Software Requirements Specification

for

Pileferage & Theft Prevention System (P&TPS)

Version 1.0 approved

Prepared by:

1) Surajit Hati (2106074)

2) Abhigya Ishan (2106086)

3) Dhananjay Sharma (2106112)

4) Kanishk Shukla (2106121)

5) Nilesh Kumar Thakur (2106126)

6) Rahul Kumar (2106142)

7) Spandan Basack (2106164)

11/11/2023

Table of Contents

Revision History

Name	Date	Reason For Changes	Version

Problem Statement

The objective of this project is to develop a comprehensive Logistic Pilferage and Theft Prevention System that effectively detects, prevents, and mitigates incidents of pilferage and theft in the logistics and supply chain industry. This system will utilize innovative technologies such as IoT sensors, GPS tracking, and data analytic to provide real-time monitoring and intelligent alerts. It aims to enhance the security and integrity of cargo shipments, reduce financial losses, and ensure the seamless flow of goods in the supply chain while complying with relevant regulations.

1. Introduction

1.1 Purpose

The purpose of the P&TPS application is to detect theft in the supply chain of cement bags and provide real-time notifications to users. The application will also allow users to track the current location of their shipments.

1.2 Project scope

The scope of the project includes the development of a web-based application that allows users to register cement bag shipments, monitor their movement, and receive theft alerts. The application will also provide a map-based interface to visualize the location of stolen cement bags

1.3 Intended Audience and Reading Suggestions

The intended audience for this Software Requirements Specification (SRS) document includes:

- Project stakeholders: This document provides a comprehensive understanding of the project's scope, features, and requirements for stakeholders such as project managers, product owners, and executives.
- Development team: The SRS document serves as a reference for the development team, helping them understand the project's goals, functionalities, and constraints.
- Quality assurance team: The document provides insights into the expected behavior of the application, helping the QA team in designing test cases and ensuring the application meets the specified requirements.
- Designers and UX/UI team: The SRS document provides an overview of the user interface requirements and features, aiding designers in creating an intuitive and user-friendly interface.

Reading Suggestions:

- Project stakeholders should read the entire document to gain a comprehensive understanding of the project's requirements and constraints.
- Development team members should focus on the functional requirements and system features sections to understand the specific functionalities they need to implement.
- Quality assurance team members should pay attention to the functional requirements and non-functional requirements sections to design appropriate test cases.
- Designers and UX/UI team members should focus on the user interface requirements and features sections to understand the design constraints and user expectations.

1.4 Features of the Project

- **User Registration and Login:**
  - Users can create an account and log in to the SupplyGuard application.
- **Shipment Registration:**
  - Users can register cement bag shipments with details such as source, destination, and expected delivery date.
- **Continuous Monitoring and Theft Detection:**
  - The system continuously monitors the movement of cement bags using sensors or RFID readers.
  - The system detects theft incidents by analyzing data from sensors or RFID readers.
- **Notification System:**
  - Users receive real-time notifications via email or SMS when theft incidents are detected.
- **Generation of Reports:**
  - Users can generate reports for analyzing theft patterns and vulnerabilities in the supply chain.

These features provide users with the ability to track their shipments, receive timely theft alerts and generate reports for analysis and decision-making.

1.5 References

https://www.gofclogistics.com/how-to-protect-your-supply-chain-from-cargo-theft/

2. Overall Description

2.1 Product Perspective

The P&TPS application will be a standalone system that interacts with sensors or RFID readers placed at checkpoints along the supply chain. It will communicate with a backend server to store and retrieve data.

2.2 Product Functions

- User registration and login
- Shipment registration with details such as source, destination, and expected delivery date
- Continuous monitoring of cement bag movement using sensors or RFID readers

- Theft detection and real-time notification to users
- Generation of reports for analyzing theft patterns

2.3 User Classes and Characteristics

The users of the P&TPS application include:

- Administrators: Responsible for managing user accounts and system settings.
- Shippers: Register cement bag shipments and track their movement.
- Recipients: Receive theft alerts and view the location of stolen cement bags.

