TrackMe: Implementation document
Software Engineer 2 - 2018/2019

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

Version 1.0
Link to source code: TODO INSERT LINK HERE
Link to what has to be installed: TODO INSERT LINK HERE

December 19, 2018

Contents

1 Introduction

The purpose of this document is to provide all the information regarding the implementation of a viable product of the TrackMe project: in particular it regards the services of Data4Help and AutomatedSOS. It follows a brief description of the structure of the document:

- First of all, in the front page it is possible to find links to the source code and to what needs to be installed
- The second section illustrates what are the requirements that have been actually implemented, providing some useful motivations in order to understand the choices that were made
- The third one takes into consideration the frameworks adopted, recapping and introducing further comments on what was already mentioned in the Design Document. Moreover, benefits and drawbacks are better analyzed, and ulterior decisions are discussed
- The fourth chapter analyzes the structure of the source code and an UML class diagram is present to illustrate a precise structure of the written code
- The fifth section provides information on how tests were written. Coverage is here presented and system tests is presented and commented
- The final chapter helps in understanding what is necessary to do in order to install and run the software, with all the necessary prerequisites

2 Requirements and functions implemented

As already mentioned, in this section it is possible to find information regarding the requirements and the functions that are actually implemented with some motivations.

2.1 Core requirements and functions

All the core requirements from R1 to R9 have been implemented, since, as the name suggests, they are fundamental.

2.2 Data4Help requirements and functions

All the requirements related to G1, G2, G8, G9, G12 and G13 have been implemented, basically because they are considered as the main features and components of Data4Help. This is true for all the mentioned goals expects for what concerns G9, that is the blocking of third party customers, that can be considered as an additional functions, but can always be useful for engaging future users. The excluded ones are the following

- G7, that is the management of elapsing requests
- G14, that is the subscription to non existing data

The motivation that stands behind this choice is basically a constraint on development time and the fact that these were considered more as a nice feature to have, and not something really critically. Indeed, it is still possible to have a good prototype of the service, even without these features. It should be noted, however, that they do not require big efforts and can be easily integrated into the project in a second time: in particular, G7 can be considered as a periodical task to be scheduled that checks and manages the time stamp of the pending requests. For what concerns G14, instead, the discussion is a bit more complex, but it basically consists in introducing a new status for the requests and a task that operates with the requests that are in such status and that performs some checks w.r.t. to the provided dates (that are the starting date and the ending date of a request: this will be clear inspecting the source code of the entities that regard the requests).
A final note on the requirements of Data4Help is the following and it regards the type of aggregated data that third parties can request. All the filters mentioned in the design document have been developed, from a server-side point of view. For clarifying this statement, that may sound obscure, consider that every available filter, except the one that regards GPS position data, is only related to some plain input that a third party customer inserts in the application and that is sent to the system. However, for filtering on GPS position a third party should define the interested region by specifying the coordinates that specify the bounds of the interested region. Since, of course, this is totally no user friendly, the application could provide a list of possible cities and region and automatically translates it. Of course, this feature could also be deployed directly on the server.
Nevertheless, up to now, what is present is the possibility of inserting group requests specifying the GPS filters, but this has not been implemented in the mobile application for the discussed reason, and, because, at this stage, it is considered sufficient to have all the other filters.

2.3 AutomatedSOS

The goals, and the related requirements, that involves AutomatedSOS are G3 and G4. However, in this case, not many of the requirements have been implemented, also due to some external limitations: indeed, considering the Android system and hardware, it is not possible to just intercept the phone call and access the microphone (for automating the phone call) and the speakers (to retrieve the response). Therefore, in order to fully develop the requirements it would be necessary to use VoIP api, that requires some sort of payments. However, some requirements such as R12, R13, R15 and R17 have been implemented anyway, with the difference that the VoIP calls are mocked with normal phone calls and no automation is present for interacting with the emergency room operator. This has been considered enough for a viable product also because it has been chosen to give more importance to the core business of the company, that is considered to be Data4Help. Another few words should be spent on R17, that is "during phone calls, the GPS is set on high precision": this is automatically performed by the Android system when calling emergency services [1].
Finally, for what concerns the part regarding the 5 seconds the following shrewdness have been adopted: the maxitum timeout for retrieving the position takes in the worst case 1 second. After that, the more critical part is parsing a

JSON that contains the emergency numbers of the various countries, but this weights only 120kB. It is thought that this should be fast enough to satisfies the requirements of the five seconds. However, the process speed of code is a problem always related with the performance of the user device and the consumed resources of other applications, therefore being 100% sure that the task is accomplished within that time is impossible. Nevertheless, some tests are perfomed and the avarage speeds satisfies this requirement.

