Central Resource Dashboard (CRD) Project Documentation

Central Resource Dashboard (CRD) Project Documentation

Table of Contents

1. Project Overview

1.1 Introduction

The Central Resource Dashboard (CRD) is a comprehensive web-based resource management and reporting system designed specifically for the Maharashtra State Police to efficiently manage and track communication equipment, IT resources, and personnel. The system addresses critical needs for centralized data management, verification workflows, and secure reporting mechanisms.

Purpose:

- To create a single source of truth for all communication and IT resources across Maharashtra Police units
- To standardize data collection, verification, and reporting processes
- To enable data-driven decision-making through secure, verified information
- To maintain an auditable trail of resource management activities

Objectives:

- Implement a secure, role-based authentication system using government employee credentials (Sevarth ID)
- Establish a three-layer cross-verification system for equipment and personnel data
- Create an automated report generation and approval workflow with digital signatures
- Develop a comprehensive logging system for accountability and auditing
- Integrate data warehousing capabilities for historical analysis and business intelligence

1.2 Scope

Inclusions:

- Authentication and user management with role-based access control
- Equipment inventory management (radios, repeaters, handhelds, etc.)
- Personnel management with posting history and hierarchical relationships
- Three-layer verification system for equipment, personnel, and license records
- PDF report generation with digital signature verification
- Automated report routing and approval workflow
- Comprehensive logging and auditing system
- Data warehousing with ETL pipeline for historical analysis
- Future integration with Power BI for advanced analytics

1.3 Features & Functionalities

1. Authentication & Security

- Sevarth ID & Password Login (Government employee system)
- OTP Verification for approvals & sensitive actions
- Secure Persistent Login (90-day token-based authentication)
- Session Management (Admins can view & terminate active sessions)

2. Equipment & Personnel Management

- Equipment CRUD operations (radios, repeaters, handhelds, etc.)
- Personnel Management (Sevarth ID, posting history, unit hierarchy)
- Data Entry Locking: Users cannot edit submitted records

3. Cross-Verification System

- Verification Teams approve or edit-and-approve submitted data
- Three Cross-Verification Layers:
  - Equipment Verification (Matches physical records)
  - Personnel Verification (Confirms employee details & postings)
  - License Verification (Legal records cross-check)

4. Report Generation & Approval System

- PDF Reports with Digital Signature via OTP
- Auto-Forwarding of reports to higher authorities for approval
- Only approved reports are stored in the system

5. Logging & Auditing (Admin-Only Access)

- Tracks logins, data entries, approvals, and rejections
- Ensures accountability and data security

6. Data Warehousing & Analytics

- ETL Pipeline (Azure Data Factory) for extracting operational data from MySQL
- Data Warehouse Schema (Star Schema) for structured storage and historical analysis
- Future Power BI Integration for real-time dashboards and analytics

2. System Architecture & Design

2.1 Architecture Overview

The CRD system implements a three-tier architecture model that separates the presentation, application logic, and data storage layers:

1. **Client Layer** (Presentation Tier)
   - Web-based user interface built with HTML, CSS, JavaScript, and Bootstrap
   - Responsive design for access from different devices (desktop, laptop, tablet, mobile)
   - Role-specific dashboards and views
2. **Application Layer** (Logic Tier)
   - PHP-based backend (PDO for database connections)
   - Business logic for authentication, data processing, verification workflows
   - Report generation and digital signature implementation
   - Session management and security controls
3. **Data Layer** (Storage Tier)
   - Operational Database: MySQL (cPanel-hosted)
   - Data Warehouse: Azure Synapse Analytics
   - ETL Pipeline: Azure Data Factory
   - File Storage: PDF reports and system documents

2.2 System Diagrams

2.2.1 System Architecture Diagram

The system architecture diagram illustrates the complete technical infrastructure of the CRD system, including:

- Client devices (Desktop, Laptop, Tablet, Mobile)
- Web server (Apache)
- Application server (PHP 8.4)
- Database servers (MySQL, Azure Synapse)
- External services (OTP, Digital Signature)
- File storage and session cache components

