Security Service Management System for RALL

Project Proposal

Sri Lanka Institute of Information Technology

IT2080 – Information Technology Project

Group ID: ITP24R_B1_W22

August 2024

Declaration

This project report is our original work and the content is not plagiarized from any resource, References for all the content taken from external resources are correctly cited. To the best of our knowledge, this report does not contain any material published or written by third parties, expect as acknowledged in the text.

Authors:

Author SID	Author Name with Initials	Signature
IT22325228	Fernando K. K. C	
IT22907998	Sadisha R. M. M	
IT20145552	Dissanayaka D. M. S. M	
IT22257086	Randiw E. Y	
IT22293480	Jayodhya J. D. H	
IT22127082	Medawatte W. W. M. T. N. B	
IT22132628	Kusumsiri P. A. S. S	
IT22197146	Ranasinghe R. A. R. V. C	

Date: 04.08.2024

Contents

01.Background

1.1. Company Background

Rakna Arakshaka Lanka Limited is the privately-owned limited liability company formed in the year 2006 and registered under the Companies Act, No 7 of 2007 in Sri Lanka. It's an affiliated institution of the Ministry of Defence. [1] RALL is the premier security service provider that offers superior security solutions toward the safeguarding of people, assets, and reputation through advanced technology, rapid response, and intelligence services. As such, the company empowers businesses to operate securely locally and globally while making sure lives and property are safe.

RALL is extremely well-known for its quality and workmanship and has carved a niche as one of the largest security service providers in any industrial, commercial, maritime security-related industry, specialized training, and special projects. The organization provides manifold employment opportunities to ex-service members of the nation by utilizing their gigantic experience in the military, police, and special task forces.

RALL security personnel are well trained and highly experienced to discreetly and professionally protect clients. The company's services are nationally and internationally acclaimed, with a pool of security personnel fully equipped to provide security solutions to all clients. Their Maritime Security division has particularly been in the limelight as highly effective in safeguarding vessels from piracy attacks and other forms of threats.

RALL is strongly dedicated to full compliance with all international and national laws and guidelines concerning the practical application of the International Code of Conduct for Private Security Companies, United Nations Basic Principles on the Use of Force & Firearms, and all applicable maritime legislation. The Company serves a diverse clientele, including some of the world's largest shipping lines, offering services that include junior security officers up to highly professionalized Maritime Security Teams.

1.2. What is Security Service?

Security services denote a bundle of activities aimed at ensuring the protection of people, assets, and property from various heterogeneous threats. These services include providing physical security through guarding, surveillance, and patrolling, along with specialized services like risk assessment, security consulting, and emergency response. The security services can be availed specifically for residential, commercial, industrial, and maritime clients for the purpose of safety and mitigation of risks

1.3. What is Security Service Management System?

An SSMS stands for Security Service Management System and is designed to handle and coordinate security services efficiently and effectively. It contains the management of personnel, scheduling, interaction with clients, incident reporting, and many more security companies. A few of the great benefits of an SSMS are that it levels up the operations through taming communication and service delivery in security companies. This tool gives real-time visibility into security operations, ensuring effective allocation of resources while serving the client's requirements efficiently.

1.4. Our Web-based Application

Our team is developing a comprehensive web-based Security Service Management System specifically for Rakna Arakshaka Lanka Limited (RALL). This application is designed to streamline various operational aspects, including employee management, training, client interactions, and inventory control. The system aims to enable efficient handling of employee recruitment and training, ensuring that security officers are well-prepared and appropriately deployed. Clients will be able to book security services, manage their accounts, and provide feedback through an intuitive interface, enhancing their overall experience with RALL.

Additionally, the application will include robust modules for payment processing, inventory management, and supplier coordination, ensuring that all logistical aspects are managed effectively. The system is planned to support real-time incident reporting, helping to address and resolve issues swiftly. Role-based access control will ensure secure data management and access, tailored to the specific needs of different user roles within the organization.

This project aims to enhance operational efficiency for RALL and provide a modern, integrated approach to managing security services, making it a valuable tool for the organization and setting a new standard in the industry.

02.Problem and Motivation

2.1. Problems

Rakna Arakshaka Lanka Limited currently faces challenges in managing extensive security services. The manual procedures for recruiting employees, training, client management, and operations are time-consuming and error-prone. Because of this non-automation, inefficiencies result in delayed responses to the clients, difficulty in tracing the security personnel deployment and status, and difficulty in managing inventory and relationships with suppliers. There is also no centralized system for payment processing and reporting of incidents, and that obviously weakens the organization's ability to provide transparent and efficient service to clients.

2.2. Motivation

These problems are to be addressed by putting in place a web-based Security Service Management System for RALL. The system is aimed at automating and streamlining a number of operational processes, enhancing how RALL efficiently manages its workforce, including making sure that security officers are well-trained, deployed, and monitored. The system will also enhance the delivery of services to clients by giving flexibility in terms of booking services, managing accounts, and providing feedback. The application will enhance inventory and supplier management, enabling RALL to meet client demand on time.

It will also provide real-time insights into operations, helping RALL to respond more quickly to incidents and work out a better management of resources. By this system, RALL will be able to enhance operational efficiency, reduce administrative overheads, and improve client satisfaction. Eventually, this project will help in accomplishing the task assigned to RALL: to render qualitative security-related services and help the organization uphold its repute as one of the regional leaders in this sphere of activity.

