

# On the Use of Information and Infrastructure Technologies for the Smart City Research in Europe: A Survey

Juan Ramón SANTANA<sup>†a)</sup>, Martino MAGGIO<sup>††</sup>, Roberto DI BERNARDO<sup>††</sup>, Pablo SOTRES<sup>†</sup>, Luis SÁNCHEZ<sup>†</sup>, and Luis MUÑOZ<sup>†</sup>, *Nonmembers*

**SUMMARY** The Smart City paradigm has become one of the most important research topics around the globe. Particularly in Europe, it is considered as a solution for the unstoppable increase of high density urban environments and the European Commission has included the Smart City research as one of the key objectives for the FP7 (Seventh Framework Program) and H2020 (Horizon 2020) research initiatives. As a result, a considerable amount of quality research, with particular emphasis on information and communication technologies, has been produced. In this paper, we review the current efforts dedicated in Europe to this research topic. Particular attention is paid in the review to the platforms and infrastructure technologies adopted to introduce the Internet of Things into the city, taking into account the constraints and harshness of urban environments. Furthermore, this paper also considers the efforts in the experimental perspective, which includes the review of existing Smart City testbeds, part of wider European initiatives such as FIRE (Future Internet Research and Experimentation) and FIWARE. Last but not least, the main efforts in providing interoperability between the different experimental facilities are also presented.

**key words:** *Internet of things, Smart City, Horizon 2020, 7th Framework Program, FIWARE, FIRE*

## 1. Introduction

The European Union has many challenges to be faced during the following years: an increasing urban population, the existing economic crisis in some of their countries, or the pollution in the continent, just to mention a few. Hereof, in 2010, the European Union defined the so-called 2020 strategies, which imply the action in three main areas based on the following concepts:

- *Smart*: increasing the effort in research, innovation and education.
- *Sustainable*: moving to low-carbon dependant economies.
- *Inclusive*: facing the crisis, creating new jobs and at the same time reducing poverty.

Those goals are ambitious, but fundamental in an aging society and when the competitiveness is increasing in a globalized world. In that sense, up to 7 flagship initiatives are in place in the European Union to address such

challenges. In particular, the “Innovation Union” flagship [1] represents the efforts in research and innovation within Europe. After the successful 7th Framework Programme, the European Commission decided to create the Horizon 2020 (H2020) programme, which runs from 2014 to 2020, providing nearly €80 billion for research and innovation, a considerable increase from the nearly €50 billion dedicated during the FP7, which covered the period from 2007 to 2013 [2].

In this paper, we focus on one of the pillars of the innovation in Europe, which is the Future Internet, and one of its branch, the Smart City research. More precisely, the focus is on the ICT (Information and Communication Technology) research in the Smart City area, taking into account the deployments performed throughout some cities from the European Union, which address the Internet of Things (IoT) ecosystem to solve the current city problems.

The Smart City research domain has been addressed in numerous research calls, but we can highlight the two most important ones at the time of writing this paper. On the one hand, the recent Smart City and Communities calls are an example of the Smart City investment during H2020. These research calls, which are under the framework of the Cross-cutting activities [3], started in 2015. Currently, 7 projects are ongoing, with a total investment of €174 million. Although this initiative is focused mainly on the energy development, it also encourages the use of existing IoT infrastructures and open platforms. From the different research calls regarding the Future Internet and the IoT in the Smart City, we can highlight the Future Internet and Research Experimentation (FIRE) initiative [4].

Officially launched during the second ICT Call of Framework Programme 7, the FIRE initiative started in summer 2008 with an initial budget of 40 million. FIRE main concept is the promotion of experimentally driven research. In that sense, FIRE initiatives are intended to combine the academic research with the current needs of industry, providing sustainable large-scale experimental facilities, being enlarged gradually with the federation of new testbeds. Hence, the main scope of FIRE is the research in the field of the Future Internet, providing a framework for research in Europe, as it was done before in the United States through the GENI (Global Environment for Network Innovations) program. Other countries followed this approach creating alternative programs (e.g. Japan with the AKARI program) [5].

Manuscript received February 20, 2017.

Manuscript revised May 23, 2017.

Manuscript publicized July 5, 2017.

<sup>†</sup>The authors are with University of Cantabria, Plaza de la Ciencia s/n, Santander 39005, Spain.

<sup>††</sup>The authors are with Engineering Ingegneria Informatica SpA, viale Regione Siciliana, 7275-90146, Palermo, Italy.

a) E-mail: jrsantana@tlmat.unican.es

DOI: 10.1587/transcom.2017ITI0001

The European Union has also invested on the creation of open tools to replicate the Smart City vision in any city. In this regard, the European Commission launched the FIWARE initiative [6], an open platform aiming at easing the development of Future Internet applications. This initiative is also introduced in this paper, as a supporting platform for several testbeds. The paper structure is described as follows. In Sect. 2, the analysis of existing IoT infrastructure for experimentation in the Smart City domain is presented, considering the architecture and deployment carried out in the different testbeds. Section 3 presents FIWARE, as a basic platform of some of the infrastructures included in this survey. Section 4 presents the current trends in Europe, apart from the deployment of new testbeds, to ease the access to the existing ones. Finally, Sect. 5 concludes the survey.

## 2. European Smart City IoT Infrastructures for Experimentation

Taking into account the aforesaid different research initiatives in Europe, most of the IoT infrastructures for experimentation are part of FIRE, as they are more related to the research experimentation testbeds with reprogrammable IoT devices. However, we have also included the Bristol Is Open testbed, which is not participating in FIRE projects, as its basis for IoT experimentation are in line with the aim of the present paper.

Within FIRE up to 58 projects have been funded since its inception, while there are another 29 projects that are yet to finish. Current projects can be divided into 5 groups, depending on the technology they are focused on: Federation, Data Management, IoT, Smart Cities and Networking. From the previous groups, we focus on the testbeds infrastructure related to projects on Smart Cities and IoT research technologies. In the Smart Cities group there are 4 ongoing projects: OrganiCity, Select4Cities, Embers and SmartBuy. On the other hand, there are up to 6 projects within the IoT group, including ARMOUR, RAWFIE, FIESTA-IoT, WAZIUP and F-Interop.

Considering the previous list of projects, we can highlight three important IoT Smart City testbeds, built to experiment with WSN (Wireless Sensor Network) technologies. Table 1 summarizes the main information about the chosen IoT testbeds, detailed information is also provided in the following subsections.

### 2.1 SmartSantander

The SmartSantander testbed [7], [8] started to be deployed in 2010, within the framework of a FIRE European Project that shares the same name. The SmartSantander testbed is a city-scale experimental research facility in support of typical applications and services for a Smart City. SmartSantander follows a two-fold approach: on the one hand, it provides a large-scale IoT sensor deployment in the city of Santander, aiming at providing large amount of data from different sources to create new services for the citizens; on the

other hand, it provides a large network of reprogrammable devices that include a native IEEE 802.15.4 interfaces for the scientific community to experiment with novel protocols in a real world scenario.

During the project lifetime, more than 12000 sensors were deployed. These sensors are divided in the following categories:

- Environmental sensor nodes: they consist of fixed nodes deployed in the city building facades or public lamp-posts. Each node has a set of different attached sensors including temperature, illuminance, sound pressure level and carbon monoxide.
- Irrigation sensor nodes: similar to the environmental nodes, these consist in fixed nodes placed in three of the main gardens of the city, aiming at measuring specific parameters for improving irrigation. The sensors attached to each of these nodes are the following: temperature and relative humidity, solar radiation, atmospheric pressure, soil moisture, soil temperature, wind direction, wind speed and rainfall.
- Mobile sensor nodes: in contrast with the irrigation and environmental sensor nodes, these sensors are placed on top of vehicles belonging to Santander city public transportation network (including buses and taxis) as well as on top of vehicles owned by the parks and gardens management company in the city. The purpose of these nodes is to wider the measuring area of the city as the vehicles are not focused only in the city center. Every node is equipped with a GPRS interface and a GPS sensor, being located and reachable permanently. In addition, mobile sensors are focused on the analysis of pollutants, measuring the carbon monoxide, temperature, relative humidity, nitrogen dioxide, ozone and air particles. Finally, some vehicle data such as the vehicle course, speed or total mileage are also measured.
- Parking monitoring sensor nodes: SmartSantander also deployed around 350 parking sensors in public outdoor areas. These sensors are buried under the asphalt measuring car presence on top of them.
- Traffic sensor nodes: in addition to the parking nodes, a set of sensors deployed in the entrances and way-outs of the city measure the occupancy in each lane, as well as the number of vehicles and the average and median speed.

