جامعة عفت

EFFAT UNIVERSITY

CS 3151 - Software Engineering

Final Project - Spring 2025

MyPLC: AI-Powered Powerline Communication

Celine Al Harake - Layal Canoe - Rzan Hamid
S22107613 - S22107598 - S18105018

Instructor: **Dr. Passent Elkafrawy**

Contents

1 Project Description

This project aims to develop an AI-driven security and optimization system for Powerline Communication (PLC) networks. PLC technology allows data transmission over electrical wiring, making it essential for smart homes, businesses, and industrial environments. However, security threats, network interference, and lack of real-time monitoring present challenges for users.

Our solution will feature a mobile app (iOS & Android) and a web dashboard that enables users to monitor their PLC networks in real time, detect unauthorized access, optimize bandwidth, and receive AI-powered security alerts. Key features include intrusion detection, automated threat response, network performance optimization, and intelligent device management. By integrating artificial intelligence, this system will enhance the security, stability, and efficiency of PLC networks, ensuring a safer and more reliable experience for users. The project will be developed over a 12-month timeline, progressing through research, AI model training, software development, testing, and deployment.

2 Analysis Phase

2.1 Feasibility Study

To evaluate the practicality of implementing our AI-powered Powerline Communication System, we examined several key feasibility aspects: process feasibility, budget and time estimation, market analysis, and the business model canvas. Together, these dimensions confirm that the project is achievable within the academic semester and meets a real-world technological demand.

2.1.1 Process Feasibility

The process feasibility evaluates whether the proposed system could be realistically developed using current technologies.

The project envisions a smart monitoring system for PLC networks that uses artificial intelligence to detect security threats and optimize data transmission. The following components are planned:

- **AI Model:** The team proposes using Python-based tools (e.g., scikit-learn) to simulate an AI model capable of detecting anomalies in PLC network traffic.
- **Simulated Network Monitoring:** It is proposed that the system will simulate PLC network data, allowing the AI model to analyze patterns and detect irregular behavior.
- **Mobile App Interface:** A React Native-based mobile application is envisioned to display real-time security alerts, device activity, and network status.
- **System Integration:** The proposed plan includes integrating the backend, AI logic, and frontend interface to form a seamless, interactive system.

The project would follow **Agile development** principles, incorporating iterative development and regular team collaboration to manage scope and deliverables.

2.1.2 Budget and Time Estimation

Budget Estimation: Although this project is hypothetical, the following cost estimates reflect what would be required if we were to actually implement the system. The estimations are based on real-world prices from platforms such as Upwork, Toptal, Glassdoor, Amazon, Firebase, Namecheap, and TP-Link.

Category	Item/Description	Estimated Cost(USD)
Personnel	Software Engineer (1 x $30/hr x 160 hrs)	$4,800
	AI/ML Engineer (1 x $35/hr x 120 hrs)	$4,200
	UI/UX Designer (1 x $25/hr x 80 hrs)	$2,000
	Project Manager (1 x $35/hr x 40 hrs)	$1,400
Hardware	PLC Testing Hardware Kits	$1,500
	Development Laptops or PCs	$2,000
	IoT/Embedded Devices (for simulation or edge computing)	$1,000
Software & Services	Cloud Hosting	$300
	Domain Name + SSL + DNS setup	$50
	Backend Infrastructure	$150
	Firebase (Authentication, Notifications, Realtime DB)	$100
Design Tools	Figma Professional Plan	$144/year
Security Services	Network security monitoring APIs, penetration testing tools	$500
Marketing & Legal	Branding, logo, basic website, legal fees, privacy policy	$800
Testing & QA	Device testing, compatibility tests, user feedback collection	$500
Total Cost		around $19,744

Table 1: Budget Estimation

Time Estimation: Assuming the project is carried out over a 12-month timeline, the estimated time for each phase is broken down below. This schedule is hypothetical and designed to simulate a realistic workload.

Phase	Task Description	Estimated Duration
Planning & Research	Project scope definition, market research, technology stack selection	months 1-5
UI/UX Design	Wireframes, user flow diagrams, high-fidelity prototypes	months 5-8
Frontend Development	Implementing the UI using React.js & React Native	months 6-10
Backend Development	Building backend APIs, database models, and server logic (Python/Node.js)	months 6-10
Security & Optimization	Implementing AI models, threat detection, and optimization algorithms	months 6-10
Integration & Testing	System integration, functional and non-functional testing	months 10-12
Deployment	Final deployment to cloud infrastructure, production monitoring setup	months 11-12
Total Duration		12 months

Table 2: Time Estimation

2.1.3 Market Analysis

Our project addresses a real and emerging market concern; the need for intelligent security and optimization solutions for PLC networks. It suggests that a real-world version of the proposed system could have relevance in both academic and industrial contexts.

Key Market Insights:

- PLC technology is increasingly used in smart homes, smart grids, and industrial automation due to its use of existing electrical infrastructure.
- However, PLC networks are vulnerable to data loss, interference, and potential security breaches.
- The integration of AI in cybersecurity is a rapidly growing field, highlighting a need for research and development in this area.

2.1.4 Hardware and Software Requirements

Hardware Requirements:

Component	**Requirements**
Processor (CPU)	Intel Core i5 or higher
Memory (RAM)	8 GB or higher
Storage	256 GB SSD or higher
Network Adapter	Dual-band Ethernet/Wi-Fi adapter
Additional Devices	PLC Adapters, IoT-compatible Smart Plugs
Mobile Devices	Android/iOS smartphone

Table 3: Hardware Requirements

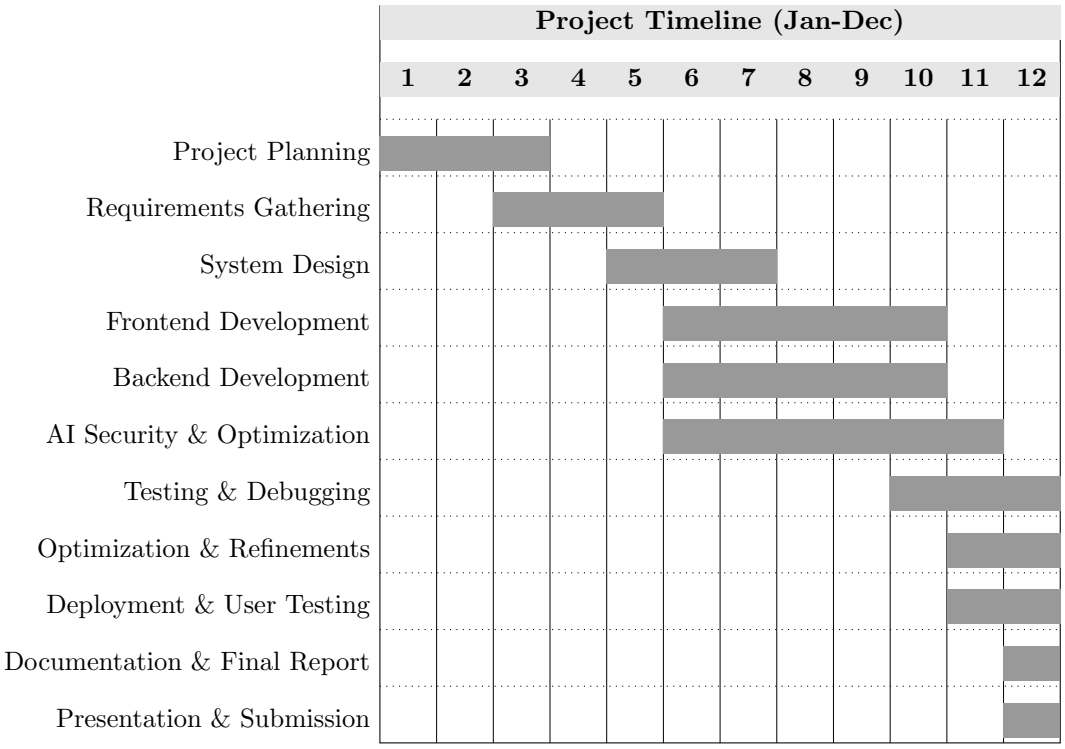
Software Requirements:

Software	**Purpose**
React Native	Cross-platform mobile app development
React.js	Web dashboard and admin panel development
Node.js / Python	Backend server and API handling
MongoDB / MySQL	Database for user and network data storage
Docker	Containerization of services (optional)
VS Code / IntelliJ	Code editor / IDE
Postman	API testing
Git / GitHub	Version control
Figma / Adobe XD	UI/UX Design (optional for frontend polish)
Wireshark	Network traffic analysis and monitoring
PLC Simulation Tools	To emulate and test PLC network behavior
Trello / Jira	Task management and agile workflow

Table 4: Software Requirements

2.1.5 Gantt Chart

The Gantt chart provides a visual timeline of project activities, displaying the sequence, duration, and dependencies of tasks involved in developing the project. This structured timeline ensures smooth execution, allowing for effective time management and team coordination.



