



**HORIZON 2020**

The EU Framework Programme for Research and Innovation



## **HORIZONS 2020 PROGRAMME**

### **Research and Innovation Action – FIRE Initiative**

Call Identifier:	H2020–ICT–2014–1
Project Number:	643943
Project Acronym:	FIESTA-IoT
Project Title:	Federated Interoperable Semantic IoT/cloud Testbeds and Applications

## **D5.3 - Experiments Implementation, Integration and Evaluation V2**

Document Id:	FIESTA-IoT-D53-20180630-Draft
File Name:	FIESTA-IoT-D53-20180630-Draft.pdf
Document reference:	Deliverable 5.3
Version:	Draft
Editor:	Juan Ramón Santana Martínez
Organisation:	UC
Date:	30 / 06 / 2018
Document type:	Deliverable
Dissemination level:	PU

Copyright © 2018 FIESTA-IoT Consortium: National University of Ireland Galway - NUIG / Coordinator (Ireland), University of Southampton IT Innovation - ITINNOV (United Kingdom), Institut National Recherche en Informatique & Automatique - INRIA, (France), University of Surrey - UNIS (United Kingdom), Unparallel Innovation, Lda - UNPARALLEL (Portugal), Easy Global Market - EGM (France), NEC Europe Ltd. NEC (United Kingdom), University of Cantabria UNICAN (Spain), Research and Education Laboratory in Information Technologies - Athens Information Technology - AIT (Greece), Sociedad para el desarrollo de Cantabria – SODERCAN (Spain), Fraunhofer Institute for Open Communications Systems – FOKUS (Germany), Ayuntamiento de Santander – SDR (Spain), Korea Electronics Technology Institute KETI, (Korea).

#### **PROPRIETARY RIGHTS STATEMENT**

This document contains information, which is proprietary to the FIESTA-IoT Consortium.  
Neither this document nor the information contained herein shall be used, duplicated or communicated by any means to any third party, in whole or in parts, except with prior written consent of the consortium.

## DOCUMENT HISTORY

Rev.	Author(s)	Organisation(s)	Date	Comments
V01	Juan Ramón Santana	UC	2018/03/12	ToC definition
V011	Flavio Cirillo	NEC	2018/04/03	Data Assembly and Services Portability Experiment
V012	Elias Tragos	NUIG-INSIGHT	2018/04/03	Privacy dashboard section
V013	Rachit Agarwal	Inria	2018/04/05	Added large scale experiment related text
V014	Rachit Agarwal	Inria	2018/04/16	Updates to the large-scale experiment
V02	Juan Ramón Santana	UC	2018/04/19	Update on Dynamic Discovery of IoT Resources for Testbed Agnostic Data Access. Updates on external experiments summaries. Document integration.
V021	Flavio Cirillo	NEC	2018/04/27	Added section 3
V022	Mengxuan Zhao	EGM	2018/05/02	Update section 3
V023	Tarek Elsaleh	SURREY	2018/05/14	Added section 5
V03	Luis Sánchez, Jorge Lanza	UC	2018/05/30	Integrated version including section 1, 6 and 7.
V031	Luis Sánchez, Jorge Lanza	UC	2018/06/12	Updated section 6
V032	Tarek Elsaleh	SURREY	2018/06/12	Updated section 5
Rev	Tiago Teixeira	UNPARALLEL	2018/06/18	Document Review
Rev	Ronald Steinke	FHG-FOKUS	2018/06/22	Document Review
V33	Martin Serrano, Hung Nguyen, Luis Sánchez, Jorge Lanza	NUIG-INSIGHT, UC	2018/06/28	GDPR update
V10	Luis Sánchez, Jorge Lanza	UC	2018/06/28	Final version
V11	Martin Serrano	NUIG-Insight	2018/06/30	Circulated for Approval
Draft	Martin Serrano	NUIG-Insight	2018/06/30	EC Submitted

## TABLE OF CONTENTS

<b>1</b>	<b>EXECUTIVE SUMMARY .....</b>	<b>8</b>
<b>2</b>	<b>IN-HOUSE EXPERIMENTS: IMPLEMENTATION AND INTEGRATION .....</b>	<b>10</b>
2.1	Data Assembly and Services Portability Experiment .....	10
2.1.1	Third year update .....	10
	Cloud-Edge stream processing .....	10
	FIESTA-IoT ontology to NGSI mapping.....	13
	Crowd estimation and mobility analytics (CEMA) New Zealand Deployments.....	17
	CEMA Algorithms.....	19
	CEMA output integration with FIESTA-IoT framework.....	21
2.1.2	Final outcomes .....	21
	Cloud-Edge framework outcome .....	22
	KPIs achievement update .....	25
2.2	Dynamic Discovery of IoT Resources for Testbed Agnostic Data Access.....	26
2.2.1	Third year update .....	27
2.2.2	Final outcomes .....	27
2.3	Large Scale Crowdsensing Experiment .....	27
2.3.1	Third year update.....	28
2.3.2	Final outcomes .....	30
<b>3</b>	<b>EXTERNAL EXPERIMENTS .....</b>	<b>31</b>
3.1	External Experiments Summaries.....	32
3.1.1	Call for Experimenters 1 .....	32
3.1.1.1	IoT data management at the network edge by decentralized community service (DATE) .....	32
3.1.1.2	Smart Polyhedron Indicator for Asset Management .....	32
3.1.1.3	Data Quality and Easy Services Creation in FIESTA-IoT.....	33
3.1.1.4	TALK2FIESTA.....	34
3.1.1.5	CorRelations bEtween Data graphs and IoT topologies (CREDIT) .....	34
3.1.1.6	Smart Monitoring (Pilot Things).....	35
3.1.2	Call for Experimenters 3 .....	36
3.1.2.1	Energy-IoT.....	36
3.1.2.2	Smart IoT Data Collection (BeSmart) .....	37
3.1.2.3	SemantiC Coordination for intelligENT sensors (2CENTS).....	37
3.1.2.4	Smart Urban Routing for FIESTA-IoT (SURF).....	38
3.1.2.5	FINETUNE.....	39
3.1.2.6	Smart Pedestrian movement for Smart Cities .....	40
3.1.2.7	Internet of Things Application for a Better and Smart Comfort (SmartComfort).....	40
3.1.2.8	Knowledge as a Service for Assisted Living in Smart City (KaaS_SCL) .....	41
3.1.2.9	Security and Privacy for IoT infrastructures experiment (SpyIoT).....	42
3.1.2.10	KPI Model for social & business events (REDEvents).....	43
3.1.2.11	Fault Management and Isolation for IoT field devices (FM2I).....	43
3.1.2.12	Monitoring Energy Efficiency for Data Centres by Correlating IoT Sensor Readings and Weather Conditions Data (DC-IoT) .....	43
3.1.2.13	PARKNOW .....	44
3.1.3	Call for Experimenters 4 .....	45
3.1.3.1	Advanced predictive models for energy consumption in Buildings and Data Centers (B-MODEL) .....	45
3.1.3.2	Real-time data quality assessment in IoT environments (StreamingQualityAnalyser) .....	46
3.1.3.3	Experimentation for developing business services that use real-time data analytics for realizing proactive microenvironmental monitoring in agriculture (Agrolytics) .....	47
3.1.3.4	VIRTUS: Virtual IoT Gateway for the provision of SDN-based multi-tenant Service Isolation and Interoperability over Heterogeneous IoT Domains.....	48
3.1.3.5	Distributed Data Stream Process Gateway Service Empowering FIESTA-IoT Applications (StreamGateway).....	49
3.1.4	Rolling Call .....	49
3.1.4.1	LoRa testbed dimensioning and real-time monitoring.....	49
3.2	External Experiments: Functional Evaluation .....	50

3.2.1	Evaluation criteria .....	50
3.2.2	Evaluation results .....	50
	Quantity and quality of the documentation .....	50
	Ease of setting up, ease of deployment .....	51
	During the experiment.....	53
	Ending the experiment .....	54
	Open feedback from experimenters.....	57
	Conclusion .....	57
<b>4</b>	<b>TESTBEDS INTEGRATION.....</b>	<b>58</b>
4.1	Testbeds integration Summaries.....	58
4.1.1	NITOS.....	58
4.1.2	GRIDNET .....	58
4.1.3	ADREAM.....	59
4.1.4	FINE.....	59
4.1.5	Tera4Agri.....	60
4.1.6	RealDC .....	61
4.1.7	Grasse Smart Territory.....	61
4.2	Testbeds Integration: Functional Evaluation.....	62
4.2.1	Evaluation of FIESTA-IoT Resources and Tools .....	62
4.3	Conclusions .....	67
<b>5</b>	<b>FIESTA-IOT PLATFORM: NON-FUNCTIONAL EVALUATION .....</b>	<b>68</b>
5.1	Introduction .....	68
5.2	Probe implementation for performance analysis.....	70
5.3	Analysis of the platform performance.....	71
	Conclusions.....	80
<b>6</b>	<b>PRIVACY PROTECTION AND ITS IMPLICATIONS FOR FIESTA-IOT .....</b>	<b>82</b>
6.1	FIESTA-IoT Technical Assessment .....	82
6.1.1	FIESTA-IoT Web Portal.....	89
6.2	FIESTA-IoT Platform V1.5 (GDPR compliance) .....	90
6.2.1	FIESTA-IoT Security View.....	90
	Data Policy & Data Protection .....	90
	Data Privacy View.....	94
6.2.2	FIESTA-IoT Data Model View .....	94
6.3	Privacy Dashboard (endpoint privacy policies).....	95
6.3.1	Background and motivation .....	95
6.3.2	Component architecture .....	96
6.3.3	User interface .....	98
	4.1.3.1 Data owner .....	98
	4.1.3.2 End user .....	105
6.3.4	Discussion.....	106
<b>7</b>	<b>CONCLUSIONS .....</b>	<b>107</b>
<b>8</b>	<b>REFERENCES .....</b>	<b>108</b>
	<b>ANNEX I QUESTIONNAIRE FOR EXPERIMENTERS.....</b>	<b>109</b>
	<b>ANNEX II QUESTIONNAIRE FOR TESTBEDS.....</b>	<b>116</b>
	<b>ANNEX III LARGE SCALE EXPERIMENT QUERIES.....</b>	<b>124</b>



## LIST OF FIGURES

Figure 1. Smart City Magnifier architecture with the FIWARE stream processing framework FogFlow.....	12
Figure 2. Processing task topology for the Smart City Magnifier. ....	13
Figure 3. Mapping between ontology the FIESTA-IoT ontology to NGSI. Each FIESTA-IoT observation is mapped to a NGSI Context Element. ....	14
Figure 4. Lab experiments with stereoscopic camera. Left: The camera on the office room door. Right: The viewing angle of the camera.....	18
Figure 5. Stereoscopic camera deployment places in Wellington Railway Station. Left: Example platform entrance gates (entrance), right: Views from the opposite side (exit).....	19
Figure 6. Schematic deployment with three compound devices.....	19
Figure 7. Extension dashboard of the Smart City Magnifier offered by FogFlowt. ....	22
Figure 8. Smart City Magnifier dashboard for New Zealand data.....	23
Figure 9. Visualization dashboard for the Wellington Railway Station. ....	24
Figure 10. Screenshot of the Dynamic Discovery application.....	26
Figure 11. Large scale crowdsourcing experiment use case 1 (noisy locations) (a) all recently collected samples, (b) zoomed in view of Santander region. ....	29
Figure 12. Large scale crowdsourcing experiment use case 3 (recent sound samples in an area).....	30
Figure 13. Pilot Things dashboard. ....	35
Figure 14. PARKNOW application. ....	45
Figure 15. Documentation consulted; on the left side is the quantification of the document consulted among the available one, on the right side is the assessment of the quality of documentation.....	50
Figure 16. Quality and relevance of documentation. ....	51
Figure 17. Time for integration. ....	51
Figure 18. Assessment on FIESTA-IoT tools.....	52
Figure 19. Usage of API or Experimental portal. ....	52
Figure 20. Assessment over the platform and experimental portal.....	53
Figure 21. Usage of the different support channels.....	53
Figure 22. Feedback over the usage of the ticketing system.....	54
Figure 23. Overall satisfaction of experimenters. ....	54
Figure 24. Market appealing of the FIESTA-IoT platform. ....	55
Figure 25. Documentation evaluation. ....	63
Figure 26. Quality and Relevance of the Documentation. ....	63
Figure 27. Testbed integration evaluation. ....	64
Figure 28. Support Evaluation. ....	65
Figure 29. Overall Experience Evaluation.....	65
Figure 30. Evaluation of Future Plans.....	66
Figure 31. FIESTA-IoT recommendation.....	66
Figure 32. Probes integration for FIESTA-IoT performance analysis.....	69

Figure 33. Data Readings vs Data Writings against the platform .....	72
Figure 34. (Left) Data Readings vs Wrong Formatted Calls and Server Errors. (Right) Data Writings vs Wrong Formatted Calls and Server Errors.....	72
Figure 35. Data readings per day.....	73
Figure 36. Data writings per day. ....	73
Figure 37. Data readings and data writings per day. ....	74
Figure 38. Cumulative Probability Function of processing times for data readings.....	75
Figure 39. Probability of different processing times for data readings limited to 90% of the queries. ....	75
Figure 40. Probability of different processing times for data readings limited to 50 ms.....	76
Figure 41. Cumulative Probability Function of processing times for data writings. ....	77
Figure 42. Probability of different processing times for data writings limited to 90% of the queries. ....	77
Figure 43. Probability of different processing times for data writings limited to 100 ms. ....	78
Figure 44. Unique users per day taking into account IPs sources.....	78
Figure 45. Unique users per day taking into account user agents.....	79
Figure 46. Percentage of the calls performed from the localhost vs all other IPs sources....	79
Figure 47. Countries accessing the platform based on the IPs geolocation. ....	81
Figure 49. FIESTA-IoT Architecture with Security - Current Version.....	83
Figure 50. FIESTA-IoT Login portal. ....	89
Figure 51. FIESTA-IoT Architecture GDPR Compliance – 1.5 Version.....	90
Figure 51. IoT-Registry new TDB structure .....	91
Figure 51. Restricting access to IoT-Registry information .....	92
Figure 51. SPARQL request procedure.....	93
Figure 52. FIESTA-IoT Data Model Extensions for GDPR Compliance Check.....	95
Figure 53. Privacy dashboard overall architecture. ....	97
Figure 54. Initial screen of the data owner privacy component.....	99
Figure 55. Setting policies per user.....	100
Figure 56. Single endpoint policy initial screen. ....	101
Figure 57. Setting policies per user for single sensor. ....	101
Figure 58. List of shared devices. ....	102
Figure 59. Consent request list. ....	103
Figure 60. Consent request information.....	103
Figure 61. Approve or reject a consent request.....	104
Figure 62. Access log list.....	104
Figure 63. Sensor explorer initial screen.....	105
Figure 64. Declaring the purpose for the consent request.....	106

## LIST OF TABLES

Table 1. Open-Calls Experiments sorted by domain.....	8
Table 2. Number of sensors deployed in the two test sites.....	18
Table 3. Mapping between CEMA output and FIESAT-IoT ontology. ....	21
Table 4. Evaluation of the Data Assembly and Service Portability through KPIs for the Y3. ....	25
Table 5. Number of Experiments and Testbeds integration in the different Open-Calls. ....	31
Table 6. Tools validated by third-parties experimenter. An X indicates a full validation, a + indicates a partial validation. ....	56
Table 7. “sparq_query_execution_log” table with the information gathered from requests.....	70
Table 8. "semantic_storage_log" table with the information gathered from observation injection requests. ....	71
Table 9. Features from data readings per day. ....	74
Table 10. Features from data writings per day.....	74
Table 11. Unique users per day based on the source IPs.....	79
Table 12. Unique users per day based on the user agents.....	80
Table 13. Experiment duration based on the calls performed by the different IPs. ....	80
Table 14. Experiment duration based on the calls performed by the different IPs (without taking into account the localhost).....	80
Table 15. Number of queries per IP. ....	80
Table 16. Features of number of queries per IP (without taking into account the localhost).....	80
Table 17. FIESTA-IoT identified functionalities from DPIA.....	84

## TERMS AND ACRONYMS

API	Application Program Interface
CM	Context Management
CEP	Complex Event Processing
DB	Database
DC	Data Centres
DoW	Description of Work
DSL	Domain Specific Language
EaaS	Experiment as a Service
EEE	Experiment Execution Engine
EMC	Experiment Management Control
EDR	Experiment Data Receiver
ERM	Experiment Registry Module
FED-Spec	FIESTA-IoT Experiment Description
FEMO	FIESTA-IoT Experiment Model Object
FIRE	Future Internet Research and Experimentation
FISMO	FIESTA-IoT Service Model Object
GE	Generic Enabler
GEri	Generic Enabler reference implementation
GDPR	General Data Protection Regulation
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol
ID	Identifier
IoT	Internet of Things
KPI	Key Performance Indicator
NGSI	Next Generation Service Interface
OC	Open-Call
OCTP	Open-Call Testbed Providers
QoE	Quality of Experience
SCM	Smart City Magnifier
SMG	Semantic Mediation Gateway
SPARQL	SPARQL Protocol and RDF Query Language
UI	User Interface
VE	Virtual Entity
WP	Work Package
WSN	Wireless Sensor Network

## 1 EXECUTIVE SUMMARY

The present document is reporting about the works carried out within work package 5 (WP5). More precisely including the in-house experiments updates (task T5.2) and the validation and evaluation of the experiments (task T5.4).

In contrast to the deliverable D5.2, this document focuses on the integration of third-party's experiments from the four Open-Calls carried out during the project and the platform evaluation from their experience. However, in-house experiments are also described in this deliverable, in order to include the updates carried out on each of them, as well as the differences in the platform evaluation regarding to the first version of the platform and its final version.

### Third-party's experiments and Four Open-Calls:

As aforementioned, this deliverable includes a deeply analysis of the third-party's evaluation of the platform, including both, experiments and testbeds, through the analysis of the surveys provided by them at the end of the experiments and testbeds integration. Furthermore, this deliverable also includes the publishable summaries delivered by these experiments.

*Table 1. Open-Calls Experiments sorted by domain.*

Domain	Experiment
<b>Smart City</b>	SURF: Smart Urban Routing for Fiesta-IoT
	Smart Pedestrian movement for Smart Cities
	PARKNOW
	REDEvents: KPI Model for social & business events
	SmartComfort
	Knowledge as a Service for Assisted Living in Smart City
<b>Smart Energy</b>	Energy-IoT
	B-MODEL: Advanced predictive models for energy consumption in Buildings
	BeSmart: Smart IoT Data Collection
	DC-IoT: Monitoring Energy Efficiency for Data Centres
<b>Smart Agriculture</b>	Agrolytics
<b>Data Science</b>	StreamingQualityAnalyser
	FINETUNE
	FM2I: Fault Management and Isolation for IoT field devices

	DataQuest: Data Quality and Easy Services Creation in FIESTA-IoT
	CREDIT: CorRelations bEtween Data graphs and IoT topologies
	Pilot Things: Smart Monitoring
<b>Data Representation</b>	SPIAM: Smart Polyhedron Indicator for Asset Management
<b>IoT Platforms</b>	DATE: IoT data management at the network edge by decentralized community service
	TALK2FIESTA
	StreamGateway
<b>IoT Networking</b>	2CENTS: SemantiC Coordination for intelligENT sensors
	VIRTUS: Virtual IoT Gateway for the provision of SDN-based multi-tenant Service Isolation and Interoperability over Heterogeneous IoT Domains

On the other hand, in order to accomplish the analysis, in addition to the functional evaluation of the platform through the analysis of the different surveys, the deliverable also includes a thoroughly analysis of the platform performance during the third-party's experimentation. This non-functional analysis has been carried out by analysing the statistics stored in the platform during the semantic calls performed by the experimenters and testbeds.

### General Data Protection Regulation (GDPR) Analysis

It is worth mentioning that the present document also addresses the technical updates in regard to the privacy considerations looking for paving the way for aligning the FIESTA-IoT Platform design with the requirements derived from the new General Data Protection Regulation (GDPR). In this regard, this deliverable also includes the “privacy dashboard”, which addresses the issue of sharing sensitive data with specific users. Through this tool, testbed owners can apply specific policies to datasets that cannot be shared publicly with all the platform users.

The deliverable is structured as follows. Section II presents the latest updates in the in-house experiments, integrated during the last year. Section III describes the analysis carried out on top of the surveys provided by the experimenters, providing a thoroughly functional evaluation of the platform. While Section III is focused on the experiment plane, Section IV focuses on the non-functional analysis from the feedback received by the testbeds, which were integrated into the FIESTA-IoT platform. Section V includes the non-functional analysis of the platform through the review of the performance of the platform during the last Open-Calls activities. Section VI is focused on the technical developments regarding to the new GDPR, including the description of the “privacy dashboard” component. Finally, Section VII provides the conclusions, with which the present report is closed.

## 2 IN-HOUSE EXPERIMENTS: IMPLEMENTATION AND INTEGRATION

This section describes the three in-house experiments. More precisely, it describes the new updates performed on top of the experiments since the last report in (FIESTA-IoT D5.2, 2017).

### 2.1 Data Assembly and Services Portability Experiment

The Data Assembly and Service Portability experiment has been shaped as a smart city application, named Smart City Magnifier, which is capable of analysing and reporting situations of a city with different level of details on multiple degrees of freedom such as geographic scope and abstraction (that goes from sensor level till building, city or country level).

#### 2.1.1 Third year update

During the last year of FIESTA-IoT project the backend part of the Data Assembly and Service Portability experiment has changed a lot. Whilst the version of Y2 of the experiment was at an embryonal phase where the core analytics technology was a monolithical component more suited to be ran on cloud, now the system is much more evolved and based on a different computing paradigm which foresees the modularization of analytics component in simple tasks for easy offloading computation to the middle layer components which are IoT gateways and edge/core networks, called Fog Computing (Bonomi, Milito, Zhu, & Addepalli, 2012).

For this purpose, we have integrated a brand-new framework of the FIWARE ecosystem FogFlow GE<sup>1</sup>.

With the adoption of this new approach we aimed to have an easy extensible smart city framework where even third parties can participate on developing new data stream analytics. The deployment of analytics function is now agile and can be done at runtime and on demand of users.

Furthermore, we have made real trials of our Smart City Magnifier in partnership with the NEC unit in New Zealand in the cities of Wellington and Christchurch. Their major interest was to monitor the situations within the city in the realm of crowd estimation and mobility of crowd. For that reason, stereoscopic camera and Wi-Fi monitoring sensors have been deployed in multiple test fields. Due to the big amount of raw data produced, significant effort has been made in order to integrate the data produced in FIESTA-IoT by the implementation of analytics algorithm for aggregating data and then be able to visualize the data in the Smart City Magnifier dashboard.

#### Cloud-Edge stream processing

FogFlow is a distributed execution framework to support dynamic processing flows over cloud and edges. It can dynamically and automatically compose multiple NGSI-based data processing tasks to form high level IoT services, and then orchestrate and optimize the deployment of those services within a shared cloud-edge environment, with regards to the availability, locality, and mobility of IoT devices.

---

<sup>1</sup> <https://catalogue.fiware.org/enablers/fogflow>



Processing tasks are packed in docker<sup>2</sup> containers and are automatically pulled by the system from a shared Docker repository (e.g. DockerHub).

A view of the new experiment architecture can be seen in Figure .

- The **FogFlow** framework that is handling the dynamic allocation of stream processing tasks to computing nodes.
- On the bottom it is possible to see the FIESTA-IoT platform as data provider. **The Semantic Mediation Gateway** (SMG) component is in charge to retrieve IoT data from the FIESTA platform and mapping it to NGSI.
- The **NGSI Nominatim** is an NGSI service that exposes an NGSI interface to which a NGSI-10 query can be used in order to request the associations of a geographic point to a set of real geographic items touched by such point. The system is using the OpenStreetMap Nominatim service as a remote service.
- A **Persistent Context Management** for storing historically the data with persistence since the FogFlow framework is working only on runtime and on data flows. We have chosen to add this component in order to have backup data for the dashboard in case of lost connection.
- A **dashboard** for showing the results of the analytics. The dashboard is pretty similar to the one created up to Y2.
- Several **processing tasks**:
  - **Contextualizer task**: it associates virtual entities, making usage of the NGSI Nominatim service, to the incoming observations flowing from FIESTA-IoT. Contextualizing, in this scope, is the act of inferring the location context (e.g. a building, a street, a square, a suburb, a city etc.) to which each geotagged observation belongs.
  - **Aggregator task**: it aggregates the incoming observations from FIESTA-IoT by the virtual entities. The aggregation makes usage of statistics means.
  - **IoT quality of deployment task**: it calculates the quality of the deployment (in the form of number of resources, geographical density of resources, etc.,) for each of the virtual entities contextualized.
  - **IoT deployment monitor task**: it monitors the amount of observations coming from resources from each the virtual entities contextualized.

The processing tasks are places in a topology similar to the one shown in Figure , where:

- 2 input streams enable the flow of observations and resources in the analytics tasks
- A *contextualizer* task that is in charge of contextualize the resource and/or the pushed observation by the means of the external NGSI-Nominatim service and produce as output the associations between the observation and/or resource and virtual entities.
- A *stats* task that takes as input observations and association between sensors and virtual entities, and computes as output stats for each of the attribute
- A *qualityofdeployment* task that takes as input the resources and the associations between resources and virtual entity, and computes the quality of deployment parameters for each of the virtual entities like number of sensor of a certain type, density of sensors of a certain type, etc.

---

<sup>2</sup> [www.docker.io](http://www.docker.io)



- A *monitorofdeployment* task that takes as input statistics of the observations for each of the virtual entities (output of the *stats* task) and the quality of deployment parameters (output of the *qualityofdeplotment* task) and monitor the activity of the sensor through the time.

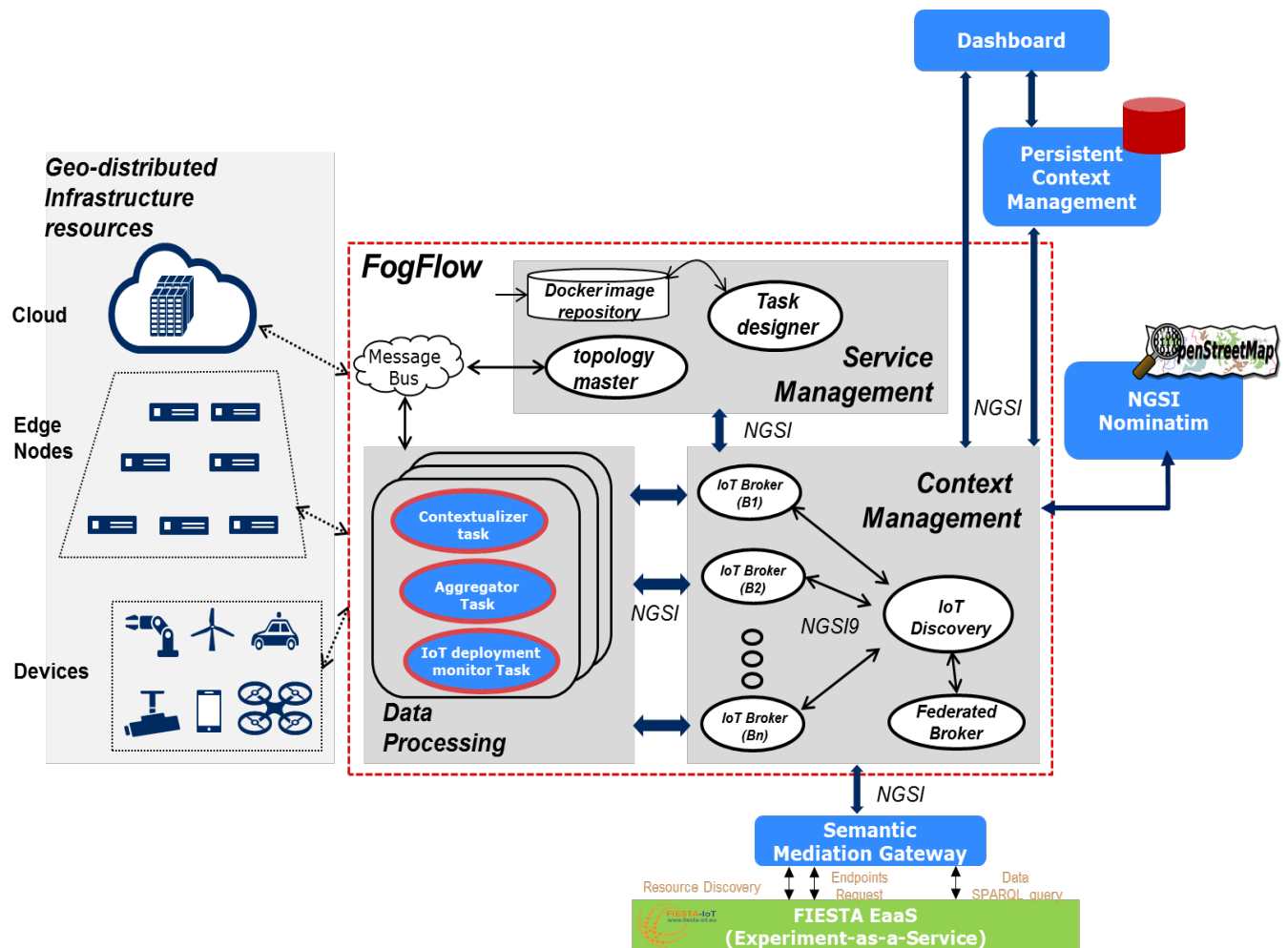


Figure 1. Smart City Magnifier architecture with the FIWARE stream processing framework FogFlow.