Apart from the nodes described above, the SmartSantander testbed also counts with 2500 QR and NFC tags deployed in the main Points of Interests of the city, such as monuments, bus stops and shops. Deployed tags are used by one of the two smartphone applications developed during the project lifetime, the SmartSantander RA. It is able to read such tags and provided geo-localized context information to the user using augmented reality. An additional app was also developed, including software to retrieve values from the smartphone sensors where it is installed. These values are also gathered by the SmartSantander testbed.

All the previous sensors are deployed following a three-

**Table 1** IoT Smart City deployments.

	SmartSantander	City of Things	IoT-LAB	Bristol Is Open
City of Deployment	Santander	Antwerp	Grenoble, Lille, Paris, Rennes, Paris, Strasbourg, Saclay and Berlin	Bristol
Entities in charge	University of Cantabria and the Municipality of Santander	Imec, City of Antwerp and Mobile Vikings	Université Pierre et Marie Curie (UPMC), Inria, Université de Strasbourg, Institut Mines Télécom and CNRS	Bristol Is Open (University of Bristol, Bristol City Council)
IoT devices	More than 12000 IoT sensors, including fixed nodes, smartphone applications and NFC tags. Sensors installed are related to environmental, traffic and parking parameters	The deployment is ongoing. Sensors related to traffic are being installed	2728 IoT devices. 232 of them equipped with GPS for time-synchronization purposes. Light and temperature sensors.	1500 ready-to-use lampposts with wireless connectivity.
Mobile IoT devices	Yes, 200 nodes deployed in local buses, taxis and parks and gardens management company vehicles. Environmental parameters such as CO, O <sub>3</sub> , NO <sub>2</sub> , temperature and humidity. Speed, course and GPS location as well	Yes, deployed in the vehicles from the Belgian Postal company. Temperature, relative humidity, CO <sub>2</sub> and organic particles with GPS position	117 wireless mobile robots. Indoor location sensors. All re-programmable	No
IoT radio technologies in use	IEEE 802.15.4, Digimesh, GPRS, UMTS, IEEE 802.11g	IEEE 802.11ac, DASH7 on 433 and 828 Mhz, Bluetooth LE, IEEE 802.15.4/g and LoRa/LoRaWAN	Wired, IEEE 802.15.4. IEEE 802.11a, b and g; MSB-A2 in Berlin sensors	Wi-Fi IEEE 802.11ac, LTE, LTE-A with Massive MIMO, 60GHz backhaul
Software platform	Proprietary platform and FIWARE open platform	FIWARE open platform	Proprietary platform	Open platform integrated with FIWARE
Openness for Experimentation	Yes. Experimenters can access to data contacting with the managers. Call for experimenters performed in SmartSantander. FIESTA-IoT, OrganiCity and FESTIVAL hold ongoing calls for experimenters	Yes, it participates in the Select4Cities European project. Data will be open	Yes. Open Access through the webpage, the scheduler will manage timeslots. It is also part of the European projects: Embers, Armour, OneLab	Yes, becoming a partner of Bristol Is Open it possible to get a slice of the network to experiment with. Partners can be: large companies, small hi-tech start-ups, public service delivery organizations, academics and others

layered approach, as described below:

- *IoT tier*: Responsible for sensing the corresponding parameter documented as described above. The majority of them are integrated in network devices named repeaters, whilst the others are stand alone and communicates wirelessly with the corresponding repeaters (this is the case for the parking sensor buried under the asphalt). As most of the devices do not have access to 24h power sources, they use rechargeable batteries. Repeaters behave as forwarding nodes to transmit all the information associated to the different measured parameters. The communication between repeaters and IoT nodes takes places through a proprietary protocol based on 802.15.4 called Digimesh.
- *Gateway tier*: Both IoT nodes and repeaters are configured to send all the information (through Digimesh protocol) service provision and network management to the gateway. Once information is received by the gateway, it forwards the information to the SmartSantander upper layers, through different interfaces depending on the installation point (GPRS/UMTS or Ethernet). Fur-

thermore, most of the gateways contain enough intelligence to manage and control the network with different tools (Over the Air Programming, network management, etc.).

- *Platform tier*: Top layer in the SmartSantander architecture. This layer is the SmartSantander platform that provides access to all the devices deployed in Santander, as well as the other of services injecting data into the platform. All the core services of the SmartSantander platform are available here, including storage services and context information management.

## 2.2 City of Things

Similar to the SmartSantander testbed, the City of Things testbed [9] aims at providing a real mass-scale deployment to allow academic and industrial researchers to perform experiments. Furthermore, the City of Things testbed aims at providing a city-scale living lab, engaging citizens to test and provide feedback about novel Smart City applications and services.

Managed by a partnership between Imec, the City of Antwerp and Mobile Vikings, the City of Things testbed is focused on 4 main pillars:

- *City-wide deployment*: it covers the full city center and the harbor.
- *Cross-technology*: supporting several radio technologies, including Bluetooth LE, IEEE 802.15.4, WiFi, LoRa and Sigfox.
- *Multi-purpose*: experiments can cover any number of devices, supporting small and large scale experiments.
- *Multi-level openness*: the testbed supports three level of experimentation, including: communication-level, where network researcher can deploy novel network protocols in a real urban scenario; data-level, providing open-data about the measurements gathered by the sensors; and user-level, engaging the citizens to provide feedback about Smart City applications.

The network configuration of the City of Things testbed also considers two completely separate network technologies for each purpose: service provision and protocol experimentation. Therefore, we can consider that the network approach followed in SmartSantander and City of Things is similar. SmartSantander testbed uses the underlying IEEE 802.15.4 technology for both, experimentation and service provision, with a dedicated radio interface for each of them and including multi-hop support for service provision. On the contrary, devices deployed in the City of Things testbed include two different technologies: one supporting LoRaWAN, for the service provision, and another one that depends on each device. Therefore, the network configuration of the City of Things testbed can be divided in two groups, depending on the underlying technologies:

- *Multi-technology gateways*: these devices compose the core of the City of Things capacity for protocol experimentation. They have been distributed throughout the city and connected to the city's fiber network. The main characteristic of these devices is that they support a wide range of different wireless technologies. Each gateway has the following radio technology interfaces: IEEE 802.11ac, DASH7 on 433 and 828 Mhz, Bluetooth LE, IEEE 802.15.4/g and LoRa.
- *LoRaWAN network*: in parallel to the multi-technology gateways, deployed sensors have a dedicated interface supporting LoRaWAN technology. The main goal of this network is to ensure the data sensor provision with a full-city coverage, keeping the network isolated from the protocol experimentation infrastructure.

At the time of writing this paper, the sensor deployment is not yet finished, although a considerable level of deployment has been reached. The different types of sensors installed are listed as follows:

- Traffic monitoring sensors, which provides information about congestion in the main bottlenecks of the city. Differently to the SmartSantander sensors, they scan

the Bluetooth and WiFi packets to infer the traffic congestion level. It turns out that the precision is lower than the equivalent in SmartSantander, but the maintenance is cheaper, as they do not require battery replacement after a certain period.

- Parking sensors: a first limited set of sensors have been deployed to measure parking occupancy in the city.
- Smart Parking Signs: portable signs equipped with GPS and accelerometer to disallow parking in certain areas temporarily.
- Mobile air quality sensors. They measures different gas levels, such as Volatile Organic Compound and carbon dioxide, along with the relative humidity and temperature. The sensors are mainly deployed in vehicles from the Belgian Postal Company, covering most of the city. Each node includes a Lora, SigFox and DASH7 radio interfaces, taking advantage of the deployed infrastructure to guarantee service provision.

### 2.3 IoT-LAB

Differently to the previous two testbeds, the IoT-LAB [10], [11] is not only intended to cover the Smart City applications and experimentation, but to serve as a massive deployment for the IoT experimentation in other fields. Considered as one of the biggest deployments of IoT testbeds, it is placed not only in one city location, but in 7 different cities from France: Grenoble, Lille, Paris, Rennes, Paris, Strasbourg and Saclay, and one from Germany, Berlin.

The IoT-LAB is managed by a consortium of 5 French entities, namely, Université Pierre et Marie Curie (UPMC), Inria, Université de Strasbourg, Institut Mines Télécom and CNRS.

