Hindawi
Mobile Information Systems
Volume 2017, Article ID 2164072, 14 pages
https://doi.org/10.1155/2017/2164072

Research Article

Design and Implementation of a Cloud-Based Platform for Unleashing the Personal and Communal Internet of Things

Ignacio Elicegui,[1] Carmen López,[1] Luis Sánchez,[1] Jorge Lanza,[1] Luis Muñoz,[1] Antonio Pintus,[2] Andrea Manchinu,[2] and Alberto Serra[2]

[1] *Universidad de Cantabria, Edificio de Ingeniería de Telecomunicación, Plaza de la Ciencia s/n, 39005 Santander, Spain*
[2] *CRS4, Science and Technology Park, Building 1, Loc. Piscina Manna, Pula, Sardinia, 09010 Cagliari, Italy*

Correspondence should be addressed to Luis Sánchez; lsanchez@tlmat.unican.es

Received 18 November 2016; Revised 10 April 2017; Accepted 19 April 2017; Published 15 June 2017

Academic Editor: Maria Bermudez-Edo

Internet of Things (IoT) concept has attracted a lot of attention in recent years and it is foreseen as one of the technologies that will leverage the Future Internet. It is seen as a major enabler of novel applications and services that will foster efficiency and will ease every day's life. However, current IoT solutions are mainly focusing on the development of centralized solutions that do not promote the democratization of the IoT but rather concentrate the IoT around a set of cloud-based platforms which pretend to be open but limit the capacity of the people to tailor their Personal and Communal IoT. This paper describes a software platform based on available generic enablers as defined by the FIWARE initiative. It extends the existing architecture models to accommodate the requirements stemming from the vision of people-sourced IoT devices which are shared to create applications and services in smart communities where the owners of the shared devices are always empowered to control who, and in which circumstances, has access to the shared information.

1. Introduction

Nowadays, Internet of Things (IoT) makes available a large variety of assets (e.g., data, devices, and services) that are used in a number of ways that were once unthinkable. Similarly, foreseeing the future use of IoT assets is difficult if not impossible. The rapidly increasing number of intelligent, cloud connected things that are embedded in our daily lives raises legitimate concerns about the privacy costs paid for the benefits these technologies provide. In this context, keeping the ownership and control of IoT assets is a crucial objective to foster the creation of new services and encourage users' trust and participation. This is particularly true when personal assets, namely, assets that are related to a person, are considered.

Before the IoT concept was developed, closed and centralized Intranet-of-Things were used to manage closed domains of IoT assets (grid monitoring, logistics tracking, etc.). This approach allowed service providers to guarantee a satisfactory Quality of Service (QoS), without need to properly address provenance of IoT assets and their associated value. This is indeed more urgent and important now that IoT is becoming an open market where services are offered beyond the boundaries of a closed organization. More recently, open access IoT networks have been delivered and vertically integrated into the cloud. However, despite the open access, such IoT networks still employ centralized cloud infrastructures, and consequently the full control of assets is still in the hands of trusted third parties. This is adequate when IoT infrastructures are owned by a single entity (e.g., city council owns the smart city IoT infrastructure or utility owns its IoT grid) but, as it happened with Internet, exponential growth of its value only came when everybody's devices were interworked. Centralized infrastructures undermine the IoT assets' owners' willingness in sharing even more of their assets as they are no longer able to control how these assets' services are offered and to whom they are exposed.

This paper presents the novel concept of personal and communal Internet of Things and describes a platform that

has been implemented in order to realize such a concept and that empowers people to handle and share the services exposing their IoT assets. Thus, the two contributions described in this paper are as follows:

(i) The identification of a novel paradigm meant to foster the uptake of the IoT in the creation of intelligent ambiences to which individuals and groups contribute while keeping full control of their devices is discussed; moreover, the discussion of the technical problems that such a novel paradigm implies has also been detailed.

(ii) The actual development and integration of the platform that enables the actual realization of this concept is the second key contribution described in the paper. This platform has been implemented using several FIWARE enablers [1] as well as additional components that correspondingly fulfill the design considerations associated with the Personal and Communal IoT paradigm. The main reason for using FIWARE enablers as the baseline for the platform implementation is to promote the uptake of this solution at a larger scale as it will be based on well-known and standardized open technologies.

It is important to note that despite the fact that nowadays there are several IoT platforms available that might seem suitable to host the Personal and Communal IoT concept just by adding the proper roles and sharing capacities to the applications and assets involved in the communal scenario, this is not the case as they fail in properly addressing some of the key requirements identified in the next section.

The remaining part of the paper is structured as follows. Next section will describe the Personal and Communal IoT concept that we consider is a key constituent on the successful uptake of the IoT grand vision. This paradigm motivates the platform we have implemented to manage the context information that is generated by people's IoT assets/devices, to allow the creation and management of communities where these IoT devices will be securely shared, and finally to simplify all this process and facilitate the interfaces to easily create value-added services with this context information. Related Work section will present a nonextensive review of existing IoT platforms both from commercial and research-oriented flavor. This review will focus on the key features considered by these platforms and will let us show how personal and community needs are not well covered by them. The core of the paper is the functional description of the Personal IoT Management platform and its building blocks. Finally, conclusions focus on highlighting the main contributions and outlining how future work will foster the uptake of a truly open and humanized IoT.

2. Personal and Communal IoT: Empowering People to Manage Their IoT

2.1. Need for Facilitating Sharing Personal Data. The volume of data is doubling every two years, of which two-thirds is created by individuals, in particular with adoption of new wearable devices [2]. This growth has been driven both by the increase in number of connected devices in our lives and their growing capabilities. This trend looks set to continue with data traffic from IoT devices rising from 2% share of the total in 2013 to 17% in 2020. However, very little attention has been put on facilitating those individuals to participate in the plethora of services that this incredible amount of data can leverage. In this sense, IoT research and development [3, 4] has focused on technology considerations and most notably has concentrated on large scale platforms gathering services and information from devices in the environment, but not on the human beings that own these devices and would like to exploit the value of these services and data. Thus, individuals do not believe they benefit from sharing personal data with organizations offering such platforms. Instead they believe it is only the organizations that are gaining from their data.

A recent work [5] remarked about the urgency for the IoT to go beyond the Machine-to-Machine paradigm to include people in its foundation. In that paper, authors project the Fiskes's Four Elementary Forms of sociality [6] to IoT, in order to define a Humanized Internet of Things (H-IoT); from the aims of this work considering the Communal Sharing and Equality Matching patterns (reported in Figure 1) is interesting in particular as people in a community collaborate to fulfill a shared goal, smart managing their IoT and related connected devices.

An IoT including personal and communal features and needs implies that not only must smart devices be controllable by the owner, but they can be also shareable by and with everyone in a given community. Thus, in the Communal Sharing pattern, building a community of trusted people represents a central point. Inside a community, there is the creator, which can be intended as the administrator of it, in the sense that they can accept new members or close or delete the community, but inside the community the hierarchy is flat and every member is equally entitled to manage shared devices. Examining the Equality Matching pattern, the idea is that every person in the Communal IoT contributes in a balanced manner to reach common goals.

In summary, the Personal and Communal IoT paradigms that we are proposing imply a future in which the ownership and control of IoT assets will be guaranteed during the whole lifecycle of the IoT asset. The objective is to increase the transparency of all the IoT asset management flow, removing the need of a centralized trusted party and shifting from the actual paradigm of discrete centralized trusted authorities to a paradigm of decentralized trust of the network as a whole. IoT Traders (individuals, communities, or corporations sharing IoT assets) will not only be capable of sharing their assets but also be able to track and manage how and by whom they are used, while gaining direct advantage from such sharing.

2.2. Key Enabling Functional Considerations. Accomplishing the above vision implies three key enabling functionalities, namely, information management, community management, and Personal and Communal IoT dashboard. These features comprise the key technical challenges that the proposed and implemented platform is addressing.

