Application Requirements Document

Bike and Parts Management System (BPMS)

v1.0

Bhuvesh Gupta
bgupta1@umd.edu
UID: 117326611

Phase1 Document

Table of Contents

List of Figures

1.0 Introduction

1.1 Purpose

The purpose of this document is to build the Bike and Parts Management System or BPMS for short. It will describe the uses and features of the application, the interfaces involved, the functionality, use cases, the system constraints in which it will operate. This document is intended for stakeholders and the developers of the system.

1.2 Intended Audience

The BPMS application is intended to be used by the bike shop supervisors and university students who are currently enrolled at the university.

1.3 Scope

The BPMS is designed to ease the commute and help the students have better, healthier and environment friendly transportation options. The students at the university would have options to buy or rent bikes and buy parts/accessories. Bike shop supervis ors can also view the sales data along with managing student accounts. Supervisors can also view and manage the inventory at the bike shop.

2.0 Overall Description

2.1 System Environment

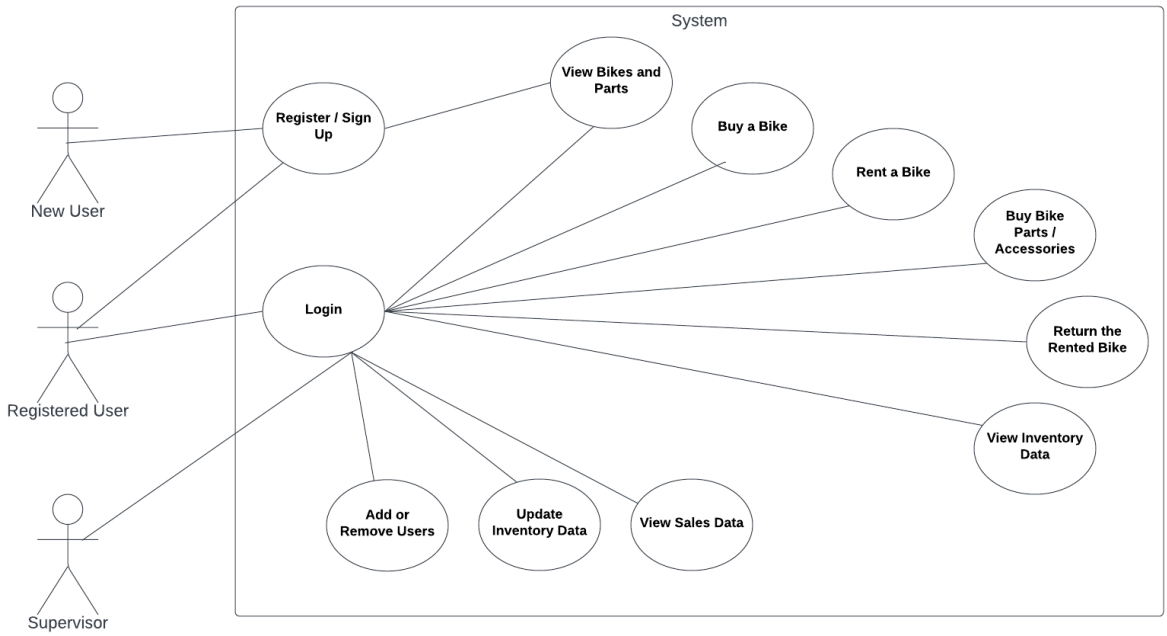

Figure 1: System Environment

The BPMS has 2 roles who are Users (New/Registered) and the Supervisors. New users would be able to view the bike and parts data and the registered users would be able to buy or rent bikes or buy parts/accessories. The supervisors would be able to view the sales data, manage the user accounts and update the shop inventory.

3.0 System Features and Requirements

3.1 Functional Requirements

3.1.1 View Bikes and Parts

Brief Description:

- Any user would be able to view the different types of bikes and parts available at the shop

Pre-Condition:

- User should have an internet connection and a browser to visit the webpage.

Step by Step Description:

- The user would open the browser and visit the webpage to view the bikes and parts available.

3.1.2 Buy a Bike

Brief Description:

- The authenticated user would be able to purchase the bikes based on their heights

Pre-Condition:

- The user should be a student at the university.
- The user should be logged in.