The main goal of the testbed is to provide direct and open access to the 2728 wireless sensors and 117 mobile robots that compose the testbed at the time being. In this sense, the experimentation in the testbed is more focused on the network site than in the sensor data analysis.

The architecture of the IoT-LAB testbed is divided in three components, from which two of them are the servers controlling the infrastructure, while the other component embraces the available nodes for experimentation.

- *Master site server*: this server controls the different sites, one per location, of the nodes. It provides a REST API interface for external users to experiment with any of the existing deployment areas.
- *Experiment Handler*: it is placed in each of the sites where the testbed has nodes deployed, and is connected to each node of the testbed, either by wire or using a wireless access point.
- *IoT-LAB node*: the main device of the testbed, deployed throughout each different location. They can be both: mobile or fixed nodes. In both cases, the nodes are divided in 3 components that provides the experimentation capabilities: the ON (Open Node), which is the re-programmable low-power device where experimenters

will have full access; the Gateway, attached through a serial port to the ON, is in charge of reprogramming the node and monitor its status, as well as gathering the experimentation results; the third component, called the Control Node, is mainly in charge of management the full IoT-LAB node, providing the interfaces to start, stop or reset the ON reprogramming, or selecting its power source.

IoT-LAB nodes are composed of multiple and heterogeneous devices, where the main differences are related to their processing capabilities and their mobility. Hence, we can divide the nodes in the following groups:

- *Fixed nodes*: including three different CPUs depending on the node. The less powerful is the WSN430, which contains a 12-bit controller with temperature and light sensors. With bigger processing capabilities, the M3 node features a 32-bit ARM Cortex-M3 and the A8, the most powerful one, features a 32-bit ARM Cortex-A8 600 MHz. All of them provides connectivity using IEEE 802.15.4 interfaces.
- *Mobile robots*: there are two types of mobile nodes in the IoT-LAB testbed: the Turtlebot and the Wifibot. They are both able to find the recharging point automatically and the main difference is the way they found it, an infrared beam and infrared sensors plus a QR code, respectively. All of them features the Cortex-M3 micro-processor. Additionally, indoor localization data are provided during the experiment lifetime.

## 2.4 Bristol Is Open

Bristol Is Open [12], [13] is a Smart City infrastructure that covers the center of Bristol including network, sensors and a software platform. It is funded by the local, national and European governments, with academic research funding, and by the private sector. Bristol Is Open is composed by a series of sensors, network infrastructures and services with the final scope of providing an open and experimental platform in the city of Bristol: this approach has also been defined as City Experimentation as a Service. The basic infrastructure of this experimental testbed is composed by:

- *Optical network*: 144-fiber core network connecting 4 active nodes, full optical switching.
- *Wireless Network*: 1 Gbps access network WIFI, LTE, LTE-A, 60 GHz, Massive MIMO.
- *IoT*: 54 Fiber-connected lamppost cluster and 1500 sensors.
- *Cloud Infrastructure*: HPC and commodity compute and storage, edge computing.

Bristol Is Open also provides a set of middleware components. For instance, the Software Defined Network Controller (SDNC), which represents one of the key functionalities because it enables multiple experiments to be carried-out simultaneously across the network. The SDNC is able

to identify flows for given applications in order to configure specific points in the infrastructure to properly route the data flows based on a pre-defined set of operational requirements, such as latency or bandwidth. SDNC is based on the OpenFlow protocol, an open standard that enables researchers to run experimental protocols in local networks.

On top of the infrastructure, different applications conform the base for the experimentation support: one example is the IoT Mesh network, which enables innovators and experimenters to test and validate their new technology solutions, in a real-time environment on a real-world, using a wide range of IoT sensors and connected devices. Bristol Is Open platform is already integrated with FIWARE platform components, and it supports HyperCat standard.

## 3. FIWARE: A Smart City Open Platform

In the previous sections, different examples of European Smart City IoT infrastructures have been compared showing their peculiarities. Beyond their architecture and hardware deployments, an important aspect to be taken in consideration is the software platform that manages all the infrastructural assets.

These Smart City IoT infrastructures showed the complexity and variety of technologies that are present in smart cities: every infrastructure is managed by a specific platform with its own specifications, architecture and interfaces for third party access. Several EU funded initiatives have been launched during the last years with a twofold scope to mitigate it: on the one hand, trying to harmonize the architecture and the specifications of Smart City platforms; and on the other hand, providing open components and specifications for smart cities. These open technological solutions have to be easily replicated in different European cities, avoiding vendor lock-in constraints. Among these initiatives, the most relevant, in terms of public investment and adoption in the European countries, is FIWARE, born as the result of a public-private collaboration between the European Commission and the private sector.

The main objective of FIWARE is the provisioning of general-purpose components called Generic Enablers (GE) (available on the FIWARE catalogue [14]), based on a public and royalty-free specification, to ease the development of smart applications in multiple sectors. In particular, the FIWARE solution provides generic functionalities to support several technological aspects of Smart City infrastructures, such as:

- *IoT devices management*: e.g. IoT gateway that is able to connect with different devices supporting several IoT protocols and legacy systems.
- *Data and Context management*: e.g. context broker that can manage context information being connected with different application/devices and provides information with standard APIs.
- *Big Data storage*: functionalities to support the storage and management of large amount of data coming from

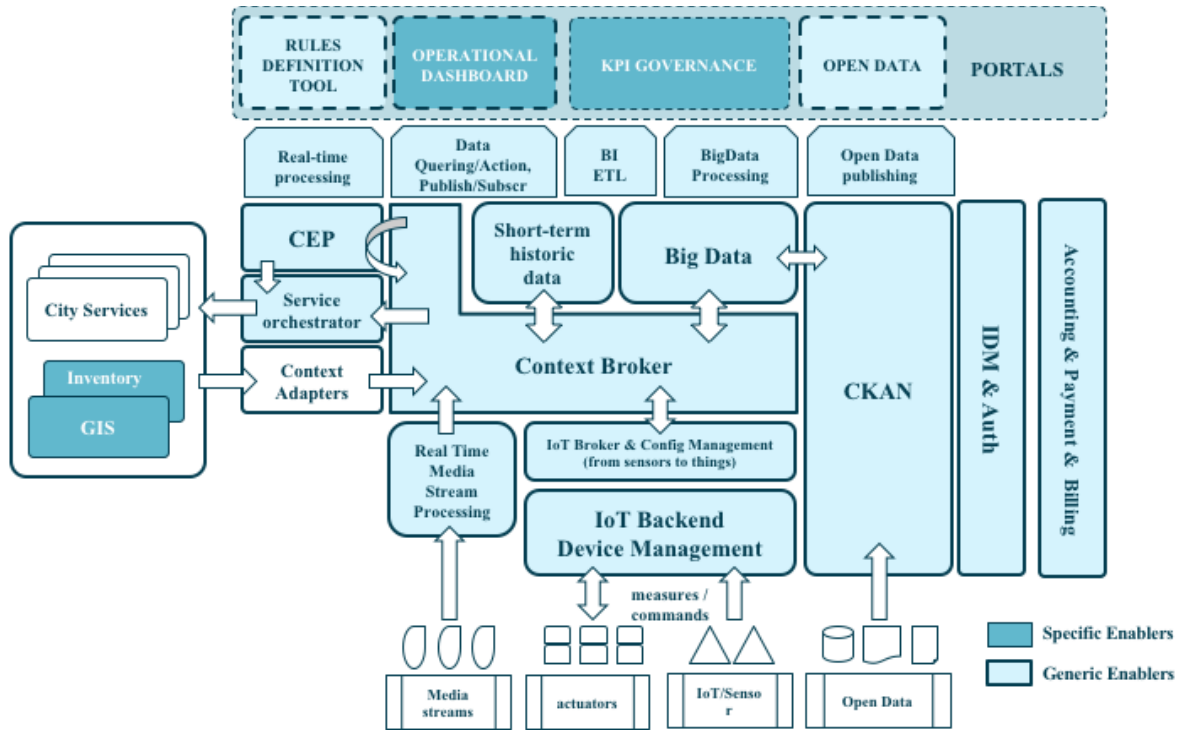


Fig. 1 FIWARE Target Smart City platform [17].

sensors and IoT devices.

- **Open Data management:** support for the publication and provisioning of open datasets.
- **Advanced dashboard:** possibility to create (mobile) user interfaces that support real time data visualization, advanced charts, cockpits etc.
- **Security:** e.g. identity manager, role based access control, privacy and anonymization.
- **Cloud:** the platform should be able to run some of its component in a cloud environment in a “as a Service” mode.