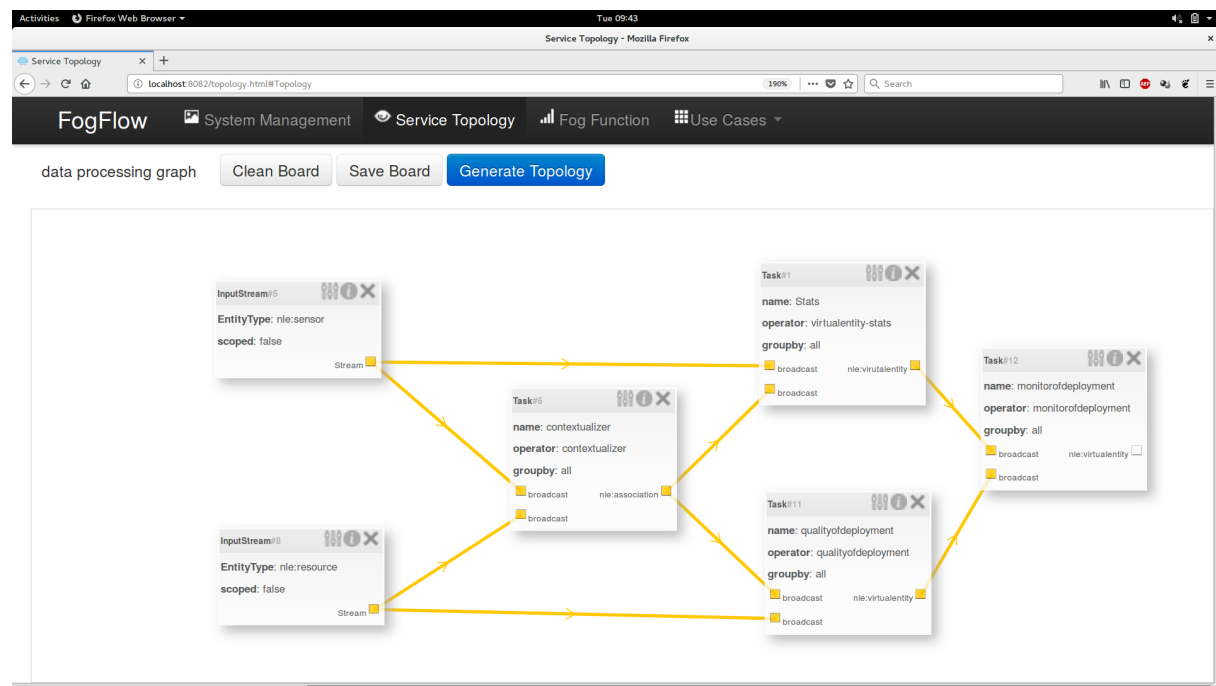


Figure 2. Processing task topology for the Smart City Magnifier.

## FIESTA-IoT ontology to NGSI mapping

In order to have the data accessible by a FIWARE component, it is necessary to make a mapping between the FIESTA-IoT ontology and NGSI (see Figure ).

Here is the mapping:

- Each FIESTA-IoT observation is mapped to a NGSI *ContextElement*.
  - The *EntityId* of the Context Element is formed by:
    - The *entityId* name mapped to the *ssn:sensor* name
    - The *entityId* type mapped to the *rdf:type* of the *ssn:sensor*
    - The *entityId* *isPattern* set to false
  - A *DomainMetadata* for the geo location of the sensor
    - The *metadata* name set to SimpleGeoLocation
    - The *metadata* type set to point
    - The *metadata* value as a pair of latitude and longitude
      - Lat mapped to *geo:lat*
      - Long mapped to *geo:long*
  - A *ContextAttribute* for the observation value
    - The *attribute* name mapped to *qu:quantityKind*
    - The *attribute* type mapped to *du:hasDataValue*
    - The *attribute* *contextValue* mapped to the *ssn:observationValue*
  - An *AttributeMetadata* for the timestamp
    - The *metadata* name set to *creation\_time*
    - The *metadata* type set to string
    - The *metadata* value set to *time:instant*
  - Another *AttributeMetadata* for the unit

- The *metadata name* set to Unit
- The *metadata type* set to string
- The *metadata value* set to *qu:unit*

It is worth to notice that the location of the observation is used as a Domain Metadata since it is assumed that the data retrieved from the knowledge base is coming from fixed sensors. This approach has been adopted in order to eliminate redundancy. In fact, in case of time-series query to the FIWARE IoT Platform, the platform is handling and retrieving only one geo location for the whole EntityId and not the same geo location for each of the ContextAttribute of the same EntityId. The same logic applies in case of different types of attribute value.

In case the observation is coming from moving sensors (e.g. buses or cars), then the Domain Metadata should become an Attribute Metadata of the specific Context Attribute.

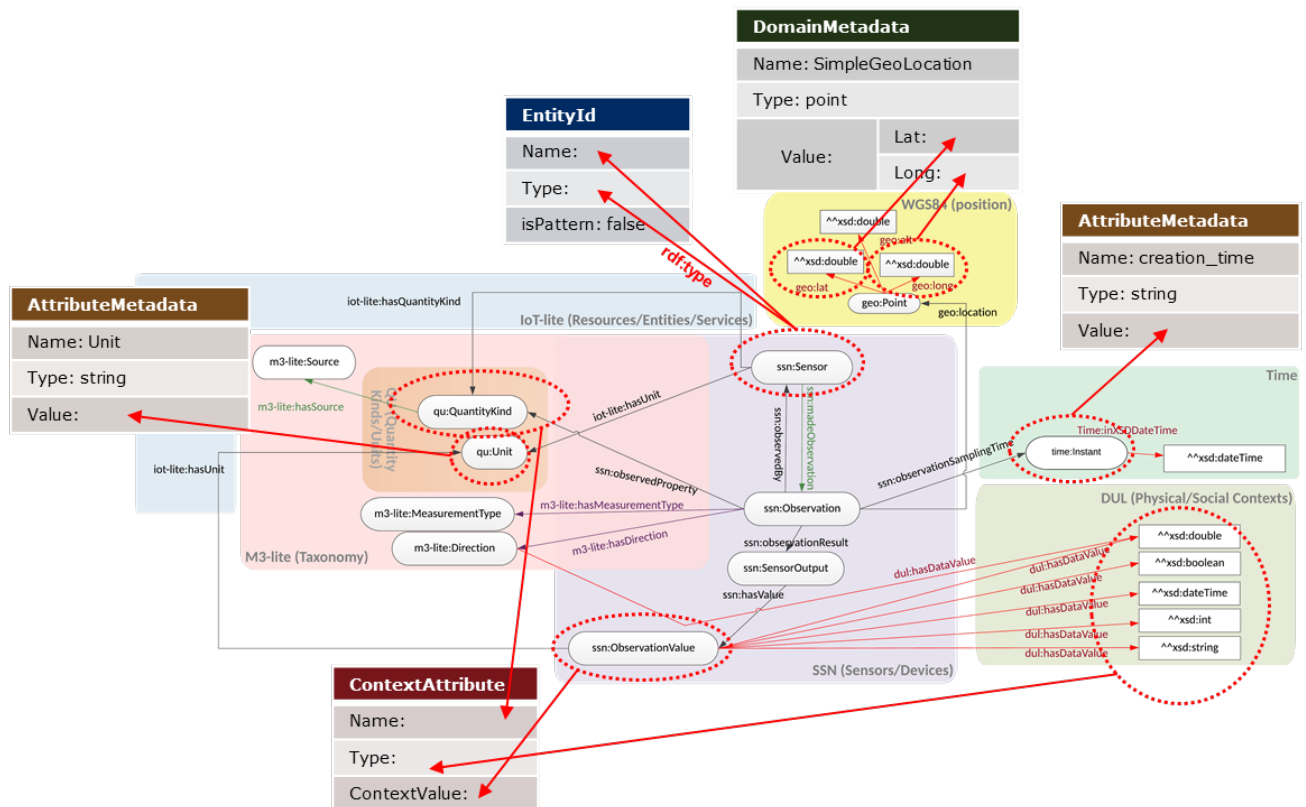


Figure 3. Mapping between ontology the FIESTA-IoT ontology to NGSI. Each FIESTA-IoT observation is mapped to a NGSI Context Element.

An example of a query to FIESTA-IoT is the following:

REQUEST
HTTP POST to: <a href="https://platform.fiesta-iot.eu/iot-registry/api/queries/execute/global">https://platform.fiesta-iot.eu/iot-registry/api/queries/execute/global</a>
Content-Type: text/plain
Accept: application/json

*iPlanetDirectoryPro: {{token}}*<sup>3</sup>

```

Prefix ssn: <http://purl.oclc.org/NET/ssnx/ssn#>
Prefix iot-lite: <http://purl.oclc.org/NET/UNIS/fiware/iot-lite#>
Prefix dul: <http://www.loa.istc.cnr.it/ontologies/DUL.owl#>
Prefix geo: <http://www.w3.org/2003/01/geo/wgs84_pos#>
Prefix time: <http://www.w3.org/2006/time#>
Prefix m3-lite: <http://purl.org/iot/vocab/m3-lite#>
Prefix xsd: <http://www.w3.org/2001/XMLSchema#>
Prefix rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#>
SELECT ?qkClass ?lat ?long ?time ?sensor ?dataValue ?sensorType ?unit
WHERE {
    ?observation a ssn:Observation .
    ?observation geo:location ?point .
    ?point geo:lat ?lat .
    ?point geo:long ?long .
    ?observation ssn:observationResult ?sensOutput .
    ?sensOutput ssn:hasValue ?obsValue .
    ?observation ssn:observedBy ?sensor .
    ?observation ssn:observedProperty ?qk .
    ?obsValue dul:hasDataValue ?dataValue .
    ?observation ssn:observationSamplingTime ?instant .
    ?instant time:inXSDDateTime ?time .
    ?qk rdf:type ?qkClass .
    ?sensor a ?sensorType .
    ?obsValue iot-lite:hasUnit ?unitNode .
    ?unitNode a ?unit .

    FILTER((xsd:dateTime(?time) > "2018-03-16T16:00:00+01:00"^^xsd:dateTime) && (xsd:dateTime(?time) < "2018-03-16T17:00:00+01:00"^^xsd:dateTime))
}

```

<sup>3</sup> The FIESTA-IoT platform is protected with a security system. Only registered users can access the services.

RESPONSE
<pre>{   "vars": [     "qkClass",     "lat",     "long",     "time",     "sensor",     "dataValue",     "observation",     "sensorType",     "unit"   ],   "items": [     {       "qkClass": "http://purl.org/iot/vocab/m3-lite#RoomTemperature",       "lat": "5.12433445E1^^http://www.w3.org/2001/XMLSchema#double",       "long": "-5.932438E-1^^http://www.w3.org/2001/XMLSchema#double",       "time": "2018-03-16T15:34:00Z^^http://www.w3.org/2001/XMLSchema#dateTime",       "sensor": "https://platform.fiesta-iot.eu/iot-registry/api/resources/RT2l7eU-zvt4HnUsE-92ELwPUO9WAd1LMhabTRlpmbpkcybV1VHFSYww7Zf0mh_mgbQ6fTf9DAUPSUsrMq2mfS1DEOR9MLe6Ezt6IM5eBmtc6rMUEQ7EunS-XRUH96qD",       "dataValue": "2.356E1^^http://www.w3.org/2001/XMLSchema#double",       "sensorType": "http://purl.org/iot/vocab/m3-lite#Thermometer",       "unit": "http://purl.org/iot/vocab/m3-lite#DegreeCelsius"     },     ....     ....   ] }</pre>

The mapped NGSI ContextElement (JSON binding):

<pre>{   "entityId": {     "id": "https://platform.fiesta-iot.eu/iot-registry/api/resources/RT2l7eU-zvt4HnUsE-92ELwPUO9WAd1LMhabTRlpmbpkcybV1VHFSYww7Zf0mh_mgbQ6fTf9DAUPSUsrMq2mfS1DEOR9MLe6Ezt6IM5eBmtc6rMUEQ7EunS-XRUH96qD",     "type": "http://purl.org/iot/vocab/m3-lite#Thermometer",     "isPattern": false   } }</pre>
--

```

},
"domainMetadata": [{
  "name": "SimpleGeolocation",
  "type": "point",
  "value": {
    "latitude": 51.243343,
    "longitude": -0.5932438
  }
}],
"attributes": [{
  "name": "http://purl.org/iot/vocab/m3-lite#RoomTemperature",
  "type": "http://www.w3.org/2001/XMLSchema#double",
  "contextValue": "23.56",
  "metadata": [{
    "name": "creation_time",
    "value": "2018.03.16 15:43:07:000Z",
    "type": "string"
  }, {
    "name": "Unit",
    "value": "http://purl.org/iot/vocab/m3-lite#DegreeCelsius",
    "type": "string"
  }]
}]
}

```

### Crowd estimation and mobility analytics (CEMA) New Zealand Deployments

We developed a real-time system for **C**rowd **E**stimation and **M**obility **A**nalytics (CEMA) for monitoring crowd mobility in two test sites in New Zealand. CEMA uses multi-modal data using Wi-Fi sniffers (motes) and stereoscopic cameras. Wi-Fi sniffers listen and collect Wi-Fi probe requests which are broadcasted from Wi-Fi-enabled mobile devices (e.g., smartphones) of the pedestrians, whereas the stereoscopic camera is used for counting people at certain areas to calibrate the Wi-Fi measurements. The testing of the prototype system is first conducted in the lab environment to see the accuracy of the stereoscopic camera. Figure shows the setup for the stereoscopic camera which counted people entering to the office room or leaving the office room. The experiment took place in NEC Laboratories Europe, Heidelberg.



Figure 4. Lab experiments with stereoscopic camera. Left: The camera on the office room door. Right: The viewing angle of the camera.

The CEMA system is tested in two large-scale pilot sites in New Zealand. The first testing site is the Re:START shopping mall in Christchurch. The RE:Start mall is an open-area shopping mall which was built in short time by using containers. The second testing site is Wellington Railway Station in Wellington. Wellington Railway Station is the main train station of Wellington visited by many train passengers every day. The Re:START mall had 5 Wi-Fi motes and 1 stereoscopic camera deployed (at the main entrance pedestrian way), whereas the train station had 4 Wi-Fi motes and 4 stereoscopic cameras. The entrance to the platforms in the train station contains 4 gates and therefore 4 cameras are deployed for accurate counting of the number of passengers.

The Wi-Fi motes placed in the areas of interest such as different landmarks/locations in the shopping mall, the main hall in the train station, or exit places of the train station. The stereoscopic cameras are placed in areas which we call “calibration choke points”. Calibration choke points are pre-selected based on the expected areas where most (if not all) pedestrians passed through. For instance, as can be seen in Figure , the entrance gates to the platforms are used as a calibration area. The passengers who take the train need to pass through these points. In the calibration choke points, Wi-Fi mote(s) and stereoscopic camera(s) are placed together for accurate counting and dynamic correlation.

	Test Site 1 RE:START mall	Test Site 2 Wellington Railway St.
<b># motes</b>	5	4
<b># Stereoscopic cameras</b>	1	4
<b># NEC Kite device (Gateway)</b>	1	1

Table 2. Number of sensors deployed in the two test sites.





Figure 5. Stereoscopic camera deployment places in Wellington Railway Station. Left: Example platform entrance gates (entrance), right: Views from the opposite side (exit).

### CEMA Algorithms

Since the amount of the data generating by this installation is too abundant and too much verbose, we have developed an analytics module in order to share with the FIESTA-IoT framework only the crowd estimation and mobility analysis.



Figure 6. Schematic deployment with three compound devices.

The CEMA real-time system currently includes 3 data analytical modules. These data analytical modules support real-time and offline analytics. Each module has the



implementation of an algorithm for crowd mobility behaviour estimation. The data analytical modules are listed as follows.

- **Crowd estimation:** CEMA crowd estimation is based on dynamically correlating multi-modal data. Currently two data types are used: 1) Wi-Fi probes (signals received with Wi-Fi motes), 2) count-in and count-out events (values received from the stereoscopic cameras). The algorithm dynamically correlates these two types of inputs in the pre-defined calibration choke points. We use the approach called dynamic proportional calibration, which is based on having certain time intervals where the calibration is done based on the proportion of count-in and count-out events as well as the number of distinct Wi-Fi probes (probes with different MAC addresses). Then, the computed correlation is applied to the nearby Wi-Fi mote areas where the stereoscopic camera is not deployed. The idea is to use a limited number of stereoscopic cameras and improve the accuracy of the Wi-Fi-only approach in a larger scale by deploying Wi-Fi motes.
- **Stay duration:** Stay duration algorithm computes the average stay durations as well as the total number of stays in a certain area. The “stay” is defined with a threshold such that if a person waits for longer than a certain time, the person is assumed to be waiting (staying) in the area. On the other hand, if a device is detected only for a couple of seconds, the person is assumed to be passing by as opposed to staying. The area of computation is defined as the expected transmission range of a Wi-Fi mote. In other words, stay duration makes the computation for each Wi-Fi mote, for the circular Wi-Fi-range area of the mote. The outputs of the stay durations for each Wi-Fi mote are independent from each other. The algorithm is based on detecting a signal in a certain time period (e.g., real-time or offline). In the real-time case, the detected signal is then backtracked through time to compute a device’s waiting time in the area (e.g., 30 minutes). The computation is then applied to all detected devices in the similar fashion and the algorithm outputs the number of waits). In the offline-case, a forward-tracking mechanism is also implemented along with back-tracking through time.
- **People flow:** The people flow module is used for understanding the movement directions of the crowd. For instance, in the case of Re:START mall, the interest of the stakeholder was to understand what type of movement behaviours the customers had inside the open-area mall. The people flow module correlates information coming from multiple Wi-Fi motes to detect a unique device in two different Wi-Fi mote areas through time. The algorithm simply outputs the estimated number of people moving from one Wi-Fi mote area to another.

A major consideration of the designed CEMA system is to protect the privacy of the people and anonymization techniques to analyse certain crowd behaviours. First of all, the algorithms designed for understanding “crowd behaviour” as opposed to “an individual’s behaviour”. The output results of CEMA only contains values such as “average stay duration of people in Wi-Fi mote 1 area is 10 minutes” or “number of people visiting the shopping mall in a morning hour is 100 compared to lunch time which is 300”. Moreover, we implement salting and hashing mechanisms for the MAC addresses of the devices. For instance, devices can only send the hashed and salted

MAC addresses to the cloud server. Similarly, stereoscopic camera has an in-built software which only counts the moving objects from the top-angle (e.g., no face detection or body type recognition) and the device only sends the count-in and count-out events in a certain time period. Lastly, the CEMA system does not collect any image or video to be stored in the cloud. The deployment setups are based on the EU regulations as well as the regulations of New Zealand. This approach of privacy-preserving compared to state-of-art approaches such as detecting faces in a corridor and saving videos in the cloud.

### CEMA output integration with FIESTA-IoT framework

The result of the CEMA algorithm has been finally integrated with the FIESTA-IoT ontology. The mapping is shown in Table .

*Table 3. Mapping between CEMA output and FIESAT-IoT ontology.*

	<b>Crowd estimation</b>	<b>Stay Count</b>	<b>Stay Duration</b>	<b>People flow</b>
<b>Sensing Device</b>	People Count Sensor	Staying People Count Sensor	People Stay Duration Sensor	People Flow Count Sensor
<b>Sensor location</b>	geo:location point	geo:location point	geo:location point	geo:location point
<b>Sensor coverage</b>	hasCoverage circle/rectangle/polygon	hasCoverage circle/rectangle/polygon	hasCoverage circle/rectangle/polygon	-
<b>Observation quantity kind</b>	Count People	Count People Staying	People Stay Duration Average	Count People Moving
<b>Observation unit</b>	Item	Item	Seconds	Item
<b>Observation hasDirection</b>	-	-	-	Direction Azimuth

### 2.1.2 Final outcomes

- Flexible analytics platform, open to new extensions for new city indicators by the implementation of atomic stream processing tasks and definition of their interactions through a topology
- Integration of IoT systems from 2 new cities Christchurch and Wellington
- Real trials.

The new outcome of Y3 from Smart City Magnifier is presented in three subsections, first the outcome on the usage of an edge-cloud analytics framework, then the outcome of the New Zealand integration and finally a new assessment of the KPIs for T3.

## Cloud-Edge framework outcome

The integration of the cloud-edge stream processing framework for handling the Smart City Magnifier analytics brought flexibility on the extension of data processing side. It opened the system to be extensible in an agile manner. New city indicators can be implemented as a topology of atomic stream processing tasks, as seen in Figure 2. Processing tasks are simply packaged in Docker containers and are automatically downloaded, on the needs, by the FogFlow system from a shared repository (for example DockerHub).

A topology can be simply pushed as an NGSI-10 message to the FogFlow framework or designed with a graphical UI (see Figure 7).

In order to trigger the actual deployment of the topology towards the available computing node, a simple NGSI-10 request suffices.

The screenshot shows the FogFlow web interface. The top navigation bar includes 'FogFlow', 'System Management', 'Service Topology', 'Fog Function', and 'Use Cases'. The main content area is titled 'to design a service topology'. On the left, there is a sidebar with 'Topology', 'Requirement', and 'Editor' tabs. The main form contains the following fields:

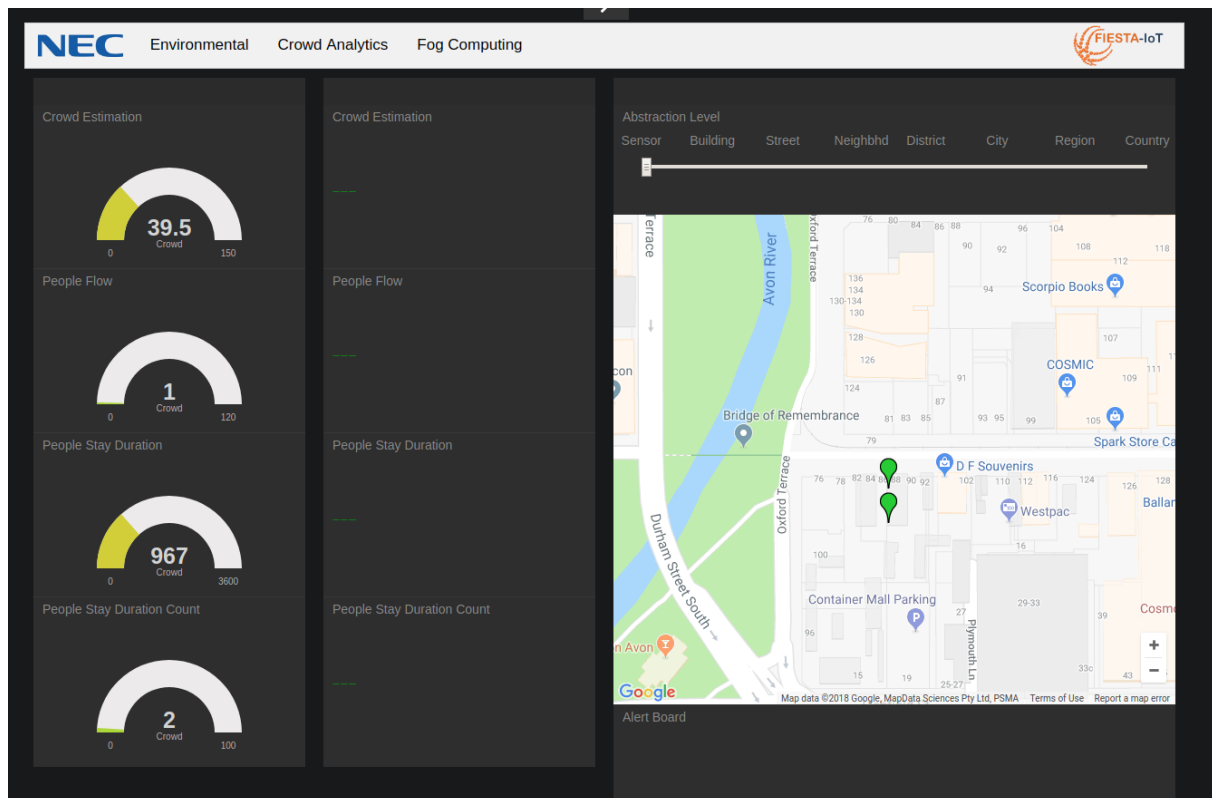
- topology name:** Complex-VirtualEntities-Stats
- service description:** Complex-VirtualEntities-Stats
- priority:** low
- resource usage:** inclusive

Below these fields are three buttons: 'Clean Board', 'Save Board', and 'Generate Topology'. At the bottom, a data processing graph is shown. It features a box on the left labeled 'InputStream#5' with properties 'EntityType: nie:sensor' and 'scoped: false'. A yellow arrow points from this box to a box on the right labeled 'Task#1'. The 'Task#1' box has properties: 'name: Stats', 'operator: virt', 'groupby: all', and two 'broadcast' outputs.

Figure 7. Extension dashboard of the Smart City Magnifier offered by FogFlowt.

## CEMA outcome

The CEMA outcomes are showcased to the city councils in New Zealand. The outcomes of CEMA could be useful for the purposes such as urban planning and efficient transportation services in smart cities.



*Figure 8. Smart City Magnifier dashboard for New Zealand data.*

The results of CEMA are shared with applications (clients) from New Zealand side, which, on top of the generic Smart City Magnifier view, used their own visualizations. In addition, CEMA has the dashboard which is shown in Figure . The dashboard includes graphs for crowd estimation results in different mote locations as well as stay duration averages. The dashboard also includes a table which shows the people flows from every Wi-Fi mote to every other. The visualization also includes a heatmap to visualize the crowdedness levels and bar charts to visualize count-in and count-out events of the stereoscopic cameras. The same interface is used for both Christchurch and Wellington test sites. This interface is also showcased in CeBIT trade fair in Hannover, Germany and in iExpo event in Tokyo, Japan in 2017.

