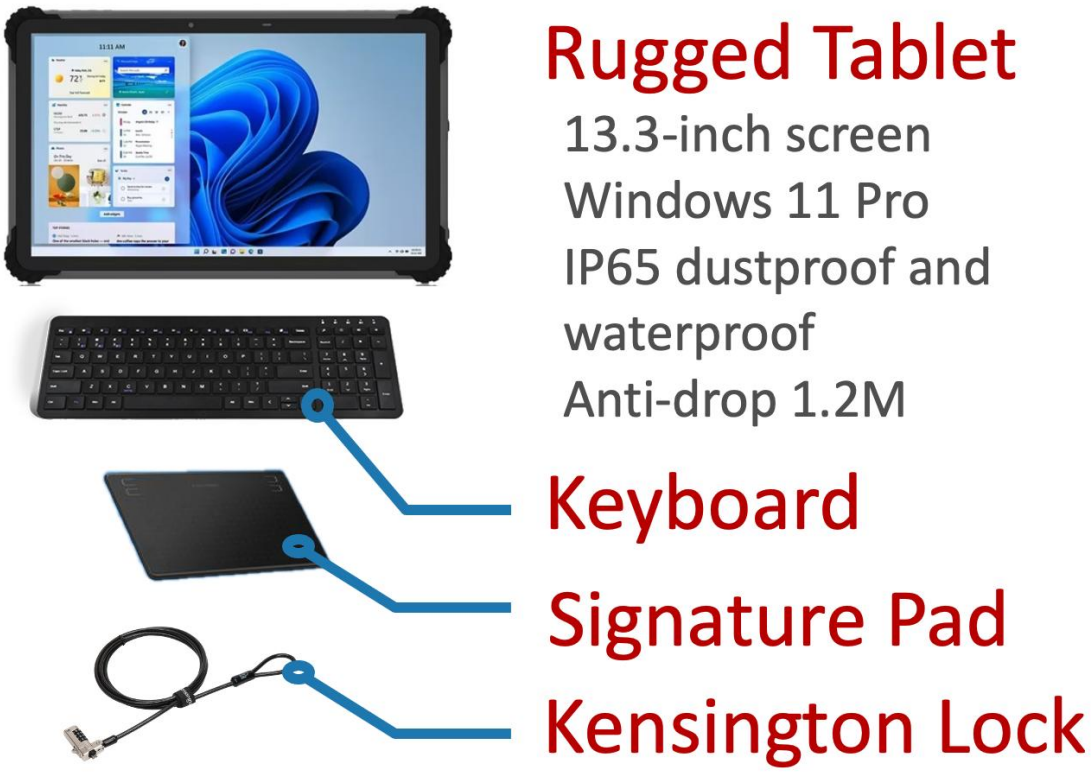
By integrating these three modules, the CEMS offers a comprehensive solution for managing all aspects of the election process, from voter registration to result tabulation. This system enhances transparency, efficiency, and accuracy, contributing to the integrity of the electoral process.

1.1. Purpose of the System

The purpose of the Comprehensive Election Management System (CEMS) is to streamline and secure the entire electoral process. It aims to improve efficiency, transparency, and accuracy in voter registration, candidate nomination, and accreditation management. By automating key processes, the CEMS reduces human error, minimizes fraud, and ensures a fair and credible election. The system also enhances data security and provides robust reporting capabilities for monitoring and analysis.

1.2. List of Hardware Component

ChempTek offers a robust and flexible portable mobility solution designed to excel in demanding environments, such as high-stakes election events. Its innovative design begins with the Basic Pack, which includes essential components: a rugged tablet, standard keyboard, signature pad, and a Kensington Lock for security. This ensures the device remains operational and secure, even during unpredictable and tumultuous election conditions.



Beyond the basics, ChempTek incorporates advanced biometric collection tools, such as a state-of-the-art fingerprint scanner, providing enhanced accuracy and security for voter authentication.

To support seamless election management, ChempTek also integrates additional peripherals for maximum efficiency. The **7-port USB Hub with Switch** facilitates multiple connections, while the high-performance printer and document scanner streamline data processing. Its auto-focus 10-megapixel camera with a 78-degree field of view captures clear, precise images. Features like automatic white balance and color correction ensure accurate visuals, even in challenging lighting conditions.

Printer

The multifunctional printer –
Printing, copying and scanning
High print yield rate
Supports wireless connectivity

ChempTek’s thoughtful design and comprehensive toolset make it a powerful, reliable solution for election events. Its blend of durability, flexibility, and advanced technology ensures smooth operations and accurate results, even in the most demanding circumstances.

Power Station

Reliable, High-Power output 300W AC with 230.4Wh battery capacity, Multiple charging options, Advanced safety

ChempTek's solution includes a reliable **Power Station**, ensuring uninterrupted operation in remote or unstable environments. This essential feature provides consistent power, safeguarding critical election processes from outages and ensuring continuous, seamless functionality.

Rugged Tablet

13.3-inch screen
Windows 11 Pro
IP65 dustproof and waterproof
Anti-drop 1.2M

Keyboard

Signature Pad

Kensington Lock

Power Station

Reliable, High-Power output 300W AC with 230.4Wh battery capacity, Multiple charging options, Advanced safety

Document Scanner

Fixed focus, 8 million pixels, transmission speed per second, real-time preview

IP67 Carry Case

Water & Dustproof
wear-resistant
Ergonomic handle
Lock firm & easy to open
Strong impact resistance

Printer

The multifunctional printer –
Printing, copying and scanning
High print yield rate
Supports wireless connectivity

Fingerprint Scanner

Support 4-finger flat, single-finger flat, and rolling capture, double thumb fingerprint collection

Webcam

Auto Focus, 10 Megapixels, Angle of View 78°
Automatic white balance & color correction

7ports USB Hub with switch

ChempTek’s robust, portable solution to ensure secure, efficient election management in diverse environments can help. Its durable design, advanced biometric tools, and reliable power supply support accurate, uninterrupted electoral processes.

1.3. Overview of Features

The Comprehensive Election Management System (CEMS) offers a range of features designed to streamline and secure the electoral process:

Voter Registration Software (VRS):

- **Voter Registration:** Captures voter details, validates applications, and generates voter cards.
- **GIS Integration:** Utilizes GIS maps for efficient polling station identification and assignment.
- **Voter Updates and Transfers:** Facilitates updates to voter information and transfers between polling stations.
- **Objections and Appeals:** Provides a mechanism for handling objections to voter registration and appeals against decisions.

- **Data Security and Backup:** Ensures data integrity and security through encryption and regular backups.

Candidate Nomination Capture System (CNC):

- **Candidate Registration:** Captures details of presidential, parliamentary, and local candidates.
- **Supporter and Agent Registration:** Records information about supporters and election agents.
- **Nomination Validation:** Verifies nomination forms and ensures compliance with eligibility criteria.
- **Data Security and Backup:** Protects sensitive candidate data through encryption and regular backups.

Accreditation Management System (AMS):

- **Accreditation Application:** Processes applications from individuals and organizations for accreditation.
- **Accreditation Verification:** Verifies applicant credentials and assigns appropriate accreditation levels.
- **Card Generation:** Generates and prints accreditation cards with security features.
- **Access Control:** Manages access to restricted areas through card scanning and authentication.
- **Data Security and Backup:** Ensures the security and integrity of accreditation data.

By combining these features, the CEMS provides a comprehensive solution for managing all aspects of the election process, from voter registration to result tabulation.

