TrackMe: RASD
Software Engineer 2 - 2018/2019

Riccardo Poiani, Mattia Tibaldi, Tang-Tang Zhou
Politecnico di Milano

Version 1.0

October 22, 2018

Contents

1 Introduction

1.1 Purpose

The Data4Help system is designed as a distributed software application which demands the usage of smartwatches, smartrings and smartphones that dispose of a NFC sensor and a GPS system inside for monitoring the position and the health of the owner. This application is thought for all people that want to keep under control their health during the day or who want to always know the position and the status of health status of a particular person in the world. Indeed, with this system a third party user can send a request to access data of some specific user, by means of his social security number: if the receiver agrees, it is possible to see in real time the last information registered about that person. The service supports the registration of individual who, by signing in, agrees that the company TrackMe acquires their data, which will be used anonymously by third parties for making statistics on groups of people.

Furthermore, in addition to the previous features, an AutomatedSOS service is available. It is thought for people that have serious health problems and, in case of illnesses (i.e. some parameters observed below the threshold), the system contacts, within 5 seconds, an ambulance. Secondly, the Track4Run service is also available. It is developed for organizers of sport events that want to monitor the runners in a race. The service allows organizers to define the path of a run, participants to enroll in the run, and spectators to see the exact position of all runners during the run on a map.

1.1.1 Goals

The goals can be distinguished into two families: the former regarding the users, and the latter regarding the third part customers.
The ones regarding the subscribed users, are the followings:

[G1] Once the health parameters of a subscribed user have been observed below the threshold, an ambulance is sent to the user location. (requires further specifications and assumptions: e.g. who owns the ambulances?)

[G2] The time experienced between the moment in which the health parameters of a subscribed user are observed below the threshold and the time in which the ambulance is sent to the user location is equal or less than 5 seconds.

[G3] Allow a subscribed user to enroll in a run, as athlete

[G4] Allow spectators too see on a map the positions of all athletes taking part in a run

[G5] Allow an organizer to set up a run, by defining its path

The goals of the project, regarding the third part customers, are the followings:

[G6] Allow a third party to access the data on a certain individual if only if he accepts. This is satisfied as soon as the request is approved

[G7] Allow a third party to access statistical and anonymized data if only on groups of individual greater than 1000. This is satisfied as soon as the request is approved

[G8] Allow a third party to subscribe to non-existing data. They will have access to them, as soon as the data is generated.

1.2 Scope

As already mentioned, the basic Data4Help service allows to monitor the position and the health status of individuals. When an user registers to the service he accepts the application's contract, that permits the acquirement of user's data from his device. The information, once received, is stored. Each ten seconds the user's device sends data to Data4Help servers that save them into the system; if a device goes offline, the latest data will be available on the server.
The people, who are probably most interested in this service, are whoever has a particular attention toward the health of himself, their family, or their close friends (e.g. parents). For instance, this application allows parents to monitor their children, when they are unable to stay with them. Moreover, Data4Help permits to the users to constantly see their health status in order to be conscious of their condition. Indeed, this will keep patients regularly updated on their progress and will provide proactive measures for a better health control.
In order to allow a third party customer to see the status of an appointed individual, he needs to send him a request of sharing data by means of the form provided by the system. Here, he must specify the social security number of the individual and a brief description which motivates the request. The receiver, obviously, can accept or reject the request according to the sender and the attached reason. If the receiver accepts the demand, the requesting customer can see his data, which is related to the date of its generation into the system.
In addition, the AutomatedSOS service results to be particularly helpful for old people or patients, that, as a matter of fact, are more subjective to health problems: thanks to this instrument they can be assisted in every moment of the day. When their health parameters go below the standard, the system, within 5 seconds, calls the 118 number autonomously, in order to send an ambulance to the user location. The ambulance is managed by the owner of the vehicle (hospitals, non-profit and privates), and it intervenes within the timing defined by the State. TrackMe, with this feature, hopes to help hospitals and private specialists to save lives. Data4Help provides different types of diagnostic procedures: blood pressure monitoring, heartbeat, and blood oxygen saturation levels.
The GPS system is also exploited by Track4Run feature, which allows third party organizers to define a certain path for a run, and to manage both participants and spectators during the race. For using this service, the organizers need to post a race event on the application, that contains a description and a timetable. Then, all the interested people (i.e. both runner and spectators) must sign up to the race in their specific section. Notes that while registering, a runner accepts to share his data during the competition. During the event, the application will automatically monitor the runners, and spectators will be able to follow the race on their smartphones. The organizers, in addition to the runner position, can also access to the health status of athletes, in order