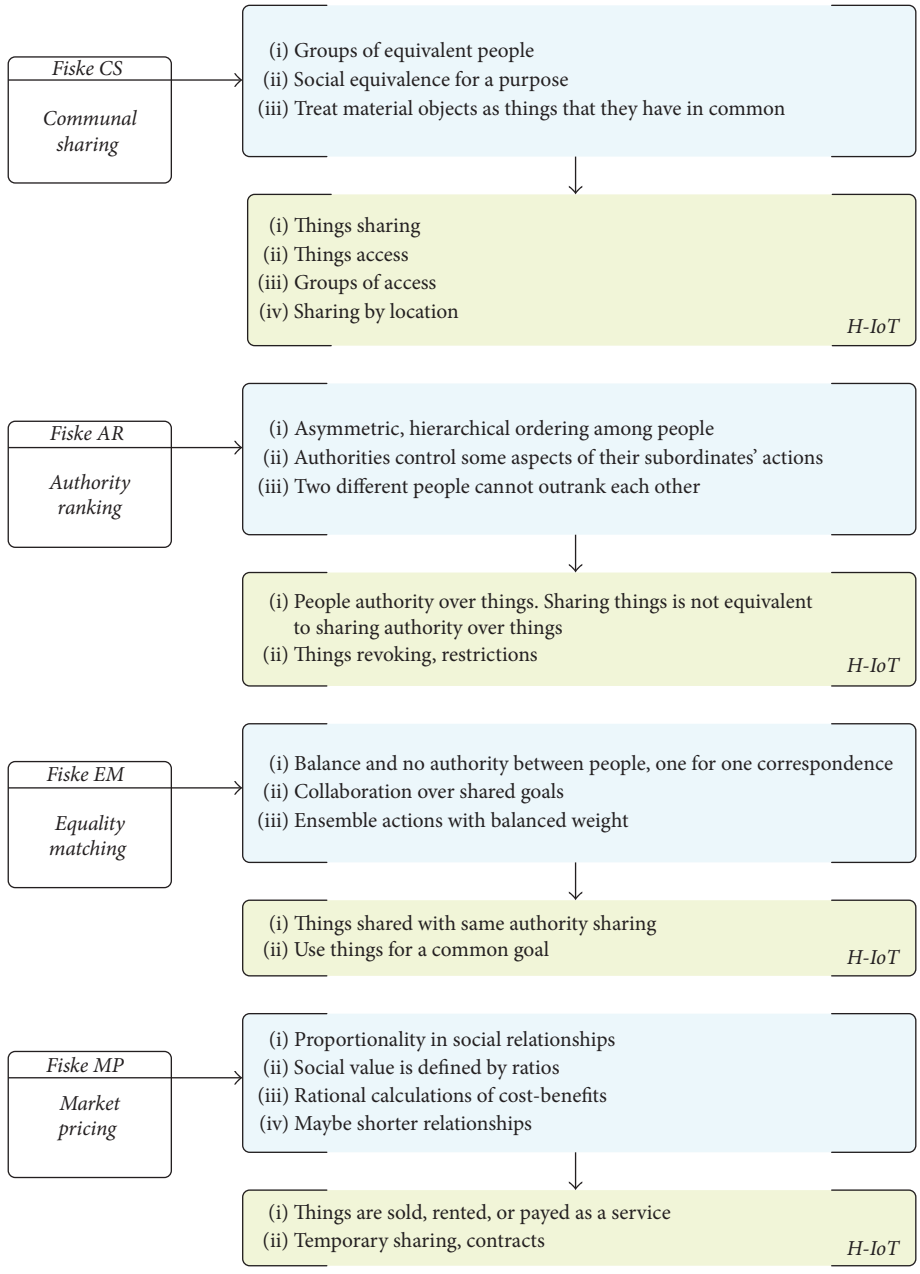


Figure 1: Fiske's Elementary Forms of sociality projected to IoT, building a humanized, people-centric IoT.

2.2.1. Information Management. The IoT vision in general and the personal IoT one in particular are characterized by the large amount of devices that surrounds us and that can provide added-value services if properly managed. Data sharing mechanisms should be implemented to guarantee that datasets and data-streams can be used in services to its best. Nowadays it remains possible to combine multiple streams into one application if the endpoint to the necessary sources of information is known, but this creates additional burden for developers. The most important of these services is the access to the information that these devices gather. It is thus, critical to first establish a way of modelling this information in such a way that it is possible to homogeneously represent something that inherently shows a large degree of heterogeneity. It is important to note that this information model has to be valid for the devices as well as for the observations that they produce. Secondly, the information has to be efficiently stored and, most importantly, efficiently discovered and retrieved.

2.2.2. Community Management. Managing your own personal devices and information is just the first step. While the amount of services available through the exploitation of personal information is considerable, the real value comes from linking each personal IoT into communities. Data and knowledge behind data are the core of the wealth produced

by the IoT. In order to make Communal IoT real it should be possible to establish an architecture for data governance, based as much as possible on open platforms, capable of supporting decentralized data and Identity Management and bottom-up participatory innovation. Community management implies the definition of access policies and the establishment of a framework in which identities can be validated. These features have to be in place in order to enable access, to third parties, to the services offered by the personal IoT.

2.2.3. Personal and Communal IoT Dashboard. In spite of recent uproar around high-profile data breaches, with the likes of Sony Pictures or Ashley Madison all falling victim, consumers view themselves as increasingly responsible for their own education on how to protect and control their personal information. The large and sensitive data that might be generated by personal devices in the IoT mandates the data management to be at the core of IoT paradigm, and it amplifies the need to maintain a certain degree of privacy and security [7]. The IoT asset owner is meant to be in control over the data, as well as over who has the access rights to it. Thus, it is critical to offer to the individuals a friendly environment that enables them to manage their devices and communities in the easiest and most straightforward way. In this sense, not only should this dashboard be limited to monitoring purposes, but it should also allow the creation of value-added services consuming the information that Personal and Communal IoT devices generate.

2.2.4. Technical Challenges Outline. Taking into account these key functionalities, the platform that has been implemented in order to realize the concept of Personal and Communal IoT, thus narrowing the gap with the vision described in Section 2.1, has addressed the following challenges:

(i) Development of the components and data models allowing multiple heterogeneous and multimodal IoT sources work in synchrony and securely aggregate data.

(ii) Implementation of the modules in charge of the management of the policies for data sharing and the enforcement of corresponding access rights defined in that policies.

(iii) Definition of a distributed platform that can be composed of multiple instances of itself thus guaranteeing real data ownership while enabling community building through federation of individual instances; moreover, open access to platform instance images has been granted.

(iv) Facilitation of the platform usage for the three key involved stakeholders: (1) device manufacturers to use open and standardized interfaces for data provision; (2) application developers to access IoT data through unique service-oriented interfaces and using common information models; and (3) end-users to have simple tools to manage their IoT assets and the data that they generate.

3. Related Work

The existence of such a large amount of smart devices, applications, sensors, and so forth in our daily lives has created the necessity of platforms that are able to embrace all actors involved within this heterogeneity, from relaying technologies to final users, including also the management of all different relations among them (device-to-device, person-to-device, person-to-person, etc.). In [8, 9] different authors presented this necessity and summarized the main challenges to be overcome. In addition, they provided a possible approach to be followed and the key enabling technologies to achieve a people-centric society based on the IoT.

One of the main concepts that is currently thought to provide coherence in the IoT scenario is the Web of Things (WoT) one [10]. However, the WoT solution has to overcome the modelling of the Things in order to address the problem of publicizing, discovering and accessing the objects and the services that they expose.

Another, especially important, aspect is the cross-platform development problem [11, 12]. In order to foster an expedited development of applications, the IoT platforms are expected to provide the developers with streamlined application programming interfaces (APIs) to their functionality, preferably with the help of higher abstraction level primitives. The platform implemented provides these APIs and also builds on top of standardized information models which are meant to enable the necessary interoperability that is demanded by application developers.

In order to cover the aforementioned demand, different solutions have been developed. IoT-A [13] and FIWARE [1] appeared as leading reference architectures to encourage a faster development of new IoT solutions. The former, IoT-A, aiming to lower the barriers of interoperability and to converge upon the existence of a plethora of different models of IoT governance, proposes a global solution targeting not only the interoperability but also scalability, security, and privacy in its design. This solution relies on an architecture reference model and provides an initial set of building blocks, principles, and guidelines in order to enable the design of new protocols, interfaces, and functionalities for IoT environments. Furthermore, FIWARE, as one of the leading architectures in Europe, proposes an innovative, open, cloud-based infrastructure for cost-effective creation and delivery of Future Internet applications and services. Other service-oriented frameworks have been recently proposed [14] to enable the creation of new services and to make the management of the various data sources easier and more effective. These platforms include features like trustworthiness and provenance but fail to empower the data provider; in many cases data comes from personal devices like smartphones, to have a real control on when and who can access the data.

Additionally, to achieve a tighter approach of the IoT to potential users, different IoT platforms, which work as Platforms as a Service (PaaS) for IoT, such as Carriots (https://www.carriots.com/), ThingSpeak (https://thingspeak.com/), Xively [15], or IFTTT [16], have appeared. For more comprehensive discussions on available IoT platforms, we

invite the interested readers to refer to [12]. However, let us examine two of them, representing the state of the art of cloud-based and well-known platforms: IFTTT and Xively. The former, IFTTT (If This Then That), is a web platform that allows users to automatize tasks on the Internet. It allows connecting to services/devices adopting a "WHEN event 'e' THEN DO action 'a'" (called recipes). Its main advantages are easiness of use, recipe sharing between users, and a large set of available services/devices. Despite the recipe-sharing feature, in IFTTT, it is not possible to really share things, so a Communal IoT is not applicable. Regarding Xively, it provides a platform and a set of services to create and manage connected products and services on the IoT. It offers a developer-oriented workspace, with a strong business to business approach and related market. However, community concept is not provided and devices sharing could be performed only through APIs and developers belonging to the same organization/company.