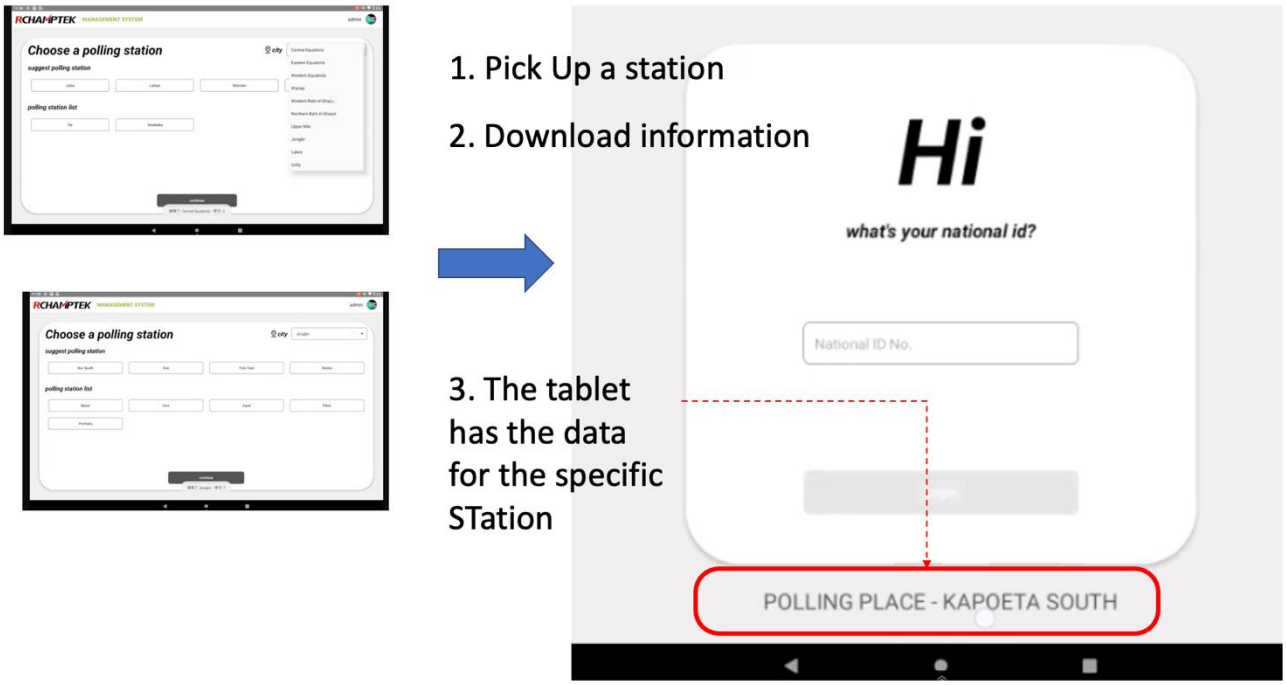
1.4. General Working process

- Auto-Start when turn on the screen

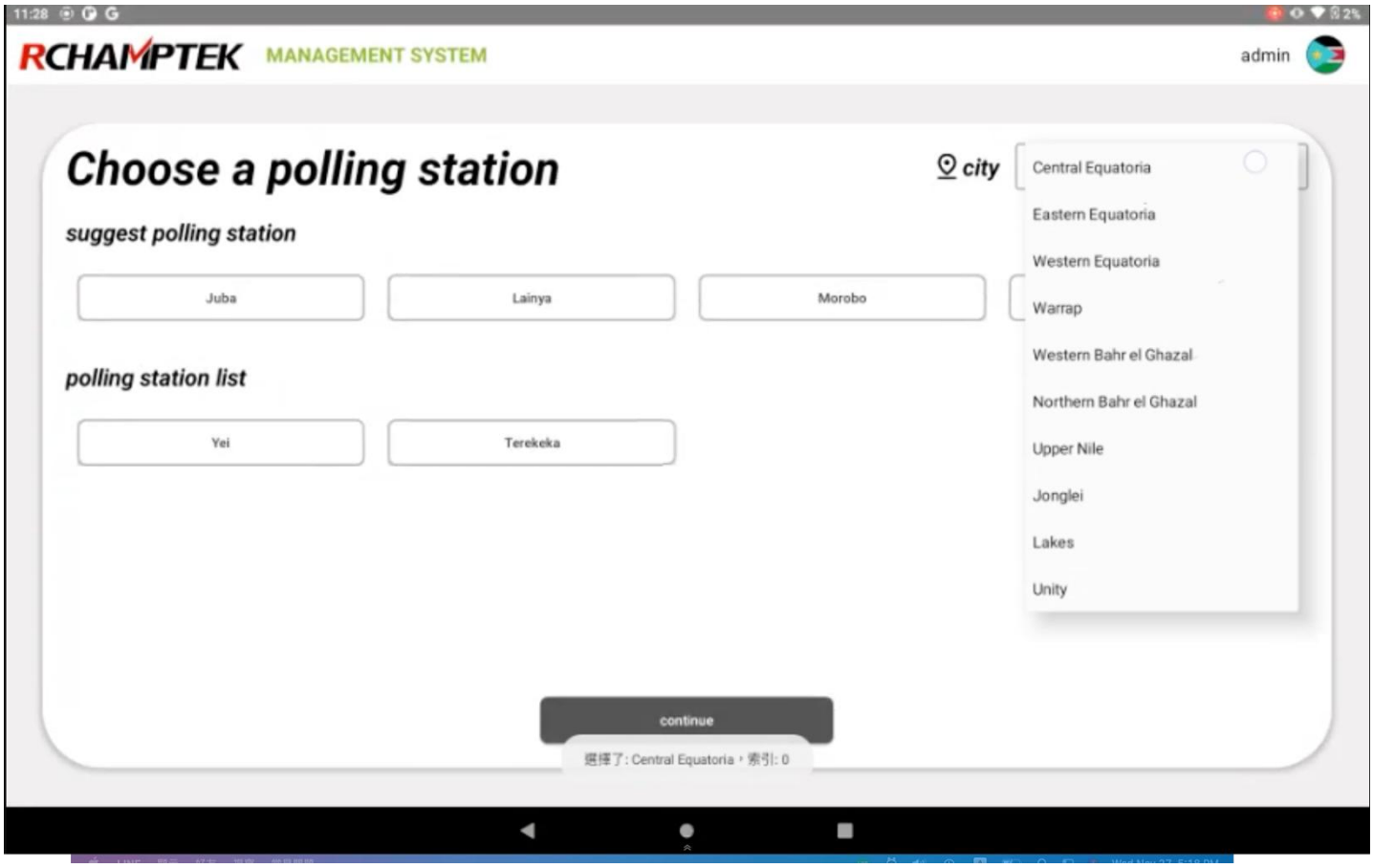
Our app features an **autostart function**, activating automatically when the screen powers on. This ensures immediate, hassle-free access, streamlining workflows and enhancing efficiency right

from startup.