03.Aim and Objectives

3.1. Aim

The aim of this project is to develop a comprehensive web-based Security Service Management System for RALL. It will simplify and automate the entire process of recruiting security officers, managing their training, client liaison, operational deployment, and administrative processes. The integrated solution will enhance operational efficiency and effectiveness of RALL in their operations, ensuring that the organization is able to address the clients' needs through high-quality, responsive, and reliable security services. This system will also improve transparency, accountability, and total management capabilities within RALL by centralizing these functions.

Particularly, these are areas it seeks to address:

- **Automation of Recruitment Process:** Making the process of hiring security officers easier by facilitating posting jobs, receiving applications, interviewing, and onboarding to ensure a seamless and efficient recruitment experience.
- **Comprehensive Client Management:** Managing client interaction in relation to the documentation of their requirements, service bookings, and feedback collection for a responsive service experience that is tailor-made.
- **Efficient operations management:** Real-time monitoring and deployment of security personnel, management of incidents, and resource optimization will ensure that clients receive security services in a timely and effective manner.
- **Inventory and supplier management:** This involves maintaining accurate accountability of uniforms, equipment, and other resources, while managing the relationship with suppliers to ensure adequate supplies.
- **Inbuilt Payment System:** This module will automate the generation of invoices and the payment history of clients for a problem-free financial management process at both ends.

This system looks to help RALL in delivering quality in Security Services, maintaining operational excellence, and improving client satisfaction by using advanced technology and process streamlining.

3.2. Objectives

To achieve the aim of the Security Service Management System for Rakna Arakshaka Lanka Limited (RALL), the project has outlined specific objectives.

These objectives provide clear and measurable steps to guide the development and implementation of the system:

1. **Develop a Recruitment Module:**
    - Design and implement a module for posting job vacancies, applying for them, arranging interviews, and onboarding processes.
    - A smooth application module for applicants and HR staff by adding features to track application statuses and reporting on recruitment metrics.

2. **Implement a Comprehensive Client Management System:**
    - Create a centralized database to store and manage client information, including service requirements, contracts, and communication history.
    - Enable clients to book services, view their service history, and provide feedback through a secure client portal.
    - Develop tools for Client Managers to monitor client satisfaction and generate client-related reports.

3. **Establish an Efficient Operations Management Platform:**
    - Develop real-time tracking and deployment functionalities for security personnel, including scheduling, assignment, and incident management.
    - Provide Operation Managers with tools to monitor the status and location of security officers, manage shift changes, and address on-site issues promptly.
    - Implement reporting capabilities to analyze operational efficiency and incident response times.

4. **Create an Integrated Inventory and Supplier Management System:**
    - Develop an inventory tracking system for uniforms, equipment, and other resources, with alerts for low stock levels.
    - Implement supplier management features to track orders, deliveries, and supplier performance.

- Enable Inventory Managers to generate reports on stock levels, usage patterns, and supplier reliability.

5. **Design an Automated Payment System:**
    - Develop features for generating invoices, tracking payment statuses, and managing financial transactions with clients.
    - Ensure the system supports multiple payment methods and provides clients with secure access to their payment history and outstanding balances.

6. **Integrate Data Analytics and Reporting Capabilities:**
    - Implement data collection and analytics tools to monitor key performance indicators (KPIs) across all system modules.
    - Develop customizable reporting features to allow management to gain insight into recruitment success, client satisfaction, operational efficiency, inventory management, and financial performance.
    - Keeping reporting tools updated regularly for insights related to effective decision-making.

7. **Ensure Effective User Access Control:**
    - Design a very robust access control system that will help in controlling users according to their roles, which were set in relation to the job functions.
    - Implement secure login mechanisms and role-based access to ensure that each user has access only to the level of information and features required in executing his/her responsibilities.
    - Provide the administrators with tools to handle, in an efficient way, user accounts, permissions, and access levels.

These objectives are designed to guide the development and implementation of the Security Service Management System for RALL, addressing the key functional and operational needs of the organization.

04.System Overview

4.1. System Diagram

In all, our system can broadly be segregated into eight main components: User Management, Training Schedule Management, Client Management, Operation Management, Employee Management, Inventory Management, Payment Management, and Supplier Management. All these modules combine to form the front end of the system in light of cohesiveness and intuitiveness in the user interface.

The Web API, implemented using REST principles with Express JS, acts as the intermediary between the front end and back end. This API facilitates communication by handling requests and responses, ensuring that data flows seamlessly between the user interface and the server.

The back end is developed using Node JS, a robust platform for building scalable network applications. It processes the data exchanged through the API, utilizing JSON objects to manage and manipulate the information. All data is securely stored in MongoDB, our chosen database server, which is known for its flexibility and scalability.

The entire system's records and data are housed within the "Security Service" database, ensuring a structured and organized repository for all relevant information. The system is hosted on an external storage solution, providing reliable access and performance for users. This architecture ensures that all components work harmoniously, delivering a comprehensive and efficient Security Service Management System.