In that sense, FIWARE is based on open and well-defined principles that should simplify and speed up its adoption:

- **Interoperability:** every FIWARE component can be easily integrated with the others and with external ones because it provides standard and open APIs.
- **Modularity:** every FIWARE component is independent, so it is not mandatory to use all the components provided in the architecture but some can be substituted (e.g. by proprietary ones related to specific technologies already in the cities).
- **Generality:** an architecture that can be customized for the different domain/use cases of the project (energy management, mobility, etc.) because is based on generic components.
- **Reusability:** the platform can be easily reused in different cities with a limited effort because is based on generic and open components.

It is possible to test the FIWARE GE in as-a-Service mode without any cost using the FIWARE Lab [15], a non-commercial sandbox environment where innovation and experimentation based on FIWARE technologies take place. Companies and developers can test their FIWARE applications on FIWARE Lab, exploiting Open Data published by cities and other organizations. FIWARE Lab is an OpenStack [16] based cloud infrastructure deployed over a geographically distributed network of federated nodes.

### 3.1 An IoT-Enabled Smart City Architecture with FIWARE

Despite the fact that FIWARE proposes technical solutions that can be considered domain-agnostic, the “Smart City” context is the one in which most of FIWARE based architectures have been adopted and deployed. Figure 1 shows an example of a FIWARE IoT-enabled smart city architecture including the components matching existing FIWARE GEs. In this section it will be described the ones that can be considered essential to build a basic IoT-Enabled Smart City platform.

The lower layer of the architecture shows the components related to the interaction with the IoT devices. The “IoT Backend Device Management” GE [18] connects IoT devices/gateways to FIWARE-based ecosystems. The scope of this component is to translate different IoT protocols into NGSI specification [19], a standard defined by OMA [20], used by FIWARE to exchange context information and represent entities.

A core component of the FIWARE platform, depicted

in the central part of the architecture, is the “Context Broker” [21]. FIWARE provides a mechanism to generate, collect, publish or query massive context information and use it for applications to react to their context: the FIWARE Context Broker is able to provide data coming from different sources (i.e. IoT devices) through an API based on the OMA NGSI, which follows a Publish/Subscribe approach. The Context Broker represents the entity that is in charge of dispatching the information that are coming from the IoT southbound layer to the northbound components that will process the information.

FIWARE provides also GE that are devoted to the management of Open Data, a crucial aspect to make accessible the huge amount of data produced in a smart city. CKAN [22] is an open source open data portal that makes data accessible through a set of features that includes a data catalogue system with data storage, data visualization, data analytics and an API for third party access.

Real time media streams represent also another important source of information that, in a FIWARE based platform, can be analyzed to extract knowledge and identify, for instance, critical situations. In this sense, real-time context information can be further analyzed using the “Complex Event Processing” GE [23] in order to identify specific event data in real-time and generate immediate insight. All the city data collected by the different sources (sensors, data repositories, devices, data stream) and processed with the aforementioned GEs, can then be analyzed by advanced components that include “Big Data” storage and processing, Business Intelligence and ETL functionalities. All of them with the final aim of providing the results to end-user applications and dashboards that can be used, for instance, for city monitoring and governance.

FIWARE, also provides Generic Enablers suitable for “Identification and Authorization”. The Identity Management GE [24] provides a series of functionalities related to users’ access to networks, devices, services and applications, including authorization & trust management and privacy. Authorization PDP GE [25] allows to get authorization decisions based on authorization policies, and authorization requests.

### 3.2 FIWARE Smart City Platforms

FIWARE has been adopted by a growing number of cities in the last years as a suitable platform to satisfy smart cities’ needs. Recently, the initiative “Open & Agile Smart Cities” [26], which involves among 100 cities from 23 countries in Europe, Latin America and Asia-Pacific, accelerated the usage of FIWARE around the world promoting an open and standardized approach and best practices, in the design and implementation of Smart City platforms. Among the most relevant existing FIWARE smart city platforms and applications we can include Turin (Italy), in which the addressed use case was focused on the issue of security as perceived by citizens. The developed application uses some FIWARE GE related to Data visualization and Business intelligence

in order to analyze data related to warnings or complaints collected by the local police contact centers, providing real time notifications to the stakeholders about the security issues and statistics. Valencia (Spain) is another example that uses FIWARE as part of its urban platform [27] (Valencia Ciudad Inteligente - VLCi) taking also advantage of the use of FIWARE-Lab as a cloud environment in which the FIWARE components and applications can be developed, deployed and tested before integrating in the main smart city platform. Nova Friburgo (Brazil), adopting an integrated Smart City platform [28] strongly based on FIWARE GE (WM9 Platform [29]) that covers different aspects related to IoT, Data Management and Business Process Management. Finally, Santander also includes FIWARE as part of the SmartSantander testbed core platform.

FIWARE platform has also been introduced in several research and innovation projects within the Smart City domain, producing a significant quantity of specific applications based on FIWARE [30].

### 3.3 Other Related Initiatives about IoT Management

Besides FIWARE, there are also other initiatives related to the definition of standards and technologies in the IoT field, the basic layer to build a Smart City platform:

- *OneM2M* [31] aims at developing a set of technical specifications to help defining a common M2M (Machine To Machine) service layer that can be readily embedded in different hardware and software. Therefore, the main goal is to overcome interoperability and connection issues between heterogeneous IoT devices and M2M application servers. The mission of oneM2M includes also the involvement of new stakeholders coming from the M2M related domains (e.g. healthcare, utilities, industrial automation, telecommunications etc.)
- *Open IoT* [32] is a project that aims at creating an open source middleware to connect and get information from sensors located in the cloud without dealing with their specific technology, enabling accessibility to IoT based resources and their capabilities. Open IoT proposes a “Sensing-as-a-Service” approach, providing instantiations of cloud-based and utility-based sensing services. The project also provides specific smart city solutions (Smart Campus, Crowd-Sensing Monitoring, & Assistance Living) with the objective of transferring smart city innovation from research-academia to industry products.

Aforementioned platforms propose different approaches and technological assets that can be compared to the FIWARE ones. In that context, one of the most challenging issues to be solved is the harmonization of the different technologies and architectures in the IoT/Smart city domain, in order to avoid fragmentation and enable the interoperability and reusability of developed solutions from one city to another. Among the initiatives that address this issue we can highlight the UNIFY-IoT project [33]. It is a partner of the

Alliance for Internet of Things Innovation (AIOTI) [34] and the Internet of Things European Research Cluster (IERC) [35], aiming at stimulating the collaboration between different IoT projects and platforms to define common approaches to platform development, interoperability and information sharing.

The “International Technical Working Group on IoT-Enabled Smart City Framework” [36], managed by NIST (US National Institute of Standard and technologies) aims, through an international public working group, at comparing different IoT architecture in order to define a framework of common architectural features to enable smart city solutions.

#### 4. Current Initiatives in Federation and Interoperability of IoT Testbeds

Nowadays, apart from the different projects that have as a goal to provide a fully working testbed or an open platform for the Smart Cities, there are some other trending initiatives which are in the scope of the research in Europe.

Currently, there is a strong focus on the provision of the different testbeds to easily replicate experiments from one to another. In that sense, federation of testbeds is now one of the main objectives of existing European projects. Testbeds federation has many advantages over traditional experimentation in a single testbed:

- Experimentation preparation and learning process is highly reduced when the experiment requires resources from different testbeds, which usually do not have the same architecture and development tools. Other practical aspects such as account creation and authorization requests for each of the testbeds are done only once.
- Similarly, the development process is significantly reduced as the experimenter will use the same existing tools for the different testbeds.
- Conducted experiments in federation platforms are easily replicable in other testbeds from the same federation. Therefore, experiment assessment in different locations can be performed without increasing the development efforts.
- Dedicated experimentation support is usually available in a single endpoint regardless the testbed you are having any issue with.
- In the case of funded experiments for projects providing federation platforms, the application process is simpler compared to the one from the standard H2020 calls, together with a rapid review process by independent external evaluators.

However, federation platforms have also their drawbacks, considering that most of them are built upon specific international research projects which have a limited duration in time. Therefore, experiments performed in a federation platform from an international project will depend as well in the sustainability of such platform, taking into account that the experiments could be only performed in the limited timeframe of the project lifetime.

