COMPUTER SCIENCE AND ENGINEERING
SOFTWARE ENGINEERING II
2025 - 2026

RASD

Requirement Analysis and Specification Document

Authors:

- Dai Run Jie Simone - 10766478
- Yang Jiaxin - 10719178
- Zheng Jiayi - 10811585

Contents

1.1 Purpose....4
1.1.1 Goals....4
1.2 Scope.... 5
1.2.1 World Phenomena....6
1.2.2 Machine Phenomena.... 6
1.2.3 Shared Phenomena.... 7
1.3 Definitions, Acronyms, Abbreviations....8
1.3.1 Definitions....8
1.3.2 Acronyms.... 9
1.4 Revision History....10
1.5 Reference Documents.... 10
1.6 Document Structure....10
2.1 Product perspective....12
2.1.1 Scenarios.... 12
2.1.2 Domain Class Diagrams....14
2.1.3 State Diagrams....14
2.2 Product Functions.... 15
2.3 User characteristics....16
2.3.1 Registered Users....16
2.3.2 Guest Users.... 16
2.4 Assumptions, dependencies and constraints....16
2.4.1 Regulatory policies.... 16
2.4.2 Domain Assumptions.... 16
3. Specific Requirements.... 18
3.1 External Interface Requirements.... 18
3.1.1 User Interfaces.... 18
3.1.2 Hardware Interfaces....24
3.1.3 Software Interfaces.... 24
3.1.4 Communication Interfaces....24
3.2 Functional Requirements.... 25
3.2.1 Use Case Diagram....26
3.2.2 Use Cases....27
3.2.3 Sequence Diagram....35
3.2.4 Mapping on Goals.... 41
3.3 Performance Requirements.... 43
3.4 Design Constraints.... 43
3.4.1 Standards Compliance....43
3.4.2 Hardware limitations....44
3.4.3 Any other constraint.... 44
3.5 Software System Attributes.... 45
3.5.1 Reliability....45
3.5.2 Availability.... 45

3.5.3 Security.......... 45
3.5.4 Maintainability.......... 45
3.5.5 Portability.......... 45
4. Formal Analysis Using Alloy.......... 46
4.1 General Part.......... 46
4.2 User and Trip Part.......... 46
4.3 Bike Path Reports.......... 47
4.4 Temporal Constraints and Evolution.......... 48
Report evolution.......... 48
Publication rules.......... 48
Freshness and consistency.......... 48
4.5 Examples.......... 49
Example 1 – Typical evolution of reports.......... 49
Example 2 – Waiting in the same state.......... 49
Example 3 – Conflicting reports resolved by freshness.......... 50
4.6 Assertions.......... 51
5. Effort Spent.......... 52
6. References.......... 53

1| Introduction

Online platforms supporting outdoor mobility and community-driven mapping have become increasingly valuable resources for cyclists and urban commuters. These systems allow users to access reliable route information, benefit from shared experiences, and contribute to enhancing the safety and quality of existing infrastructures. In particular, applications focused on bike paths can significantly improve the cycling experience by helping riders identify optimal routes, avoid hazards, and monitor their personal performance.
The *Best Bike Paths* (BBP) platform embraces this vision by combining user-generated data, real-time device-based sensing, and route evaluation mechanisms. Through its collaborative approach, BBP encourages cyclists to share insights about path conditions, obstacles, and overall usability, enriching a continuously updated inventory of bike routes accessible to the entire community.
Furthermore, the system supports advanced trip tracking features, allowing users to monitor their cycling activities and analyse statistics such as travelled distance, average speed, and environmental conditions. By merging contributions from multiple users and considering their freshness and level of agreement, BBP aims to provide trustworthy and actionable information that benefits both casual cyclists and more experienced riders.

1.1 Purpose

The purpose of this document is to present a detailed description of the *Best Bike Paths* system. It is addressed to the developers who will implement the system's functionalities and may serve as a formal agreement between the customer and the development team. Additionally, this document provides the customer with a clear, precise, and unambiguous description of the system's functionalities, operational modes, and constraints, ensuring a shared understanding of the system's expected behaviour.

1.1.1 Goals

The following table provides an overview of all the goals identified for the BBP system.

ID	DESCRIPTION
G1	**Users** would like to record their cycling trips and store them.
G2	**Users** would like to have statistics and performance metrics for each trip.
G3	**Users** would like to enrich their trip data with meteorological information when available.
G4	**Users** would like to manually provide information about bike paths.
G5	**Users** would like to acquire bike path data.
G6	**Users** would like to review, confirm, or correct automatically detected bike path issues.
G7	**Users** would like to publish bike path information for the community at the end of

	cycling.
G8	**Users** would like to explore and compare available bike path options between a specified origin and destination.
G9	**The system** shall merge publishable bike path information provided by multiple users.
G10	**The system** shall keep bike path condition information consistent with the most recent publishable user reports.
G11	**The system** shall allow all users to access publishable bike path information.

Table 1.1: Goals Table

1.2 Scope

The Best Bike Paths (BBP) system is designed to support cyclists in discovering, recording, and sharing information about bike-friendly routes.
Its primary goal is to improve the quality of cycling experiences by collecting, aggregating, and visualizing data about bike paths, their conditions, and their suitability for reaching specific destinations. By combining user-contributed data with automatically collected information, BBP provides value to both individual cyclists and the broader cycling community.

The platform allows registered users to record their cycling activities and maintain a personal history of trips. For each recorded trip, BBP computes and presents relevant statistics such as total distance, duration, average speed, and other performance indicators. When available, trip data can be enriched with meteorological information, including weather conditions, temperature, and wind speed, retrieved from external services, enabling users to better understand the context in which their activities took place.

Beyond personal tracking, BBP enables registered users to contribute information about bike paths. Users can describe paths in terms of the streets involved, their overall status (e.g., optimal, medium, or requiring maintenance), and the presence of relevant obstacles such as potholes or surface irregularities. Information can be inserted manually or acquired automatically while cycling. In the automated mode, BBP infers that a user is biking based on movement speed, reconstructs the followed path using GPS data, and analyzes accelerometer and gyroscope signals to detect potential issues along the route. Since such detections may include false positives, users are required to review, confirm, or correct the collected information before making it available to others.

All information provided to BBP can be marked as publishable by its owner. Publishable data contribute to a shared knowledge base that can be accessed by any user, including unregistered ones. Users can specify an origin and a destination and request the visualization of one or more bike paths between these points on a map. When multiple alternatives are available, BBP ranks and displays them according to a computed score that reflects both the quality of the path, based on its status and reported issues, and its effectiveness in reaching the destination.

When multiple users provide publishable information about the same bike path, BBP merges these contributions by considering their freshness and the level of agreement among users. Conflicting assessments are resolved by favoring the most recent and most frequently confirmed data, allowing the system to adapt over time to changes in path conditions. Through this combination of personal activity tracking, collaborative data collection, and intelligent path evaluation, BBP aims to foster a reliable, community-driven platform for identifying and promoting the best bike paths.

1.2.1 World Phenomena

The following section summarizes the previous description into a list of phenomena (events) that occur in the world of interest for the system to be developed. Phenomena are interpreted as events occurring in the whole domain that is being analyzed and are therefore described without constraints, which will be specified in the requirements section. We only focus on the main mechanism of our app.

World phenomena are events happening outside the system and on which the system has no control.

ID	DESCRIPTION
WP1	**A user** rides a bicycle along bike paths.
WP2	**A bike path** changes its physical condition over time.
WP3	**Obstacles** may be present on a bike path.
WP4	**Weather conditions** vary over time.
WP5	**Maintenance activities** may affect the condition of a bike path.
WP6	**A user** chooses an origin and a destination for a trip.

Table 1.2.1: World Phenomena Table

1.2.2 Machine Phenomena

Machine phenomena are events happening internally in the system, independent from the outside world.

ID	DESCRIPTION
MP1	**The system** stores and manages data related to users, trips, and bike paths.
MP2	**The system** computes statistics for recorded trips.
MP3	**The system** reconstructs bike paths from collected location data.

MP4	**The system** computes a quality score for each bike path.
MP5	**The system** evaluates freshness and consistency of bike path information.
MP6	**The system** merges multiple assessments of the same bike path into a single representation.
MP7	**The system** associates meteorological data with recorded trips.

Table 1.2.2: Machine Phenomena Table

1.2.3 Shared Phenomena

Shared phenomena are events that influence both the system and the surrounding world. They are further divided into:

- **World-controlled shared phenomena:** events initiated by entities in the world that impact the system.
- **Machine-controlled shared phenomena:** events initiated by the system and observable in the world or affecting users.

ID	DESCRIPTION
WSP1	**User** manually inserts information about a bike path.
WSP2	**User** starts recording a cycling trip.
WSP3	**User** stops recording a cycling trip.
WSP4	**User** reviews, confirms, or corrects automatically collected bike path information.
WSP5	**User** makes information as publishable.
WSP6	**User** requests bike paths between an origin and a destination.

Table 1.2.3 (1): World-Controlled Shared Phenomena Table

ID	DESCRIPTION
MSP1	**The system** acquires location data related to a **user**'s cycling activity.
MSP2	**The system** acquires motion-related data during a cycling activity.
MSP3	**The system** presents trip statistics to the **user**.
MSP4	**The system** visualizes bike paths on a **map**.
MSP5	**The system** presents ranked alternative paths to the **user**.
MSP6	**The system** makes publishable bike path information accessible to **users**.

Table 1.2.3 (2): Machine-Controlled Shared Phenomena Table

1.3 Definitions, Acronyms, Abbreviations

1.3.1 Definitions

A brief list of the most meaningful and relevant terms and synonyms used in this document is reported here, in order to make reading process smoother and clearer:

TERM	DESCRIPTION
Bike Path	A path intended for people riding bicycles. Where a proper bike track exists or where cars are rare and speed limits are compatible with the average speed of a bike.
Registered User	A person who has an account on the platform.
Trip	A cycling activity from one place to another.
Trip Recording, Activity Tracking	An activity that allows a registered user to record a cycling session while the system collects data related to the trip.
Trip Statistics Computation, Performance Evaluation	A system capability that calculates metrics such as total distance, average speed, and other performance indicators for recorded trips.
Meteorological Data Enrichment	A functionality through which weather-related information retrieved from an external service is associated with recorded trips.
Manual Path Insertion, Manual Mode	A user-driven operation in which information about bike paths is explicitly entered, including street names and path status.
Automated Path Insertion, Automated Mode	A system-supported operation in which information about bike paths is automatically collected while the user is cycling using mobile device data.
Biking activity Detection	A system inference mechanism that determines whether a user is cycling based on detected movement speed.
Path Reconstruction	A system operation that rebuilds the followed bike path by analyzing collected GPS location data.
Accelerometer	A device that measures acceleration.
Gyroscope	A sensor that is used for measuring or maintaining orientation and angular velocity.
Obstacle Detection	A detection mechanism that identifies potential

	obstacles, such as potholes, by analyzing accelerometer and gyroscope data.
False Positive Handling	A validation activity that allows users to review, confirm, or correct automatically detected obstacles.
User Confirmation, Data Validation	A user interaction through which automatically collected information is verified before being made available to others.
Publishable Information	Information that can be known to the public.
Route Search	A user-initiated request in which an origin and a destination are specified to obtain suitable bike paths.
Route Visualization, Map Display	A visual presentation of one or more bike paths on a map interface.
Path Scoring	An evaluation mechanism that assigns a score to bike paths based on their condition and effectiveness.
Path Ranking, Route Ordering	A comparison activity that orders multiple bike paths according to their assigned scores.
Information Aggregation, Data Merging	A consolidation activity that combines contributions from multiple users describing the same bike path.
ISO/IEC 27001	Defines the requirements for establishing, implementing, maintaining, and continually improving an information security management system aimed at protecting the confidentiality, integrity, and availability of information.

Table 1.3.1: Definitions Table

1.3.2 Acronyms

A list of acronyms used throughout the document for simplicity and readability:

1. RASD: Requirements Analysis and Specification Document.
2. BBP: Best Bike Path.
3. GPS: Global Positioning System.
4. UC: Use-Case.
5. GDPR: General Data Protection Regulation.

1.4 Revision History

- 20/12/2025: identified several inconsistencies and errors in the document. The affected sections were reviewed and updated.
- 22/12/2025:

1.5 Reference Documents

Here's a list of reference documents that have been used in order to shape the Requirements Analysis and Specification Document of the Best Bike Path system.
In the following, all external sources of information that have contributed to the design of this document are mentioned.
- Specification Document Assignment.
- IEEE Standard Documentation For RASD.
- Stakeholders' specification provided by the R&DD assignment for the Software Engineering II course at Politecnico Di Milano.

1.6 Document Structure

The document is divided into six sections, each with its unique focus, as outlined below.

Introduction: In the first section, we lay out the project's objectives, purposes, and offer a concise examination of global and shared phenomena. This section also includes a compilation of abbreviations and definitions that are essential for comprehending the problem.
- The Purpose section outlines the reasons motivating the existence of the product.
- The Scope section identifies the product and application domain.

Overall Description: The second section provides a comprehensive overview of the problem. It delves into further details about the domain and various scenarios involved, in addition to discussing product and user characteristics, assumptions, dependencies and constraints.
- The Product Perspective section defines the system's relationship to other products. Describes external interfaces: system, user, hardware, software.
- The Product Functions section summarises the major functions.
- The User Characteristics section describes the general characteristics of the intended groups of users, including those that may influence usability.
- The Assumptions, Dependencies, Constraints section describes anything that will limit the developer's options.

Specific Requirements: The third section is dedicated to an in-depth analysis of the specific requirements. It offers detailed insights into external interface requirements, functional requirements, and performance requirements.

Formal Analysis Using Alloy: The fourth section employs Alloy to conduct a formal analysis. This chapter's primary purpose is to validate the accuracy of the model described in the preceding sections. A brief presentation of the main objectives driving the formal modeling activity, as well as a description of the model itself, what can be proved with it, and why that is important given the problem at hand. It focuses on presenting the results of the conducted checks and meaningful assertions.

Effort Spent: Section five outlines the individual efforts contributed by each group member to compose this document. In this section we will include information about the number of hours each group member has worked for this document.

References: The final section serves as a bibliography, listing the references and additional resources used in the creation of this document.

2| Overall Description

2.1 Product perspective

This section presents a set of representative scenarios describing typical interactions between users and the Best Bike Paths (BBP) system. The scenarios aim to illustrate how the system is expected to be used in realistic situations and to clarify the functional requirements derived from the problem description. They are expressed at a high level, focusing on observable interactions between actors and the system, and deliberately avoid assumptions about implementation details or design solutions.