Regarding the person-to-device relations, different studies have been done related to the critical field of the Personal Networks such as [17]. Among them, the MAGNET project [18] can be highlighted. Starting on the basis that Personal Networks were secure, self-organizing and user-centric networks which provide ubiquitous access to personal devices, the project undertook the challenge of developing short-range user-centered wireless networks and the establishment of trust relationships between them so that communal networks could be created. Other approaches, closer to the Personal and Communal IoT concept that we are proposing, can be found in [19, 20]. They coincide with the paradigms that we are proposing in the fact that while IoT is associated with a vision of everything being connected to everything, for meaningful applications to be developed, what really matters is how qualitative relations and more selective connections can be established between smart objects, and how their owners can keep control over object relations. However, while, in [19], they focus on geographical proximity for selective artefact communication, using the context of artefacts for matchmaking, in [20], authors describe a framework that enables smart things to form social groups autonomously, for the benefit of human beings but without their intervention. This latter approach is closer to our vision and to the objectives of the platform that we have implemented.

As it has been described through the aforementioned examples, IoT platforms still miss the strong personal and communal aspects that Internet of Things needs to flourish. As a consequence, this work presents the development of an Internet of Things platform, built on top of existing IoT enablers, but addressing the functional considerations presented in the previous section to foster personal centricity. It focuses on allowing final users to easily manage their devices, plus the provided information, and share them with other users based on established relationships.

4. Personal IoT Management Platform

The IoT platform here described represents a step beyond towards user engagement in IoT development and deployment, since it focuses its main features on overcoming the difficulties which citizens (as users with very basic technical knowledge) face when introduced to these technologies and on creating secure groups where these users can take control of the information they are managing. In essence, the proposed IoT platform builds the bridge to allow new nondeveloper users to be able to initiate into the IoT environment smoothly and confidently.

In order to keep it easy to use, this implementation takes the core functionalities of current IoT platforms related to data gathering/accessing and extends them with the "communities" concept, reinforcing all the security aspects regarding privacy and trust. As a result, a modular, open, and decentralized architecture has been developed, based on existing components from FIWARE IoT platform but supporting the Personal and Communal IoT paradigm. This decentralized design of the platform allows a powerful scalability granting the use at different levels: from a private perspective where a user wants to deploy their own instance for personal use, to big communities like cities that want to provide IoT services to its inhabitants in a secure manner.

The simplest instance of this architecture, and its backbone, includes three main enablers: the Context Manager, which stores all information sources and provides the tools to query/retrieve context data; the Communities Manager, that allows users to create their own groups for information sharing and link them with the information sources registered within the Context Manager; and, on top of these, the User Environment, which provides the user with an intuitive front end to quickly create and manage their IoT environment and share their data with other platform users. The platform allows citizens to easily register and share their IoT devices through the platform users' tools or developers create their own advanced/specific IoT applications using the different APIs supported directly by the enablers.

A key factor in this architecture is the already mentioned *"Context Entity."* This element describes how an entity, which may be a device, a smartphone, any information source, or even a human being, will be defined within the platform and how its associated data, what is called *"Context Information"* or just *"Context,"* will be linked and stored. The OMA Context Information Model [21] is used here to homogeneously create and describe entities, including all associated information they will share within the platform. The simplicity and versatility of this data model structure allow the user to map an infinite range of devices, sensors, actuators, and information sources, by providing just a user-created *entity ID* and a set of user-defined *attributes* that describe its capabilities and contain the information. As an example (Box 1), a weather station entity can be registered in the platform with *"platformInstance01:sensor:weatherStation:device01"* as id (which includes extra information about the instance it belongs to and the type of device it is) and *"AirTemperature"* and *"RelativeHumidity"* as attributes. Each attribute will include also the updated corresponding values (24°C and 73%) and, if required, a set of associated *metadata* that complements the provided data with extra information like date and time of when it was captured, location, unit of measurement, special characteristics, and so forth. The type of supported attributes

```
{
  "contextElements": [
    {
      "id": "platformInstance01:sensor:weatherStation:device01",
      "type": "weatherStation",
      "isPattern": "false",
      "attributes": [
        {
          "name": "AirTemperature",
          "value": "24",
          "type": "http://purl.org/iot/vocab/m3-lite#AirTemperature",
          "metadatas": [
            {
            "name": "uom",
            "value": "Celsius",
            "type": "http://purl.org/iot/vocab/m3-lite#DegreeCelsius"
            }
          ]
        },
        {
          "name": "RelativeHumidity",
          "value": "73",
          "type": "http://purl.org/iot/vocab/m3-lite#RelativeHumidity",
          "metadatas": [
            {
            "name": "uom",
            "value": "Percent",
            "type": "http://purl.org/iot/vocab/m3-lite#Percent"
            }
          ]
        }
      ]
    }
  ]
}
```

Box 1: Example of an entity data model structure.

and their metadata structure have no special limitation, what gives this model its flexibility.

In addition to the mentioned platform backbone, other functional components have been developed in the context of the 7th Framework Programme of the European Community SocIoTal project to be directly plugged. These components provide extra capabilities to the whole platform related to security access to resources, users' identification, and authentication and trust management. Other set of enablers helps in capturing special context information, such as face-to-face position or indoor location, which enriches the initially provided entity's information and assists in granting access to context information. On the other side, FIWARE components, like Big Data enablers, connectors, or special gateways to upload context, can be also easily linked to this platform, extending even more the IoT provided capabilities.

Following, the main components of the implemented platform will be described which covers the key enabling functional considerations mentioned in Section 2.2.

4.1. Context Manager. The Context Manager is the core of the presented IoT platform. Its set of functionalities can be divided into three related but differentiated main blocks: on one side, it acts as the resource directory of the platform, keeping a complete list and corresponding descriptions of all context entities registered and managed by the users; second, it stores and retrieves the context information uploaded by these context entities, and, finally, it supports the different links with the rest of platform enablers and components, which gives the Context Manager its integrator role. To provide these functionalities to the final user, this component exposes a complete RESTful API [22] compliant with the OMA NGSI-9 and NGSI-10 recommendations. The Context Manager implements a set of NGSI-9 methods to register, modify, and discover context entities and a collection of NGSI-10 compliant methods related to the resource directory management to update, query, and retrieve context information and to manage subscriptions to information sources and data types. In addition to standard OMA NGSI interfaces