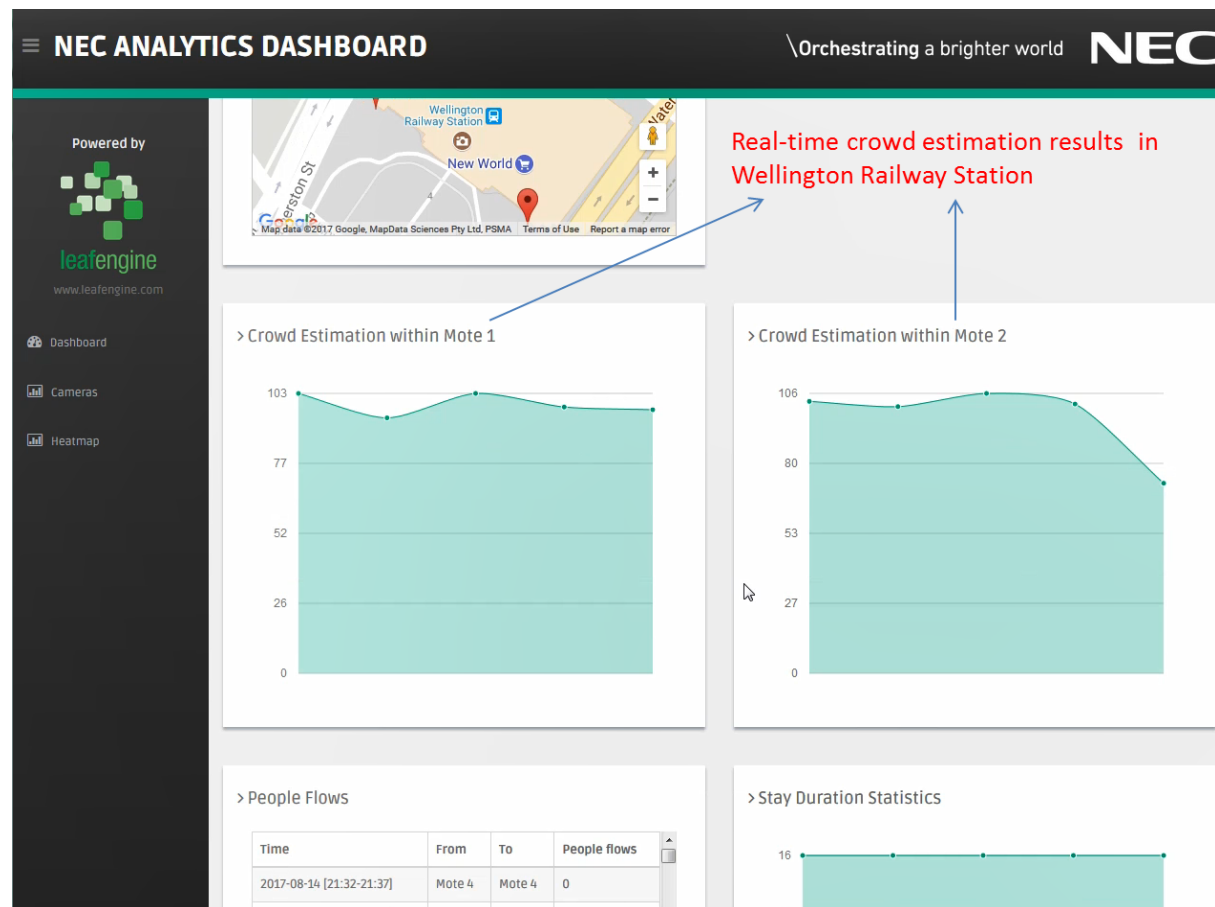


Figure 9. Visualization dashboard for the Wellington Railway Station.

The CEMA system observed certain similarities throughout the months, weeks, and weekdays. Moreover, the similar regularities can be considered, for instance, for morning vs. night comparison of the visitors in the shopping mall or train passengers. In the case of a certain event, the CEMA system is capable of visualizing it where an unexpected crowd size or behaviour can be detected.

The lab experiments for the stereoscopic cameras resulted in 96.8% for “static crowds” where the office room is in its ordinary use. The test is also conducted with a more “dynamic crowd” where 14 people are invited to the small office room for an event and they were also walking in and out of the office room. In this experiment, 41 count-in and count-out events are detected in 20 minutes time period and the accuracy for the dynamic scenario is 97.5%.

The field tests that are conducted in the Wellington pilot show that stereoscopic cameras provide a minimum accuracy of 85% and it can easily serve as “near ground-truth” for accurate calibration of Wi-Fi data. Moreover, the proposed calibration algorithms provide 43.68% average reduction compared to the approach which is based on only Wi-Fi inputs. The high accuracy of the calibration in the train station shows that similar systems with high accuracy crowd behaviour detections can be used in future smart-city applications.

More information about the CEMA system, crowd estimation algorithms, deployment considerations, experiments, and other information can be found in the conference paper (Wu & Solmaz, June 2018.), which will appear in the proceedings of “16th ACM

International Conference on Mobile Systems, Applications, and Services (**ACM MobiSys'18**)” and a CEMA demo using the CEMA dashboard visualization is considered to be showcased in the conference in Munich, Germany.

#### KPIs achievement update

During the last year of the project we have also improved our KPIs (see Table 4), both because of improvement in the experimentation development and because of the integration of new testbeds.

*Table 4. Evaluation of the Data Assembly and Service Portability through KPIs for the Y3.*

KPI	Details	Status
<b>Creation of more than 200 Virtual Entities</b>	More than 460 (in Y2 it was 250) Virtual Entities have been already created. For each of such Virtual Entity analytics functions are automatically instantiated and performed and augmented data was created within the experiment. The number doubled in respect of Y2 due to the integration of new testbeds during Y3.	Achieved
<b>Data aggregated on more than 2 abstraction levels</b>	The experiment is aggregating data over 7 (in Y2 it was 4) different abstraction level (Building, Street, City, Neighbourhood, District, Region, Country).	Achieved
<b>Have 1 or more indicators based on Observation-oriented analytics</b>	The experiment is performing 1 analytics task based on observation: data statistics (average, minimum, maximum) sensor deployment quality (observation density per area, number of active sensors of a certain type per virtual entity).	Achieved
<b>Have 1 or more indicators based on Resource-oriented analytics</b>	The experiment is performing a task of <i>quality of deployment</i> based only on resource discovery. This KPI was still not achieved in Y2.	Achieved
<b>Leverage data from at least 3 testbeds</b>	The experiment is acquiring and using data already from all the testbeds registered in the FIESTA-IoT federation together with the New Zealand data. The total amount is 11 (4 in Y2) testbeds.	Achieved
<b>Apply analytics functions on data coming from at least 2 testbeds</b>	The dashboard, which is aggregating data based on the focused geographic scope, is able to show the situation of the entire European continent on the lateral gauge widget exploiting data from the	Achieved



	SmartSantander testbeds and the crowdsensing testbed of SoundCity.	
<b>Have 1 or more indicators based on Hybrid-oriented analytics</b>	The experiment is combining the output of two analytics task, one Observation-oriented and one Resource-oriented: the <i>monitor of deployment</i> task. This is a brand new KPI.	Achieved

## 2.2 Dynamic Discovery of IoT Resources for Testbed Agnostic Data Access

The Dynamic Discovery of IoT Resources for Testbed Agnostic Data Access focuses on the (dynamic) harvest of IoT-based data in a testbed agnostic manner. In that sense, the web application accesses to the FIESTA-IoT API to collect measurements (related to environmental parameters) and provide a Graphical User Interface to interact with them. The features provided by this experiment can be summarised in the following ones:

- Graphical representation of available resources in FIESTA-IoT.
- Location and phenomena-based resource discovery.
- Retrieval of observations.
- Statistical analysis of the data generated from resources.
- Graphical representation of these stats (e.g. candlestick graphs).
- Modular implementation for component reutilisation.

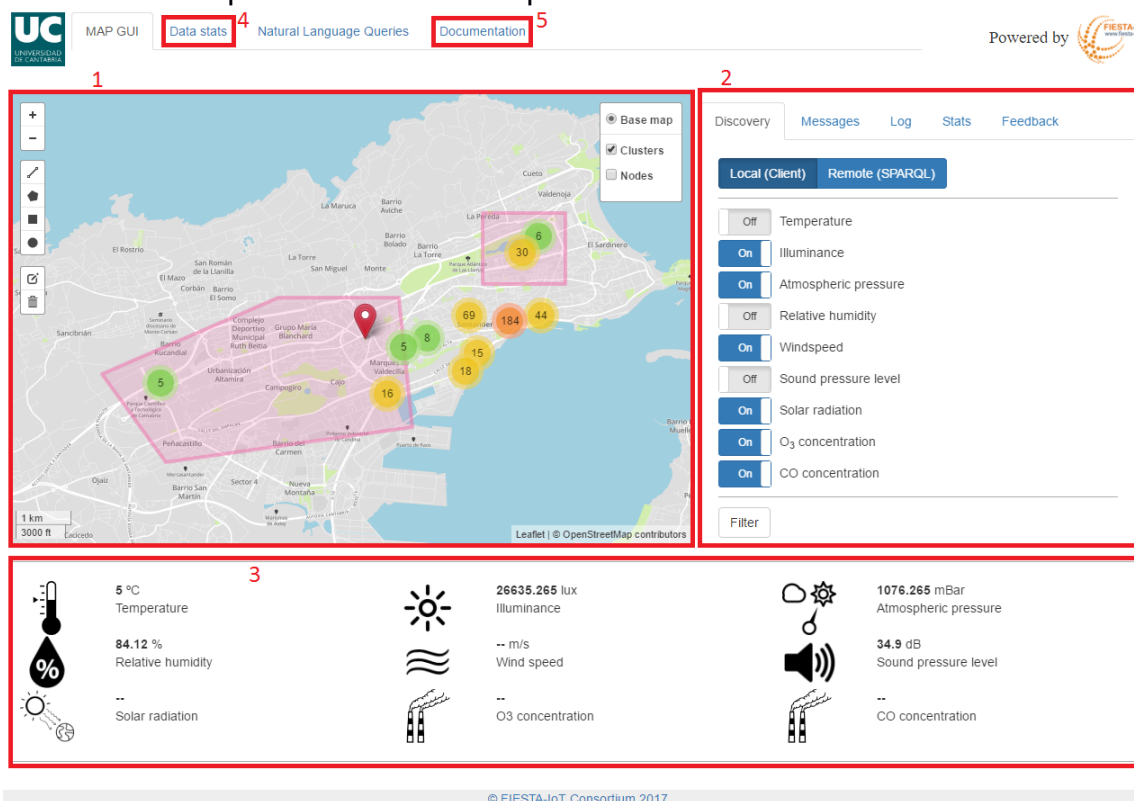


Figure 10. Screenshot of the Dynamic Discovery application.

### 2.2.1 Third year update

During the last year of the project, the focus on this experiment aimed mainly at the stabilisation of the web application, providing a reliable web application on top of the FIESTA-IoT platform. Additionally, some of the foreseen future steps envisioned in deliverable D5.2 (FIESTA-IoT D5.2, 2017) have been implemented.

- Integration with the new platform improvements

Due to the large quantity of data being stored in the triplestore database, the system was improved including a solution to split the global graph of observations into a number of subgraphs.

- SSL access connection implementation

The experiment now provides connectivity through the implementation of HTTPS protocol. The implementation has been carried out using the “Let’s Encrypt” certificate, which is free and renewable every 3 months.

- Modularisation of the experiment

So as to deploy the experiment easily, it has been integrated in a Docker container solution, thus providing the easiness to deploy it in other systems.

### 2.2.2 Final outcomes

The “Dynamic Discovery of IoT Resources for Testbed Agnostic Data Access” experiment has demonstrated the usage of the FIESTA-IoT platform to discover IoT resources in a user-friendly fashion.

As a summary, the experiment included the implementation of a client/server web application for environmental resource discovery in a testbed agnostic manner. The resource discovery implementation can be performed in several ways:

- Using the graphical tools provided by the interactive map representation in the experiment. Geographical forms can be placed on the map to select a specific set of nodes.
- Using the filters to discover resources of specific type.
- Introduce manually specific SPARQL queries to discover and show resources graphically.

## 2.3 Large Scale Crowdsensing Experiment

The large scale crowdsensing experiment<sup>4</sup> focuses on providing its users an overview of noisy and quite locations in a city/region over time. It also serves the purpose of a proof of concept experiment to show the need and usability of the FIESTA-IoT EaaS (Experiment as a Service) tools. The experiment relies on tools such as Experiment Editor, Experiment Registry Module (ERM), Experiment Execution Engine (EEE) and Experiment Management Console (EMC) for its execution. To bring back readers on how an experiment works we present a brief overview of architecture. For the complete detailed description, we refer readers to (FIESTA-IoT D5.2, 2017). The experiment is described using the FIESTA-IoT experiment specific DSL (Domain Specific language).

---

<sup>4</sup> Our experiment is available at [https://mimove-apps.paris.inria.fr/fiesta/index\\_fiesta.html](https://mimove-apps.paris.inria.fr/fiesta/index_fiesta.html)



This DSL is stored in the ERM. The EMC reads experimenter specific DSL details from the ERM and displays them to us (the experimenter). We then enable the execution of particular services (the use cases that we have described) using EEE that we have described in the DSL. Upon the execution of a particular service, the results are sent to us via Experiment Data Receiver (EDR), where we store the results in our local repository. The experiment UI reads use case specific most recent results and displays them to the user of our experiment. The experiment internally uses Node.js<sup>5</sup> technology to build the UI.

### 2.3.1 Third year update.

As described previously (FIESTA-IoT D5.2, 2017) in the third year we envisioned to finalize the experiment with remaining use case that we had described in D5.1 (FIESTA-IoT D5.1, 2016) and D2.3 (FIESTA-IoT D2.3, 2016). Since the last reported version, as the final outcome, we have implemented three other use cases using FIESTA-IoT tools answering namely:

- What were the least noisy locations over time and over a region?
- What is the most recent sound level over a region?
- What is the most recent sound level over a location?

The above cases are implemented as specific queries that are executed at defined interval using EEE. For reference, we provide the queries as part of Annex III Large Scale Experiment Queries (Note that `%%fromDateTime%` && `%%toDateTime%` refer to the dynamic time interval feature provided within the DSL). As the above case are mostly similar in terms of experiment architecture and workflow, to implement the above cases, we needed to update the experiment DSL (queries therein), execute the created services (FISMOs: FIESTA-IoT Service Modelling Object) using EEE and get the results of the services using EDR. Due to the internals of the EEE and the easy to use EDR, we only needed to update the experiment UI to show the results of the different implemented use cases.

To incorporate the need to show the results of the different use cases, the most significant update was done in the experiment UI. The UI was revamped to show the choices of different use cases to the user so that he can select a particular case (Figure and Figure ). Upon the selection of the use case the user was given an option to update the map using the “Get Measurement” button. The UI also provides a mechanism for the user to auto-reload the UI (done using an “Auto-reload Measurement” button). This interval is set to 1 minute for the auto-reload. The auto-reload reads the recent result sets that are obtained after the execution of the selected use-case and displays the results on the map. Note that, for the case of noise/quiet places, we show a heatmap while for the case of recent sample in a given area (or a particular location) the experiment shows the marker at a location with information like the sample value and the time parameter. For this case, where we show the markers, we also provide a slider which a user can use to point out a particular measurement in the map. When using the slider, the marker is highlighted on the map. Note that while traversing through the slider, it provides a time sorted values. The slider also enables the user to see/note different overlapping measurements.

---

<sup>5</sup> <https://nodejs.org/en/>

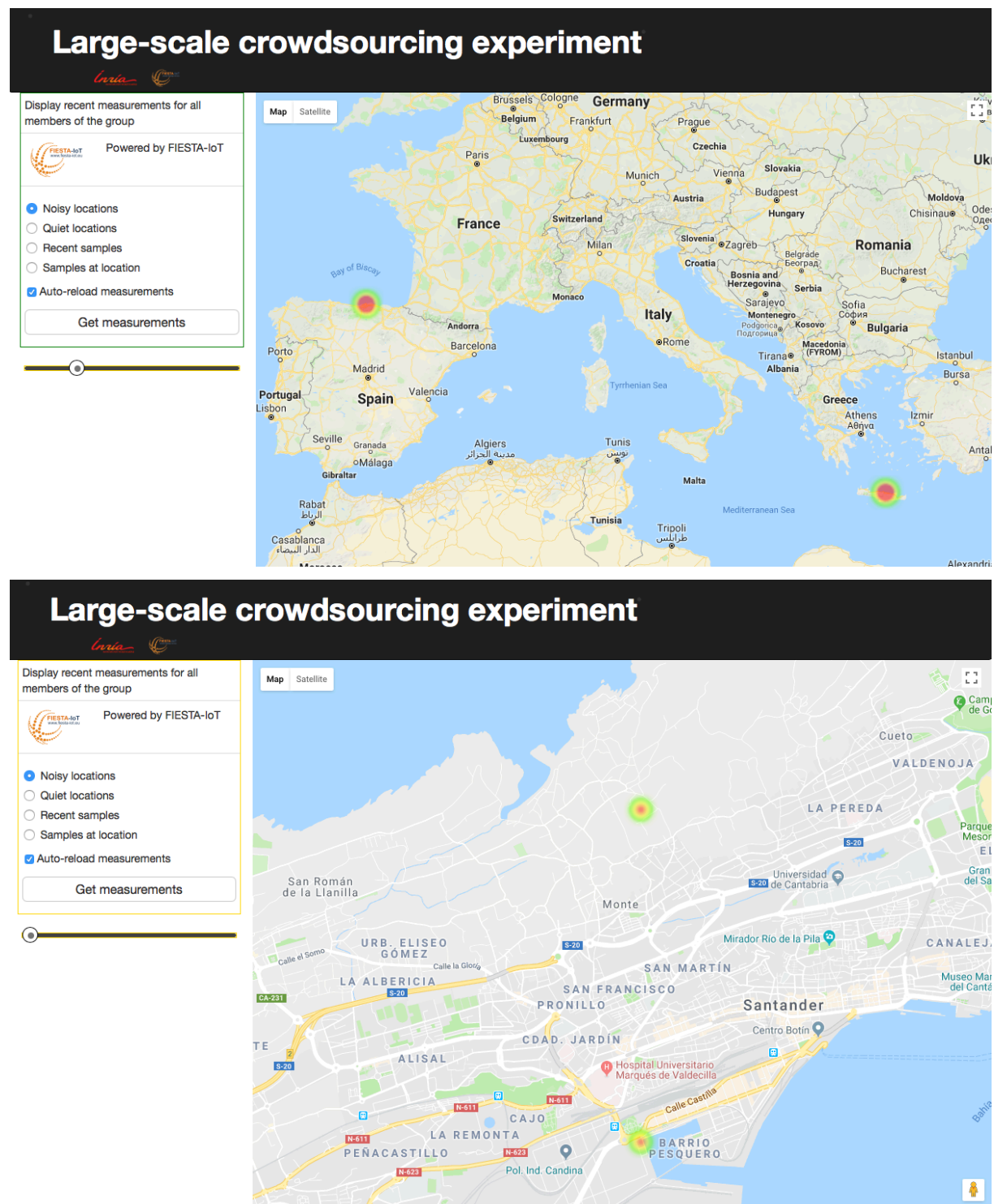


Figure 11. Large scale crowdsourcing experiment use case 1 (noisy locations) (a) all recently collected samples, (b) zoomed in view of Santander region.

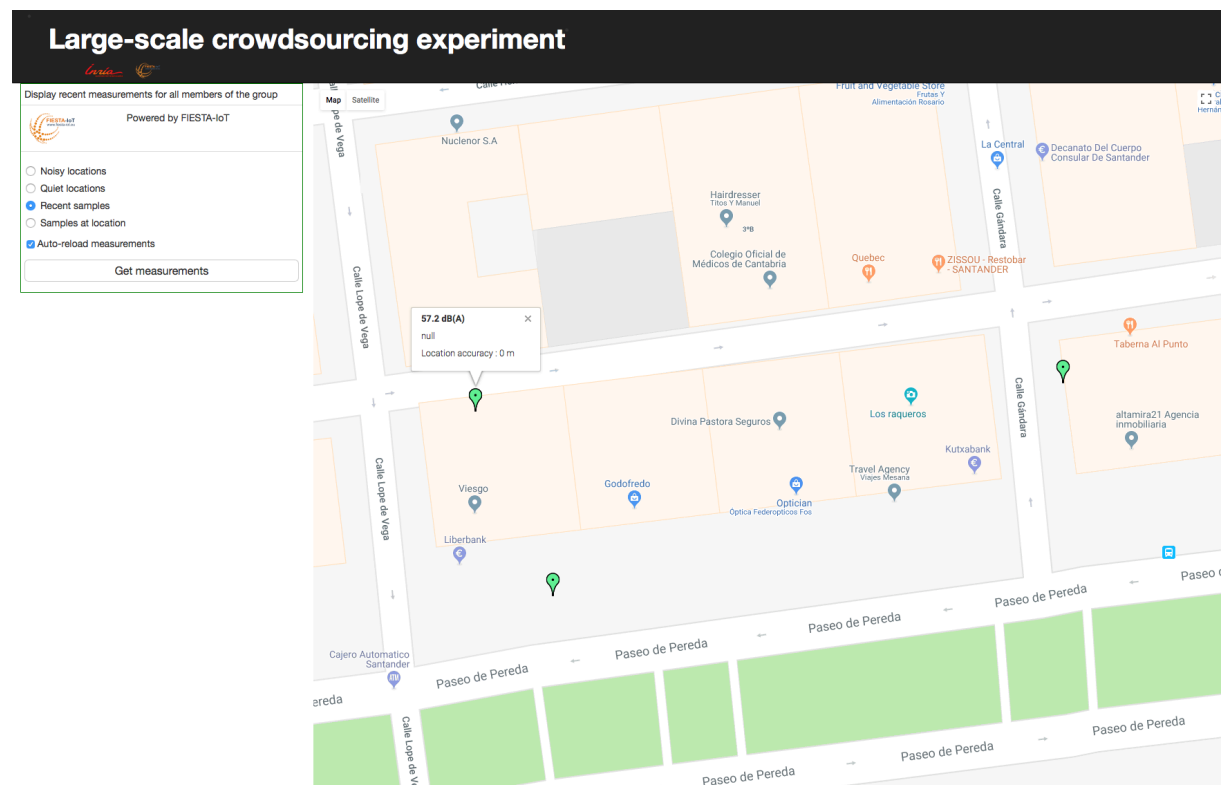


Figure 12. Large scale crowdsourcing experiment use case 3 (recent sound samples in an area).

### 2.3.2 Final outcomes

As part of the final outcomes of the experiment, we have validated the use of the FIESTA-IoT tools and fulfilled the experiment needs. As mentioned before, using our experiment, the user of the experiment is now able to get informed about the noisy/quiet places in the region and can plan his/her travel accordingly. Further, one issue that we faced was, that in the triple store, there are not many observations related to sound measurements available. Although SmartSantander, SmartICS, Soundcity, NITOS and FINE testbed have sound sensors, they are limited in number. Moreover, with the Soundcity testbed the observations are not produced at regular interval. Thus, it is still hard to validate the KPI: large number of samples needed for high quality result.

### 3 EXTERNAL EXPERIMENTS

One of the main goals of the FIESTA-IoT project is the usage of the platform by external experimenters, having a two-fold approach: validate the platform possibilities and provide a framework for the scientific community to research on top of the testbeds involved in the project. In order to fulfill this objective, a set of Open-Calls have been launched throughout the project.

*Table 5. Number of Experiments and Testbeds integration in the different Open-Calls.*

CALL	Experiments	Testbeds	Submission deadline	Experimentation Period
Open Call 1	6	3	26/10/2016	01/12/2016 to 30/06/2017
Open Call 2	-	3	28/02/2017	01/04/2017 to 30/09/2017
Open Call 3	13	-	29/06/2017	15/08/2017 to 09/03/2018
Open Call 4	5	-	18/09/2017	09/10/2017 to 31/03/2018

There have been 4 Open-Calls launched during the FIESTA-IoT project. These Open-Calls can be divided in those that support two types of FIESTA-IoT platform usage: experimentation and testbed integration. While in the first Open-Call both possibilities were accepted, Open-Call 2 was meant for testbed integrations and Open-Calls 3 and 4 were limited to experimentation. Table shows the different experiments carried out on top of the FIESTA-IoT platform in the different Open-Calls. Additionally, testbeds integration are also included. In summary, 24 funded experiments have been carried out on top of the platform, and 6 new testbeds have been integrated.

Within this section we present the experiments that have participated in the different Open-Calls being held during the project lifetime. In that sense, section 3.1 includes the publishable summaries of the experiments, provided at the time of experiment reporting. Furthermore, we are also presenting the functional evaluation of the experimenters about the platform, through the analysis of the results obtained from the surveys provided to the experimenters.

## 3.1 External Experiments Summaries

### 3.1.1 Call for Experimenters 1

#### 3.1.1.1 *IoT data management at the network edge by decentralized community service (DATE)*

In the DATE experiment, we explored the deployment of advanced services at the network edge to provide support for IoT data management services with a distributed microcloud infrastructure. By leveraging resources and datasets from the FIESTA-IoT testbed, the DATE project developed and conducted experiments to shape support services to be integrated in the Cloudy microcloud platform, which enables the deployment of IoT data management components. The project results are extensions developed and integrated in the microcloud platform that enable a more flexible and user-friendly deployment of applications, the integration of support services for being able to choose from a more diverse set of applications, and the evaluation of the platform with the deployment of components for IoT data management. The obtained improvements open up the Cloudy microcloud platform to a larger target audience and demonstrate the possibility of an open platform for IoT data management with low entry barriers as a mean to facilitate the deployment of innovative services by third parties.

#### 3.1.1.2 *Smart Polyhedron Indicator for Asset Management*

A smart city provides effective integration of physical, digital and human systems in the built environment to deliver a sustainable, prosperous and inclusive future for its citizens. When organised well by using the concepts of space and time, information about cities can be the basis for many powerful services, analytics and decision-making. This experiment brings to the infrastructure for experimentation under the FIESTA-IoT project further spatial "intelligence" capabilities, namely the integration of IoT data with Building Information Models (BIM) as means for the management of assets in a context that can span from a single building to an entire city. For proof of concept purposes, and since it is still very early days for the integration of IoT and BIM, we build a BIM-based 3D visualisation of what we call the Smart Polyhedron Indicator, a compelling, comprehensive, seamless and dynamic representation of environmental data across several FIESTA-IoT sites. Integrating sensor-related data coming from environmental conditions presents challenges using current available standards under BIM. Our experiment addresses these challenges, generating new knowledge on how to further and systematise this integration. In summary, the specific objectives of this experiment and the overall project are:

- Investigate and further develop the inclusion of sensor data into BIM models
- Prototype capabilities that link sensor readings or disaggregated key performance indicators to visual elements in a compound BIM-based 3D Smart Polyhedron Indicator.
- Visualise the sensor readings and indicators in a comprehensive way that is useful for urban and city planner and decision makers through the use of BIM models
- Plan and develop a visual demonstrator using the integration services offered by the FIESTA-IoT meta-platform.
- Provide specific feedback to FIESTA-IoT, addressing factors, barriers or considerations that may have impacted the course of the experiment.



- Deliver reports to document the outcomes achieved.

#### 3.1.1.3 *Data Quality and Easy Services Creation in FIESTA-IoT*

The complexity, dynamism and heterogeneity of the FIESTA-IoT platform make the provision of knowledge about the data quality and their transmission very difficult. Thus, we propose to extract this knowledge dynamically analysing the "linked data set" offered by the FIESTA-IoT platform.

To do this, we mainly use the portal to be able to load FEDspec files and receive information about all available testbeds and infer network parameters applied in the world of communications networks to that information.

Therefore, we analyse the information provided by the FIESTA-IoT platform, draw conclusions and adapt them to the existing ontology. This information is shown on an additional server, which allows SPARQL requests, according to the extended ontology.

We can summarize the objectives in the following:

- Extract information about all testbeds periodically and analyse it to calculate a set of network parameters.
  - Analyse the operation and interaction with the FIESTA-IoT platform.
  - Program the network parameter algorithms.
  - Create a database to store the metadata of the received files.
  - Manage the received files and extract the required data to apply the algorithms.
- Present the results obtained in an ontological format accessible universally, thus enriching the ontological model of FIESTA-IoT.
  - Convert the numerical results obtained previously to fit in the ontology of FIESTA-IoT.
  - Send the information to a server that is able to work in RDF (Fuseki server) format and make it available to any user, accessible through SPARQL requests.

Although it was not possible to make an analysis of the network parameters corresponding to the space between the testbeds and the FIESTA-IoT platform (because we do not have direct access to that network), we have inferred network parameters adapted to the information we could analyse, corresponding to all the testbeds. In particular, we have calculated the Delay, Jitter, Payload and, in addition, the location area of a complete deployment.

- KPI = 60% (Extract information from Testbeds and analyse it to calculate network parameters) + 40% (Show the results obtained in an ontological format accessible to all interested users)

At the same time, we can divide it into smaller objectives:

- KPI = 15% (Analyse the FIESTA-IoT platform) + 25% (Algorithms programming) + 5% (Database creation) + 15% (Received files management) + 15% (Adaptation of the results to the FIESTA-IoT ontology) + 25% (Fuseki server creation).