2.4 Non functional requirements

For what concerns the non function requirements, as mentioned in the Design document, a microservices architecture has been developed. In particular, the main implemented features of the architecture are the following:

- Communication between microservices, since this is crucial in order to have a viable product. Indeed, without this, almost no requirement could be fully accomplished
- API Gateway that performs also authentication and authorization: this is also a core feature, since it is the entry point for accessing all the Rest API that the various microservices provide
- Service registry, because otherwise, one should have set up all the network communication in a more static way, and also the management of forwarding requests from the gateway would have been more complex

The load balancer has not been implemented because, among the functions mentioned above is the last one that should be considered, since it is very complex to have one if you an API gateway and a service registry is not present.

Some basic security feature have been developed also: indeed, all the passwords are stored in the database with bcrypt and the only type of communication allowed between clients and the API gateway, is HTTPS. In order to do this, a custom SSL certificate has been generated using the java keytool [2].
The authentication have been implemented by means of an UUID random token and the APIs has been secured in such a way that a certain client can access only the method that he should access: for example, a user can't access methods that regards a third party customer, but, also a user can't access API that regards another user (i.e. a user can access only his pending request, and not the pending requests of any user)
As one can claim, using UUID random tokens is for sure not the best way of achieving authentication, however, the code has been designed in such a way that is easily possible to upgrade this to the usage of JWT just implementing a single interface. This choice has been done in order to simplify a bit the security issue and to focus more on the business core of the project.

2.5 Other comments

The database regarding the collected health and position data, has not been deployed on the cloud at this early stage, because the integration was not considered necessary. Indeed, a viable prototype can be exists even without this.

Indeed, it is more something that regards the deploy, rather than the implementation itself.
The same reasoning has been applied also for the deployment of JARs in docker containers.

3 Adopted development framework

Most of the choices that regards the frameworks were already briefly introduced and motivated in the section 2.7 of the design document (that is, other design decision). However, here frameworks and other API are recapped:

- Spring boot has been adopted since it fits well for microservices and the set up of pattern components of the architecture (i.e. service registry) can be easily integrated with the usage of Spring Cloud. The main drawback of this choice is that spring boot doesn't offer much control to the developer: this of course limit the development time, but when something goes wrong, it may take time to fix the issue
- Spring security has been used to develop the authentication and the access control of the application. It is basically the de-facto standard for securing Spring-based application.
- Spring Cloud Netflix has been used to integrate and set up the API Gateway and the service registry. In particular, Zuul has been set up as the API gateway and Eureka as the service registry. These were of a great help because it is only necessary to find the right configuration settings and then everything works as expected.
- RabbitMQ were used to set up the communications among microservices. TODO INSERT BENEFITS, DRAWBACKS, COMMENTS HERE FOR TANG TANG
- Android: the mobile application has been developed for android. Here, Butter Knife has been used in order to easily bind the layout with the activities. It also enables to automatically configure listener to onClick methods. Also, room persistence library has been used to store collected data that has not been sent to the system yet, and information on the performed emergency calls TODO FURTHER COMMENTS HERE FOR MATTIA

Moreover, not already cited APIs has been adopted, and, therefore, are listed:

- Project Lombok, that is a java library that automatically, by use of annotators, creates certain code in order to reduce the amount of boilerplate code that one write
- Jayway JsonPath for manipulating JSON
- MySQL has been adopted as a DBMS
- JPA for the management of persistence and object/relation mapping

- Google guava for the usage of immutable maps
- Jackson, that is an high performance JSON processor for Java has been used, since it the default library used by Spring boot to convert object to json and viceversa. This has been very useful in the set up of the controllers: indeed, it was possible to define POJOs as controller attributes, and the conversion between HTTP requests and Java is perfectly handled. Jackson has been used also to define views in controller method: this allows to set up that in certain controller methods only certain attributes of a POJO are used. For instance one can specify that when the user is accessing its own information, his password is not sent back, but, when registering, of course the password is needed Using different views in different methods helps in achieving what mentioned
- HATEOS is used to provide hypermedia content to the clients. This helps the client mobile application in accessing the right methods and it makes the APIs restful
- GeoNames has been used in order to find the country codes, if the Android geocoder doesn't work properly

TODO MATTIA AND TANG INSERT FURTHER COMMENTS ON THIS LIBRARY

4 Structure of the source code

4.1 Microservices

Here the code regarding the microservices architecture is explained.
The source code that meets the requirements mentioned above has been organized in the following way: for each microservices a project has been set up. Indeed, when dealing with this type of architecture, one should think of a microservice as a project that should me as much independent as possible from the others: this is the reason that stands behind the choice that has been made. Of course, in this way, it is possible to easily generate the single jars that will be deployed, when necessary, with, as mentioned in the design document, dockers. Therefore, the following projects are present: API gateway, service registry, group individual request service, individual request service and share data service. As one may notice, the one containing the set up of the API gateway also accesses all the information related with the accounts, and, therefore, authentication and authorization functions are coded here. In the following sections the structure of the single projects are analyzed.

4.1.1 API Gateway

4.2 Mobile code

5 Testing

6 Installation instruction

References

[1] Android emergency location service, URL https://crisisresponse.google/emergencylocationservice/how-it-works/

[2] Working with certificates and SSL, URL https://docs.oracle.com/cd/E19830-01/819-4712/ablqw/index.html