Software Requirements Specification

for

Attendance Management System

Airport and Aviation Services (Sri Lanka) (Private) Limited

Table of Contents

1. Introduction

1.1 Purpose

This Software Requirements Specification (SRS) describes the functional and non-functional requirements for the AASL Attendance Management System. The system is designed to manage employee attendance tracking, report generation, and user administration for Airport & Aviation Services (Sri Lanka) Private Limited. This SRS covers the complete web-based attendance management solution including user authentication, attendance tracking, and comprehensive reporting capabilities.

1.2 Document Conventions

This Software Requirements Specification (SRS) follows specific conventions to ensure clarity and consistency throughout the document. Headings are presented in bold with larger font sizes, while subheadings are bolded with slightly smaller fonts, and the main body text is in regular font. Each functional requirement is labeled with a prefix such as REQ-# (e.g., REQ-1, REQ-2) for easy reference.

1.3 Intended Audience and Reading Suggestions

This Software Requirements Specification (SRS) document is intended to be used by a diverse group of stakeholders involved in the development, deployment, and usage of the **Attendance Management System** for **Airport & Aviation Services (Sri Lanka) (Private) Limited**. The document aims to ensure a shared understanding of the system's purpose, design, and functionalities among all concerned parties.

Intended Audience

- **Project Managers**: To oversee the project's timeline, resource allocation, and deliverables while ensuring the system aligns with organizational needs. This document supports milestone tracking, requirement verification, and stakeholder communication.

- **Software Developers and Engineers**: To understand and implement functional and non-functional requirements in the form of user interfaces, backend services, database design, and integrations.

- **Quality Assurance (QA) Testers**: To create test cases and validation plans based on specified requirements to ensure the system performs as expected under various conditions.

- **Client Representatives and HR/Admin Staff**: To validate that the system's functionalities support organizational policies for attendance monitoring, and to provide feedback for improvement.

- **Technical Writers and Documentation Specialists**: To develop training materials, user manuals, help files, and onboarding guides based on the documented system behavior.

Reading Suggestions To understand and use this document effectively, readers are encouraged to follow this sequence:

1. **Section 1 – Introduction**: Establishes context by outlining the system’s objectives and target audience.
2. **Section 2 – Overall Description**: Describes the system’s environment, features, constraints, and user roles.
3. **Section 3 – Specific Requirements**: Details functional and non-functional requirements critical for system development and validation.
4. **Appendices**: Offers additional information including report types, system rules, and supplementary documentation.

This structure helps each reader focus on the sections most relevant to their role and contributes to a coordinated, efficient development process.

1.4 Product Scope

The Attendance Management System is a centralized web application that records employee attendance through digital IN, OUT, and IN/OUT entries. It supports detailed reporting, user role-based access, and administrative functions for managing users. It ensures accurate tracking of attendance, reduces manual errors, and simplifies reporting across departments and sections. The solution enhances operational transparency and supports data-driven decision-making for human resource management.

2. Overall Description

2.1 Product Perspective

The AASL Attendance Management System is a standalone web-based application designed specifically for Airport & Aviation Services (Sri Lanka) Private Limited. The system consists of a React.js frontend interface, Node.js/Express.js backend server, and Microsoft SQL Server database. It operates within the organization's existing IT infrastructure and integrates with current departmental structures and employee hierarchies.

2.2 Product Functions

The Attendance Management System provides the following major functions:

- **Attendance Data Retrieval:**
  The system obtains attendance records (IN, OUT, and IN/OUT entries with timestamps) from the Microsoft SQL Server database. Note that the actual attendance data is captured and saved by an external fingerprint machine system, which is outside the scope of this application.

- **Report Generation:**

  Generate various attendance reports based on the retrieved data, including:

  - Daily Attendance Report
  - Daily Attendance Report 2 (alternative format)
  - Monthly Attendance Report
  - Absence Report (highlighting missing attendance entries)

  Reports can be filtered by Department, Section, Type (IN/OUT), Date Range, and optionally by EPF Number—if an EPF Number is provided, the report is generated for that specific user; otherwise, it includes all users in the selected Department and Section based on the chosen filters.

- **User Management:**

  Enable authorized users (Admin and Super Admin) to create, modify, and delete user accounts with appropriate role assignments (User, Admin, Super Admin).

- **Password Management:**

  Allow all users to securely change their own passwords, enforcing password validation.

- **Section Assignment:**

  Facilitate assignment of users to specific departments and sections for accurate attendance tracking and reporting.

- **Role-Based Access Control:**

  Differentiate access levels between User, Admin, and Super Admin roles

- **Department Filtering:**

  Provide department- and section-specific data filtering in reports and user management interfaces based on the logged-in user's role and assignments.

This clarifies that your system focuses on data management, reporting, and user administration, while the biometric attendance capture is handled externally. Let me know if you want me to help with other sections.

2.3 User Classes and Characteristics

User: Access limited to personal attendance data and reports for their assigned department.
Admin: Access to manage users and generate reports within their assigned department.
Super Admin: Full access across all departments and sections, including comprehensive report generation and user management.

