11

Combining Internet of Things and Crowdsourcing for Pervasive Research and End-user Centric Experimental Infrastructures (IoT Lab)

Sébastien Ziegler[1], Cedric Crettaz[1], Michael Hazan[1], Panagiotis Alexandrou[2,3], Gabriel Filios[2,3], Sotiris Nikoletseas[2,3], Theofanis P. Raptis[2,3], Xenia Ziouvelou[4], Frank McGroarty[4], Aleksandra Rankov[5], Srdjan Krčo[5], Constantinos Marios Angelopoulos[6], Orestis Evangelatos[6], Marios Karagiannis[6], Jose Rolim[6] and Nikolaos Loumis[7]

[1]Mandat International, Switzerland
[2]University of Patras, Greece
[3]Computer Technology Institute and Press Diophantus, Greece
[4]University of Southampton, United Kingdom
[5]DunavNET, Novi Sad, Serbia
[6]University of Geneva
[7]University of Surrey, United Kingdom

11.1 Introduction

The Internet of Things will be massive and pervasive. It will impact many and diverse application domains such as environmental monitoring, transportation, energy and water management, security and safety, assisted living, smart homes and eHealth, etc. Developing and testing technologies in conventional research labs appears to be insufficient to really grasp, fine tune and validate new IoT technologies. Moreover, an approach purely focused on technical requirements may lead to a missed target if the end-user perspective is not properly taken into account. End-user acceptance is probably as much important as technical performance, and better understanding their acceptance and satisfaction is critical.

IoT Lab (www.iotlab.eu) is a European research project [1], which has developed a hybrid research infrastructure combining Internet of Things (IoT) testbeds together with crowdsourcing and crowd-sensing capabilities. It enables researchers to use IoT testbeds, including in public spaces, while collecting inputs from end-users through crowdsourcing and crowd-sensing. It enables researchers to exploit the potential of crowdsourcing and Internet of Things testbeds for multidisciplinary research with more end-user interactions. IoT Lab approach puts the end-users at the centre of the research and innovation process. The crowd is at the core of the research cycle with an active role in research from its inception to the results' evaluation. It enables a better alignment of the research with the society and end-users needs and requirements. On the other side, IoT Lab aims at enhancing existing IoT testbeds, by integrating them together into a testbed as a service and by extending the platform with crowdsourcing and crowd-sensing capacities.

11.2 Approach

In order to achieve such aims, IoT Lab has researched complementary set of technologies and approaches, including:

- Crowdsourcing and crowd-sensing mechanisms and tools, by developing a smart phone application enabling researchers to collect real time feedbacks from research participants. It also enables participants to share data from their smart phone embedded sensors.
- Integration of heterogeneous testbeds together, by federating together several European IoT testbeds located in different parts of Europe.
- Virtualization of IoT testbeds and crowdsourcing resources into a fully integrated Testbed as a Service;

The IoT lab framework has been designed and developed bearing in mind two key objectives:

- Enabling and supporting multidisciplinary researches;
- Ensuring privacy by design and a full compliance with European personal data protection obligations, including the newly adopted General data Protection Regulation.

In order to validate the designed model, several research and experiments have been tested, including “Crowd-driven research”.

We will now present with more details some key technological developments.

11.3 Architecture

IoT Lab platform architecture design addressed a double challenge: on one hand, it had to integrate diverse IoT-related testbeds (static, portable, mobile) located in different regions of Europe; on the other hand, it had to integrate smart phones with existing FIRE testbed infrastructures, thus representing a novel approach with respect to existing crowdsourcing solutions. An architecture generation process started with the analysis of technical and end user related requirements derived from selected representative use cases in order to identify key platform components, their functionalities, interaction patterns, interfaces and communication links and enable fully supported experimentation through both crowd and IoT interactions.

At the top level key components are:

- **IoT Lab Accounts Manager** for the profile management of all users' accounts, including the access control and support for incentives and reputation
- **IoT Resources Management Interface** based on Fed4FIRE enablers enabling interactions with IoT components from testbeds and smart phones and access to collected IoT data
- **Crowd Interaction Management Interface** completely independent from Fed4FIRE, that handles interaction with participants, including editors to set up a survey, and enables access the collected crowd knowledge data.

The architecture derivation process followed an IoT-A methodology [2] to support interoperability and scalability and to enable use of a wide range of heterogeneous devices and testbeds from different application domains thus satisfying a high number of requirements. Privacy by design concept is followed to ensure participants are requested minimal information and, that for each research and its belonging experiments a clear description of the required user and device data is presented.

IoT Lab architecture illustrating its federation strategy and modularity is presented at Figure 11.1. Each individual static testbed facility uses a SFAWrap via which the testbed resources are exposed through the Aggregate Manager.

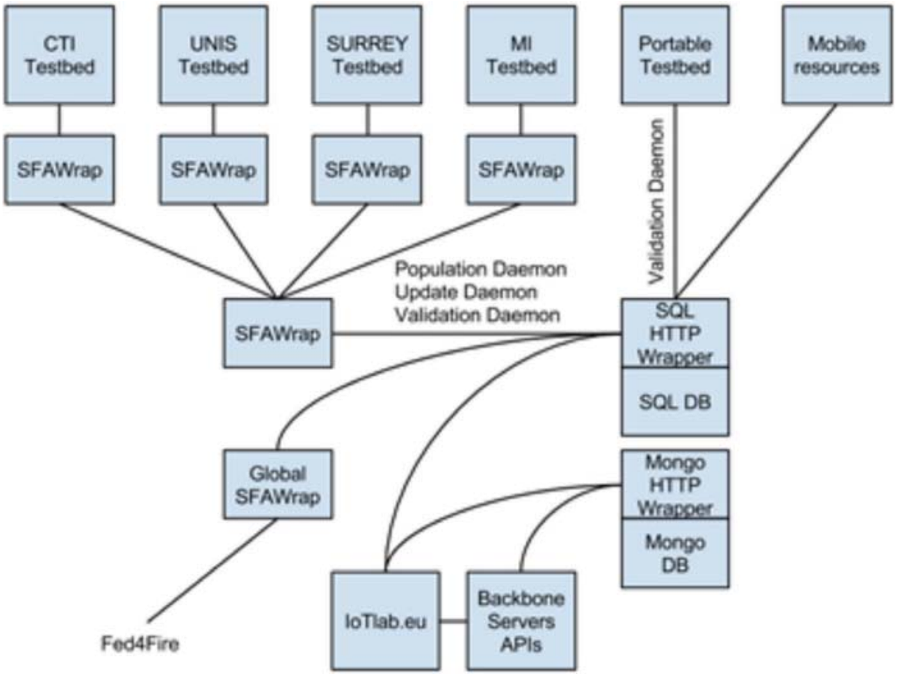


Figure 11.1 Overview of the IoT Lab architecture defining the federation strategy and showing the modular architecture.

All information regarding the type of the resources, their availability and the way of accessing and interacting with them is stored in an SQL database acting as a Resource Directory. Access to this Resource Directory is provided via a HTTP API. Resources that are provided in an ad-hoc manner, such as those of portable testbeds or the crowdsourced resources via the IoT Lab smartphone application, are registered to the system by directly accessing the Resource Directory. This registration process is regulated by a validation daemon. Although these resources do not utilize the SFAWrap (the wrapper is not designed to address the ephemeral nature of such resources), they do use the same resource description schemes and tools (e.g. RSpec documents). All resources stored in the Resource Directory (individual and portable testbeds and crowdsourced resources) are exposed to third party entities via a global SFA Wrapper that wraps around the database. This way, all registered resources are virtualized and exposed via the common interfaces of Fed4FIRE enabling other facilities to discover them. At the end-user application layer of the IoT Lab platform, a researcher conducting the experimenter can access all available resources via the IoT Lab Web page. After having been identified, a researcher can create a new research project, review and select required resources, define the experiment and dispatch it for execution at the back-end of the platform. During the execution of the experiment, all collected measurements are stored in a second database, the Measurements Database. Measurements Database is developed using MongoDB to better address the nature of the stored information as well as their expected big volume.