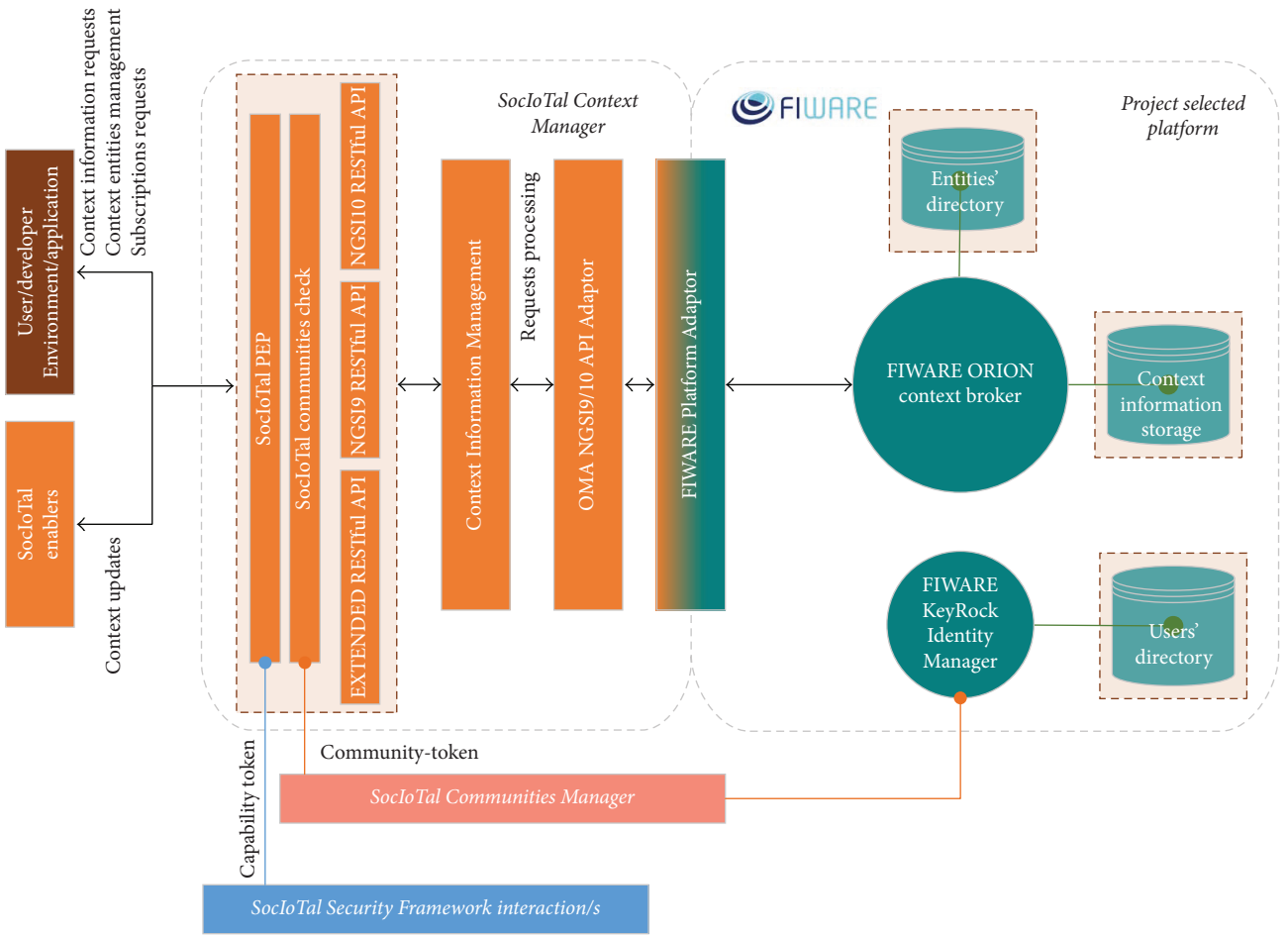


Figure 2: The Context Manager architecture.

the Context Manager implements some extended methods to provide the user with shortcuts and preformatted requests that make it easier to retrieve specific data or execute concrete operations. With the first deployed version of the Context Manager, these extended methods are restricted to assist in creating/deleting context entities and retrieving all context information shared by a given entity, but this set will be, in turn, extended to cover those required functionalities, captured through the enabled support channels, as the platform expands and the final users' groups grow up.

The Context Manager here described was built on top of FIWARE architecture (Figure 2), enriching its context data management features and complementing its Data/Context management enabler, the Orion Context Broker [1], with communities' support in order to allow final users to easily organize, protect, and manage their information sources while they share data among identified users with similar interests. This platform component has been designed to be centralized, deployed in the cloud, if the instance is oriented to be open, for example, for citizens to develop and share their own applications and data, or in an intranet server, if the platform is set up for private developments such as domestics' solutions or proprietary applications. Whatever is the configuration instantiated, this component will support all entities registered and provide the tools to manage all the information shared within the platform.

4.2. Community Manager. One of the most important barriers in the Internet of Things user's acceptance is data privacy. When users want to share information about them, their devices, or their environment, they will only share it with people, devices, and networks they completely trust, always being sure that no one without the corresponding permission will access that information. This requirement comes to greater importance when the type of data refers to very sensitive information due to privacy or security issues such as IoT patient monitoring (e.g., blood pressure data) or surveillance systems (e.g., home security cameras). There exist some platforms in the market that allow one of the two extremes: the management of their devices without sharing the information with other users or sharing all the information with all the users of the platform without any kind of discrimination. In order to fill the gap and provide users with a tool which gives them the overall control of data, the Communities Manager tool was developed and implemented. Through it, users will be properly identified

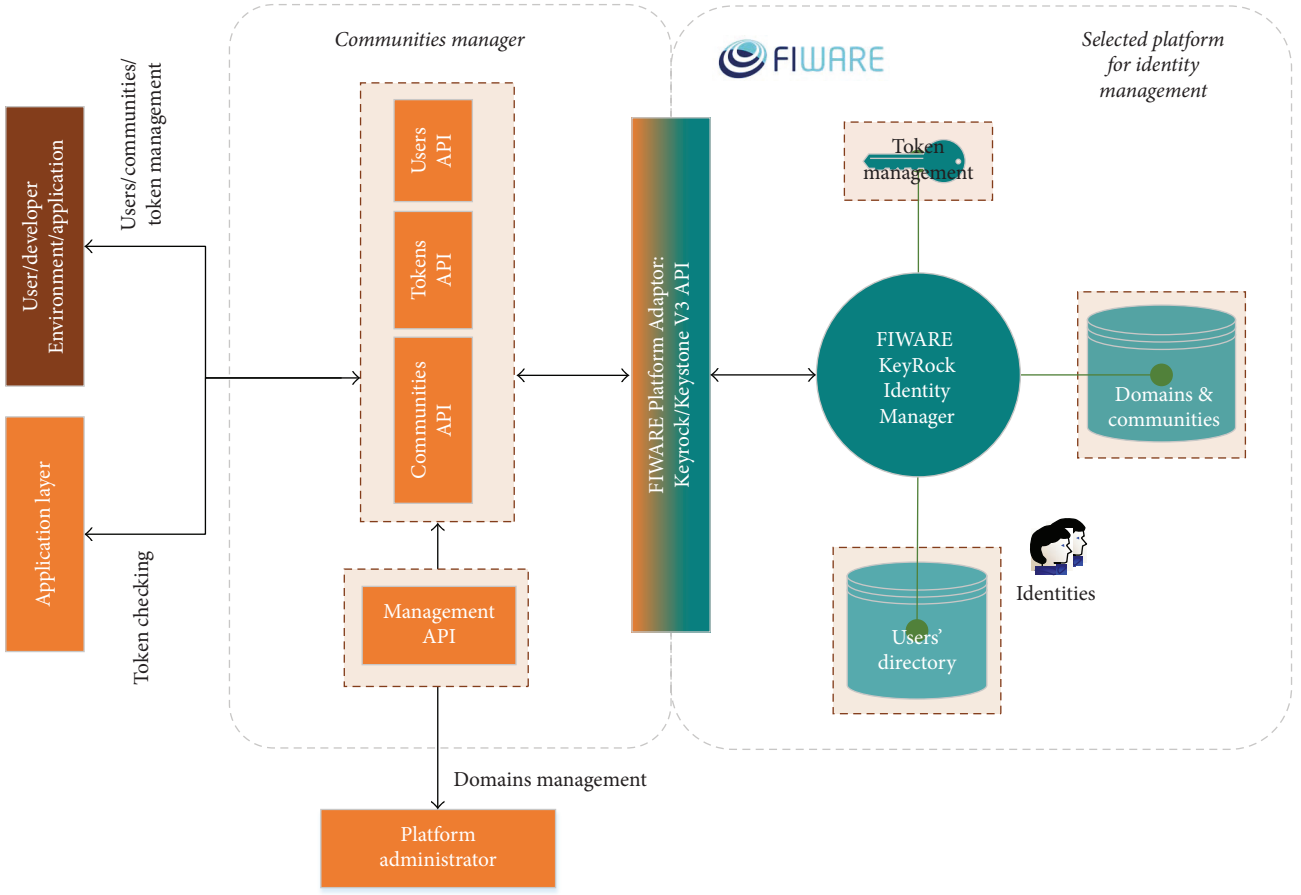


Figure 3: Communities manager tool and its relation with the Identity Manager platform and the application layer.

and authenticated and will be able, from that point, to specify both the relation between them and their smart objects and the relation of other users with that resources.

The Communities Manager tool provides an API [23] which allows users to first register themselves into the platform in order to, then, be able to create communities and register their devices within them. The creators of those communities will decide whether or not to approve other users within their communities. In case they give their approval, the owner will be able to provide the new members with a role to be played in the community, therefore specifying the actions they are allowed to perform over the entities (read or/and write actions). All this information related to the user and their relation with certain communities and their resources is defined by a community-token. This token is an alphanumeric key which relates the user with the community to which they have access and with the role they have within it, thus protecting the access to the information provided by the users from information leakage. In addition, although out of the Communities Manager tool functionalities, encryption and decryption information techniques are employed within the platform to secure data from the devices to the Context Manager.

The integration of this tool with the Context Manager previously defined derives from the use of the aforementioned community-token, since the management of the different resources allowed by the Context Manager will be determined by the relation of the user with the resource to be handled, which is perfectly defined by the community-token. In practice, when a user wants to access a resource in the Context Manager, they must attach the corresponding community-token to the API request which will validate if the user belongs to a community where that resource is registered and if they have the rights to perform the requested action (query, update, delete, etc.)

Figure 3 shows a diagram with the main components which structure the implemented Communities Manager tool, presenting also the relations with the application layer and the components where the Identity Management responsibility falls, in this case the FIWARE KeyRock Identity Manager (IdM) [24]. From a developer point of view, Communities Manager provides a HTTP/HTTPS RESTful API divided into three main sets of methods: users' API, which groups the functionalities related to the users' creation and management; communities' API which provides methods to create (and manage) communities and assign users and roles; and community-Token's API that allows community-tokens operations and validation. In addition to this, and focused on both developers and ordinary users, the communities' tool is totally integrated within the web User Environment tool

which will be presented in the following section. From this friendly environment, users will be able to easily create and manage their resources and communities.