- Two Steps of voters collection



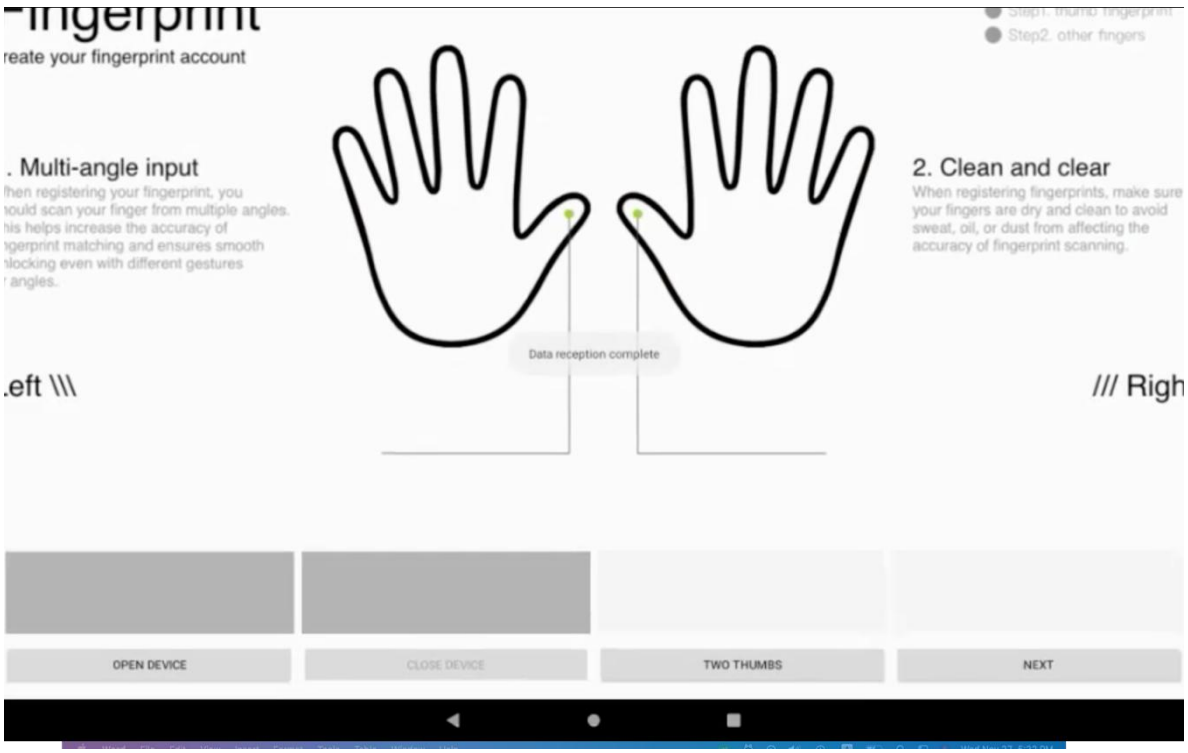
- ARO-TS Login Screen



- Scan Barcode/ID:

The operator can scan the barcode on an existing voter ID card or scan a passport to begin the voter registration process. The scanning of the card enables the system to auto-populate voter details from pre-existing records stored on the device, streamlining the process.

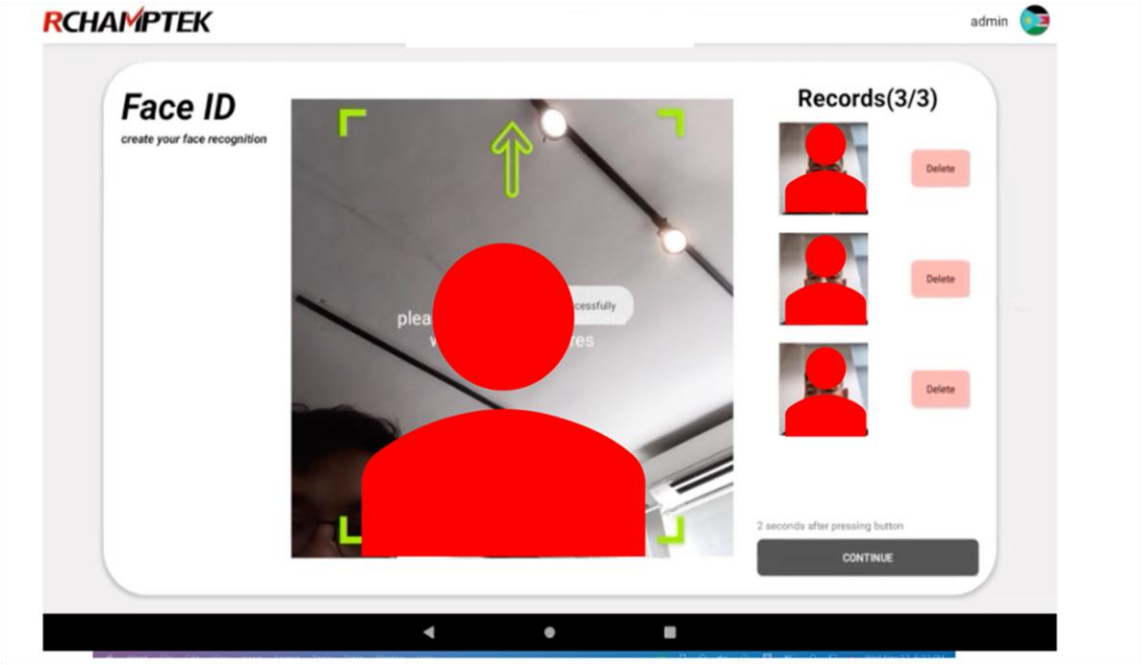
- Capture Biometric Data (Fingerprints):



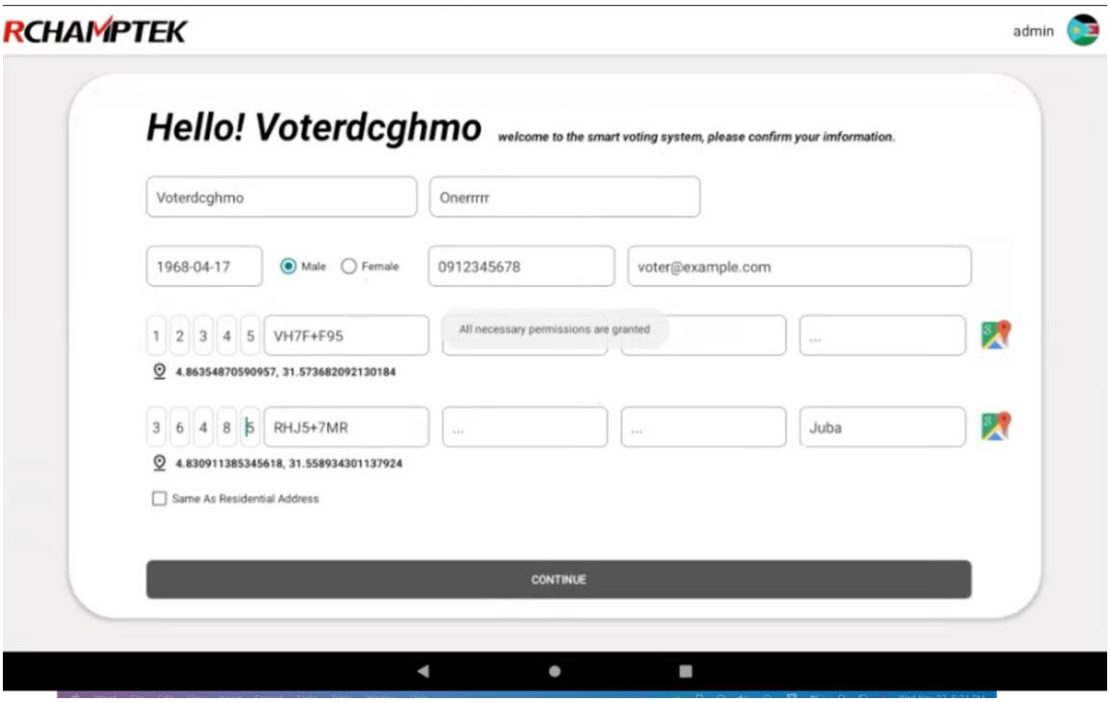
The system is capable of capturing 10 fingerprints of the voter. With an integrated Quality Management SDK, the application ensures high-quality biometric data is captured and provides real-time alerts to the operator for quality checks.