A view of deployed IoT Lab architecture is presented in Figure 11.2 [3] illustrating all the modules and their belonging components: Account and Profile Manager, Resource Manager, Experiment Manager, User Interface (Web and Mobile app), Testbeds (static, portable/mobile and smartphone) as devices, Communication components and Security and Privacy.

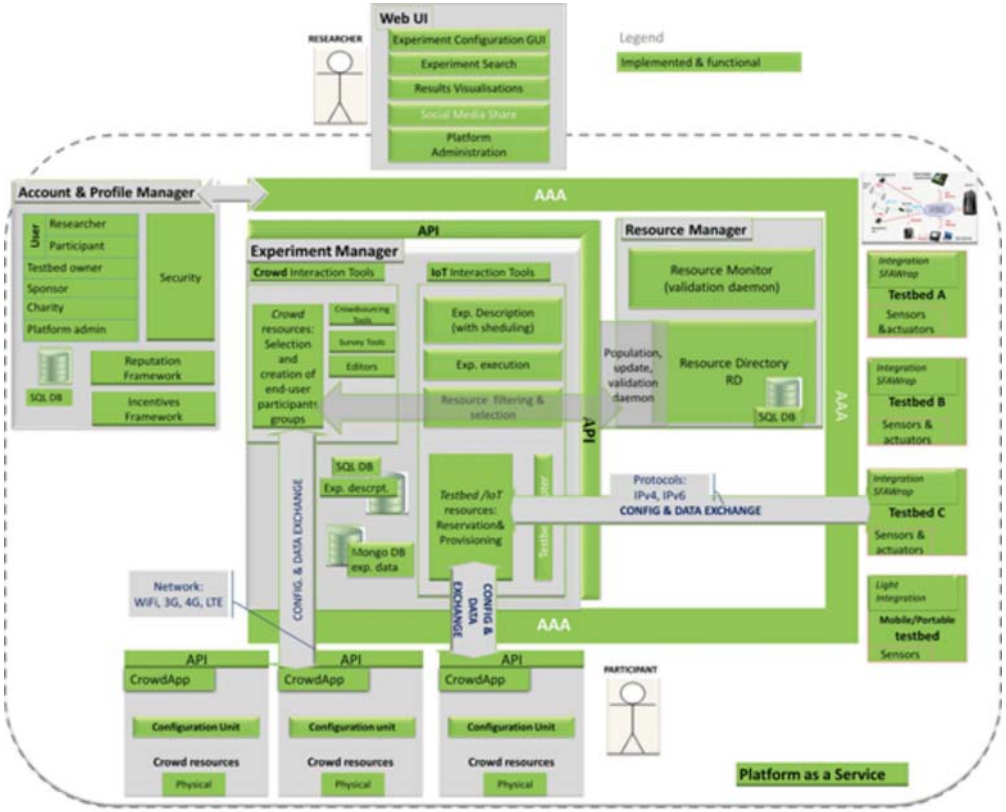
IoT Lab architecture represents a service based architecture for IoT testbeds exposing all the testbed operations as services (Testbed as a Service), enabling federation of diverse resources in a scalable and standardised way and enabling smooth and seamless integration of crowdsourced resources. Researchers performing experiments via Testbed as a Service can via a common interface (Web UI) access a diverse set of resources and conduct experiments.

The IoT Lab network architecture with all components (application, testbeds and server) is shown in Figure 11.3. The current platform is scalable to a considerable number of mobile and testbed resources [4]. For the average scenario with the IoT Lab server working at 50% of its capacity, we can have 2.8 M devices connected to the platform, whereas for the testbeds 24 M devices can be connected. Even if in a very remote use case the number of resources reaches or exceeds the limit, the server capacity can be increased in order to support all connections and data.

11.4 Heterogeneous Tesbeds Integration

IoT Lab brought together several pre-existing IoT testbeds from UK, Switzerland, Greece, Serbia and Sweden, including:

- University of Surrey smart campus testbed;
- Mandat International Smart HEPIA and Smart Office testbeds;
- University of Geneva IoT testbed;
- Dunavnet EkoNet testbed of mobile environmental sensors;
- CTI in Patras IoT testbed;



Note: There is only one SQL DB which stores data related to all resources and experiment description. For visual purposes it is presented on this figure as 3 separate DBs.

Figure 11.2 IoT Lab platform deployment.

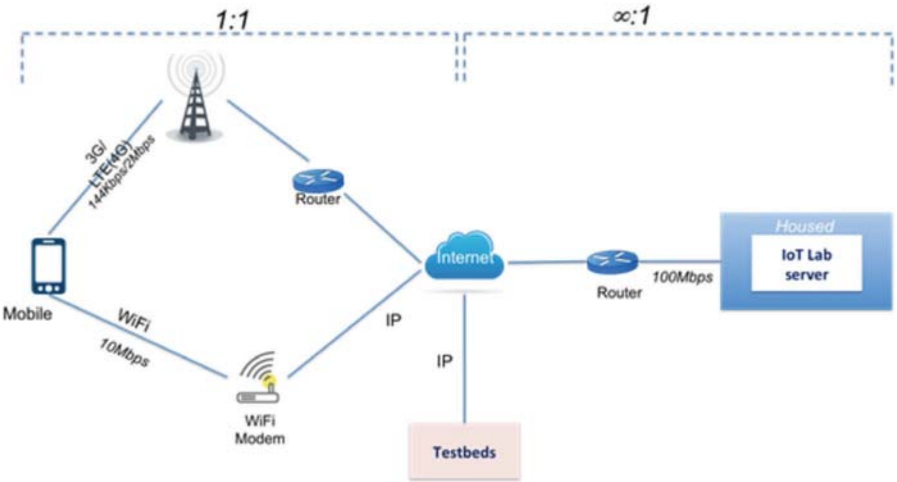


Figure 11.3 IoT Lab – network architecture with all its components.

The various testbeds were developed with distinct technologies and architectures. In order to enable a proper integration of these various and heterogeneous resources together and to enable end-to-end interconnection, the consortium opted to leverage on IPv6 as a network integrator. It leveraged on IoT6 European research project results [5] and initial attempts to enable IPv6-based testbeds integration between Europe and China [6].

An important challenge was related to the diversity of compliance levels with IPv6. Being distributed cross various countries, the corresponding ISP services offer was uneven too. We ended up with four distinct testbed profiles in terms of network configurations and connectivity,- all to be integrated together. The Figure 11.1 details the various cases:

- **Case A – Local IPv6 integration, including with non-IP IoT devices:** In this case, the ISP constraints were avoided through a direct integration. However, the testbed included both IPv6 and non-IP IoT devices, using communication protocols such as KNX, ZigBee, EnOcean, BACnet and others. In order to integrate these heterogeneous devices, a UDG proxy has been used to generate consistent and scalable IPv6 addresses to the legacy devices.
- **Case B – Remote full end-to-end IPv6 compliance:** In this case (TB-B), the testbed integration was achieved through end-to-end IPv6 integration, including 6LoWPAN end nodes directly parsed into IPv6 addresses.

- **Case C – Remote IPv6 testbed through IPv4 ISP access:**
  In this case (TB-C), in order to overcome the lack of IPv6 connection at the ISP level, the testbed integration has been performed through v6 in v4 end-to-end tunnelling, with a very limited latency impact.
- **Case D – Remote IPv4 testbed:**
  Finally, one of the testbed was fully and exclusively IPv4 based (TB-D). In this context, we decided to use a UDG proxy on the server side to map IPv6 addresses on top of the local IPv4 addresses.

The address definitions across the testbeds were maintained consistent by clearly separating the management of the Host ID on one side (IoT address) from the Network ID (Testbed address). This simple approach resulted in a consistent and highly scalable model, enabling the Testbed as a Service (TBaaS) to use a fully integrated and homogenized addressing scheme, including with mobile devices.