2.2.2 Database Schema (ERD)

The Entity Relationship Diagram illustrates the database tables and their relationships, including:

- Equipment inventory tables
- Personnel and posting records
- Unit and deployment information
- Verification tables with finalization flags
- Report generation and approval tables
- Logging and auditing tables

2.2.3 User Flow Diagram

The user flow diagram demonstrates the paths different user roles take through the system:

- Authentication flows
- Equipment and personnel management
- Verification workflows
- Report generation and approval routing
- Administrative functions

2.2.4 Data Flow Diagram (DFD)

The DFD shows how data moves through the system:

- Level 0 (Context Diagram): Overall system interactions
- Level 1: Detailed processes including authentication, equipment management, personnel management, report generation, and verification workflows

2.2.5 Deployment Diagram

The deployment diagram illustrates how the system components are deployed across the hosting infrastructure:

- cPanel hosting environment
- Database server configuration
- File storage systems
- Backup mechanisms
- Integration with Azure services for data warehousing

3. Technology Stack

3.1 Frontend

- **HTML5/CSS3**: For page structure and styling
- **JavaScript**: For client-side interactivity
- **Bootstrap**: For responsive design and UI components

3.2 Backend

- **PHP (PDO)**: For server-side logic and database connectivity
- **PDF Generation Library**: For creating standardized PDF reports
- **Digital Signature API**: For enabling e-signatures on official reports
- **OTP Service**: For verification of sensitive actions (using D7 Networks API)

3.3 Database

- **Operational Database**: MySQL (cPanel-hosted)
- **Data Warehouse**: Azure Synapse Analytics
- **ETL Pipeline**: Azure Data Factory
- **Schema Design**: Normalized schema for operational data, Star schema for data warehouse

3.4 Hosting & Deployment

- **Web Server**: Apache (cPanel-hosted)
- **Version Control**: GitHub for source code management
- **Deployment**: Manual deployment via cPanel file manager or GitHub integration

- **Backup**: Daily automated database backups

3.5 Third-party Integrations

- **OTP Service**: D7 Networks API for secure verification of sensitive actions
- **Digital Signature Service**: For report authentication
- **Azure Synapse Analytics**: For data warehousing and analytics
- **Future Integration**: Power BI for advanced data visualization and dashboards

4. Directory Structure

```
pcit_crd/
├── app/
│   ├── login.php
│   ├── signup.php
│   ├── dashboard.php
│   ├── equipment_management.php
│   └── database.php
├── public/
│   ├── index.php
│   ├── css/
│   ├── js/
│   ├── images/
│   └── .htaccess
└── logs/
```

5. User Roles & Permissions

5.1 User Categories & Access Levels

1. **End Users (Unit-Level Data Entry Personnel)**
   - Can enter equipment & personnel data
   - Cannot edit data after submission
   - Can generate basic reports for their unit
2. **Moderators (Level 1-4)**
   - **Level 1 (Unit)**: First level verification, can make entries.
   - **Level 2 (District)**: District-level verification and consolidation
   - **Level 3 (Region)**: Regional verification, consolidation and reporting
   - **Level 4 (HQ)**: Headquarters-level verification, consolidation and final approval
3. **Specialized Branches**
   - **License Branch**: Verifies license-related information
   - **Store Branch**: Verifies inventory and equipment details
   - **Establishment Branch**: Verifies personnel information
4. **System Administrators**
   - Complete system access
   - User management capabilities

- Configuration control
- Access to logging and auditing functions

5.2 Role-Based Access Control (RBAC)

The RBAC system implements hierarchical access control based on user roles:

Role	Equipment Management	Personnel Management	Report Generation	Report Approval	Verification	User Management	System Confi
End User	Create Only	Create Only	Basic Reports	No	No	No	No
Level 1 Moderator	View, Edit	View, Edit	All Unit Reports	Unit Level	Unit Level	No	No
Level 2 Moderator	View, Edit	View, Edit	District Reports	District Level	District Level	No	No
Level 3 Moderator	View	View	Region Reports	Region Level	Region Level	No	No
Level 4 Moderator	View	View	State Reports	State Level	State Level	No	No
License Branch	View, Verify	No	License Reports	No	License Data	No	No
Store Branch	View, Verify	No	Store Reports	No	Equipment Data	No	No
Establishment Branch	No	View, Verify	Personnel Reports	No	Personnel Data	No	No
Administrator	Full Access	Full Access	All Reports	All Levels	All Types	Full Access	Full Access

6. Database Schema & Data Management

6.1 Tables & Relationships

Core Tables:

1. **User_Roles**
   - ID (PK)
   - Role_Name
   - Access_Level (for role-based access control)
2. **Employee**
   - UID (PK)
   - Sevarth_ID
   - First_Name, Last_Name
   - Personal Details (Father_Name, Mother_Name, Spouse_Name)
   - DOB
   - Mobile_Number
   - Email_ID
   - Aadhar_Number
   - Retirement_Date (Auto-generated)
   - Current_Posting (FK to posting)
   - Login_User_Role (FK to user_roles)
   - Reporting_Person (FK to employee - self-referencing)

- Verification_Status (Boolean - verified by admin after sign-up)
- Password_Hash (Secure password storage)
- Last_Login (Timestamp)

3. **Equipment_Status**
   - ID (PK)
   - Name (Working/Non-working/Theft/Damage)
4. **Equipment**
   - UID (PK)
   - Serial_Number
   - Make (separate field for better clarity)
   - Model (separate field for better clarity)
   - Modulation_Type (Digital/Analog/Trunking)
   - Freq_Band (UHF/VHF/400/800)
   - Equipment_Type (Radio Set/Handheld/Repeater)
   - Status (FK to equipment_status)
   - Deployment_ID (FK to deployment)
   - Unit_ID (FK to unit)
   - Created_By (FK to employee)
   - Locked (Boolean)
   - Note: License, Inventory, and Purchase Information fields to be added later
5. **Unit**
   - Unit_ID (PK)
   - Unit_Name
   - Location Details (Latitude, Longitude)
   - Unit_Photo
   - Unit_Description
   - Unit_Incharge (FK to employee)
   - SP, DySP, PI, PSI (FK to employee)
6. **Deployment**
   - Deployment_ID (PK)
   - Name
   - Deployment_Type
   - Height_of_Mast
   - Type_of_Mast (SSM/Lattice)
   - Location (coordinates)
7. **Posting**
   - UID (PK)
   - Sevarth_ID (FK to employee)

- Posting_Unit (FK to unit)
- Joining_Unit_Date
- Relieve_Unit_Date
- Post (FK to post_types)
- Sub_Post (FK to sub_post_types)

8. **Personnel_Info** (New Table)
   - UID (PK)
   - Sevarth_ID
   - Employee Details (consolidated from employee table)
   - Posting Details (consolidated from posting table)
   - Retirement_Date (Auto-generated)
   - Unit_Posting_Details

Verification Tables:

1. **Equipment_Verification**
   - ID (PK)
   - Equipment_ID (FK to equipment)
   - Verified_By (FK to employee)
   - Status (Verified/Pending/Mismatch)
   - Finalized (Boolean)
   - Verification_Date
2. **Personnel_Verification**
   - ID (PK)
   - Employee_ID (FK to employee)
   - Verified_By (FK to employee)
   - Status (Verified/Pending/Mismatch)
   - Finalized (Boolean)
   - Verification_Date
3. **License_Verification**
   - ID (PK)
   - Equipment_ID (FK to equipment)
   - Verified_By (FK to employee)
   - Status (Verified/Pending/Mismatch)
   - Finalized (Boolean)
   - Verification_Date

Supporting Tables:

1. **Post_Types** and **Sub_Post_Types**
   - ID (PK)
   - Name

- Description/Priority

System Tables:

1. **Logs**
   - ID (PK)
   - User_ID (FK to employee)
   - Action_Type (Login/Data Entry/Report Generation/Approval)
   - Timestamp
   - IP_Address
   - User_Agent
2. **Reports**
   - ID (PK)
   - Generated_By (FK to employee)
   - Generated_Date
   - Report_File_Path
   - Is_Signed (Boolean)
   - OTP_Verified (Boolean)
   - Sent_Date

6.2 Data Flow & Integrity Rules

1. **Data Entry Process**
   - End users create equipment and personnel records
   - Once submitted, records are locked for editing by the original user
   - Records enter the verification workflow
2. **Verification Workflow**
   - Three parallel verification processes:
     - Equipment verification (physical records)
     - Personnel verification (employee records)
     - License verification (legal documentation)
   - Verification teams can either approve directly or edit-and-approve
   - Once verified and finalized, records cannot be modified
3. **Data Integrity Rules**
   - Foreign key constraints ensure referential integrity
   - Required fields validation enforces data completeness
   - Status tracking fields ensure proper workflow progression
   - Finalization flags prevent unauthorized modifications
   - Audit logs maintain a record of all changes

7. Security & Compliance

7.1 Authentication & Authorization

1. **User Authentication**
   - Sevarth ID & Password (Government employee credentials)
   - OTP verification via D7 Networks API for sensitive actions and approvals
   - 90-day persistent login with secure token-based authentication
   - Password policies enforcing complexity and regular changes
   - Password storage using secure hashing algorithms (password_hash)
   - Admin approval required for new user registrations (verification_status in employee table)
2. **Session Management**
   - Secure session handling with expiration controls
   - Administrative visibility of active sessions
   - Ability to terminate sessions remotely
   - Automatic timeout for inactive sessions
   - Session tracking with last_login timestamp in employee table
3. **Authorization Controls**
   - Role-based access control (RBAC) with predefined access_level in user_roles table
   - Hierarchical approval workflows based on reporting_person relationship
   - Function-level permission checks
   - Data-level access restrictions
   - Self-referencing foreign key for hierarchical reporting structure

7.2 Data Encryption & Protection

1. **Transport Security**
   - HTTPS/TLS for all communications
   - Secure API endpoints for external services (D7 Networks OTP API)
   - Protected routes requiring authentication
2. **Data Security**
   - Hashed passwords with strong algorithms (replacing deprecated methods)
   - Encrypted sensitive personal information
   - Secure storage of authentication tokens
   - Input validation and sanitization to prevent SQL injection
   - Data entry locking (locked flag in equipment table) to prevent unauthorized modifications
3. **Report Security**
   - Digital signatures for verification
   - OTP-based approval of official reports
   - Secure PDF generation and storage
   - Finalization flags in verification tables to prevent data tampering

7.3 Session Management & Logging

1. **Session Controls**
   - Token-based authentication with secure cookies

- IP-based session validation
- Browser fingerprinting for additional security
- Concurrent session limitations
- Improved error handling for failed authentication attempts

2. **Activity Logging**
   - Comprehensive audit trail of all user actions
   - Login/logout tracking with timestamp and user information
   - Data modification logging
   - Report generation and approval tracking
   - IP address and user agent tracking for security analysis

7.4 Security Implementation Updates

1. **Authentication Enhancements**
   - Switched from TextBelt API to D7 Networks API for OTP verification
   - Added OTP expiration and re-verification mechanisms
   - Implemented detailed error handling for failed API requests
   - Enhanced input validation with client-side and server-side checks
2. **Admin Approval Process**
   - Added verification_status flag in employee table
   - New users cannot log in until approved by an administrator
   - Enhanced password validation with real-time strength checks
   - Auto-formatting for sensitive data (like Aadhar number)
3. **Database Security**
   - Optimized schema to enforce referential integrity through foreign keys
   - Implemented finalization flags to prevent unauthorized data changes
   - Added data entry locking mechanisms
   - Enhanced status tracking for security auditing
4. **Error Handling & Security Logging**
   - Added detailed error logs and debugging mechanisms
   - Resolved deprecated security function warnings (FILTER_SANITIZE_STRING)
   - Enhanced input validation and error reporting
   - Structured error handling for API interactions