Step by Step Description:

- The user logs in to the BPMS with valid credentials.
- The user then clicks on the Purchase Bikes page.
- The user can choose amongst the several bike options for their purchase.
- Upon clicking the Checkout button, the user would then be redirected to the payment page for payments.

3.1.3 Rent a Bike

Brief Description:

- The authenticated user would be able to rent a bike for the semester.

Pre-Condition:

- The user should be a student at the university
- The user should be logged in
- The user does not have any pending bike returns

Step by Step Description:

- The user logs in to the BPMS with valid credentials.
- The user then clicks on the Bike Rentals page.
- The user can select the bike which it wants to rent for a semester.

- A due date would be given to the user for returning the bike after which there would be penalty.
- Then the user can click on Checkout from where it would be redirected to the payments page.

3.1.4 Return a Bike

Brief Description:

- The authenticated user would be able to return the previously rented bike.

Pre-Condition:

- The user should be a student at the university.
- The user should be logged in.
- The user should have already taken a bike for rent.

Step by Step Description:

- The user logs in to the BPMS with valid credentials.
- The user would be able to return the bike by going to Return Bike page and check the final bill if it has incurred any late submission charges by going over the due date.
- The user would be taken to the payment page for completing the transaction.

3.1.5 Buy Bike Parts/Accessories

Brief Description:

- The authenticated user would be able to buy the bike parts and accessories.

Pre-Condition:

- The user should be a student at the university.
- The user should be logged in.

Step by Step Description:

- The user logs in to the BPMS with valid credentials.
- The user then clicks on the Parts and Accessories page.
- The user would be able to select the desired parts and accessories.
- Then the user can click on Checkout to be redirected to the payments page.

3.1.6 View Inventory

Brief Description:

- The authenticated user would be able to view the inventory data to check for the number of items left in stock.

Pre-Condition:

- The user should be a student at the university.
- The user should be logged in.

Step by Step Description:

- The user logs in to the BPMS with valid credentials.
- The user then would be able to view the number of items left in stock along with the products (Bikes and Parts)

3.1.7 Add/Remove User Accounts

Brief Description:

- The supervisors would be able to manage the user accounts.

Pre-Condition:

- The supervisor must be logged in to the system.

Step by Step Description:

- The supervisor would login to the system
- The supervisor can visit the Students page from where it can Add, Modify or Delete a student record.

3.1.8 Update Inventory Data

Brief Description:

- The supervisors would be able to update and modify the inventory data.

Pre-Condition:

- The supervisor must be logged in to the system.

Step by Step Description:

- The supervisor would login to the system.
- Then they would be able to visit the Inventory page from where they can Add, Modify and Delete the inventory items.

3.1.9 View Sales Data

Brief Description:

- The supervisors can view the sales data to check their earnings.

Pre-Condition:

- The supervisor must be logged in to the system.

Step by Step Description:

- The supervisor would login to the system.
- The supervisor would be able to visit the Sales page to view the sales records and their earnings through the shop.

3.2 Use Cases

Use Case	View Bikes and Parts
Description	The users can visit the webpage and view the bikes, parts and accessories to buy or rent.

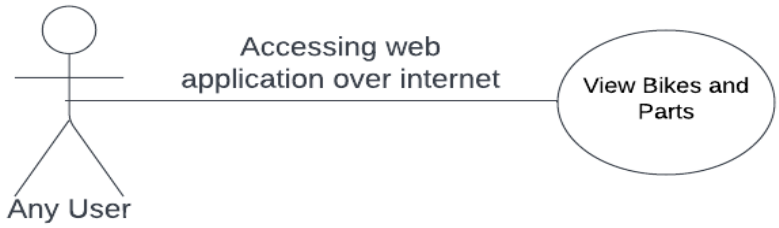

Figure 2: View Bikes and Parts

Use Case	Buy a Bike
Description	The authenticated user can go to Purchase Bike page and select a bike in stock which it wants to purchase and choose the bike size based on its height. Available heights would be S(Small), M(Medium) and L(Large). After checkout, the user would be taken to the payments page.