#### 3.1.1.4 TALK2FIESTA

The Talk2Fiesta experiment aimed at developing and deploying a chatbot allowing citizens to interact with IoT devices through a conversational interface. The vision behind the experiment is that individuals should be able to ‘chat’ with their smart city in much the same way they do with friends and family. Accordingly, people should be able to ask questions to IoT-connected devices (e.g., information about their current status), as well as to send commands to IoT actuators. And they should be able to do it without having to know the low-level technical details of the specific sensor or IoT technology implemented.

During the experiment, the U-Hopper team developed a set of core enablers for connecting various chat applications (Facebook Messenger, Slack) to the FIESTA-IoT platform APIs via a Natural Language Processing engine. The experiment, in particular, showed that the semantic interoperability feature of the FIESTA-IoT platform, which conceals the heterogeneity of underlying devices, data and testbed infrastructure, allows for the fast and cost-effective development of chatbots. The chatbot was connected to SmartSantander and SmartICS testbeds and able to converse in three different languages (English, Spanish and Italian).

The chatbot was showcased to a plurality of stakeholders (including smart city councils, municipalities, investors and IT companies), and commercial exploitation activities are currently ongoing.

#### 3.1.1.5 *CorRelations bEtween Data graphs and IoT topologies (CREDIT)*

Fully utilizing the big sensory data produced by smart-city/building sensor networks requires discovering hidden correlations in the corresponding datasets. To achieve this, CREDIT experiment suggested using enhanced community detection algorithms for data clustering of datasets obtained from very large smart-city/building infrastructures. Our scientific approach capitalizes on a recently developed framework for big network data analytics, namely Hyperbolic Data Analytics, which embeds network graphs in the hyperbolic space, computing distances between node pairs as hyperbolic coordinate distances and allowing more efficient computation of network metrics, such as the Edge-Betweenness Centrality (EBC). CREDIT took the framework one step ahead and modified a well-known community detection algorithm (Girvan-Newman, GN), by computing EBC in the hyperbolic space, speeding up the computations without significantly sacrificing accuracy. By first obtaining a data dependency graph on the collected sensory data, in CREDIT we mapped the problem of data clustering to a community detection one over a graph embedded in the hyperbolic space. We demonstrated its efficacy by doing an analysis over benchmark datasets, as well as an analysis of real multi-dimensional data collected by the FIESTA-IoT platform. CREDIT verified that the Hyperbolic GN (HGN) is capable of coping with large volumes of diverse sensory data, obtained from real, operational smart-city/building topologies, and at realistic scales, depicting its feasibility and quantifying its performance potentials.

Additionally, CREDIT exploited the developed analytics methodology in an application for reducing the energy cost associated with the sensing nodes, using data from real scenarios obtained from FIESTA-IoT. Through the analysis of the obtained datasets, it became possible to do so in a twofold way. First determine in an efficient manner which sampling instances can be omitted in a specific set of measurements defined by a

sampling rate, thus conserving the associated energy for all employed sensors, and secondly, identify the sensors that exhibit practically identical behaviour in the data clusters and use them either for monitoring load balancing or measurement prediction. In both cases, energy savings are gained by determining additional idle periods for sensors.

Access to FIESTA-IoT allowed us to validate the operation of HGN and quantify its performance potentials with real data in a short time period, contributing to the fast evolution of our research work. The role of the datasets obtained by FIESTA-IoT was the key and aided in promoting our position in the state-of-the-art. At the same time, we were able to provide multi-facet feedback regarding the operation of FIESTA-IoT and potential improvements/extensions, hopefully contributing towards making FIESTA-IoT an attractive and promising venue for experimenting with multi-dimensional big data networking applications.

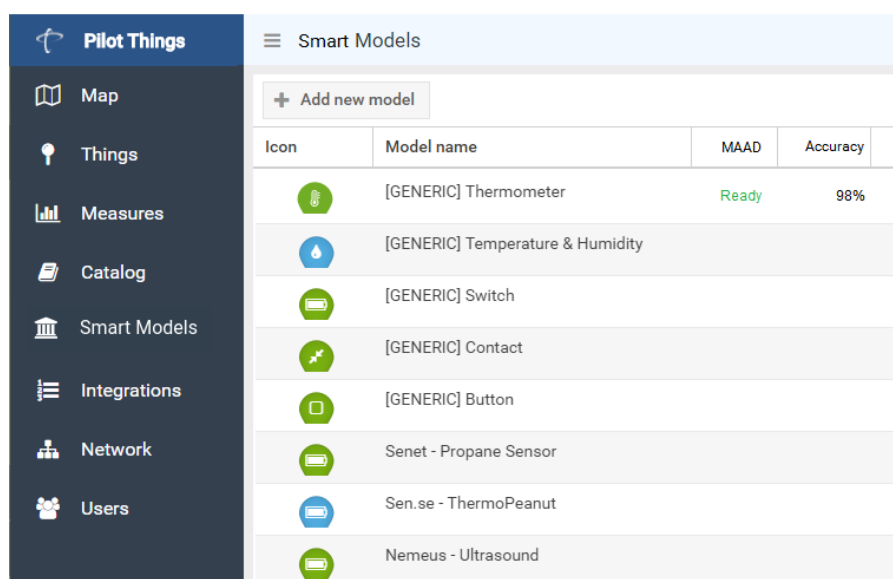
### 3.1.1.6 Smart Monitoring (Pilot Things)

The European FIESTA-IoT project provides their members access to testbeds with numerous live sensors. The project selects European companies for their innovative solution using these data. Pilot Things was selected in 2017 to build a software feature that automatically detects IoT sensor data anomalies on the smart city of Santander in Spain.

In 2010, the European Commission selected the Smart Santander project to become the testbed of the European Union in the realm of smart cities. This middle-sized city (180,000 inhabitants on 40 km<sup>2</sup>) holds the world record of smart sensors with nearly 20,000 fixed and mobile connected devices.

Pilot Things can create smart networks for the Internet of Things on a city scale. With the constant influx of data from thousands of sensors, it becomes essential to have an automated system detecting failures and anomalies. However, such system should not come at the expense of easy configuration and low operational overhead.

In answer to these needs, we have created the Measurements Advanced Anomaly Detection (MAAD) technology available only within the Pilot Things network.



The screenshot shows the Pilot Things dashboard. On the left is a dark sidebar with navigation icons and labels: Pilot Things, Map, Things, Measures, Catalog, Smart Models, Integrations, Network, and Users. The main area is titled 'Smart Models' and contains a table of models. The table has columns for Icon, Model name, MAAD status, and Accuracy. The first model, '[GENERIC] Thermometer', is highlighted in green and shows a 'Ready' MAAD status and 98% accuracy. Other models include '[GENERIC] Temperature & Humidity', '[GENERIC] Switch', '[GENERIC] Contact', '[GENERIC] Button', 'Senet - Propane Sensor', 'Sen.se - ThermoPeanut', and 'Nemeus - Ultrasound'.

Icon	Model name	MAAD	Accuracy
	[GENERIC] Thermometer	Ready	98%
	[GENERIC] Temperature & Humidity		
	[GENERIC] Switch		
	[GENERIC] Contact		
	[GENERIC] Button		
	Senet - Propane Sensor		
	Sen.se - ThermoPeanut		
	Nemeus - Ultrasound		

Figure 13. Pilot Things dashboard.



When the Pilot Things network is deployed, we associate the sensors with machine learning models automatically learning the normal behaviour of the sensors and are able to predict new values within a short time frame.

The data collected by the sensors is then compared to the data calculated by MAAD. When receiving values outside the predicted interval, the city receives a malfunction alert.

After one month of learning, MAAD can detect sensor data anomalies with a 90% accuracy rate.

The benefits of such a system for smart city are as follow:

- A central supervision system for their IoT network,
- Automatic sensor failure detection,
- Automatic value correction,

MAAD has also use cases in other domains like the industrial realm.

This technology is available exclusively on the market place Microsoft Azure for selected customers<sup>6</sup>.

### **3.1.2 Call for Experimenters 3**

#### *3.1.2.1 Energy-IoT*

In the European Union, energy consumption in buildings represents about 40% of the total energy consumption (FIESTA-IoT D5.2, 2017). Accurate energy forecasting models is a key element of the building control and optimization process. However, the prediction of energy usage in buildings and modelling the nonlinear behaviour of the corresponding energy system, are complex tasks due to influential factors such as weather variables, building construction, thermal properties of the physical materials, occupants' activities and end-users' behaviours. To address this challenge current research work is mainly focused on machine learning techniques with single time series data, i.e. using only historical energy consumption records.

With more IoT sensors being deployed in buildings and more time series data being gathered, is important to investigate how this new data streams can improve the forecasting capabilities of buildings energy consumption. However, IoT subsystems are usually designed in a vertical logic and structured in independent and closed areas ("IoT silos"), what makes it difficult to get access to heterogeneous sensing data to test the performance of advanced predictive models that combines heterogeneous sources of data.

In this experiment we have exploited the semantic interoperability provided by FIESTA-IoT to overcome this issue by using two smart buildings environments: SMARTICS and ADREAM with hundreds of sensor nodes and associated data sets available. A dashboard with a set of visualization tools was developed to help to understand the buildings environment and associated energy consumption. Multivariate predictive

---

<sup>6</sup> <https://azuremarketplace.microsoft.com/en-us/marketplace/apps/src-solution.pilot-things-iot-vpn?tab=Overview>

models of energy consumption were validated taking advantage of FIESTA-IoT framework.

The main conclusion is that interoperability across IoT heterogeneous sensors can potentiate a better understanding on buildings energy consumption. In fact, there is a significant improvement on the accuracy of the energy consumption prediction when using multivariate time series (e.g. human activity in the building, temperature and historic power consumption). A main requirement to make this possible is an IoT architecture that allows interoperability among IoT data silos, as the one provided by FIESTA-IoT.

#### *3.1.2.2 Smart IoT Data Collection (BeSmart)*

The Internet of Things will involve a huge number of sensors. Periodically collecting data from all IoT sensors will waste a significant amount of communication and storage resources, in addition to a significant amount of energy, which impedes the scalability of IoT systems. Moreover, it introduces significant privacy risks. The goal of BeSmart was to experiment with procedures for efficiently collecting IoT data while achieving target requirements in terms of data accuracy, timeliness, energy efficiency, and privacy protection. The procedures dynamically adapt the IoT data request density in time (frequency of requests to a particular IoT sensor) and space (requests for the same type of data from IoT sensors located in the same area), as well as add noise to measurements in order to preserve data privacy. The performance evaluations performed by BeSmart involved different data types/phenomena from different testbeds and in different time windows, illustrating the ability of the FIESTA-IoT platform to provide uniform access to measurements of different data types/phenomena and from different testbeds.

#### *3.1.2.3 SemantiC Coordination for intelligENT sensors (2CENTS)*

Diversity of radio access technologies, such as ZigBee, Bluetooth, LTE and Wi-Fi, together with growing requirements for their simultaneous use, significantly increases the complexity of IoT wireless networks. A number of open challenges affect practical deployments, such as simultaneous use of multiple technologies, intelligent coordination of a subset of nodes, coexistence of different technologies using the same spectrum, efficient management of (simultaneously used) heterogeneous radio links, etc. Adoption of Semantic Technology (ST) is a promising approach to coordination in such complex wireless infrastructures especially in cases where interference models are not well understood. SemantiC Coordination for intelligENT sensors (2CENTS) implements network intelligence on top of the FIESTA-IoT platform by reasoning for the network state estimation based on ST. ST facilitates reasoning about coordination, application priority, frequency selection and dynamic spectrum access. Potentially problematic network states could be proactively avoided instead of reactively corrected particularly in priority critical applications. The 2CENTS controller collects network environment data, processes it for knowledge generation and uses the knowledge to facilitate making informative decisions about coordination. The 2CENTS experimentally investigated the performance benefits and unique challenges of coordination in complex infrastructures such as Smart Cities. We designed experimental scenarios that use the 2CENTS controller and the FIESTA-IoT platform to evaluate a set of strategies for future intelligent coordination in heterogeneous wireless networks (i.e. selection of WiFi and ZigBee channels in the case of mutual interference) based on

collected measurements from different sensors application-dependent priority management.

#### *3.1.2.4 Smart Urban Routing for FIESTA-IoT (SURF)*

The era of the car as we know it has ended. Recent EU countries regulations, combined with the statements issued by several EU car manufacturers about stopping production of fossil fuel-based cars are making a world without the sounds or smells that dominated the 20th century suddenly imaginable. In this scenario, urban transportation will change radically and cleaner ways of mobility will arise. Aside electric cars and public transports, people will rediscover the joy of zero-emission mobility by increasingly using bicycles or simply walking. Although many initiatives for using bicycles in cities are more and more frequent (e.g., station-less bike sharing services such as Ofo or Mobike), urban navigation is still relying on traditional routing systems developed primarily for cars. Some navigation services (e.g., Google Maps) provides options for pedestrians and bikers, but the routes they compute are generally based on time only and do not take into account other important factors such as pollution or noise.

At the same time, the Internet of Things (IoT) paradigm is populating the world with an increasing number of sensors able to sense the surrounding environment and communicate such measurements remotely for higher level services. In particular, it is envisioned that the application of such a paradigm to urban environments will foster the rise of the so called Smart Cities. This evolution generates several practical challenges still to be solved, such as the management of massive amount of data coming from city-wide deployed sensor networks or the integration of such data into user-friendly data consumer platforms able to scale and be used in a flexible way.

In this scenario, the objective of the SURF experiment is to showcase the feasibility of a smart routing system specifically addressing urban mobility for pedestrians and cyclists using IoT technologies. Leveraging the data accessible through the FIESTA-IoT framework, the proposed routing system computes several alternatives to traditional shortest-path routes such as the ones computed by standard services like Google Maps. Such alternative routes are computed fusing geographical information obtained from publicly available navigation services with the data retrieved by sensors available in the location of interests and made available through the FIESTA-IoT platform in a completely agnostic fashion.

Combining the two sources of data allows creating a greatly flexible and customizable urban routing system. A user has several degrees of freedom in selecting the best path for reaching his or her final destination. Some examples include:

- For geographical areas where air quality sensors are installed, select the least polluted route
- For areas where temperature or solar radiation sensors are installed, select the route with the highest or lowest temperature
- For areas where sound sensors are installed, select the quietest route

The choice of the specific option to select depends of course on the sensor resources available in a particular area, which are conveniently discovered through the FIESTA-IoT platform. For each sensor resource available in the location of interest for the user, the SURF experiment also performs two important processing operations in space and time: i) data retrieved from the platform is spatially interpolated to increase its

granularity and ii) prediction models are individually created for each sensor resource in order to allow the user to obtain routes also in the future.

#### 3.1.2.5 *FINETUNE*

Lately, cities activities are increasing, the more people are, the more are pollution we can find in our streets and roads due to, for example, people usage of different kinds of motor transport. This have increased the need of study this phenomenon, in order to find a solution suitable from everyone, a solution which is easy and scalable.

Environmental monitoring is the basis in a Smart City infrastructure to obtain a high level of awareness about the impact of urbanization, mobility and industrialization. For that purpose, smart cities are deploying gases sensors (NO<sub>2</sub>, SO<sub>2</sub>, O<sub>3</sub>, CO) as recommended by the World Health Organization (WHO) to determinate the air quality index.

Unfortunately, air quality and gases sensors have a complex behaviour based on electrochemical reactions, which require a calibration and tuning process to provide an accurate value, at the same time, even when they are calibrated in laboratory, chemical material is sensitivity to multiple gases (cross-sensitivity) making it not very selective. In addition, sensors lose their sensitivity and accuracy after six months and they are totally considered useless for monitoring after 2 years (maximum lifetime). Therefore, it presents a high maintenance cost and also a big challenge to guarantee its sustainability in long term.

Recent studies have demonstrated a correlation among the different gases concentration for every city; these values can be calculated in order to compensate cross-sensitivity. These algorithms and relationships among gases will enable maintenance/tuning of sensors during time, taking into account correlations, cross-validation and region characterization. Additionally, it is required to obtain some parameters (meta-data) about quality of data, in order to avoid wrong decisions or misunderstandings based on inaccuracies coming from sensors, therefor it is necessary the identification of sensors misbehaving in order to discard the data to mitigate errors, and in the best cases to recalibrate them (self-healing) in order to recover the system to obtain good values for the future.

FineTune aims to establish these algorithms/correlations among gases in Crete and Santander based on the historical data, in order to use them in new deployments. For this purpose, it has been used the real data from existing deployments from SmartSantander and FINE Testbeds.

FineTune has developed algorithms/correlations to validate air quality sensors, and it has also defined a holistic approach to the usual calibration approach based on the evolution of the sensors and cross-validation among the different sensors, gases correlation and cross-sensitivity.

FineTune has been able to identify all the performances, metrics, data quality from all the sensors in Crete and Santander, at the same time that it has been able to correlate and obtain relevant insights about gases sensors behaviours and evolution.

FIESTA-IoT has been crucial for this experiment, since it provides the homogenization of the data coming from the different testbeds from FIESTA-IoT in the vertical of Smart Cities, and it has enabled us the opportunity to evaluate several conclusions and contrast results from a location in other location.

After FIESTA-IoT experimentation, now we have the baseline of knowledge for air quality sensors calibration which is being continued through a deployment of a laboratory for air quality sensors calibration including Mass Flow Controller, incubators and different air concentrations generation. We have found out that a proper calibration requires of a reference system with a high accuracy in order to be able to build the models that define each sensor; since they are electrochemical sensors every system is different and every system requires a full modelling and calibration process. For that reason, it is required to have a stable environment where one can understand the differences and offsets among the different sensors.

Finally, we will continue this research line as a key part for HOP Ubiquitous portfolio (in particular for Smart spot product extensions for air quality sensors), in order to define new techniques and methods to calibrate sensors and evaluate their accuracy. In particular, we are defining a new calibration methodology which is being patented.

#### *3.1.2.6 Smart Pedestrian movement for Smart Cities*

Smart pedestrian movement is one of the major determining factors for designing a smart city. Organization and segregation of activities is the key to achieve a walkable street. Well designed and well-maintained details make the space visually appealing and encourage walking.

An urban street consists of a large variety of activities and different types of users. Most of the shopping activities as well as social activities take place on streets. Streets with shop fronts, eating joints, encourage heavy pedestrian movements. But these activities are often unsegregated and unorganized what makes the streets inaccessible and unsafe for pedestrians.

This experiment will use, amongst others, the Human Presence domain from the FIESTA-IoT testbeds for represent pedestrians inside a BIM City Model. In this way, we can understand how people will move through our cities. The target software for representing simulations is Oasys Mass Motion.

Basically, the experiment will map FIESTA-IoT sensors to Mass Motion objects (portals), and generate people flow, according to the data analysed. Additionally, the developed framework facilitates the generation of additional flows of people to achieve more realistic simulations.

#### *3.1.2.7 Internet of Things Application for a Better and Smart Comfort (SmartComfort)*

EUROB Creative has developed a software module, named SmartComfort, which provides a measure of the level of comfort of a specific area in real time: this software provides the thermal comfort, acoustic comfort and luminous comfort measurements calculation in real time, and also an estimation of the global comfort level of the surroundings.

The data gathering process collects all the necessary data from selected testbeds of the FIESTA-IoT platform, in particular, from SmartSantander for outdoor measurements and from NITOS for indoor. This task also establishes procedures to identify and discard anomalous values due to malfunctions of the smart sensors. The selected data is semantically processed in order to establish an overall comfort level.



The first version of the SmartComfort prototype has been improved, based on the feedback received during the first evaluations, leading to the final version of the SmartComfort software, on which the final tests and validation have been carried out.

The final version of our SmartComfort module for outdoor scenarios has been designed as a new feature of our Android App, InCity Together (with more than 15,000 downloads in Google Play), for the users in the region of Santander (Spain). By integrating the SmartComfort module in this application, InCity Together will be able to provide users a map of smart comfort places in real time, taking into account IoT sensors data from the city of Santander.

On the other hand, the final version of our SmartComfort module for indoor scenarios has been designed as a web page, allowing users to check comfort places in real time within the offices of NITlab, in the city of Volos (Greece).

In summary, the SmartComfort experiment determines the level of comfort of a particular area in real time, providing users with a new tool for improving their well-being, and delivering additional value services.

The SmartComfort project has been accomplished thanks to the possibility of accessing the smart sensors' data from the FIESTA-IoT platform, together with the different tools and the support provided by the FIESTA-IoT platform members.

#### *3.1.2.8 Knowledge as a Service for Assisted Living in Smart City (KaaS\_SCL)*

Solutions for home automation and assisted living require a lot of manual configuration and/or programming from the users. This calls for greater intelligence with increasing programmability, systems that learn. Knowledge as a Service for Assisted Living in Smart City (KaaS\_SCL) provides smart, personalised assistance to individuals indoors and outdoors based on the user profile as well as predictions on health status, traffic, weather, pollution, etc. KaaS\_SCL offers a combination of services:

- **Automated indoor environment adaptation** with functionality for learning user patterns to forecast user desires regarding indoor environment/home appliances configuration and proactively take actions/offer recommendations.
- **Remote Health Monitoring and Forecasting** comprising functionality for learning patterns in user physical status to identify any abnormality in usual patterns. Family members and/or professional caretakers can be informed and appropriate alarms may be raised if necessary.
- **Smart city life** providing navigation instructions, information on dangerous locations in the proximity, public transportation help considering user preferences and health/well-being status and a city dashboard.

The aim of the experiment was to perform experiment-based validation of KaaS\_SCL based on an existing prototype implementation (done in the H2020 EU Japan project iKaaS). Experimentation is a vital step as it enables the provision of critical insights on the performance of the KaaS\_SCL components, to allow for its further exploitation and commercialisation.

Our approach included: (a) Specification of experiment scenarios, validation/performance metrics; (b) Set-up of the KaaS\_SCL experimentation framework through the integration of the corresponding prototype with FIESTA-IoT facilities; (c) Experiments, results-analysis (including user experience) and



refinements; (d) Promotion of the validated KaaS\_SCL experimentation framework and of the FIESTA-IoT platform, through dissemination and demonstrations activities.

### *3.1.2.9 Security and Privacy for IoT infrastructures experiment (SpyIoT)*

Objective of the work has been the integration on the top of the FIESTA-IoT platform of the FINCONS IoT Security Layer (ISL) component, for the experimentation of its encryption features designed to provide end-to-end data protection, especially for privacy-related data.

The FINCONS IoT Security Layer (ISL) component is designed according to the Security-by-Design, Privacy-by-Design and Security-by-Default and Privacy-by-Default principles. Security/Privacy-by-Design means that the system has been designed taking into account the security and confidential data management needs, so the security and privacy (i.e., proper management of confidential data) is an essential element of the system. Security/Privacy-by-Default means that the security design and default configuration of the system already ensures a minimum level (which means an acceptable level which can be increased only) of security and privacy (i.e., confidential data management) that: (1) cannot be lowered, (2) is configured by default. Indeed, one of the most relevant features of the system is the end-to-end protection of confidential data using new CP-ABE (Bethencourt, Sahai, & Waters, 2007) techniques, which are asymmetric encryption schemes where: (1) explicit policies are used to control access to the protected information, (2) subjects have their own personal key, (3) personal keys are generated based on subject's attributes and (4) the decryption process succeeds only if those subject's attributes meet the access policy. The CP-ABE approach, therefore, avoids issues related to keys distribution, sharing, etc.

The features this layer provides have acquired paramount importance in consequence of the inclusion of Big Data paradigm in our everyday life, thing that is giving rise to different IoT scenarios with a continuous sharing of sensitive/personal data. For such scenarios, the protection of such data is a key challenge to achieve end-users' acceptance and legal viability (according to the recently established General Data Protection Regulation<sup>7</sup>) of new services and systems.

The security layer, therefore, represents an asset that FINCONS intends to exploit as a software component pluggable in all the IoT solutions / frameworks that support the concept of reserved access to resources.

The experimentation has been performed by implementing a monitoring application (suitable for different applicative domains, such as Smart City / Environment Monitoring and Health Monitoring) enabled to access a huge variety of assets made available by FIESTA-IoT (datasets and data-streams generated by different testbeds and referred to different geographic and applicative contexts), thing that demonstrates flexibility and wide-scope applicability of both FIESTA-IoT platform and the security component.

---

<sup>7</sup> Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data (<http://eur-lex.europa.eu/legalcontent/EN/TXT/?qid=1518606139593&uri=CELEX:32016L0680> , retrieved in February 2018).

#### *3.1.2.10 KPI Model for social & business events (REDEvents)*

The main objective of this experiment is to learn and gain experience in working with new methodology and ontologies related to Internet of Things and Machine 2 Machine communication. The goal, with previously mentioned objectives is to build and test a KPI model consisting of a set of services that will provide information to manage and monitor different aspects of a social or business event. These services will provide a set of indicators addressing relevant information of an event: security, social & city influence, degree of success. For this purpose, a heterogeneous data collection across two different participating testbeds is a target. These data combined with one self-generated, once analysed will provide a set of indicators. This experience will be used to build an event-monitoring system. This project and platform represent for Redborder an opportunity to define and test new functionalities and to go a step further towards the objective of developing a complete and integral solution for the monitoring and management of events and propose ways to maximize the benefits of these events in their upcoming editions.

There has been experimental investigation undertaken in order to analyse the performance benefits and unique challenges of coordination in complex infrastructure with high quantity of communication nodes such as those published by testbeds. This approach leads to explore business opportunities of a new Redborder for Events (Redborder4Events, RedEvents) product-line, the company aims to develop a Minimum Viable Product (MVP), designed for use on large and medium scale events, and test it in a real environment.

#### *3.1.2.11 Fault Management and Isolation for IoT field devices (FM2I)*

IoT devices and sensors can generate incorrect measurements which can be attributed to software and hardware issues. Ensuring accurate datasets through fault monitoring and isolation is crucial for operational IoT deployments. As an example, if an IoT system is used to perform predictive maintenance of a smart building, the collected IoT datasets must accurately reflect the status of the monitored system. To overcome this challenge, the FM2I experiment improved and validated an IoT monitoring module for fault detection in smart building environments. Multiple reactive and proactive fault detections algorithms are developed, fine-tuned and integrated including: Rule Based (RB), Simple Moving average (SMA), and Autoregressive Integrated Moving Average (ARIMA). The FIESTA-IoT API including both authentication and data query are considered to establish seamless interaction between the FM2I experiment and the testbeds through FIESTA-IoT platform. SPARQL over HTTP is adopted for querying and discovering devices and observations from heterogeneous testbeds in a seamless way. The FM2I experiment contributed in fine-tuning multiple fault detections algorithms with regards to data variety, volume and velocity in an interoperable environment.

#### *3.1.2.12 Monitoring Energy Efficiency for Data Centres by Correlating IoT Sensor Readings and Weather Conditions Data (DC-IoT)*

This project aims to find the appropriate number of measurements needed for the evaluation of power consumption profile of the data centre (DC) and their correlation with external weather conditions. As a large portion of the energy consumption of DCs is driven towards cooling the IT infrastructure it is of great interest to investigate the

factors that affect it. Air cooling systems that bring air from the external premises are usually deployed for the cooling of the interior of the DCs. This project focused on weather data (e.g. temperature, humidity, wind, atmospheric pressure) collected by weather station sensors in order to examine the correlation with the energy consumption of the DC. Additionally, we modelled the power consumption related to weather trends in order to effectively forecast the energy consumption and validated this through live measurements from RealDC testbed.

The DC-IoT project main outcome is the delivery of an application that calculates the forecast values of the energy consumption of a data centre, given a weather forecast for specific physical parameters, like the air temperature and the atmospheric pressure. In order to achieve that, we have studied the correlation between the weather conditions and energy consumption of data centres. Using real data obtained from the sensors of the RealDC testbed, part of the FIESTA-IoT platform, we investigated the correlation between the variations in weather conditions and how they affect the energy consumption. Our analysis showed that only certain weather features have significant impact on the energy consumption. We then used the correlated data to build a forecast model using linear regression algorithm. The experimental results showed that the forecast energy consumption manages to predict the energy consumption from the weather conditions with adequate accuracy. These results are indicative as they could provide data centres operators and power distribution companies with tools to manage their power needs distribution. Our future work will include using weather data of longer periods of time to provide more accurate forecast of the energy consumption. The outcomes of the experiment are showcased in the following video<sup>8</sup>.