2.4 Operating Environment

The SupplyGuard application will be web-based and accessible through modern web browsers. It will be developed using technologies such as React for the frontend and Node.js for the backend. The application will require an internet connection and access to the sensors or RFID readers.

2.5 Design and Implementation Constraints

- The application should be designed to handle a large number of registered shipments and theft alerts.
- The system should ensure the security and privacy of user data.
- The application should comply with relevant laws and regulations regarding privacy, data protection, and supply chain management.

2.6 User Documentation

User documentation will include user manuals and online help. These will be provided in digital formats (PDFs) and hosted on the system for easy access.

2.7 Assumptions and Dependencies

- **Hardware Infrastructure:**
  - The application requires sensors or RFID readers to monitor cement bag movement.
  - Users must ensure proper installation and functioning of hardware components.
- **Internet Connectivity:**
  - The application needs a stable internet connection for effective use.
  - Users require a reliable internet connection for real-time notifications and shipment tracking.
- **Sensor Integration:**

- The application depends on sensors or RFID readers at various checkpoints along the supply chain.
- Users must ensure proper installation and functioning of sensors for accurate theft detection.

- **Mapping Services:**
  - The application relies on mapping services to display the current location of stolen cement bags on a map.
  - Users must have access to mapping services and ensure their proper integration with the application.

- **User Authentication:**
  - The application assumes secure user authentication mechanisms, such as username and password.
  - Users should choose strong and unique passwords and keep their login credentials confidential.

2.8 System Features and Requirements

2.9 User Interfaces

The P&TPS application will have a web-based user interface that users can access through their web browsers. The user interface will be designed to be intuitive and user-friendly, allowing users to easily navigate through different sections and perform required actions. The interface will be responsive and compatible with different screen sizes and devices.

2.10 Hardware Interfaces

The P&TPS application relies on the integration of hardware components for monitoring the movement of cement bags and detecting theft incidents. The specific hardware interfaces required for the application will depend on the chosen sensor or RFID reader technology. The application should be compatible with the hardware interfaces provided by the chosen sensors or RFID readers.Software Interfaces.

2.11 Software Interfaces

- Database: The application will interact with a database system to store and retrieve data related to user accounts, shipment details, theft incidents, and other relevant information. The specific database system to be used will be determined during the development process.
- Mapping Services: The application will integrate with mapping services, such as Google Maps or Leaflet, to display the current location of stolen cement bags on a map. The integration will involve using APIs provided by the mapping service to retrieve and display the map data.

- Notification Services: The application will integrate with notification services, such as email or SMS gateways, to send real-time theft alerts to users. The integration will involve using APIs or protocols provided by the notification service to send notifications.

2.12 Communications Interfaces

- *Internet Protocol (IP): The application will communicate over IP networks to access the web-based user interface, interact with the backend API, and send/receive notifications.*

- *HTTP/HTTPS: The application will use the HTTP/HTTPS protocol to communicate between the user interface and the backend API. This protocol will be used for sending requests and receiving responses for various operations, such as user authentication, shipment registration, and theft alerts.*

- *Email/SMS Gateways: The application will utilize email or SMS gateways to send theft alert notifications to users. The specific protocols and APIs provided by the email or SMS gateway service will be used for communication.*

3.0) System Features and Requirements

- **User Registration and Login**
  - Users can create an account and log in to the SupplyGuard application
  - The system provides a user registration form to collect user details such as username and password
  - The system validates user input and ensures unique usernames
  - Users can log in using their registered credentials
  - The registration and login process is secure and protects user data

- **Shipment Registration**
  - Users can register cement bag shipments with relevant details
  - The system provides a form to collect shipment details such as source, destination, and expected delivery date
  - Each cement bag is assigned a unique identifier or RFID tag for tracking purposes
  - The system ensures the accuracy and integrity of the registered shipment data

- **Continuous Monitoring and Theft Detection**
  - The system continuously monitors the movement of cement bags and detects theft incidents
  - The system integrates with sensors or RFID readers placed at checkpoints along the supply chain
  - The system analyzes the data from sensors or RFID readers to identify suspicious activities or anomalies indicating theft