2.1.1 Scenarios

Scenario 1: Recording a Personal Bike Trip by a Registered User.
A registered user starts a bike ride and activates the BBP application on their mobile device. While the user is biking, BBP records GPS points to reconstruct the **route** followed during the trip and computes basic performance metrics such as the total distance covered and the average speed. When available, BBP retrieves meteorological information from an external weather service and associates it with the recorded bike trip. At the end of the ride, the user stops the recording and stores the trip, which becomes part of their personal trip history and can be accessed later for review.

Scenario 2: Manual Insertion of Bike Path Information by a Registered User
A registered user wants to contribute information about a bike path they know. Using BBP, the user manually defines a **bike path** by specifying one or more **path segments**, each corresponding to a continuous portion of the path. For each path segment, the user indicates the current path condition, such as optimal, medium, or requiring maintenance. After reviewing the inserted information, the user marks the corresponding reports as publishable. Once published, the bike path information becomes available to other users of the system.

Scenario 3: Automatic Collection and Confirmation of Bike Path Conditions by a Registered User
A registered user enables the automated mode of BBP before starting a bike ride. While the user is biking, the system detects the biking activity based on the user's speed and collects GPS points to reconstruct the traveled route. At the same time, BBP acquires data from the mobile device's sensors, such as the accelerometer and gyroscope, to identify potential anomalies that may indicate the presence of potholes or other obstacles along specific **path segments**.
At the end of the ride, BBP presents the automatically collected reports associated with the identified path segments to the user, who reviews and confirms or corrects them. After confirmation, the reports can be marked as publishable.

Scenario 4: Viewing Personal Profile and Recorded Trips by a Registered User
A registered user accesses the BBP system and opens their personal area. The system presents the user's profile information together with the list of previously recorded bike trips. For each recorded trip, BBP displays the associated route reconstructed from GPS

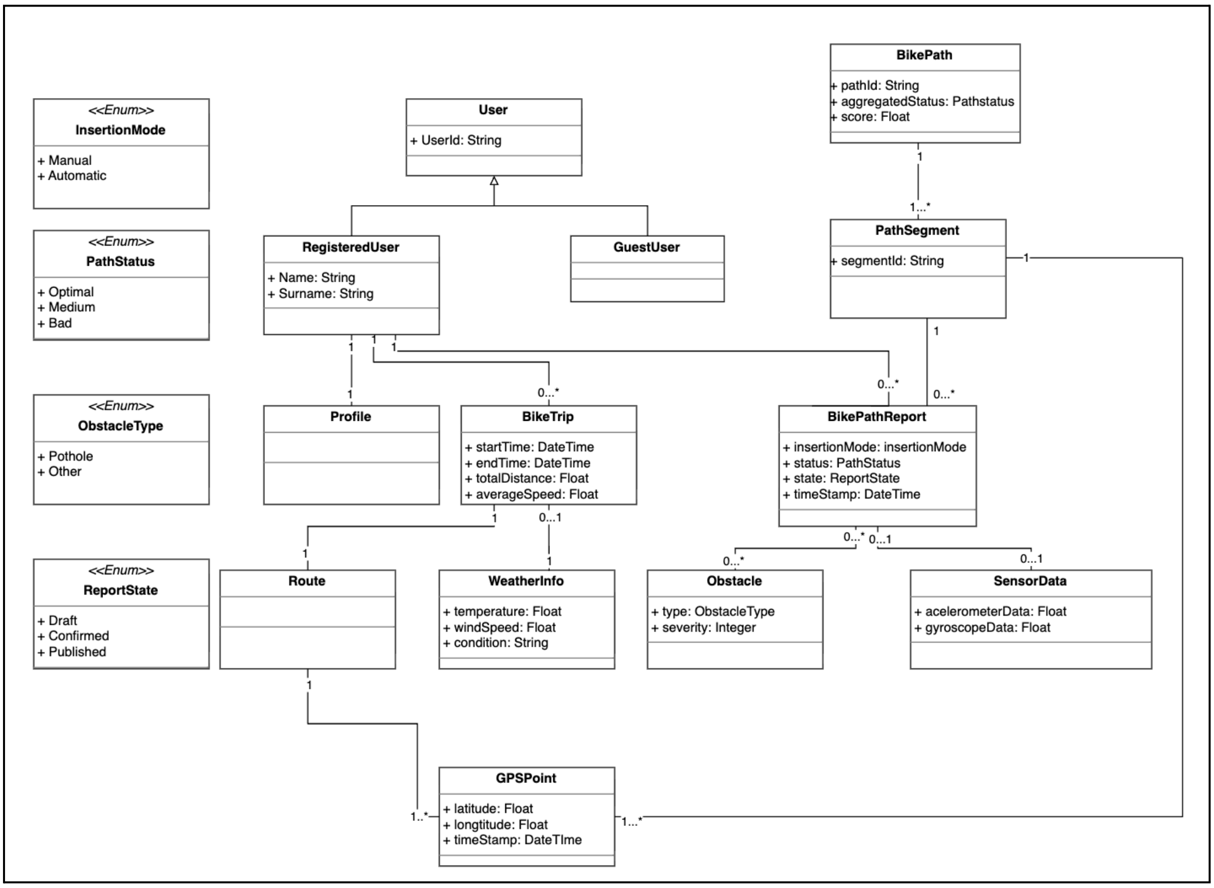
points and the main statistics, such as total distance and average speed. The user can browse their trip history and inspect the details of individual recordings.

Scenario 5: Browsing Bike Paths Between an Origin and a Destination by Any User
Any user opens the BBP system and specifies an origin and a destination. The system retrieves the available bike paths connecting the two locations and presents them together with aggregated information, such as distance, estimated travel time, and overall path condition. The overall condition of a bike path is derived from the conditions of its path segments. This information supports the user in comparing alternatives and selecting a suitable route.

Scenario 6: Merging Bike Path Information Provided by Multiple Registered Users
Over time, multiple registered users provide publishable reports related to the same **path segments** of a bike path. BBP collects this information and merges it by considering both the freshness of the reports and the number of users providing consistent evaluations for each segment. When conflicting information is available for a path segment, the system applies predefined rules to determine a consolidated segment condition. The overall status of a bike path is then derived by aggregating the consolidated conditions of its path segments and is used when presenting bike paths to users querying the system.

2.1.2 Domain Class Diagrams

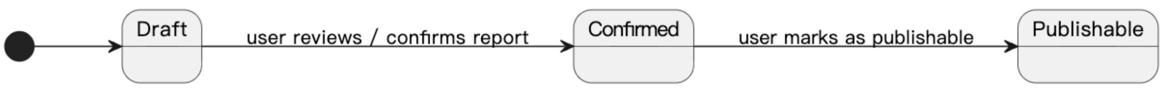
The class diagram provided below offers a high-level overview of the domains of interest for the software implementation.



2.1.3 State Diagrams

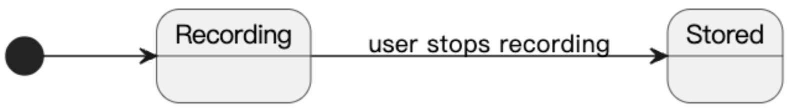
In this section, we analyze the state diagrams related to the bike path report and the bike trip creation. We believe these two scenarios are the most significant to represent with this type of diagram due to their structured sequences of well-defined events.

BikePathReport



A BikePathReport represents user-provided information about the condition of a path segment. A report is initially created in the Draft state, either through manual insertion or automatic data collection. After reviewing the information, the user can confirm it, causing the report to move to the Confirmed state. Once the user decides to share the information with other users, the report enters the Publishable state. Only reports in the publishable state are used by the system to merge information and compute aggregated path conditions.

BikeTrip



A **BikeTrip** is created when a registered user starts recording a bike ride.
While the ride is ongoing, the trip is in the **Recording** state, during which GPS data and performance metrics are collected. When the user stops the recording, the trip transitions to the **Stored** state and becomes part of the user's trip history.

2.2 Product Functions

This section presents a detailed list of functional requirements that the Best Bike Paths (BBP) system must fulfill during its development. Functional requirements describe the operations and decisions that the system is required to perform in order to meet the needs of its stakeholders. These requirements have been derived through an elicitation and abstraction process discussed in the previous sections of this document. The analysis of the domain, the identification of relevant phenomena, the validation of user needs through scenarios, and the use of supporting diagrams provide a solid foundation for the design activities presented in the subsequent part of this document.

Record a Bike Trip
The system allows a registered user to record a bike trip. During recording, the system collects GPS points to reconstruct the traveled route and computes performance metrics such as total distance and average speed. When available, meteorological information is associated with the recorded trip. At the end of the ride, the trip is stored and becomes part of the user's trip history.

View Personal Profile and Recorded Trips
The system allows a registered user to access their personal area. The user can view profile information and browse the list of previously recorded bike trips. For each trip, the system provides access to the reconstructed route and the associated statistics.

Manually Insert Bike Path Information
The system allows a registered user to manually insert information about a bike path. The user defines the path through one or more path segments and specifies the condition of each segment. The inserted information is initially stored as a draft report and can later be marked as publishable.

Automatically Collect Bike Path Condition and Weather Information
The system allows a registered user to enable an automated mode during a bike ride. While the user is biking, the system collects GPS and sensor data to infer bike path conditions and, when available, acquires weather information. The collected data are associated with the corresponding path segments and stored as draft reports pending user confirmation.

Confirm and Publish Bike Path Reports
The system allows a registered user to review, confirm, or correct bike path reports generated either manually or automatically. After confirmation, the user can mark reports as publishable, making them available for aggregation and community use.

Merge Bike Path Information
The system merges publishable reports provided by multiple registered users. The merging process considers the freshness of reports and the number of consistent evaluations for each

path segment. The aggregated segment conditions are used to derive the overall status of a bike path.

Browse Bike Paths Between an Origin and a Destination
The system allows any user, registered or not, to browse available bike paths between a specified origin and destination. For each path, the system presents aggregated information such as distance, estimated travel time, and overall path condition to support route selection.

2.3 User characteristics

2.3.1 Registered Users

Registered users have access to the full functionality of the BBP system. They can record bike trips, view their personal trip history, and provide information about bike paths by manually inserting or automatically collecting path segment reports. Registered users can review, confirm, and mark their reports as publishable.

2.3.2 Guest Users

Guest users can access the BBP system without registration. They are allowed to browse available bike paths between an origin and a destination and to view aggregated path information. Guest users cannot record bike trips or provide information about bike paths.

2.4 Assumptions, dependencies and constraints

2.4.1 Regulatory policies

The BBP system is assumed to comply with applicable regulations concerning the protection and processing of personal data. In particular, personal information associated with registered users and recorded bike trips must be managed in accordance with data protection laws in force.

The system does not introduce domain-specific regulatory constraints beyond those related to data privacy and lawful use of collected information. No financial transactions or safety-critical operations are performed by the system.

2.4.2 Domain Assumptions

D1: Users who record bike trips or provide bike path information are assumed to be actually biking while using the BBP system.

D2: Registered users are assumed to own or have access to a mobile device equipped with GPS and basic motion sensors.

D3: GPS data collected during bike trips are assumed to be sufficiently accurate to reconstruct routes and to associate path segments with spatial locations.

D4: External services used to retrieve meteorological information are assumed to be available and to provide correct data when queried.

D5: Automatically collected path condition information is assumed to be reviewed and confirmed by registered users before being marked as publishable.

D6: Registered users are assumed to provide path condition information in good faith and to reasonably verify the correctness of reports before marking them as publishable.

D7: Geographic and map data used to interpret GPS information and support path visualization are assumed to be sufficiently accurate and up to date.

3| Specific Requirements

3.1 External Interface Requirements

3.1.1 User Interfaces

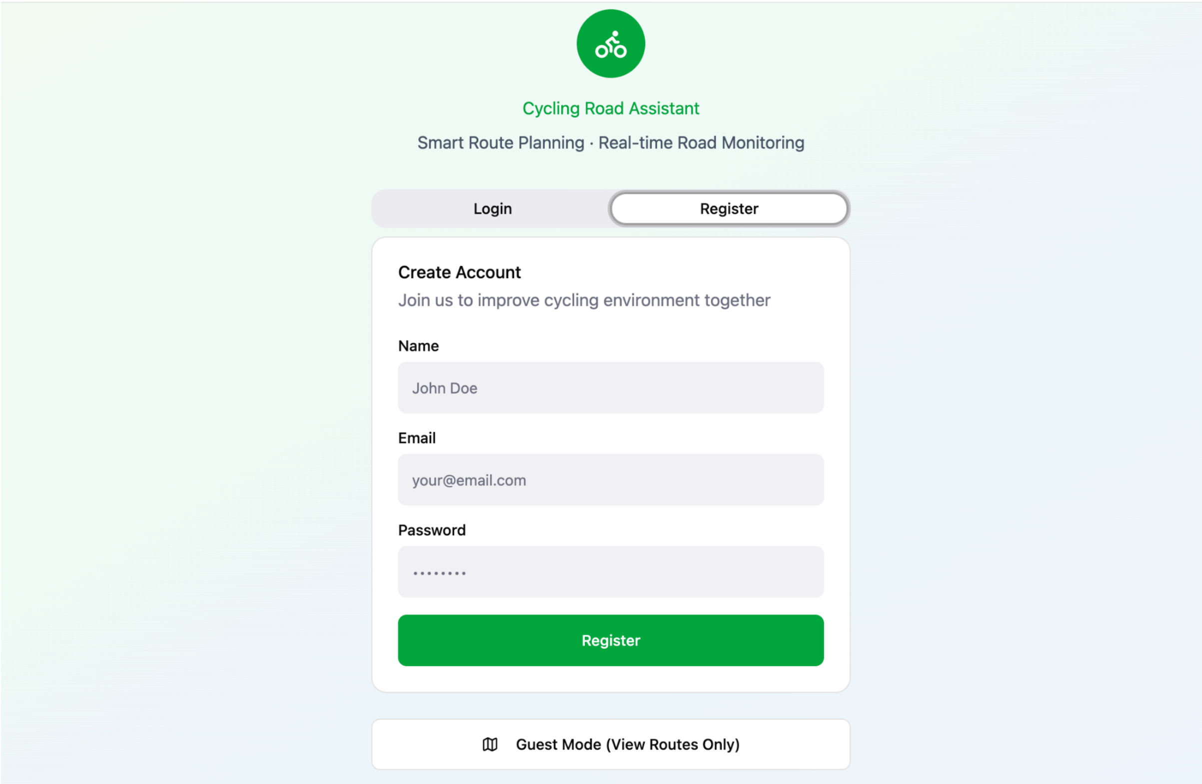
The system provides a web-based and mobile-accessible user interface designed for cyclists with varying levels of technical expertise. The interface shall be intuitive and easy to use, enabling users to record cycling trips, view personal statistics, browse available bike paths, and contribute bike path information with minimal effort.