Another challenge was related to the heterogeneity of communication protocols used in some of the testbeds. In order to overcome this challenge, IoT Lab leveraged on the Universal Device Gateway (UDG) [7], a multi-protocol control and monitoring system developed by a research project initiated in Switzerland. It aimed at integrating heterogeneous communication protocols into IPv6. The UDG control and monitoring system enables cross protocol interoperability. It demonstrated the potential of IPv6 to support the integration among various communication protocols and devices, such as KNX, X10, ZigBee, GSM/GPRS, Bluetooth, and RFID tags. It provides connected device with a unique IPv6 address that serves as unique identifier for that object, regardless its native communication protocol. It has been used in several research projects, including by IoT6, where it has been used as an IPv6 and CoAP proxy for all kinds of devices.

In IoT Lab, the UDG platform has been used as a locally deployed proxy in the local testbed (TB-A in the Figure 11.4) and as a cloud-based proxy in some other cases (TB-C and TB-D in the Figure 11.4). However, for communication protocols which are non-compliant with the Internet Protocol, a local deployment was required.

11.5 IoT Lab Smart Phone Application

IoT Lab intends to put the end users in the centre of research and innovation. It required the development and introduction of a tool that offers ubiquitous and seamless interaction capabilities with the crowd participants. A specific

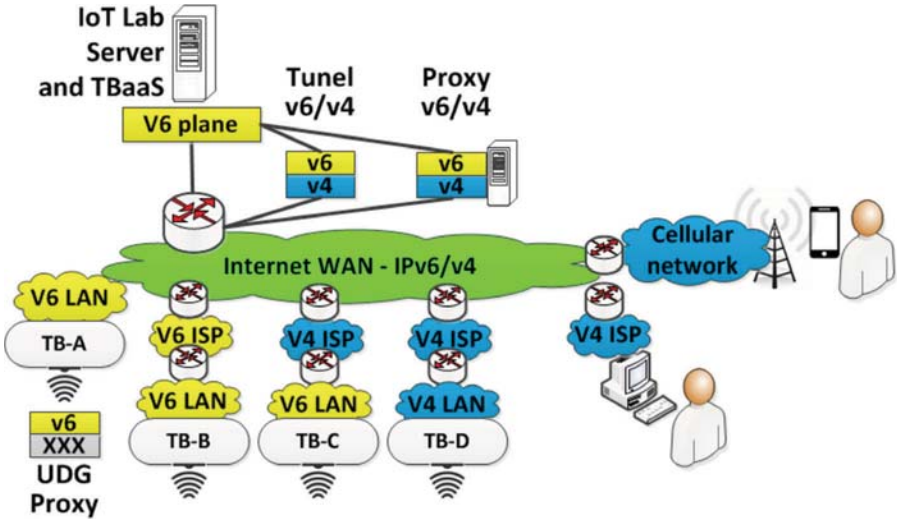


Figure 11.4 IoT Lab IPv6-based network integration representing the four main testbed profiles.

IoT Lab smart phone application was developed, which can be installed to all the devices that run Android OS 4.1.1, or later.

Ensuring a user-friendly interface with a state of the art user experience led to focus on the user experience and feedbacks with iterative adaptations and fine tuning during the project. Moreover, frequent updates made sure that all the found bugs were solved, as well as, the provided functionalities were optimised constantly.

Smart Phone Application Functionalities

The mobile smart phone application provides a set of functionalities that are described below:

- **Add idea**: through a limited number of steps, any user can be part of the platform and express a new idea. The predefined options help make this process faster and users more keen to use it.
- **Rank idea**: every user can see and rank the aforementioned proposed ideas. By selecting one out of the list of all the available, the user can see more information about it and rank it using the provided tools.
- **Available researches**: IoT Lab application is, among others, a tool for crowdsourcing and crowdsensing. Hence, it can be used during ongoing

researches. A user can see all the available researches, browse them, and learn more about each one of them. If he/she wishes to join one of them, it can be done by simply clicking the equivalent button.

- **Surveys**: Experimenters can push surveys to all or to a set of participants in the context of a research. The user can access them through the application and fill them whenever he/she wishes to do so.
- **Update location**: our tool provides a functionality that updates mobiles' location by scanning a QR code. This is used during researches that need fine grained location updates.
- **Map**: IoT lab application can display all the resources of our platform on an anonymised map. This helps the users to visualise the magnitude of our project and feel part of the community, without having any privacy issue.

Additionally, each device that runs our application can be potentially used as a multi-purpose sensing mote. In order to do that, the user/owner of the device can to explicitly allow the application to make the embedded sensors of the device available to future researches, or to manually join a research. Moreover, since IoT Lab was designed with respect to users' privacy, each time one's device is about to be exploited in a crowdsensing scenario, multiple notifications are sent to the device informing about the ongoing background tasks. More about the IoT interactions and experiment composition will be presented in the next section of this chapter.

Crowdsensing Using IoT Lab Application

Crowdsensing takes place as a part of an ongoing research. As described in the previous section, a device can be manually or automatically assigned to one research according to user's settings and configuration. The background mechanism that sets crowdsensing to work is Google Cloud Messaging (GCM).

Protocol Selection

Before digging more into the steps that need to be taken during a crowdsensing experiment, it is important to present the reasons that led us to the selection of the used IoT communication protocol. The deciding factors were

- computational requirements,
- bandwidth usage,
- scalability,
- robustness,
- support from the community.

MQTT is a lightweight-by-design IoT protocol that is widely aligned with our system requirements, and was the other candidate except GCM. IBM claims [8] that in real life scenarios we can preserve 4.1% energy per day, just by switching from HTTPS to MQTT. Additionally, there is a plethora of free brokers that can numerous active connections at all time. Finally, the Eclipse community hosts and supports the MQTT project over the past years.

On the other hand, GCM is a service created and provided by the IT giant, Google. With a dedicated community ready to answer and tackle all the emerged problems, GCM was a great candidate. Moreover, GCM is not limiting the number of active devices.

Both protocols were selected after reflecting the type of communication needed between the devices and the back end. Due to their nature, smartphones do not have a static IP. Hence, we were troubled by the need to be able to access specific devices from the back end. MQTT and GCM offer mechanisms that handle message delivery.

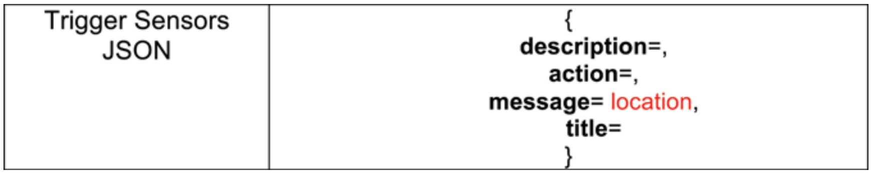
We chose GCM other approaches, as it is open source, scalable, free for a big amount of users, and is optimised in terms of energy consumption during idle states. Additionally, all the back end support is handled by Google itself and we do not need to do any more provisioning.

Mobile Crowdsensing

Google Cloud Message carries JSON messages that can be easily modified and are used in order to send sensing triggers to a specific, or a set of mobile devices. An example of such a message is displayed in Figure 11.5.

As presented if Figure 11.6 bellow, the steps that take place during a crowdsensing experiments are the following:

- Back end sends a notification to all the devices that are about to participate in the crowdsensing experiment. The notification is delivered using the GCM.
- After a period of time, the crowdsensing loop starts.
- A sensing trigger is pushed to the mobile phone using GCM.
- When the trigger is received, the OS is responsible to “wake up” the IoT Lab application.
- IoT Lab application analyses the sensing request and samples the desired measurement.
- The measurement is stored to the IoT Lab database using the appropriate API.



Trigger Sensors
JSON
	{
	description=,
	action=,
	message= location,
	title=
	}

Figure 11.5 A sensing trigger message.