- The system provides real-time theft alerts to users

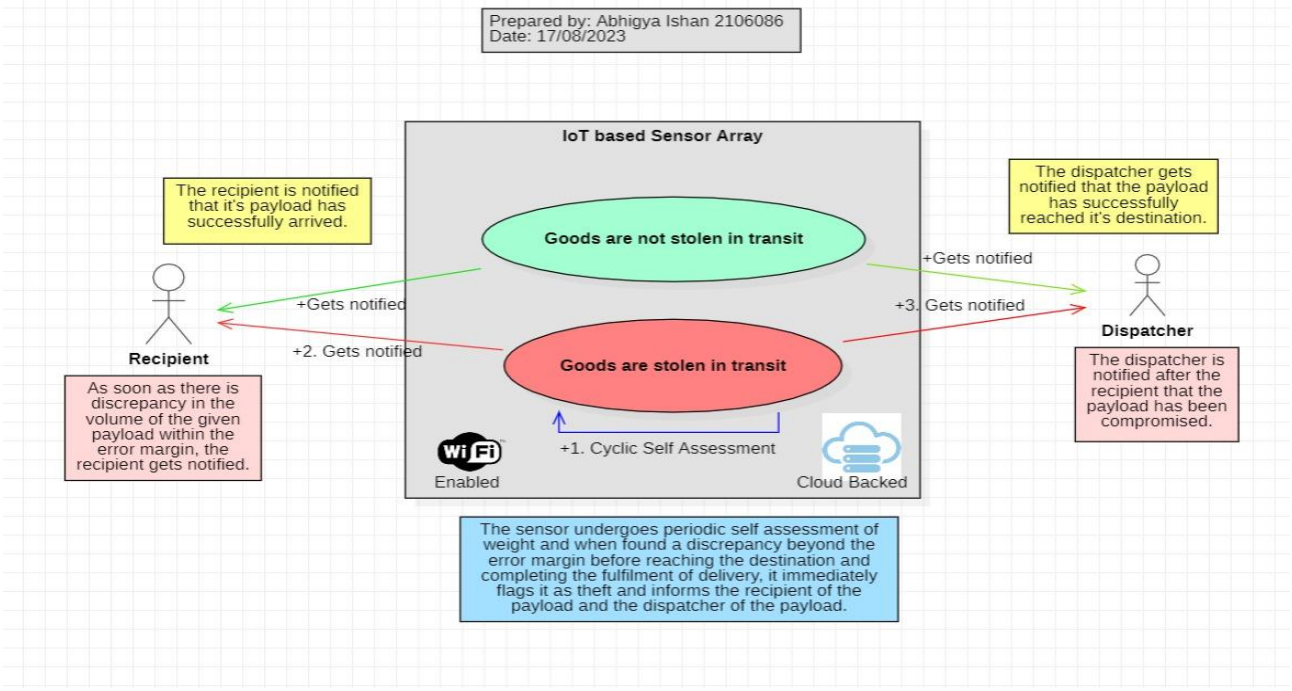
- **Notification System**

  - Users receive real-time notifications when theft incidents are detected
  - The system sends notifications to users via email or SMS
  - The notifications include details of the theft incident, such as the shipment ID and location
  - The notification system is reliable and delivers notifications in a timely manner