to intervene in case of illness. Notes that the possibility of downloading data from the Track4Run service is allowed only when the competition is taking place.

The TrackMe company business concerns the sale of anonymous statistic data to companies, which can request both the health statuses and the positions of specific groups of people (e.g. people over 40). The policy implemented by TrackMe, prevents third parties from finding real owners of data. Indeed, a request from a company can be accepted only if the group of people involved is greater than 1000 individuals.

1.3 Definitions, Acronyms, Abbreviations

1.3.1 Definitions

- user: a person who has registered on the system (it is equivalent to subscribed user).
- athlete: a user who has subscribed to a race and intends to participate as a runner.
- individual requests: requests that third party customers can send that allow, if permissions are granted, to access the data of a specific user
- aggregated requests: requests that third party customers can send that allow, if permissions are granted, to access aggregated and statistical data on a certain group of user

1.3.2 Acronyms

- RASD - Requirement Analysis and Specification Document
- NFC - Near Field Communication
- GPS - Global Positioning System
- API - Application Program Interface
- JDBC - Java DataBase Connectivity
- DSS - Data Storage System
- SSL - Secure Sockets Layer
- TLS - Transport Layer Security

1.3.3 Abbreviations

1.4 Revision history

1.5 Reference documents

1.6 Document structure

2 Overall Description

2.1 Product perspective

TrackMe is a system which has to be designed as a completely new platform. It can be divided into two parts: a software application designed for the stakeholders (e.g. users, third parties, ...) and a core system interacting with the application via Internet.

The former one is intended to be a mobile application which requires, necessarily, other devices to work as expected by the functionality defined in the Product functions section. For instance, a possible gear to interact with the mobile application is a smartwatch, which helps, mainly, the application to gather information about the user's health data. Another essential requirement for the application to work is to have a stable connection to the Internet; without this obligation, the core system cannot collect information about the user. All these requirements are not essentials for third party users.

The latter system has to provide a central connection for every user. The most important object, that has to be regarded as a core, is the data. Overall, the TrackMe system is designed to share data and information about users. Therefore, a Data Storage System (DSS) is necessary and enables the core application to be able to save data and share it when asked. For instance, the DSS can be a database that can be accessed through standard interfaces, such as JDBC. Another essential requirement for the system is to safeguard the data collected; during the connection between the mobile application and the core system, TrackMe has to guarantee that nobody is tracing their data. Therefore, it is necessary to use some sort of strong network security, such as SSL/TLS protocols. Further functionality of AutomatedSOS and Track4Run are satisfied by using APIs of other companies (e.g. Google API for maps and voice recognition).

Regarding the environment of the TrackMe system, the following diagram (Figure: 1) is provided to describe better the domain model adopted:

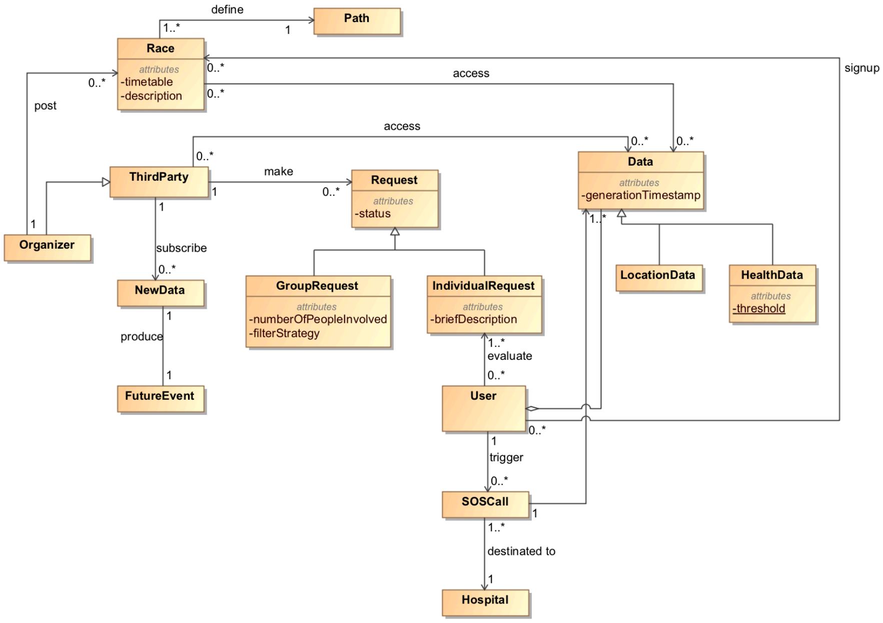

Figure 1: Class diagram of the environment

This diagram specifies the interaction with the actors and the objects of the world. The core point of the environment is the data, but what should be analyzed are its entry point and exit point (i.e. usage):

1. Request: an entry point essential to share the data;
2. SOSCall: an very important usage for unhealthy people;
3. Race: a feature necessary for runners.

2.1.1 Request perspective

Since people's data are very confidential information, a request has to be asked if someone desires it. Therefore, the design of how requests should work is essential. To give a better understanding of this, the following state diagram (Figure: 2) describes the possible states of a request:

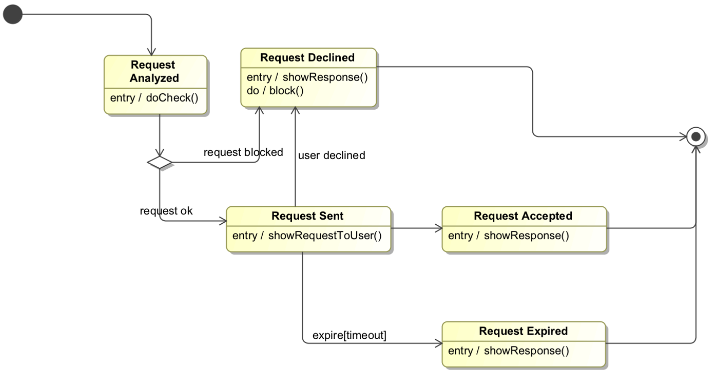

Figure 2: State diagram of a request

2.1.2 SOSCall perspective

For unhealthy people, a latency in a help call is a problem of life and death. Therefore, a better description of these calls is crucial. The following state diagram (Figure: 3) describes the possible states of a SOSCall:

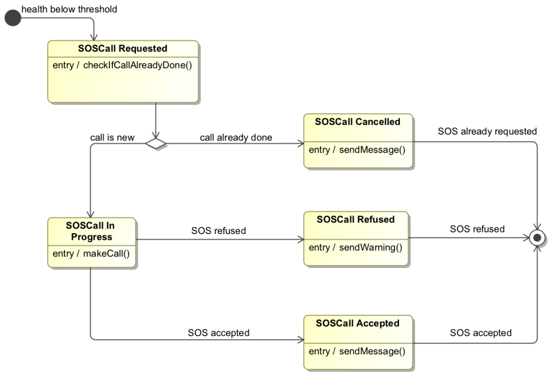

Figure 3: State diagram of a SOSCall

2.1.3 Race perspective

For someone, running is something that they cannot live without; since spectators can watch their position every time, it is important to describe better how a race works for better privatization of data. Thus, the following state diagram (Figure: 4) is shown:

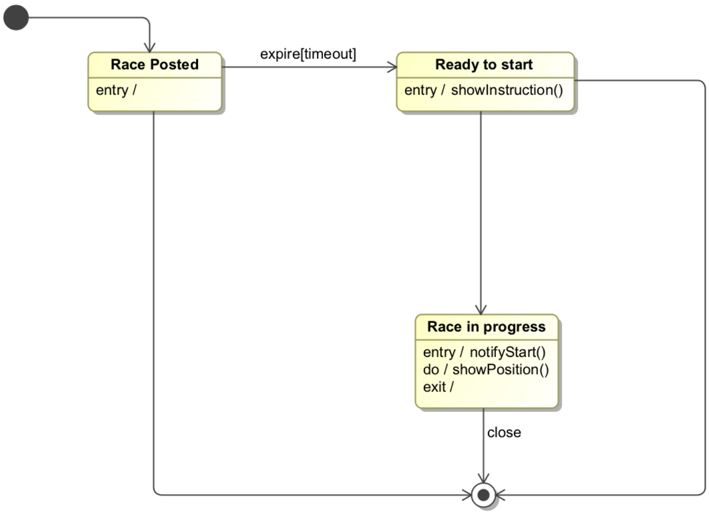

Figure 4: State diagram of a race

2.2 Product functions

The major functions of the projects can be divided and explained into four more specific aspects that are listed below:

2.2.1 Monitoring user's location and health status

Users subscribed to the application have agreed to being constantly monitored: in particular their locations and health statuses are kept under control. The information collection process continuously receives updated data from the users: these updates are sent every 10 seconds.

2.2.2 Data requests from third party customers

Third party customers can send two types of requests: individual requests and aggregated requests. In order to perform the former, the petitioner must provide the social security number of the individual and a brief motivation: as soon as he accepts (if he does), the access will be granted to the customer. Individual requests regard any subset of the stored information of the specified user; furthermore, it is possible to demand for new data that will be generated during a well-defined and limited period of time in the future. More specifically, this last point means that third parties can ask, also, for information that will be generated, for instance, during the next month.
Note that in the case in which a request will be pending for a month, it will expire and the user will no longer be able to accept it.
Furthermore, it is also possible for an user to block, and thus prevent, requests that he receives from a certain third party customer: in this case the system will abort the demanding process at the beginning, during a brief analysis.
Aggregated requests involves, instead, anonymized set of people registered in

the application. This access will be granted automatically by the system in the case in which the dimension of the group is greater than 1000.

2.2.3 Subscriptions to new data

Third party customers are allowed to subscribe to aggregated data that still does not exists: the access will be granted as soon as the data is generated.
For instance, a petitioner could ask for the health statuses of the next month that belongs to old people (e.g. age is greater then 68) that lives in Milan.
The same constraints on anonymisation (i.e. dimension of the group is greater then 1000) is applied here as well.

2.2.4 Automated calls of SOS help

When the health parameters of an user are detected below a certain threshold, an automated call to the nearest hospital is performed by the user device within 5 seconds.
The call is handled in an totally autonomous way: the hospital can accept or declines a certain request of help.
Furthermore, the call can be requested only every minute and won't be performed in case another call from the same user has been already accepted in the previous 4 hours: this will prevent call flooding toward the hospital.

2.2.5 Run organization

Organizers of run events, are able to select a date for a run, to define its path, and to specify an expiration date for the subscriptions. Since a race is set up, athletes can subscribe and unsubscribe to the run, according to their will and preferences.
When a race is taking place, the athletes' information are monitored: their position can be seen on a map by users who have subscribed to the race, and their health status is kept under control in order to intervene in case of necessity.
An event may not be able to start (e.g. not enough runners are present, bad weather conditions and so on and so forth): in this case all the participants are notified.
When a run is completed, the winner will be announced and the information regarding racers will no longer be available to the spectators.

2.3 User characteristics

2.4 Assumptions, dependecies and constraints

3 Specific Requirements

4 Formal Analysis using Alloy

5 Effort Spent

6 References