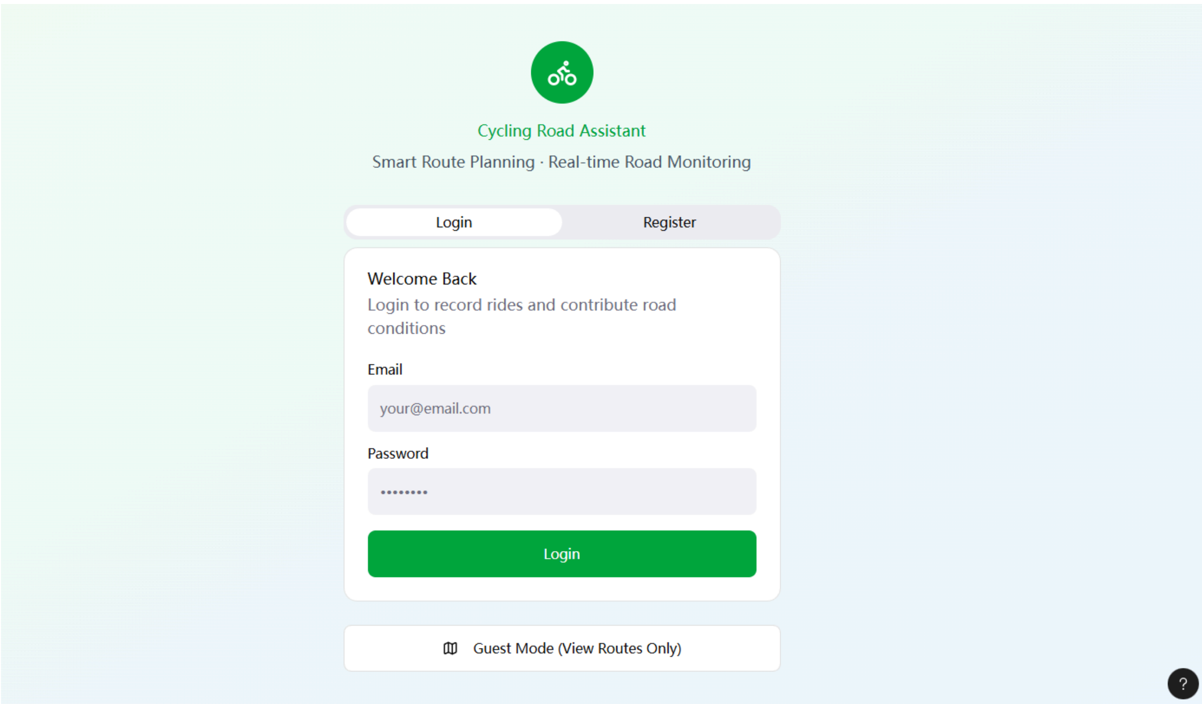
Registered users access the system through a common login and registration interface, after which they can manage their personal profiles, recorded trips, and bike path reports. Users who are not registered may access publicly available bike path information, such as published bike path conditions and route options, without authentication.

The user interface shall provide clear visual representations of routes, statistics, and bike path conditions, ensuring readability on both desktop and mobile devices.

Login/Register page

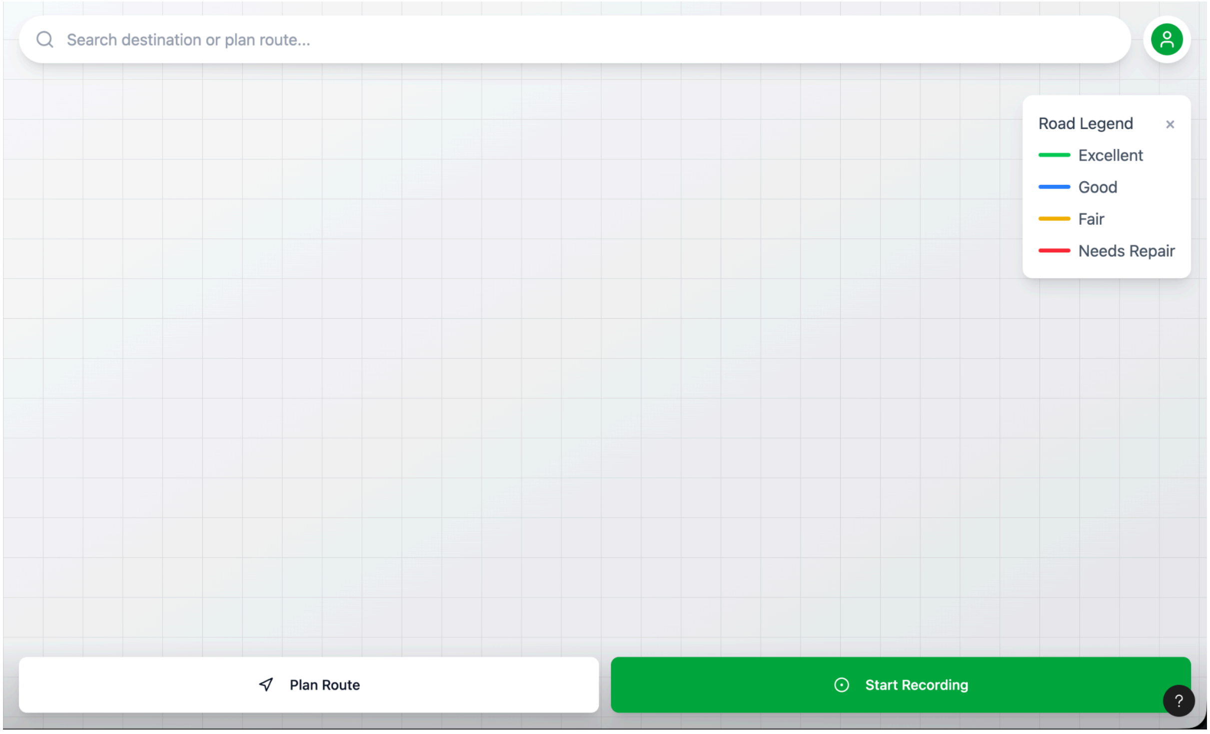
The login and registration page allows users to securely create an account or access the system in order to use personalized cycling and bike path features.

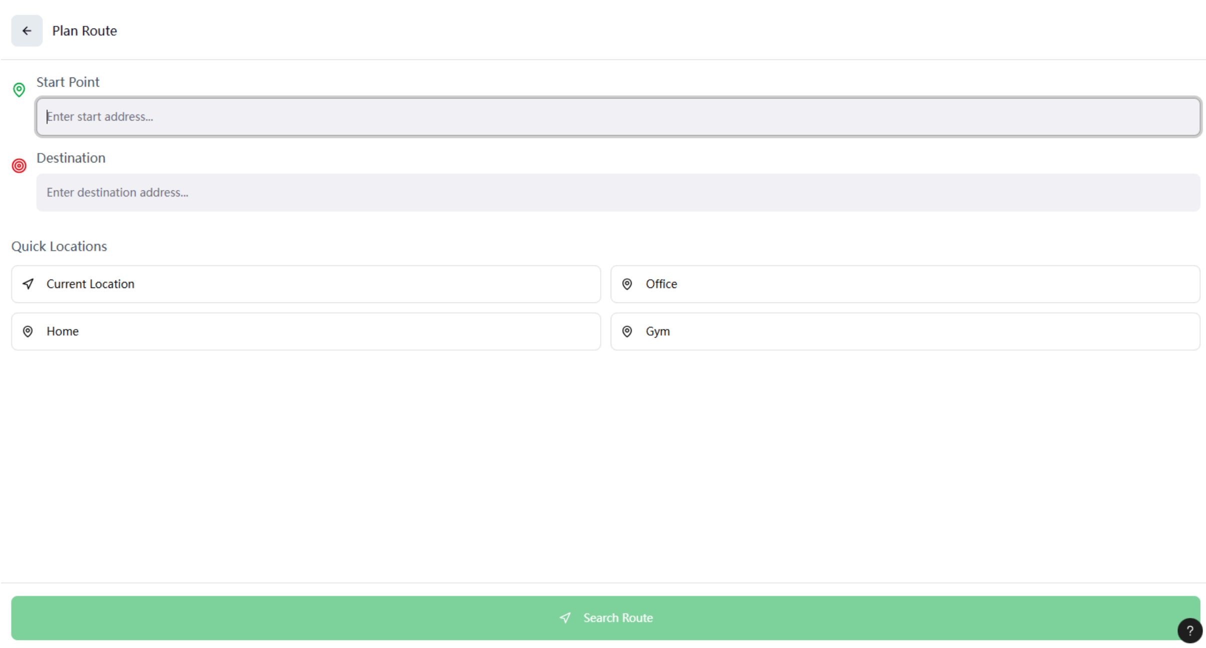




Path Search Page

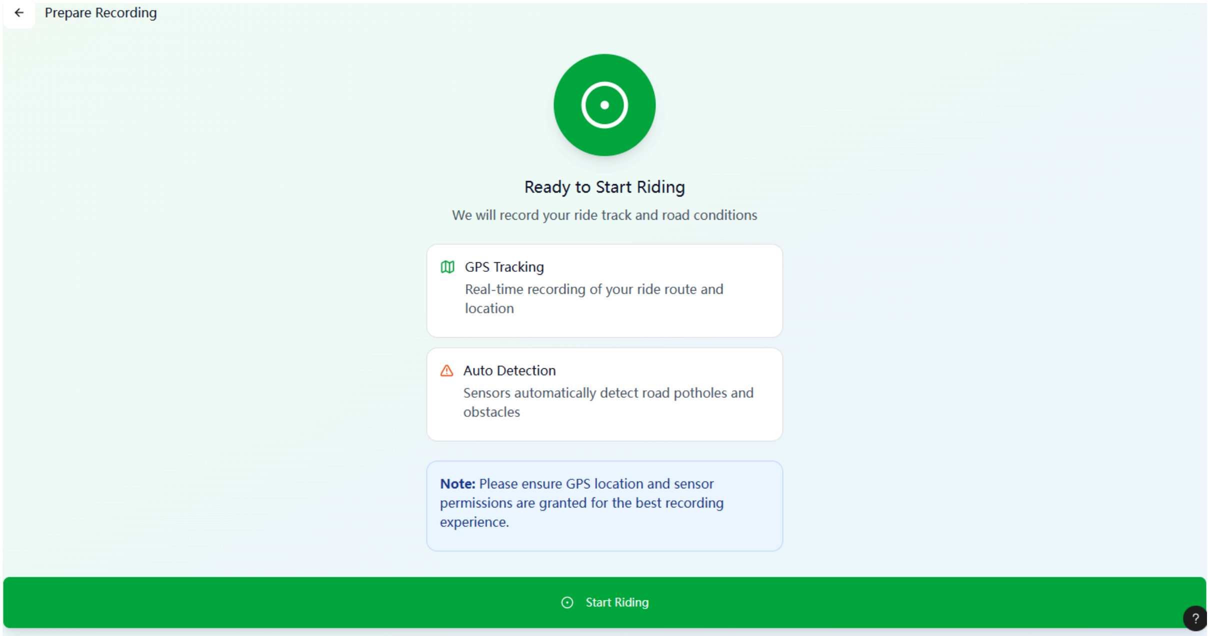
The path search page enables users to search for and compare bike paths between a specified origin and destination.

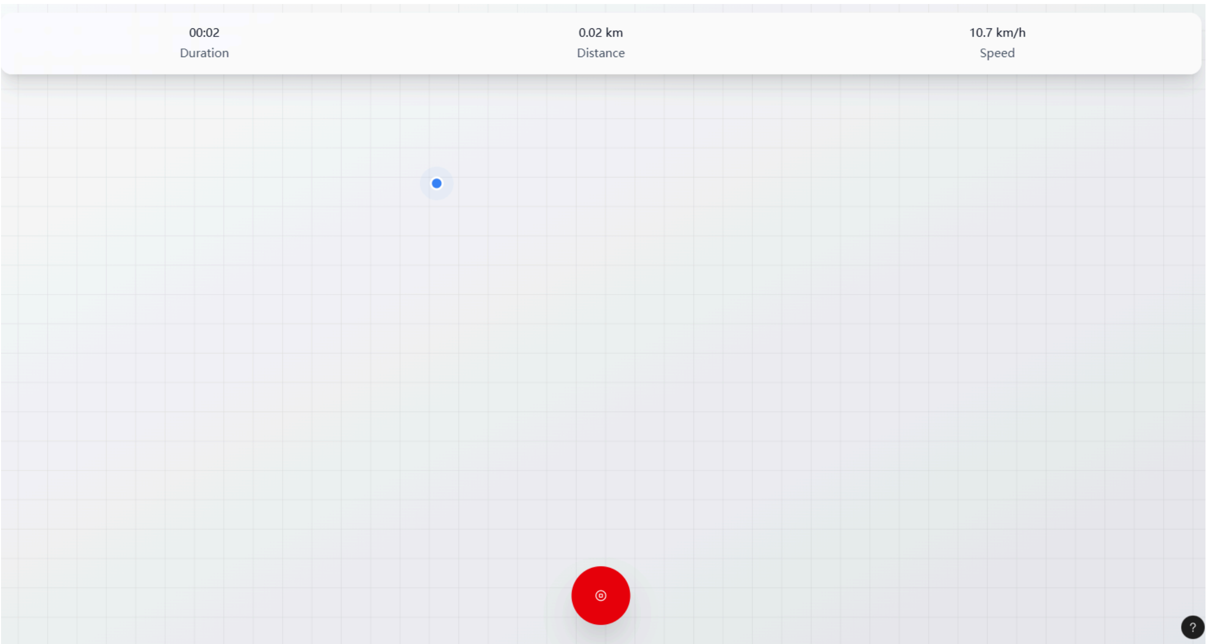




Riding Recording Page

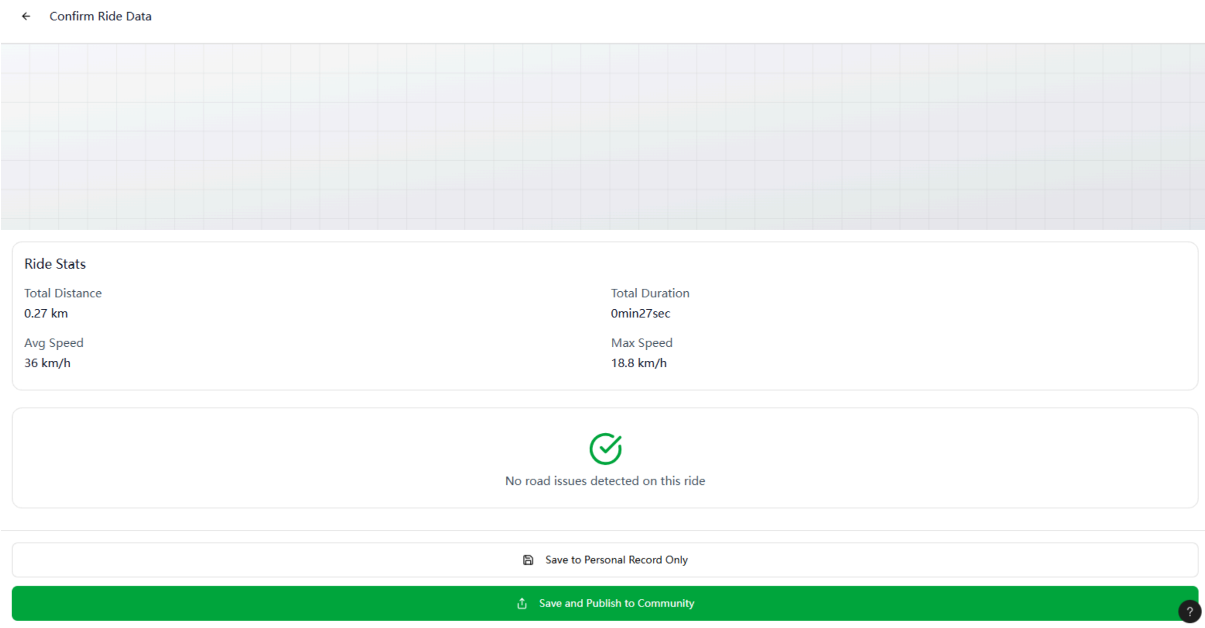
The **Riding Recording Page** allows a registered user to start, monitor, and stop the recording of a cycling trip. From this page, the user can initiate or terminate trip recording and optionally enable the automated mode for collecting bike path condition information during the ride.