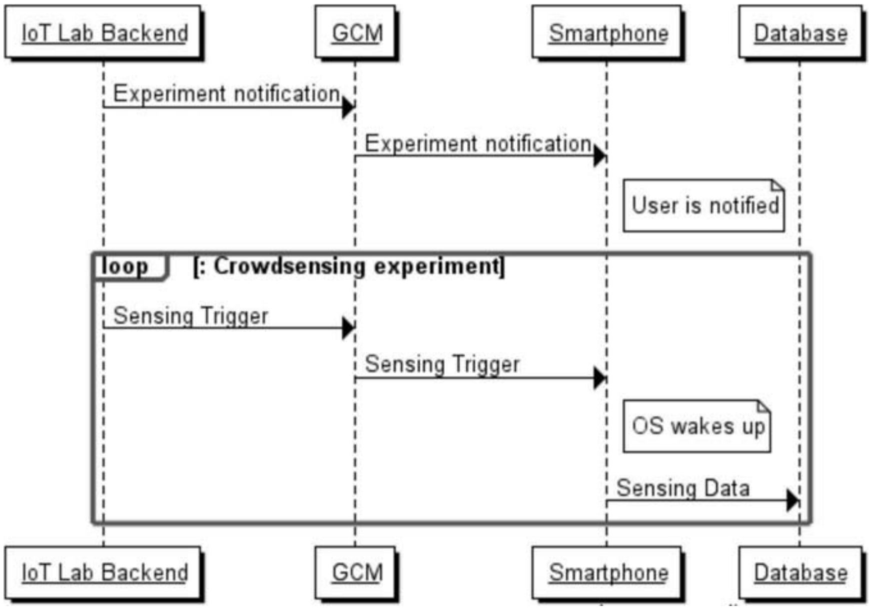


Figure 11.6 Sequence diagram of the Crowdsensing steps.

11.6 Testbed as a Service

The IoT Lab platform federates a variety of resources, ranging from static IoT devices to mobile phones. The role of these mobile devices is twofold: they can function as multi-purpose sensing motes (i.e., using accelerometer, GPS, luminosity) or as a source of interaction with their owners. From the above we can distinguish the two kinds of experiments: The first one with IoT devices either mobile or static and the second one involving the owners of mobile phones. These experiments are realised through IoT and Crowd Interactions functionalities.

IoT Interactions

In IoT interactions the experimenter is provided with a list of available resources that he can view and reserve for their experiment. After the experimenter chooses and reserves the desired resources, he/she is prompted to the experiment composition module. In the background, an XML schema called RSpec is used to transfer the information regarding the resources reserved between the reservation module and the experiment composition module along with some meta-information on the experiment itself; e.g. duration and period of execution, human readable description of the experiment, etc. This information is incorporated in the RSpec document via tags such as the <research id> tag, that provides the id of the parent research of the experiment to be composed, the <experiment title> tag which provides the title the experimenter has given to the experiment to be composed and the <experiment desc> which provides a short description of the experiment.

Experiment Composition

The experiment composition module receives this information and provides a simple but powerful mechanism with which the experimenter can define the details of how resources will be used in the context of "If This Then That" (IFTTT) scenarios. The final experiment consists of a set of these scenarios.

The experiment composition module allows the experimenter to set the following actions:

- **Get a value from specified resources**. The frequency of the reading request is set in minutes or hours and includes one or more resources. The resources must be of type "sensor" and must be included in the experiment before the experimenter enters the main composition module. This action is called "reading". As an example, a reading can be "Get a value from sensor 1 every 5 minutes between these 2 dates and times".
- **Set a condition**. A condition can be the average, absolute, minimum or maximum value of one or more resources being greater, equal or lesser than a set value. In the case of multiple resources a logical operator can be set. An example of a condition can be "The maximum value of sensor 1 OR the maximum value of sensor 2 to be greater than 5".

- **Set an outcome**. An outcome is an action that can be taken. This action is either to take more measurements from sensors or to actuate an actuator. Outcomes also include a logical operator in case there is more than one conditions. An example of an outcome could be "Actuate actuator 1, if all conditions are met (with logical AND)".
- **Define an action**. Actions are combinations of conditions and outcomes. Actions are set in an "IF-THEN" form in order to clarify their meaning. An example of an action can be "IF condition1 AND condition2 are true THEN perform outcome 1". The logical operator AND is actually defined in the outcome and not in the conditions, as specified above.

After the experiment scenario has been defined, it is dispatched to the execution module. The scenario is described in an XML schema called Experiment Description XML schema (ED XML). The Experiment Description XML defines a parent tag <experiment> </experiment> that encloses all other elements. The <measurements> tag defines the measurements database server information along with the <ip> and <port> sub-tags inside it. The next tag is a random identifier tag. This is generated during the ED creation randomly and is used to uniquely identify the experiment description. The tag that provides this identifier is the <identifier> tag.

Readings are included in the <reading> tag. Inside this tag, a <frequency> tag with a "unit" property defines the frequency of the reading while <start> and <end> tags define the start and end of the readings period for the specified reading. The <resources> tag then defines which resources have to be probed for a reading every time it's needed. These are defined using <id> tags that include properties "component", "resource id", "port", "ip", "protocol" and "path". The combination of these properties allows the execution engine to identify and reach the resources directly.

Actions are defined using the <action> tag. These include <conditions> and <outcome> tags. The <conditions> tag include the aggregation and logical operations as a tag and property respectively (e.g. <average logic="and">). Inside this tag, the resources are defined using an <id> tag and also the threshold is defined using a <threshold> tag. The <outcome> tag includes a property for the logical operator and inside the tag, resources are defined (either sensors or actuators) using <id> tags as above. An example of an ED XML is shown in Listing 1.1 in the Appendix.

Experiment Execution

When an experimenter finalizes the definition of an experiment at the Experiment Composition module, an Experiment Description XML document is created which is transferred to the Experiment Execution module which proceeds in parsing it and finding all necessary information in order to start running the Experiment.

At first, the research ID, the experiment title and the experiment description are identified and posted as a new ‘research’ entity in the Resource Directory database. As already described, the Experiment Description XML document contains a number of readings and action tags. Each of these tags will spawn a new celery job to handle their tasks.

Each reading tag has several resources with their contact information and a frequency with which they are to be read. Every one of those readings, spawns a celery task tasked with obtaining the measurements from the resources in the time and with the frequency specified by the experimenter. When the time to obtain measurements comes the task creates a new task responsible for the next set of measurements. When the measurement comes, a new task responsible for the action tag will be called. Inside the actions tag there are a number of tied conditions and outcomes. Their information is parsed and summarized in two lists: one for the conditions called conditionsList and one for the outcomes called outcomeList. A task for the function called conditionChecker(), with the two aforementioned lists as parameters is called after the resolution of each reading tag. This task, will evaluate the logic of conditionsList as specified in the Experiment Description XML. If it is evaluated to ‘True’, then the outcomes from outcomeList will be executed.

Crowd Interactions

In Crowd interactions the experimenters ask for inputs from the smartphone users through surveys and questionnaires (Figure 11.7). The surveys are constructed using LimeSurvey which is integrated within our platform. The process of filtering and selecting the user in order to engage him/her in the specific research includes the following mechanisms available through the architecture: survey queries, survey lists, geofencing and project code.