#### 4.1 Federation Initiatives in European Projects

For instance, FESTIVAL [37], a Europe-Japan collaborative project, is focused on the federation of different Smart ICT testbeds. In particular, federated facilities belong to different 4 different domains, including IoT, Open Data platforms, IT infrastructure and Living Labs. The ultimate goal is to provide a platform where external experimenters can easily manage heterogeneous and different resources with a common API. FESTIVAL addresses 3 main domains: Smart Energy, Smart Building and Smart Shopping, with the addition of the Smart City through the inclusion of the SmartSantander testbed in the federation.

Following recent trends within the Smart City domain, the OrganiCity project [38] aims at providing a platform to experiment with vast amount of data generated from different cities, concretely London, Aarhus, Patras and Santander. The key point in this project is the use of co-creation tools, so as to involve the citizens and the stakeholders in the experimentation process. Hence, by means of a co-creative experimentation, OrganiCity pursues the definition and creation of new services. Similar to FESTIVAL, the project federates the resources from the participant cities, although in this case the focus is on data resources, therefore making data access as easier as possible.

Whilst in the case of OrganiCity the idea is to provide a platform ready to experiment with, Select4Cities project envisions the organization of a competition to create it. The approach followed is the organization of a call for tenders, so as to let third parties to work and provide the best Smart City platform solution. The project also defines a set of requirements, from which we can highlight: data-driven, providing access to real-time and non-real-time data while being compatible with complex data analytics algorithms; service-oriented, being easy to deploy in several components and supporting third party data sources; co-created, differently to OrganiCity, making all the code open source engage a coding community behind the platform; large-scale testing support, with the inclusion of validations tools; and finally, being user-centric, providing a digital access to data to individual users in a personalized way. The solutions proposed in the call will be tested with the data provided by the participant cities: Helsinki, Copenhagen and Antwerp, with the City of Things testbed, analyzed in Sect. 2.

#### 4.2 Semantic Interoperability in the Smart City

One of the great existing challenges in the previous federation projects of Smart City facilities and testbeds is the heterogeneous nature of the smart city deployments based on the IoT paradigm. Usually, each service deployed in a city can be considered as a vertical silo, with minor integration among other services in the same city, and even less with other cities. Hence, each facility uses a different convention in the way they do handle their own information, giving rise to a number of orthogonal (and most likely disjointed)



alternatives.

FIESTA-IoT project [39] aims at providing a common semantic framework to make city interoperability services a reality. The final goal within the project is to provide a holistic cradle where a number of different testbeds can converge in a unique and semantic federation. This way, experiment would only need to rely on a single manner to get access to all the information.

On this aspect, one of the outcomes of the project is the definition of a common semantic data model [40], based on a mixture of mainstream ontologies. Unlike these ones, the clear objective of FIESTA-IoT's is the provision of a lightweight solution, which does not jeopardize the overall system performance. Together with this, they have also defined a taxonomy that encompasses a wide range of physical phenomena, units of measurement, measurement types and domains of interest, with no other goal but settling down an unanimous way to describe a resource and its underlying measurements. On top of this framework, any experimenter or application developer would only need to rely on a single interface to get access to the subjacent data, instead of dealing individually with each testbed.

It is worth mentioning that, due to the tens of coexisting languages in the European Union, semantic interoperability turns to be an even more challenging problem. Therefore, the European Commission is also taking some interoperability actions, apart from projects like FIESTA-IoT, to overcome this situation. Furthermore, IoT sensor infrastructures suffer from this problem specially, as their resource descriptions can be found in several languages depending on the city. In that sense, one of the most well-known action is the creation of EuroVoc [41]. It is a multilingual and multidisciplinary thesaurus covering the activities of the EU, such as the IoT sensors and open data catalogues. This tool is managed by the Publications Office, which moved forward to ontology-based thesaurus management and semantic web technologies conformant to W3C recommendations as well as latest trends in thesaurus standards.

#### 4.3 Platform Architectures in European Federation Projects

One of the major issues regarding to the federation of different testbeds is the heterogeneous coexistence of different access tools, such as APIs, web platforms and applications. This is especially important when the goal is to provide a homogenous access experience for their users. Projects presented above have addressed this issue differently, depending mainly on their requirements and the testbeds included in the federation. Hence, one of the main activities at the beginning of such projects is the definition and implementation of an architecture that could deal with these kind of problems. During this section we analyze three architecture approaches in the FESTIVAL, OrganiCity and FIESTA-IoT federation platforms.

FESTIVAL project presents an architecture [42] that focuses in the problems related to the heterogeneity of the

resources from the testbeds federated. In that sense, FESTIVAL envisions the creation of four aggregators that are in charge of linking the testbeds with the platform. These aggregators have a proactive role, meaning that they will not request developments in the testbed side, but will use the interfaces provided by the testbeds to communicate with them.

FESTIVAL architecture, depicted in Fig. 2, is divided in two main layers plus a graphical user interface: the Uniform Access Layer and the Experimentation as a Service layer. The graphical user interface, a web-based portal called Experimentation Portal, has also been developed as an external tool to ease experiment creation and management.

- The Uniform access layer is composed of four different aggregators implemented for the platform. These aggregators connect federated testbeds with the FESTIVAL federation platform to gather the information, which is retrieved in real-time when possible. IT and IoT aggregators have been built reusing existing federation tools, ensuring the compatibility with the technologies implemented in the testbeds. Thus, the IT aggregator uses the Sliced Federation Architecture [43] from GENI. Similarly, the IoT aggregator is based on sensiNact [44], a horizontal platform which is able to manage multiple IoT protocols. On the contrary, the Living Lab aggregator is built specifically for the project, easing the communication with the Living Lab managers. The Open Data aggregator has been also developed for the project and handles automatically Open Data platforms based on Socrata and CKAN technologies.
- The Experimentation as a Service layer is composed of different modules to ease the experiment management. Therefore, it is an experiment-centric layer that provides functionalities such as experiment creation, resource reservation and release, storage and monitoring. Furthermore, this layer manages the resources univocally, providing a single identifier to each one and a common REST API to access them, independently of the resource type.
- The upper layer is composed by the Experimentation Portal, a graphical user interface that provides a user-friendly management system to interact with the platform. Although it provides many functionalities, complex experiments must be performed using the API directly. The Experimentation Portal is loaded locally and make use of the API provided by the Experimentation as a Service layer.

It is worth mentioning that FESTIVAL federation platform access is secured based on a system of roles to authorize users. API usage requires a token that can be obtained by login into the platform. This token has to be included in each HTTPS call, and the security module will determine if the user has the proper rights to access to a specific resource. The security implementation has been built upon the security modules in FIWARE, introduced in Sect. 4.

As for OrganiCity project, whose architecture is de-

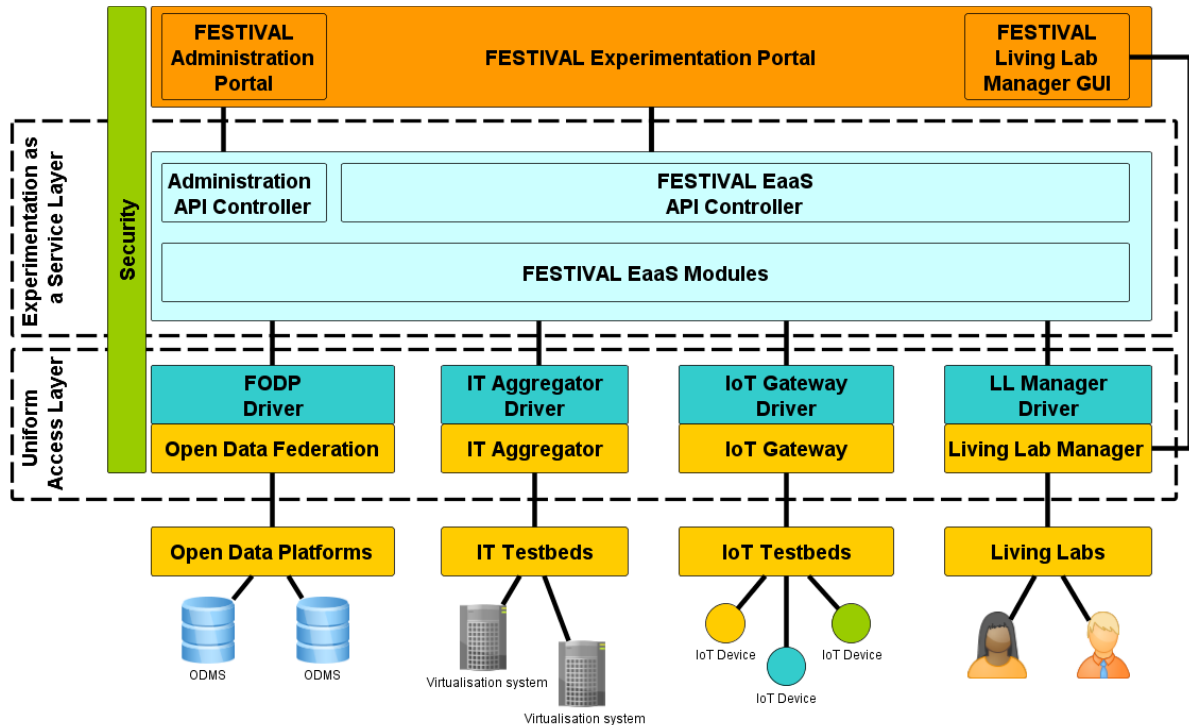


Fig. 2 FESTIVAL EaaS platform architecture.