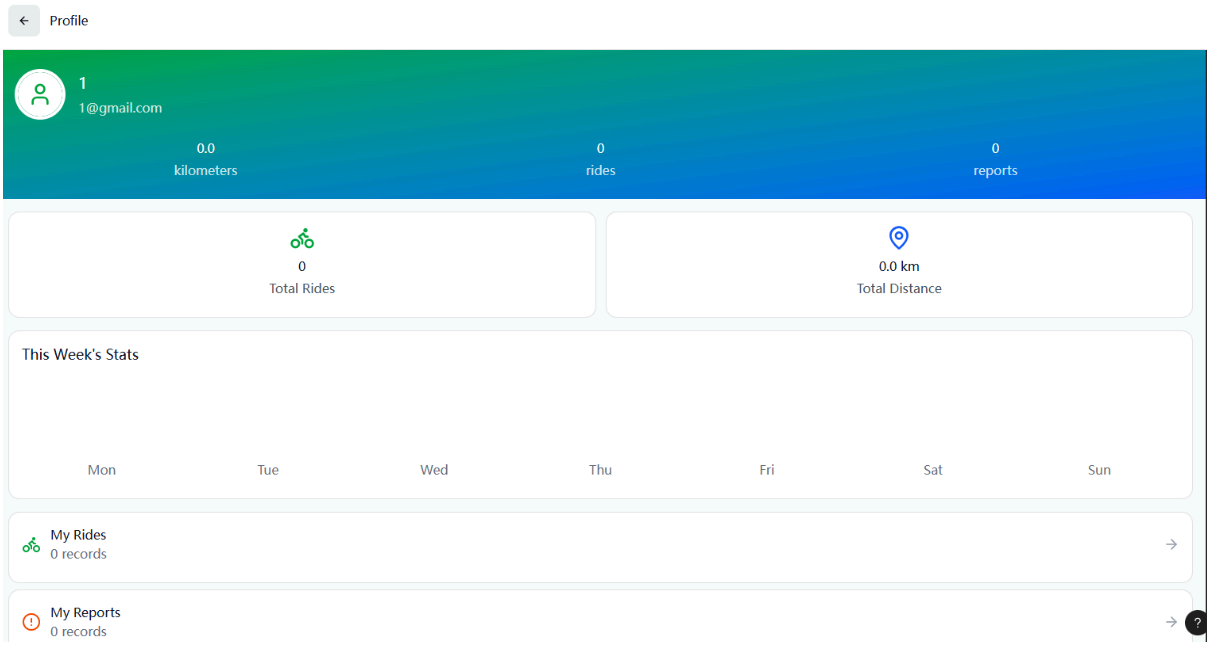
Confirm Page

The Confirm Page allows a registered user to review, validate, and finalize bike path information collected either automatically during a ride or manually inserted. Only after successful validation on this page can the reports be marked as publishable and made available for aggregation and route evaluation within the system.



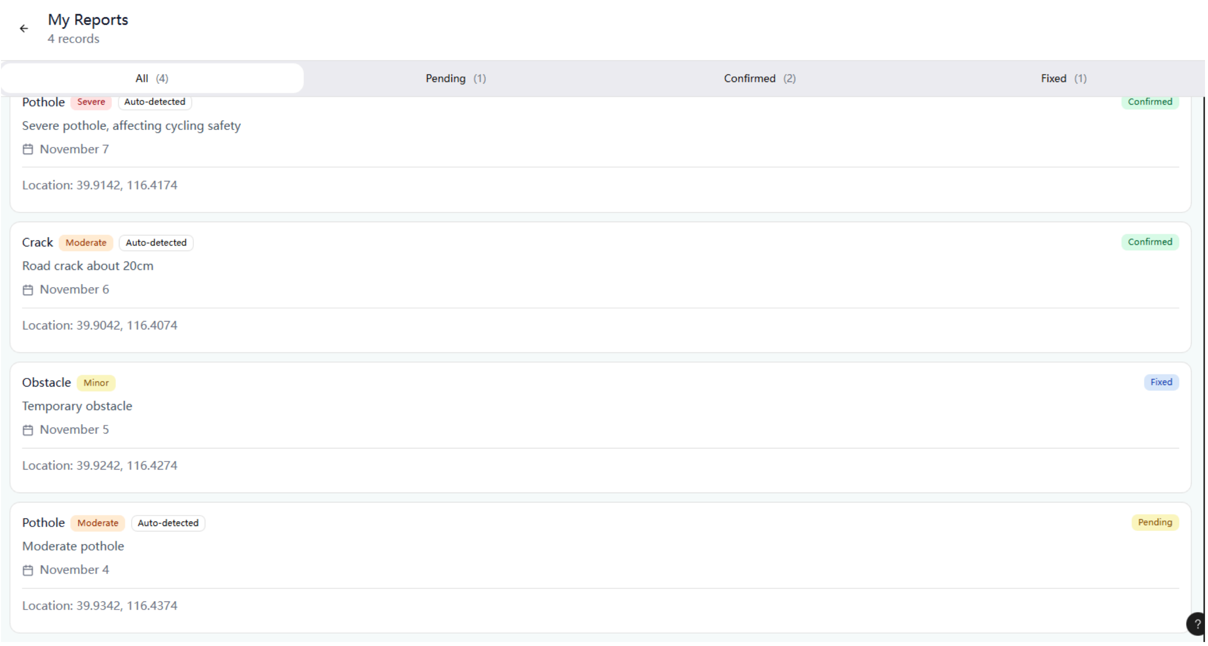
Profile Page

The profile page provides users with access to their personal information, trip history, and cycling statistics.



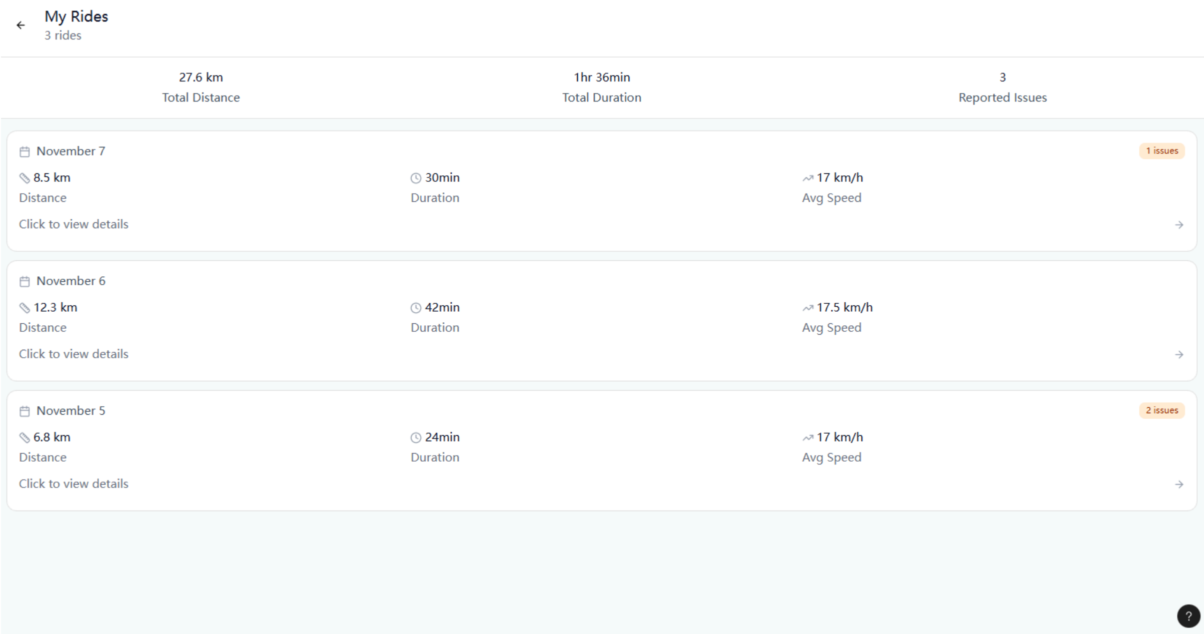
My Report page

The My Report page enables users to manage and review their submitted bike path reports and their publication status.



My Rides Page

The My Rides page provides users with access to their recorded cycling trips and related statistics.



3.1.2 Hardware Interfaces

The system does not require any specialized hardware interfaces. It operates on standard consumer devices, including smartphones, tablets, laptops, and desktop computers, provided that they are equipped with a compatible web browser or mobile operating system.

When accessed via mobile devices, the system interfaces with built-in hardware components such as GPS receivers and motion sensors to support trip recording and automated bike path data collection. No external or additional hardware devices are required.

3.1.3 Software Interfaces

The system interacts with external software services to support its core functionalities. In particular, it may interface with:

- Mapping and geolocation services to display routes, reconstruct traveled paths, and support origin–destination searches.

- Meteorological data services to retrieve weather information associated with recorded cycling trips.

- Database management systems to store user profiles, trip data, and bike path reports.

All software interfaces shall rely on well-defined APIs and follow standard data exchange formats to ensure interoperability and maintainability.

3.1.4 Communication Interfaces

Users access the system through an internet connection to utilize all available features, including trip recording, route exploration, bike path reporting, and data visualization.

All communication between client devices and backend services shall occur over secure communication channels. The system shall fully support HTTPS protocols to ensure data confidentiality, integrity, and secure transmission of sensitive information such as user credentials, location data, and cycling records.

3.2 Functional Requirements

This section describes the functional requirements of the Best Bike Paths (BBP) system. Functional requirements specify the services that the system must provide to support cyclists in recording trips, sharing bike path information, and discovering suitable routes.

Record a Bike Trip

[R1] The system allows registered users to start and stop the recording of a cycling trip.

[R2] During trip recording, the system collects GPS data to reconstruct the traveled route.

[R3] The system computes and stores statistics for each recorded trip, including total distance, duration, and average speed.

[R4] The system allows registered users to enable an automated mode that collects bike path information while cycling.

[R5] In automated mode, the system detects biking activity based on movement speed and collects sensor data from the user's mobile device.

Automatically Collect Bike Path Condition and Weather Information

[R6] The system acquires meteorological information related to a recorded trip when available.

[R7] The system associates meteorological data, such as weather conditions and temperature, with recorded trips.

View Personal Profile and Recorded Trips

[R8] The system allows registered users to view their personal trip history and detailed statistics for each trip.

Manually Insert Bike Path Information

[R9] The system allows registered users to manually insert information about bike paths by specifying path segments and their conditions.

Confirm and Publish Bike Path Reports

[R10] The system allows registered users to review, confirm, or correct automatically or manually generated bike path reports.

[R11] The system allows registered users to mark validated bike path reports as publishable.

[R12] Only publishable bike path reports are used by the system for aggregation and route evaluation.

Browse Bike Paths Between an Origin and a Destination

[R13] The system allows users to specify an origin and a destination to search for available bike paths.

[R14] The system displays one or more available bike paths between the selected origin and destination.

[R15] The system ranks available bike paths based on their overall condition and effectiveness in reaching the destination.

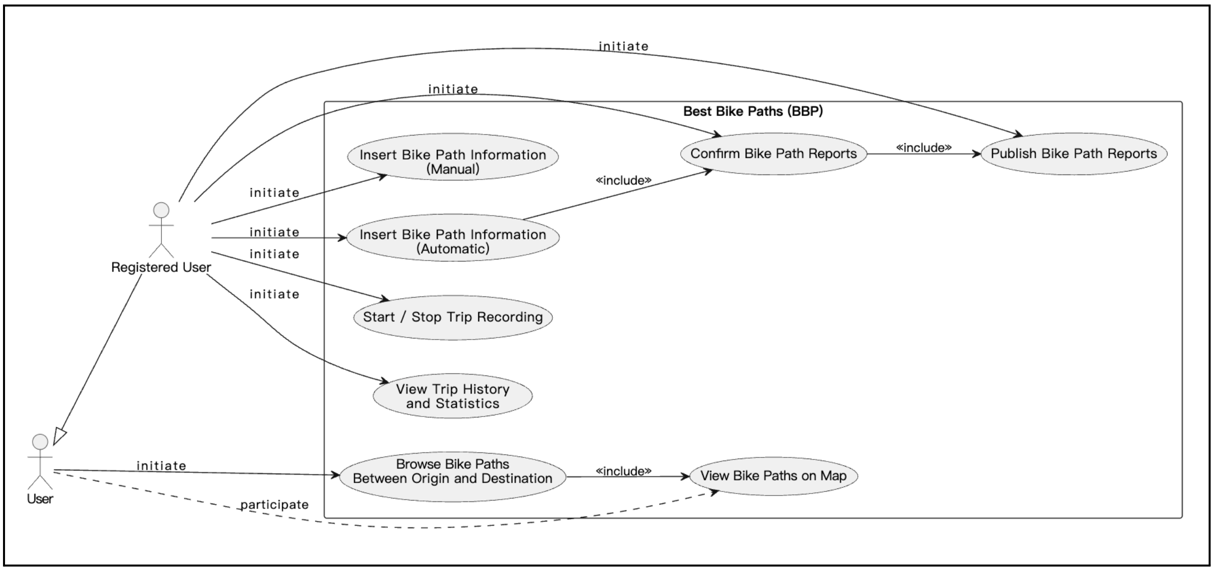
Merge Bike Path Information

[R16] The system merges publishable bike path reports provided by multiple registered users.