2.4 Operating Environment

- The client-side of the system operates on modern web browsers such as Google Chrome, Mozilla Firefox, Microsoft Edge, and Apple Safari, with JavaScript enabled and support for HTML5 and CSS3.

- The frontend is built with **React** and uses **React Query** to efficiently communicate with the backend API, handling data fetching, caching, and background updates.

- The server-side runs on the **Node.js** runtime environment (version 18.x or later), using the **Express.js** framework to manage routes, middleware, and RESTful API services.

- Communication between the client and server is designed to use HTTP/HTTPS with JSON format.

- The system connects to a **Microsoft SQL Server** database (2016 or later), using **Sequelize ORM** for querying and database operations, supporting joins, filters, and stored procedures where needed.

- It can be accessed via a **Local Area Network (LAN)** for internal deployment or over the **internet** with proper security configurations for remote access.

2.5 Design and Implementation Constraints

The system must comply with the organization's cybersecurity and internal IT security standards, ensuring that all sensitive data such as passwords, authentication tokens, and user information—is encrypted both at rest and during transmission. All user passwords must be securely hashed using the bcrypt algorithm, and JSON Web Tokens (JWT) are required for all API interactions to maintain secure and stateless user authentication. The system must support concurrent access by multiple authorized users without compromising performance or data integrity. Reports generated by the system should be exportable in PDF format for record-keeping and distribution purposes. Additionally, development must follow standardized coding practices to ensure the maintainability, scalability, and ease of future enhancements to the application.

2.6 Assumptions and Dependencies

- Users have basic computer literacy and web browser familiarity
- Reliable network connectivity is available during system usage
- Microsoft SQL Server licensing and infrastructure are provided by the organization
- System administrators will manage regular database backups and maintenance
- Employee information and departmental structures are maintained through existing HR systems

3. External Interface Requirements

3.1 User Interfaces

The user interface of the Attendance Management System is designed to be intuitive and role-specific, enhancing both usability and security. Upon logging in, users are directed to a personalized dashboard that serves as the central hub for accessing system features. The dashboard prominently displays the attendance layout, enabling users to view and generate attendance reports efficiently.

All users have access to a Change Password feature, allowing them to securely update their credentials. Additionally, a User Settings section is available exclusively to Admin and Super Admin roles. This section provides advanced administrative functions, such as creating new users, assigning them to specific sections, and deleting user accounts.

The system enforces strict role-based access control, ensuring that sensitive administrative tasks are restricted to authorized personnel only. This approach provides a streamlined and secure experience tailored to each user's responsibilities.

3.2 Hardware Interfaces

The system operates through standard web browsers and does not require specialized hardware interfaces. Standard computer hardware with network connectivity is sufficient for system operation.

3.3 Software Interfaces

Frontend (User Interface):
Built using **React**, a powerful JavaScript library for building interactive user interfaces. It uses reusable components to simplify development and improve consistency. **React Query** is used to fetch and manage server data, allowing for fast loading, background updates, and smooth user experience.

Backend (Server):

Runs on **Node.js** with the **Express.js** framework, which handles routing, processing user requests, and sending responses. It provides secure and organized REST API endpoints to manage attendance records, users, roles, and report data. Access to sensitive features is restricted based on user roles (User, Admin, Super Admin).

Database:

Uses **Microsoft SQL Server (MSSQL)** to store all attendance data, user information, department details, logs, and role assignments. The database is structured with normalized tables and relationships to support fast queries and accurate report generation. Sequelize ORM is used to interact with the database in a clean and consistent manner.

Security:

User authentication is handled using **JWT (JSON Web Tokens)**. Once logged in, each request includes a token that verifies the user's identity.

APIs (Communication):

The frontend and backend communicate through RESTful APIs using standard HTTP methods like GET, POST, PUT, and DELETE. All data is sent and received in JSON format, allowing for structured, readable, and easy-to-process data exchange.

PDF Reports:

Users can generate attendance reports in PDF format using jsPDF, a client-side JavaScript library. Reports such as daily, monthly, and absence reports can be downloaded.

4. System Features

4.1 User Authentication and Authorization

Description: Secure login system with role-based access control.

Priority: High

Functional Requirements:

REQ-4.1.1: System shall authenticate users using username and password credentials.

REQ-4.1.2: System shall support three user roles: User, Admin, and Super Admin.

REQ-4.1.3: System shall redirect users to appropriate interfaces based on their role.

REQ-4.1.3: System shall maintain secure sessions with automatic timeout.

4.2 Attendance Data Retrieval

Description: Retrieve and display attendance records from the database, sourced from external fingerprint machines.

Priority: High

Functional Requirements:

REQ-4.2.1: System shall retrieve attendance records (IN, OUT, IN/OUT) with timestamps from the Microsoft SQL Server database.

REQ-4.2.2: System shall not permit manual entry or modification of attendance data within the application.