2.2 Requirements Specification (RSS)

2.2.1 Requirements List

- **RQ1. Real-Time Device Monitoring:** The system shall display all active devices connected to the PLC network with their IP and MAC addresses within 2 seconds of connection.
- **RQ2. Device Access Control:** Users shall be able to block or allow specific devices on the PLC network through the app, with changes taking effect within 5 seconds.
- **RQ3. AI-Based Threat Detection & Prevention:** The system shall use AI to analyze network traffic and detect unauthorized access or abnormal activity with 95% accuracy within 5 seconds of occurrence.
- **RQ4. Security Alerts & Notifications:** The system shall send real-time alerts (push, email, or in-app) to users within 3 seconds of detecting unauthorized access or security threats.
- **RQ5. Automated Network Optimization:** The system shall detect interference sources and adjust bandwidth allocation automatically, reducing network latency by at least 20% in real time.
- **RQ6. User Dashboard:** The system shall provide a responsive and intuitive dashboard displaying real-time performance stats, device status, and security logs within 1 second of launch.
- **RQ7. Weekly Reports & Logging:** The system shall generate downloadable weekly reports summarizing security events, device activity, and performance. It shall also log all device connections and disconnections with timestamps.

- **RQ8. Energy Usage Tracking:** The system shall track and display energy consumption of each connected device and the total network usage, viewable by all users.
- **RQ9. User Authentication & Roles:** The system shall support secure user login and role-based access (admin and regular user).
- **RQ10. Platform Compatibility:** The app shall be accessible via web, Android, and iOS, ensuring users can connect from multiple devices.
- **RQ11. Data Protection & Encryption:** The system shall encrypt all sensitive data and comply with security regulations. Multi-factor authentication shall be implemented for admin accounts.
- **RQ12. Performance & Scalability:** The system shall support at least 1000 concurrent device connections without performance degradation.
- **RQ13. Reliability & Availability:** The system shall ensure 99.9% uptime and maintain critical functions during partial system failures.
- **RQ14. Maintainability & Usability:** The system shall be built using modular, well-documented code and feature an intuitive UI requiring minimal user training.

2.2.2 Use Case List

- **UC1. User Authentication & Access:** Users log in securely via mobile/web. Access depends on roles (Admin/User).
  - **Preconditions:** The user has a registered account. A stable internet connection is available. The system supports secure protocols.
  - **Postconditions:** If credentials are valid, the user is logged in with access based on their role (Admin/User). If invalid, access is denied and an error message is shown.
- **UC2. Monitor Network & Devices:** View real-time connected devices, device logs, and energy usage stats.
  - **Preconditions:** The user is authenticated. Devices are connected to the PLC network. Energy reporting is enabled (for energy stats).
  - **Postconditions:** The user views live data on connected devices, energy usage, and device logs. No changes are made to the network.
- **UC3. Detect & Prevent Security Threats:** AI module detects suspicious activity and prevents unauthorized access.
  - **Preconditions:** The AI security module is running. Devices are actively communicating over the PLC network.
  - **Postconditions:** If threats are detected, they are blocked or quarantined. Logs are updated with threat details and actions taken.
- **UC4. Receive Security Notifications:** Users receive push/in-app/email alerts for network threats and activities.
  - **Preconditions:** Security monitoring is active. The user is registered and has enabled alert notifications.
  - **Postconditions:** The user receives a notification (push, email, or in-app). The alert is logged for future reference.
- **UC5. Manage Devices & Users:** Admins block/unblock devices and manage user accounts and roles.

  - **Preconditions:** The admin is authenticated and authorized. The target device/user exists in the system.
  - **Postconditions:** Devices are blocked/unblocked. User accounts are created, updated, or deactivated. System logs reflect the changes.

- **UC6. Optimize Network Performance:** AI module analyzes traffic and optimizes bandwidth dynamically.
  - **Preconditions:** Devices are connected and generating network traffic. Optimization is enabled.
  - **Postconditions:** Bandwidth is redistributed for optimal performance. Optimization metrics are logged.

- **UC7. Dashboard & Reporting:** Users and admins can view dashboards and download weekly reports.
  - **Preconditions:** The user is authenticated. System has logged sufficient activity and events.
  - **Postconditions:** The user views network statistics, device history, and energy trends. Weekly reports are generated and available for download.

2.2.3 Use Case Prioritization

Use Case ID	Use Case Name	Priority
UC1	User Authentication & Access	High
UC2	Monitor Network & Devices	High
UC3	Detect & Prevent Security Threats	High
UC4	Receive Security Notifications	High
UC5	Manage Devices & Users	Medium
UC6	Optimize Network Performance	Medium
UC7	Dashboard & Reporting	Medium

Table 5: Use Case Priority

2.2.4 User Stories

- **RQ1:** The system shall display all active devices connected to the PLC network with their IP and MAC addresses within 2 seconds of connection.
  - **Use Cases:** UC2: Monitor Network & Devices
  - **User Stories:**
    * As a user, I want to view connected devices in real time so that I can monitor the network.
    * As an admin, I want to see each device's IP and MAC address so that I can identify and track them accurately.

- **RQ2:** Users shall be able to block or allow specific devices on the PLC network through the app, with changes taking effect within 5 seconds.
  - **Use Cases:** UC5: Manage Devices & Users
  - **User Stories:**
    * As an admin, I want to block or allow devices so that I can control who uses the network.
    * As a user, I want to request device access changes so that I can maintain my privacy.

- **RQ3:** The system shall use AI to analyze network traffic and detect unauthorized access or abnormal activity with 95% accuracy within 5 seconds of occurrence.
  - **Use Cases:** UC3: Detect & Prevent Security Threats
  - **User Stories:**
    - As a user, I want the system to detect suspicious activity using AI so that threats are stopped before harm is done.
    - As an admin, I want AI-based threat detection so that I don't need to manually monitor traffic 24/7.
- **RQ4:** The system shall send real-time alerts (push, email, or in-app) to users within 3 seconds of detecting unauthorized access or security threats.
  - **Use Cases:** UC4: Receive Security Notifications
  - **User Stories:**
    - As a user, I want to receive immediate alerts when a threat is detected so that I can take action quickly.
    - As an admin, I want all threat alerts logged and sent automatically so I can review system security.
- **RQ5:** The system shall detect interference sources and adjust bandwidth allocation automatically, reducing network latency by at least 20% in real time.
  - **Use Cases:** UC6: Optimize Network Performance
  - **User Stories:**
    - As a user, I want the system to optimize bandwidth automatically so that my connection remains fast.
    - As an admin, I want AI to reduce latency during high traffic so that network quality is preserved.
- **RQ6:** The system shall provide a responsive and intuitive dashboard displaying real-time performance stats, device status, and security logs within 1 second of launch.
  - **Use Cases:** UC7: Dashboard & Reporting
  - **User Stories:**
    - As a user, I want to view a dashboard with live stats so that I can easily understand network health.
    - As an admin, I want to access detailed security logs from the dashboard so that I can track past events.
- **RQ7:** The system shall generate downloadable weekly reports summarizing security events, device activity, and performance. It shall also log all device connections and disconnections with timestamps.
  - **Use Cases:** UC7: Dashboard & Reporting
  - **User Stories:**
    - As a user, I want to download weekly reports so that I can keep records of network activity.
    - As an admin, I want connection logs with timestamps so I can audit device usage.
- **RQ8:** The system shall track and display energy consumption of each connected device and the total network usage, viewable by all users.
  - **Use Cases:** UC2: Monitor Network & Devices
  - **User Stories:**
    - As a user, I want to track energy usage of each device so I can manage power consumption.