[R17] The merging process considers the freshness of reports and the level of agreement among users.

3.2.1 Use Case Diagram

The use case diagram illustrates the interactions between the BBP system and its actors, namely Registered Users and Guest Users. It provides a high-level overview of the main functionalities offered by the system, including trip recording, bike path contribution, and route discovery.



3.2.2 Use Cases

[UC1] Start Trip Recording

FIELD	DESCRIPTION
Name	Start Trip Recording
Actors	Registered User
Entry Condition	The user is logged in and has granted location permissions.
Event Flow	A. The user opens the trip recording module. B. The user clicks “Start Recording”. C. The system starts acquiring GPS points. D. The system initializes trip statistics (time, distance, speed).
Exit Condition	The trip is in “Recording” state.
Exception	Location permission denied / GPS not available.

[UC2] Stop and Store Trip

FIELD	DESCRIPTION
Name	Stop and Store Trip
Actors	Registered User
Entry Condition	A trip is currently being recorded.
Event Flow	A. The user clicks "Stop Recording". B. The system stops acquiring GPS points. C. The system finalizes trip statistics (distance, duration, average speed). D. The system stores the trip and adds it to the user's trip history.
Exit Condition	The trip is stored and available in history.
Exception	Storage error: the system displays an error and keeps the trip as "not stored" until retry.

[UC3] View Trip History and Trip Details

FIELD	DESCRIPTION
Name	View Trip History and Trip Details
Actors	Registered User
Entry Condition	The user is logged in.
Event Flow	A. The user navigates to the personal area. B. The system displays the list of stored trips. C. The user selects one trip. D. The system displays route visualization and statistics for the selected trip.
Exit Condition	The user views trip details.
Exception	No trips available: the system displays "No trips recorded yet".

[UC4] Enrich Trip with Weather Data

FIELD	DESCRIPTION
Name	Enrich Trip with Weather Data
Actors	Registered User, External Weather Service
Entry Condition	A trip is stored (or is being finalized) and external service is reachable.
Event Flow	A. The system prepares a weather query based on trip time and location. B. The system requests meteorological data from an external weather service. C. The system receives the weather data (conditions, temperature, wind, etc.). D. The system associates weather data with the trip and stores it.
Exit Condition	The trip is enriched with meteorological information.
Exception	Weather service unavailable: the system stores the trip without enrichment and may retry later.

[UC5] Manually Insert Bike Path Report

FIELD	DESCRIPTION
Name	Manually Insert Bike Path Report
Actors	Registered User
Entry Condition	The user is logged in
Event Flow	A. The user selects “Manual Mode” for bike path insertion. B. The system asks the user to define the path (street/segments). C. The user enters one or more path segments. D. The user assigns a condition (optimal/medium/maintenance needed) and optionally adds obstacles notes. E. The system stores the report in “Draft” state.
Exit Condition	A draft bike path report is created.
Exception	Missing segment data / invalid location: system prompts corrections.

[UC6] Enable Automated Collection Mode

FIELD	DESCRIPTION
Name	Enable Automated Collection Mode
Actors	Registered User
Entry Condition	The user is logged in and has granted sensor and location permissions.
Event Flow	A. The user enables "Automated Mode" before cycling. B. The system starts acquiring GPS and motion sensor data (accelerometer, gyroscope). C. The system monitors speed to detect biking activity.
Exit Condition	Automated mode is active.
Exception	Sensor permission denied / sensors not available.

[UC7] Detect Biking Activity Automatically

FIELD	DESCRIPTION
Name	Detect Biking Activity Automatically
Actors	Registered User
Entry Condition	Automated mode is active and sensor data is being collected.
Event Flow	A. The system continuously estimates user speed from location data. B. The system compares the speed with biking thresholds. C. If biking is detected, the system marks the session as "Cycling" and continues data acquisition.
Exit Condition	The system identifies that the user is cycling.
Exception	Ambiguous movement pattern: the system keeps monitoring without confirming cycling.

[UC8] Reconstruct Followed Path from GPS Data

FIELD	DESCRIPTION
Name	Reconstruct Followed Path from GPS Data
Actors	Registered User
Entry Condition	A GPS trace is available from a recorded cycling session.
Event Flow	A. The system processes collected GPS points. B. The system reconstructs the traveled path and identifies path segments. C. The system links detected segments to map data for visualization.
Exit Condition	A reconstructed path representation is created.
Exception	GPS too noisy: the system reconstructs a partial path and flags low confidence.

[UC9] Detect Obstacles from Sensor Data

FIELD	DESCRIPTION
Name	Detect Obstacles from Sensor Data
Actors	Registered User
Entry Condition	Automated mode is active and motion sensor data is available.
Event Flow	A. The system analyzes accelerometer and gyroscope signals. B. The system identifies anomalies that may indicate obstacles (e.g., potholes). C. The system associates each detected issue with a path segment and stores it in a draft report.
Exit Condition	Draft obstacle reports are created and linked to segments.
Exception	Insufficient sensor data: the system skips detection for the affected portion.

[UC10] Review and Confirm/Correct Path Reports

FIELD	DESCRIPTION
Name	Review and Confirm/Correct Path Reports
Actors	Registered User
Entry Condition	At least one draft path report exists (manual or automatic).
Event Flow	A. The system displays the list of draft reports to the user. B. The user opens a report and reviews condition/obstacles and segment location. C. The user confirms the report or edits incorrect information. D. The system stores the updated report in “Confirmed” state.
Exit Condition	The report becomes confirmed.
Exception	User cancels review: report remains in “Draft” state.

[UC11] Mark Path Report as Publishable

FIELD	DESCRIPTION
Name	Mark Path Report as Publishable
Actors	Registered User
Entry Condition	A path report is in “Confirmed” state.
Event Flow	A. The user selects a confirmed report. B. The user enables the “Publish” / “Make Publishable” option. C. The system changes the report state to “Publishable” and makes it available to community aggregation.
Exit Condition	The report is publishable.
Exception	Report not confirmed: the system prevents publishing and prompts confirmation.

[UC12] Search Bike Paths Between Origin and Destination

FIELD	DESCRIPTION
Name	Search Bike Paths Between Origin and Destination
Actors	User (Guest or Registered)
Entry Condition	The user opens the route search function.
Event Flow	A. The user inputs origin and destination. B. The system retrieves candidate bike paths connecting the two locations. C. The system computes aggregated information for each path (distance, estimated time, overall condition). D. The system presents alternative paths to the user.
Exit Condition	Candidate paths are displayed.
Exception	No route available: the system displays “No bike paths found”.

[UC13] Visualize Bike Paths on Map

FIELD	DESCRIPTION
Name	Visualize Bike Paths on Map
Actors	User (Guest or Registered)
Entry Condition	Search results exist or a specific path is selected.
Event Flow	A. The user selects one or more paths. B. The system renders the selected path(s) on the map. C. The system shows relevant information (segment conditions, obstacles, overall score).
Exit Condition	The map visualization is displayed.
Exception	Map service unavailable: the system displays an error message.

[UC14] Rank and Score Available Bike Paths

FIELD	DESCRIPTION
Name	Rank and Score Available Bike Paths
Actors	User (Guest or Registered)
Entry Condition	Candidate bike paths are retrieved for a query.
Event Flow	A. The system evaluates each path segment condition and reported issues. B. The system computes a score for each candidate path. C. The system sorts paths by score and presents ranked alternatives.
Exit Condition	Paths are ranked and displayed.
Exception	Insufficient publishable data: system ranks using partial information and flags low confidence.

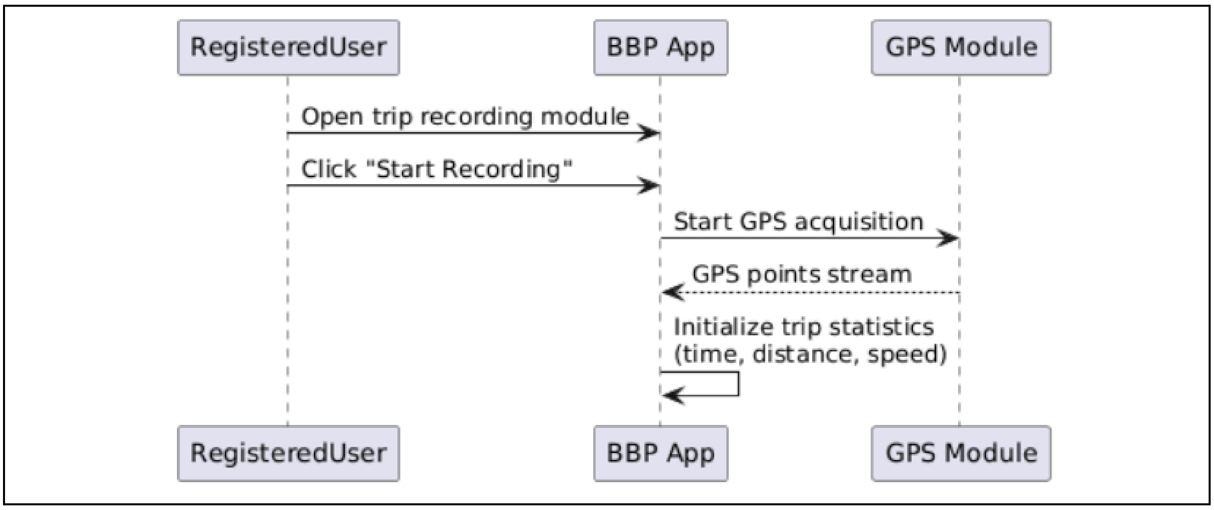
[UC15] Merge Publishable Reports from Multiple Users

FIELD	DESCRIPTION
Name	Merge Publishable Reports from Multiple Users
Actors	System
Entry Condition	Multiple publishable reports exist for the same path segment.
Event Flow	A. The system groups publishable reports by segment B. The system evaluates the freshness of each report. C. The system evaluates agreement level among users. D. The system produces a consolidated segment condition and obstacle list.
Exit Condition	A merged representation is stored and used for route evaluation.
Exception	Conflicting reports with similar freshness: system applies predefined tie-breaking rules.

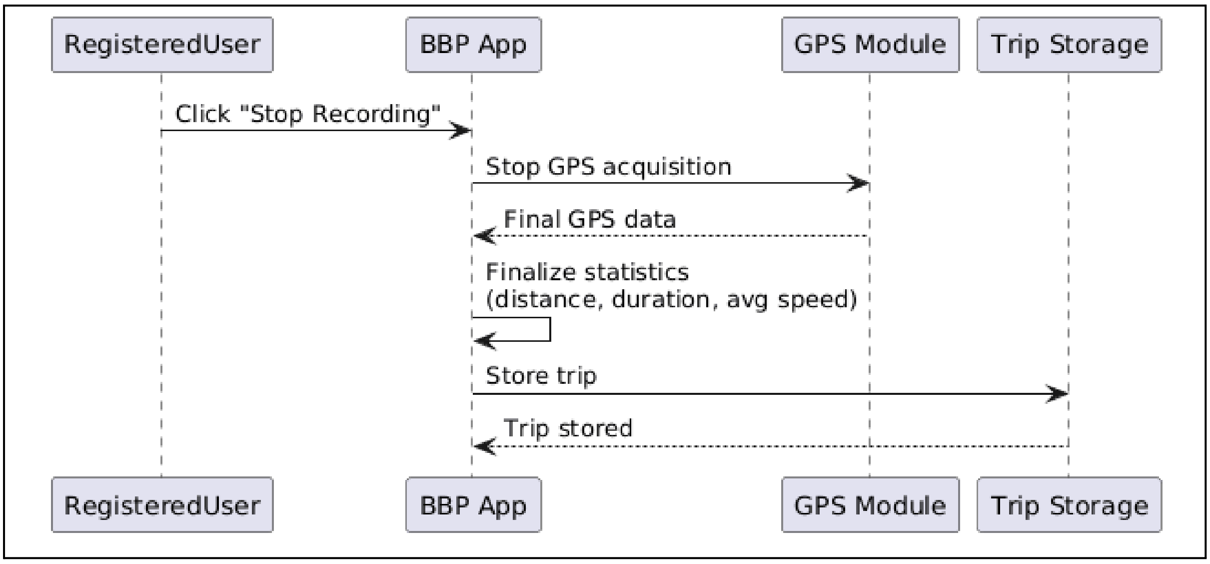
3.2.3 Sequence Diagram

This section presents sequence diagrams illustrating the interaction between users and the BBP system for key functionalities.