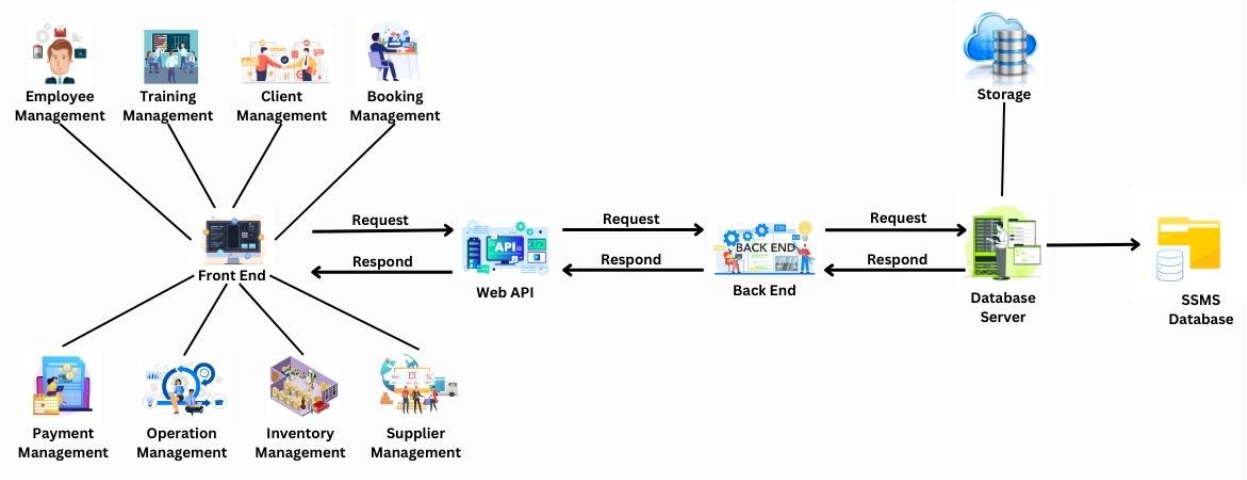

Figure 4.1.1: System Diagram

4.2. Functional Requirements

1. Employee Management

The Employee Management function in our Security Service Management System offers a comprehensive suite of tools for managing all aspects of human resources. This function begins with the recruitment process, where job vacancies for security officers and other staff positions are advertised. Candidates apply by completing a detailed registration form, which includes sections for basic details, professional qualifications (categorized for roles like JSO, LSO, OIC, and VVIP), and interview scheduling. This organized approach ensures efficient hiring.

Once onboarded, the system allows the Manager to add, read, update, and delete employee details, including storing basic information and professional qualifications. The system also facilitates user access control by creating and providing secure login details for employees and department managers, ensuring that permissions are granted based on their roles.

The function handles interviews, manages security officer requirements, and includes a leave management feature that tracks various types of leave, allowing employees to request leave and managers to approve and manage absences. The Operation Manager also has access to the employee leave database, enabling the efficient deployment of security officers based on availability and operational needs. Additionally, the function enables the generation of monthly reports, including net income and profit reports, helping the organization keep track of financial performance. This centralized approach to managing employee data enhances data accuracy, security, and operational efficiency, providing a seamless experience in workforce management.

2. Training Management

As the Training Manager in this security service system, I have a number of roles that will help train the security personnel efficiently and effectively. The functions include course creation, training schedule management, report generation, and integrating feedback from security officers.

Functions of the Training Manager

1. Course Design: This is the most fundamental of all responsibilities. Designing comprehensive courses that would help meet the diverse requirements of security personnel. The courses are structured in such a way that theoretical knowledge and practical skills needed for the job be given attention. The four main courses particularly offered are:

- **Security Consultancy and Management Course**
- **Outbound and Personal Skills Development**
- **Firearm Training**
- **Communication Skills Development Training**

The other associated key responsibility here is the scheduling of training sessions. This would involve liaising with trainers, booking training facilities, and ensuring that all logistic arrangements are made.

3. Report Generation

- It should generate detailed training activity reports concerning information containing attendance, course completion rates, trainee performance, and feedback from trainers and trainees

4. Integrating Feedback from Security Officers

- The feedback from security officers in this continuous development process is important. As the Training Manager, I always look for and implement improvements to courses from the feedback received.

5. Training Cart Management

- The function of the training cart management encompasses all the materials and resources that shall be needed in a training session, like training manuals, equipment, among others, and other logistical needs.

That serves as the multifaceted and critical role of the Training Manager in the security service system towards the success of the organization. The Training Manager develops structured training courses, manages the training schedule, and integrates feedback from security officers to ensure that security personnel are well-equipped with the necessary skills to perform assigned duties effectively.

3. Client Management

This feature of the Security Service Management System is developed to manage all clients in an effective and efficient manner regarding customer interactions and service delivery. This facility helps the Client Manager to configure and maintain client profiles and therefore ensure that every minute detail of the clients and their requirements is correctly maintained and updated. It serves in assembling and processing requests for services that will be either requested by the clients or scheduled in advance.

A tailored dashboard allows clients to view the history of service and the bookings near them; hence transparency made readily available to service information. It also allows the Client Manager to gather information on the feedback of the clients to set the satisfaction levels and take appropriate action on the disaggregated levels of satisfaction. It also helps in the writing of reports regarding client tendencies, service quality, and general satisfaction, which all comes in handy in the evaluation of performance and appropriate improvement in the services delivered.

This feature facilitates easier management of clients by centralizing all the information, service requests, and maintenance of high standards of satisfaction that a client would require.

4. Operation Management

The Operation Management function in the Security Service Management System is designed to oversee and optimize the deployment and performance of security personnel. This function enables the Operation Manager to monitor the real-time status and location of security officers, ensuring they are effectively assigned to various service locations as needed. The system supports the management of security officer deployments, allowing the Operation Manager to coordinate schedules, handle assignments, and address any issues or incidents that arise.

The function includes features for managing and resolving security-related incidents, providing a streamlined process for reporting and tracking problems. Security officers can report issues directly to the Operation Manager, who can then take appropriate action to resolve them. Additionally, the system facilitates the generation of operational reports, including deployment schedules and incident logs, which help in assessing performance, optimizing resource allocation, and maintaining high service standards.