Furthermore, a web application has been developed, which demonstrates live the outcome of the DC-IoT project.

#### 3.1.2.13 *PARKNOW*

PARKNOW pursues the digital transformation of parking areas, exploiting the possibilities of Internet of Things networks to improve urban mobility efficiency based on the mobility habits of parking users.

PARKNOW takes advantage of FIESTA-IoT platform to access to a network of car parks and traffic information in order to give any developer the ability to build mobile applications to guide and provide useful information to users:

- As drivers, looking for parking their car in the area
- As pedestrians, before taking their car and after leaving their car
- Outdoors and indoors
- Without complex installations or hardware in the infrastructure

---

<sup>8</sup> [https://www.youtube.com/watch?v=9Vyo8G\\_Lblg](https://www.youtube.com/watch?v=9Vyo8G_Lblg)

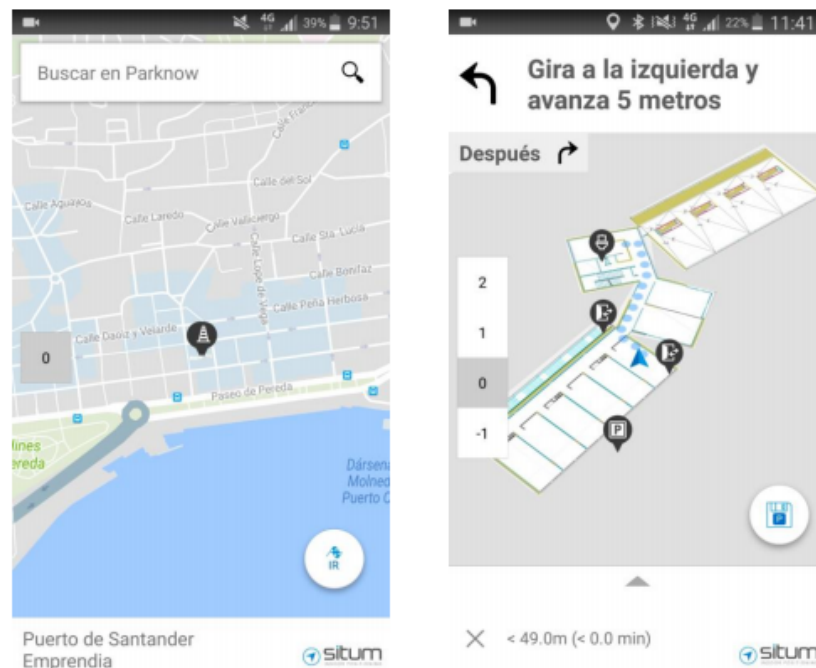


Figure 14. PARKNOW application.

### 3.1.3 Call for Experimenters 4

#### 3.1.3.1 Advanced predictive models for energy consumption in Buildings and Data Centers (B-MODEL)

The B-Model experiment uses the FIESTA-IoT platform to gather large volumes of IoT observations, which are then used to validate advanced Machine Learning algorithms for the prediction of energy consumption in office buildings and data centres.

The experiment uses data from two different testbeds:

- Real DC: a data centre with very high-power consumption, where energy consumption depends mostly on computing resources' usage, cooling needs and weather;
- Smart ICS: an office environment with personal monitoring of energy usage, where energy consumption depends mostly on human occupancy.

To feed the prediction algorithms with multidomain data, this experiment collects heterogeneous data, such as historical energy consumption, cooling temperature, outdoor weather and building's occupancy across the RealDC and the SmartICS testbeds.

Two forecast algorithms for energy consumption have been implemented and validated in this experiment: Deep Learning LSTM (Long Short-Term Memory) univariate and multi-variate models. This experiment has shown that the multi-variate model outperforms the univariate model because is able to exploit underlay correlations between IoT data coming from heterogeneous sources.

A dashboard with a set of visualization tools helps to understand these environments, the associated energy consumption and the performance of these two different predictive algorithms.

- This experiment is also validating some key features of the FIESTA-IoT platform, namely: Testbed-agnostic access to different resources, which means that the hosting testbed is irrelevant to the resource access method;
- Unique platform entry point, which means that all the resources of FIESTA-IoT platform are only accessible through the only entry point with a validated set of credentials.

Thanks to this experiment, ALLBESMART will kick off the development of new products for smart buildings and operational intelligence derived from the analysis of data integrated across multiple and heterogeneous IoT data streams.

#### *3.1.3.2 Real-time data quality assessment in IoT environments (StreamingQualityAnalyser)*

StreamingQualityAnalyser introduces data quality assessment of IoT data streams through probabilistic approaches that according to the literature exhibit strong accuracy.

Our strategic goal is that our new service will complement our Qiqbus commercial streaming analytics platform for IoT, enabling end-users to improve the quality of their data-driven IoT applications and services. This is realized via using our Qiqbus' data quality assessment service in order to indicate sensors producing low-quality data, which might degrade the performance of end-user's applications or services. To further contribute to our goal, we complement our new service with intuitive mapbased User Interfaces (UIs), which help end-users to identify possible flaws within their sensor substrate (based on Modio's service's low quality data indications) and accordingly undertake corrective actions (e.g. replace specific sensors with new ones or update the sensor topology in case that data are lost or delayed due to networking issues) in order to overall improve the performance of their data-driven applications and services.

In terms of our experiments industrial impact, Modio's founding team, having a strong background in cloud, machine learning and data analytics technologies, has decided to grasp the business opportunity in the emerging IoT market including manufacturing, healthcare, smart cities, homes and cars. Our strategic goal is to innovate in the IoT domain with quality assessment techniques for streaming data as well as with novel privacy technologies ensuring that sensitive streaming data are always kept confidential. Both of these two features are not currently supported by existing IoT analytics commercial packages.

During the experiment, we validate the performance of the following innovative approaches to outliers' detection specifically targeting time series:

- i. The 'Generalized Autoregressive Conditional Heteroscedasticity' (GARCH) algorithm that is known to operate with data streams that exhibit temporal locality, i.e. data whose range of uncertainty varies over time.
- ii. A validated outlier detection approach implemented in R's forecast package, `tsoutliers`<sup>9</sup>, that identifies residuals by fitting a loess curve for non-seasonal

---

<sup>9</sup> <https://github.com/robjhyndman/forecast>



- data and via a periodic Seasonal and Trend decomposition using Loess (STL) for seasonal data.
- iii. An outlier detection approach based on Long Short-Term Memory (LSTM) implementation of Recurrent Neural Networks (RNNs).

To validate the performance of the aforementioned algorithms, we leverage the FIESTA-IoT semantics for the following two purposes:

- a) For training our machine learning models, we use historical data which we gather via testbed-agnostic queries of datasets and data-streams.
- b) For acquiring real-time data, we invoke semantic-enabled discovery of resources and observations.

The StreamingQualityAnalyser continuously retrieves data from the FIESTA-IoT platform and specifically from sensors located in the ADREAM, KETI and NITOS testbeds. The data is stored and then analysed on demand to identify outliers using one of the aforementioned approaches above.

The results of the data quality analysis are rendered through a single page web application. The web application helps end-users to identify possible flaws within their sensor substrate and accordingly undertake corrective actions. The application is accessible on the public Internet and available for testing.

Finally, the implementation of our methods for sensor data quality assessment is committed to our Git repository and it is available to the FIESTA-IoT consortium only.

#### *3.1.3.3 Experimentation for developing business services that use real-time data analytics for realizing proactive microenvironmental monitoring in agriculture (Agrolytics)*

Due to huge expansion of IoT sensors, micro-environmental monitoring has become a very important trend in the agriculture. It enables better understanding of the local phenomena and a more proper reaction in case of any variations which might be critical for the micro-environment. Especially important is the possibility to use data analytics methods to learn hidden correlations between the (huge number of) parameters that characterize the micro-environment, which generates completely new knowledge that can be used for proactive acting (before an issue happens). One of the main challenges is the need for an efficient real-time processing of measurements in the field in order to understand the current trend and react proactively, if needed (e.g. due to deviations from usual behaviour). This proactivity is usually based on the models of the normal behaviour, which can be learned from existing datasets or directly from streaming data. These requirements imply the need for realizing micro-environmental monitoring with the support of data analytics, incl. real-time (fast) data processing and predictive analytics.

The vision of Agrolytics is to support the development of advanced data analytics services for proactive agriculture micro-environmental monitoring, through an intensive experimentation related to the performances of such services.

The approach is based on the available sensor data as described in the Call text for SmartSantander and Tera4Agri, which will be combined with the domain knowledge. The framework realizes novel data analytics services that combines CEP (complex event processing) and prediction service, which is proven to be very useful in the case of finding hidden co-relations as described above.



The market we will focus on is precision agriculture where the importance of data analytics is clear and business opportunities for affordable and efficient solutions (as we intend to do) are emerging. We already had contacts with some vineyard owners, being interested in enabling the high-quality grape production through advanced microenvironmental monitoring.

#### *3.1.3.4 VIRTUS: Virtual IoT Gateway for the provision of SDN-based multi-tenant Service Isolation and Interoperability over Heterogeneous IoT Domains*

VIRTUS experiment successfully addresses the IoT interoperability challenge within the framework of 5G networks through the agility brought by the combination of virtualization and SDN, which allow network services to be automatically deployed and programmed.

VIRTUS experiment focuses on using sound data originating from the FIESTA-IoT testbeds in order to validate the INFOLYSiS interoperable IoT virtual GW prototype and then to define the specifications and the computing resource requirements of each IoT mapping function for different data volumes.

In specific, VIRTUS focuses on experimenting on top of individual FIESTA-IoT testbeds by receiving through the unique API data that originate from different testbeds, which are encapsulated in different IoT data protocols (CoAP, MQTT, HTTP) and then are fed in the IoT mapping functions that have been developed by INFOLYSiS. The mapping functions are deployed utilizing the relevant Docker containers INFOLYSiS private cloud infrastructure, where the set of the encapsulated to different IoT data protocols of the FIESTA-IoT datasets are aggregated.

VIRTUS objectives are verified by the results/metrics obtained by four experiments:

- Experiment #1: IoT interoperability provision as a Service between CoAP and HTTP over Docker-enabled infrastructure
- Experiment #2: IoT interoperability provision as a Service between MQTT and HTTP over Docker-enabled infrastructure
- Experiment #3: IoT interoperability provision as a Service between CoAP, MQTT and HTTP over Docker-enabled infrastructure
- Experiment #4: Multi-tenant IoT service isolation of three semantic specific service layers/ domains over Docker-enabled infrastructure

VIRTUS experiment results allowed INFOLYSiS to proceed with the commercialization and market introduction of the two IoT mapping functions as a Service at different price packages. INFOLYSiS two services (CoAP-to-HTTP and MQTT-to-HTTP mapping functions) will be introduced in the market following the dynamic pricing model approach where INFOLYSiS offers two different sets of three price packages depending on the customers' data volume needs and instance requirements (one or multiple).

In specific, based on the results of the experiments 1, 2 and 3, three different packages (Small, Medium and Business) were tested, providing as outcome the minimum requirements needed for the efficiently operation of the two mapping functions under different data rates/volume. Moreover, experiment #4 confirmed the successful service isolation of the mapping functions in an SDN-enabled environment. Consequently, based on these findings, INFOLYSiS proposes the commercialization of the two mapping services under specific PaaS/VPS packages that bear sufficient

characteristics for satisfying end-users needs in terms of data volume and number of instances.

Overall, analysis of VIRTUS experiment results assist INFOLYSiS to accurately develop and adapt its pricing models/strategy and based on them to further proceed with the commercialization and market introduction of its two IoT mapping functions aiming to the satisfaction of the current market needs and requirements for IoT interoperability.

#### *3.1.3.5 Distributed Data Stream Process Gateway Service Empowering FIESTA-IoT Applications (StreamGateway)*

The main objective of the project has been the realization of a usable Distributed Data Stream Processor (DDSP), leveraging artificial intelligence to anticipate problems, detect unexpected event patterns and to optimize processes, services and decisions. In particular, the proposed DDSP has been designed to easily extend the FIESTA-IoT platform as additional modules providing innovative services and making such a disruptive technology accessible at low costs also to SMEs tearing down technological entry barriers. An open and interoperable DDSP gateway has been developed and integrated with the FIESTA-IoT platform to enable self-service, easy and secure analytics workflows development on top of the FIESTA-IoT platform exploiting the provided services and testbeds.

### **3.1.4 Rolling Call**

This section includes the experiments that does not belong to the open calls, but use the FIESTA-IoT platform.

#### *3.1.4.1 LoRa testbed dimensioning and real-time monitoring*

LoRaWAN is a Low Power Wide Area Network (LPWAN) specification intended for wireless battery-operated things in a regional, national or global network. The technology is extremely low power consumption that the battery life is considerably extended, and with the long-range feature, a given area can be completely covered by only a few of such sensors. For the network dimensioning of the LoRa network to be deployed, in order to cover the territory with the minimum sensors, some pre-deployment network tests need to be performed to determine the needed total number of LoRa devices and the position of each of them by drawing a map of network quality related parameters. For a functional LoRa network, the real-time monitoring of the network quality is also mandatory to perform appropriate device management in order to guarantee a certain service level by provisioning necessary backup devices in case of deterioration of some devices. For achieving that, a real-time network quality map is also necessary.

In the project, the network quality related parameters from the Grasse Smart Territory testbed will be used to dimension the ongoing LoRa network deployment in this area, as well as to monitor the LoRa devices already deployed. By crossing the evolution of the network quality with other information such as weather conditions and geographical profiles of the given area, more information can be deducted such as the prediction for additional device provisioning in some weather conditions. The real measurement data will be compared to the theoretical data obtained by running network simulation in order to understand the gap between the theory and reality situation.

The expected outcome of the project will be a service to the operator providing real-time network quality map showing the LoRa network of the Grasse Smart Territory testbed, as well as to better dimension the devices to be deployed in the future.

## 3.2 External Experiments: Functional Evaluation

### 3.2.1 Evaluation criteria

As final users of the FIESTA-IoT platform, the OC experimenters are asked to fill up a questionnaire and a KPI evaluation form, to evaluate the functions and quality of the platform.

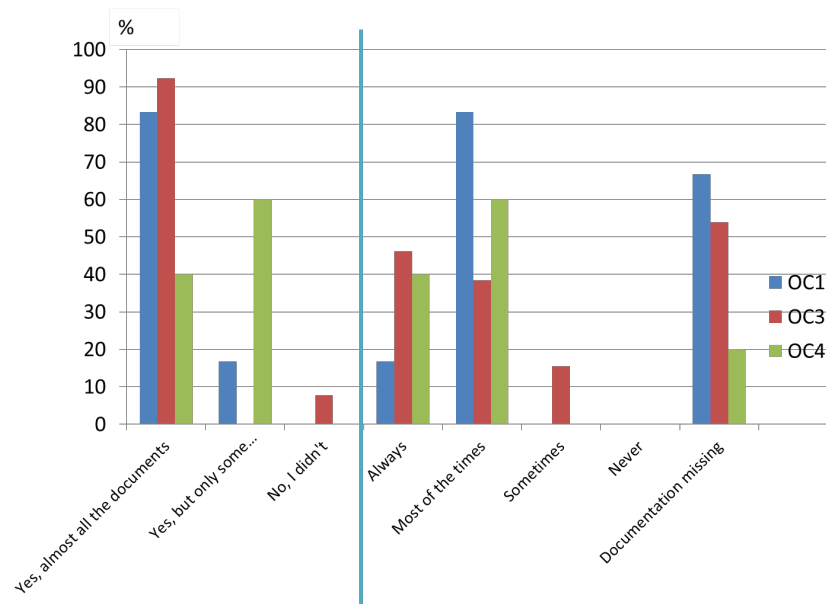
Already explained in D5.2 (FIESTA-IoT D5.2, 2017), the interactions between the experiments and the FIESTA-IoT platform can be grouped into two phases: integration phase and execution phase. At the end of each phase, experimenters are asked to evaluate the FIESTA-IoT concept, tools and resources. For more details of the questionnaire and the KPIs evaluated by the experimenters, please refer to D5.2 (FIESTA-IoT D5.2, 2017) Annex V.

### 3.2.2 Evaluation results

After analysing the KPIs evaluation and the responses to the questionnaire from the 3 waves of Open-Call (OC1, OC3 and OC4), we obtain the following results.

#### *Quantity and quality of the documentation*

Figure 15 shows the percentage of the useful document among all the offered documentation, and the percentage of users that find the needed document. Most of the users confirm that they have used all the documents and they were able to find the needed information for their development and deployment in most of the time. Missing documents are reported less in OC4 regarding to the previous OCs.



*Figure 15. Documentation consulted; on the left side is the quantification of the document consulted among the available one, on the right side is the assessment of the quality of documentation.*

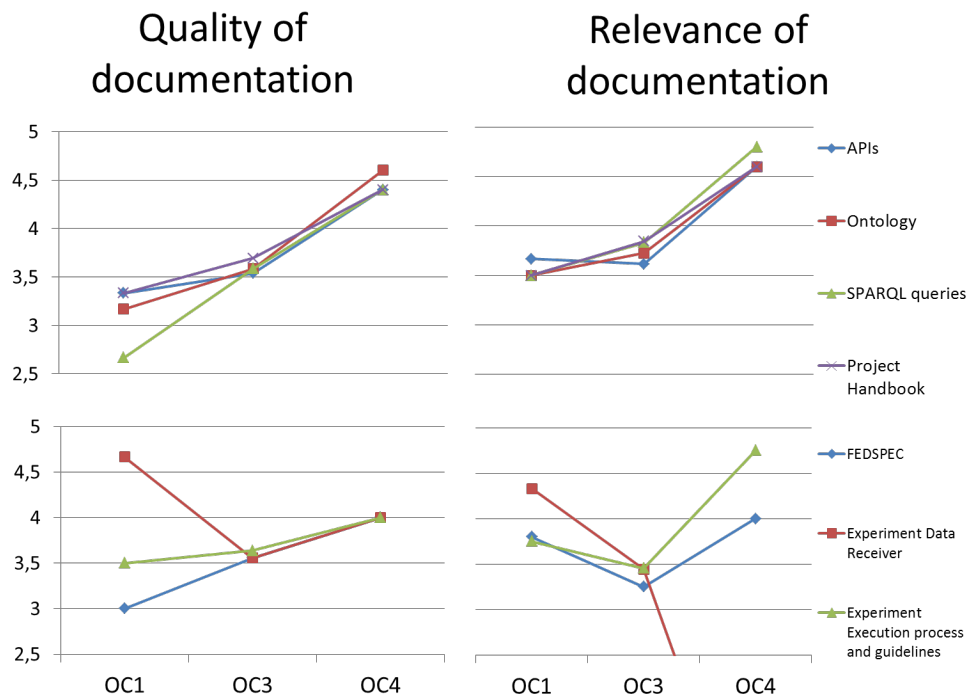


Figure 16. Quality and relevance of documentation.

Figure 16 shows the evolution of average score of the quality and relevance of the documentation from OC1 to OC4. It is obvious that all the concerned aspects have been improved during the Open-Calls. The only line that drops after OC3 is the one about the “relevance of documentation” on the aspect “experiment data receiver”. The reason behind this anomaly is that this aspect is marked “N/A” by all the OC4 experimenters because it was not used by anyone. The “low position” of this point actually points to “N/A”.

### Ease of setting up, ease of deployment

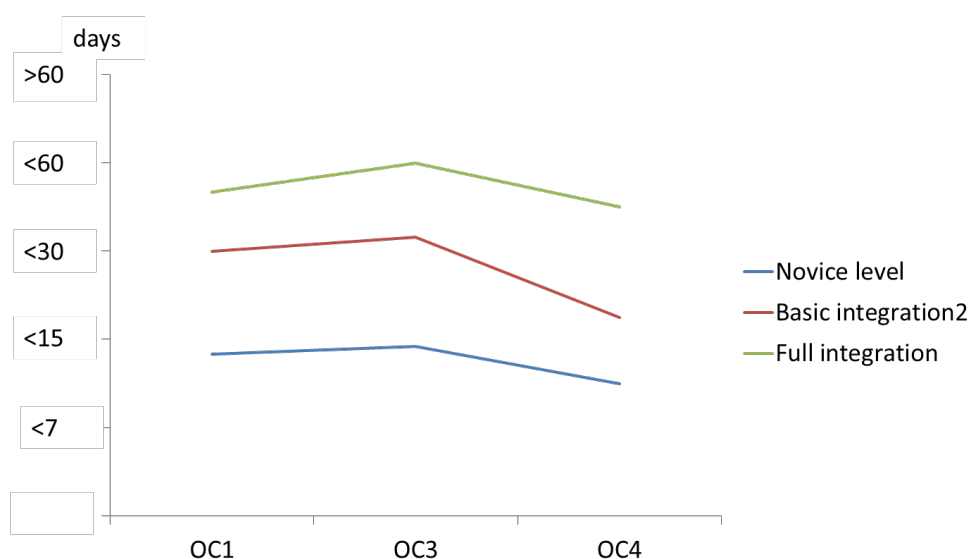


Figure 17. Time for integration.

Figure 17 shows the average time for integration of the experiments on the FIESTA-IoT platform. It is obvious that the average time for integration is shorter in the last OC than the previous ones in every integration level.

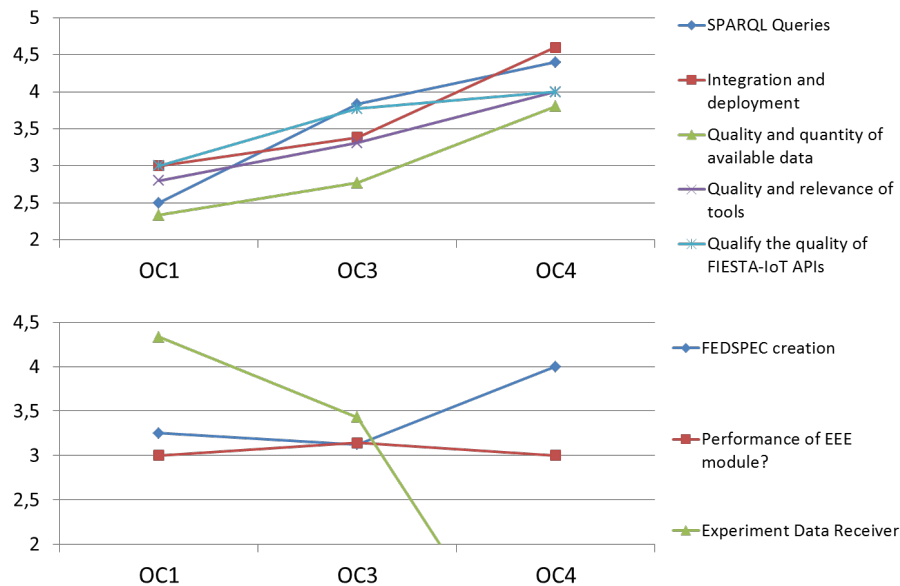


Figure 18. Assessment on FIESTA-IoT tools.

In Figure 18, every line represents the evaluation of one FIESTA-IoT tool. The scores 5 to 1 represent respectively “Excellent”, “Very good”, “Good”, “fair” and “poor”. The score 0 is attributed to “N/A” (not applicable) which is not taken into account for the average score calculation. From the graph we can clearly see that most of the tools have been improved during the three OCs. The score of “EEE module” stagnates and the “Experiment Data Receiver” score drops because it is N/A as no experimenters of OC4 have used the Experiment portal. All the tools have reached the “Good” level so that we can say the quality of all the tools is satisfactory.

Figure 19 shows the percentage of usage of the FIESTA-IoT platform API increases through the OCs, which indicates that the experimenters prefer more flexible interactions with the platform.

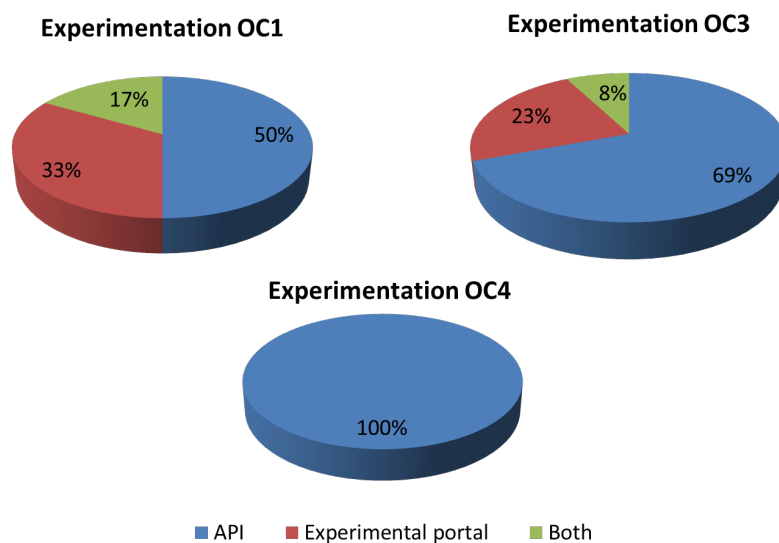


Figure 19. Usage of API or Experimental portal.

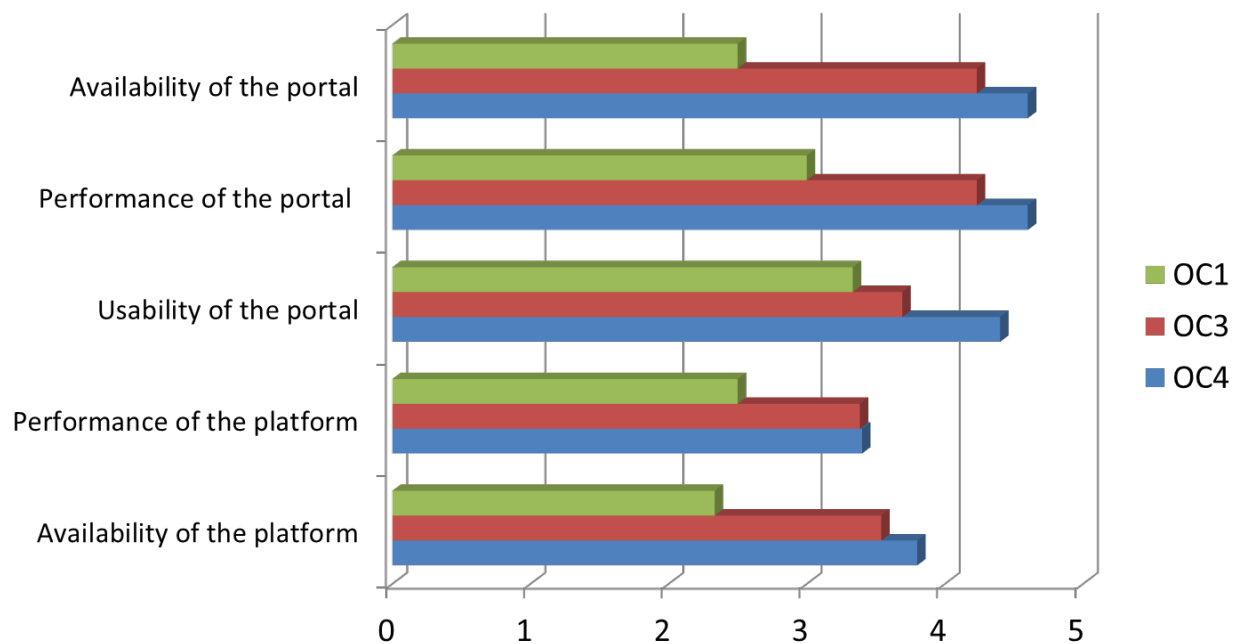


Figure 20. Assessment over the platform and experimental portal.

Figure 20 shows the evaluation on different aspects of the quality of the experiment portal and the platform, including availability, performance, and usability. It can be observed that all the aspects have been improved during the OCs, and all have reached a satisfaction level more than “Good”.