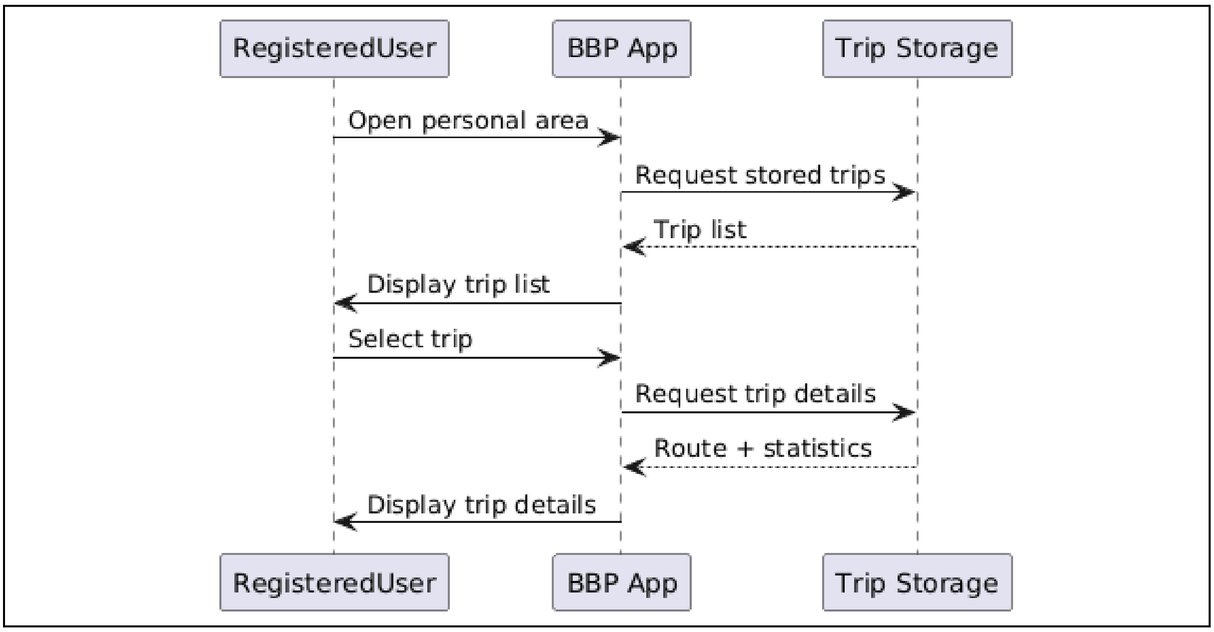
[UC1] Start Trip Recording



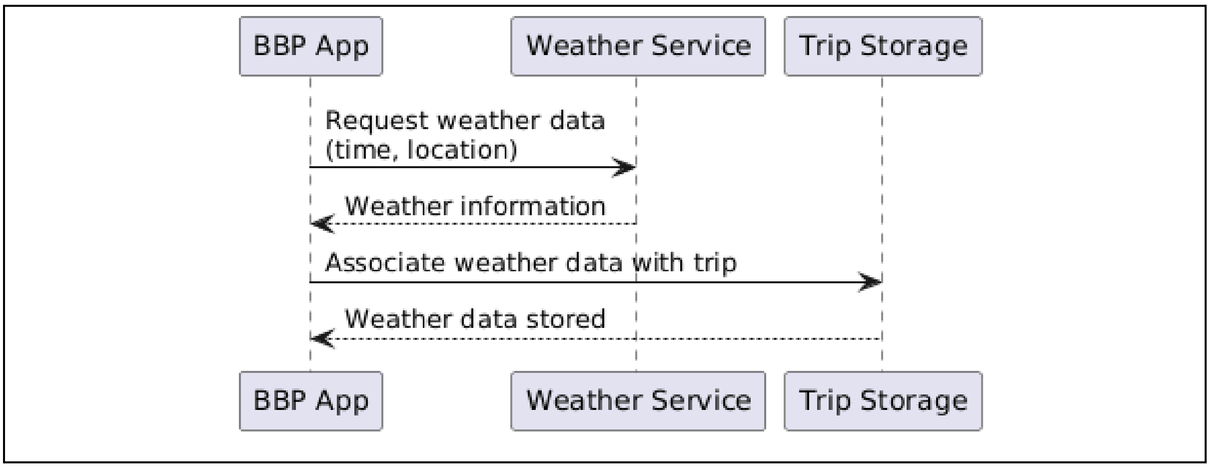
[UC2] Stop and Store Trip



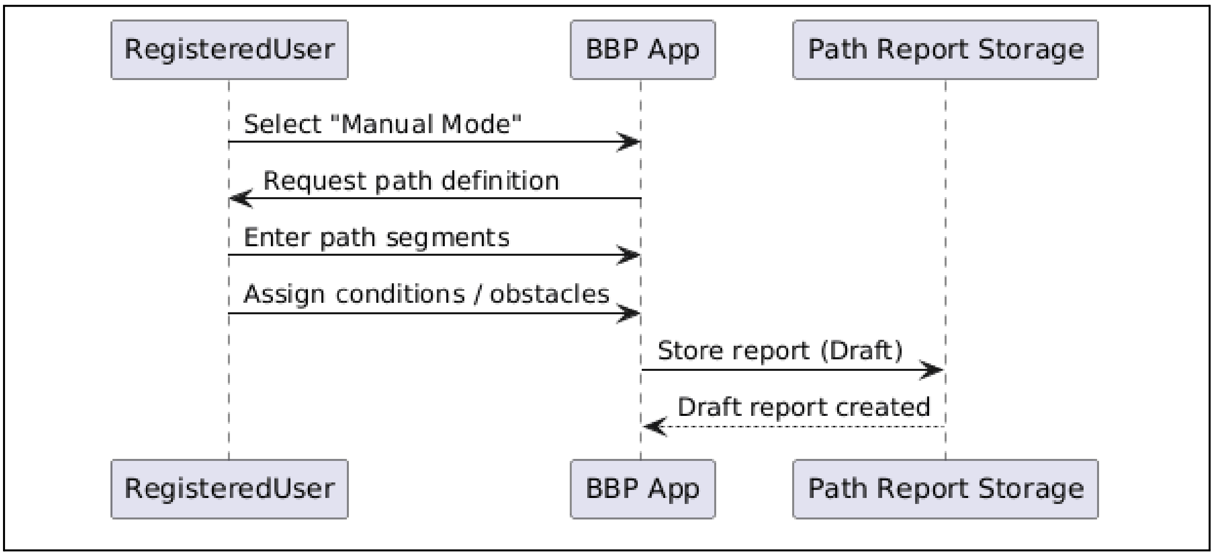
[UC3] View Trip History and Trip Details



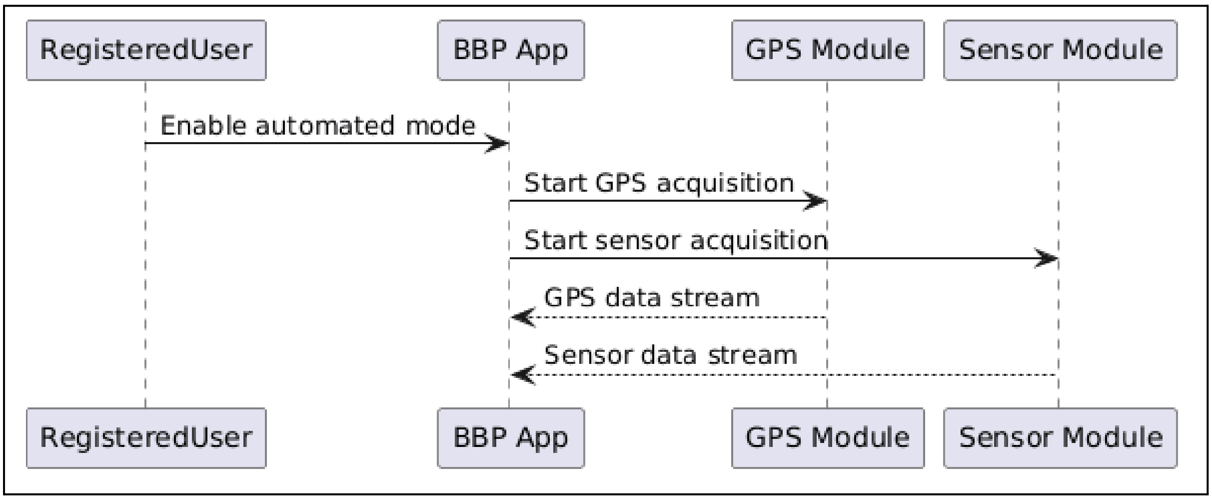
[UC4] Enrich Trip With Weather Data



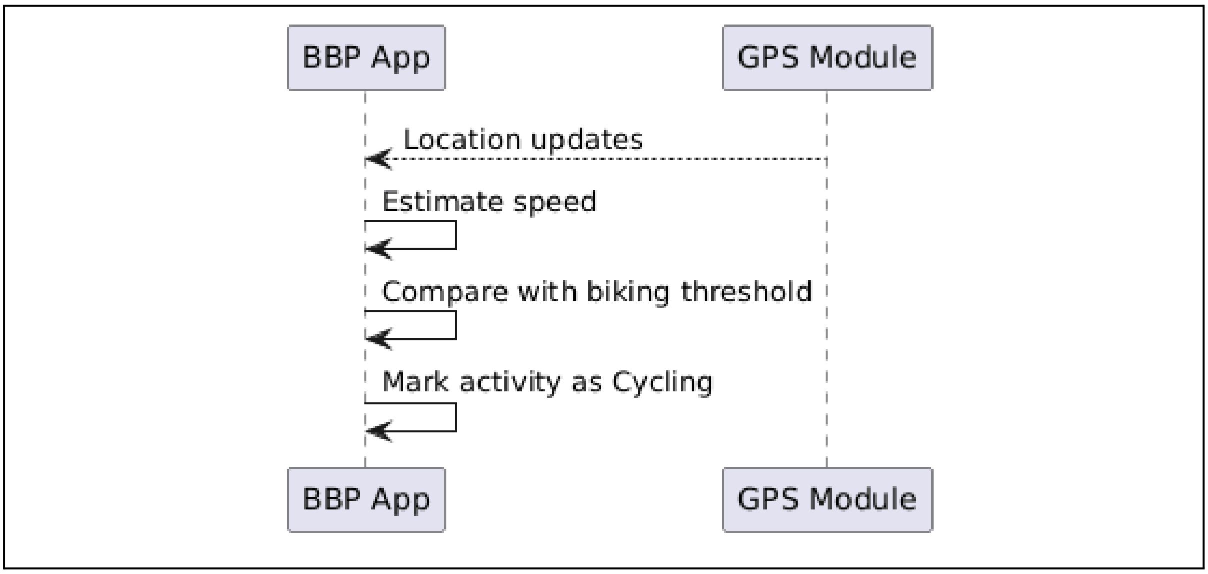
[UC5] Manually Insert Bike Path Report



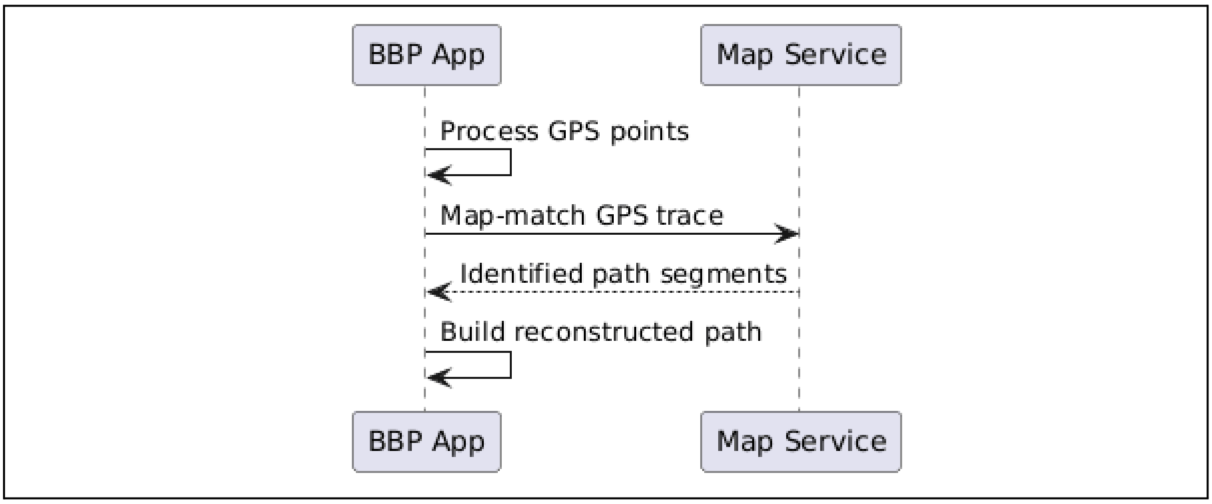
[UC6] Enable Automated Collection Mode



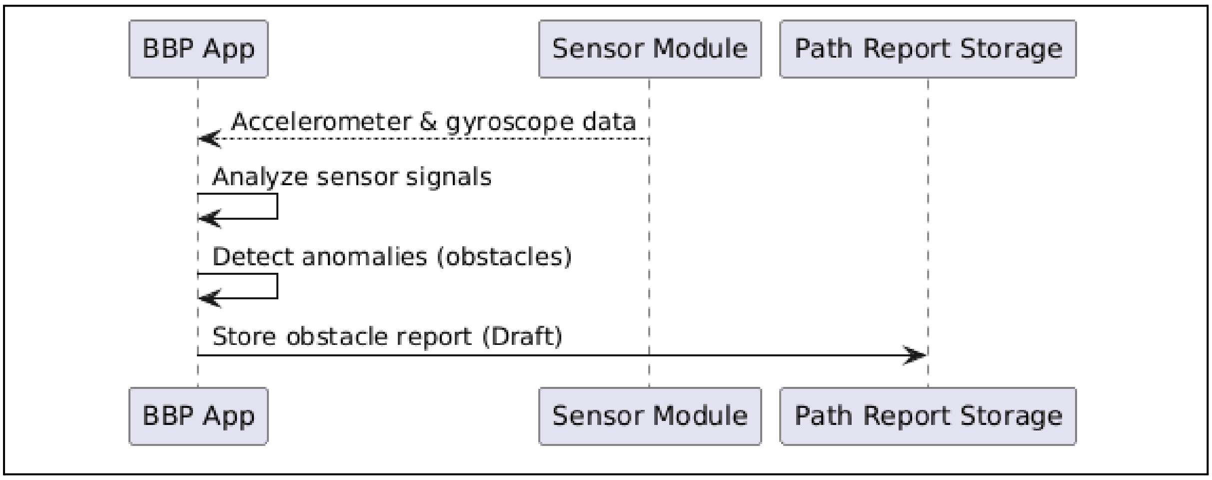
[UC7] Detect Biking Activity Automatically



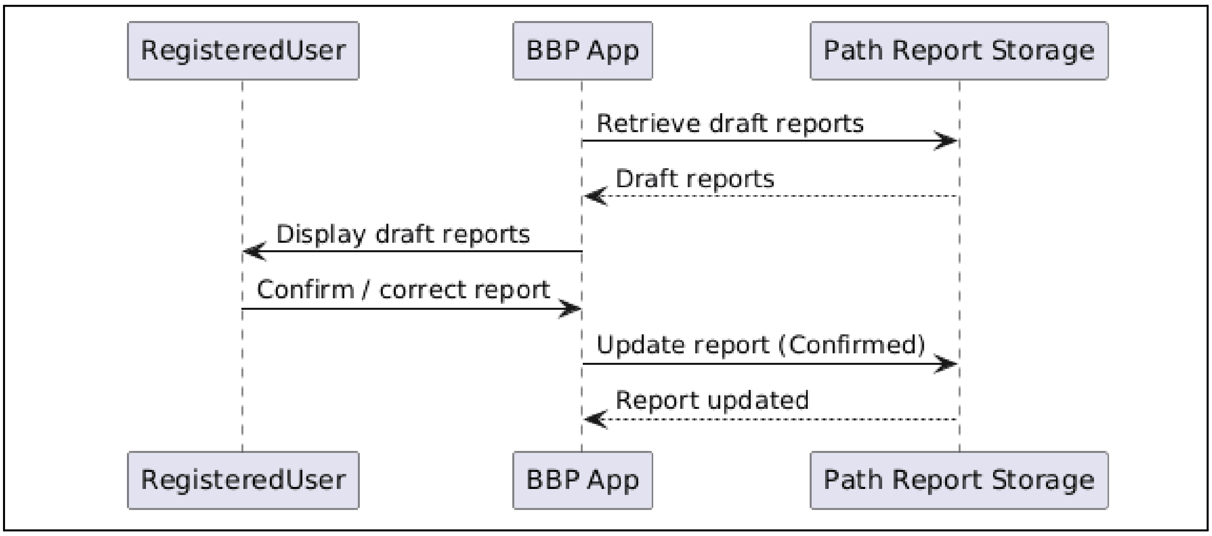
[UC8] Reconstruct Followed Path From GPS Data