Survey Queries: A query is a mechanism that allows the experimenter to filter crowd users in a meaningful way in order to select the users needed for the post of a mobile query. The filtering function is based on the socio-economic profile of the user which they voluntarily include during anonymous registration through the mobile app. The query is defined and then saved in the experimenter’s profile so that it can be easily reused in the future, which makes it a very powerful tool as the crowd users constantly change in number

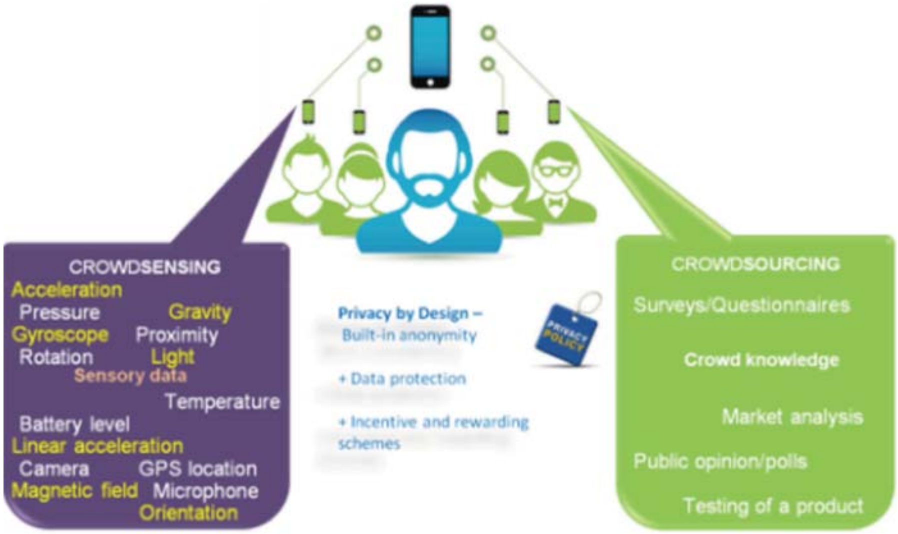


Figure 11.7 Crowd participation in TBaaS.

throughout the architecture's lifetime. Queries, although static themselves, provide dynamic results in the form of sets of users that fit the set criteria.

Survey Lists: Every time a query is used, an up-to-date list of crowd users that meet the query's criteria is presented. The experimenter then has the opportunity to select individual recipients to form a survey list. A survey list is a static list of survey recipients that is used to send a survey to the mobile devices recipients. The content of the user list is anonymous and only social and economic data are associated with each entry. When the final survey list is compiled, it is saved under the experimenter's profile and can be used as the destination list in which to post a survey. A special case of a survey recipient list is the "all users" static list which includes all available users of the architecture.

Geofencing: Geofencing refers to the experimentation activity in which it is possible to setup a virtual perimeter on a real world geographic area and utilize this perimeter for determining if a mobile resource enters the area defined by the perimeter, exits such an area or is located inside or outside this area. This could be achieved, for example through the use of the GPS sensors, which are usually available on modern smartphones.

Project Code: A project code is a mechanism that allows the experimenter to advertise an experiment (e.g. through social media) and select all the users that responded to his call. It allows both the filtering of crowd resources as well as creating a survey list.

11.7 Virtual & Modelled Testbeds

In order for research in networks and systems to be conducted in a systematic way, there is a need for environments that will provide the necessary control and tools for designing and conducting experiments with the aforementioned attributes. Such integrated environments are called testbeds; i.e., facilities particularly designed for conducting scientifically correct experiments in order to test analytic results, computational tools, architectures and technologies.

Typically, testbeds are developed with a focus on a particular class of applications (e.g. wired networks, IoT systems, etc.). Apart from the development of the system under study per se, auxiliary components are also developed in parallel that help define the parameters of the experiment and monitor the operation of the system. Typical examples include tools for automatic reconfiguration of the system architecture (e.g. selecting a specific sub-set of the resources), automatic definition of parameters such as generated volume of data, on-line monitoring of the operation of the system and data collection for post-experiment processing. Such toolsets standardize the experimenting process and alleviate a great burden from the researchers thus helping them focus on the actual research.

However, despite their great advantages, testbeds also pose limitations on experimental research. The way a testbed is designed and developed designates (sometimes to a significant extent) the way experiments can be conducted and therefore may greatly affect research. The hardware that is being used, the size and the architecture of the testbed are indicative factors which have great effect on experiment design. For instance, a facility may be focusing on IoT applications (e.g. use case scenarios for smart rooms) and can be equipped with specialized hardware for monitoring energy consumption. On the other hand, it may provide limited support for developing and evaluating low power routing algorithms.

In this context, software-based facilities can be used in order to alleviate such restrictions. An existing physical testbed can be qualitatively and quantitatively extended with the aid of software-based facilities. IoT Lab has identified and investigated two different classes of such facilities. On one hand virtual testbeds, which quantitatively augment a physical testbed via emulated nodes, and on the other hand modelled testbeds which qualitatively extend a testbed via specialized simulation software.

Virtual Networks as Testbeds

Sometimes, the need arises for a physical testbed to be augmented quantitatively, but the physical resources are limited and cannot be easily extended on demand. In order to address such cases and provide the facility providers with a higher degree of agility, IoT Lab has proposed a method for augmenting an existing physical testbed with virtual nodes. Of course, the proposed method is not generic and does not apply to any kind of testbed facility. Following the thematic scope of IoT Lab, the proposed method addresses IoT experimenting facilities with a focus on studying use case scenarios (e.g. instead of evaluating networking algorithms and protocols)

In this method, the Cooja network simulator is used, which is an actual compiled and executing Contiki system available also in its latest release of 3.0. The advantage of this system is that Contiki is compiled for the native platform as a shared library which is then loaded into Java using Java Native Interfaces making the system fully compatible with physical resources running the same Contiki code. Apart from the fact that the simulated resources do not actually sense the environment and are not physically placed in the same space as their physical counterparts, the resulting resources are identical to the physical ones, running the same firmware and interfaces.

The simulated nodes form a virtual network which communicates with the provider's gateway. The gateway then exposes the virtual network to the rest of the IoT Lab platform using the same methods and interfaces as the physical nodes. This allows for the experimenter to discover, reserve and utilize them using the standard IoT Lab interfaces and processes, thus augmenting the testbed and extending the availability of resources as needed.

When advertised to the IoT Lab platform, the simulated resources are marked as virtual so as to be identifiable from the experimenters, who will choose whether they want/need to use them along with the actual physical resources. The pool of simulated resources is predefined for each testbed and each resource is utilized only when needed. This choice is made in order to mitigate any potential issues regarding the stability of the provider's gateway and the quality of service provided to the experimenters. The size of the pool of the simulated resources depends on the capabilities of the gateway and is to be decided by the provider.

The simulated resources report sensor values by either taking into account only other simulated resources in the system (isolated simulation environment) or by being interlaced with physical resources of the same provider. These resources will be interlaced with the physical resources of the testbed in the sense that the sensor values reported by the simulated nodes will be extrapolated from the values measured by the physical motes. The extrapolation will be based on their relational (virtual) position in the space of the modelled testbed.

Modelled Testbeds

Some of the restrictions posed by testbed facilities come from the limited number of available resources (e.g. sensor motes) as well as the usually fixed positions of the resources in the area of deployment. In a typical physical IoT testbed adding more resources or changing their topology may not be so easy (either due to lack of hardware or due to configurations needed). In an effort to mitigate such issues IoT Lab studies modelled testbeds.

In this study, modelled testbeds although operating and heavily relying on software, are tightly connected with existing physical testbeds; both in terms of semantics and in terms of operation. This way, the benefits coming from both solutions are combined. On one hand, physical testbeds provide the desired level of realism – an issue that commonly emerges in simulation studies – and on the other hand modelled testbeds provide the desired agility and ease of deployment. The modelled testbed contains data on which physical resources are taken into consideration as well as which virtual resources were created in its context (virtual resources created in the context of a modelled testbed are not shared or used along with resources of other modelled testbeds). In terms of semantics, a modelled testbed is connected to the physical testbed it models. So, it also maintains data on the physical space of the modelled testbed in the form of building topology data.

Regarding physical resources, these are described in the Resource Specification XML (aka RSpec) along with the paths needed for them to be accessed and serve measurement queries. A similar mechanism is provided for the virtual resources of a modelled testbed in the form of a Virtual Measurements Interface. This interface provides paths to be used by the experiment execution module of the IoT Lab platform for each virtual resource that is contained in a modelled testbed. Behind the scenes, it also calculates the measurement values that the virtual resources return as a response to measurement queries. These responses are based on the real measurements obtained by the physical resources as well as their relative placement in the 3D space.