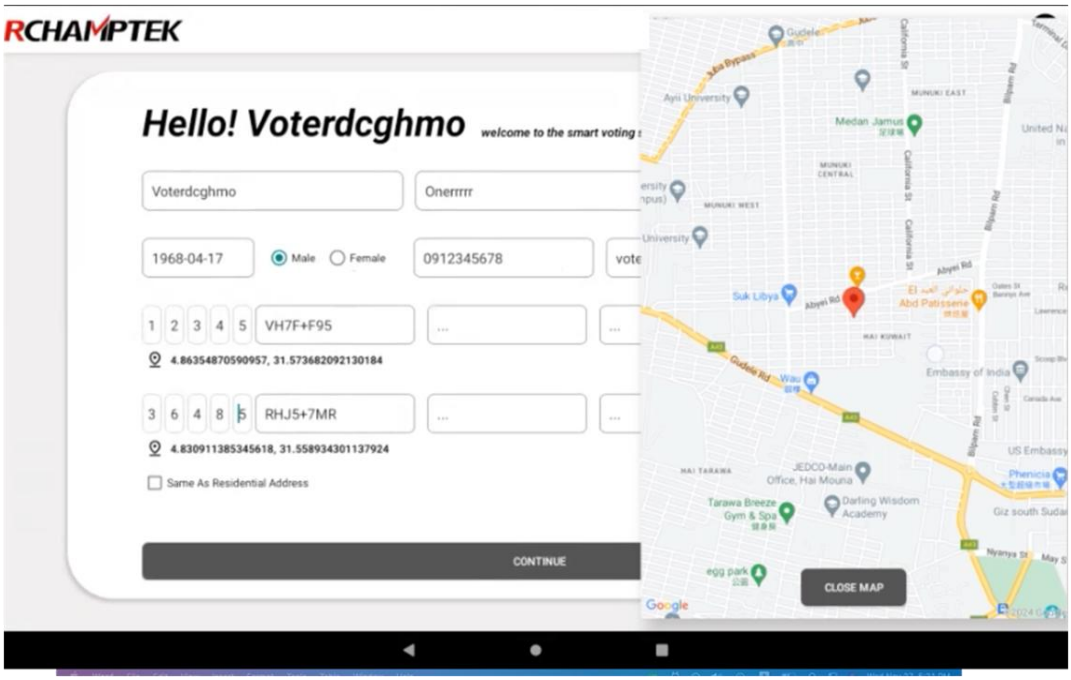
- Capture Photograph:

The operator can capture a high-quality photograph of the voter, adhering to ICAO standards. Real-time quality feedback is available to ensure the photo meets the required standards for voter identification.



- GIS Intergrated

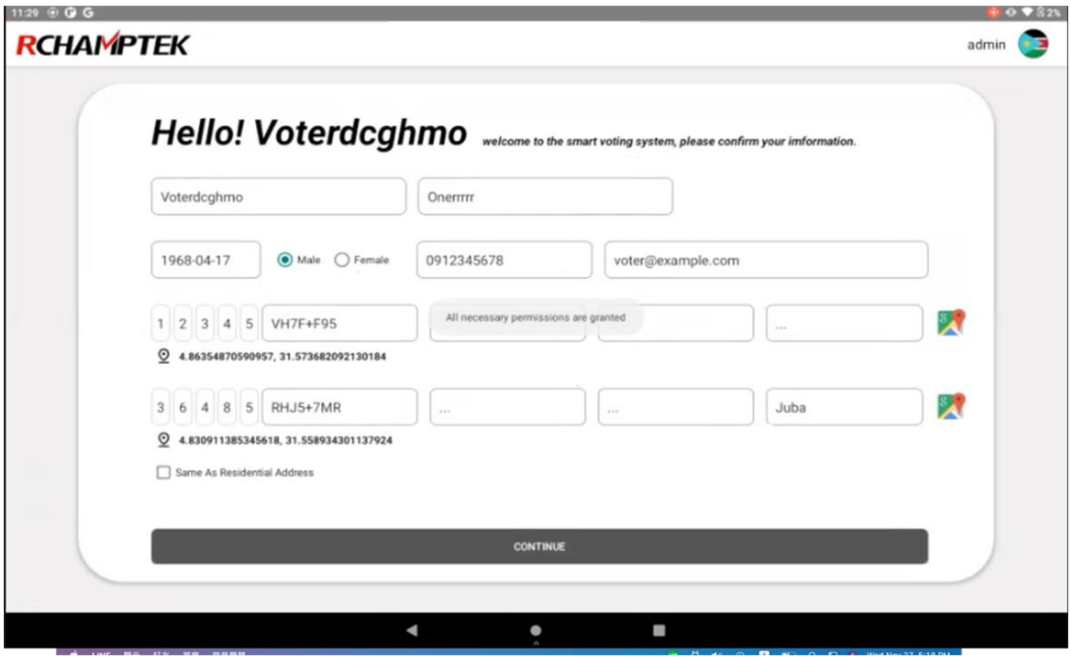




CHAMPTEK, a versatile election application, leverages GIS technology to map and analyze voter data geographically. By integrating spatial data, it enables efficient planning, resource allocation, and real-time monitoring of election processes. This GIS-powered solution enhances the accuracy and transparency of elections.

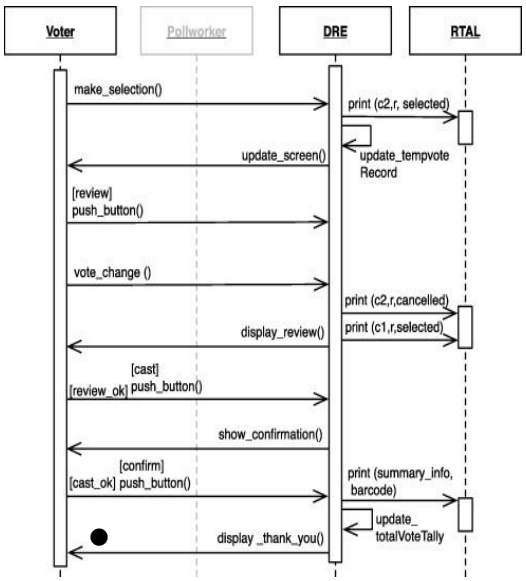
- Local De-duplication:

The application includes a duplicate check feature. If a voter attempts to register multiple times, the system will detect the duplicate and alert the operator, ensuring that only one registration is maintained for each voter.

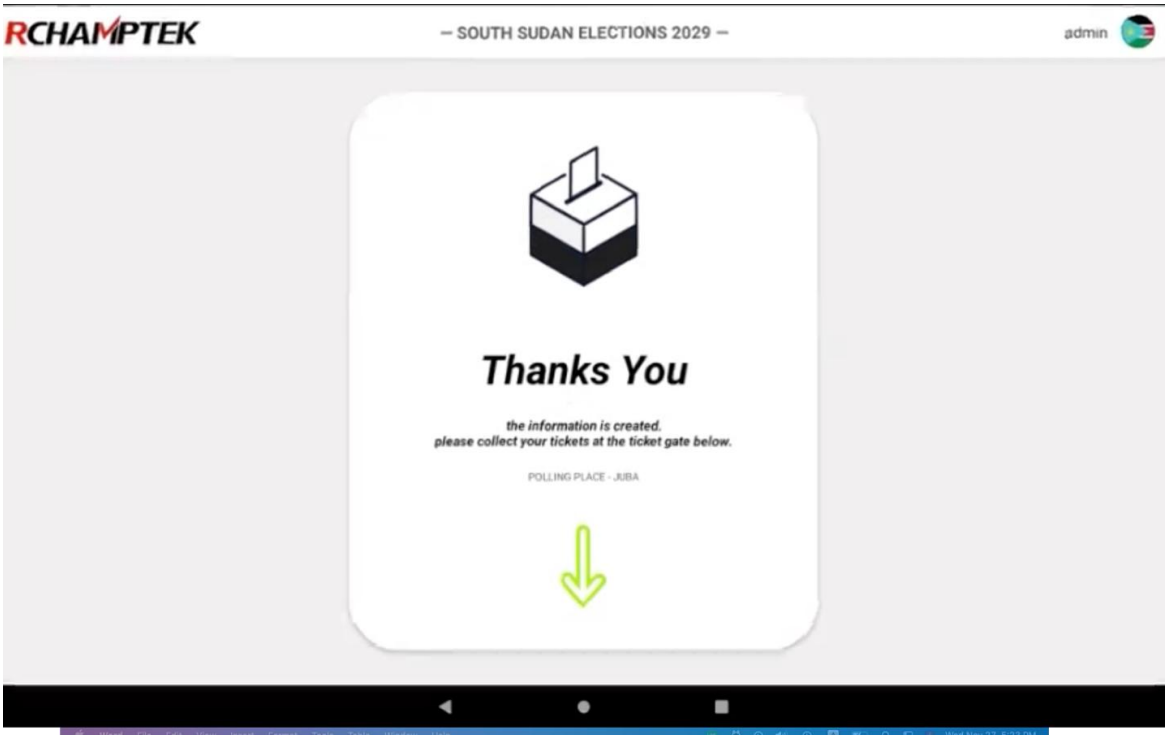


- Logs & Reporting:

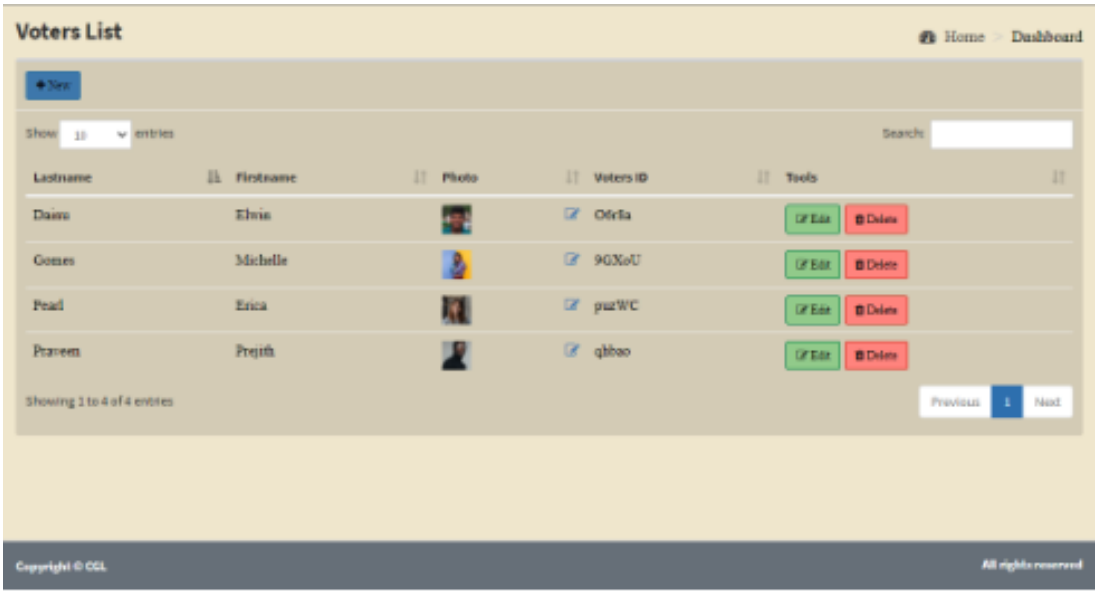
The system maintains detailed logs of all activities performed on the device, including polling station details, operator information, timestamps, and activity descriptions. These logs are encrypted to ensure data integrity and prevent tampering, and are only accessible by authorized personnel. This feature ensures the election process is transparent and verifiable.

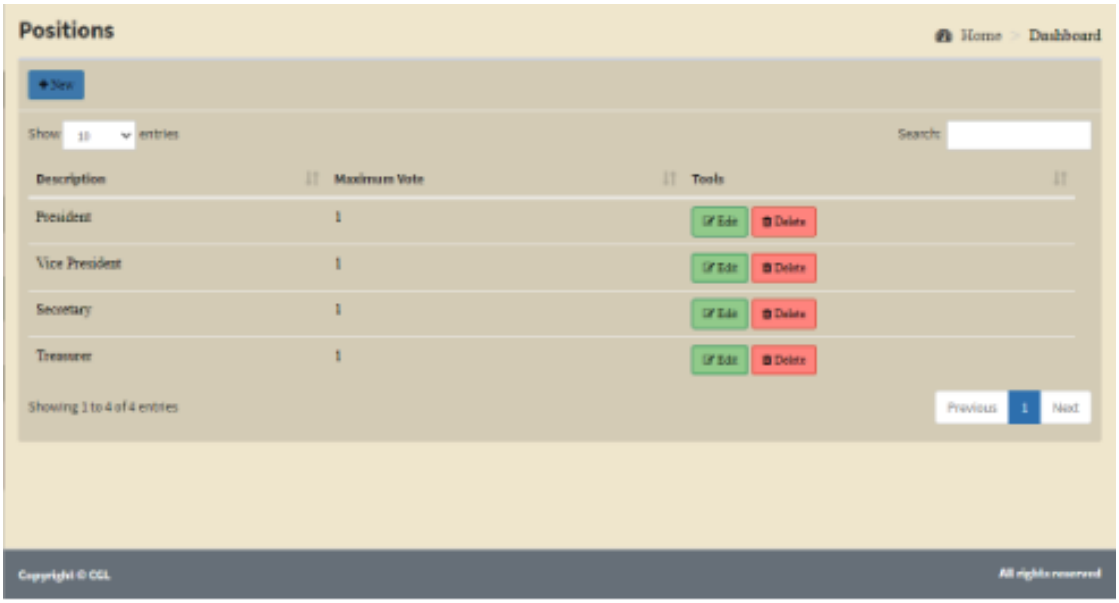


- Flexible Ticket PrintOut:



- User Management



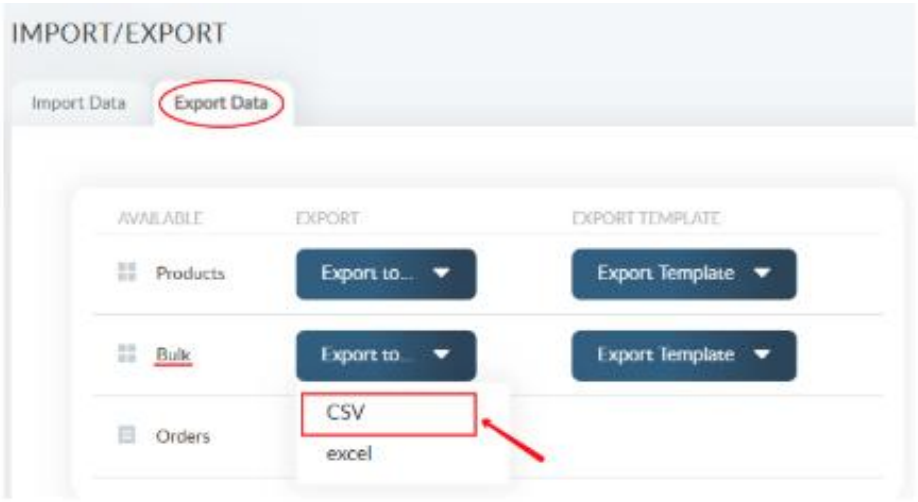


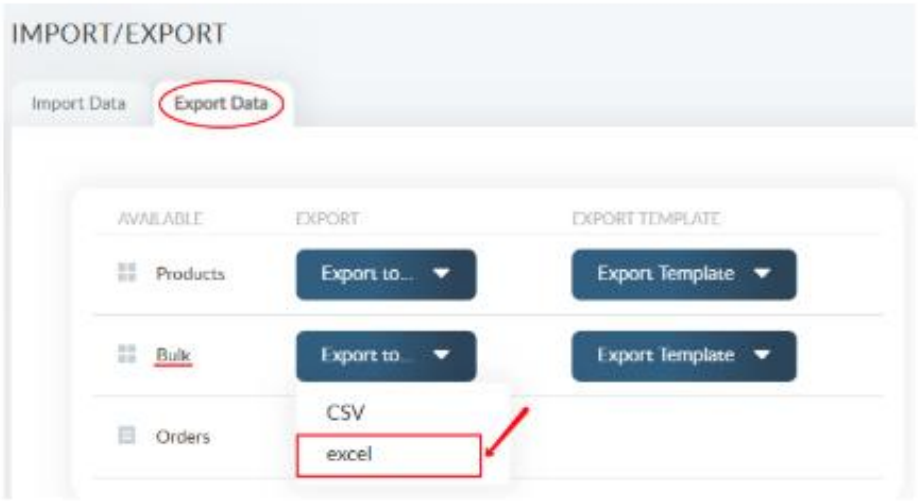
- Data Encryption:

All data captured by the system is encrypted before transmission using 128/256-bit AES encryption. This ensures that sensitive voter data is secure during transfer to the Biometric Voter Management Server, preventing any manipulation or tampering. Only the integrated application at the central site can decrypt the data, ensuring that data privacy and security are maintained.