4.3. User Environment. Considering Fiske's Elementary Forms of sociality projected to IoT [6], reported in Figure 1, we can envision a community of persons in which one member wants to share a weather station to the others. For example, in a community of neighbours, a person can use data gathered from this device and decide whether or not to irrigate the garden manually or automatically with another IoT application based on the provided platform API. In this case of Communal IoT, people in the same community contribute in a balanced way to fulfilling a common goal (e.g., a social gardening application), going beyond the concept of a strict, personal IoT.

In our IoT platform, the User Environment offers these features with easy-to-use and end-users targeted tools going beyond the concept of typical centralized cloud-based IoT platform examined in the state of the art. Thus the community and "humanized" aspect of the project represent an innovative approach in the IoT field, emphasizing the collaboration of sharing own devices.

This tool is a web-based, responsive, and user-friendly workspace to manage connected devices, targeting not only the ones from a personal point of view, but also communal needs. The web User Environment integrates the other platform components to provide several facilities and a user interface (UI), allowing people to (among other features) manage their connected devices, from smartphones to programmable boards, adding them to the Context Manager component; add or join communities of other persons and share with them connected devices and produced data.

In order to build little applications towards a personal IoT, the tool allows connecting devices together. Connections between a device Dev1 and a device Dev2 can be configured through a simple and intuitive UI. Configuration happens specifying a set of rules following the "WHEN 'E' DO 'A'" pattern. In other words, the pattern has the following meaning (using the natural language): WHEN an event of type "E" is triggered by Dev1, then DO the action "A" on Dev2. For example, a configured rule could be as follows: WHEN temperature is greater than 60°C then DO send a notification to my smartphone with the message "check cooler system, temperature is becoming high in server farm."

Figure 4 shows two different screenshots of the web User Environment workspace: the first one, on the upper side, represents the page related to a particular device, showing all the details about it and data it generates, in real time. At the bottom of the image, the second screenshot reports the details of the UI about a particular community, including the current members.

The social aspects of the web User Environment are faced by the communities feature. Users are able to create their own communities and to see all the existing ones, already created by other users. They can view all the community details, such as the name of the owner and the domain where it is created. Furthermore, they can join a community sending an affiliation request to the "owner" that can decide to agree or deny the request. When a user joins a community they can see all the members who belong to it and the devices that they have registered and shared within it. As previously remarked in this paper, all these features made available by the User Environment allow people to really build a personal IoT. Thus, thanks to communities, people can operate in a communal, secure, privacy-aware, protected social circle, allowing them to act towards shared, common goals, for example, goals like administrating together the neighbourhood devices installed in gardens, alarm systems, elevators, and buildings maintenance or other daily activities needed by a particular community.

5. Platform Use Case Workflow

This section provides a use case example where the platform is used to create a private community where users can share information among members without leaking of information. Firstly, the example scenario will be presented; following it a summary of the workflow will be detailed. The complete script of the use case can be found at [25].

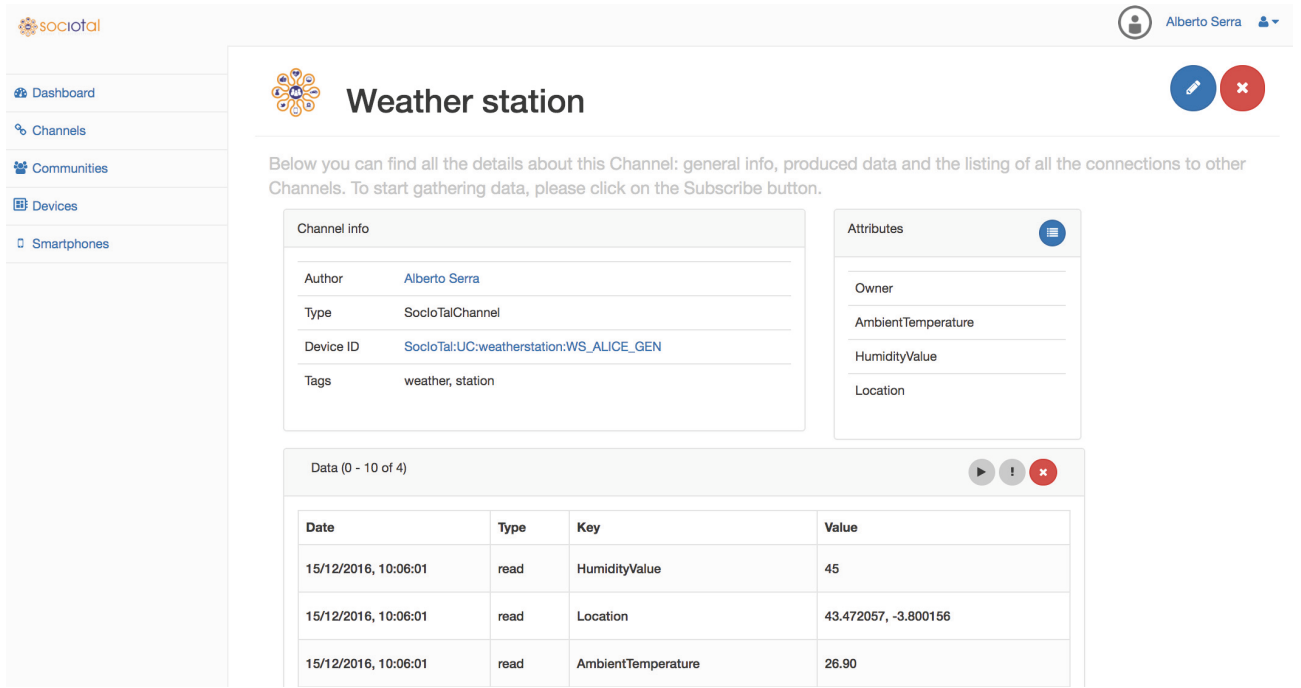
5.1. The Scenario. Alice's grandfather has Alzheimer's disease and, due to this, he sometimes suffers from sudden episodes of disorientation and confusion when he walks outside home. In order to help her family to take care of her grandfather and avoid him getting lost, Alice has created an easy android app, based on platform's APIs, to be installed in her relative's smartphones, and mainly in her grandfather's one. This app captures the GPS coordinates and sends it every 2 minutes to the IoT platform. She plans to create an IoT community, made up of her family members, install her application on their smartphones, register them within her community, and share the position of each of them. This way, every Alice relative (and ONLY Alice's relatives) will easily know the last valid position of each other, including Alice's grandfather, which could help in finding him if necessary. The practical steps are described in the following.

5.2. Create a SocIoTal User. All required actions here presented can be fulfilled either using the platform's APIs or through its web user interface. First step will be to create the set of users needed (Alice, Alice's mother, and Alice's grandfather), so credentials to access and read/write info can be obtained. Using API's "addUser" HTTP POST method [23] or accessing "sign up" screen (Figure 5), user's name and password, among others, can be registered.

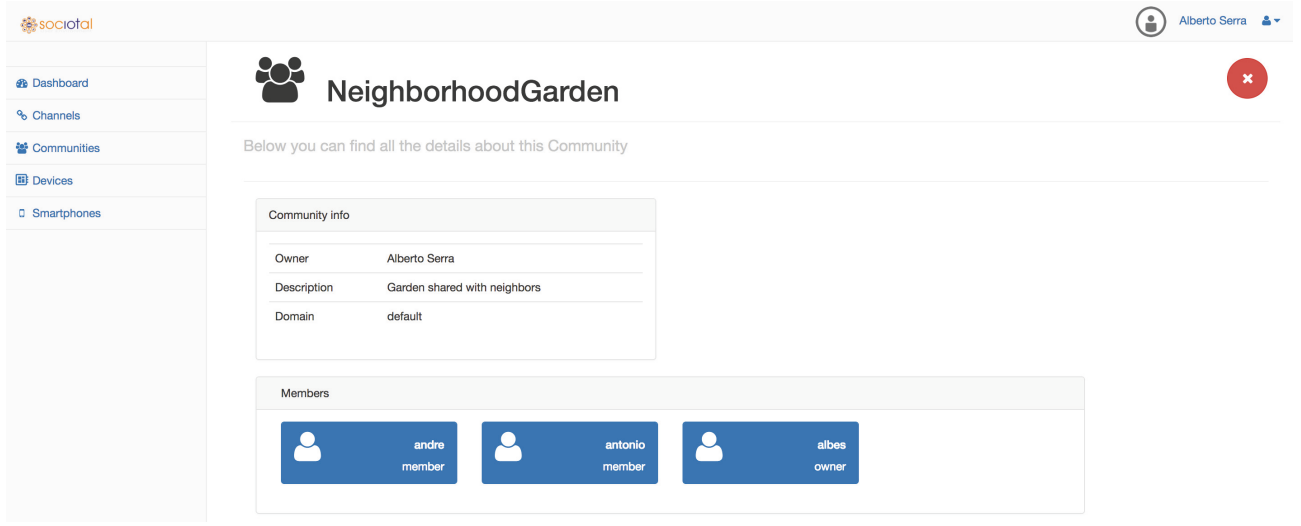
5.3. Create the Community. Accessing the web environment as Alice, from her dashboard (Figure 6), Alice creates "MyFamily" community.