As an indicative example, consider a modelled testbed modelling a given IoT testbed, which is equipped with several environment sensors (ambient luminance, temperature, relative humidity, etc.). An experimenter spawns a new virtual temperature sensor, in the context of this modelled testbed, and places it in between two other temperature sensors which correspond to physical sensor motes in the physical testbed. When queried, the sensor values that the virtual sensor will report, will be a function of the real values measured by the two physical sensors. For instance, this function can be defined as the weighted average of the two real measurements with respect to the distance among the sensors. The actual form of this computing function can vary and therefore, can be defined by the testbed owner. We also investigate the possibility of each modelled testbed to support several such functions and give the ability to the experimenter to freely choose among them. The specific forms of the function could include several types of average (in terms of central tendency) depending on the relative distances and number of neighbouring physical resources of the same sensory type and could be weighted depending on several other topology data, such as walls blocking direct line-of-sight between physical and virtual resources.

11.8 Privacy by Design

IoT Lab is deeply committed to respect and embed privacy and personal data protection. The whole platform is designed and developed with a *"privacy by design"* approach. The privacy and personal data protections are part of the project's requirements and are impacted the platform architecture, as well as the technologies used. Any data collection is based on the prior informed consent of the users and the potential use of personal data will be fully in line with the European directives and regulations.

The European Personal Data Protection Norms

Personal data protection is a fundamental requirement and objective of IoT Lab. The project committed to align and fully abide to the European personal data protection norms. It voluntarily decided to align with the newly adopted General Data Protection Regulation (GDPR).

According to the GDPR, article 4, *""personal data" means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;"*

In its recital 26, the GDPR states that: *"The principles of data protection should apply to any information concerning an identified or identifiable natural person. Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information, should be considered to be information on an identifiable natural person. To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments."*

The same recital highlights that: *"The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes."*

The Dilemma and the IoT Lab Approach

The main dilemma in IoT Lab Privacy policy is between complete end-user controlled process and the scope of the platform to serve and support researches. On the one hand, the project intends to maximize personal data protection. However, if users can modify/delete the provided data, it will impact and change a posteriori the results of the research, which is a real problem for the researchers that are using the platform. This can be considered as a trade-off between a complete end-user controlled process and the purpose of the platform to serve and support researches. IoT Lab, being a research oriented platform, is assigning the priority to the researcher. The adopted policy will be based on clear prior informed consent mechanisms. Participants will explicitly accept to give away experiments data, provided that they are fully anonymized.

IoT Lab main purpose is to support the research community by providing a tool enabling researchers to perform experiments, collect data and publish their results, without any risk that their results may be compromised by later modifications or manipulations. The capacity of IoT Lab to anonymize the collected data is hence of upmost importance. By failing to do so, the platform should enable the participants to access, modify and delete their data at any time. This would translate in modifying research results at posteriori. It would be a major problem for researchers, as their published results could be later changed by the participants' posterior interaction.

In order to address this complex situation, IoT Lab has adopted a dual strategy:

- IoT Lab has researched and aimed at ensuring systematic, complete and effective anonymity of participants and anonymization of data collected from the participants in line with Recital 26 of the GDPR. The IoT Lab platform voluntarily intends not to know who are the natural persons taking part in its experiments.
- In parallel, IoT Lab has developed mechanisms that enable, in case of technology or jurisprudence evolution, to access and delete specific data sets provided by the participants.

IoT Lab is committed to fully respect the European personal data protection norms, and is treating other specific data sets, such as information related to the researchers, as personal data, by enabling the non-anonymized data subjects to access, modify, and delete their personal data, as well as to benefit from the right to be forgotten. Moreover, the platform has adopted a very clear and explicit prior informed consent mechanism, as well as the possibility for the participants to control and modify at any time the data they share and provide to experiments.

Our Strategy and Technical Measures

Based on the considerations in the previous subsections, our consortium has taken full measures to implement applicable EU policies and good practices in order to ensure the privacy of the data subjects who participate in experiments with the IoT Lab platform. Our consortium has decided to adopt a privacy protection strategy based on the following anchor points:

- *Full compliance with European personal data protection norms.* We have followed the guidelines given by the EU privacy protection legislation (e.g. EU Data Protection Supervisors, Opinion 05/2014 on Anonymization Techniques – ARTICLE 29 DATA PROTECTION WORKING PARTY etc.) so as to be fully compliant with existing EU legislation with regard to protecting the privacy of the IoT platform participants.

- *Leverage on effective participants data anonymity* as specified in Recital 26 of the GDPR.
- *Principle of proportionality*. The IoT platform will never ask from a participant any information not directly linked to an experiment or research conducted through the platform. This precludes the collection of any personal information leading to the identification of the participant as it is not directly linked with the types of experiments allowed by the platform.
- *Clear Prior informed consent mechanism*. We have implemented a user consent mechanism which is ubiquitous throughout the interactions of a participant with the platform. At any step of the interactions where any kind of information is send by the participant to the platform (e.g. sensor data), a specially designed interface informs the participant about this and asks for his/her explicit consent to perform the sending operation.
- *Sliced informed user consent*: We have implemented a sliced (granular) user consent mechanism whereby it is ensured that the crowdsourcing tool users are timely informed about the policies of the IoT Lab for privacy, anonymity and security when a given data processing is going to take place.
- *The right to be forgotten.* Even if their data are fully anonymized, the participants can at any time easily access their profile, modify it and delete it. The modification or deletion of profile is immediate, and is applied to any new data collection. Modification of deletion of profile is not impacting previously collected data as long as these data are deemed fully anonymized. As an additional protection and safeguard, a complementary mechanism enables the administrator to manually give access, modify and delete data sets according to the anonymized user ID.
- *Role-based access control*: an identity management scheme is implemented with a role-based authentication and authorisation policy. In this scheme, individual identifiers are assigned to all the types of users of the platform that are used for their authentication, authorization and management of privileges across the platform. The access rights differ from user to user, depending on the role of the user (administrator, researcher, participant, sponsor, charity, etc.).
- *Actively ensuring that collected data from the participants are effectively anonymized and cannot be linked to an individual*. This measure enables to treat the collected data as non-personal data from the start. However, in order to give full flexibility and generality to the platform, we have

developed complementary mechanisms that will enable the participants to delete their data on request (or automatically if they wished so).

- *Decreasing raw data granularity.* Raw data are not personal data per se; however, when combined with other pieces of information they may enable the data controller to infer some detailed information on users. Therefore, limiting raw data granularity when not necessary is a way to prevent potential unnecessary combination of the latter with other information relating to an individual.

11.9 Incentive Mechanisms and Model

While ensuring that end-user privacy is protected, as presented above, it is equally important to motivate and engage with the crowd not only to participate (initial use) but also to sustain its engagement at all times (continued use). Thus, keeping participants motivated and engaged across time, while accounting for their individual evolution within the system is of critical importance for the success of any crowd-driven ecosystem whose participatory value creation processes are driven by users (Ziouvelou et al., 2016). Existing research in the area indicates that enjoyment, career concerns, satisfying intellectual interest, increase of status, community support, feeling affiliated and creating social contacts are a few of the most important motives for crowdsourcing and crowdsensing systems (Brabham (2010), Kaufmann et al., (2011), Nov (2007)); which vary with the type of crowd-driven initiative.

The IoT Incentive Model

In the context of IoT Lab we have placed special emphasis on the motivation and engagement of the crowd-participants as well as on the rest of the ecosystem stakeholders via the design of an incentive mechanism that triggers motivation and engages user participation while accounting for the evolutional parameter of the user within the system.