REQ-4.2.3: System shall display attendance data in the attendance layout for authorized users, filtered by department, section, and user role.

REQ-4.2.4: System shall ensure attendance data integrity and prevent unauthorized access or tampering.

4.3 Report Generation

Description: Generate and export various attendance reports based on retrieved data and user-selected filters.

Priority: High

Functional Requirements:

REQ-4.3.1: System shall generate Daily Attendance, Daily Attendance Report 2, Monthly Attendance, and Absence Reports.

REQ-4.3.2: System shall allow filtering of reports by Department, Section, Attendance Type (IN/OUT/IN-OUT), Date Range, and EPF Number.

REQ-4.3.3: If EPF Number is provided, system shall generate the report for that specific user; if left blank, system shall include all users in the selected Department and Section.

REQ-4.3.4: System shall restrict report access based on user role (User, Admin, Super Admin).

REQ-4.3.5: System shall allow export of generated reports in PDF format.

4.4 User Management

Description: Manage user accounts and assignments with role-based restrictions.

Priority: Medium

Functional Requirements:

REQ-4.4.1: System shall allow Admin and Super Admin users to create new user accounts.

REQ-4.4.2: System shall allow Admin and Super Admin users to assign users to specific sections.

REQ-4.4.3: System shall allow Admin and Super Admin users to activate/deactivate or delete user accounts.

4.5 Password Management

Description: Enable secure password change functionality for all users.

Priority: Medium

Functional Requirements:

REQ-4.5.1: System shall allow all users to change their own passwords.

REQ-4.5.2: System shall securely hash all passwords using the bcrypt algorithm.

4.6 Section Assignment

Description: Assign users to departments and sections for accurate reporting and access control..

Priority: Medium

Functional Requirements:

REQ-4.6.1: System shall allow Admin and Super Admin users to assign or update section assignments for users.

REQ-4.6.2: System shall use these assignments to filter attendance data and reports according to user roles.

4.7 Role-Based Access Control

Description: Enforce differentiated access and permissions according to user roles.

Priority: High

Functional Requirements:

REQ-4.7.1: System shall restrict access to features and data based on the user's assigned role.

REQ-4.7.2: System shall allow Admins to manage users and reports within their assigned department and sections.

REQ-4.7.3: System shall allow Admins to manage users and reports within their assigned department and sections.

REQ-4.7.4: System shall grant Super Admins unrestricted access to all departments, sections, and user management features.

5. Other Nonfunctional Requirements

5.1 Performance Requirements

- The system shall respond to user requests within 3 seconds under normal operating conditions.

- Report generation for daily reports shall complete within 10 seconds; monthly reports shall complete within 30 seconds.
- The system shall support concurrent access by at least 100 users without performance degradation.
- Database queries shall be optimized to minimize load times and ensure smooth user experience.

5.2 Security Requirements

- All sensitive data, including passwords and authentication tokens, shall be encrypted both in transit (using HTTPS/TLS) and at rest.
- Passwords shall be securely hashed using the bcrypt algorithm.
- Authentication shall be managed via JSON Web Tokens (JWT) to maintain stateless and secure sessions.
- Role-based access control (RBAC) shall be strictly enforced to prevent unauthorized access to data and functionalities.
- The system shall log all user activities related to login, report generation, and user management for audit purposes.

5.3 Software Quality Attributes

- **Availability:**
  The system must be available at least 99% of the time during operational hours to ensure continuous access for attendance tracking and report generation.

- **Maintainability:**
  The codebase must follow modular and well-documented practices to allow updates, bug fixes, and feature enhancements without impacting unrelated modules.

- **Usability:**
  The system should require minimal training for all user roles and include clear labels, tooltips, and validation messages for all input fields to facilitate ease of use.

- **Reliability:**
  The system must ensure that attendance data is accurately retrieved and reported without loss, duplication, or corruption, even under concurrent multi-user access.

- **Flexibility:**
  The system should be easily adaptable to support future enhancements such as integration with mobile attendance apps, email notifications for absences, or additional report types.

- **Robustness:**
  The system must handle invalid inputs gracefully, provide helpful error messages, and prevent crashes or data inconsistencies during operation.

5.4 Business Rules

- Only authenticated users with valid credentials can access the system, including the dashboard, attendance reports, and user management features.
- User roles (User, Admin, Super Admin) determine access permissions, with Admin and Super Admin having elevated privileges for user management and comprehensive reporting.
- Attendance data is sourced exclusively from the fingerprint machine system and imported into the database; manual modification or deletion of attendance records within the system is prohibited.
- Reports can be generated for individual employees by specifying their EPF Number or for all users within selected departments and sections if the EPF Number is left blank.
- All user actions related to user management (creation, modification, deletion), password changes, and report generation must be logged with timestamps and user IDs to ensure accountability.

- Department and section assignments must be maintained accurately to enforce access control and ensure correct attendance reporting.
- The system shall prevent duplicate user accounts with the same EPF Number to maintain data integrity.