#### During the experiment

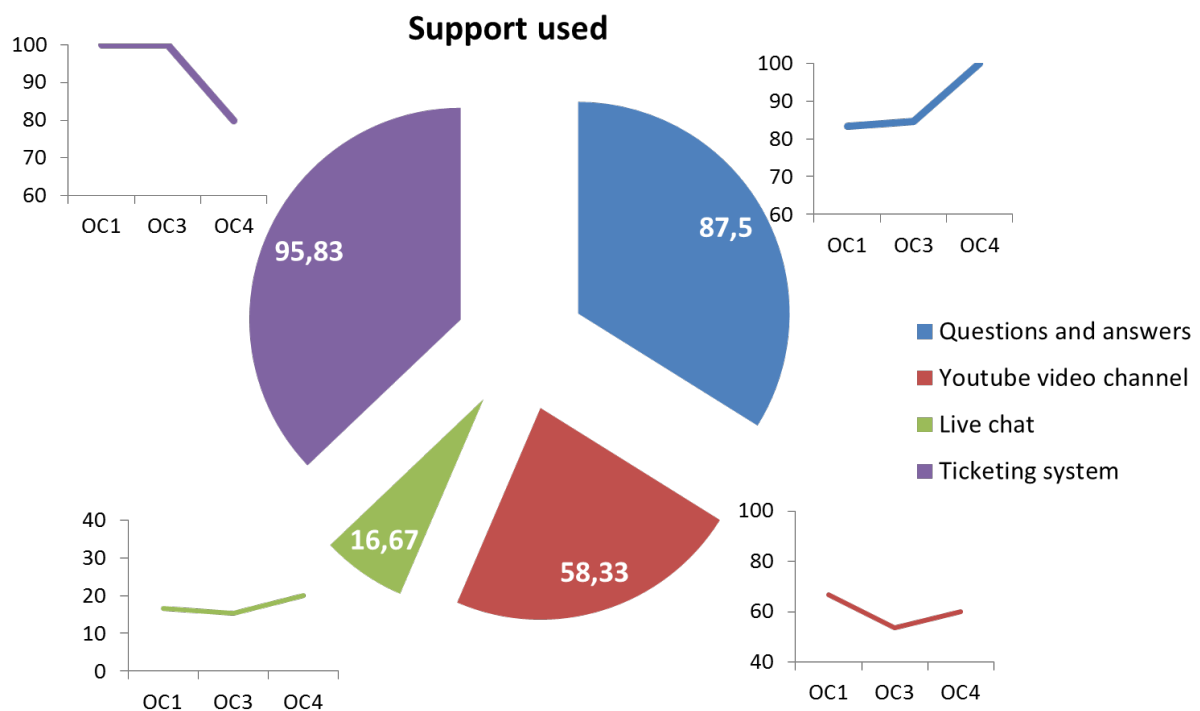


Figure 21. Usage of the different support channels.



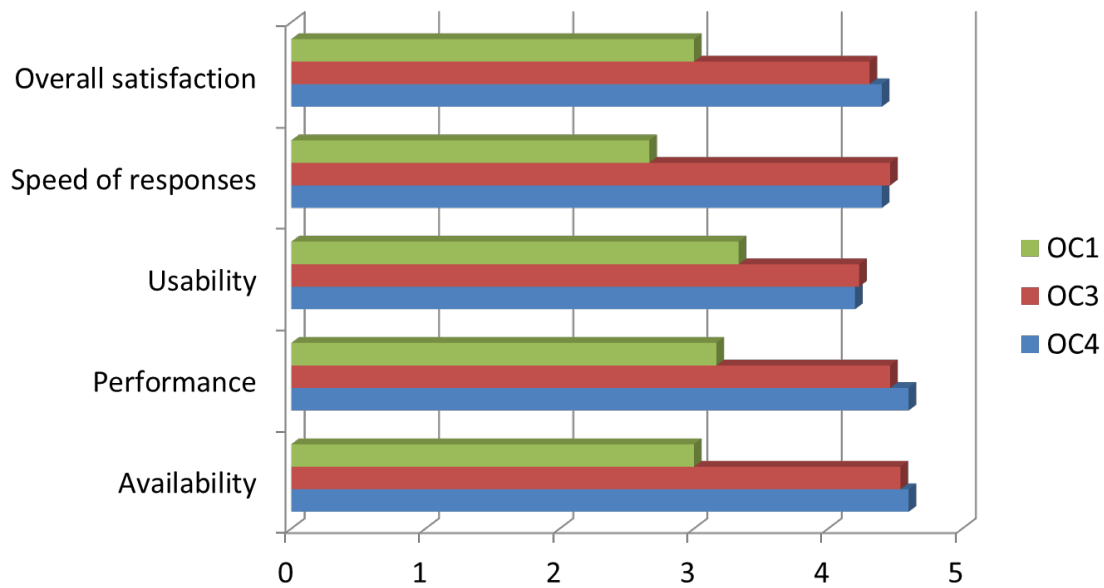


Figure 22. Feedback over the usage of the ticketing system.

The above Figure 21 and Figure 22 show the evaluation and feedback on the usage of the support channels. The Pie Chart shows the overall percentage of the experimenters who used the channel over the total of the experimenters. The ticketing system and the online FAQ are the most used ways by the users. However, it can be observed that the percentage of usage of one channel evolves during the OCs. With the questions and interactions with the experimenters during the first OCs, the FAQ have been enriched during the time with the contents that interest the experimenters. Therefore, the usage of the ticketing system dropped while the usage of the FAQ increased as the answers to most of the questions can be found in the FAQ. The YouTube videos are highly consulted and reported as very useful from most of the experimenters. Figure 22 and Figure 23 shows that the quality of the ticketing system has been much improved from OC1 to OC4 that it reached finally an average of “Very Good” score from the users.

### Ending the experiment

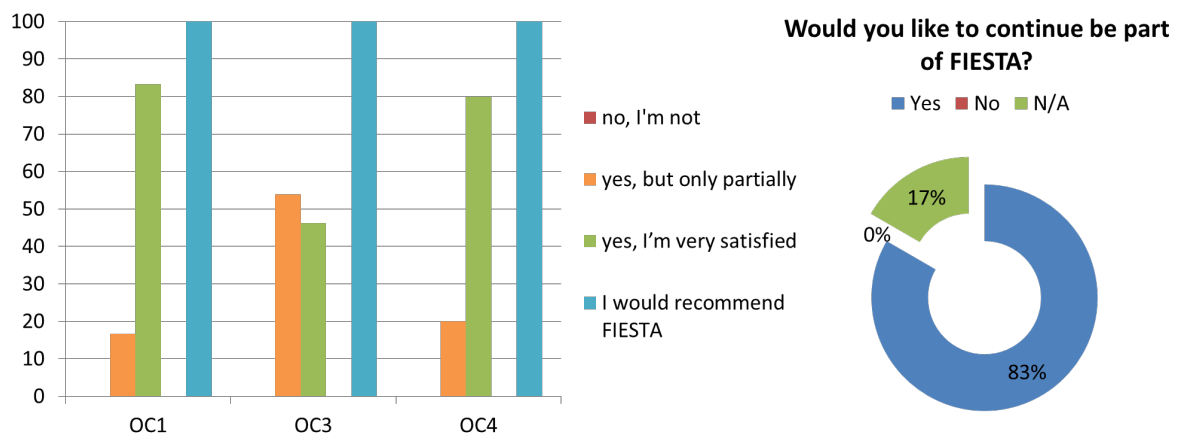
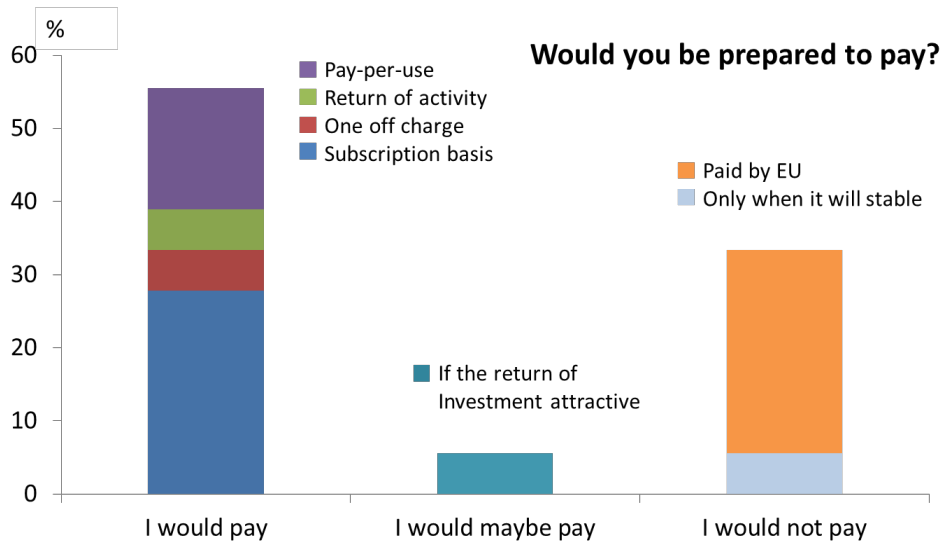


Figure 23. Overall satisfaction of experimenters.

In *Figure 23* the satisfaction decreased on OC3 most likely because third-party testbeds were perhaps not working very well. In OC4 it seems that the satisfaction grew again, therefore the new integrated testbeds were better integrated.



*Figure 24. Market appealing of the FIESTA-IoT platform.*

*Figure 24* shows the market interest of the FIESTA-IoT platform. These questions were only added from OC3. The answers are diversified to almost 50-50 for paying/not paying. The platform needs to present more stability and added value to attract companies or institutes to pay for it.

*Table 6. Tools validated by third-parties experimenter. An X indicates a full validation, a + indicates a partial validation.*

	DataQuest	DATE	CREDIT	PilotThings	SPIAM	Talk2FIESTA	FM2I	FINETUNE	SmartComfort	RedEvents	2CENTs	SpyIoT	Surf	SmartPedestrian	BeSmart	KaaS_SCL	DCIoT	Energylot	Parknow	VIRTUS	B-MODEL	DDSP-GW	StreamingQualityAnalyzer	Agrolytics	Count
OpenAM	X	X	X	X			X	X	X	X	X	X	X	X	X	X		X			X	X	X		
IoT Registry		X	X	X			X	X	X	X	X	X	X	X	X	X	X	X		X	X	X	X	X	
IoT service endpoints	X	X	X				X		X	X	X	X	X					X				X	X	X	
FIESTA-IoT Ontology											X														
SPARQL endpoints						X																			
API REST	+	X		X		X	X			X	X		X	X	X	X	X	X	X						
Rersouce browser																									
Moodle	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X		X	X	X	X	X	
ERM			X		X				X																
EMC			X		X				X																
EEE			+		X				X																
Experiment Data Receiver									X																
Portal			X						X						X										
Postman collection					X																				
Testbed Monitor																		X			X				
Analytics																		X							
Ticketing system	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X		X	X	X	X	

Table 6 shows a complementary result of platform tool validation via OC experiments regarding to Figure 18.

### *Open feedback from experimenters*

From the many open comments done by experimenters it was quite general satisfaction about the concepts of the FIESTA-IoT project. In particular the access to a vast variety of IoT data with a single interface in an agnostically manner was the most appreciated feature. A long learning phase of the initial knowledge of the FIESTA-IoT platform has been suffered by many experimenters. We believe that this is due to the quite innovative approach of the FIESTA-IoT project and therefore a different mindset on conceiving silos IoT experiments. In fact, in *Figure 17* it is reported that 15 days are necessary to have a basic understanding of the platform. Nevertheless, after breaking the initial barrier, a full integration and experiment execution needs not more than 2 months. Indeed, the basic requirement of creation of the SPARQL query was not seen as a big obstacle to overcome since the documentation and the example provided by the FIESTA-IoT has been well appreciated and brought to a straightforward implementation of the needed queries. This is also implicitly shown in *Figure 18* where the creation of SPARQL queries assessment has achieved, in the last phase, a 4.5.

The weaknesses of the platforms are more related to technical issues like the stability of the performances of the API calls. These problems have been reported by different experimenters that are also acknowledging a sensible improvement over the time and a good support from the FIESTA-IoT team. In fact, together with the numeric parameter in *Figure 20*, also open comments stated the considerable enhancements on stability and performances of the platform, also by the means of the implementation of the new handling strategy of the historical data in time-sliced graphs. In addition, despite having a wide range of available resources, the observations from testbed were often not of good quality or even missing. This aspect, not directly due to the FIESTA platform, can be improved with continuously monitoring of the integrated testbed. Finally, the ticketing system is not seen as a user-friendly support system, since the procedure to create the tickets and get an answer might take too long, whilst an up-to-date set of FAQs would be a much more appreciated by experimenters. FIESTA-IoT team has already made steps towards this direction as reported in (*FIESTA-IoT D5.4, 2018*).

### *Conclusion*

The feedback and evaluation from the OC experiments have given us insights not only on the quality of the FIESTA-IoT platform, but also on the evolution of the quality thanks to the interactions with the external users. The quality of the platform has been proved sufficient and improved by the experimenters.

## **4 TESTBEDS INTEGRATION**

The FIESTA-IoT platform aims to provide a practical framework for integrating IoT testbeds focusing on a diverse range of domains, by the provision of accessible and updated online documentation on modelling and interfacing, a step-by-step validation mechanism, and simple but effective interfaces. This can only be verified by new coming testbed providers. In addition to successful integration, the Open-Call Testbed providers (OCTP) were requested to provide feedback on the process of integration.

### **4.1 Testbeds integration Summaries**

A summary for each integrated testbed is presented below.

#### **4.1.1 NITOS**

The iNFInITE project was a great opportunity for NITOS to join a well-established federation, by integrating the NITOS Wireless Sensor Network (WSN) Testbed to one of Europe's biggest Platforms (FIESTA-IoT Platform) in the area of IoT technologies. NITOS Future Internet Facility is an integrated facility with heterogeneous testbeds, located in Volos Greece, which focuses on supporting experimentation-based research in the area of wired networks, wireless networks and IoT in general. NITOS WSN testbed is deployed in University of Thessaly's (UTH) premises, in NITlab (1) and it consists of NITOS Wireless Sensor (WS) Motes prototypes developed by UTH, capable of supporting open-source and easy to use firmware and exploit several wireless technologies for communication (ZigBee, Wi-Fi, BLE and LoRa). The office/building setup provides metrics related to the environment conditions and composes an integrated application of WSN in real-life scenarios. In order to integrate NITOS WSN testbed to the FIESTA-IoT, we followed a well-documented, straightforward procedure that consists of several steps. Through the NITOS integration with FIESTA-IoT users from both communities, benefit by the new capabilities that NITOS brings to FIESTA-IoT and vice versa.

#### **4.1.2 GRIDNET**

By means of the MARINE testbed integration, we aimed at enhancing the domain diversity and experimentation capacity of FIESTA-IoT. The integration introduced 7 sensing devices to the platform that are spread between two totally different deployment environments, namely a city environment and a coastal one, both located in the area of Volos city, in Greece. The different sensor devices are able to generate 16 different types of measurements, spanning from air and sea water quality measurements to energy consumption data. The testbed integration process was straightforward, well documented and greatly supported by the FIESTA-IoT members whenever required. In GRIDNET SME, we look forward to having FIESTA-IoT users accessing the data being continuously generated and pushed to the platform by the MARINE testbed, as we believe that it is of great value for experimenters and developers working in the city and marine IoT domains.

### 4.1.3 ADREAM

The ADREAM building is a living lab providing a horizontal platform to foster research projects, either focused on one aspect of the building or cross-domain. The building is meant to have as little energy footprint as possible and is thus equipped with large sets of solar panels. Its heating and air conditioning systems are also energy-optimized, with the use of natural ventilation, heat pumps and a ground-coupled heat exchanger. To monitor the activity in the building, over 6500 sensors are deployed and produce around 500.000 data points daily. These sensors are organized in 4 sub-systems:

- Lightning, monitoring the luminosity in the building and the power consumption of lamps, as well as controlling the lightning dynamically
- HVAC, monitoring and controlling temperature and air flows
- Energy, monitoring the energy consumption of all the appliances in the building
- Photovoltaic, measuring the power produced by the solar panels as well as the
- Environmental conditions.

#### Technical characteristics

- Area: 1,700 m<sup>2</sup>
- Technical facilities: 500 m<sup>2</sup>
- Office: 700 m<sup>2</sup>
- Photovoltaic: 100 kWp
- Solar panels area: 720 m<sup>2</sup>

#### Chronology

- Start of construction: June 2010
- Delivery of the building, installation of platforms: December 2011
- Host the 1st project: January 2012

The building was initially built in order for the data produced by the sensors to be used for research purposes internally. The integration of the ADREAM testbed to the federation has the double objective to make our data available for research outside of our laboratory, potentially leading to collaborations, and to enable our experimentations to be run on external testbeds. Integrating our testbed to a larger federation provides us visibility.

### 4.1.4 FINE

IoT technology fragmentation, along with the lack of global IoT standards, has led to the creation of isolated IoT systems, incapable of communicating with other systems that use different technologies; hence, creating barriers for interoperable heterogeneous IoT systems. FIESTA-IoT focuses on the problem of formulating and managing IoT data from heterogeneous systems and environments by integrating IoT platforms, testbeds and their associated silo applications within cloud infrastructures. The main aim is to enable an Experimentation-as-a-Service (EaaS) paradigm for IoT experimenters, making feasible the use of a single EaaS for executing experiments over multiple IoT platforms.

FINE has designed and developed a FIESTA-enabled heterogeneous testbed, significantly contributing to the FIESTA-IoT vision. FINE re-uses the architecture, software and hardware components of the IoT project RERUM [1] and provides a



plethora of sensory data for: (i) environmental monitoring (ambient temperature, humidity, ambient light, noise, PM10, NOx, O3, SO2, VOC, atmospheric pressure, wind direction and speed, rainfall), (ii) electricity consumption (AC current and voltage), (iii) network monitoring (RSSI, LQI, network statistics, etc.), (iv) device energy consumption (CPU, LPM, Transmit, Listen), (v) outdoor parking (magnetic field differentiation) and (vi) smart home management (voice direction-of-arrival). Significant effort has been put to the voice-enabled IoT interface during the development of the FINE extension. The data are collected every nine minutes and are transmitted to the FIESTA-IoT platform.

There are several benefits from the integration with the FIESTA-IoT platform:

1. FORTH can showcase the flexibility of the RERUM platform and how it can contribute to the vision of the IoT interoperability
2. FORTH members involved in FINE have gained significant experience on IoT interoperability issues and more specifically on semantic interoperability
3. FIESTA-IoT members will get significant feedback that will help them to improve the FIESTA-IoT platform
4. FIESTA-IoT experimenters will gain access to a number of available datasets.

#### **4.1.5 Tera4Agri**

Today agronomists need to use information from many different data sources, difficult to integrate in a meaningful way because very often relevant data sources do not offer open data interfaces, so agronomists need to either manually verify data or dump data into csv files and process them in some common purpose tools.

Considering the data formats that currently used in the agricultural production environment, we can say that the conversion in LOD compatible format of the data created within this environment can allow the easy integration of data providing the possibility to make queries on them by means of SPARQL language. Tera4Agri experiment allowed us to integrate data concerning the smart agriculture domain within the FIESTA-IoT platform, enabling the platform for the implementation of innovative experiments in the domains of agriculture, as well as can do other testbed of this domain, integrating data from several types of sensor for Agriculture. In this way, it will be possible to consider the testbed for the experimenters in order to show the added benefits that FIESTA-IoT can provide in this domain.

The testbed is located in Minervino Murge (BT – Apulia Region - Italy) in the Tormaresca - “Bocca di Lupo” estate: a farm which covers an area of about 500 hectares of which 350 are planted with vines and 85 with olive trees. It stretches along the Adriatic coast, thus creating a unique landscape of vineyards that are born through woods and pine forests and are lost before their eyes up to merge with the sea. The Tormaresca- “Bocca di Lupo” Estate is part of Marchesi Antinori Spa company. Marchesi Antinori Group is one of Italy’s top wineries.

The Florence-based company had a turnover of around 220 Mio Euro in 2016. It produces more than 23 million bottles per year, most of which is pressed from the company's own grape production. Thanks to the Tera’s gateway GloE, the testbed is able to collect data from sensors installed by TERA in the estate.

The sensors installed in the estate are essentially of two types: sensors for environmental monitoring and sensors for the soil monitoring.

#### **4.1.6 RealDC**

Data centres (DCs) are currently consuming an average of 2% of the electricity produced (based on U.S. consumption alone). Efforts to improve the efficiency of these facilities has yielded impressive results in the last 5 years but authoritative sources assert that better data is needed to continue further. We believe that IoT in DCs provides the best solution to monitor and improve DC efficiencies. A critical mass of DCs publishing their usage data is required to correlate and develop best practice solutions for energy savings. Different types of data centres have varying power and water consumption profiles. The current best practice of using PUE (Power Usage Efficiency) doesn't provide the full picture of DC performance.

In response to the above, the purpose of this project was to integrate a live Data Centre into the FIESTA-IoT ecosystem. This integration comes in the form of sensor data on power, cooling and ambient weather, captured at five-minute intervals, which will be made available to experimenters and other data centre owners as open linked data set through the FIESTA-IoT facilities.

#### **4.1.7 Grasse Smart Territory**

This testbed has been integrated by EGM as partner of the consortium.

The Grasse Smart Territory testbed is an experimental testbed for Smart City applications for the urban, suburb and rural areas of the City of Grasse. It is still under development with the collaboration of the local authorities and other local associations and companies. It aims to provide more digital facilities and applications to the citizens to make life greener and more efficient using state-of-the-art IoT technologies. The main interest of the public authorities' managers is to understand the way IoT technologies can benefit to citizens in urban, peri-urban and rural areas and identify the sustainability model of such deployments at a time of reduced budgets and increasing constraints on data management (such as GDPR or open-data regulations).

The testbed privileges the use of LoRa technology for the connectivity of devices, which can significantly extend the battery life on the field devices. Several environmental sensors, i.e. CO<sub>2</sub>, pollen, humidity, are being deployed and tested to be connected to the testbed. Another advantage of LoRa technology is its "long range" that a gateway can serve for an area of several kilometers of radius in which all the devices can connect if there is no obstacle between them. Several devices have been deployed on the field to monitor the network quality (i.e. RSSI, HDOP) between them and the gateway in order to provide real-time information of the network quality.

Several Smart City applications are planned to use the testbed. Among them: "digital playground for education" application aims to create a pedagogical platform for local high school students to learn and to practice with the latest IoT technologies. "Green transportation" aims to monitor the noise and air pollution status in the city in order to trigger necessary actions to encourage citizens to use public transportation as a function of the level of pollution. "Waste management" aims to spot abnormal behaviour or objects around the waste container in order to trigger necessary measures at the related authorities or organizations.

Data centres (DCs) are currently consuming an average of 2% of the electricity produced (based on U.S. consumption alone). Efforts to improve the efficiency of these facilities has yielded impressive results in the last 5 years but authoritative sources assert that better data is needed to continue further. We believe that IoT in DCs provides the best solution to monitor and improve DC efficiencies. A critical mass of DCs publishing their usage data is required to correlate and develop best practice solutions for energy savings. Different types of data centres have varying power and water consumption profiles. The current best practice of using PUE (Power Usage Efficiency) doesn't provide the full picture of DC performance.

In response to the above, the purpose of this project was to integrate a live Data Centre into the FIESTA-IoT ecosystem. This integration comes in the form of sensor data on power, cooling and ambient weather, captured at five-minute intervals, which will be made available to experimenters and other data centre owners as open linked data set through the FIESTA-IoT facilities.

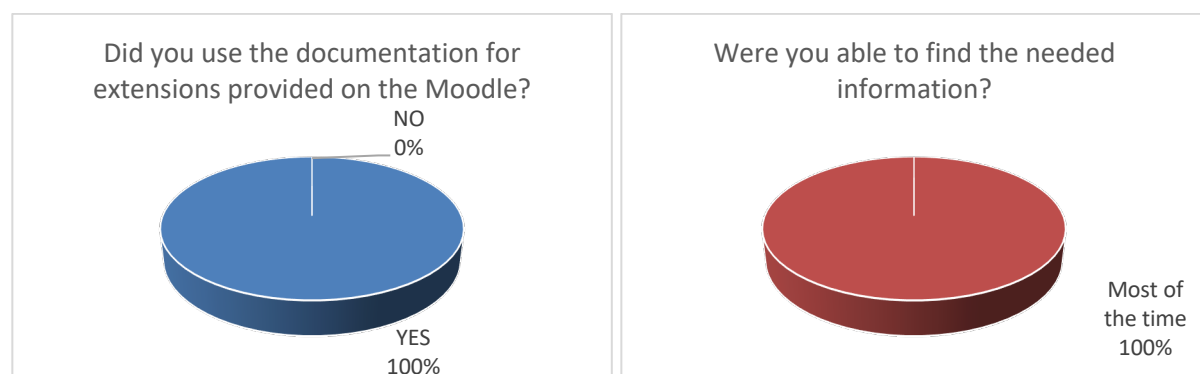
## 4.2 Testbeds Integration: Functional Evaluation

The functional evaluation of the testbed integration process was based on feedback provided by the Open-Call Testbed Providers (OCTP). The format of the feedback was based on a set of two questionnaires which reflected the requirements that were set by the FIESTA-IoT platform for successful integration. The feedback was split into two sections:

- The **evaluation** of the usability and convenience of the FIESTA-IoT tools and resources made available for the testbed providers to complete the testbed integration process.
- The **assessment** of the requirements, and the effort to address them, (like annotation process, certification of yhr testbed, and interfaces implementation) in order to complete the testbed integration.

### 4.2.1 Evaluation of FIESTA-IoT Resources and Tools

The first set of questions focused on the material available to guide the OCTP to integrate.



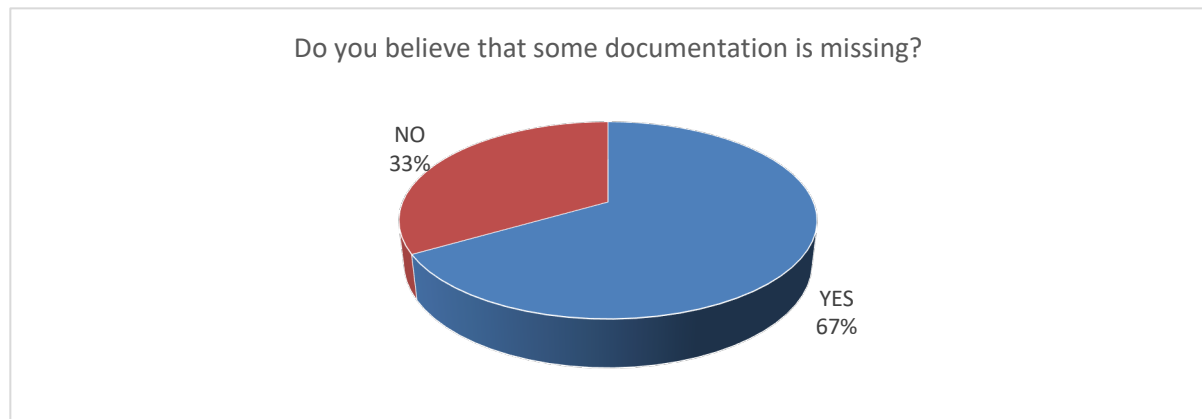


Figure 25. Documentation evaluation.

All OCTP made use of the documentation provided on Moodle and were able to find the required information most of the time. Most of the OCTP stated that there was missing information. This was mainly related to security access mechanisms, error codes, more SPARQL examples, available testing facilities, certification process and APIs.