picted in Fig. 3 [45], focuses on the integration of citizens and communities in the decision-making of the cities by means of experimenting with urban data. In order to simplify such experimentation, a set of tools (co-creation tools) are integrated with the core of the platform. From an overarching perspective, the architecture is divided in three layers, depending each one devotes to different actors:

- The OC site Tier embraces cities that federate their data into OrganiCity, by using the so called federation API. This API is available and also provides authentication and authorization mechanisms. From an integration angle, any city willing to federate its data into OrganiCity would have to develop the proper connectors to interact with the federation API. It is worth mentioning that entities who want to federate services other than data (e.g. actuators) must provide a specific API which will extend the federation API, as the OrganiCity platform does not contemplate this kind of services on the given federation functionalities.
- The second layer, namely OC Platform Tier, provides the core components to manage the experimentation process and the federated assets in the platform. Within this layer we can highlight the ADS, or Asset Discovery Service, which facilitates the discovery of resources for external experimenters. This component leverages and extends the FIWARE Generic Enabler Context Broker, also introduced in Sect. 4, which provides context information of the different data assets. Apart from that, this layer implements other key components to manage both the platform itself by the administrators and the

experimentation process.

- The OC Experimentation layer is the upper and comprises all the tools and services developed to ease the creation of experiments, applications and services running on top of OrganiCity. These components interact with the platform core by using the north bound interface. In this layer, the experimenter can find a set of graphical interfaces to make use of the services provided by the OC Platform Tier, including the Urban Data Observatory (UDO), which is the portal on top the ADS. Apart from services interacting with the core components of the facility, this layer also allocates the co-creation tools, which aim is to simplify the experimentation according to the field of interest.

Finally, the main aim in the FIESTA-IoT federation [46] is to enable an Experimentation as a Service paradigm for IoT experiments. Therefore, FIESTA-IoT also presents a testbed agnostic API, virtualizing federated testbeds.

To this end, FIESTA-IoT requires to the testbeds willing to participate in the federation to implement the common standardized semantics and interfaces defined within the project. This will enable the FIESTA-IoT meta-platform to access their data, resources' and services' descriptions and other low-level capabilities.

The platform has been built upon two main design decisions. A primary decision was to take as reference the IoT ARM as defined in the IoT-A project, following the domain model defined in ARM, which introduces the key concepts in IoT and their relations; and the information model also defined in ARM, which introduces how to structure infor-

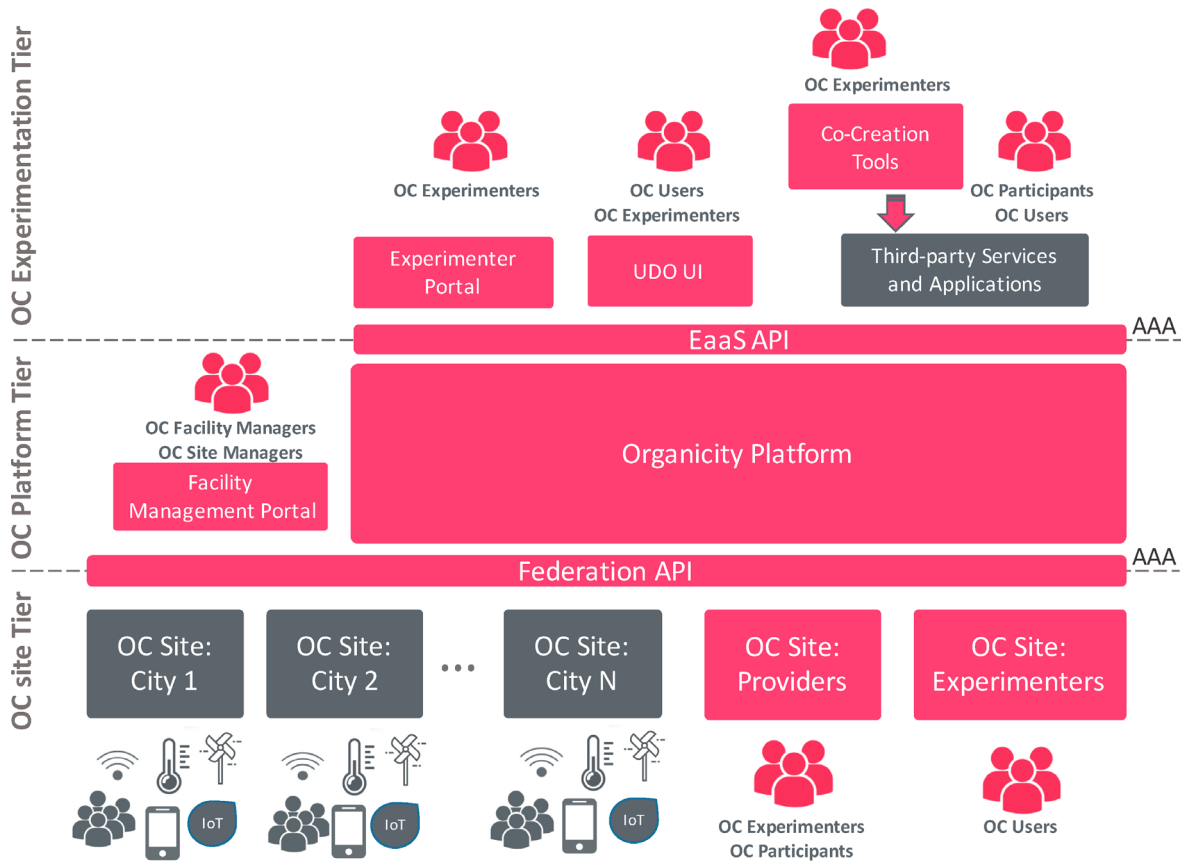


Fig. 3 Organicity platform architecture.

mation in IoT platforms. A second decision was based on the usage of semantic technologies to support the interoperability between heterogeneous IoT platforms and testbeds. In that sense, FIESTA-IoT focuses on the introduction of taxonomies and ontologies to seamlessly deal with data from different sources.

As can be seen in Fig. 4, the central component of the FIESTA-IoT meta-platform is a directory service. This Meta-Directory, or IoT-Registry, is where all the observations, produced by the IoT devices from the federated testbeds, are stored. This repository enables the dynamic discovery and use of resources (e.g. sensors or services) from all the interconnected IoT deployments.

The IoT-Registry's main function is to keep and maintain all the (semantic) resource descriptions and observations which the underlying testbeds, federated within FIESTA-IoT, have provided. On top of this "collector" behavior, a fully-fledged REST API allows the interplay between users (FIESTA-IoT admins, testbed providers, experimenters or observers) and the databases that store the information. The core of the component of the IoT-Registry is the Triplestore Database (TDB) where the Resource Descriptions from the devices belonging to the federated testbeds and the Observations produced by these devices are stored. Both the Resource Descriptions and the Observations are semantic documents that uses RDF serialization to describe them. In this

sense, the TDB implements the information model that is specified by the FIESTA-IoT ontology.