By centralizing these tasks, the Operation Management function enhances operational efficiency and ensures that clients receive timely and effective security services, thereby supporting the overall effectiveness of the security operations.

5. Booking Management

The Booking Management function in the Security Service Management System is designed to streamline and automate the process of scheduling and managing security services for clients. This function allows clients to request security officers for various events or needs, specifying their preferences for officer types.

Clients can use the system to make bookings by selecting available time slots and service types, while the Booking Manager oversees and manages these requests. The system facilitates the tracking and confirmation of new bookings, handling any issues or adjustments that may arise..

Booking management part outlines the key responsibilities of a Booking Manager and the functionalities of the system.

Role of the Booking Manager

- Check for New Bookings
    - The Booking Manager monitors new client requests, verifies booking details, and ensures resources are available. Prompt updates and clear communication with the Operations Manager and security personnel are crucial.
- Manage All Bookings
    - Overseeing the entire booking process, the Booking Manager ensures each request is handled efficiently. Includes coordinating with clients and security officers, updating booking statuses, and maintaining accurate records.
- Resolve Online Booking Issues
    - Addressing technical issues with the booking system and responding to client queries ensures a smooth booking experience. Collaboration with the IT department is essential to maintain system functionality.

Booking Management System Functionalities

- Client Requests for Security Officers
    - Clients can request security officers for events, specifying the type and number of officers needed.
    - Clients can request specific types of officers, such as lady officers or VVIP officers, to meet their event needs.
- Check and Manage New Bookings
- Resolve Online Booking Issues
- Check Security Officers' Payments

6. Payment Management

The Payment Management function within the Security Service Management System is designed to handle all financial transactions related to client services. This includes generating invoices for the security services provided and tracking payments to ensure accurate financial management.

The Payment Manager is responsible for confirming client payments, which involves verifying payment status and ensuring that all transactions are properly recorded. Once payments are confirmed, the system generates detailed invoices that outline the services rendered and any applicable charges.

The function also supports the generation of financial reports that provide insights into payment statuses, outstanding invoices, and overall revenue. This ensures that the organization maintains a clear and accurate view of its financial operations, facilitating efficient billing and financial management processes.

7. Inventory Management

The Inventory Management System is the pivotal component of a security company as it ensures that all the essential tools and equipment are well taken care of and available whenever needed. In other words, this system simplifies the activities, minimizes human mistakes, and assures that security employees have what they need to do their jobs.

Role of the Inventory Manager

The Inventory Manager plays a central role in the efficiency of the Inventory Management System. Some of their responsibilities include communication about inventory, controlling stock levels and issuing equipment to staff. Each of these roles is important in keeping the security firm running smoothly.

- Inform Inventory Details
    - Informing inventory details is all about giving the Inventory Manager information that is a summary of what is inside the warehouse. This involves keeping track of products currently available, documenting goods received and dispatched in or out of the firm and ensuring proper registration into the system. The principal purpose hereof is to enable informed decision making on stock replenishment and equipment allocation among others. These updates along with detailed reports help to reduce discrepancies and ensure transparency within organization activities.

- Manage Stock Levels
    - Keeping the right stock levels is a crucial role that involves managing an efficient inventory to meet operational requirements of the company. The stock levels must be monitored by the Inventory Manager who needs to identify patterns and make predictions for future requirements so as not to experience any low stocks or overstocks. To achieve this, reorder points are set, purchase orders are created and coordination with suppliers is done in order to ensure timely replenishment of stocks. Secondly, the Supplier Manager works closely with the Inventory Manager so as to keep stock levels up and prompt suppliers for necessary items in time.
- Provide Equipment for Employees
    - Another one of the major functions performed by the Inventory Manager is the procurement of equipment for employees. This entails issuing out all materials including uniforms, firearms, and other working tools to employees depending on their positions. It starts where the Employee Manager recruits new employees and oversees them to be trained by the Training Manager. After the training is over, the Training Manager issues ID cards and checks readiness of the employees to receive the equipment. Specifically, the Inventory Manager then supplies the necessary items to bodyguards, VIPs, VVIPs, and security officers to guarantee the employees are well-equipped to accomplish their tasks.
- The major functions of the Inventory Manager include being engaged in the system of inventory management and allocating suitable tools to the workers. By executing the mission of providing details of inventory, managing the stocking status, and supplying the appropriate tools to the firm's employees, the Inventory Manager plays a vital role in enhancing the firm's security threshold while acting more efficiently. Other supportive ones such as the Supplier Manager, Employee Manager, and Training Manager make the system more complete by also highlighting the preparedness of guards in executing their duties. This is particularly wise given the fact the inventories are a key component of operational readiness, protection and security.

8. Supplier Management

Our Online Security Service Management System contains a solid Supplier Management function that gives you all the ways to manage your relationships with various suppliers. This feature starts with support for the Supplier Manager, where he can add, read, update, and delete the supplier details to ensure that correct information is always available. This allows for contact information, a list of products and services you provide or offer, pricing, and other common company performance metrics. By organizing the supplier manager, we will be able to get all the precise information so that the supplier manager can have up-to-date data by themselves.

After the suppliers get onboard, it enables the supplier manager to reorder stocks and manage their relationships properly. Our job is all about ordering the uniforms and weapons, or any bacon, flour, or weapons we need to keep our garrison alive, and making sure they get processed. It also allows suppliers to accept or reject such orders and updates a central system, which effectively streamlines the order management process. This means the supplier manager and suppliers are always informed together, meaning they know which orders need to be processed next.