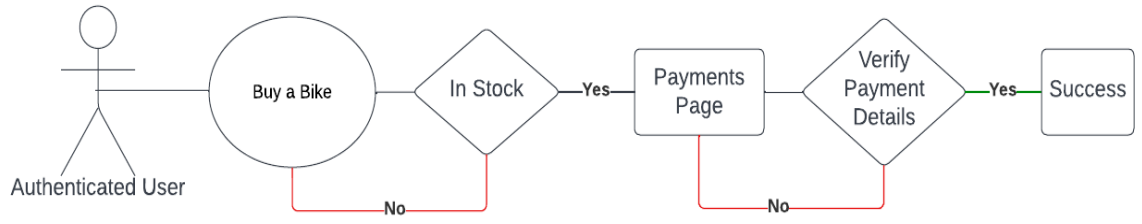

Figure 3: Buy a Bike

Use Case	Rent a Bike
Description	The authenticated user can visit Bike Rentals page to select a bike in stock which it wants to rent (for 1 semester) and choose the bike size based on its height. Available heights would be S(Small), M(Medium) and L(Large). After checkout, the user would be taken to the payments page. The user would also be given a due date before which the bike needs to be returned to avoid penalty.

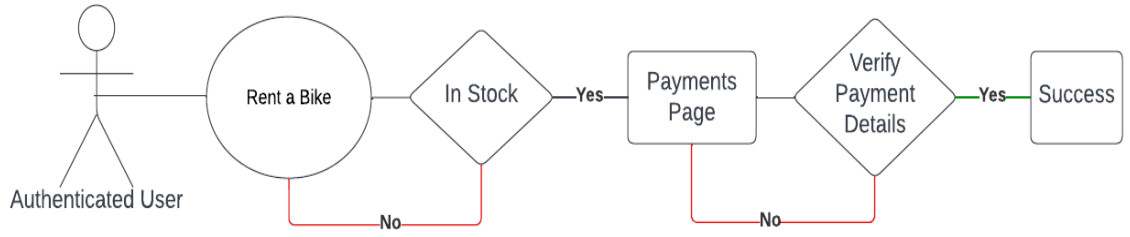

Figure 4: Rent a Bike

Use Case	Return a Bike

Description	The authenticated user can return the bike by visiting the Return Bike page. The user can then view the final bill (if any late charges incurred due to late submission) and would be taken to the payments page.

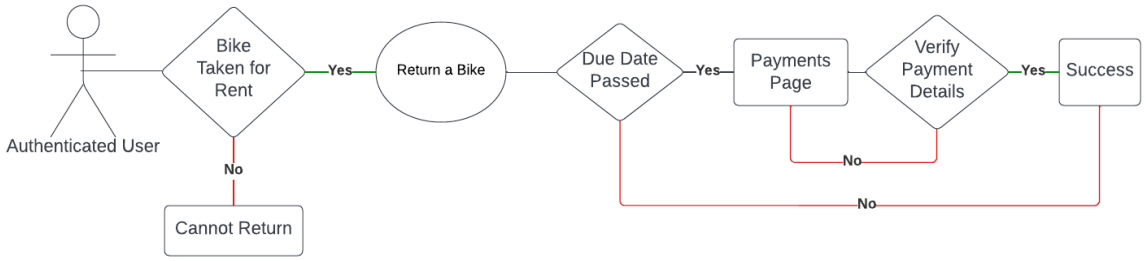

Figure 5: Return a Bike

Use Case	Buy Bike Parts/Accessories
Description	The authenticated user can visit the Parts and Accessories page to select the items in stock which it wants to buy. Upon clicking Checkout, the user would be redirected to the payments page.