Behind this web, the system uses platform APIs to authenticate Alice as a registered user and obtain a platform token. This token is straightaway used within communities' creation method to create "MyFamily" community and assign Alice the owner role on it.

5.4. Add Members to the Community. "MyFamily" community should be composed of Alice relatives. From their



(a)



(b)

Figure 4: The web User Environment, through its simplified workspace, allows people to manage their connected devices, to create and join communities, and to share devices with other users in a person-centric, humanized IoT.

communities screen, "MyFamily" community appears (but no info about it is shown) and they can send a membership request to Alice's mail. This request includes a direct link to add the requestor to MyFamily. Hence, when Alice click on the link the following automatic process is launched and performed with the communities' API: identify Alice as owner of the community returning the right communities' token and assign a role (member) to the requestor user within the community, so it can be considered as a new member. After this, the community will look like Figure 7.

5.5. Add Devices to the Community. Every community member can register new devices and access info shared within MyFamily community. From user's registering device screen (Figure 8) we can add a new device to the selected community, detailing the type of device and the data it provides. This will

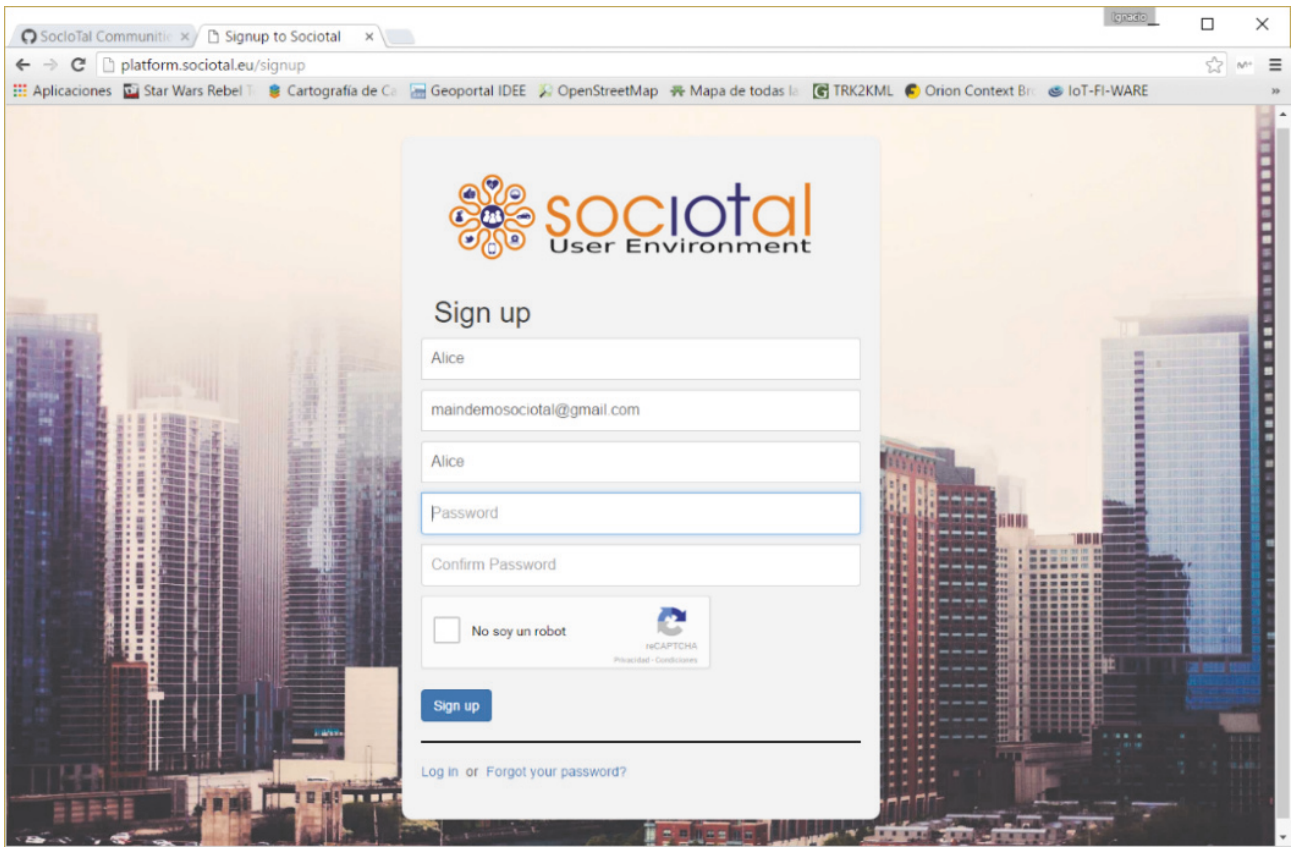


Figure 5: Create user account.

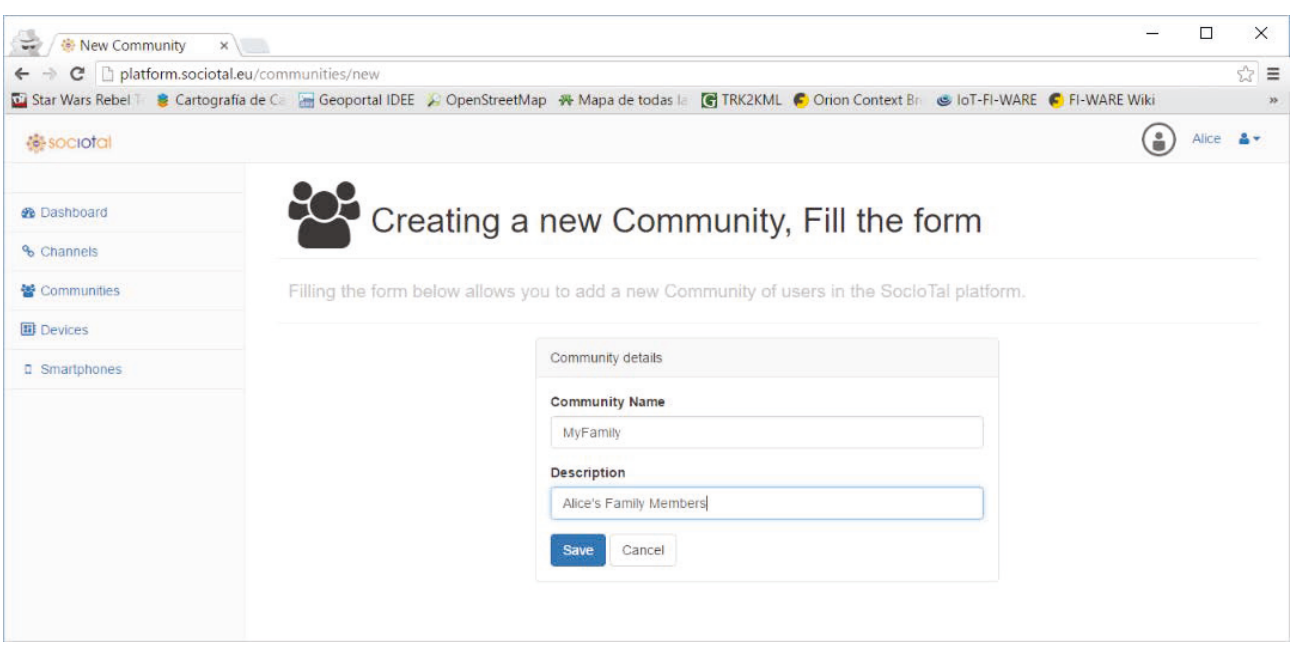


Figure 6: User's dashboard community creation screen.