    - As an admin, I want to monitor network-wide energy stats for reporting and optimization.

- **RQ9:** The system shall support secure user login and role-based access (admin and regular user).
  - **Use Cases:** UC1: User Authentication & Access
  - **User Stories:**
    - As a user, I want to securely log in so that my data and features are protected.
    - As an admin, I want to control who accesses the system based on user roles.

- **RQ10:** The app shall be accessible via web, Android, and iOS, ensuring users can connect from multiple devices.
  - **Use Cases:** UC1: User Authentication & Access
  - **User Stories:**
    - As a user, I want to access the app from any device so that I can manage the network conveniently.
    - As an admin, I want full control on both mobile and web platforms so I can act anytime, anywhere.

- **RQ11:** The system shall encrypt all sensitive data and comply with security regulations. Multi-factor authentication shall be implemented for admin accounts.
  - **Use Cases:** UC1: User Authentication & Access
  - **User Stories:**
    - As a user, I want my data to be encrypted so that no one else can see it.
    - As an admin, I want multi-factor login to protect administrative access.

- **RQ12:** The system shall support at least 1000 concurrent device connections without performance degradation.
  - **Use Cases:** UC6: Optimize Network Performance
  - **User Stories:**
    - As a user, I want the system to handle many devices so that my experience isn't affected by others.
    - As an admin, I want high scalability so I can deploy the system in large environments.

- **RQ13:** The system shall ensure 99.9% uptime and maintain critical functions during partial system failures.
  - **Use Cases:** UC3: Detect & Prevent Security Threats
  - **User Stories:**
    - As a user, I want the system to be available all the time so that I'm never left unprotected.
    - As an admin, I want core functions to keep working during failures so I can ensure continuity.

- **RQ14:** The system shall be built using modular, well-documented code and feature an intuitive UI requiring minimal user training.
  - **Use Cases:** UC7: Dashboard & Reporting
  - **User Stories:**
    - As a user, I want the interface to be simple and intuitive so that I can use it without training.
    - As a developer, I want the code to be modular and documented so that future updates are easy.

2.2.5 Traceability Matrix

The traceability matrix maps the functional requirements to their corresponding use cases to ensure comprehensive coverage. It helps verify that all requirements are addressed in the system design and implementation. By systematically linking each requirement to relevant use cases, the matrix ensures completeness, consistency, and alignment between the project's objectives and development tasks.

Req.	**UC1**	**UC2**	**UC3**	**UC4**	**UC5**	**UC6**	**UC7**
RQ1		✓					
RQ2					✓		
RQ3			✓				
RQ4				✓			
RQ5						✓	
RQ6							✓
RQ7							✓
RQ8		✓					
RQ9	✓						
RQ10	✓						
RQ11	✓						
RQ12						✓	
RQ13			✓				
RQ14							✓

2.2.6 User Types

1. **Admin:** The Admin has the highest level of control over the system. They manage users, configure system settings, and have full access to all modules. An admin can:
   - Add/edit/delete user accounts.
   - Block/unblock devices on the PLC network.
   - View and export all security logs and reports.
   - Monitor and optimize network bandwidth.
   - Access energy usage statistics.
   - Configure security settings and thresholds.
   - Receive and review all security alerts.
   - Generate weekly/monthly system-wide reports.
   - Full access via both web and mobile platforms.
2. **Regular User:** A standard user who interacts with the system primarily for personal usage insights and basic device control. A user can:
   - View real-time connected devices.
   - Receive security alerts related to their own devices.
   - View energy usage statistics.

- Access dashboard with limited visibility.
- Report suspicious activity to admin.
- Secure login via mobile or web.
- Cannot modify critical system configurations or user accounts.

3. **Network Security AI System:** Not a human user but a core intelligent system entity responsible for monitoring and reacting to threats. The AI system can:
   - Detect and prevent real-time threats.
   - Generate alerts and logs.
   - Optimize bandwidth automatically using Strategy Pattern.
   - Monitor device connection behavior and flag anomalies.
   - Notify users/admin of unusual activity.
   - Trigger security protocols without manual input.

2.2.7 Use Case Designs

1. **Use Case 1: User Authentication & Access**

   - **Use Case Description**
     - *Preconditions:*
       - The user has already registered with a valid account.
       - Internet connection is active.
       - The system is running and accessible via web or mobile.
     - *Basic Flow:*
       (a) The user opens the application.
       (b) The system displays the login screen.
       (c) The user enters their username and password.
       (d) The system validates the credentials.
       (e) If the credentials are correct, the user is logged in and directed to the dashboard.
       (f) Based on the role (Admin/User), different permissions and UI elements are loaded.
     - *Postconditions:*
       - The user is authenticated and logged in.
       - Role-based access is granted (Admin or User).
       - Login time and IP address are logged for security.
   - **User Scenario** A user opens the mobile application to check the device logs. They enter their username and password on the login screen. After successful authentication, they are directed to the main dashboard, where they can monitor the connected devices. As a regular user, they can view stats but cannot manage other users or block devices.
   - **Use Case Diagram**
     - Actors: Admin / User
     - Use Case: Log In / Access Dashboard / Access Admin Features
     - Relationship: Both Admin and User initiate the login process. After authentication, the system grants role-based access. Users access standard dashboard functionalities. Admins access both standard and admin-specific features like user/device management.

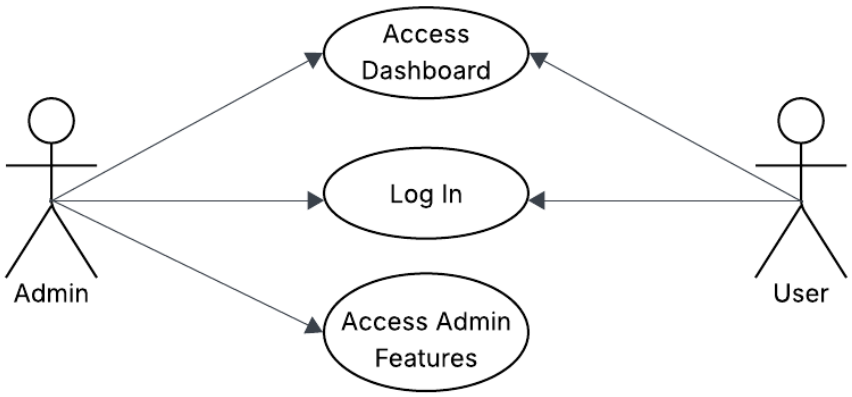


Figure 1: Use Case 1: User Authentication & Access

2. **Use Case 2: Monitor Network & Devices**

   - **Use Case Description**
     - *Preconditions:*
       - The user must be authenticated.
       - Devices must be connected to the PLC network.
       - Energy usage tracking must be enabled to view energy-related data.
     - *Basic Flow:*
       (a) User logs into the system.
       (b) User navigates to the dashboard or device monitoring page.
       (c) The system fetches and displays real-time data on: active devices, device logs, energy usage statistics.
       (d) User observes the data for monitoring purposes.
     - *Postconditions:*
       - No changes are made to the network.
       - The user gains awareness of device status, activity, and energy consumption.
       - The system may continue updating data in real-time.
   - **User Scenario** A regular user logs in and accesses the dashboard. They want to check if all their smart devices are connected and see how much energy each one has consumed today. They view a list of currently connected devices with details such as IP address and energy usage. The user notices a spike in energy usage for one device and decides to investigate further.
   - **Use Case Diagram**
     - Actors: Admin / User
     - Use Case: View Connected Devices / View Device Logs / View Energy Stats
     - Relationship: Both Admin and User can initiate the use case by accessing the dashboard. The system responds by displaying real-time network and energy monitoring data.