The TDB can be accessed through HTTP requests, where SPARQL queries can be encapsulated. TBD SPARQL results are also encapsulated into HTTP response packets. Last but not least, FIESTA-IoT platform also considers the provision of a set of tools to ease the experimentation on the platform. Among these tools we can highlight the Experiment Execution Engine which provides the possibility to the experimenter to define the complete experiment lifecycle in an XML-based document using a Domain Specific Language. This document is loaded within the platform for the experiment to be autonomously executed. Finally, FIESTA-IoT federation platform focuses on the integration of testbeds semantic interoperability for federated testbeds. Similarly to OrganiCity, FIESTA-IoT is only focused on IoT data management. Therefore, the main challenge of the FIESTA-IoT project is the introduction of a semantic annotator in the testbeds for data search and usage. They assume the existence of a Resource Directory in each of the testbeds that is being federated, and introduces a new module, the Semantic Annotator, which will process all the measurements produced by the testbeds and annotate them with a common ontology. Thus, any testbed that wants to participate will have to implement the common standardized semantics and interfaces defined in FIESTA-IoT project.

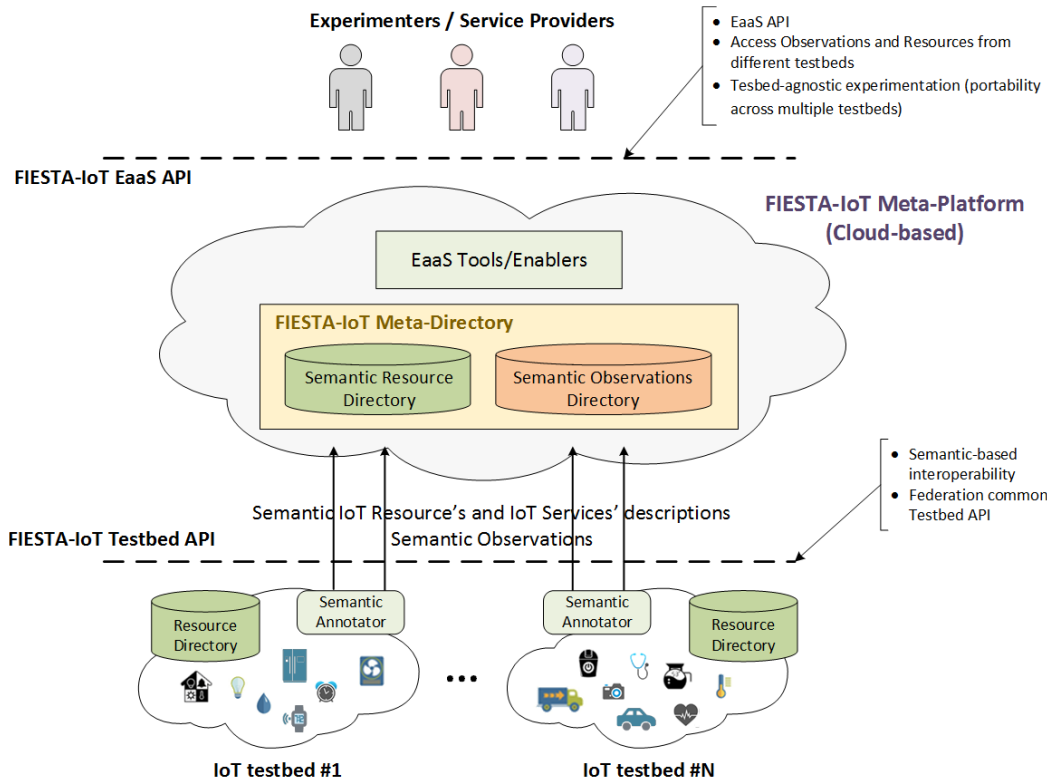


Fig. 4 FIESTA-IoT platform architecture.

This federation approach has a great advantage to produce an API for experimenters that is agnostic to the original producer and semantically accessible. It is needed as the FIESTA-IoT platform does not know how to establish the relationship between the measurements and the information of the different nodes. However, the inclusion of specific developments in each testbed can increase the time-to-federation period for new testbeds. Annotated resources are then injected into the FIESTA-IoT platform through a common API interface.

We can consider a unique layer where the FIESTA-IoT platform develops its central components, the so-called FIESTA-IoT Meta-Platform. This is composed of the FIESTA-IoT Meta-Directory component and a set of tools that are meant to ease the experimentation process and produce a common API, also REST-ful as the rest of the platforms considered in this paper.

The Semantic Resource Directory can be considered the central component in the architecture and is in charge of resource identification and discovery. It is composed of in two directories that gather both, the annotated resource description and the annotated observations. In that sense, the platform not only stores the devices but the observations produced. Both directories provide the registry endpoint, which through HTTP calls new observations and resources can be registered. Additionally, a SPARQL endpoint is also provided, providing an endpoint to discover resources and observations.

Last but not least, FIESTA-IoT platform also considers

the provision of a set of tools to ease the experimentation. Among these tools we can highlight the flow chart functionality, providing the possibility of programming a set of actions that can be performed sequentially in the platform.

### 5. Conclusions

Undoubtedly, considering the growing urban population and the limited resources, the transition from traditional cities to Smart Cities is one of the next big challenges in the world. In that sense, the European Commission is investing a great amount of resources to address the challenge and take the leadership in this matter research. Within this paper, we have thoroughly reviewed the existing solutions in Europe to provide a framework for the research in the field of Smart City paradigm. Hence, the main existing testbed infrastructures for Smart City research have been analyzed in detail, along with the current initiatives in the provision of a framework, such as the FIWARE open platform, for the creation of novel services based on the Internet of Things in the city. Furthermore, the review process has included the current research efforts in the European Union to address interoperability issues related to the myriad of existing heterogeneous IoT technologies and deployments.

### Acknowledgments

This work was funded in part by the European Union’s Horizon 2020 Programme of the FESTIVAL project (Federated

Interoperable Smart ICT Services Development and Testing Platforms) under grant agreement 643275, and from the Japanese National Institute of Information and Communications Technology.