Based on our analysis of a variety of different incentive models, the most appropriate model for IoT Lab has been found to be a "*hybrid gamified incentive model*" that combines two key types of incentives, namely: (i) intrinsic and (ii) extrinsic incentives, while it also includes innovative approaches that aim to enhance both the extrinsic, intrinsic and social motives such as the "*gamification approach*" (Figure 11.8). Such an amalgamation will not only motivate users' participation during their initial usage decision but also play

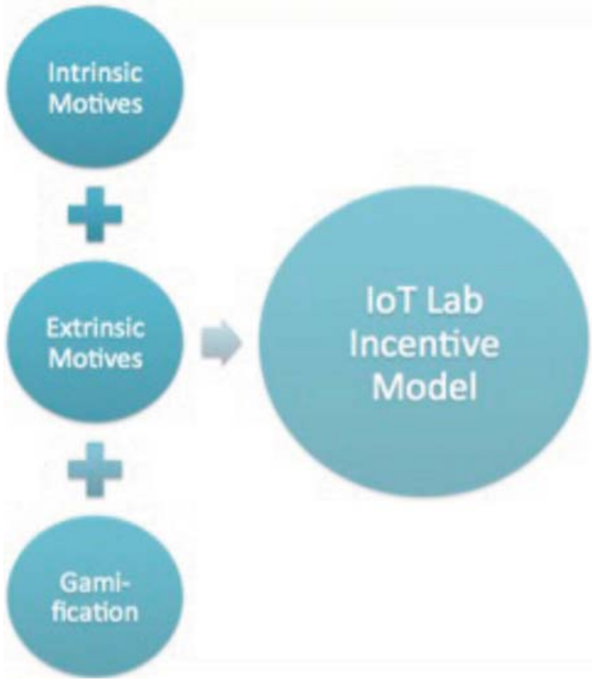


Figure 11.8 The IoT Lab Incentive Model.

a critical role during the subsequent user decisions facilitating a continued and engaged use of the IoT Lab system. In addition this model accounts for the dynamic evolution of the ecosystem as well as its users via the integration of a gamification practices that will act as an important incentivisation scheme that will enhance user experience and will sustain their on-going engagement.

Gamification by Design

The IoT Lab hybrid-gamified incentive model, integrates a number of key gamification [9] techniques such as points, badges and leaderboards (Morschheuser et al., 2016). A *point-based reward system* has been designed taking into account the specificities of the IoT Lab experimentation process for the crowd participants and the researchers, awarding points/credits for the different actions of the users inside the IoT Lab platform.

Having adopted a "*social good business model*" IoT Lab will allow its community members to allocate the points/credits collected by participating in the experiment to a charity of their choice, out of a list that will be provided by the platform. This approach is based on the assumption that a research sponsor provides a budget for an experiment, out of which a small amount of the budget ("social revenue distribution") will be used for the platform maintenance and the rest will be allocated to the users so that they can in turn re-allocate them to the charities proportionally to their point/credit distribution. This will enhance further the intrinsic motives of the crowd participants, as they will be contributing to a greater cause that goes beyond contributing to emerging research.

Furthermore users will also be able to earn badges for different activities (resulting in different levels), providing a sense of accomplishment for the different types of user-effort (simple/complex crowdsourcing and crowdsensing tasks) and signify user status and progress within the IoT Lab ecosystem. In addition, users will be able to track their performance over time and subjective to anonymous other users of the ecosystem via leaderboards.

Finally a novel incentivisation scheme has been designed for the purposes of the project. The ***"Reputation Scoring" (R-Score)*** (Figure 11.9) is a dynamic scoring mechanism that aims to enhance the user engagement within the platform while considering the user behaviour in a qualitative

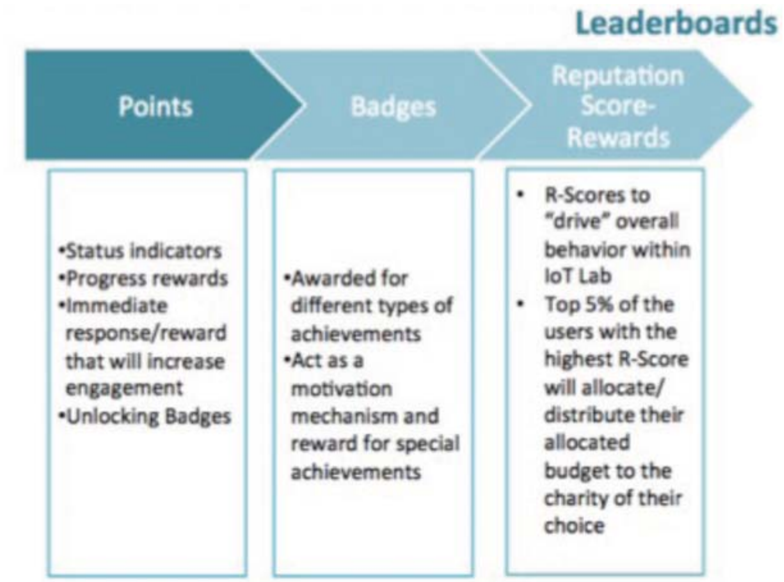

Leaderboards
Points
Badges
Reputation Score-Rewards
•Status indicators
•Progress rewards
•Immediate response/reward that will increase engagement
•Unlocking Badges
•Awarded for different types of achievements
•Act as a motivation mechanism and reward for special achievements
• R-Scores to "drive" overall behavior within IoT Lab
• Top 5% of the users with the highest R-Score will allocate/ distribute their allocated budget to the charity of their choice

Figure 11.9 IoT Lab Leaderboards.

and quantitative manner. The R-Score, accounts for the users' overall activity (crowd-driven research value-added) from different perspectives and associated KPIs namely: (a) *Incentive-based KPI* (i.e., account for points and badges gathered by the user, among others); (b) *Crowd-driven research KPI* (i.e., proportion of proposed ideas, rate of proposed ideas, evolution of ideas into experiment, among others) and (c) *Behaviour KPI* (i.e., usage history, experiment contribution score, market assessment contribution score, among others). As such the R-score facilitates a different rewarding that encourages users on-going contribution. The R-score based rewards will be provided to the top 5% of the users with the highest R-Score: (i) *Social rewards:* Top Contributor Reward & Badge and (ii) *"Good-cause" reward:* Distinct badge and ability to do select the charity of their choice to receive part of the IoT Lab donations that will be allocated to the user.

11.10 Examples of IoT Lab Based Researches

Energy Efficiency

An energy saving scenario is being run in the University of Patras. The end goals are to monitor the energy consumption, to automate the lighting and climate and to save energy. The scenario uses static and crowd lent IoT devices together with surveys, as a way to learn the crowd's opinion. The first step is to monitor the energy consumption. Then a group of crowd users using project code is created and a message is sent, informing them about the experiment and their role in it. The research requires passive light measurements from their sensors as well as opportunistic ones for their location within the building. These values determine whether or not the lights and air-condition will be turned on or off. Follow up questionnaires determine the user's satisfaction and the need to read just the parameters of the experiment. Key challenges are the need to engage the crowd with a strong suit of incentives and to optimize the environmental parameters (i.e., light and cooling) of the space while trying to maximise energy saving.

Smart HEPIA

A smart building testbed infrastructure has been deployed in the HEPIA building of Geneva, a branch of the University on Applied Sciences Western Switzerland. The testbed enables to monitor and interact with two floors of the building. It includes temperature, light, humidity and presence monitoring, energy metering, as well as actuation on heaters, blinds and lighting system.

The testbed has been integrated to the IoT Lab platform and is used with a dual purpose: to support education of ICT engineers and to support research activities.

The Smart HEPIA deployment is used to research new solutions for improving energy efficiency of the building. Students are using the IoT Lab testbed as a service to experiment and measure the impact of various algorithmic solutions. The project is closely followed by the local authorities, which have designed the building as a reference one for future energy optimization strategies in all publicly owned constructions.

Brewery

In cooperation with the Brewery of Heineken Group at the industrial area of Patras (Greece), a use-case scenario that uses the IoT Lab platform runs at the department of New Cellars of the factory (Figure 11.10). The end goal of this use-case is to show the ability of the IoT Lab platform to serve as a useful tool for the industrial community to implement IoT technologies in their Factories and use their equipment as a service. Via this use-case it is able to achieve energy saving in satisfactory levels for the energy managers of the factory

Figure 11.10 Heineken factory in Patras, Greece.

and at the same time to provide the optimal conditions for the employees, the production and the equipment.