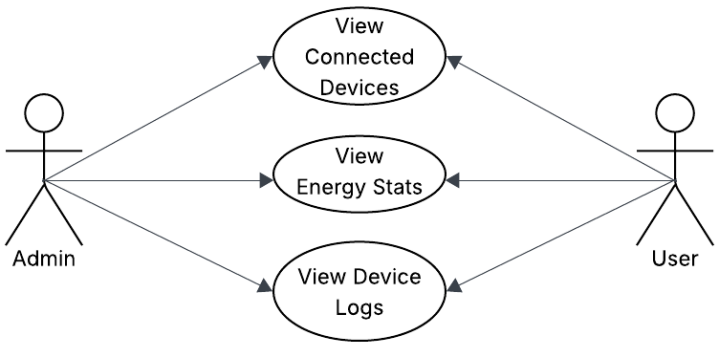


Figure 2: Use Case 2: Monitor Network & Devices

3. **Use Case 3: Detect & Prevent Security Threats**

- **Use Case Description**
  - *Preconditions:*
    - The PLC monitoring system must be actively running.
    - The user must be logged into the application.
    - Network threat detection must be enabled.
  - *Basic Flow:*
    (a) User opens the notification center or dashboard.
    (b) System checks for new security alerts generated by threat detection.
    (c) System displays alerts with timestamp, affected device, and threat type.
    (d) User can mark alerts as read, archive them, or take further actions (e.g., investigate or block devices).
  - *Postconditions:*
    - Alerts are acknowledged or archived.
    - Admin may take corrective security actions.
    - System updates alert logs in real time.
- **User Scenario** An Admin receives a push notification indicating a potential network intrusion attempt. Upon logging into the dashboard, they navigate to the "Security Alerts" section. They view the detailed alert message, including the source IP address and affected PLC device. The Admin immediately selects the "Block Device" option and archives the alert. The alert log is updated with a timestamp and action taken.
- **Use Case Diagram**
  - Actors: Admin / User
  - Use Case: Configure Alert Preferences / Receive Real-Time Alerts / Acknowledge or Act on Alerts
  - Relationship: Actor initiates the request to view security alerts / System responds by displaying all security alerts with relevant metadata / System allows the user to acknowledge, archive, or act on the alerts

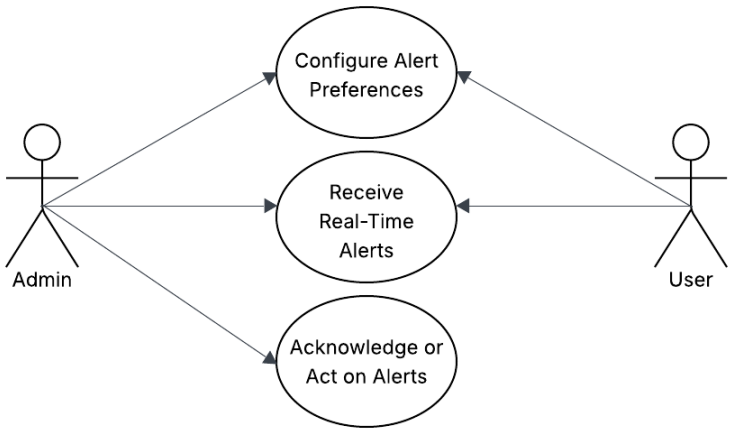


Figure 3: Use Case 3: Detect & Prevent Security Threats

4. **Use Case 4: Receive Security Notifications**

   - **Use Case Description**
     - *Preconditions:*
       * The PLC monitoring system must be running.
       * The user must be logged in.
       * Real-time notifications must be enabled.
     - *Basic Flow:*
       (a) AI system continuously monitors the PLC network.
       (b) When suspicious behavior is detected, a security alert is triggered.
       (c) The system pushes a real-time notification to the user's dashboard or device.
       (d) User opens the alert to review threat details (e.g., time, type, affected device).
       (e) User acknowledges or archives the alert and may take further action.
     - *Postconditions:*
       * Alerts are reviewed and archived.
       * User may initiate further investigation or mitigation.
       * System logs alert activity and user responses.
   - **User Scenario** A user receives a real-time push notification about suspicious behavior on one of the connected PLC devices. They tap on the alert and review the details: an unexpected IP address was attempting access. The user marks the alert as "Reviewed" and forwards it to the admin for investigation. The alert is then archived, and the system logs the user's response.
   - **Use Case Diagram**
     - Actors: User / Admin
     - Use Case: Monitor Network / Receive Real-Time Alert / Acknowledge or Archive Alert
     - Relationship: Actor receives system-generated alerts. System delivers alert data. Actor responds to or acknowledges alerts.

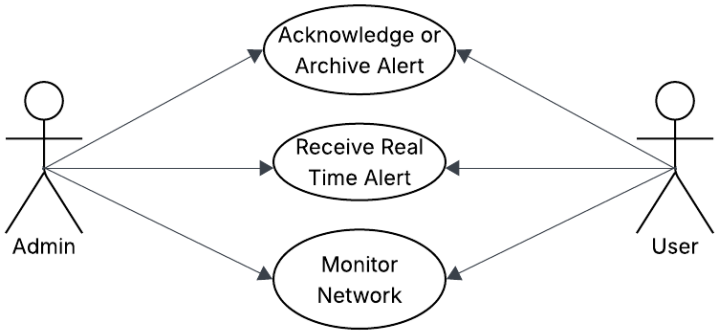


Figure 4: Use Case 4: Receive Security Notifications

5. **Use Case 5: Manage Devices & Users**

- **Use Case Description**
  - *Preconditions:*
    - The user must be logged into the system.
    - The user must have admin privileges.
    - The system must be actively connected to the PLC network.
  - *Basic Flow:*
    (a) Admin logs in and accesses the "Device Management" section.
    (b) The system displays a list of all connected PLC devices and user accounts.
    (c) Admin selects a device or user to manage.
    (d) Admin can perform actions such as: add a new device, remove a device, block/unblock user access, assign roles, or view device/user activity logs.
    (e) System updates changes in real time and confirms the action.
  - *Postconditions:*
    - Device/user records are updated.
    - Unauthorized or inactive devices/users are removed or blocked.
    - Audit logs reflect the management actions taken.
- **User Scenario** An Admin accesses the dashboard and navigates to the 'Device Management' section. They notice an unfamiliar device on the network. After reviewing the activity log, they determine it's unauthorized and select the 'Remove Device' option. The device is immediately disconnected, and a log entry is generated with the action details and timestamp. The Admin then assigns restricted access to a new user joining the network.
- **Use Case Diagram**
  - Actors: Admin
  - Use Case: View Device List / Manage Devices / Manage User Access
  - Relationship: Admin initiates device and user management tasks. System enables real-time updates and displays management confirmation. Admin actions trigger log updates for security purposes.