## References

- [1] Publications Office of the European Union, "Europe 2020 flagship initiative innovation union: SEC(2010) 1161," 2011.
- [2] Directorate-General for internal policies, "Assessment of HORIZON 2020 programme," 2016.
- [3] European Commission, "Horizon 2020 work programme 2016 - 2017," 2016.
- [4] "FIRE future Internet research experimentation," <http://www.ict-fire.eu/>, Accessed May 20, 2017.
- [5] S. Paul, J. Pan, and R. Jain, "Architectures for the future networks and the next generation internet: A survey," *Comput. Commun.*, vol.34, no.1, pp.2–42, Jan. 2011.
- [6] "FIWARE," <https://www.ict-fire.eu/>, Accessed May 20, 2017.
- [7] L. Sanchez, L. Muñoz, J.A. Galache, P. Sotres, J.R. Santana, V. Gutierrez, R. Ramdhany, A. Gluhak, S. Krco, E. Theodoridis, and D. Pfisterer, "SmartSantander: IoT experimentation over a smart city testbed," *Computer Networks*, vol.61, pp.217–238, 2014.
- [8] "SmartSantander project," <http://smartsantander.eu/>, Accessed May 20, 2017.
- [9] S. Latré, P. Leroux, T. Coenen, B. Braem, P. Ballon, and P. Demeester, "City of things: An integrated and multi-technology testbed for IoT smart city experiments," *IEEE 2nd International Smart Cities Conference: Improving the Citizens Quality of Life, ISC2 2016 - Proceedings*, 2016.
- [10] C. Adjih, E. Baccelli, E. Fleury, G. Harter, N. Mitton, T. Noel, R. Pissard-Gibollet, F. Saint-Marcel, G. Schreiner, J. Vandaele, and T. Watteyne, "FIT IoT-LAB: A large scale open experimental IoT testbed," *IEEE World Forum on Internet of Things, WF-IoT 2015 - Proceedings*, pp.459–464, 2016.
- [11] "FIT/IoT-LAB: A very large scale open wireless sensor network testbed," <https://www.ict-lab.info/>, Accessed May 20, 2017.
- [12] D. Simeonidou, "Bristol is open," *5G Radio Technology Seminar. Exploring Technical Challenges in the Emerging 5G Ecosystem*, pp.1–32, IET, 2015.
- [13] "Open programmable city," <http://www.bristolisopen.com/>, Accessed May 20, 2017.
- [14] "FIWARE catalogue," <https://catalogue.fiware.org/>, Accessed May 20, 2017.
- [15] T. Zahariadis, A. Papadakis, F. Alvarez, J. Gonzalez, F. Lopez, F. Facca, and Y. Al-Hazmi, "Fiware lab: Managing resources and services in a cloud federation supporting future internet applications," *2014 IEEE/ACM 7th International Conference on Utility and Cloud Computing*, pp.792–799, Dec. 2014.
- [16] "OpenStack cloud operating system," <https://www.openstack.org/>, Accessed May 20, 2017.
- [17] J. Hierro, "FIWARE: An open standard platform for smart cities," <https://www.slideshare.net/JuanjoHierro/fiware-a-standard-platform-or-smart-cities>, Accessed May 20, 2017.
- [18] "IoT backend device management specification," <https://forge.fiware.org/plugins/mediawiki/wiki/fiware/index.php/FIWARE.ArchitectureDescription.IoT.Backend.DeviceManagement>, Accessed May 20, 2017.
- [19] "FI-WARE NGSI-10 open RESTful API specification," [https://forge.fiware.org/plugins/mediawiki/wiki/fiware/index.php/FI-WARE\\_NGSI-10\\_Open\\_RESTful\\_API\\_Specification](https://forge.fiware.org/plugins/mediawiki/wiki/fiware/index.php/FI-WARE_NGSI-10_Open_RESTful_API_Specification), Accessed May 20, 2017.
- [20] "Open mobile alliance," <http://www.openmobilealliance.org/>, Accessed May 20, 2017.
- [21] "FIWARE context broker specification," <https://forge.fiware.org/plugins/mediawiki/wiki/fiware/index.php/FIWARE.OpenSpecification>, Accessed May 20, 2017.
- [22] "CKAN - Open data portal," <https://catalogue.fiware.org/enablers/ckan>, Accessed May 20, 2017.
- [23] "FIWARE complex event processing specification," <https://forge.fiware.org/plugins/mediawiki/wiki/fiware/index.php/FIWARE.ArchitectureDescription.Data.CEP>, Accessed May 20, 2017.
- [24] "FIWARE identity management specification," [https://forge.fiware.org/plugins/mediawiki/wiki/fiware/index.php/FIWARE.ArchitectureDescription.Security.Identity\\_Management\\_Generic\\_Enabler](https://forge.fiware.org/plugins/mediawiki/wiki/fiware/index.php/FIWARE.ArchitectureDescription.Security.Identity_Management_Generic_Enabler), Accessed May 20, 2017.
- [25] "FIWARE authorization PDP specification," <https://forge.fiware.org/plugins/mediawiki/wiki/fiware/index.php/FIWARE.OpenSpecification.Security.AuthorizationPDP>, Accessed May 20, 2017.
- [26] "Open agile smart cities," <http://www.oascities.org/>, Accessed May 20, 2017.
- [27] "Valencia ciudad inteligente – VLCi," <http://vlci.inndeavalencia.com/>, Accessed May 20, 2017.
- [28] "Nova friburgo city as a platform," <http://novafriburgo.cityasplatform.info>, Accessed May 20, 2017.
- [29] "VM9 platform," <http://vm9it.com/vm9-platform.html>, Accessed May 20, 2017.
- [30] "FIWARE success stories," [https://www.fiware.org/success\\_stories](https://www.fiware.org/success_stories), Accessed May 20, 2017.
- [31] "OneM2M," <http://www.onem2m.org>, Accessed May 20, 2017.
- [32] "Open IoT platform," <http://www.openiot.eu>, Accessed May 20, 2017.
- [33] "UNIFY-IoT project," <http://www.unify-iot.eu>, Accessed May 20, 2017.
- [34] "AIOTI initiative," <https://ec.europa.eu/digital-single-market/alliance-internet-things-innovation-aioti>, Accessed May 20, 2017.
- [35] "European research cluster on the Internet of things," <http://www.internet-of-things-research.eu>, Accessed May 20, 2017.
- [36] "International technical working group on IoT-enabled smart city framework," <https://pages.nist.gov/smartcitiesarchitecture/>, Accessed May 20, 2017.
- [37] J.R. Santana, J.A. Galache, T. Akiyama, L. Gurgun, M. Matsuoka, M. Maggio, and S. Murata, "Festival: Towards an intercontinental federation approach," *International Conference on Mobile Networks and Management*, pp.269–280, Springer, 2015.
- [38] "OrganiCity project," <http://organicity.eu/>, Accessed May 20, 2017.
- [39] "FIESTA-IoT project," <http://fiesta-iot.eu/>, Accessed May 20, 2017.
- [40] R. Agarwal, D.G. Fernandez, T. Elsaleh, A. Gyrard, J. Lanza, L. Sanchez, N. Georgantas, and V. Issarny, "Unified IoT ontology to enable interoperability and federation of testbeds," *3rd IEEE World Forum on Internet of Things*, 2016.
- [41] "EuroVoc," <http://eurovoc.europa.eu/drupal/>, Accessed May 20, 2017.
- [42] T. Akiyama, S. Murata, K. Tsuchiya, T. Yokoyama, M. Maggio, G. Ciulla, J.R. Santana, M. Zhao, J.B. Do Nascimento, and L. Gurgun, "Festival: Design and implementation of federated interoperable smart ICT services development and testing platform," *J. Information Processing*, vol.25, pp.278–287, 2017.
- [43] L. Peterson, R. Ricci, A. Falk, and J. Chase, "Slice-based federation architecture (SFA)," *Working draft, version, vol.2*, 2010.
- [44] "sensiNact IoT platform," <https://projects.eclipse.org/projects/technology.sensinact>, Accessed May 20, 2017.
- [45] V. Gutiérrez, E. Theodoridis, G. Mylonas, F. Shi, U. Adeel, L. Diez, D. Amaxilatis, J. Choque, G. Camprodom, J. McCann, and L. Muñoz, "Co-creating the cities of the future," *Sensors*, vol.16, no.11, p.1971, 2016.
- [46] J. Lanza, L. Sanchez, D. Gomez, T. Elsaleh, R. Steinke, and F. Cirillo, "A proof-of-concept for semantically interoperable federation of IoT experimentation facilities," *Sensors*, vol.16, no.7, p.1006, 2016.



**Juan Ramón Santana** is a Telecommunication Engineer graduated in 2010 in the University of Cantabria. He is a research fellow in the Network Planning and Mobile Communications Laboratory, a telecommunication research group from the same university. He has been involved in projects such as SmartSantander, EAR-IT, ClouT or FESTIVAL, European projects related to the Smart City paradigm and the Internet of Things.



**Martino Maggio** got his Computer Science Engineering Master Degree in 2005 from University of Palermo and he started to work as a researcher in Engineering Ingegneria Informatica. He has been involved in several European and Italian research projects: at present he is involved in two EU-Japan collaborative projects: BigClouT and FESTIVAL.



**Roberto Di Bernardo** is an Electronic Engineer and got in 2014 a Master's Degree in "Clinical Engineering" from University of Trieste, while in 2003 a Master's Degree in "Internet Software Engineering" from University of Catania. He has worked as researcher, in Engineering Ingegneria Informatica, in many Italian and European projects. At present, he is involved in WeLive and EU-Japan FESTIVAL projects.



**Pablo Sotres** works as research fellow in the Network Planning and Mobile Communications Laboratory, which belongs to the Communications Engineering department at the University of Cantabria, Spain. He received Telecommunications Engineering degree from the University of Cantabria in 2008. He is currently involved in different European projects framed under the smart city paradigm, such as SmartSantander; and related to inter-testbed federation, such as Fed4FIRE and Fed4FIRE+.



**Luis Sánchez** received both the Telecommunications Engineering and Ph.D. degree by the University of Cantabria, Spain, in 2002 and 2009 respectively. He is assistant professor at the Dept. of Communications Engineering at the same University. He is active on meshed networking on wireless scenarios and optimization of network performance through cognitive networking techniques.



**Luis Muñoz** received both the Telecommunications Engineering degree and Ph.D. from the Polytechnical University of Cataluña (UPC), Spain, in 1990 and 1995, respectively. He is head of the Network Planning and Mobile Communications Laboratory belonging to the Communications Engineering Department (DICOM) at the University of Cantabria, Spain. His research focuses on advanced data transmission techniques, heterogeneous wireless multihop networks and applied mathematical methods for telecommunications. He has participated in several National and European research projects belonging to the 4th, 5th, 6th and 7th Framework Program in which he is technical manager of SmartSantander. He has published over 150 journal and conference papers. He serves as editor of several journals. In parallel to this activity, he serves as consultant for the Spanish Government as well as for different companies in Europe and USA.