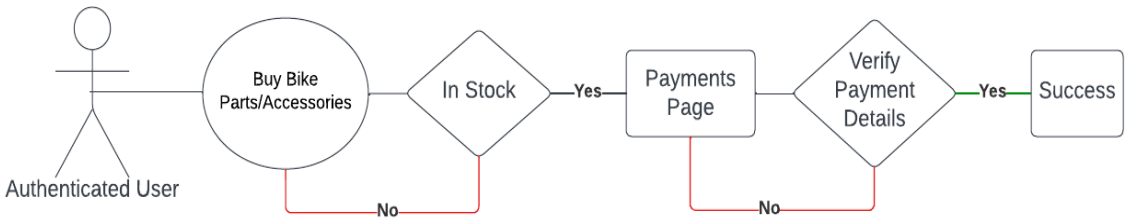

Figure 6: Buy Bike Parts/Accessories

Use Case	View Inventory

Description	The authenticated user would be able to see the items left in stock from where it is selecting the items to buy or rent.

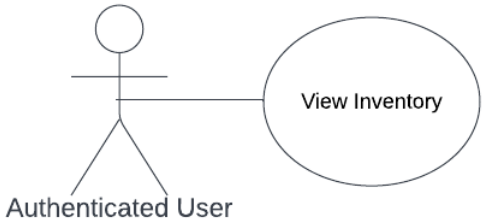

Figure 7: View Inventory

Use Case	Manage User Accounts
Description	The supervisor after logging in can visit the Students page to manage the student accounts. The accounts can be Added, Modified or Deleted.

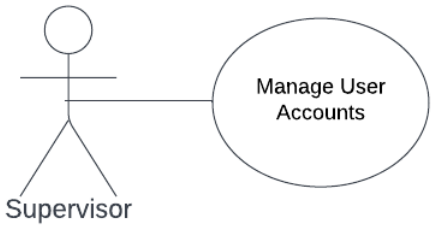

Figure 8: Manage User Accounts

Use Case	Update Inventory Data
Description	The supervisor after logging in can visit the Inventory page to Add, Modify and Delete items from the stock.

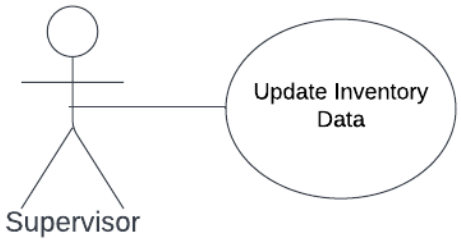

Figure 9: Update Inventory Data

Use Case	View Sales Data
Description	The supervisor after logging in can visit the Sales page and view the sales data to check their earnings from the shop.

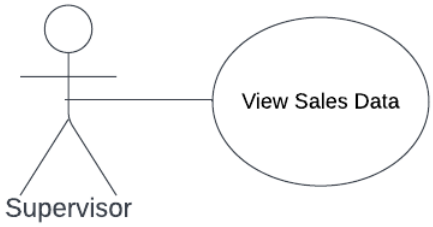

Figure 10: View Sales Data

4.0 Misuse Cases

Misuse Case	URL Tampering
Description	An attacker can modify or tamper with URL to execute a command or a script in the BPMS.
Prevention	URL validations and sanitization should be performed.

Misuse Case	Brute force Attack
Description	An attacker can try to brute force user accounts by trying out several different combinations of username and password until it gets successful
Prevention	Locking the user account for a certain amount of time if the number failed attempts reach 5 within a span of 5 minutes.

Misuse Case	Privilege Escalation
Description	An attacker or a normal user can find ways to access data and take actions which are only visible and available to the supervisors.
Prevention	Implementing the principle of least privilege and setting clear and distinct user roles. We can also implement input sanitization.

Misuse Case	Alumni or non-students Accessing Account
Description	Alumni or other non-students can try to access the website with their old credentials.

Prevention	The website should be kept updated with the list of current students and the accounts of alumni should be terminated.

Misuse Case	XSS Attack
Description	XSS attack can be performed on the website to either spoof a victim to some other page or cause a stored XSS attack and modify the website.
Prevention	Input sanitization and validation should be performed.

Misuse Case	Database Compromise
Description	An attacker may be able to compromise the database using SQL Injection and get all the stored information.
Prevention	Encrypting the database especially passwords using some strong hash algorithm.