It also supports performance tracking and reporting. Supplier management checks that it is possible to monitor the performance of the suppliers by means of indicators, such as delivery time correctly indicated and, above all, product quality. Always ensure proper packaging condition on each container received from the supplier. Compliance with agreements These are key performance metrics in determining the reliability of a supplier and making decisions on future partnerships. Moreover, the system can produce detailed reports of supplier activities and order statuses, providing visibility in terms of supply chain efficiency from which learnings can be made.

In addition, this feature helps generate performance summaries that cover statistics on how orders were fulfilled, the timeliness of deliveries, and the quality of products provided. These summaries assist the supplier manager in making choices based on data, improving supplier performance, and upholding top-notch service standards. The centralized method of handling supplier details boosts transparency, operational effectiveness, and strategic decision-making.

In our Online Security Service Management System, the Supplier Management function provides a solution for handling supplier interactions. It helps the organization effectively meet its requirements and maintain relationships with suppliers. This streamlined approach ensures that the supply chain functions smoothly, which in turn enhances the success and dependability of the security service.

4.3. Non-Functional Requirements

Non-functional requirements are quality attributes of the Security Service Management System that would convene the functionality work effectively, securely, and reliably. Given below are the significant non-functional requirements of the system:

- **Performance and Scalability:** The system should be able to handle high loads of concurrent users and high volumes of data transactions without degrading the performance significantly. It should be scalable enough to increase the user load, security officers or clients, and transactions held with organizational growth.
- **Reliability and Availability:** It should be highly reliable, available, and with low or no downtime. It should also detail the backup mechanisms to guarantee data integrity and continuity of service in cases of failure or disaster.
- **Security:** The system must ensure that the data is appropriately secured in terms of confidentiality, integrity, and availability. That means strong authentication of the end-user, authorization, sensitive data encryption, protection from unauthorized access, and cyber-attacks.
- **Usability:** This is the system being user-friendly and easy to use for all users; it shall also include a highly mobile user interface for all represented users such as managers, security officers, clients, and suppliers. It should also be able to display guided instructions with feedback to help the end-user experience and reduce the learning curve.
- **Maintainability:** The system shall have easy maintenance, wherein updates can be done quickly, bugs can be fixed, and enhancements made. That is, it has to be associated with extensive documentation and troubleshooting facilities for solution of problems.
- **Accuracy and integrity of data:** Accuracy and integrity of the data in the system throughout the data life cycle should be assured. To avoid errors during data entry, the system should have the mechanisms of validation and thus provide reliable data processing and reporting.
- **Compliance:** The system will be developed in accordance with all relevant industry standards, legal regulations, and organizational policies. Comply with relevant data protection laws, industry best practice, and security standards.
- **Accessibility:** This is concerned with the usage of the system through various devices and platforms - for example, desktop, tablet, and mobile devices. so that users can access the system from various places or contexts.
- **Responsiveness:** System responsiveness includes prompt response for user interaction and data processing to foster user experience smoothly.

4.4. Technical Requirements

1. Hardware:

- The system shall be deployed on servers that have sufficient processing power, memory, and storage for running expected loads smoothly. Specific hardware requirements will depend on the size of the deployment and on the level of user activity forecasted.

2. Operating System:

- The system shall be compatible with major operating systems, including Windows, MacOS, and Linux. In this case, the operating system for deployment would therefore depend on the choice of target hosting environment and, correspondingly, the infrastructure requirements.

3. Database:

- **MongoDB**: This will be achieved using MongoDB, a NoSQL document-oriented database designed to efficiently manage and store data. Because the MongoDB schema is flexible, it supports agile development, scaling, and handling of different types and structures of data.

4. User Interface:

- **React**: The system's user interface shall be designed using the React JavaScript library, which is built for building efficient, flexible, and very performant dynamic and responsive user interfaces.

5. Performance:

- **Node.js**: It's a free source, Node.js runtime environment, single-threaded for fast and scalable server-side operations at the back end of the system.

6. Compatibility:

- The system should be compatible with various hardware and software components required for its operation, including web browsers and server environments. This would ensure the system's interoperability across different platforms and devices.

7. Scalability:

- This system will horizontally and vertically scale with increasing data and number of users. MongoDB scalability features enhance the growth of the system under growing demands.

8. Frameworks and Libraries:

- **ExpressJS**: The server will use ExpressJS to implement routing, middleware, and server-side logic. ExpressJS is fast, unopinionated, and minimalist, a web framework for Node.js that helps to develop robust web applications.

05.Literature Review

In our literature review, we analyzed three existing web-based security service management systems: TechCERT [2], NobleProg [3], and Gajashakthi [4]. Our analysis revealed that most platforms offer basic functionalities such as user account management and employee management but often lack advanced features like detailed recruitment processes and comprehensive supplier management. While payment processing and client interaction functions are commonly included, enhanced capabilities such as customizable training schedules and robust inventory management are less prevalent. Our system seeks to bridge these gaps by incorporating a streamlined recruitment process, detailed leave management, integrated supplier and inventory management, and customizable training features, aiming to provide a more complete and efficient solution for security service operations.