- Data Export:

The system allows for data export as required, sending voter registration information securely to the Voter Management Server or other designated locations. This feature facilitates efficient data management and synchronization with central systems.





- Different Role Login:

Staff Login

Voter Login

By integrating these features, the Voter Turnout Analysis module helps election officials track voter participation, identify trends, and improve the overall voter engagement strategy, ensuring a more inclusive and efficient electoral process.

1.5. Biometric Voter Registration process

The CHAMPTEK Biometric Voter Registration application is an excellent choice for integration into the voter registration system due to its robust, customized design tailored for large-scale, fast, and accurate voter enrollment. It offers a self-contained, complete solution for capturing and storing both biographic and biometric data, which is essential for ensuring voter integrity and minimizing fraud.
The application supports the full enrollment workflow, including the capture of key data elements, such as:

✓ Biographic and Registration Data

✓ Biometric Information (facial images and fingerprints)

✓ Biometric Templates and Minutiae from fingerprints

✓ Scans of Document Copies

✓ Unique Registration Number Generation

This application is equipped with integrated biometric quality control, which guarantees high-quality data capture, vital for preventing errors and ensuring the authenticity of voter records. The built-in quality management SDK for fingerprint capture ensures that the biometric data is precise and reliable, while real-time feedback on photographs ensures high-quality image capture, adhering to ICAO standards.

The CHAMPTEK system is also highly secure, offering data encryption using 128-bit / 256-bit AES encryption, ensuring that voter data remains safe and tamper-proof during transmission to the central server. This level of security, combined with local de-duplication features that prevent duplicate registrations, strengthens the integrity of the entire voter registration process.

Furthermore, the system supports logs and reporting, allowing election officials to track all activities in real time, ensuring transparency and compliance with election protocols. The data export feature ensures seamless integration with centralized voter management systems, while the data import functionality supports smooth updates of voter records from different locations.

Overall, the CHAMPTEK Biometric Voter Registration application is a powerful, scalable, and secure tool that is well-suited for large-scale voter registration projects, ensuring accuracy, security, and efficiency in capturing voter information while maintaining the integrity of the electoral process.

1.6. Importance of Securing Electoral Processes

Security is crucial in the Accreditation Management System (AMS) due to the sensitive nature of the data being handled. The system manages personal and biometric information, including National Registration Card numbers, passport details, photographs, signatures, and fingerprints, which must be protected against unauthorized access, data breaches, and tampering.

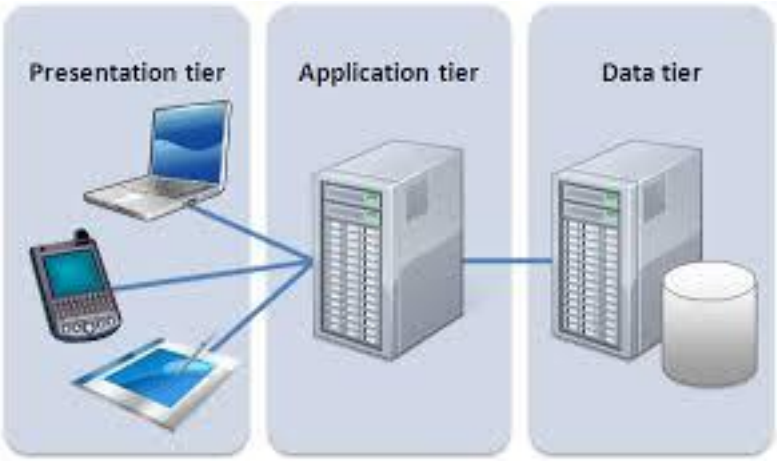
Here are key reasons why security is essential:

- Protection of Sensitive Data: The system handles highly sensitive personal and biometric information that, if compromised, could lead to identity theft or misuse. Ensuring data confidentiality, integrity, and availability is critical.
- Regulatory Compliance: The system must comply with data protection regulations and industry standards, such as the use of encryption (AES 256-bit) to secure data both in transit and at rest, ensuring that it meets legal and organizational privacy requirements.
- Audit and Accountability: Security measures like multi-factor authentication, user log tracking, and event journaling ensure that actions within the system are traceable. This helps maintain accountability for users accessing the system and performing critical tasks, providing an audit trail for forensic purposes.
- Preventing Fraud: With the potential for multiple stakeholders involved in elections or accreditation processes, security ensures that no unauthorized personnel can manipulate data or impersonate legitimate applicants or officials. Secure login mechanisms and biometric authentication safeguard against fraudulent access.

- Data Backup and Recovery: Security ensures that backup procedures are encrypted and stored safely, enabling recovery in case of system failure or data loss, reducing risks associated with system downtimes and data corruption.
- Maintaining Trust: The integrity of the accreditation process is vital for public trust in elections and other critical events. Security prevents malicious interference and ensures the system's credibility and reliability.