8. Report Generation & Workflow

8.1 Report Types

1. **Equipment Reports**
   - Inventory by unit, type, status
   - Equipment deployment reports
   - Maintenance and status reports

- Reports filtered by equipment status (Working/Non-working/Theft/Damage)

2. **Personnel Reports**
   - Unit staffing reports
   - Posting history reports
   - Retirement planning reports (using auto-generated retirement dates)
   - Hierarchical reporting structure reports
3. **Combined Reports**
   - Equipment-personnel allocation reports
   - Verification status reports
   - Compliance and audit reports
   - Unit performance and resource utilization reports

8.2 Approval Process

1. **Report Generation**
   - User selects report type and parameters
   - System generates draft report in PDF format
   - User reviews draft report before submission
   - Locked data ensures report integrity
2. **Digital Signature Process**
   - System sends OTP to user's registered mobile via D7 Networks API
   - User enters OTP to verify identity
   - System applies digital signature to PDF
   - Signed report is stored in the system with verification status
3. **Approval Workflow**
   - Signed reports are automatically forwarded to the appropriate higher-level moderator
   - Hierarchical approval chain: Unit → District → Region → Headquarters
   - Each level can approve or return for corrections
   - Final approved reports are stored as official records
   - Reporting follows the established hierarchy via reporting_person relationship

8.3 Export Formats

1. **Primary Format**
   - PDF with digital signature
   - Secured and verified through OTP authentication
2. **Additional Formats (For Internal Use)**
   - CSV for data analysis
   - Excel for tabular reporting
   - HTML for web viewing
   - Data exports filtered based on user's role and permissions

9. Deployment & Hosting

9.1 Server Setup

1. **Web Server Configuration**
   - Apache on cPanel hosting
   - PHP 8.x configuration
   - MySQL database setup
   - SSL certificate installation
   - Optimized PHP settings for security and performance
2. **Security Configurations**
   - Firewall rules and access controls
   - IP whitelisting for remote MySQL access
   - File permission hardening
   - SSL/TLS configuration
   - Enhanced error handling and logging

9.2 Version Control & Deployment

1. **GitHub Integration**
   - Repository structure and organization
   - Branch management strategy
   - Collaborative development workflow
   - Code review process
   - Documented code changes and updates
2. **Deployment Process**
   - Manual deployment via cPanel file manager
   - GitHub integration for push-based deployment
   - Configuration management across environments
   - Database migration procedures
   - Security testing before production deployment

9.3 Backup & Recovery

1. **Backup Strategy**
   - Daily automated database backups
   - Weekly full system backups
   - Offsite backup storage
   - Regular backup testing
   - Version-controlled configuration files
2. **Recovery Procedures**
   - Database restoration process
   - Application recovery steps

- Point-in-time recovery options
- Disaster recovery documentation
- Data integrity verification after restoration

10. Logging & Auditing

10.1 Activity Logs

1. **User Activity Logging**
   - Login/logout events with timestamps and IP addresses
   - Data creation, modification, and deletion tracking
   - Report generation and submission
   - Approval actions
   - OTP verification attempts and results
2. **System Logs**
   - Application errors and exceptions
   - Performance metrics
   - Security events
   - Integration service calls
   - API interaction success/failure tracking

10.2 Error Handling & Debugging

1. **Error Management**
   - Structured error logging
   - User-friendly error messages
   - Administrative error notifications
   - Detailed debug information (admin-only)
   - Enhanced debugging tools for development environment
2. **Monitoring**
   - Performance monitoring
   - Security monitoring
   - Database query monitoring
   - API call tracking
   - Resource utilization tracking

11. Data Warehousing & ETL

11.1 ETL Pipeline

1. **Data Extraction**
   - Azure Data Factory configuration
   - Scheduled data extraction from operational MySQL database
   - Delta extraction for incremental updates