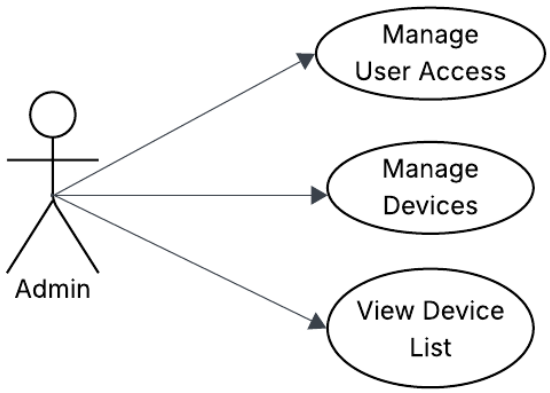


Figure 5: Use Case 5: Manage Devices & Users

6. **Use Case 6: Optimize Network Performance**
   - **Use Case Description**
     - *Preconditions:*
       - User is authenticated.
       - The PLC network is actively monitored.
       - Bandwidth usage data is available for analysis.
     - *Basic Flow:*
       (a) User accesses the network optimization feature from the dashboard.
       (b) System analyzes real-time bandwidth usage across connected devices.
       (c) System identifies bottlenecks or high-usage devices.
       (d) System suggests optimization actions (e.g., limit bandwidth to non-critical devices).
       (e) User confirms or modifies the optimization suggestions.
       (f) System applies bandwidth optimization settings.
     - *Postconditions:*
       - Network bandwidth is redistributed or optimized based on the system's AI analysis.
       - The user is notified of the changes made.
       - Action is logged for future reference.
   - **User Scenario** A user logs in and notices that their network is slower than usual. They navigate to the optimization tab, where the system shows which devices are consuming the most bandwidth. The system suggests limiting the bandwidth of a non-critical camera. The user approves, and the system reconfigures the bandwidth allocation, improving overall network speed.
   - **Use Case Diagram**
     - Actors: Admin / User
     - Use Case: Analyze Real-Time Bandwidth Usage / Identify Bandwidth Issues / Apply Optimization Settings / Log Optimization Activity
     - Relationship: Actor initiates the request to optimize bandwidth / System analyzes real-time usage and suggests optimizations / Actor approves and system applies changes to enhance performance

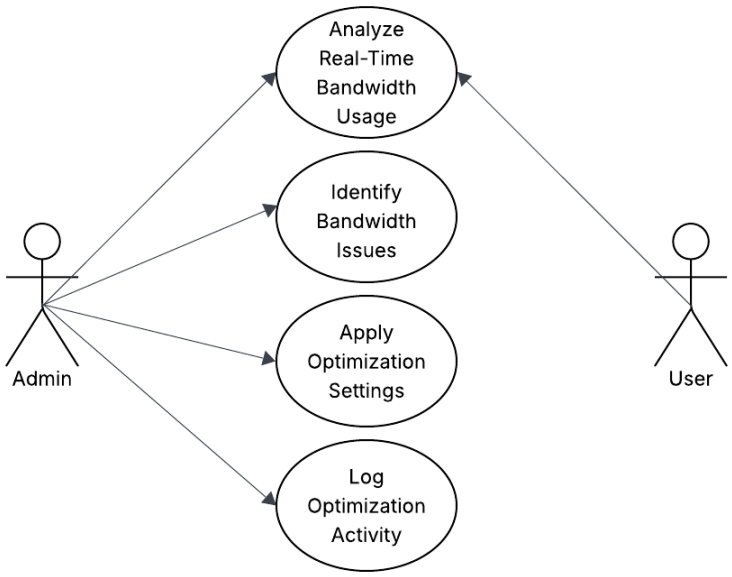


Figure 6: Use Case 6: Optimize Network Performance

7. **Use Case 7: Dashboard & Reporting**

- **Use Case Description**
  - *Preconditions:*
    - User or Admin must be logged in.
    - The PLC network must be actively monitored and logging data.
    - Dashboard and reporting modules must be enabled.
  - *Basic Flow:*
    (a) User navigates to the dashboard from the main menu.
    (b) System fetches real-time performance metrics, device statuses, and threat summaries.
    (c) User selects a report type (e.g., security log, performance, energy usage).
    (d) System generates a visual report (charts, tables, graphs).
    (e) User can download, print, or export the report.
  - *Postconditions:*
    - User reviews system health and performance insights.
    - Reports are optionally exported or printed.
    - System logs report generation actions for audit purposes.
- **User Scenario** An admin logs into the system and opens the dashboard to check the overall health of the PLC network. They select 'Security Logs' from the report options, and a visual report appears showing recent alerts, response actions, and timestamps. The admin downloads the report for monthly security review and saves a copy as PDF.
- **Use Case Diagram**
  - Actors: Admin / User
  - Use Case: View Dashboard / Generate Report / Export Report
  - Relationship: Actor initiates dashboard access. System visualizes real-time data and reports. Actor downloads or exports the report.

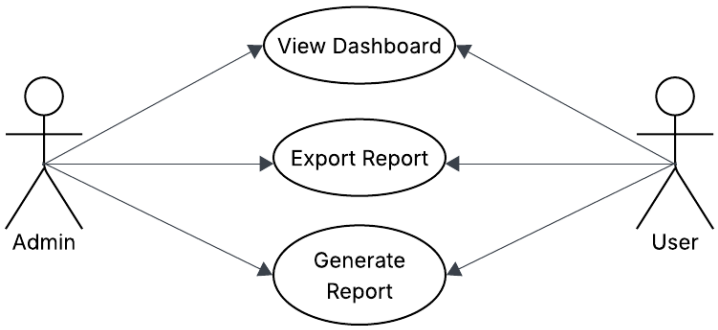


Figure 7: Use Case 7: Dashboard & Reporting

3 Design Phase

3.1 Context Diagram

The context diagram provides a high-level overview of the AI-Powered PLC System and its interactions with external entities. The system is at the core of the diagram, acting as a centralized platform that facilitates real-time monitoring, threat detection, network optimization, and user management across the PLC network. The system interfaces with four primary external entities:

1. **Admin:** The admin interacts with the system to perform high-level management tasks such as user account control, device configuration, and system monitoring. They can view detailed security alerts, access network statistics, and receive weekly reports generated by the system.
2. **Regular User:** Regular users authenticate through the system and are provided access to personalized dashboards, energy usage statistics, and optimization tools. They can view reports and receive real-time notifications regarding their connected devices or network status.
3. **PLC Devices:** These devices continuously transmit real-time data and security status to the system. In return, they receive commands related to bandwidth optimization and security actions, such as blocking or unblocking unauthorized devices.
4. **Mobile & Web Interface:** The mobile and web interfaces serve as the front-end access points through which users interact with the system. They enable login, visualization of reports and dashboards, notification delivery, and secure access to all system features, both remotely and on-site.