2. System Architecture

2.1. Software Framework and Development Environment



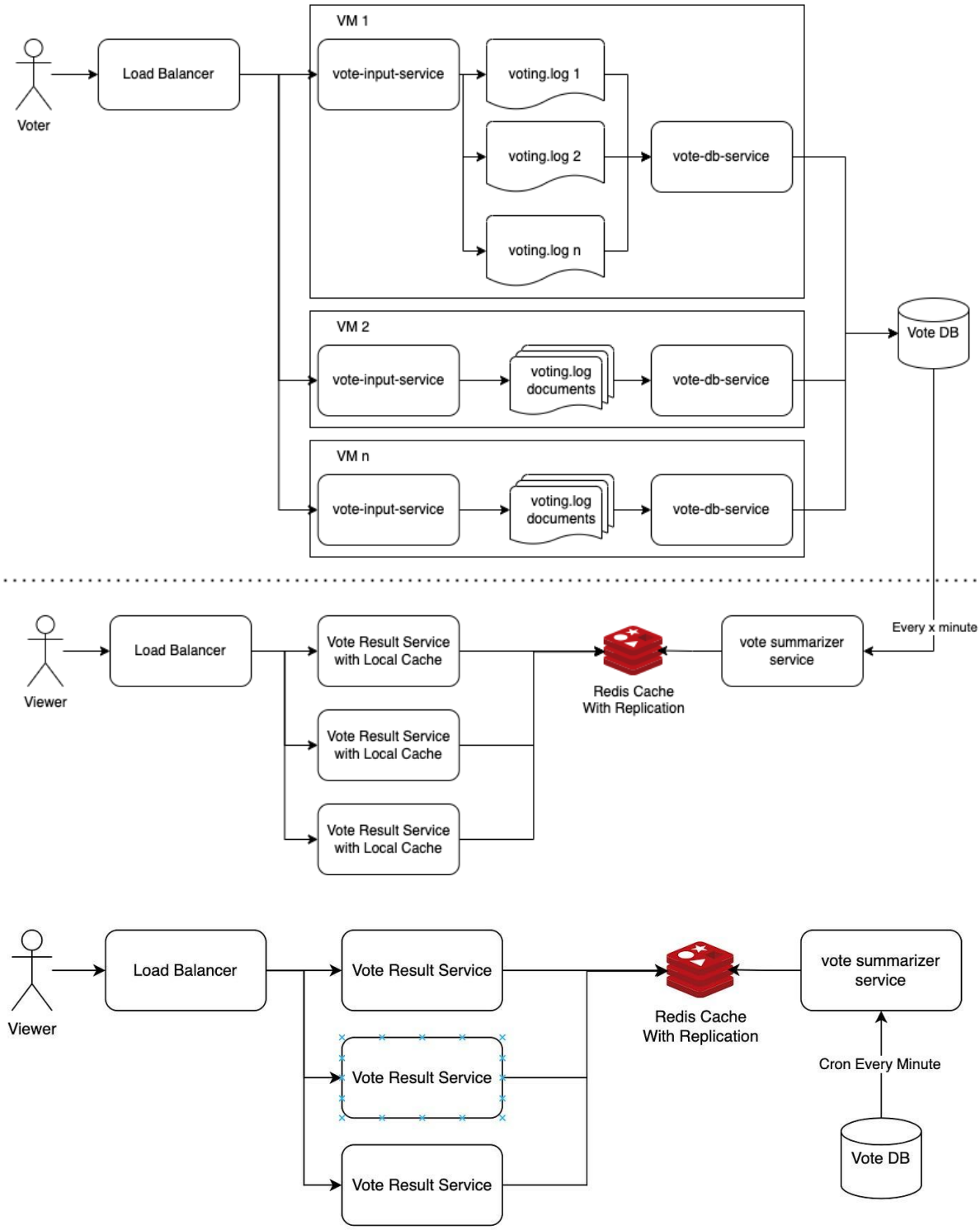
2.1.1. Backend

2.1.1.1. Database: SQL Server:Relational database for structured data storage.

2.1.1.2. Application Server: Next.js

- React framework for building server-rendered and static websites.
- Provides flexibility for both server-side rendering (SSR) and client-side rendering (CSR).

- Offers features like API routes, image optimization, and more.



2.1.2. Frontend

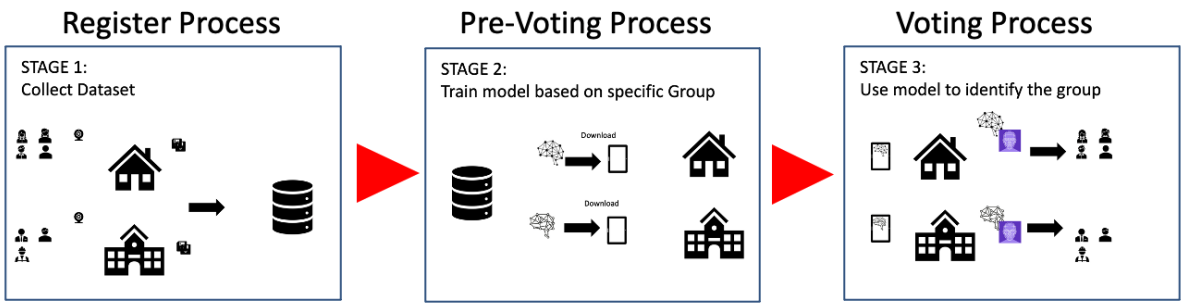
- Web: HTML5, Angular
- Mobile: Windows C#

2.1.3. Testing and Quality Assurance

- Unit Testing: Write unit tests for individual components and functions.

- Integration Testing: Test the integration of different components.
- End-to-End Testing: Test the entire application flow from user interaction to database operations.
- Performance Testing: Evaluate application performance under various load conditions.

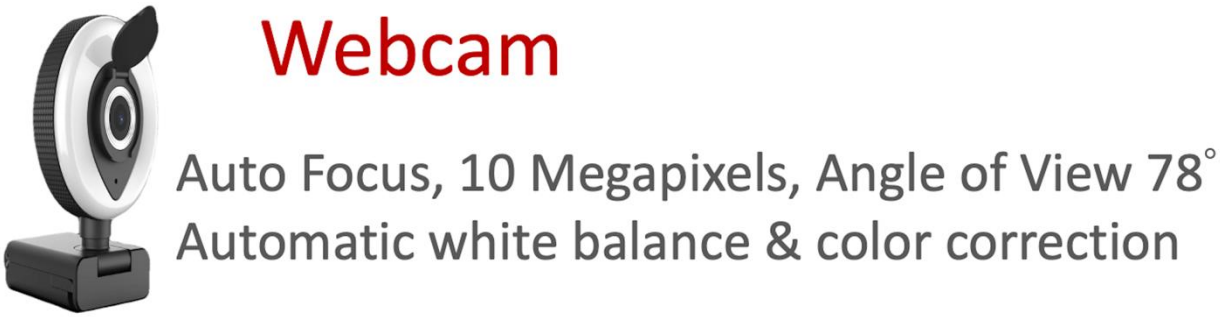
3. Biometric Features



3.1. Facial Recognition

The system captures voters' images during registration to create a localized dataset for each voting station. Using deep learning algorithms, the backend trains a lightweight facial recognition model to accurately identify registered voters on-site. This approach enhances verification efficiency and ensures only eligible voters can cast their ballots at specific stations.

3.2. Image Capture and Matching



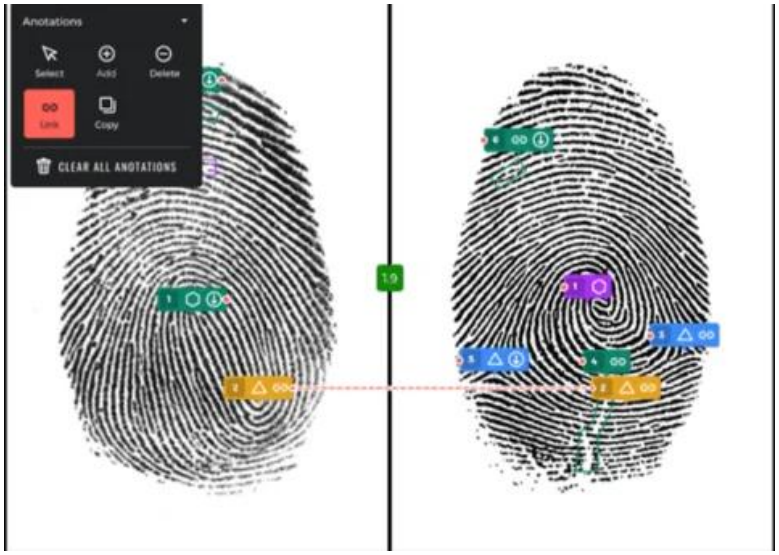
The system uses a high-quality camera to capture voter photos following ICAO standards. Real-time feedback ensures image quality, and facial recognition software matches photos against preloaded database records for verification.

3.3. Integration with National Identification Databases

The voting system integrates with national identification databases via secure APIs, enabling real-time identity verification, preventing duplicate registrations, and ensuring accurate voter records using biometric and demographic data synchronization.

3.4. Fingerprint Recognition

The system captures fingerprints using a high-resolution scanner with quality management SDKs to ensure clarity. Captured prints are converted into templates and matched against a database using an advanced Automated Fingerprint Identification System (AFIS), which checks for duplicates in real-time to ensure accurate voter identification and prevent fraudulent registrations.



3.5. Fingerprint Capture and Matching

3.6. Anti-Spoofing Measures

To ensure data integrity, prevent fraudulent activities, and authenticate genuine users during voter registration and voting.

- Biometric Validation

  Fingerprint and Facial Recognition: Use multi-factor biometric checks to prevent spoofing through forged identities.

  Liveness Detection: Include algorithms to detect live fingerprints and facial gestures to avoid use of fake biometrics.

- Encrypted Authentication

  Secure QR Codes: Voter cards include encrypted QR codes that validate against a central database, preventing duplication.

  Digital Signatures: All transactions and data entries are signed to ensure authenticity.