- Data validation during extraction

2. **Data Transformation**
   - Data cleansing and normalization
   - Dimensional modeling transformations
   - Calculated metrics and aggregations
   - Historical change tracking
3. **Data Loading**
   - Incremental loading to Azure Synapse Analytics
   - Data partitioning strategies
   - Loading validation and error handling
   - Historical data management

11.2 Data Warehouse Schema

1. **Star Schema Design**
   - Fact Tables:
     - Equipment Facts
     - Personnel Facts
     - Verification Facts
     - Report Generation Facts
   - Dimension Tables:
     - Date Dimension
     - Unit Dimension
     - Equipment Type Dimension
     - Personnel Dimension
     - Status Dimension
2. **Analytics Infrastructure**
   - Azure Synapse Analytics configuration
   - Query optimization strategies
   - Performance tuning considerations
   - Data refresh schedules
3. **Future Power BI Integration**
   - Dashboard design plans
   - Report templates
   - Data model integration
   - User access controls

12. Future Enhancements & Scalability

12.1 Planned Features

1. **Advanced Analytics**

- Power BI integration for interactive dashboards
- Predictive maintenance for equipment
- Resource optimization analytics
- Trend analysis and forecasting

2. **Mobile Application**
   - Native mobile app for field operations
   - Offline capability for remote areas
   - Mobile-specific workflows
3. **Advanced Integration**
   - Integration with other government systems
   - GPS tracking for mobile equipment
   - Automated inventory reconciliation

12.2 Performance Optimization

1. **Database Optimization**
   - Query optimization
   - Indexing strategies
   - Caching implementation
   - Scheduled maintenance procedures
2. **Application Scalability**
   - Load balancing considerations
   - Horizontal scaling options
   - Performance monitoring and tuning
   - Resource allocation strategies

13. Troubleshooting & FAQs

13.1 Common Issues & Solutions

1. **Authentication Issues**
   - OTP delivery problems: Verify phone number, check network connectivity
   - Login failures: Check Sevarth ID, reset password if necessary
   - Session expiration: Re-login, check browser cookie settings
2. **Data Entry Problems**
   - Submission errors: Verify all required fields, check for format issues
   - Unable to edit: Confirm if record is locked, contact moderator if correction needed
   - Verification rejections: Review feedback, correct data, and resubmit
3. **Report Generation Issues**
   - PDF generation failures: Check data completeness, try alternative browser
   - Digital signature errors: Verify OTP delivery, confirm mobile number
   - Approval process delays: Contact relevant moderator, check workflow status

13.2 Debugging Guidelines

1. **For End Users**
   - Clear browser cache and cookies
   - Try alternative browsers
   - Document exact error messages
   - Contact unit administrator with details
2. **For Administrators**
   - Check server error logs
   - Verify database connectivity
   - Test authentication services
   - Review recent system changes
   - Check external service integrations
   - Monitor server resource usage (CPU, memory, disk space)
   - Verify SSL certificate validity and expiration
   - Ensure proper file permissions on critical system files
   - Review database query performance for bottlenecks
   - Test backup and restoration procedures regularly
3. **For System Developers**
   - Enable detailed debugging logs in development environment
   - Implement comprehensive error handling with meaningful messages
   - Utilize error tracking and monitoring tools
   - Maintain comprehensive documentation of system dependencies
   - Follow established code review processes for all changes
   - Implement automated testing for critical system components
   - Document all configuration changes with timestamps and reasons
   - Maintain a development changelog for tracking system modifications
4. **Escalation Procedures**
   - Define clear escalation paths for different types of issues
   - Establish severity levels and appropriate response times
   - Document contact information for all responsible parties
   - Implement notification system for critical failures
   - Maintain an issue tracking system with resolution documentation
   - Conduct regular review of recurring issues for systemic improvements
   - Schedule post-incident analyses for major system failures
5. **Performance Troubleshooting**
   - Monitor response times for critical operations
   - Implement database query optimization for slow-performing reports
   - Analyze server logs for resource-intensive operations

- Conduct regular performance testing under various load conditions
- Implement caching strategies for frequently accessed data
- Document baseline performance metrics for comparison
- Schedule regular maintenance windows for system optimization

---