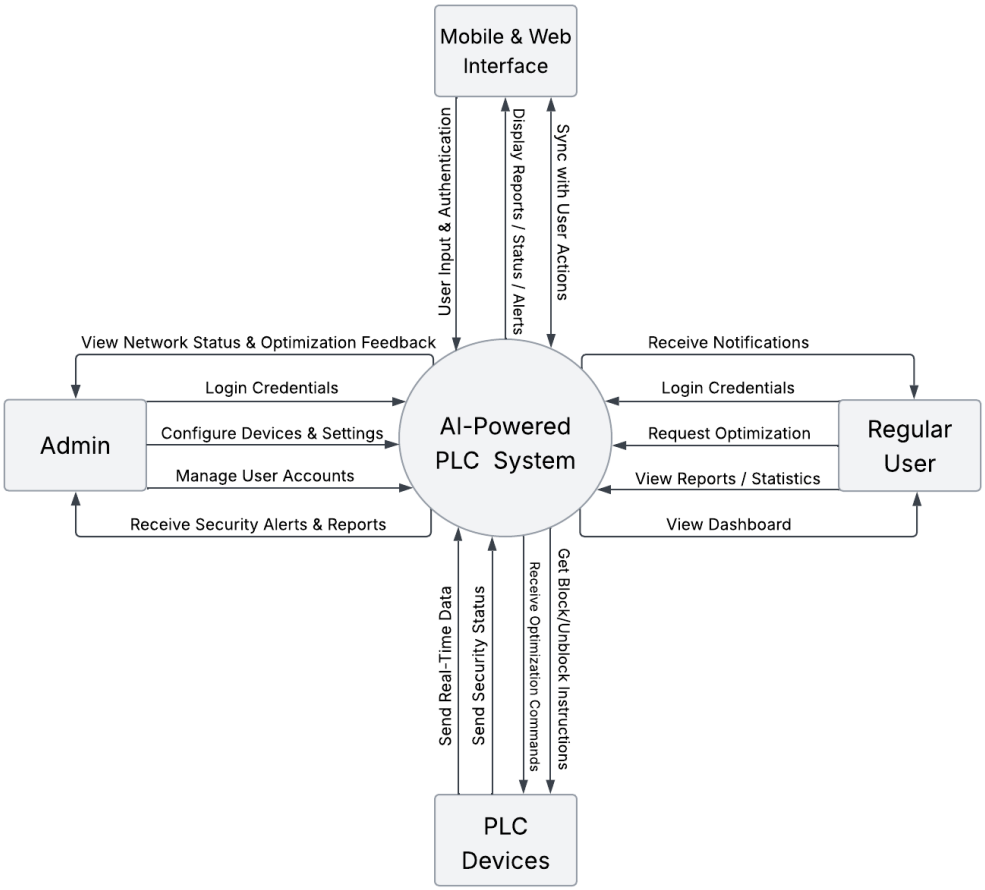


Figure 8: Context Diagram

3.2 UML Class Diagram

The UML class diagram outlines the key components of the AI-Powered PLC System and how they interact. It includes classes like **User**, **AuthenticationService**, and **Dashboard** to handle login, account management, and UI access for both Admins and Regular Users. The **Device** and **NetworkMonitor** classes manage connected devices, track their status, and monitor network activity.

Security is handled by the **SecurityManager**, which detects threats and works with **SecurityAlert** and **SecurityReport** to notify users and generate weekly summaries. The **EnergyUsageStatistics** class offer insights into energy consumption and device history. This structured design ensures each class has a clear responsibility, supporting system functionality, security, and optimization in a scalable way.

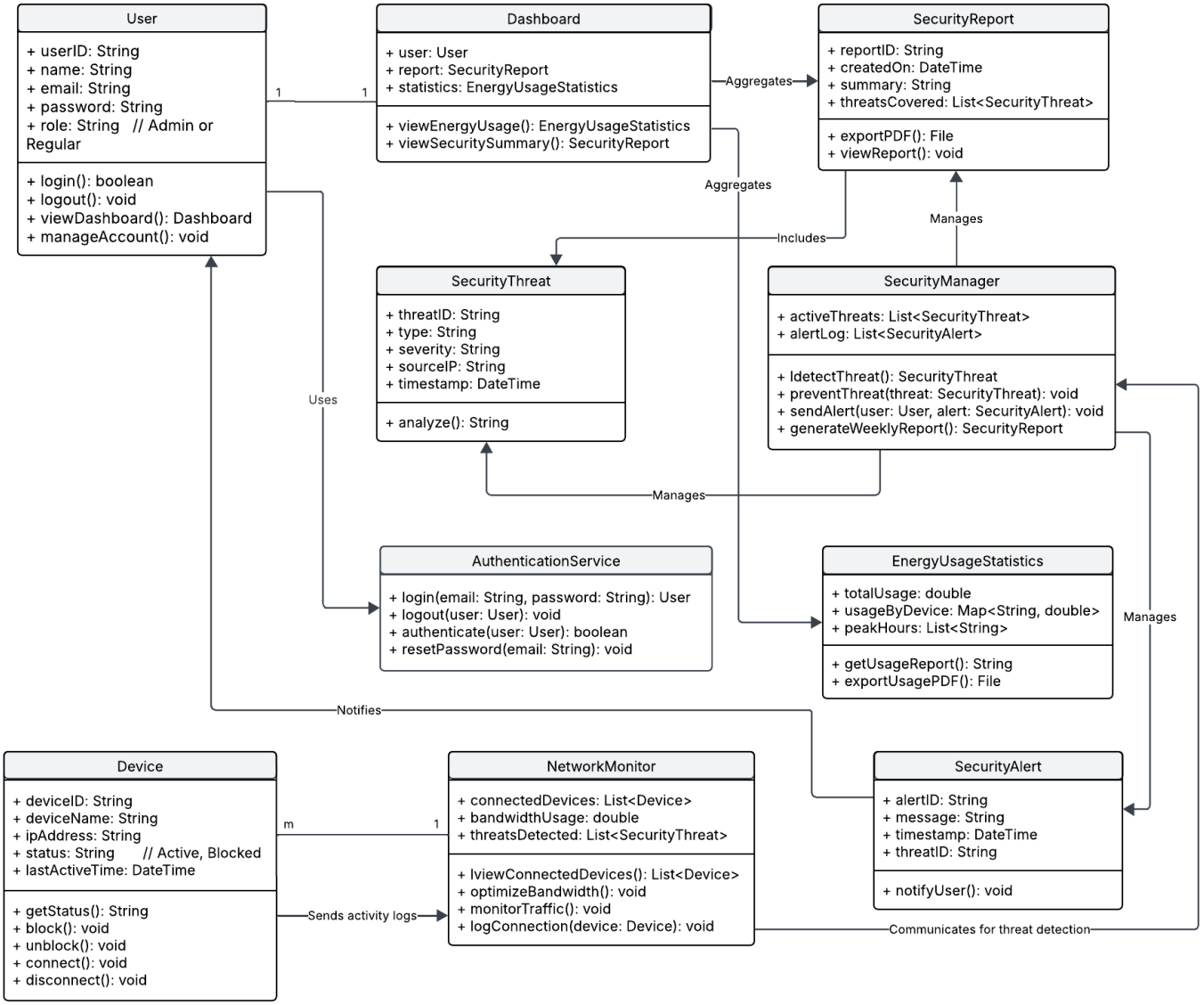


Figure 9: Class Diagram

3.3 Design Pattern

To enhance the modularity, scalability, and maintainability of the AI-powered PLC System, four essential design patterns were applied: Observer, Singleton, Factory, and Strategy.

1. **Observer Pattern:** It defines a one-to-many relationship between objects so that when one object changes state, all its dependents are notified and updated automatically.
    - **Usage in System:** Used in the real-time monitoring and alert modules. For example, when a new threat is detected, all relevant components (e.g., dashboard, alert manager, log system) are notified and respond accordingly.
2. **Singleton Pattern:** It ensures that a class has only one instance and provides a global point of access to it.
    - **Usage in System:** Used to manage central resources such as the network optimization engine and the security manager. This guarantees a consistent state and prevents conflicts from multiple instantiations.
3. **Factory Pattern:** It defines an interface for creating objects, but allows subclasses to alter the type of objects that will be created.
    - **Usage in System:** Used to create different types of user accounts (Admin, User), alert types, and report generators. This makes object creation more flexible and scalable.
4. **Strategy Pattern:** It defines a family of algorithms, encapsulates each one, and makes them interchangeable. This pattern lets the algorithm vary independently from clients that use it.
    - **Usage in System:** Applied to the bandwidth optimization module. Different optimization strategies (e.g., device-priority-based, time-based) can be switched without changing the system logic.

Design Pattern	**Definition**	**Usage in System**
Observer	Defines a one-to-many dependency so when one object changes state, all its dependents are notified and updated automatically.	Real-time alerts, dashboard updates, and device monitoring.
Singleton	Ensures a class has only one instance and provides a global access point to it.	Centralized control of the Security Manager and Optimization Engine.
Factory	Provides an interface for creating objects in a superclass, but allows subclasses to alter the type of created objects.	Dynamic creation of user roles, alert types, and report formats.
Strategy	Encapsulates interchangeable algorithms and allows them to be selected at runtime.	Swappable bandwidth optimization strategies (e.g., priority-based, time-based).

Table 6: Summary of the Design Patterns used in the System

3.4 ER Diagram

The ER diagram represents the key entities involved in monitoring and securing the PLC network. Core entities include **User**, **Device**, **SecurityAlert**, **LoginHistory**, **DeviceLog**, **Report**, and **EnergyUsage**. Each entity has relevant attributes like usernames, IP addresses, timestamps, etc. The diagram also shows relationships that help ensure that all interactions on the network are tracked, secured, and available for analysis and optimization. Such as:

- A User can own multiple Devices and receive multiple SecurityAlerts.
- Devices generate DeviceLog and are associated with EnergyUsage records.
- Reports are generated weekly and linked to the User who requested them.
- LoginHistory logs each User login, while SecurityAlert recieves real-time threat detection.