- Tamper Detection

Device Integrity Checks: Voting devices perform regular self-checks to detect unauthorized hardware or software modifications.

Log Monitoring: Automated analysis of system logs to identify suspicious or unauthorized access patterns.

- Geo-Fencing

  Restrict voting and registration activities to specific, predefined locations using GPS tracking.

- User Behavior Analysis

  Monitor operator actions for unusual patterns (e.g., rapid voter registrations) to flag potential fraudulent activities.

4. Role-Based Access Control (RBAC)

4.1. User Roles and Permissions

4.1.1. Chief Electoral Officer (CEO)

- Full access to all system modules and settings.
- Ability to approve or reject accreditation applications and organisation registrations.
- View and generate all system reports.
- Manage user roles, permissions, and access control.
- Configure system settings and manage system-wide functionalities.
- Perform data export and import for central repository integration.
- Oversee audit trails, logs, and security monitoring.
- Initiate software updates and manage system backups.

4.1.2. District Election Officer (DEO)

- Access to district-level accreditation data.
- Approve or reject accreditation applications within their jurisdiction.
- Manage user accounts for district-level staff (ARO-IT, ARO-TS).
- Perform diagnostics on system components (e.g., kit hardware).
- Generate reports specific to district accreditation.
- Perform district-level data export, backup, and restoration.

4.1.3. Assistant Returning Officer – IT (ARO-IT)

- System administration at the district level for IT support.
- Manage IT security and infrastructure for the accreditation kits.
- View and manage user logs, audit trails, and application statuses.
- Access data import/export functions for district-level data.
- Monitor system performance and ensure smooth operation of IT systems.
- Perform diagnostics and troubleshooting for IT-related issues.

4.1.4. Assistant Returning Officer – Technical Support (ARO-TS)

- Provide technical support for system users and equipment.
- Perform diagnostic tests and ensure all components are functioning.
- Support with backup and data restoration processes.
- Assist in software updates and troubleshooting kit malfunctions.

4.1.5. Data Entry Operator (DEO)

- Enter and update accreditation application data, including personal and biometric information.
- Upload supporting documents (e.g., NRC, passport copies) for applicants.
- Validate and verify applicant details.
- Access limited data import/export features for managing accreditation data.
- Generate reports related to data entry errors or discrepancies.

4.1.6. Security Officer

- Manage and validate access control for accreditation areas (e.g., restricted zones).
- Monitor the movement of accredited individuals.
- Flag and restrict access for individuals or organisations that are blacklisted.
- View and generate security-related reports.
- Maintain audit trails for access and movement within secured areas.

4.1.7. System Administrator

- Manage system settings and configurations across the entire system.
- Full access to manage user roles, permissions, and security settings.
- Perform system-wide diagnostics and troubleshooting.
- Oversee backup and restore functionalities.
- Implement and monitor software updates across the system.

4.2. User Roles and Permissions

The system follows a **multi-level access control** structure:

- High-level Users (e.g., CEO, DEO, System Administrators) have full access to all system settings, configurations, and reports.
- Operational Users (e.g., ARO-IT, ARO-TS, Data Entry Operators) have access tailored to their functional roles, such as data entry, technical support, and system diagnostics.
- Event-Based Users (e.g., Security Officers, Observers, Media, Political Party Representatives) have restricted access based on their roles and event participation, ensuring they only interact with the data necessary for their duties.

5. General Features

5.1. Reporting:

The system generates detailed reports for various actions, such as malfunctioning components in the accreditation system, and audit trails for voter registrations and candidate

nominations. These reports ensure transparency, accountability, and help monitor system health.

5.2. Data Import/Export:

- The system supports the import of data (e.g., voter lists, candidate nominations) via Local or Wide Area Networks (LAN/WAN), ensuring seamless integration with external databases.
- Export functionality is available, with data encrypted (AES 256-bit) for secure transmission to central repositories, ensuring data integrity during transfers.

5.3. Backup:

Automatic and manual backup options are provided to secure all transaction data. Backups are encrypted (AES 256-bit) and can be stored on USB drives or across secure wide-area networks, ensuring that data can be restored in case of equipment failure or loss.

5.4. Diagnostics:

The system includes a diagnostics module that allows users to test and verify the functionality of all connected components. It generates status reports, identifying malfunctioning parts and providing details like the identification number of the kit and the malfunctioning component.

5.5. Software Updates:

The system includes an update module, allowing software to be updated via USB drives or remotely through a secure FTP site. This ensures that the system remains current with new features, security patches, or performance improvements, without reinstalling the entire system.

6. Voter Registration Module

6.1. RegistrationRegistration and Data Capture:

Allows for the registration of voters, capturing necessary personal details (name, ID number, photo, etc.) and biometric data (e.g., fingerprints).

6.2. Objection Handling:

Provides functionality for objections against the inclusion of names in the voter register, with automated processes for approval or rejection.

6.3. Data Validation:

Ensures the integrity of the captured data with validation rules, ensuring compliance with legal standards.

6.4. Support for Data Import/Export:

Enables the import of data (e.g., voter lists) and export to central repositories securely using encryption (AES 256-bit).

6.5. Audit Trail:

Keeps logs of actions taken during the registration process, ensuring transparency and accountability.

6.6. User Role Management:

Differentiated access rights for various roles such as administrators, data entry operators, and voters.

7. Candidate Nomination Capture System

7.1. Nomination Management:

Facilitates the capture of candidate nominations for various election positions, including presidential, national assembly, and council elections.

7.2. Support for Multiple Nominations:

Handles nominations for different levels and positions, such as presidential, national assembly, mayoral, and councillor.

7.3. Data Verification:

Ensures candidate details are verified, including support for uploading documents like photos, identification, and nomination forms.

7.4. Dynamic Workflow:

Supports multiple workflows for nomination processing, allowing updates, amendments, and status tracking for each nomination.

7.5. Audit Logs and Reporting:

Tracks and logs each step of the nomination process, generating reports for audit purposes.

7.6. Customizable Data Entry:

Provides flexibility for capturing nomination-specific data, such as party affiliations, nomination dates, and support information.

8. Accreditation Management System

8.1. Accreditation Card Issuance:

Issues accreditation cards for election stakeholders (e.g., observers, political party agents, media), including key details such as personal information, event details, and security features (QR codes, watermarks).

8.2. Bulk Card Printing:

Supports the bulk printing of accreditation cards, including multiple cards per A4 sheet for efficiency.

8.3. API Integration:

Allows the automatic synchronization of local kit data with a remote central database via API, ensuring data consistency across the system.

8.4. Data Import/Export:

Facilitates importing and exporting data securely (AES 256-bit encryption) across local and wide-area networks.

8.5. Diagnostics and System Health Checks:

Provides tools for diagnosing issues with connected components, generating status reports, and identifying malfunctions.

8.6. Backup and Restore:

Offers data backup and restore functionality, both locally (via USB) and across secure networks, ensuring data recovery in case of failure.

8.7. Software Updates:

Enables software updates either via USB or remote FTP, ensuring the system remains up to date with necessary patches and enhancements.

8.8. Audit Trail and Security:

Maintains logs of all changes to data and system configurations for accountability, with event journaling and user credential tracking.

8.9. User Roles and Permissions:

Implements a role-based access control system to ensure that users have appropriate permissions for their specific functions (e.g., CEO, DEO, IT support).

9. Reporting and Analytics

9.1. Voter Turnout Analysis

The **Voter Turnout Analysis** module is designed to provide real-time insights into voter participation during elections. It integrates data from biometric devices and polling stations, analyzing turnout trends by region, gender, age group, and time intervals. The module features an interactive dashboard for election officials to monitor turnout percentages, identify low-performing areas, and compare current turnout against historical data. It supports the generation of detailed reports for audit and decision-making purposes. Data encryption ensures secure handling of turnout statistics, while export options allow seamless sharing with centralized election management systems for comprehensive analysis and post-election reviews.