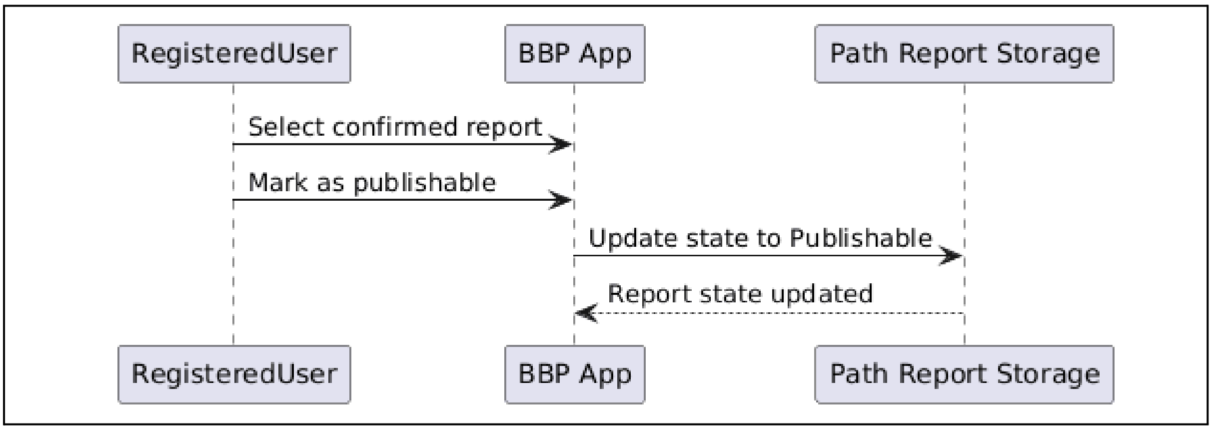
[UC9] Detect Obstacles From Sensor Data



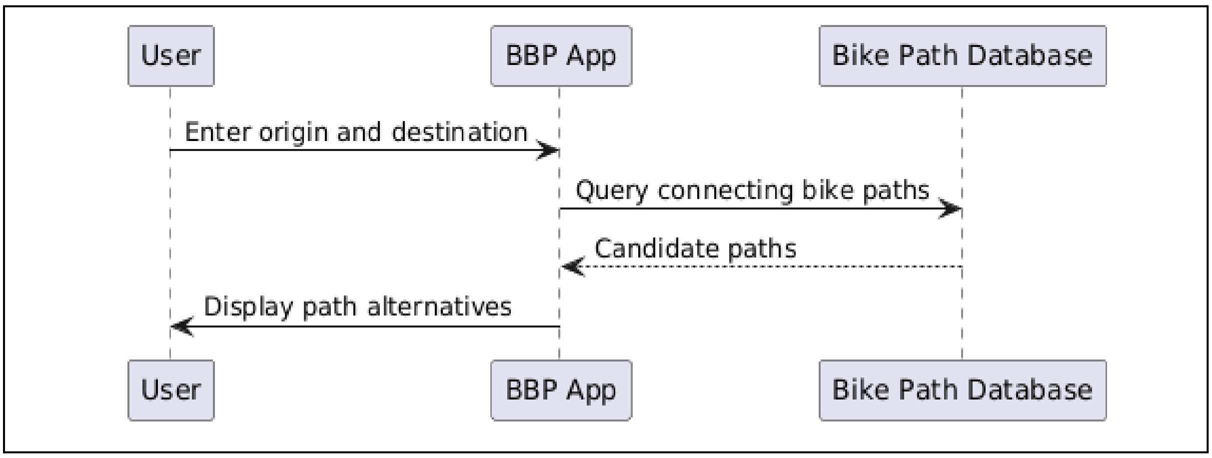
[UC10] Review And Confirm/Correct Path Reports



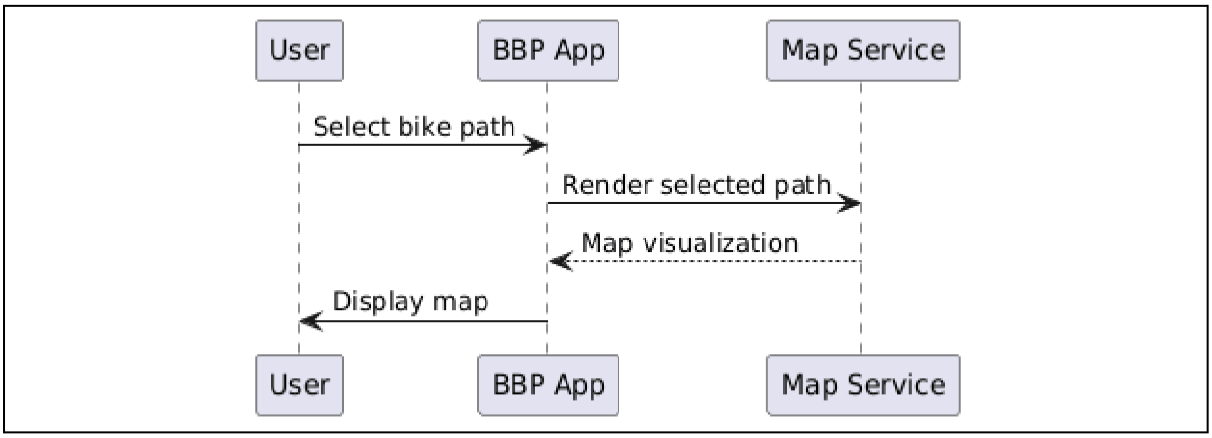
[UC11] Mark Path Report As Publishable



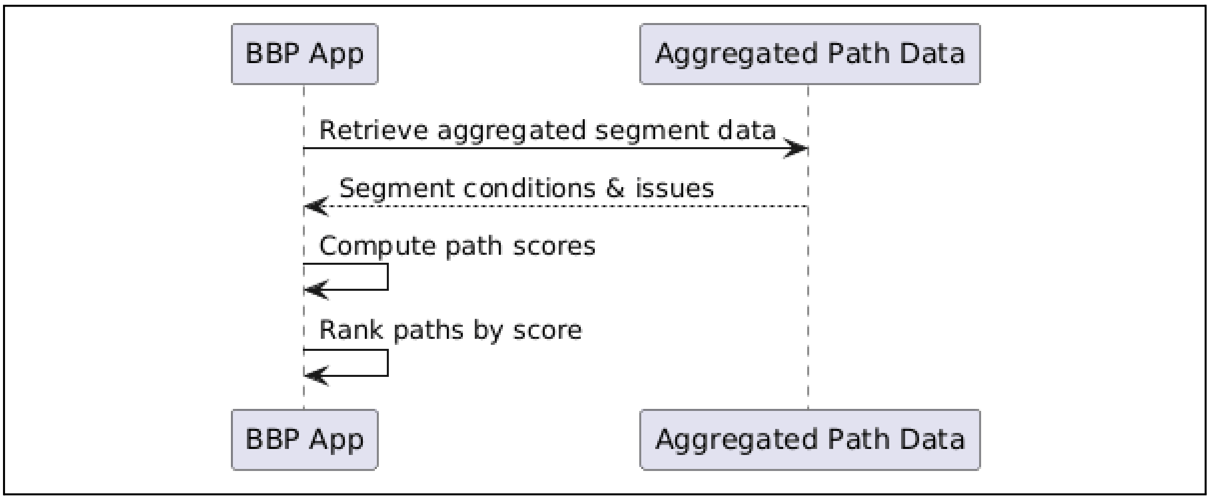
[UC12] Search Bike Paths Between Origin And Destination



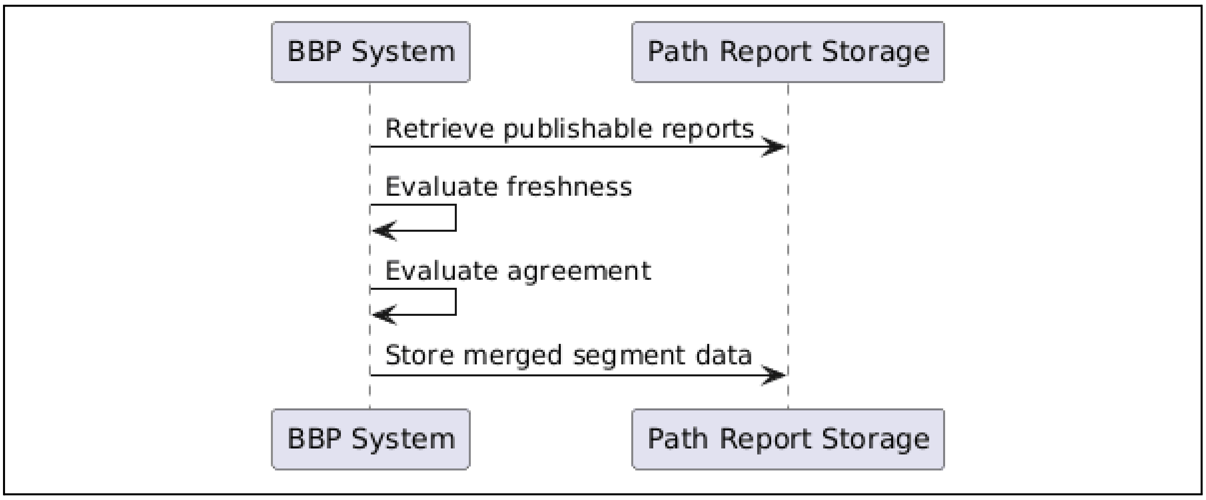
[UC13] Visualize Bike Paths On Map



[UC14] Rank And Score Available Bike Paths



[UC15] Merge Publishable Reports From Multiple Users



3.2.4 Mapping on Goals

The access requirements related to user registration and profile management form the foundation for most user-oriented goals of the system. In particular, requirements enabling registered users to record trips, manage their data, and access system functionalities (R1–R5, R8) are essential to ensure that users can effectively interact with the platform and contribute cycling and bike path information.

For **Goal 1 (G1)**, which focuses on enabling users to record and store their cycling trips, the system relies on requirements that allow users to start and stop trip recording (R1), collect GPS data (R2), and compute and store trip statistics (R3). The availability of automated data collection during cycling (R4, R5) further supports this goal by reducing manual user effort.

Goal 2 (G2) aims to provide users with statistics and performance metrics for each recorded trip. This goal is supported by the computation and storage of trip statistics (R3) and by the functionality that allows users to view their trip history and detailed statistics through their personal profile (R8).

For **Goal 3 (G3)**, which focuses on enriching trip data with meteorological information, the system requires the acquisition of weather-related data when available (R6) and its association with recorded trips (R7). The fulfillment of this goal depends on the availability of external meteorological data sources during or after the cycling activity.

Goal 4 (G4) addresses the users' need to manually provide information about bike paths. This goal is directly supported by the requirement that allows registered users to manually insert bike path information by specifying path segments and their conditions (R9).

Goal 5 (G5) focuses on enabling users to acquire bike path data. This is achieved through the use of publishable bike path reports for aggregation and route evaluation (R12), as well as through functionalities that allow users to search for bike paths between an origin and a destination and visualize available options (R13, R14).

For **Goal 6 (G6)**, which aims to allow users to review, confirm, or correct bike path issues, the system provides functionality for reviewing and validating both automatically generated and manually inserted bike path reports (R10). This goal assumes that users actively participate in validating detected information.

Goal 7 (G7) focuses on publishing bike path information for the community. This goal is supported by the ability for users to mark validated reports as publishable (R11) and by the system's use of only publishable reports for aggregation and dissemination (R12).

Goal 8 (G8) aims to enable users to explore and compare bike path options between a specified origin and destination. This goal relies on requirements that allow users to define origin and destination points (R13), display multiple bike path alternatives (R14), and rank them based on overall condition and effectiveness (R15).

The system-oriented **Goal 9 (G9)**, which focuses on merging bike path information provided by multiple users, is supported by requirements related to the merging of publishable reports (R16) and the consideration of report freshness and user agreement during the merging process (R17).

Goal 10 (G10) aims to keep bike path condition information consistent with the most recent user reports. This goal depends on the use of publishable reports only (R12) and on the merging mechanisms that prioritize recent and agreed-upon information (R16, R17).

Finally, **Goal 11 (G11)** focuses on allowing all users to access publishable bike path information. This is supported by requirements that ensure publishable data is used in route visualization and ranking (R12, R14, R15), making aggregated bike path information available to the entire user community.

Based on the analysis above, the relationships between goals and requirements are summarized in the following mapping.

Goal ID	**Goal Description**	**Supporting Requirements**	**Domains**
G1	**Users** would like to record their cycling trips and store them.	R1, R2, R3	D1, D2, D3
G2	**Users** would like to have statistics and performance metrics for each trip.	R3, R8	D1, D2, D3
G3	**Users** would like to enrich their trip data with meteorological information when available.	R6, R7	D4
G4	**Users** would like to manually provide information about bike paths.	R9	D6, D7
G5	**Users** would like to acquire bike path data.	R12, R13, R14	D1, D2, D3
G6	**Users** would like to review, confirm, or correct automatically detected bike path issues.	R10	D5, D6
G7	**Users** would like to publish bike path information for the community at the end of cycling.	R11, R12	D5, D6
G8	**Users** would like to explore and compare available bike path options between a specified origin and destination.	R13, R14, R15	D7

G9	**The system** shall merge publishable bike path information provided by multiple users.	R16, R17	D5, D6
G10	**The system** shall keep bike path condition information consistent with the most recent publishable user reports.	R12, R16, R17	D5, D6
G11	**The system** shall allow all users to access publishable bike path information.	R12, R14, R15	D5, D7

3.3 Performance Requirements

One of the main performance aspects of the BBP system is its ability to support a potentially large number of registered users who may simultaneously record cycling trips, provide bike path information, and access publishable data. As the system is community-oriented and relies on contributions from multiple users, scalability is a critical performance requirement. The system must be able to handle growth in the number of users, recorded trips, and stored bike path data while limiting performance degradation.

Responsiveness is another key performance concern. During normal operation, users expect timely feedback when recording trips, accessing statistics, searching for routes, or visualizing bike paths. In particular, operations related to trip recording and data acquisition during cycling activities should not introduce noticeable delays that could disrupt user interaction or reduce data reliability.