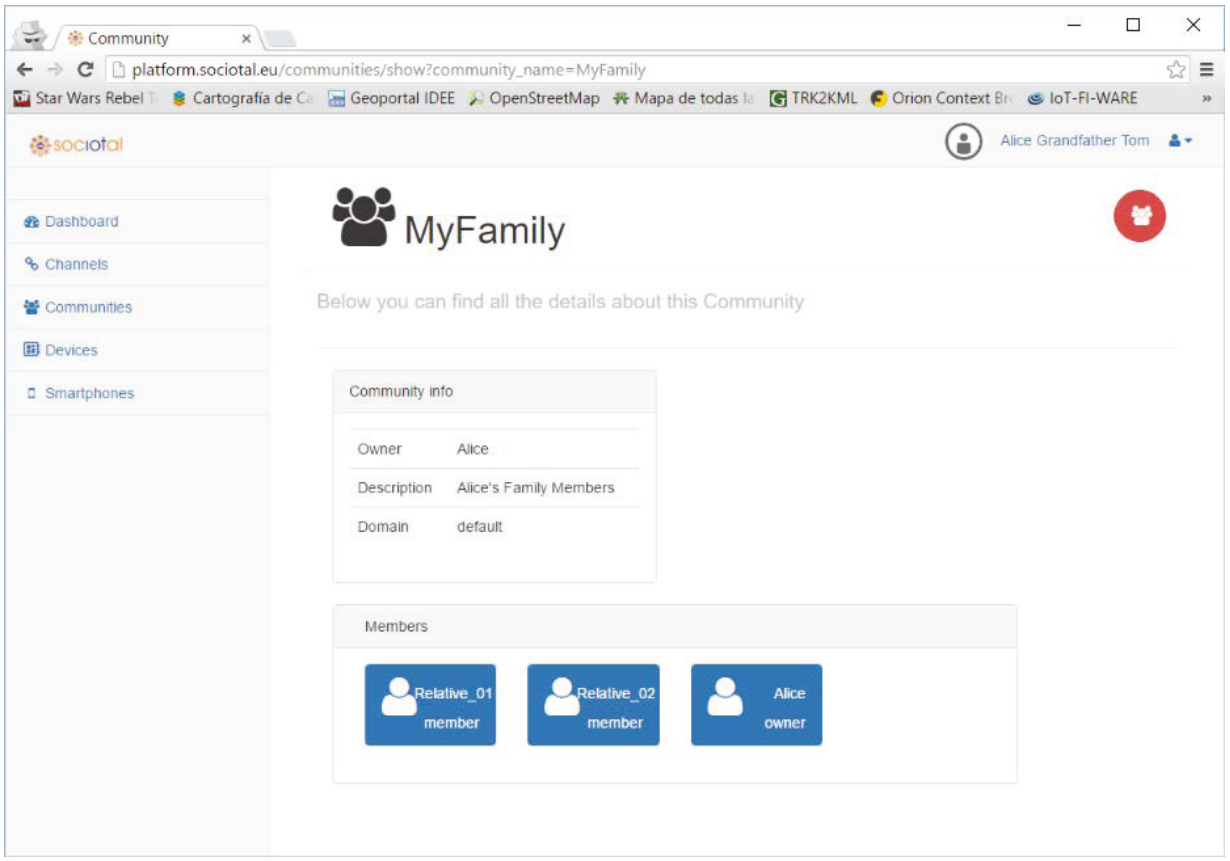


Figure 7: MyFamily community.

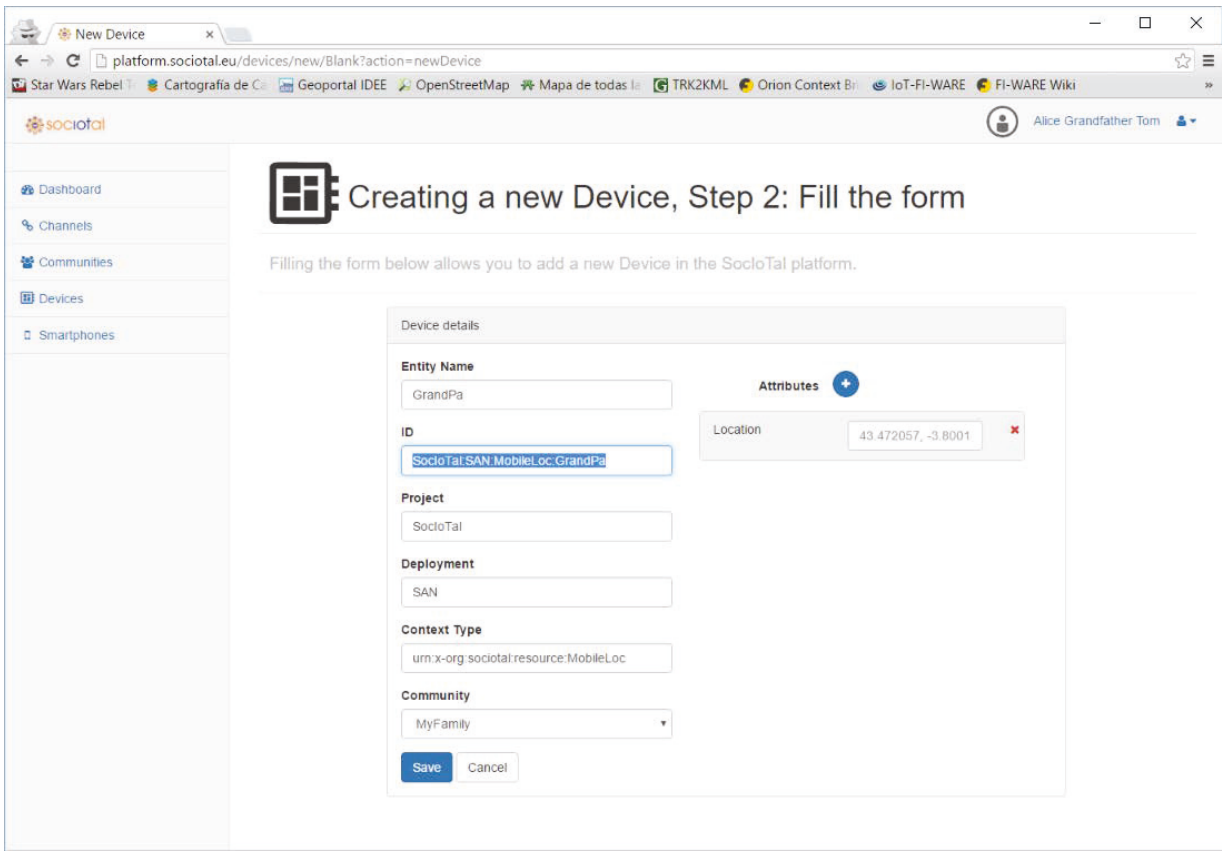


Figure 8: Registering device template.

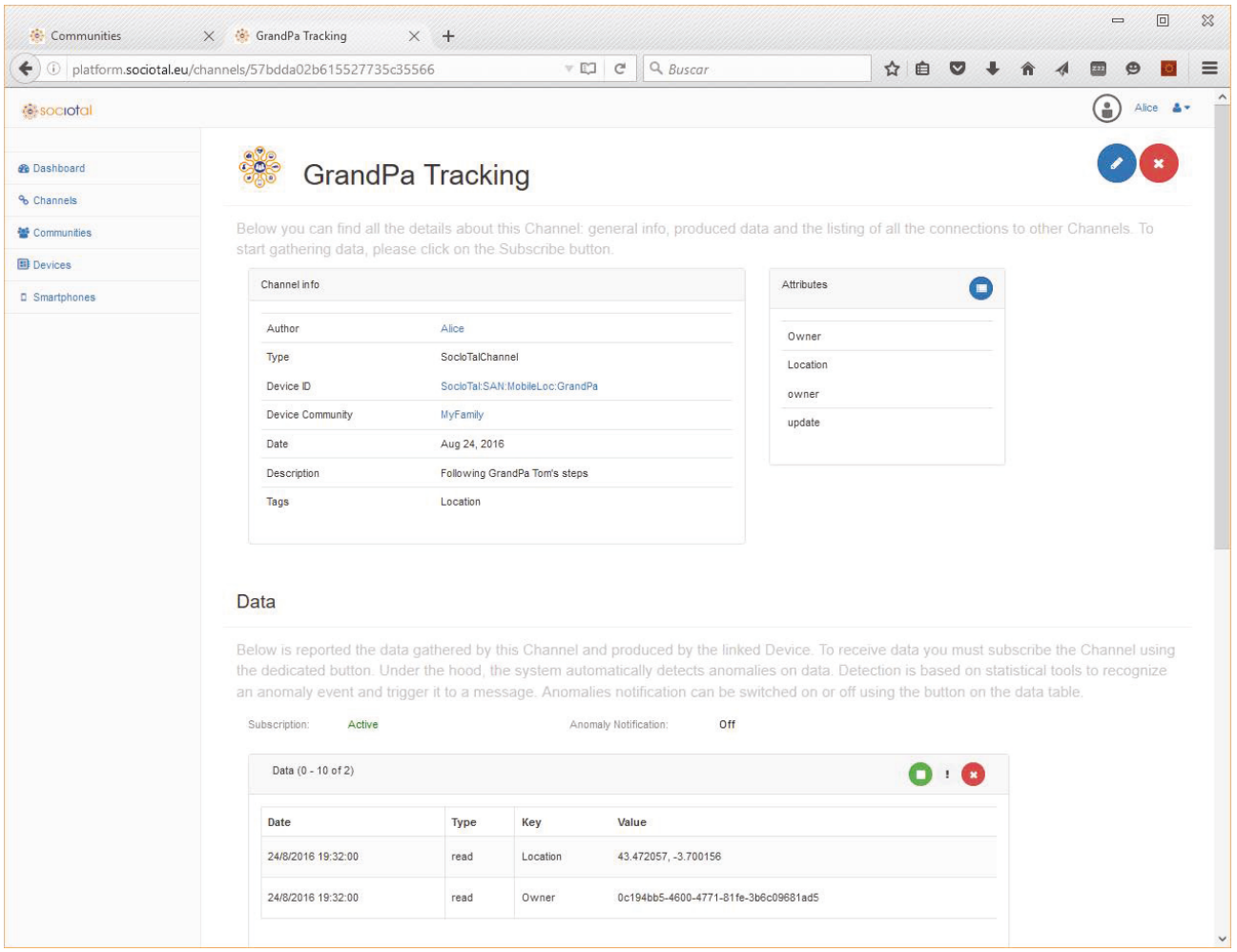


Figure 9: Channel showing subscriptions notifications for a selected device.

create the id to be used later within our real device to upload information.