Table 5.1: Literature Review

Functions	Our App	TechCERT	NobleProg	Gajashakthi
Employee Management	✓	✓	✓	✗
Training Management	✓	✗	✓	✓
Client Management	✓	✗	✓	✗
Operation Management	✓	✗	✗	✓
Booking Management	✓	✗	✗	✗
Payment Management	✓	✗	✗	✗
Inventory Management	✓	✗	✗	✓
Supplier Management	✓	✗	✗	✓

06.Methodology

6.1. Method

Agile Software Engineering Methodology

Agile means the iterative and incremental approach to software development, emphasizing flexibility, cooperation, and fast time-to-market with working software. [5] The core of the Agile manifesto has five values for the methodology: people and interaction over processes and tools; working software over comprehensive documentation; close customer collaboration; responsiveness to change over following a plan. Agile teams operate according to short iterations or sprints, which could last from one to four weeks; in each period, a team sets a set of tasks or user stories, plans, executes, and reviews. Since the tasks are processed in iterations, it enables continuous feedback and adaptation in a way that assures the final product reflects dynamically changing customer needs. These will be agile development methodologies, collaboration, emphasizing flexibility, and iterative development. They include Kanban, Scrum, Extreme Programming, and other types of methodologies. In this project, we used Kanban for the management of our development process.

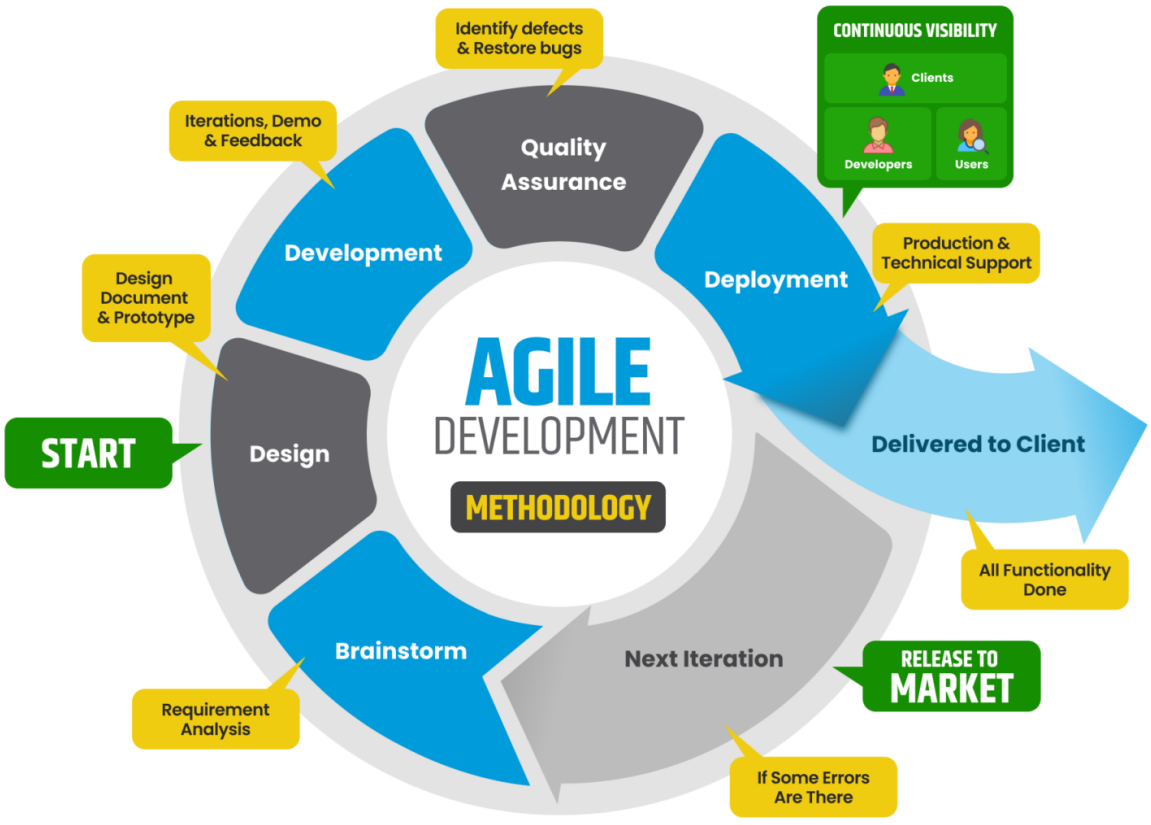

Figure 6.1.1: Agile Methodology

Reason for Selecting Agile Methodology

Agile methodology will be applied in this project because it is flexible, iterative, and collaborative by nature and very much suitable for web application development domains and other dynamic and evolving domains. The key reasons for choosing Agile are:

- **Flexibility and Adaptability:** Through its iterative approach, Agile un-Bundles let the Team respond quickly to changes in requirements, technology, or needs expressed by stakeholders. This flexibility is critical in a project environment where the requirements are likely to evolve as the project progresses.
- **Customer Involvement:** Agile does not only tolerate timely and required interactions between stakeholders; it ensures that the developed product is very close to the needs and expectations of all stakeholders. The constant feedback cycle sets up a self-improving process to deliver a product according to client needs.
- **Incremental Delivery:** Agile focuses on small, workable segments of the product that are released in short cycles, which are usually referred to as sprints. It is the approach that would support early issue detection, continuous testing, and validation for a more reliable final product.
- **Improves the quality and Risk Management:** by breaking down the project into smaller parts and with its frequent testing of each of the parts that make up the project. These iterative testing and feedback increase the quality of the product.
- **Team Collaboration and Communication:** Agile encourages a team-friendly environment where all members are closely collaborative, often including clients or end-users in the process. This fosters better communication that the goals are understood to all, providing a more harmonious working atmosphere.
- **Focus on Priorities:** Agile allows teams to make priority lists of tasks based on their importance and urgency in a way that the team would begin with the most valuable features and deliver those first. This sort of priority sets a focus on the development and refinement of the most critical components early in the project life cycle.