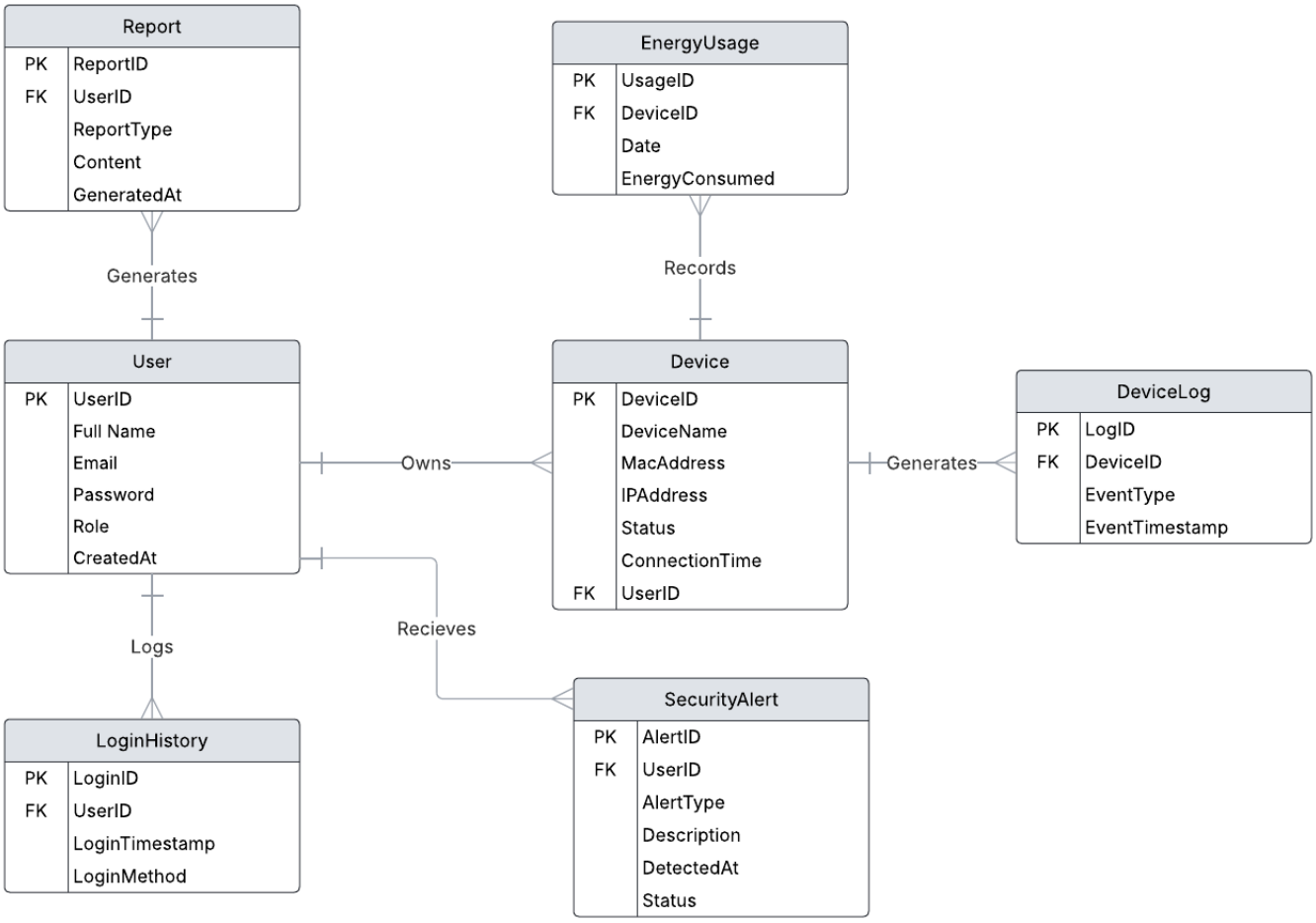
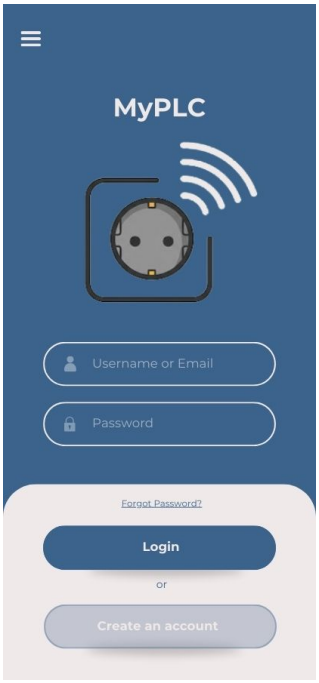


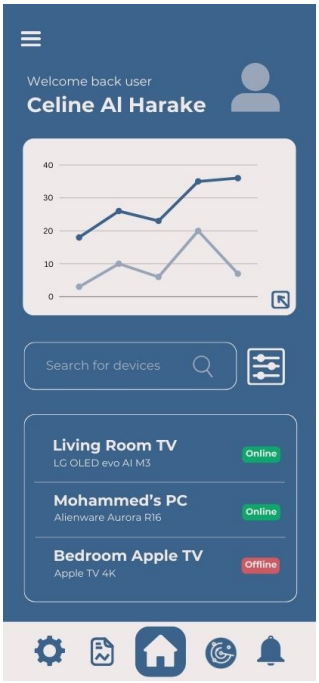
Figure 10: ER Diagram

3.5 UI/UX Design



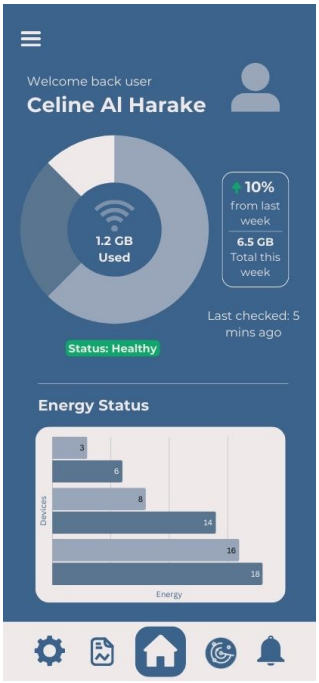
- **Login Page**

Registered users can log in by entering their username or email address along with their password. If a user does not yet have an account, they can easily create one by selecting the "Create an account" option. Additionally, if a user forgets their password, they can click on the "Forgot Password" link to initiate a password recovery process. This typically involves receiving a password reset link via their registered email address, ensuring a secure and convenient way to regain access to their account.



- **User Home Page**

After logging in, users are directed to the Home Page, which features a dashboard along with a list of devices connected to their account. At the bottom of the screen, there is a navigation bar containing icons for Home, Scan, Notifications, Reports, and Settings, providing quick access to different sections of the app. The dashboard displays a summarized overview of the user's electricity consumption. When the dashboard is expanded to full size, it reveals detailed analytics and comprehensive information about the user's energy usage patterns.

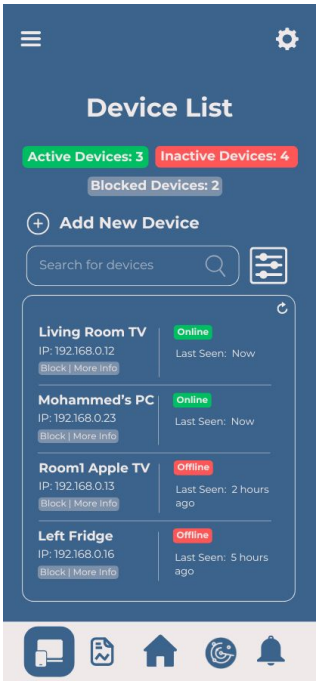


- **Dashboard**

When enlarged, the dashboard provides a detailed analysis of the user's internet consumption, including statistics compared to previous weeks. It also displays the status of the user's account, ensuring that there are no security threats detected on devices connected to the PLC network. Additionally, the dashboard breaks down the energy consumption of each connected device, showing detailed usage patterns throughout the day for better monitoring and management.