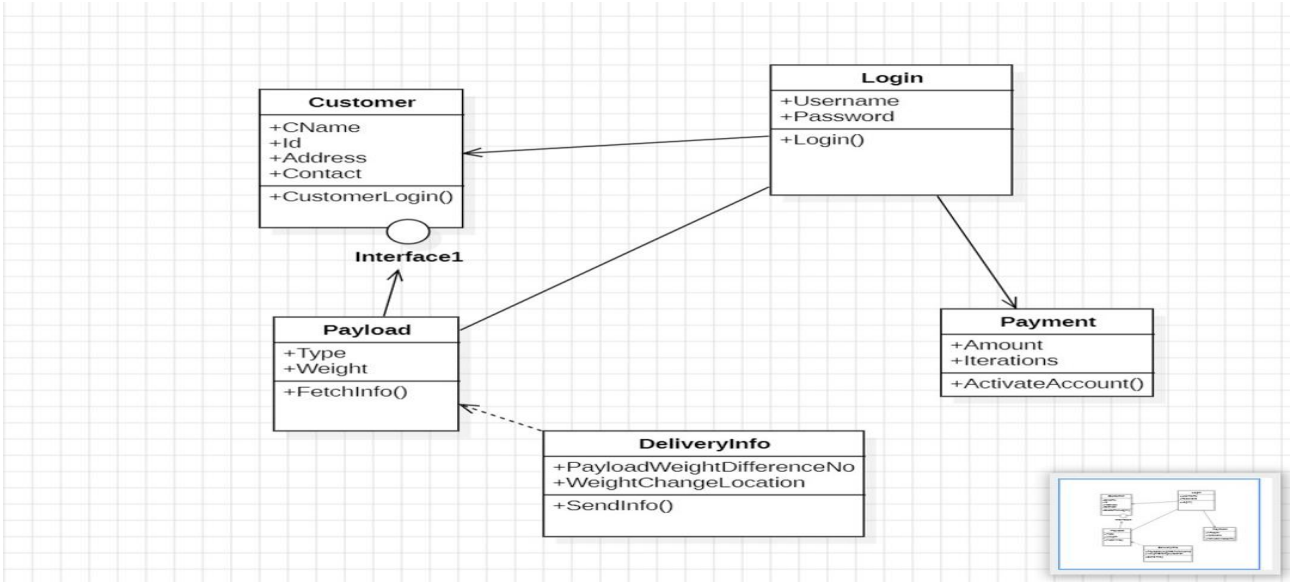
- **Generation of Reports**

  - Users can generate reports for analyzing theft patterns and vulnerabilities
  - The system provides functionality to generate reports based on theft incidents and historical data
  - The reports include visualizations and insights into theft patterns
  - The report generation is efficient and provides meaningful insights.