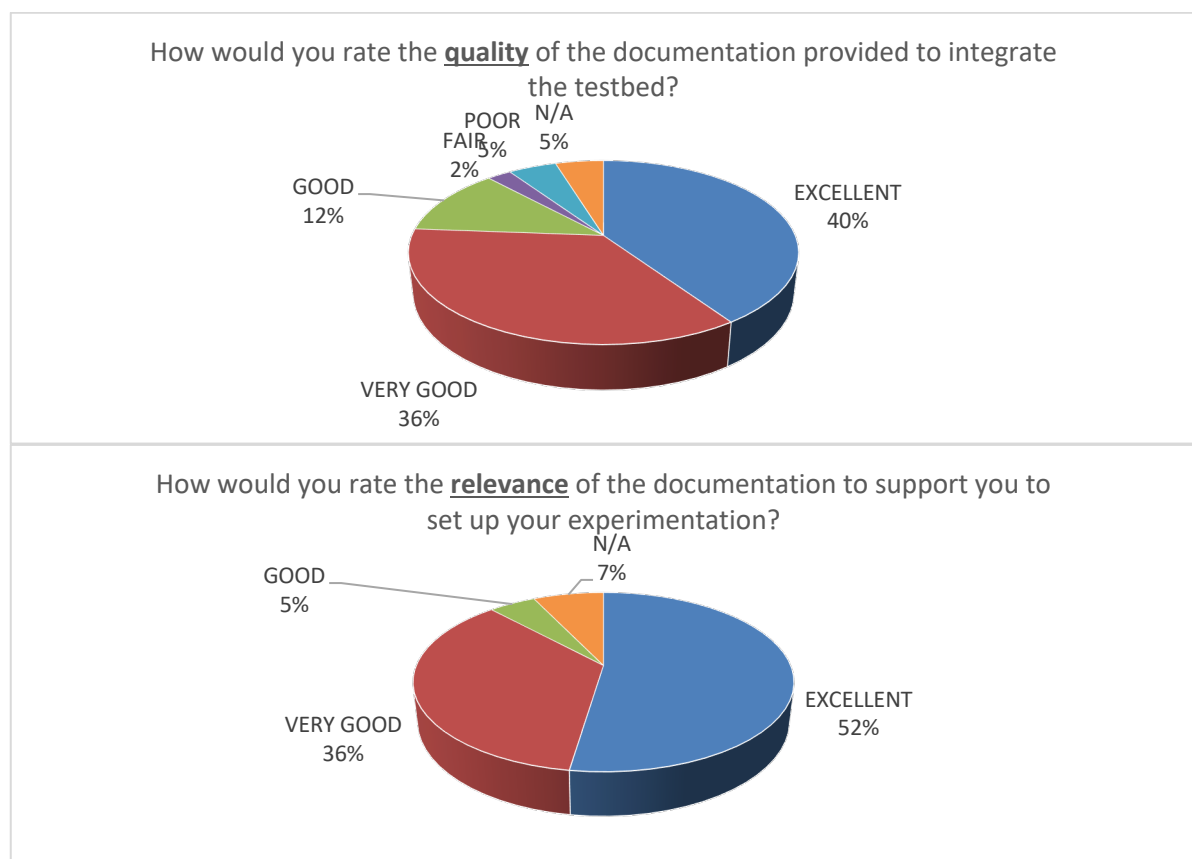


Figure 26. Quality and Relevance of the Documentation.

The quality and relevance of the documentation was then asked. This related to documentation about:

- APIs
- Ontology
- Annotators
- Annotator as a Service
- Testbed Provider Services
- Testbed integration process and guidelines
- Overall documentation in the Project Handbook

In terms of the quality of the documentation, the majority believed that it was excellent or very good. The main concern was with the documentation on the annotation and testbed integration. The relevance of the documentation was rated much better.

The next part of the questionnaire focused on the activities during the testbed integration process. The components related to this were:

- Certification Portal
- Annotator-as-a-Service tool
- Testbed Registration process
- Resource Registration process
- Testbed Provider Interface Configurator

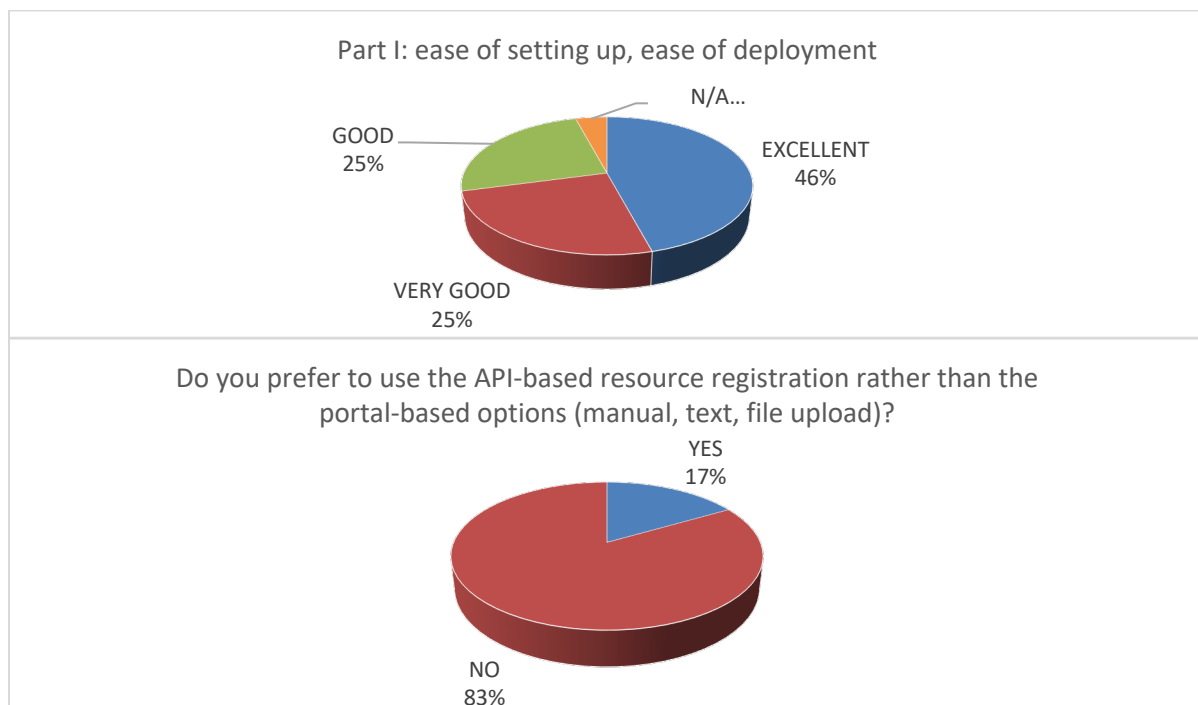


Figure 27. Testbed integration evaluation.

During the testbed integration process, most OCTP agreed that the ease of deployment was above satisfactory. When it came to Resource Registration, the majority preferred the portal-based option over the API-based option.

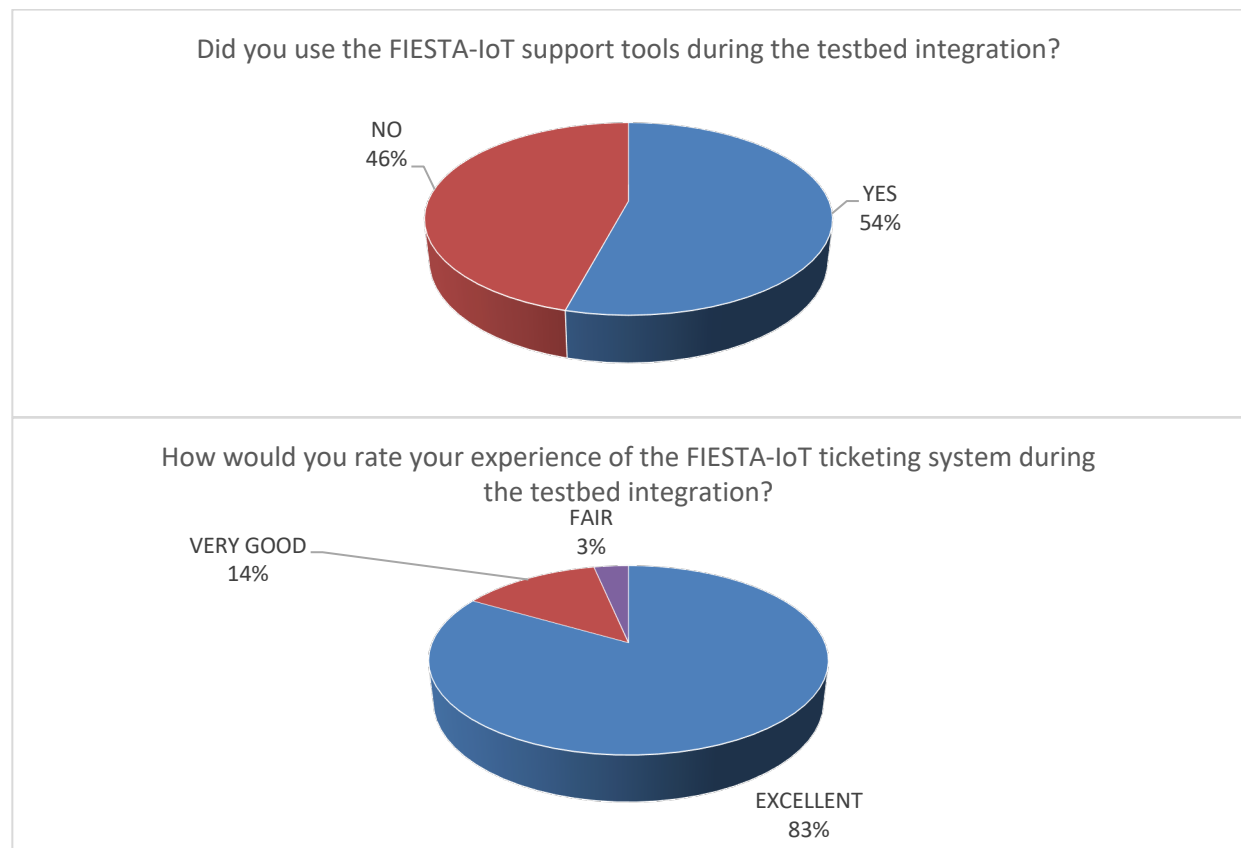


Figure 28. Support Evaluation.

For support, a slight majority made use of the support tools that were provided, i.e.:

- Q&A
- YouTube channel
- Live chat
- Ticketing system

The least effective medium was the live chat, and the most was the ticketing system.

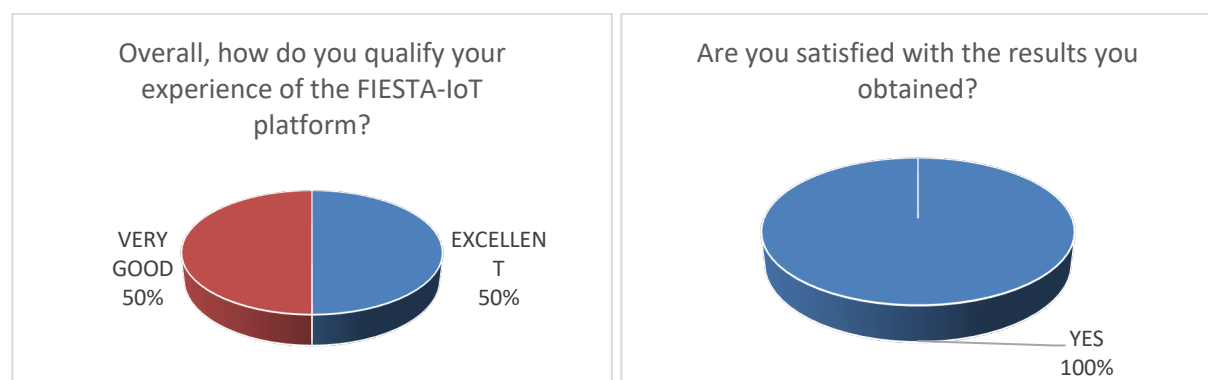


Figure 29. Overall Experience Evaluation.



All OCTP had either a very good or excellent experience of the platform, and all were satisfied with the results.

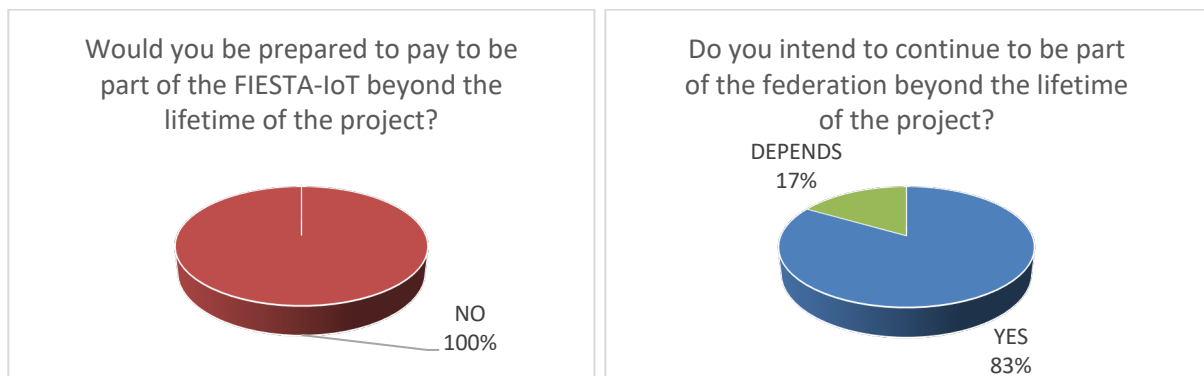


Figure 30. Evaluation of Future Plans.

None of the OCTP was prepared to pay for the service. The reasons included:

- European funding should be provided to support experimenters and SMEs to adopt the platform. Dedicated support could also be a means of income
- Data consumers of different types should provide a financial contribution to support the system
- FIESTA-IoT should seek funding from calls addressing new challenges such as blockchain and AI

Most of the OCTP intend to continue to be part of the federation after the project ends. One OCTP mentioned concerns with funding for support and maintenance.

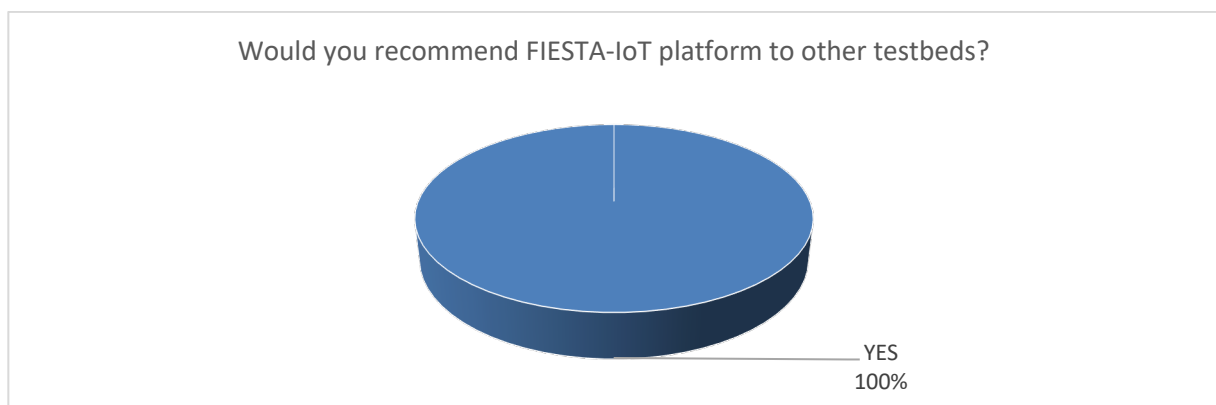


Figure 31. FIESTA-IoT recommendation.

All OCTP agreed that they would recommend the FIESTA-IoT platform to other testbeds.

### 4.3 Conclusions

Several insights can be learned from the feedback provided by the OCTPs. A significant percentage thought that the documentation was not complete. The quality of the documentation was acceptable, and was relevant to support their testbed. This demonstrates that software is as good as its documentation, and hence is a very important aspect for any adoption of technology. Once understood, the setup and deployment process were easy to conduct according to the majority of the OCTPs.

The aim of providing an API-based integration mechanism is to automate the process for quicker integration. But the majority of the OCTPs preferred to use a user interface for this process. For support, the ticketing system was most effective among all the other tools provided. When it came to the financial support of the platform, all OCTPs stressed that funding should come from sources outside of the federation, whether it be research funding or data consumers.

Finally, all OCTPS had a positive experience of the integration process, were satisfied with the results, and wanted to continue to be part of the federation. This demonstrates the FIESTA-IoT platform provides an effective and practical ecosystem for heterogeneous IoT testbeds to integrate and contribute to the diversity of the federation in its themes and domains.

## 5 FIESTA-IOT PLATFORM: NON-FUNCTIONAL EVALUATION

### 5.1 Introduction

Within section 3 we have analysed the functional evaluation of the platform, including the suggestions and comments from external experimenters. However, in order to complete the evaluation of the platform considering the technical details, we have performed a complete evaluation of the platform through the analysis of the requests performed during the Open-Calls to the IoT-Registry component.

The FIESTA-IoT platform has been built on top of the IoT-Registry component, which is the core of the platform, in which all the calls are performed. It has a two-fold approach: on the one hand, it supports the tools that provide extra functionalities for the external experimenters and testbed owners and, on the other hand, it takes care of the information management that is injected into the IoT-Registry. In that regard, it also supports the security component, openAM, which provides a direct API endpoint access to external experimenters.

The main components within the IoT-Registry are described below:

- **Semantic Triplestore database**  
This is the core of the component and provides the storage functionality for the RDF data based on the FIESTA-IoT ontology.
- **Resource Manager**  
This component is in charge of analysing and supervising the data that external testbeds are registering, if they match with the previously registered resources. Additionally, it provides access to the existing resources information, providing resource discovery functionalities.
- **Resource Broker**  
It provides access to additional services that might be attached to the resources provided by the different testbeds (e.g. actuators), while keeping the agnostic nature of the platform. Additionally, it provides an extra security layer for authorisation, based on the policies defined along with the testbeds.
- **Semantic Data Query Endpoint**  
This component exposes the endpoint to inject and retrieve data to/from the database. The access is provided by exporting the query functionality using the SPARQL protocol for RDF, meaning that all the queries must be performed using SPARQL.

As per the functionalities described above, the IoT-Registry component performance has been studied to understand the non-functional behaviour of the platform. In that sense, two probes have been integrated into the component, capturing some features while the transactions are being done. The probes implementation is described within the following section, while Figure 32 shows how they have been integrated into the FIESTA-IoT architecture.

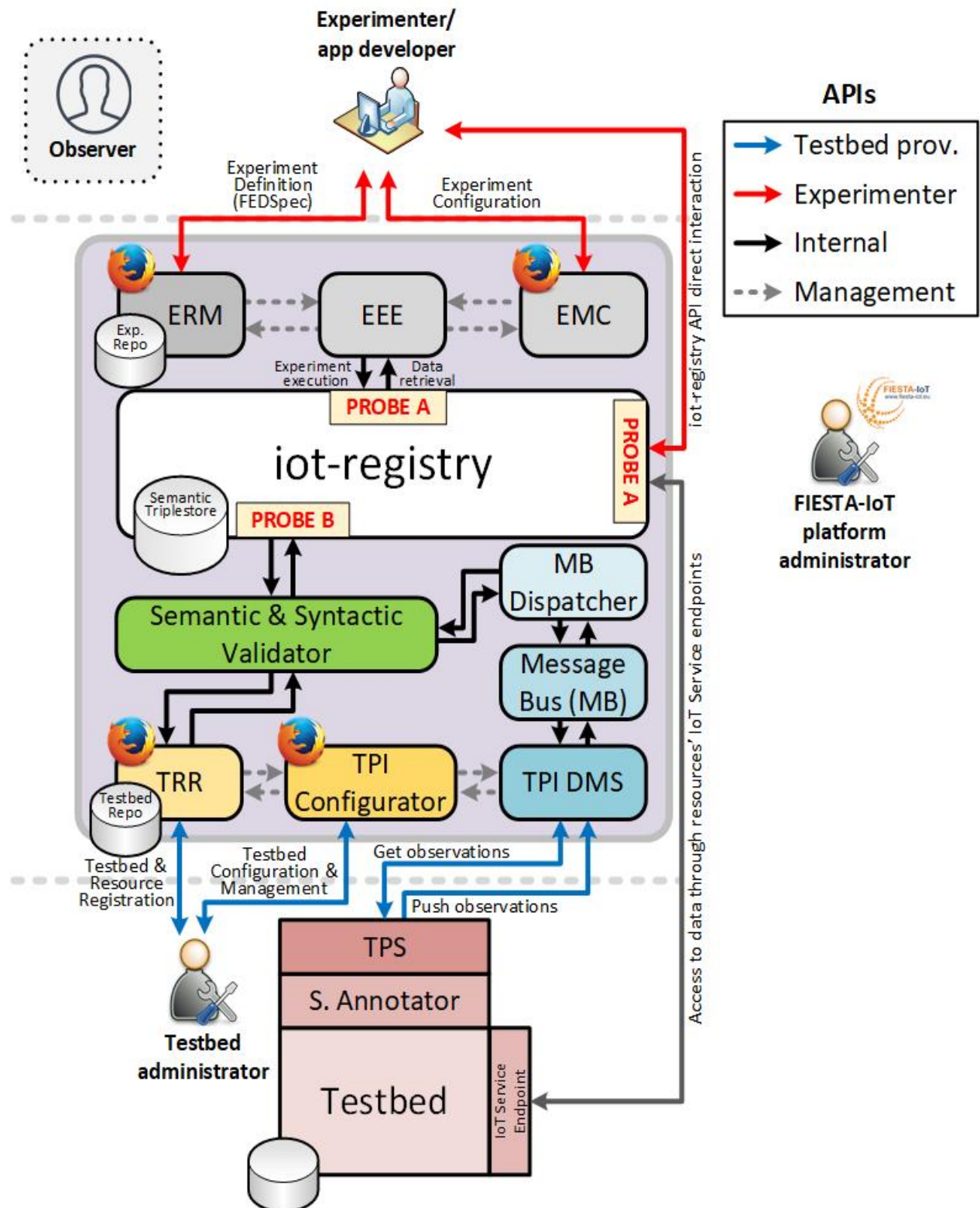


Figure 32. Probes integration for FIESTA-IoT performance analysis.

## 5.2 Probe implementation for performance analysis

As aforementioned, the methodology used to analyse the performance of the platform is based on the inclusion of some “probes” which measures and obtain different features from each request performed against the IoT-Registry. These probes capture every request performed, and stores in a database a set of measurements, such as the timestamp when the call was made, the time to process the call, etc. All the information obtained in each of the probes is stored in a MySQL database, created to this reason. The way each of the probes work is described below:

### Probe A – Platform as a data provider

This probe gathers all the measurements related to the access of the information stored in the IoT-Registry. Each time a request is received, the probe stores the information in a table called “sparql\_query\_execution\_log”. Additionally, information about the different queries performed is also stored in another table called “sparql\_query\_log”. The different pieces of information per request stored are described in Table 7.

*Table 7. “sparql\_query\_execution\_log” table with the information gathered from requests.*

Field	Description
query_hash	Hash of the query performed. Using this hash we can match the query performed with the list in the table “sparql_query_log”.
exec_time	Execution time of the call. Depending on the time we can infer whether the call was successful or not.
ip_address	IP address from where the call was made.
User	Hash with the information of the user who made the call. User information cannot be recovered from the hash.
user_agent	Indicates which tool was used to perform the request.
aborted	Indicates whether the requests were aborted before the result was delivered.
created	Timestamp when the request was made.

### Probe B – Platform as a data collector

This probe has been placed in the interface for the testbeds to inject information into the platform. The goal is to understand the technical performance of the platform while receiving observations from the different testbeds. In this case, a specific table named “semantic\_storage\_log” has been placed, and the information gathered is described in Table 8. In this case, information such as the user\_agent or the user makes no sense in this case, as all the queries for injection have to go through the intermediate component “Semantic and Syntactic validator”, which validates all the observations being pushed into the platform.

*Table 8. "semantic\_storage\_log" table with the information gathered from observation injection requests.*

Field	Description
exec_time	Execution time of the call. Depending on the time we can infer whether the call was successful or not.
entity	Indicates whether the request is to create a new RESOURCE, OBSERVATION or TESTBED.
ip_address	IP address from where the call was made.
aborted	Indicates whether the request was aborted before the result was delivered.
created	Timestamp when the request was made.

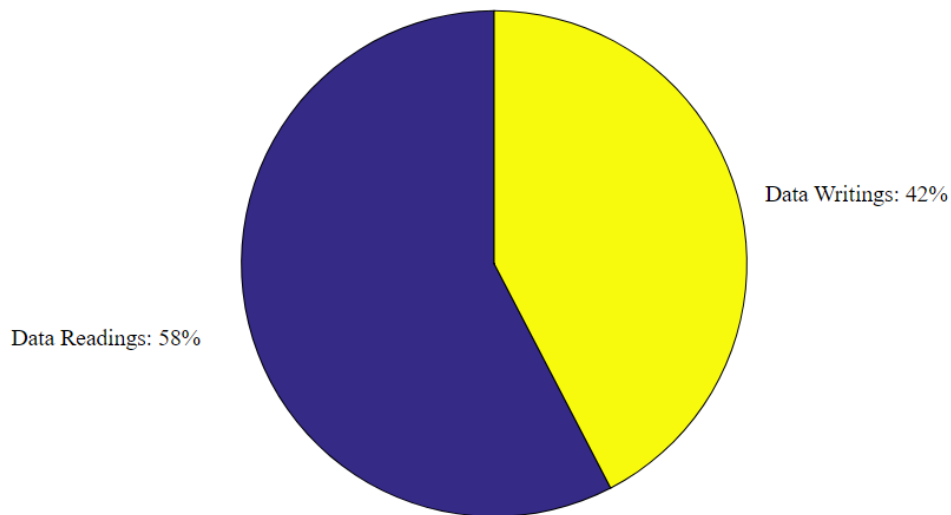
### 5.3 Analysis of the platform performance

Through this section we analyse the non-functional behaviour of the platform using the information obtained from the requests performed against the IoT-Registry, as described above.

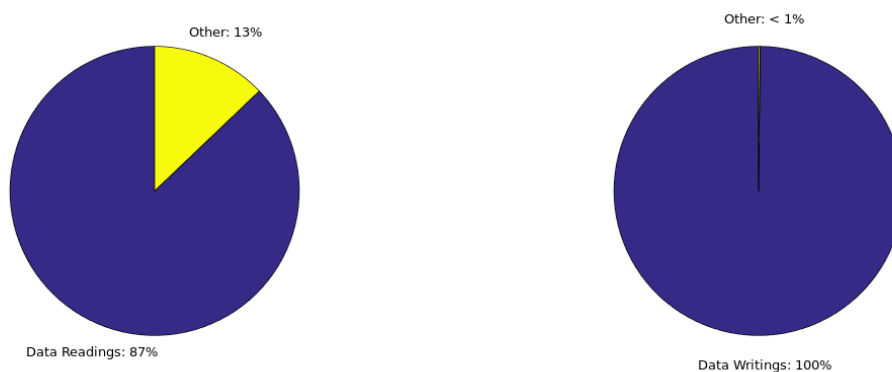
The period chosen to analyse the platform behaviour is the period from 15<sup>th</sup> of January to 15<sup>th</sup> of March. Considering that the Open-Calls OC3 and OC4 were held until March (see section 3.1), we can consider this period where most of the experiments were using the platform. Additionally, all the testbeds, either external or internal, have been already integrated into the platform, thus observation writings are expected continuously.

The number of calls performed against the platform during the chosen period was 727968, including both, observations readings and writings. In this sense, the average number of requests per hour performed against the platform is 514.1. Figure 33 shows the percentage of data writings performed against the platform versus the number of data readings. Although data readings are larger than the writings, we have to consider that testbeds usually push data in sets of observations, avoiding unnecessary calls to the platform.





*Figure 33. Data Readings vs Data Writings against the platform*



*Figure 34. (Left) Data Readings vs Wrong Formatted Calls and Server Errors. (Right) Data Writings vs Wrong Formatted Calls and Server Errors.*

Figure depicts the number of successful data queries vs the number of wrong data queries for both, data readings (performed by experimenters) and data writings (performed by testbeds). It is worth mentioning that we have included both, server errors and queries wrong formatted SPARQL queries, under the same group 'other'. Unfortunately, we cannot gather information of authentication errors from different calls, as it depends on an external module.

As we can see in the figure, most of the calls are well formatted and delivered as expected. Additionally, the number of errors when testbeds perform the data writing calls is clearly lower than the errors performed in the experimenter case. This is the expected behaviour, as the testbed calls tends to be the same over the time, and once they are integrated, wrong formatted calls are not expected. On the other hand, experimenters perform also tests on the platform, what justifies the number of wrong calls.

