Universidade de Coimbra
Faculdade de Ciências e Tecnologia

DEPARTAMENTO DE ENGENHARIA INFORMÁTICA
Introdução às Redes de Comunicação

IRC Project

2018/2019

Delivery date: The work should be uploaded to Inforestudante until 7/12/2018.

Files to submit: The submission should be a zip file containing all the sources of the project, a compiled version and a report in pdf. Do not forget to include the name of all the elements of the group in the final report.

Groups: Groups of 2 students are advised. No more than 2 students are allowed per group.

Grading: The work must be defended in a presentation where all members of the group must be present.

IoT Student Advisor and Best Lifestyle Analyzer (ISABELA)

1. Context

The advent of Internet of Things (IoT) is becoming a reality: a global network of sensors, mobile phones and computing devices that can sensor and communicate in real time. According to a recent research report, the wireless Machine-to-Machine (M2M) market is expected to account for nearly $196 Billion in revenue by 2020, following a compound annual growth rate of 21% during the six years between 2014 and 2020. From the use of these diverse computational elements rises the concept of cyber-physical systems (CPSs), which consists on the sensing and control of physical phenomena through these networks of interconnected devices that work together to achieve common goals.

While these interconnected and intelligent tools communicate with each other without any human involvement, human technology is made by humans for humans. Indeed, one important element often left out of current cyber-physical research is the human user. On the other hand, systems that consider the human context will become increasingly more important, and most future technologies will converge onto human-awareness. Since humans are often considered unpredictable, bringing them into CPSs is a very interesting challenge, as it requires modeling of behavioral, psychological and physiological aspects of human nature. Within these aspects, a multitude of variables regarding the person’s status may be measured, including movement, vital signs, attention level and any other facet that may be interesting to control the task at hand.

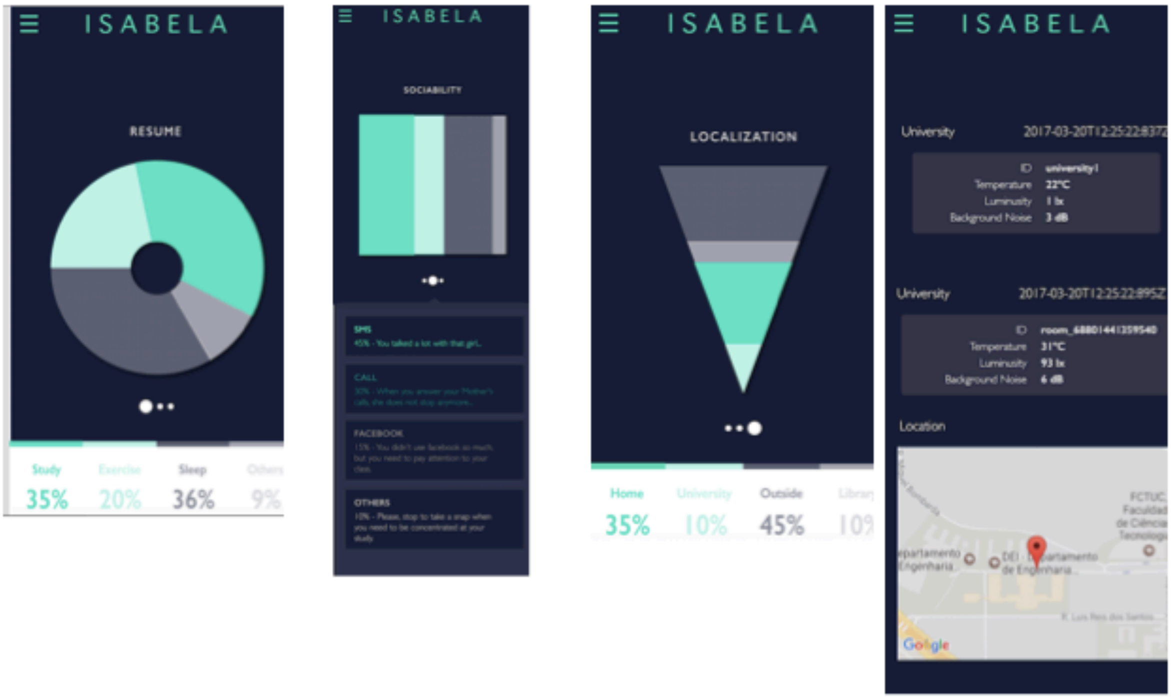
2. ISABELA

One particular scenario where the IoT and CPS concepts may be applied is the improvement of education. Previous work at Dartmouth College has presented an system named StudentLife [1], which uses Android phones to continuously sense the day-to-day impact of workload on stress, sleep, activity, mood, sociability, mental well-being and academic performance of a single class of 48 students across a 10 week term. The authors of StudentLife identified a strong correlation between the automatic sensing data and several mental well-being measures, specifically, PHQ-9 depression, perceived stress, flourishing, and loneliness scales. Their results indicated that automatically sensed conversation, activity, mobility, and sleep have significant correlations with mental well-being outcomes and academic performance.

While StudentLife provided a great example on how IoT devices (smartphones) can be very helpful in acquiring a student's context, the scope of the system was limited. The objective of the study was only to obtain a statistical dataset, containing the behavioral and mental health outcomes of the students. The system did not take any measures to counteract the student's negative academic performance or undesirable lifestyles.

ISABELA intends to extend StudentLife's ideas by taking a proactive approach to "close the loop" by the use of a chat bot (figure 2). In other words, ISABELA not only automatically infers student context (activity, sociability, stress, sleep, mood, mental well-being) but also feeds this information to a decision-making process, which takes measures to improve academic performance.