5.0 Threat Model

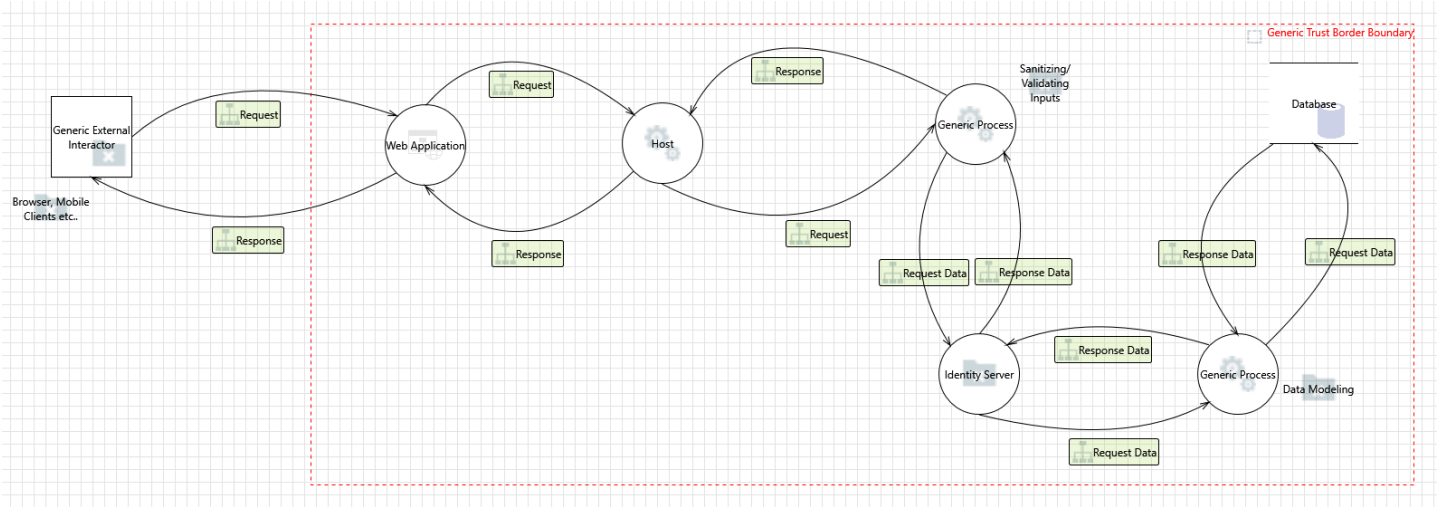

Figure 11: Threat Modelling

The model can have various threats such as:

Tampering- SQL Injection

An attacker can perform SQL Injection attack and modify any user or inventory information. It can lead to financial losses for the shop as well.

Denial of Service- DoS attack

An attacker can supply huge amount of traffic on the webserver in an attempt to make it unavailable to other students. It can also lead to financial losses for the shop as well as customer dissatisfaction.

Spoofing- Brute-force Credentials

An attacker can easily brute force weak passwords to gain access to other accounts.

6.0 Security Requirements

- To ensure only verified user access the portal, the users will have to enter their university ID and password.
- Strong password policies should be followed.
- Input validations and sanitization should be done at all the places.
- All the credentials should be encrypted and stored in the database.
- The actor's actions based on the roles should be restricted and defined. Only supervisors should be able to modify the inventory and user accounts.
- URLs should also be sanitized and always validated.
- Use static and dynamic security analysis tools that will provide necessary security feedback.
- Add proper unit test cases for each module and integration test for the whole system.
- User should be logged out from the session if the session was idle for 5 minutes or if the browser tab/window was closed.
- The logs should be written for every successful login, unsuccessful login, account changes, inventory changes and sales data. The logs should also be descriptive about the event that was recorded.
- The system should be backed up in a secure location every 24 hours in a physical drive and cloud so that in case of an emergency situation, the system can be revived.
- BPMS web application should be accessed on HTTPS connection so that the channel is secure.
- Software development should follow the security development life cycle and other security standards.
- Use the principle of least privilege.

7.0 Detailed Non-Functional Requirements

7.1 Scalability

The web application is scalable and can handle high number of requests when the traffic on server increases. Probably at the beginning of the semester there would be increased traffic as everyone would be looking to buy or rent a bike and at the end of the semester too there would high traffic as students would be looking to return their bikes before due date.

7.2 Availability

The web application remains available to be accessed by the users so that they can view products and make purchases.