Availability is also essential, users should be able to retrieve publishable path data and explore available bike path options with minimal waiting time.

Finally, the system must be capable of processing, storing, and updating large volumes of trip and path condition data generated by users. This includes supporting frequent uploads of recorded trips and publishable path information, as well as merging and updating data from multiple users, without creating bottlenecks or compromising overall system performance.

3.4 Design Constraints

3.4.1 Standards Compliance

Conformity Standards

- GDPR: The BBP system manages personal data such as user profile, trip recordings, and location information. Therefore, it must comply with the GDPR in accordance with European data protection guidelines, ensuring lawful processing, data minimization, and appropriate user consent.

- ISO/IEC 27001: The system must adopt a structured and comprehensive information security management approach in order to protect sensitive user data, such as location and trip information, and to remain adaptable to emerging security risks.

Development Standards

- ISO/IEC 12207: The development of the BBP system shall comply with the ISO/IEC 12207 standard for software life cycle processes, applying recognized best practices in all the main processes that bring to its realization.

3.4.2 Hardware limitations

Users access the BBP system primarily through mobile devices during cycling activities, as well as through web-based interfaces for data visualization and route exploration. Hardware limitations are therefore not overly restrictive, but still impose constraints on system design:

- Users are assumed to own or have access to mobile devices equipped with GPS and basic motion sensors. These devices must be capable of collecting location and movement data with sufficient accuracy to support trip recording and bike path reconstruction.

- To correctly visualize maps, statistics, and bike path information, user devices must support standard graphical interfaces and display resolutions suitable for map-based applications.

- The interaction between the user and the system is also dependent on the availability and stability of the network connection. A reasonably stable internet connection is required to upload recorded trips, retrieve publishable bike path data, and access route search and visualization functionalities.

3.4.3 Any other constraint

The browser used should be up-to-date and compatible with the recent web application standards.

Furthermore, the system design must account for integration with external services, such as meteorological data providers and geographic map services, which are assumed to be available and reliable but are outside the direct control of the BBP system.

3.5 Software System Attributes

3.5.1 Reliability

The BBP system must reliably preserve a large volume of cycling trip data and bike path information contributed by users. The system shall implement robust backup and **recovery** procedures to safeguard against failures. Additionally, secure administrative access mechanisms should be in place to allow emergency maintenance, with all access activities logged and monitored for security purposes.

3.5.2 Availability

The system should provide high availability to support continuous access by cyclists recording trips, searching routes, and publishing bike path data. Core components need to incorporate **redundancy** and **failover** capabilities to ensure service continuity even in the face of hardware or network failures. Given the possibility of a rapid increase in users and data volume, the system design must address scalability challenges to maintain an availability level of at least **99.9%** uptime.

3.5.3 Security

Though the BBP system does not require user passwords, it handles sensitive personal data such as user profiles, GPS traces, and location information. All stored data must be encrypted at rest, and communications must use secure protocols to protect data in transit. The system should incorporate protections against common web threats including injection attacks and denial-of-service attacks, minimizing their potential impact on system integrity and availability.

3.5.4 Maintainability

The system should be designed with modularity and clear separation of concerns to facilitate ease of maintenance, testing, and future extensions. Components should be reusable and loosely coupled, allowing updates or improvements without affecting unrelated parts of the system. Comprehensive and up-to-date documentation is required, including detailed API specifications, architectural diagrams, and testing strategies to support maintainers and developers.

3.5.5 Portability

The BBP system must be accessible through a wide range of mobile devices equipped with GPS and basic motion sensors, as well as desktop web browsers. The user interface should be responsive and optimized for smartphones, tablets, and desktops, ensuring consistent functionality and usability across different screen sizes and operating systems. Compatibility with common web standards and modern browsers is required to provide a seamless user experience regardless of device.

4| Formal Analysis Using Alloy

In this Alloy analysis, we chose to focus on **bike path reports and their evolution over time**.
In particular, we aim to describe:

- the evolution of bike path condition reports over time,
- the validation and publication process of reports,
- and the consistency of aggregated bike path conditions under multiple user contributions.

To achieve this, we model **BikePathReport** as a mutable entity whose state evolves over time.
Reports may be created, validated, published, or terminated, and only publishable reports are considered by the system for aggregation.
We point out that the state *"no report"* is not explicitly represented in the model.
As in the reference system, this is a *symbolic state* indicating that no information has yet been provided for a given bike path segment.
Other aspects of the system, such as user interface interactions or numerical route ranking, are excluded from this analysis, as they represent extensions of the foundational logic and do not impact the core consistency of the system.

4.1 General Part

The model focuses on the core domain entities that are relevant for validating the correctness of bike path information management: **User**, **Trip**, **BikePathSegment**, and **BikePathReport**. In particular, the model emphasizes the lifecycle of bike path reports and the rules governing their validation and publication.
While users may record trips and generate reports on bike path segments, the Alloy model abstracts away low-level data acquisition aspects, such as raw GPS points, sensor measurements, and external services, as these do not affect the correctness of the report validation process.
Aggregation of bike path conditions is modeled at a high level by considering only publishable reports and prioritizing the most recent information, since these constraints are central to ensuring consistent and reliable path evaluation.

4.2 User and Trip Part

A **User** represents a registered cyclist in the system.
Each user may record multiple trips, and each trip belongs to exactly one user.
Trips are modeled abstractly, without representing raw GPS data. Instead, a trip is associated with one or more bike path segments.

```
sig User {
	var trips: set Trip
}

sig Trip {
	owner: one User,
	path: set BikePathSegment
} {
	this in owner.trips
}

sig BikePathSegment {}
```

4.3 Bike Path Reports

A **BikePathReport** represents user-provided information about the condition of a bike path segment.
Reports are mutable and evolve over time through a validation workflow.

Each report:

- refers to exactly one bike path segment,
- is authored by exactly one user,
- has a condition,
- has a timestamp used to model freshness,
- and has a current state representing its lifecycle.

```
open util/integer

abstract sig Condition {}

one sig Excellent, Good, Fair, Poor, Closed extends Condition

enum ReportState { Created, Validated, Published }

var sig BikePathReport {
	author: one User,
	segment: one BikePathSegment,
	condition: one Condition,
	time: one Int,
	var state: one ReportState
}
```

4.4 Temporal Constraints and Evolution

Report evolution

Reports may evolve over time by:

- staying in the same state,
- moving to the next state,
- or being removed from the system.

```
fun nextState[r: BikePathReport]: one ReportState {
        (r.state = Created) => Validated else
        (r.state = Validated) => Published else
        (r.state = Published) => Published else none
}

fact ReportStateProgression {
        always (
                all r: BikePathReport |
                r.state' = r.state or
                r.state' = nextState[r] or
                r not in BikePathReport'
        )
}
```

Publication rules

Only validated reports may be published.

```
fact PublicationConstraint {
        always (
                all r: BikePathReport |
                r.state = Published implies
                before r.state = Validated
 )
}
```

Freshness and consistency

At any moment, for a given bike path segment, the system considers only **published reports**, and among them, only the most recent ones.

```
fun publishedReports[s: BikePathSegment]: set BikePathReport {
        { r: BikePathReport | r.segment = s and r.state = Published }
}
```

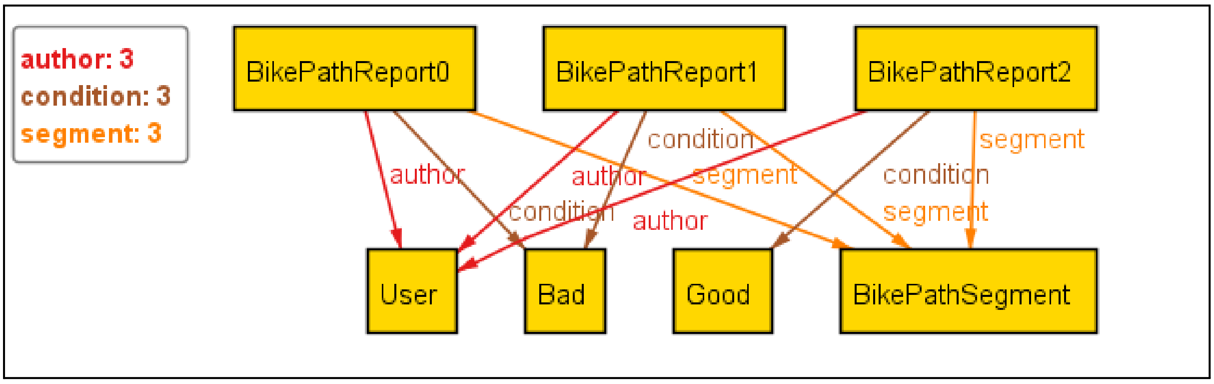
```
fun latestReports[s: BikePathSegment]: set BikePathReport {
        { r: publishedReports[s] |
                all r2: publishedReports[s] | r2.time <= r.time
        }
}
```

4.5 Examples

Example 1 – Typical evolution of reports

```
pred show[] {
        #BikePathReport = 0
        eventually (#BikePathReport = 2)
        eventually (some r: BikePathReport | r.state = Published)
}
run show for 3 but exactly 2 User
```

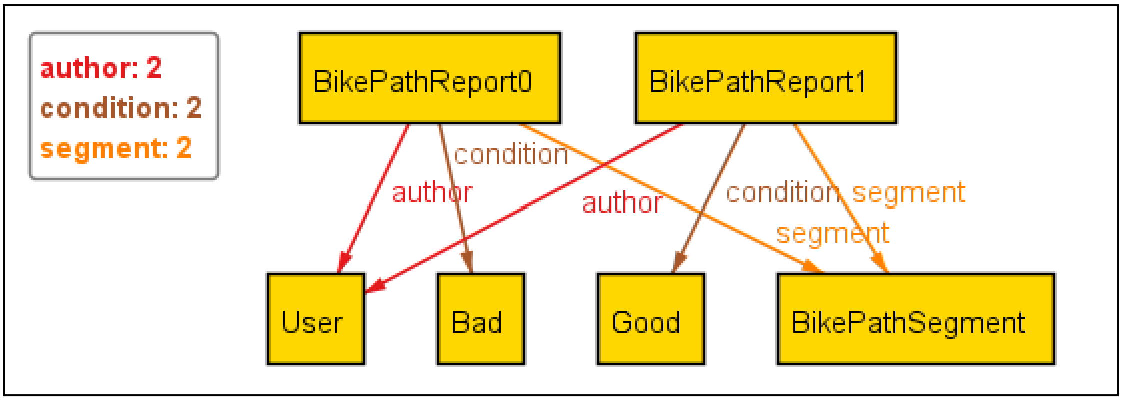
This example shows a typical scenario in which two reports are created.
One report eventually reaches the *Published* state, while the other stops earlier in the validation process.



Example 2 – Waiting in the same state

```
pred waiting[] {
        eventually (some r: BikePathReport | r.state' = r.state)
        eventually (some r: BikePathReport | r.state = Published)
}
run waiting for 3 but exactly 2 User
```

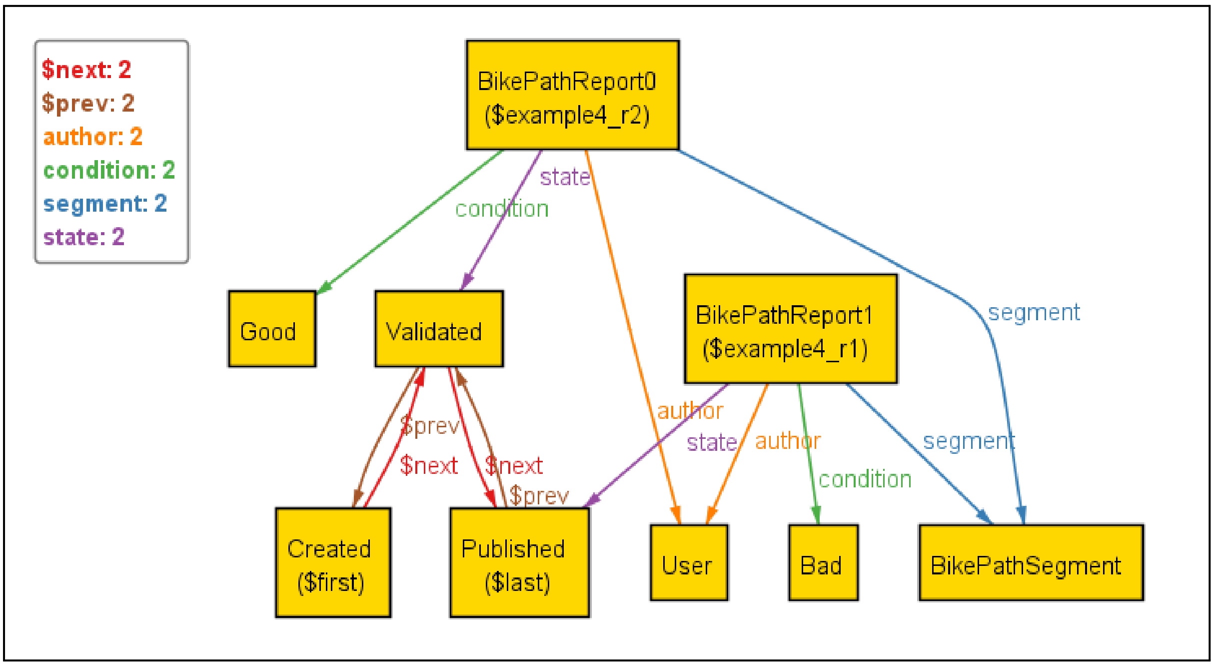
A report may remain in the same state for multiple instants, modeling delays in validation or confirmation.



Example 3 – Conflicting reports resolved by freshness

```
pred conflictingReports[] {
	some s: BikePathSegment |
	eventually (#publishedReports[s] > 1)
}
run conflictingReports for 4 but exactly 1 BikePathSegment
```

This example illustrates that multiple reports may exist for the same bike path segment, but aggregation relies on the most recent published ones.



4.6 Assertions

Finally, we verify that no report can skip mandatory states in the validation process.

```
assert NoMissingState {
        always not (
         some r: BikePathReport |
          r.state = Published and
          before historically not (r.state = Validated)
        )
}

check NoMissingState for 8
```

This assertion ensures that every report reaching the *Published* state has previously passed through the *Validated* state, preserving the correctness of the publication workflow.

5| Effort Spent

The following table summarizes the approximate number of hours each group member devoted to the different sections of the document. The reported distribution is indicative, as the preparation of each section required collaboration and joint discussion among all group members.

	Chapter 1	Chapter 2	Chapter 3	Chapter 4
Run Jie Simone Dai	2	11	18	4
Jiaxin Yang	1	18	11	5
Jiayi Zheng	9	8	12	3

6| References