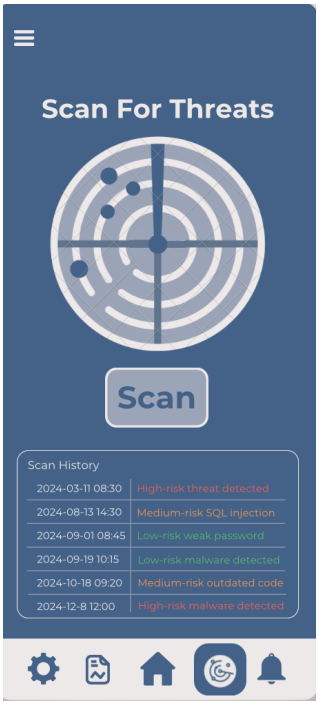
- **Admin Home Page**

The Admin Home Page is similar in layout to the User Home Page, but with additional administrative functionalities. After logging in, admins are directed to a dashboard that displays connected devices associated with user accounts. At the bottom of the screen, a navigation bar provides quick access to sections such as Home, Scan, Notifications, Reports, and a Device List. The Device List shows all devices connected to the PLC network, along with their associated users, and allows the admin to manage them, including blocking, unblocking, and monitoring device activity. The dashboard offers a summarized view of electricity consumption across users. When expanded to full size, it presents detailed analytics and comprehensive insights into the users' energy usage patterns, helping admins effectively oversee and manage the network.



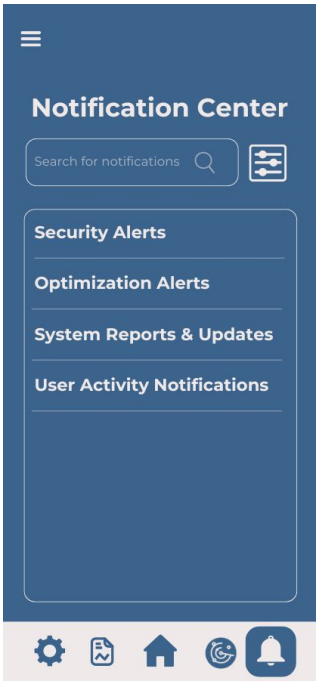
- **Admin Device List**

The admin has full access to all devices connected to the PLC network. Through the device liste interface, the admin can monitor each device, block or unblock them as needed, and perform various management actions to ensure network security and efficiency. In addition to managing existing devices, the admin also has the ability to add new devices to the PLC network, expanding and maintaining the system as required.



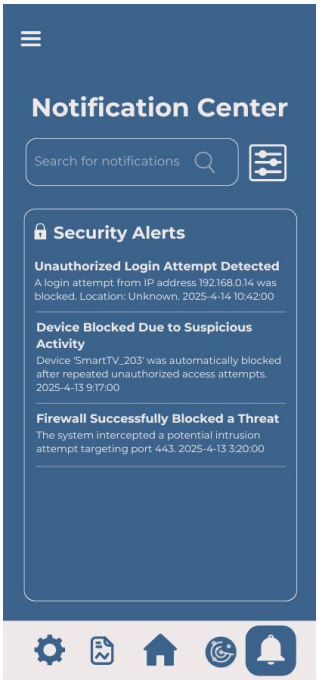
- **Network Scan**

All users have the ability to scan the network for potential threats. Each scan checks for vulnerabilities and ensures that connected devices remain secure. Every scan is automatically recorded in a scan history log, which includes the date of the scan, the identified risk level (high, medium, or low), and the reason for the detected threat. This allows users to review past scans and maintain a clear record of their network's security status over time.



- **Notifications**

All users receive notifications categorized into four different types: Security Alerts, Optimization Alerts, System Reports and Updates, and User Activity Notifications. Security Alerts inform users about potential threats or vulnerabilities. Optimization Alerts provide tips and suggestions to improve network performance and energy efficiency. System Reports and Updates notify users about important system changes, updates, or maintenance activities. User Activity Notifications keep users informed about any significant actions or changes made to their account or connected devices.



- **Notifications - Security Alerts**

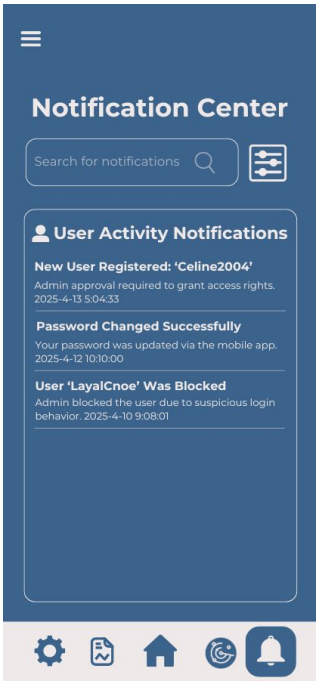
Security Alerts inform users about potential threats or vulnerabilities.

- **Notifications - Optimization Alerts**

Optimization Alerts provide tips and suggestions to improve network performance and energy efficiency.

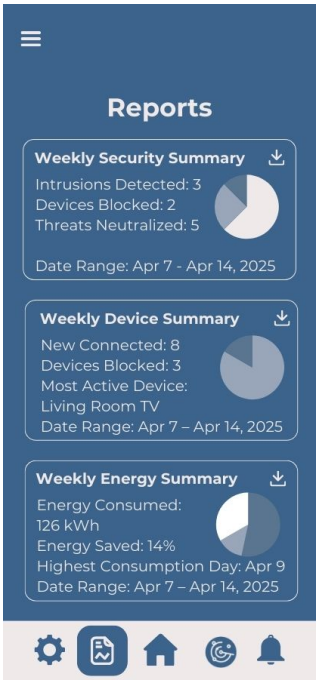
- **Notifications - System Reports & Updates**

System Reports and Updates notify users about important system changes, updates, or maintenance activities.



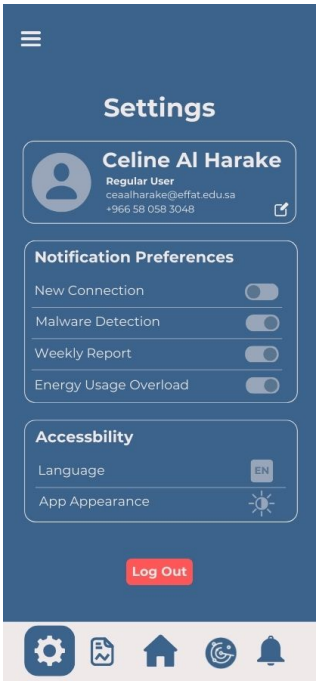
- **Notifications - User Activity Notifications**

User Activity Notifications keep users informed about any significant actions or changes made to their account or connected devices.



- **Reports**

All users receive comprehensive weekly reports that provide a detailed overview of their account activity. The security summary highlights how many intrusions were detected, how many devices were blocked, and how many threats were successfully neutralized throughout the week. The device summary presents information about new device connections and identifies the most active device during the reporting period. Additionally, the energy summary outlines the total amount of energy consumed over the week and pinpoints the day with the highest energy consumption. These reports are designed to help users monitor their network security, device activity, and energy usage effectively.



- **Settings**

All users have the ability to edit their profile information, including updating their email address and changing their password. Users can also manage their notification preferences, choosing which alerts they wish to receive, such as notifications for new device connections, malware detection, weekly reports, and energy usage overloads. Additionally, users have the option to customize the application by changing the language and adjusting the appearance settings to suit their personal preferences, enhancing their overall user experience.