These reasons make Agile the methodology most suitable to be used in the development of the web-based Security Service Management System, ensuring that the final product will be fit for the needs of the users and able to adapt to any change or challenges encountered during its development process.

6.2. Tools and Technologies

The MERN stack is a well-known web development framework of four key technologies: MongoDB, ExpressJS, ReactJS, and NodeJS. This stack enables the development of full-stack JavaScript applications by independent developers: MongoDB serves as the database, ExpressJS as the web server framework, ReactJS for the frontend user interface, and NodeJS for the runtime environment of the backend. This stack is interesting because it provides a single, efficient workflow from client to server to database.

MongoDB is a NoSQL database that provides both flexibility and high performance to data-driven applications. This document-oriented data model—where data is stored in flexible, JSON-like documents rather than rigid tables—permits rapid iteration and adaptation to changing data requirements, so it's popular in agile development environments. [6]

Express is a lightweight and flexible web application framework for Node.js, offering essential features for building web and mobile applications, such as routing and middleware support. It streamlines server-side development by simplifying request handling and server logic. [7]

React is a JavaScript library for creating dynamic and responsive user interfaces. It allows developers to build reusable UI components with a declarative approach, making it efficient for managing complex state and rendering updates. [8]

Node.js is a cross-platform, open-source runtime environment that enables developers to build fast, scalable server-side and networking applications. It uses a single-threaded, event-driven architecture, which allows for efficient handling of concurrent operations. [9]

Apart from MERN Stack we use following tools and technologies in our project.

Visual Studio Code is a lightweight code editor that supports development tasks such as debugging, task management, and version control integration. [10]

GitHub is a platform for version control and collaboration, allowing developers to work together on projects from anywhere. []

6.3. Project Plan (Gantt Chart)

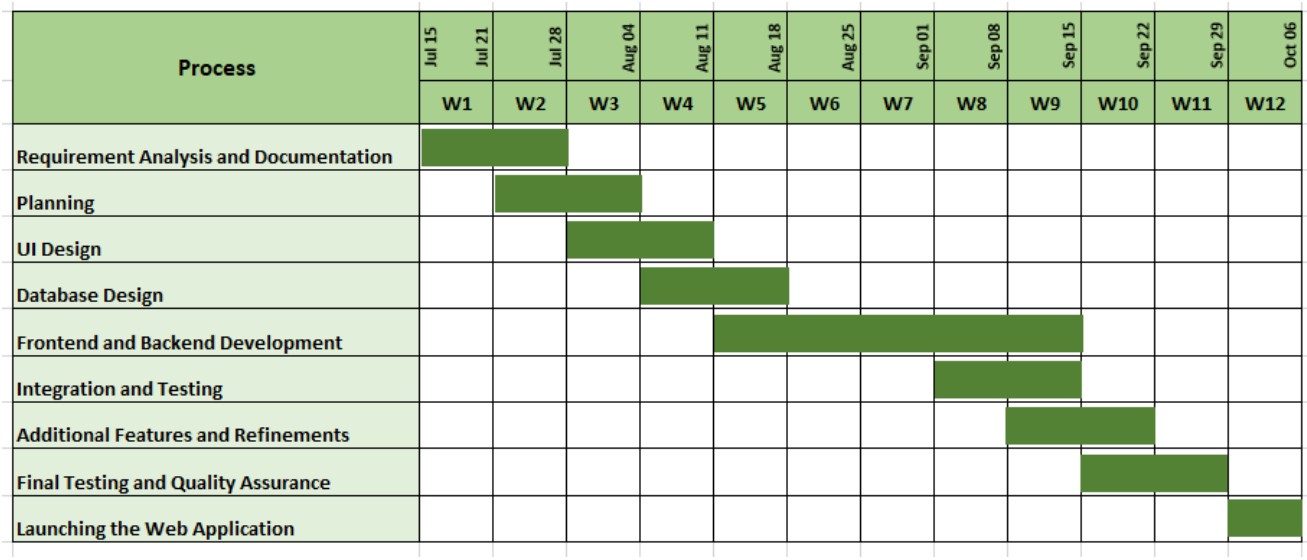

Figure 6.3.1: Gantt Chart

The project plan covers all the main phases in the development of a Security Service Management System and ensures that work on the application is structured. Via the gathering and analysis of requirements, detailed planning, and UI design, it sets a clear direction and user interface framework. This plan shall include database design, development of frontend and backend parts, and their integration. Further steps involve testing and adding more features, and finally, it goes for quality assurance measures. It helps in checking, one by one, all areas that the project contains to make sure that the application developed is functional and user-friendly.