In this application, there are sensors to monitor the ambient conditions in this department (light level, temperature and humidity) in accordance with the use of it by the employees by taking in account the human presence (PIR sensors). Also actuators are connected to the electrical panel of the lighting system which can control the lights of this department. Moreover, the energy consumption from the lighting system of this department is measured from energy meters that are connected to the IoT Lab platform and their measurements are provided to the platform as resources.

All these sensors and actuators are provided as resources over the IoT Lab platform to the key operator of the department. Then the energy manager of this department, composes via the IoT Lab platform the appropriate scenario for the lighting system to be adapted automatically and provide the light level that is needed at any time with no energy wastage.

Also depending on the readings from the sensors, the energy meters and the actuators, it is possible for the platform to send a notification to the key operator as an alarm (in case of conditions out of limits) or a report (with aggregated data).

The key challenges of this use case are

- to develop the wireless sensor network in an industrial environment with many restrictions because of the hard nature of this environment
- to assure that the platform is robust enough to guarantee stable operation of the system to provide safety, good quality of service and ease of use for the employees
- to achieve a good level of energy saving that makes the use of Iot Lab platform a sustainable solution in real applications for energy saving.

EkoNet Novi Sad

Measurement of the air quality represents an important aspect of quality of life in the cities, as well as for running responsible operations in different industries.

ekoNET portable testbeds [10] composed of low cost sensor based monitoring devices (EB800/RPi800) enable a real time monitoring of the air quality (gas and particle sensors, sensors for air pressure, humidity, temperature and noise measurements) in urban and rural areas and they can be deployed either indoor or outdoor. Advantages include high mobility and portability, easy installation, cheaper sensor technologies and a better utilisation of data.

Each device includes a GPS module for location and GPRS mobile network interface for data transfer.

The ekoNET solution with portable testbeds is integrated within the IoT Lab platform providing a description of all resources to IoT Lab database and enabling the access to measurements from EkoNET sensors via web service. ekoNET devices are deployed at several locations in Serbia including Novi Sad city buses (MobiWallet Serbian Pilot [11]), several schools in Belgrade (CitiSense project [12]), and an open pit mine in Serbia as well as at test sites in Australia and Canada.

The IoT Lab platform with an integrated ekoNET solution represents a valuable tool for setting up and deploying the use cases to address the air pollution in smart cities enabling collection of the people's perspectives and subjective feeling about the air quality as well as allowing the crowdsourcing of opinions to tackle the problem and propose solutions for reduction of air pollution.

The use case, set outdoor, in the city of Novi Sad, combines geo-localised environmental data collected by the bus mounted ekoNET devices with geo-localised inputs from the crowd on perception of the air quality and their happiness level collected through a simple survey all via IoT Lab platform. It explores the correlation between the crowd happiness level and environmental conditions taking also into account the crowd socio-economic profile. Results obtained through this use case will benefit the local administration to reduce the air pollution in the city. As part of incentive scheme each completed survey will contribute towards a small donation to local charity thus making a step forward towards the happier city.

Similar use case is planned for schools to explore relation between air quality in schools and satisfaction, performance and behavior of pupils.

11.11 Conclusions

IoT Lab has been successful in developing, testing an using a new experimental infrastructure combining IoT and crowdsourcing. It is supporting a triple paradigm shift:

Extending IoT Research to End-users

Traditional IoT-related experiments are usually focused on the technical features and dimensions of IoT deployment. However, due to its ubiquitous and pervasive dimension, the IoT will require more and more end-user perspective to be taken into account. IoT Lab enables researchers to extend their experiments to this fundamental dimension: how are solutions accepted by end-users, where and what value they perceive in a given deployment, etc.

Enabling More Pervasive Experiments

IoT Lab enables the researchers to perform experiments in all sorts of environments, including among others smart buildings and smart cities. A set of initial experiment has started to assess the potential of IoT and crowdsourcing to assess the level of smartness and sustainability of any city. This work is a direct contribution to the ITU Focus Group on Smart Sustainable Cities [23]. In other words, IoT Lab enables research to leak outside of traditional labs by exploring IoT deployments in real environment with real end-users providing real time feedbacks.

Crowd-driven Research Model

Finally, IoT Lab is enabling and testing a new model of crowd-driven experiments. The key concept is to enable anonymous participants (the crowd) to suggest research topics and to rank them. According to the results, the favorite ideas will be proposed to researchers for selecting and implementing some of them. The results are expected to be shared with the participants (the crowd) in order to get their inputs and their assessment of the generated results. The idea is to explore the potential of a bottom-up research model on the IoT based on crowdsourcing and closer interactions between the researchers and potential end-users as illustrated in Figure 11.11.

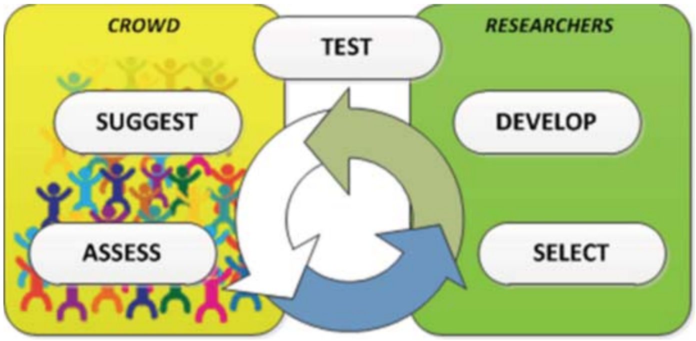


Figure 11.11 Crowd-driven Research Model enabling anonymous end-users to trigger and drive experimentation process in cooperation with researchers.

A non-for-profit association has been established to jointly maintain the IoT Lab platform and make it available to the research community. The platform is also supporting new research projects, such as F-Interop, which is developing online testing tools for the IoT.

References

[1] IoT Lab is a European research project from the FP7 research programme: http://www.iotlab.eu

[2] Internet-of-Things Architecture, http://www.iot-a.eu

[3] IoT Lab deliverables D1.2, D1.3 and D1.4 on IoT Lab architecture and component specification, and Jokic, S. et al., (2015), IoT Lab Crowdsourced Experimental Platform Architecture, 5th International Conference on Information Society and Technology (ICIST)

[4] Panagiotis Alexandrou et al., (2016), A Service Based Architecture for Multidisciplinary IoT Experiments with Crowdsourced Resources, Adhoc, Mobile, and Wireless Networks, Volume 9724 of the series Lecture Notes in Computer Science pp. 187–201.

[5] IoT6 European research project, http://www.iot6.eu

[6] S. Ziegler, M. Hazan, H. Xiaohong, L. Ladid, "IPv6-based test beds integration across Europe and China", in Testbeds and Research Infrastructure: Development of Networks and Communities, Springer, and Trident Conference 2014 proceedings.

[7] UDG is an IPv6-based multi-protocol control and monitoring system using IPv6 as a common identifier for devices using legacy protocols. It was developed by a Swiss research project and used by IoT6 for research purpose. More information on UDG ongoing developments at: www.devicegateway.com

[8] K. Holm, "Using MQTT Protocol Advantages Over HTTP in Mobile Application Development," IBM, 18 10 2012. [Online]. Available: https://www.ibm.com/developerworks/community/blogs/sowhatfordevs/entry/using_mqtt_protocol_advantages_over_http_in_mobile_application_development5?lang=en. [Accessed 02 2016].

[9] Gamification is defined as the use of game elements in non-gaming systems so as to improve the user experience and user engagement, loyalty and fun (Deterding, Khaled, Nacke, and Dixon, 2011).

[10] eKonet bus project, http://ekonet.solutions/

[11] Mobiwalet project, http://www.mobiwallet-project.eu/

[12] Citi Sense project, http://co.citi-sense.eu/