ISABELA also uses Social Sensors, from social networks like Facebook and Twitter. In fact, these can also be used as sensors of great potential to infer human states. Figure 1 presents some of screenshots of ISABELA:



SMS
45% - You talked a lot with that girl.

CALL
30% - When you answer your Mother's calls she does not stop anymore..

FACEBOOK
15% - You didn't use facebook so much, but you need to pay attention to your class.

OTHERS
10% - Please, stop to take a snap when you need to be concentrated at your study.

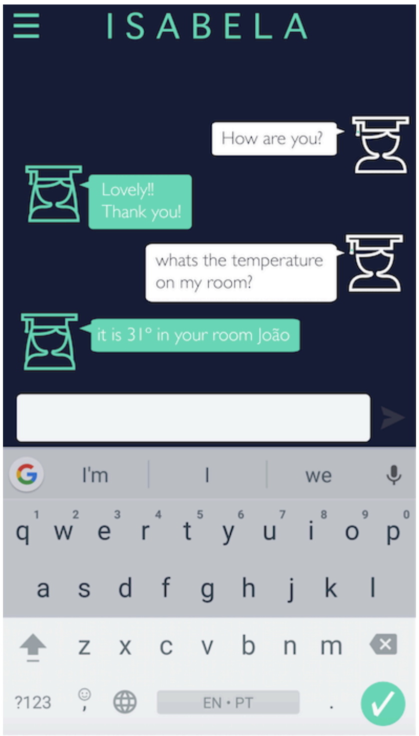
University 2017-03-20T12:25:22:837Z

ID university1
Temperature 22°C
Luminusity 1 lx
Background Noise 3 dB

University 2017-03-20T12:25:22:895Z

ID room_6880144135954
Temperature 31°C
Luminusity 93 lx
Background Noise 6 dB

Figure 1 - ISABELA



ISABELA

How are you?

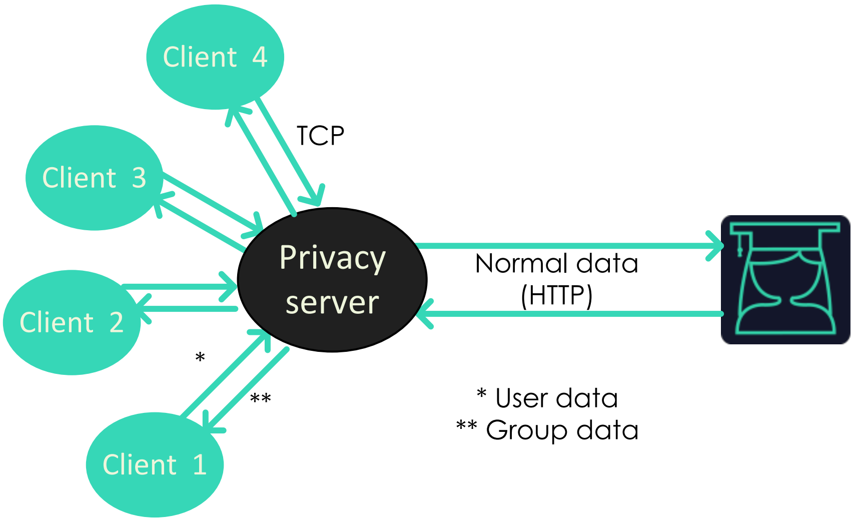
Lovely!! Thank you!

whats the temperature on my room?

it is 31° in your room João

Figure 2 - ISABELA chatbot

3. Privacy Server



Nowadays, privacy is one important requirement of information systems that collect huge quantities of personal data. As a result, the European Union (EU) created in 2016 a general data protection regulation (GDPR 2016/679) to protect the data and privacy of the user.

Taking in consideration the privacy requirements, in this project you will need to create a server (proxy) that performs the anonymization of the data available in the ISABELA server. Users that want to access the data will need to query this new privacy server.

4. Functionalities to implement

Users should be able to access two types of data: **private data** and **group data**. The first is related to the user data, and all fields should be retrieved to the student. The student is identified by an ID.
On the other hand, the second group of the data should be anonymized. Here, users can subscribe specific group data. This data should be collected in the ISABELA server, anonymized by the privacy server that should be implemented in this class assignment, and then retrieved to the subscribers. For instance, the activity of the users of a group should be anonymized by retrieving the number of users in each activity, instead of the user IDs and their activity. Similar solutions should be applied for the remaining fields. It is up to the students to select the most appropriate privacy methods for each field.

Private data:
- Any user may be able to collect each own private data and will not be allowed to query other student's data. To do it, the student will need to use its ID from the ISABELA application. The privacy server will need to block other students to access to the data.
- On receiving the data, the user needs to show the data in the client application;
- Any user may collect the data in two distinct modes: **by query** and **by subscription**. Subscriptions can be changed or deleted.

Group conversations:
- Users will be able to get the list of groups available on the privacy server. Each group will be identified by a group id;
- Similar to private data, users may be allowed to **query** or to make **subscriptions** to the group data;
- Subscriptions can be changed or deleted;
- All users that subscribe a specific group, need to be informed when changes occurred to the data of the group.

General:
- Students cannot access to other student's data, only to anonymized group data;
- The privacy server needs to anonymize all the fields of the students' data, like activity, location, nearby devices, etc.
- The privacy server will maintain all the data in memory, also because privacy concerns;
- All the data collected by the clients should be presented on the screen.

To interact with the ISABELA data API, please take a look at the GitHub repository example.

ISABELA account by default:

If you do not have an account and an USER_ID in ISABELA, you can use:
M5Oy7GKOeO5ckm870qsTNQ