6.4. Work Distribution (Work Breakdown Structure)

Table 6.4.1: Work Breakdown Structure

Student ID	Name with Initials	Tasks

IT22325228	Fernando K. K. C	• Implementing **Employee Management** Section
		• Completed,
		  ○ 3.Aim and Objectives
		  ○ 4.System Overview
		  ○ 5. Literature Review
		  ○ 6.Methodology
		  ○ 7.Evaluation Method
		  ○ 8.References
		  ○ 9.Appendix

IT22907998	Sadisha R. M. M	• Implementing **Training Management** Section

IT20145552	Dissanayaka D. M. S. M	• Implementing **Client Management** Section
		• Completed,
		  ○ 1.Background
		  ○ 2.Problem and Motivation

IT22257086	Randiw E. Y	• Implementing **Booking Management** Section
IT22293480	Jayodhya J. D. H	• Implementing **Payment Management** Section
IT22127082	Medawatte W. W. M. T. N. B	• Implementing **Operation Management** Section
IT22132628	Kusumsiri P. A. S. S	• Implementing **Inventory Management** Section
IT22197146	Ranasinghe R. A. R. V. C	• Implementing **Supplier Management** Section

07.Evaluation Method

The evaluation approach for the web-based Security Service Management System shall be holistic and detailed to ensure the realization of the project goals and the stakeholders' expectations. In this regard, the evaluation will be done at various stages, all targeting different aspects of the system's functionality, performance, and user experience. Key among the evaluation methods include:

1. Functional Testing:

- **Unit Testing:** Each module, such as Employee Management, Client Management, or Operation Management, will be tested in isolation for expected behavior. Specific functionalities of these modules, such as user access control, booking a client, or payment processing, are to be tested.
- **Integration Testing:** This would test the interfaces between modules to ensure all the modules are interacting seamlessly with each other. This checks for data flow and integration problems across the system.
- **System Testing:** This is the testing of the whole system to verify whether it confirms to specified requirements and runs accurately under different conditions.

2. Usability Testing:

- **User Interface Evaluation:** This must relate to usability, intuitiveness, and accessibility. It is where feedback from probable users, including security officers, managers, and clients, will be needed in order to assess general user experience.
- **User Acceptance Testing:** The stakeholders and end-users would participate in UAT to ascertain that the system answers their needs and expectations. The defects or deviations that come to the fore during UAT will be addressed before implementation.

3. Performance Testing:

- **Load Testing:** It involves testing the system with numerous loads to verify it for its capacity to deal with the number of users and transactions of data without performance degradation.
- **Stress Testing:** This means testing the system under extreme conditions to test its robustness and stability. It will establish a point at which the system will break down and gracefully recover from failures.

4. Security Testing:

- **Vulnerability Assessment:** The system will be checked for probable security vulnerabilities, which may include data protection issues, user authentication, and access control.
- **Security Testing:** Security testing on the system will be done by attacking it to check upon its defense against unauthorized access and data breaches by simulating security attacks using ethical hacking techniques.

5. Performance Metrics Evaluation:

- System response time, transaction speed processed, and system uptime are some of the key performance indicators that shall be observed, analyzed, and conformed to required benchmark standards.

6. Continuous Feedback and Iteration:

- During the evaluation process, feedback obtained from the testing phases will be sourced and implemented where necessary. This iterative process will assure that the system evolves to meet user needs and technical standards.

By using these methods of evaluation, the project team shall ensure reliability, security, and usability of the system to achieve the objectives of Rakna Arakshaka Lanka Ltd by providing a robust platform for security management.

08.References

[1] "RALL," [Online]. Available: https://rall.lk/. [Accessed 01 August 2024].

[2] "TechCERT," [Online]. Available: https://www.techcert.lk/our_services/managed-security-services/. [Accessed 01 Aug 2024].

[3] "NoblePRog," [Online]. Available: https://www.nobleprog.lk/security-management/training/colombo. [Accessed 01 Aug 2024].

[4] "Gajashakthi," [Online]. Available: https://www.gajashakthi.lk/. [Accessed 01 August 2024].

[5] Agiles.org, "Agile Methodology," AGIEST, [Online]. Available: https://www.agilest.org/agile-methodology/. . [Accessed 30 July 2024].

[6] "What is MongoDB?," [Online]. Available: https://www.mongodb.com/company/what-is-mongodb. [Accessed 31 July 2024].

[7] "EXPRESS," [Online]. Available: https://expressjs.com/. [Accessed 30 July 2024].

[8] "React JS," [Online]. Available: https://react.dev/. [Accessed 30 July 2024].

[9] node, "Node JS," [Online]. Available: https://nodejs.org/en/about. [Accessed 30 July 2024].

[10] Wikipedia, "VisualStudio," [Online]. Available: https://en.wikipedia.org/wiki/Visual_Studio.

09.Appendix

Figure 4.1.1: System Diagram

- A system diagram represents the graphical form, which illustrates the constituents in a system and the interrelationship between them. Elements, in most cases, include inputs, processes, and outputs. Inputs are data or materials entering the system. Processes refer to activities by which inputs are transformed into outputs. Outputs refer to the results or products realized at the end. Further added, it would be the feedback loops and control mechanisms that assess and modify the performance of a system.

Table 5.1: Literature Review

- A literature review is an essential component of research or a project that provides a comprehensive analysis of existing knowledge on a given topic. It involves summarizing, evaluating, and synthesizing previous studies, theories, and research findings to establish a foundation for understanding the current state of knowledge in the field.

Figure 6.1.1: Agile Methodology

- Agile methodology is a flexible, iterative approach to software development that focuses on collaboration, customer satisfaction, and adapting to changing requirements. It involves regular feedback, continuous improvement, and delivering small, functional increments of the software.

Figure 6.3.1: Gantt Chart

- A Gantt chart is a project management tool that visually represents a project schedule. It shows tasks, their start and end dates, and dependencies on a timeline, helping to track progress and ensure the project stays on schedule.

Table 6.4.1: Work Breakdown Structure

- The Work Breakdown Structure (WBS) assigns tasks to team members to streamline the project.