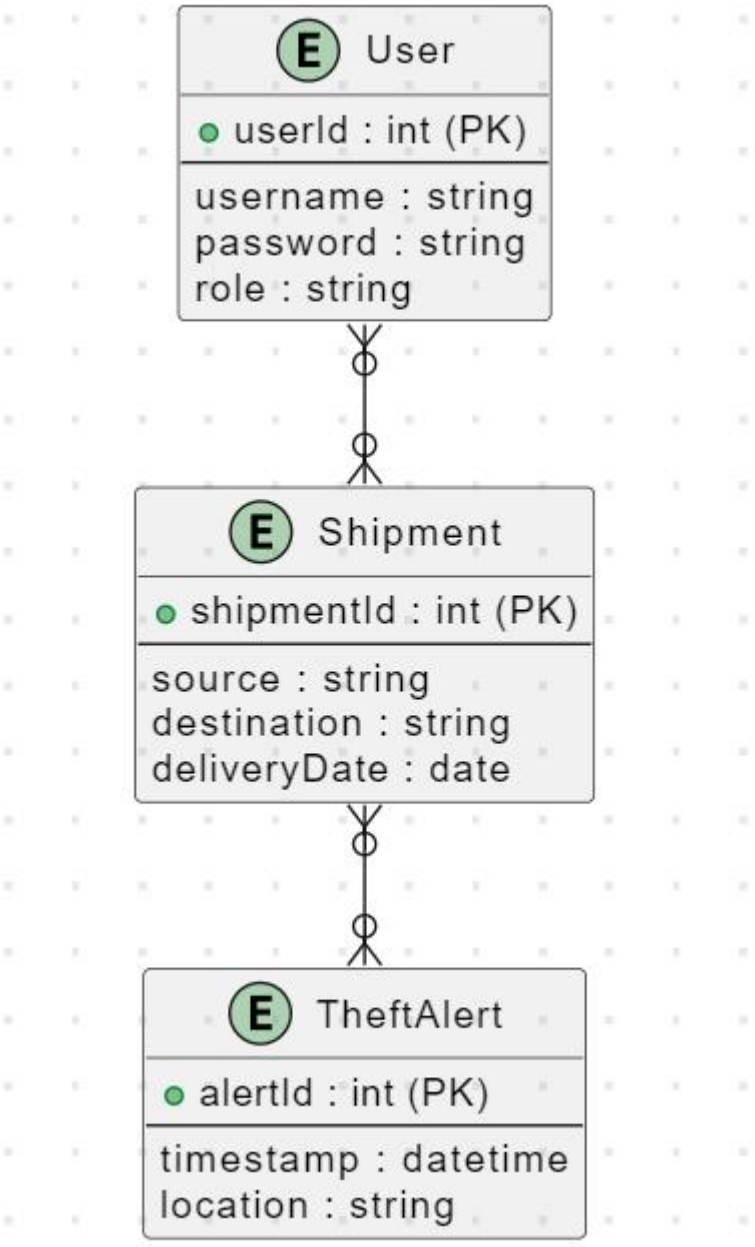
UML Diagram



Class Diagram

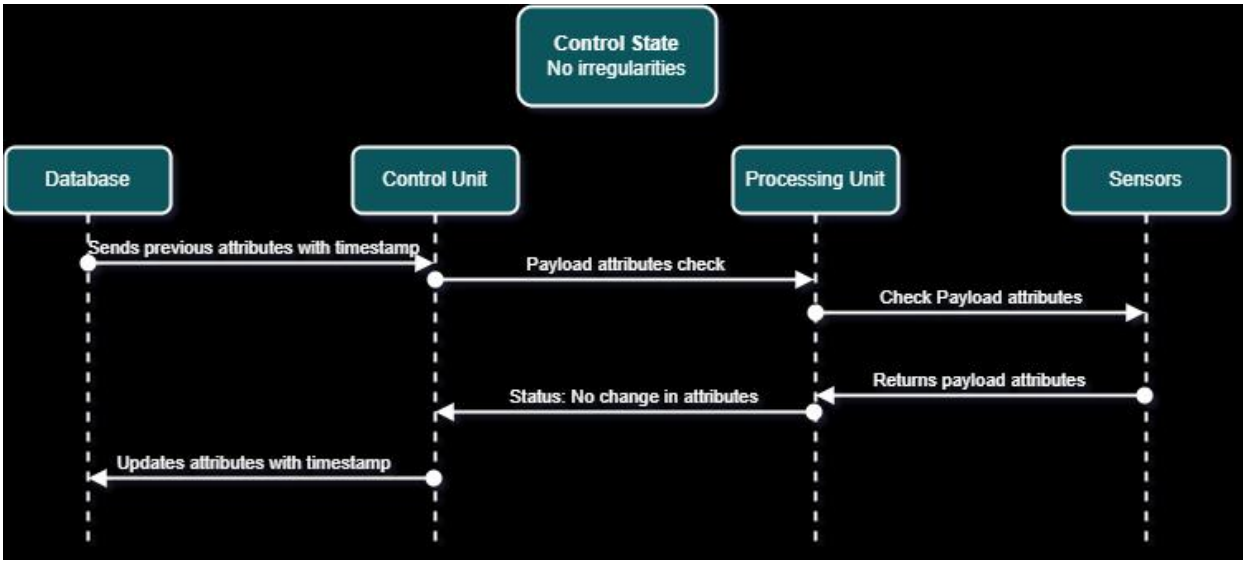


Entity-Relationship Diagram

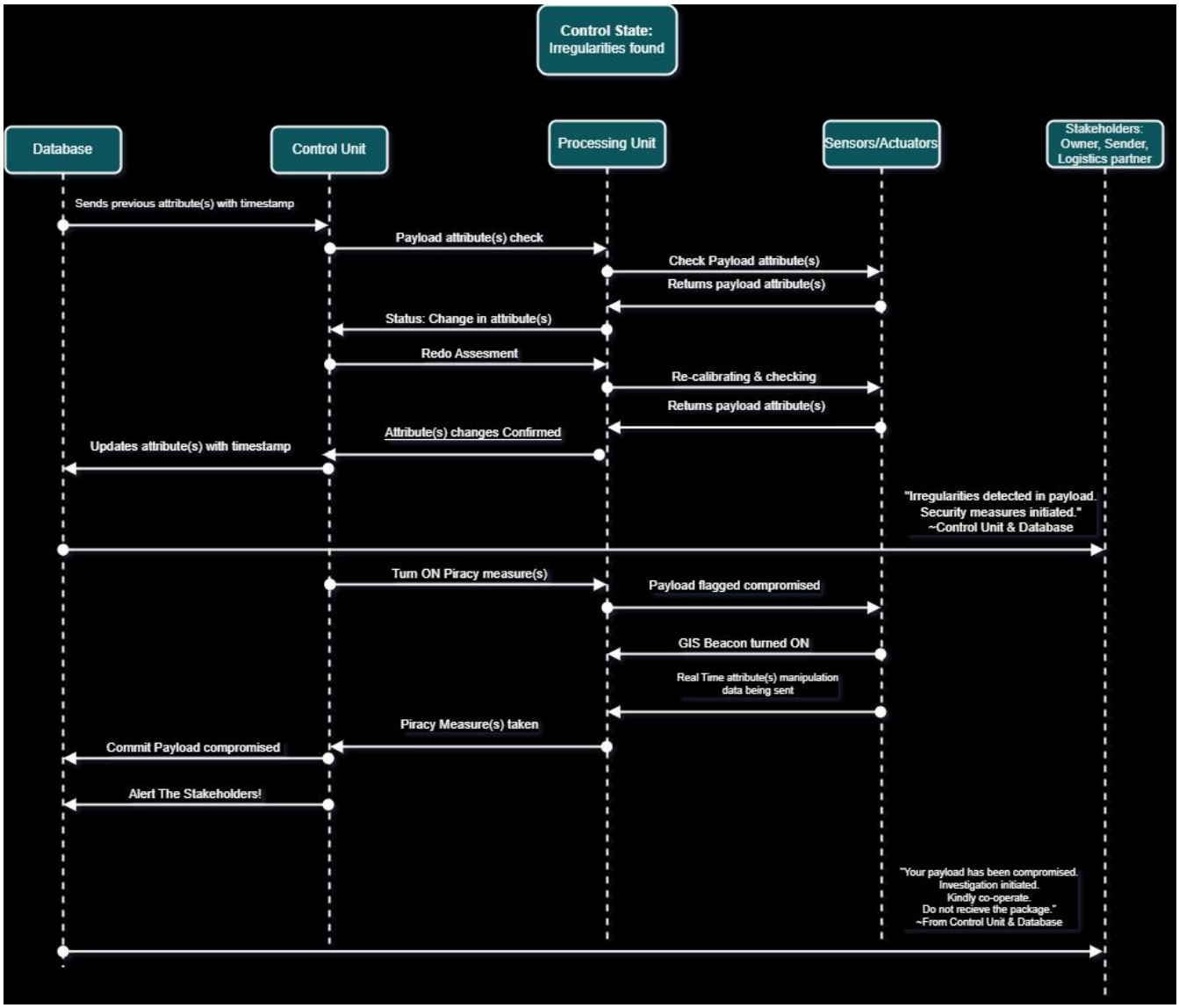


Sequence Diagrams for Controlled and Use case

Non Excited



Excited


Control State:
Irregularities found
Database
Control Unit
Processing Unit
Sensors/Actuators
Stakeholders:
Owner, Sender,
Logistics partner
Sends previous attribute(s) with timestamp
Payload attribute(s) check
Check Payload attribute(s)
Returns payload attribute(s)
Status: Change in attribute(s)
Redo Assesment
Re-calibrating & checking
Returns payload attribute(s)
Attribute(s) changes Confirmed
Updates attribute(s) with timestamp
"Irregularities detected in payload.
Security measures initiated."
~Control Unit & Database
Turn ON Piracy measure(s)
Payload flagged compromised
GIS Beacon turned ON
Real Time attribute(s) manipulation
data being sent
Piracy Measure(s) taken
Commit Payload compromised
Alert The Stakeholders!
"Your payload has been compromised.
Investigation initiated.
Kindly co-operate.
Do not recieve the package."
~From Control Unit & Database

*****