After this process, each registered device can start sending data to the IoT platform using Context Manager "updateContext" method [22], with a token identifying the user and the corresponding community.

5.6. Access to Shared Mobile Location Data. Registered users can directly query for the last update of any of the devices belonging to any of their communities using API's queryContext method [22]. They can also subscribe and receive a notification every time new interesting data is available through API's subscribeContext method [22]. The web user interface directly implements these two options just by clicking the requested device or creating a channel (Figure 9), where all data updated by the selected device of the community will be shown as it is available.

6. Conclusions

While Internet evolution has been centered on the interworking of devices, nowadays, we are witnessing a swap in this focus towards the liquid flow of data. As more and more elements of our daily environment have the capacity to offer information services, IoT technologies are being developed to fulfill this need for effective consumption of information. However, only very recently focus has been put on the key actors, namely, the human beings, that benefit from the Internet (embracing here everything, IoT, Cloud, and core network) to offer a Humanized Internet of Things.

This paper has introduced the concept of Personal and Communal IoT and presented the key enabling functional considerations to realize such paradigm. Since current IoT platforms do not properly fulfill these key functionalities, we have described the tools that complement existing IoT enablers to build a Personal IoT Management platform. This platform allows users, with different profiles and skills, to create their own set-ups, manage their resources, share information, and build on top of IoT applications that exploit these new environments. The objective of this platform is to empower people to manage their own part of the IoT establishing three basic pillars that conform to the foundation for further features expansions. Firstly, the context information management provides easy and standard mechanisms

to upload, search, discover, and retrieve IoT, oriented to application developers. Secondly, communities' management allows the creation, organization, and protection of resources and information sets. Finally, with a usability criterion in mind, an easy-to-manage dashboard provides an attractive look and feel that supports the aforementioned user-centric novel features and fosters IoT adoption.

The actual implementation and integration of the described platform is a major innovation contribution of the work presented in the paper as it should enable quickly and effectively reaching a wide spectrum of end-users. These users can immediately start experimenting with the platform and exploit it to create applications that make use of the surrounding ambient intelligence supported by their communities' IoT assets. The platform has been built using as baseline a set of the FIWARE GEs in order to take advantage of its reliable open-sourced nature and the momentum and support channels offered by the FIWARE consortium. Moreover, scalability and extensibility of the platform that we have developed will also benefit from the FIWARE environment as it facilitates inclusion of new functionalities covered by some of the FIWARE enablers such as Big Data analysis, cloud hosting, or advanced user interfaces.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work has been partially funded by the research project SOCIOTAL, under FP7-ICT-2013.1.4 (ref. 609112) of the 7th Framework Programme of the European Community. This work has been also supported by the Spanish Government (Ministerio de Economía y Competitividad, Fondo Europeo de Desarrollo Regional, FEDER) by means of the project ADVICE "Dynamic Provisioning of Connectivity in High Density 5G Wireless Scenarios" (TEC2015-71329-C2-1-R).

References

[1] "The FIWARE-catalogue," http://catalogue.fiware.org/.

[2] R. Rawassizadeh, B. A. Price, and M. Petre, "Wearables: has the age of smartwatches finally arrived?" *Communications of the ACM*, vol. 58, no. 1, pp. 45–47, 2015.

[3] A. Whitmore, A. Agarwal, and L. Da Xu, "The internet of things—a survey of topics and trends," *Information Systems Frontiers*, vol. 17, no. 2, pp. 261–274, 2015.

[4] I. Ishaq, D. Carels, G. K. Teklemariam et al., "IETF standardization in the field of the internet of things (IoT): a survey," *Journal of Sensor and Actuator Networks*, vol. 2, no. 2, pp. 235–287, 2013.

[5] A. Pintus, D. Carboni, A. Serra, and A. Manchinu, "Humanizing the internet of things-toward a human-centered internet-and-web of things," in *Proceedings of the 11th International Conference on Web Information Systems and Technologies (WEBIST '15)*, pp. 498–503, May 2015.

[6] A. P. Fiske, "The four elementary forms of sociality: framework for a unified theory of social relations," *Psychological Review*, vol. 99, no. 4, pp. 689–723, 1992.

[7] R. Roman, P. Najera, and J. Lopez, "Securing the internet of things," *Computer*, vol. 44, no. 9, pp. 51–58, 2011.

[8] F. Boavida, A. Kliem, T. Renner et al., "People-centric internet of things—challenges, approach, and enabling technologies," in *In Intelligent Distributed Computing IX*, pp. 463–474, Springer International Publishing, 2016.

[9] I. Thoma, L. Fedon, A. Jara, and Y. Bocchi, "Towards a human centric intelligent society: using cloud and the web of everything to facilitate new social infrastructures," in *The proceedings of the 9th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS '15)*, pp. 319–324, IEEE, Blumenau, Brazil, July 2015.

[10] S. Duquennoy, G. Grimaud, and J.-J. Vandewalle, "The web of things: interconnecting devices with high usability and performance," in *Proceedings of the International Conference on Embedded Software and Systems (ICESS '09)*, pp. 323–330, IEEE, Zhejiang, China, May 2009.

[11] H. Kim, M. Ahn, S. Hong, S. Lee, and S. Lee, "Wearable device control platform technology for network application development," *Mobile Information Systems*, vol. 2016, Article ID 3038515, 20 pages, 2016.

[12] J. Mineraud, O. Mazhelis, X. Su, and S. Tarkoma, "A gap analysis of internet-of-things platforms," *Computer Communications*, vol. 89, pp. 5–16, 2016.

[13] A. Bassi, M. Bauer, M. Fiedler et al., *Enabling Things to Talk: Designing IoT Solutions with the IoT Architectural Reference Model*, Springer Berlin Heidelberg, 2013.

[14] S. Mirri, C. Prandi, P. Salomoni, F. Callegati, A. Melis, and M. Prandini, *A Service-Oriented Approach to Crowdsensing for Accessible Smart Mobility Scenarios*, Mobile Information Systems, 2016.

[15] Xively, "IoT platform as a service for the IoT," https://xively.com.

[16] IFTTT, "Web-tool to connect services and things with the statement 'If This Then That'," https://ifttt.com.

[17] I. G. Niemegeers and S. M. Heemstra de Groot, "From personal area networks to personal networks: a user oriented approach," *Wireless Personal Communications*, vol. 22, no. 2, pp. 175–186, 2002.

[18] R. Prasad, *My Personal Adaptive Global NET (MAGNET)*, Springer, Berlin, Germany, 2010.

[19] L. E. Holmquist, F. Mattern, B. Schiele, P. Alahuhta, M. Beigl, and H. W. Gellersen, "Smart-its friends: a technique for users to easily establish connections between smart artefacts," in *Proceedings of the International Conference on Ubiquitous Computing*, pp. 116–122, Springer, Berlin, Germany, 2001.

[20] L. Atzori, A. Iera, and G. Morabito, "SIoT: giving a social structure to the internet of things," *IEEE Communications Letters*, vol. 15, no. 11, pp. 1193–1195, 2011.

[21] "NGSI context management V1.0," Open Mobile Alliance (OMA), 2010, http://technical.openmobilealliance.org/Techical/release_program/docs/NGSI/V1_0-20101207-C/OMA-TS-NGSI_Context_Management-V1_0-20100803-C.pdf.

[22] Context Manager API, https://github.com/sociotal/SOCIOTAL/wiki/SocIoTal-Context-Manager.

[23] Communities Manager API, https://github.com/sociotal/SOCIOTAL/wiki/SocIoTal-Communities-Manager.

[24] "Keyrock identity management from fiware-catalogue," https://catalogue.fiware.org/enablers/identity-management-keyrock.

[25] SocIoTal tutorial, https://github.com/sociotal/SOCIOTAL/wiki/SocIoTal-Tutorial.