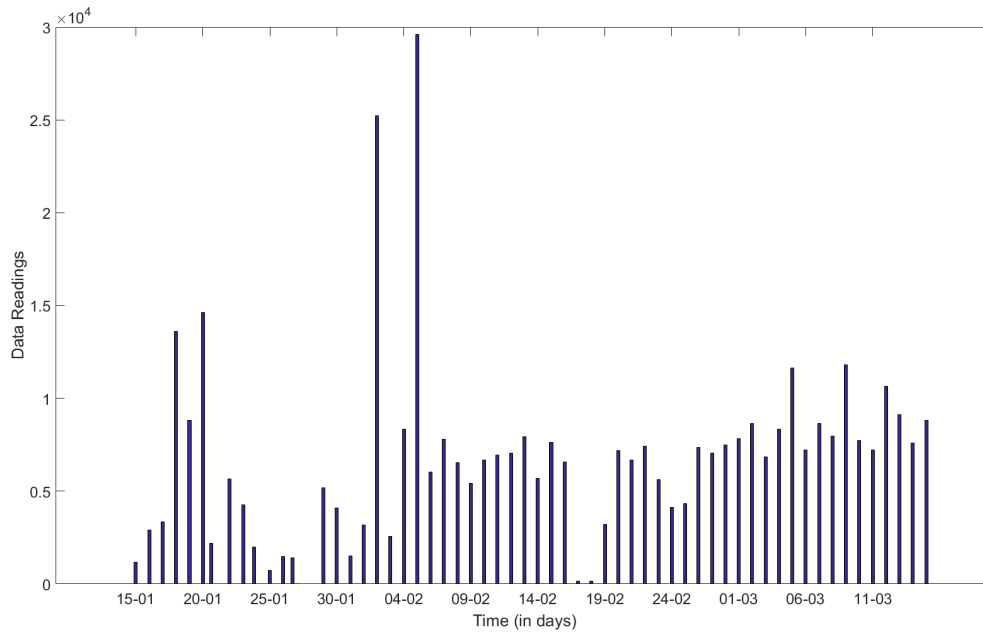


Figure 35. Data readings per day.

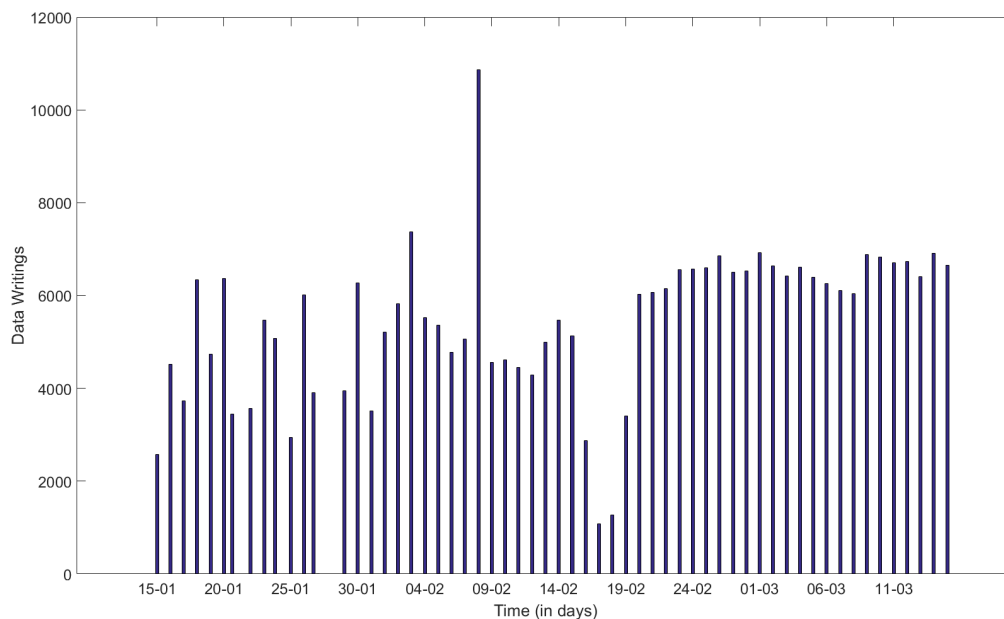


Figure 36. Data writings per day.

If we analyse the behaviour of the platform in different days, we can see that the number of calls diverge more when they are readings, justified by the usage of the platform for testing or stressing it in certain days (see Figure 35) to perform the experiments or gather historical information. On the contrary, data writings tend to be more consistent, as the testbeds send information periodically in the same basis (see Figure 36). Additionally, although data writings are consistent over time as we saw, it can be noticed that on the 8<sup>th</sup> of February an unusual set of data writings were performed against the platform. This is probably due to some testbed integration (e.g. injection of additional data to the platform).

Table 9. Features from data readings per day.

Data readings per day			
Average	Standard Deviation	Max	Min
6898.8	5014.6	29614	139

Table 10. Features from data writings per day.

Data writings per day			
Average	Standard Deviation	Max	Min
5439.6	1619.2	10872	1082

In Figure 37 we can notice the unusual behaviour of the platform in several days, 17<sup>th</sup>, 18<sup>th</sup> of February and 28<sup>th</sup> of January, which is due to specific platform maintenance. If we consider the date were most of the calls were made, on 5<sup>th</sup> of February, there were up to 29614 data readings and 5360 data writings. Therefore, 34974 queries were performed, getting a rate of 1457.25 queries per hour. If we consider the average number of the queries, we get that the platform was able to manage up to 8.6 queries per minute in average.

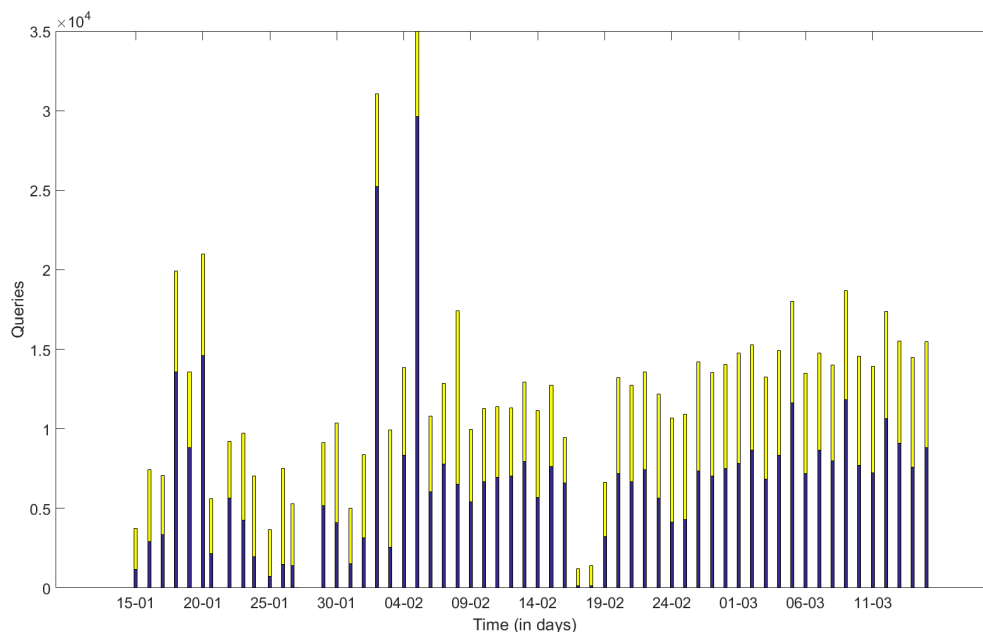
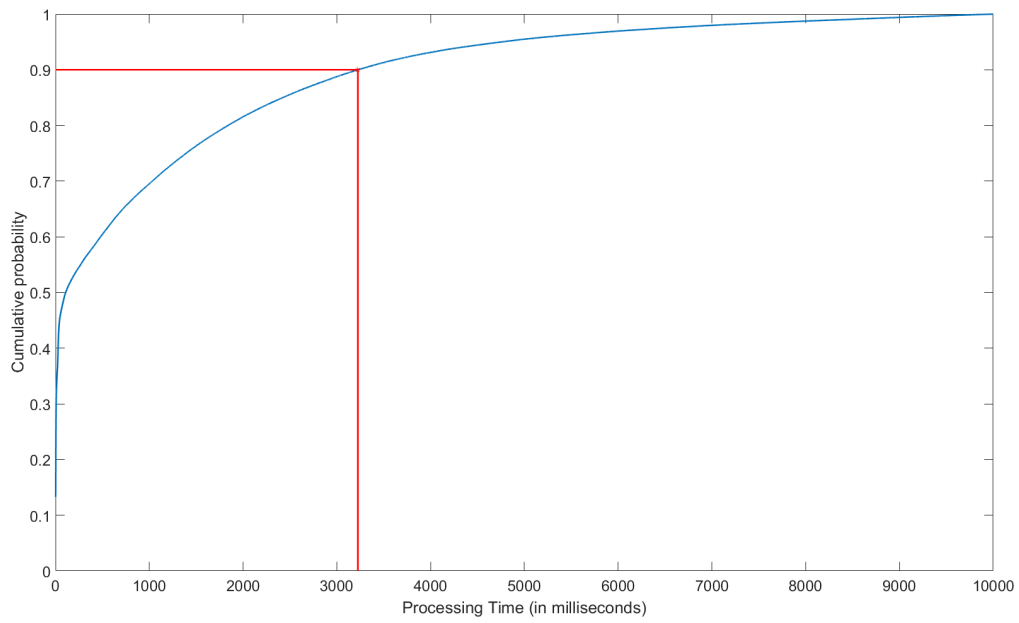


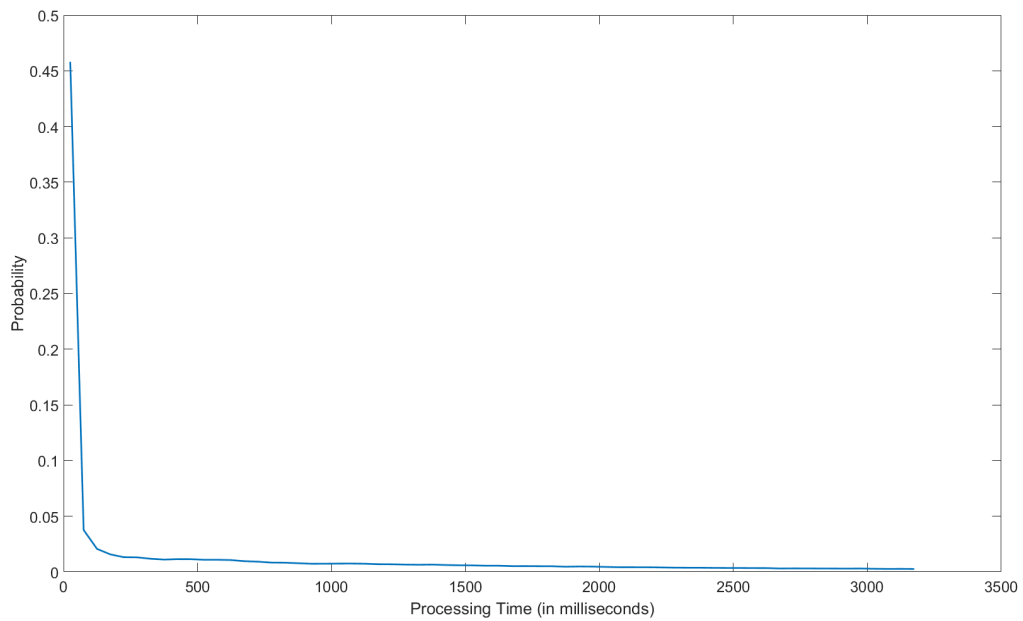
Figure 37. Data readings and data writings per day.

In addition to the number of queries performed against the platform, we have also considered the processing times for each of them. These measurements indicate the time taken by the IoT-Registry to process the different calls.

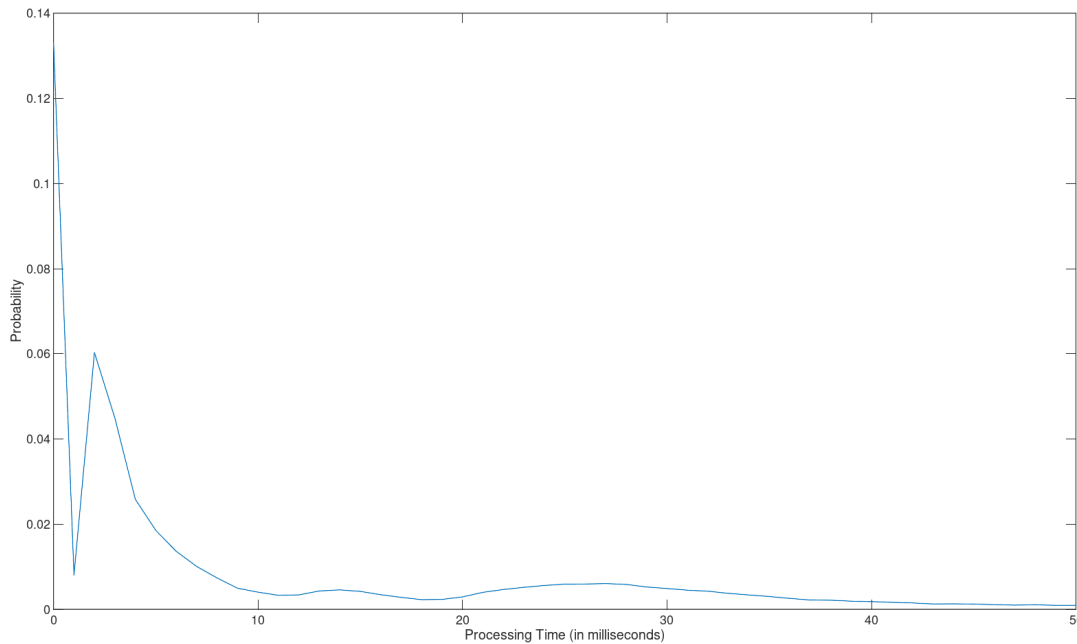
Figure 38 shows the cumulative probability function of processing times for data readings. The figure indicates that most of the queries (> 90%) are processed in less than 3224 milliseconds, although there are queries that can take much longer (e.g. historical queries with complex conditions). As we can see in the figures, query processing times follow an exponential distribution.



*Figure 38. Cumulative Probability Function of processing times for data readings.*



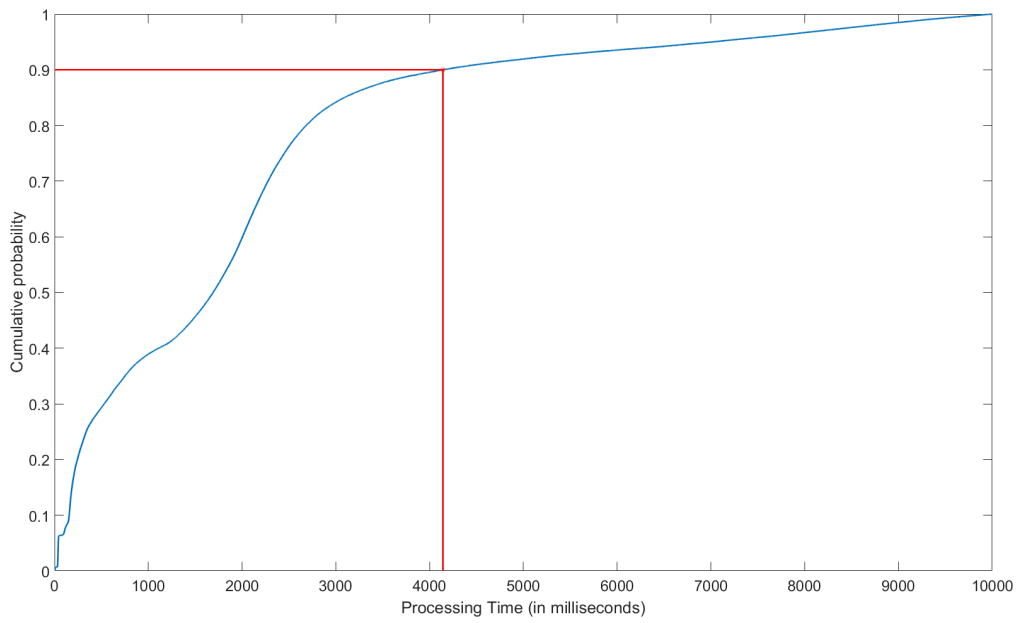
*Figure 39. Probability of different processing times for data readings limited to 90% of the queries.*



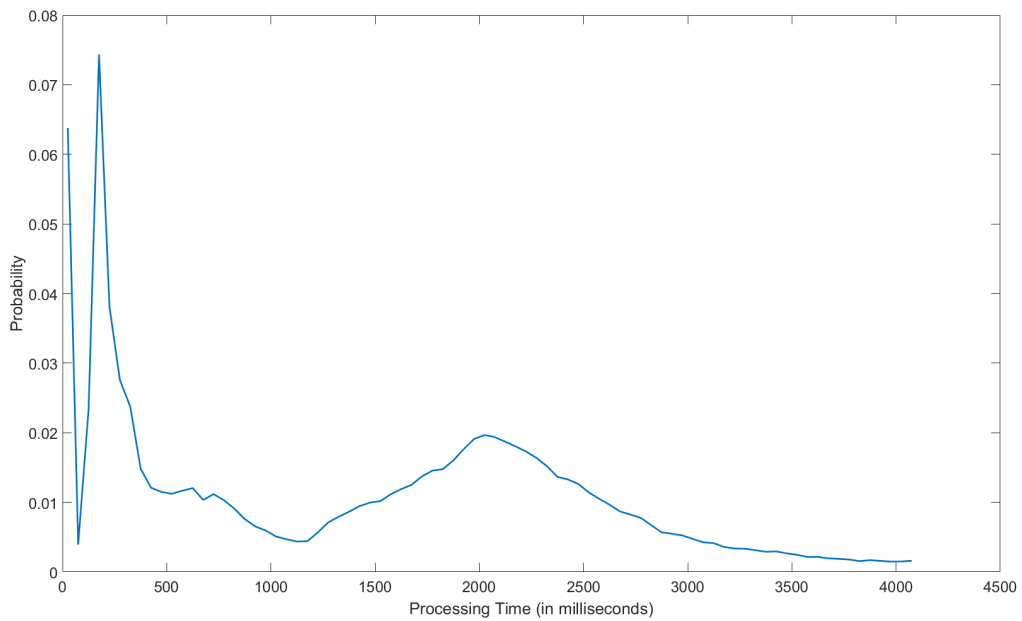
*Figure 40. Probability of different processing times for data readings limited to 50 ms.*

Figure 39 shows the probability for the different processing times until 3224 milliseconds, where 90% of the queries are. It is clear that the probability of processing times decreases over time. As we can notice, the highest probability of a processing time is found in the interval from 0 (wrong formatted calls and server errors) and 100 milliseconds, while the rest are distributed much more uniformly. This is probably due to the use of the platform for experimentation, as the experimenters will test different calls (e.g. to discover resources), and they can be processed quickly (e.g. no results or wrong formatted SPARQL query). Additionally, Figure 40 shows the probabilities within the first 50 milliseconds, which show that the second most possible processing time for query processing is in 3 milliseconds.

On the other hand, Figure 41 shows the cumulative probability function and the probability of processing times for data writings. Similarly to data readings, most of data writings are below of 4142 milliseconds. In that sense, we can notice that the distribution is not completely exponential, and most probable processing times are around 0, 40, 200 and 2000 milliseconds. This can be seen in detail in Figure 42 and Figure 43.



*Figure 41. Cumulative Probability Function of processing times for data writings.*



*Figure 42. Probability of different processing times for data writings limited to 90% of the queries.*



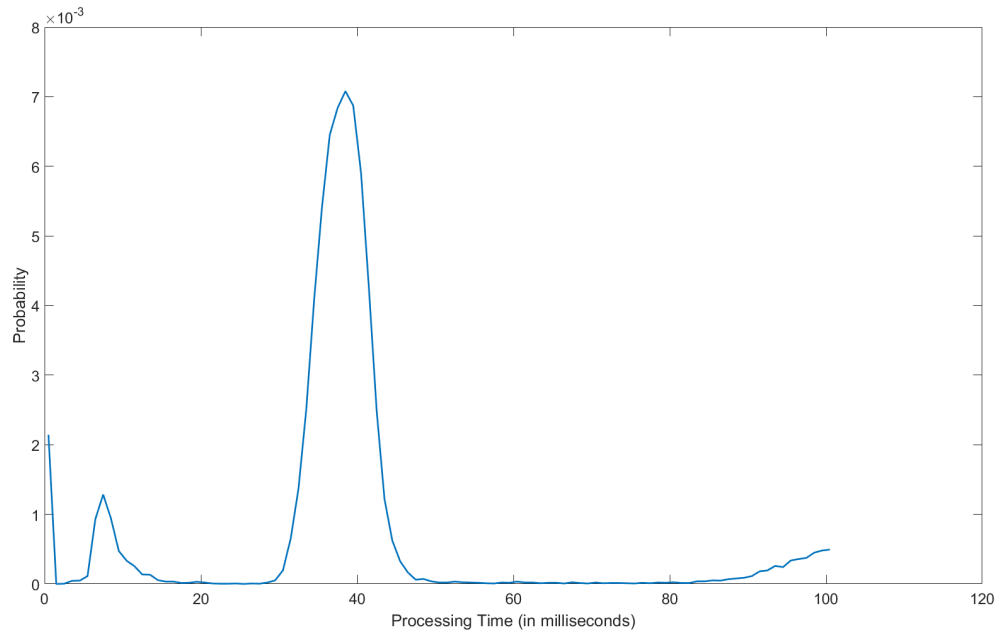


Figure 43. Probability of different processing times for data writings limited to 100 ms.

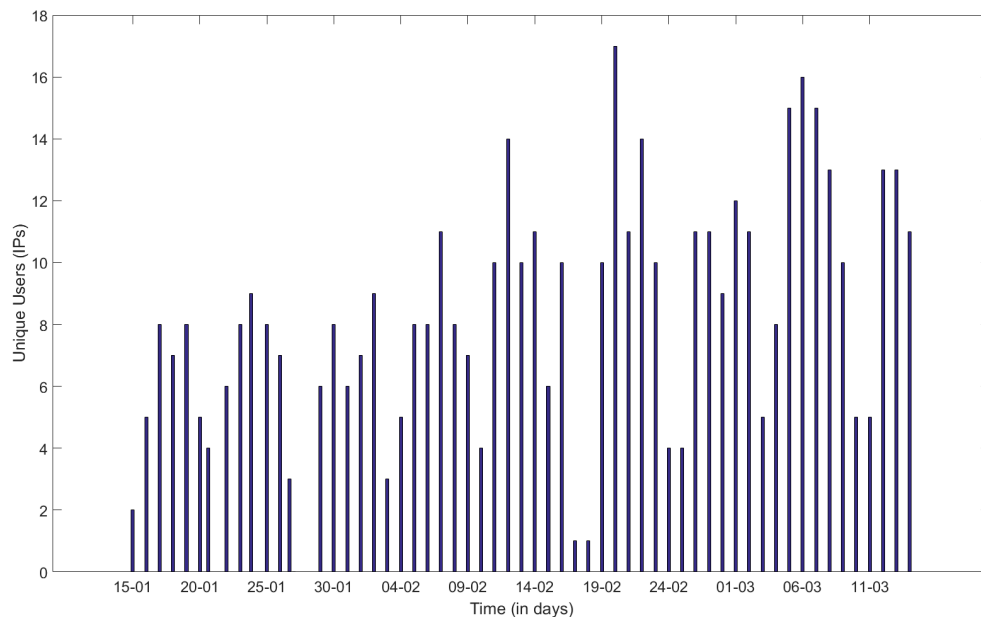


Figure 44. Unique users per day taking into account IPs sources.

During the analysis of the platform performance we have also studied the number of calls from different sources based on the IP and the user agent making the call. Figure 44 shows the number of different IPs accessing the platform during the different days. As we can see in the figure, the 20<sup>th</sup> of February was the day with the most different IPs accessing the platform, although it was not the day with most number of calls. If we consider the user agents, Figure 45 shows the time-series distribution for the two months analysed. Normally, the detected user agents are less than the number of IPs per day, although with several exceptions (e.g. 24<sup>th</sup> of February) due to the use of different technologies from the same source (e.g. localhost hosts several programs for

platform monitoring and data access, which are all deployed in the same machine as the IoT-Registry).

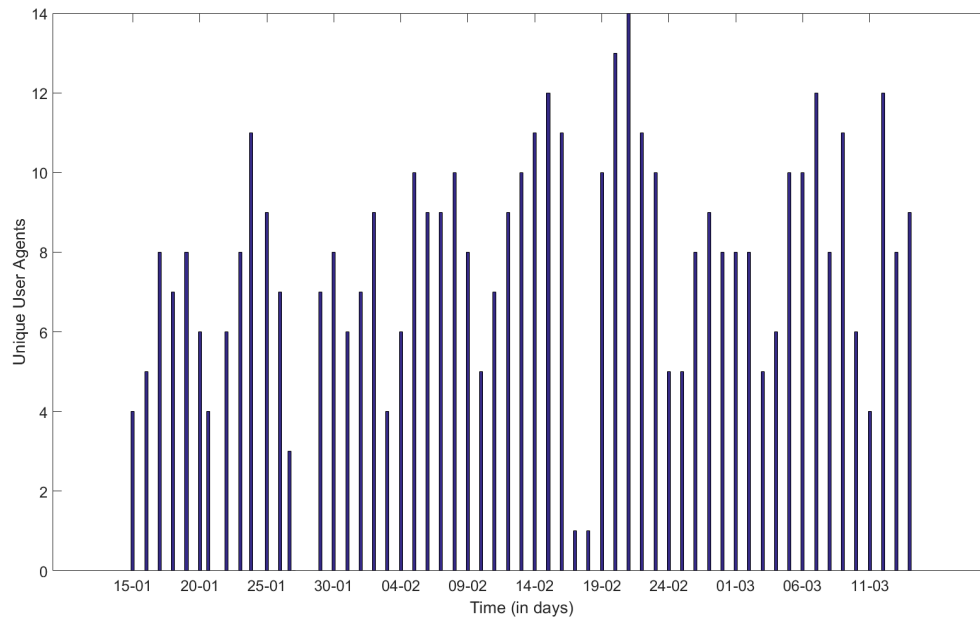


Figure 45. Unique users per day taking into account user agents.

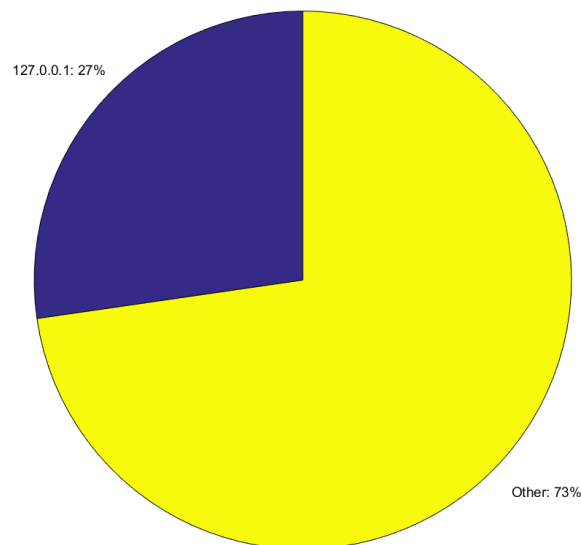


Figure 46. Percentage of the calls performed from the localhost vs all other IPs sources.

As expected, most of the queries are performed from the localhost, being around one fourth of the total. However, it is worth mentioning that some external sources also performed a high number of queries (almost half of the queries from the localhost).

Table 11. Unique users per day based on the source IPs.

Unique Users per day (IPs)			
Average	Standard Deviation	Max	Min
8.1	4.003	17	0

*Table 12. Unique users per day based on the user agents.*

Unique User Agents per day			
Average	Standard Deviation	Max	Min
7.6	3.1039	14	0

*Table 13. Experiment duration based on the calls performed by the different IPs.*

Experiment duration per IP (days)			
Average	Standard Deviation	Max	Min
12.27	17.88	60	0

*Table 14. Experiment duration based on the calls performed by the different IPs (without taking into account the localhost).*

Experiment duration per IP without localhost (days)			
Average	Standard Deviation	Max	Min
11.59	17.17	57.35	0

*Table 15. Number of queries per IP.*

Number of queries per IP			
Average	Standard Deviation	Max	Min
4732.8953	16140.4129	111061	1

*Table 16. Features of number of queries per IP (without taking into account the localhost).*

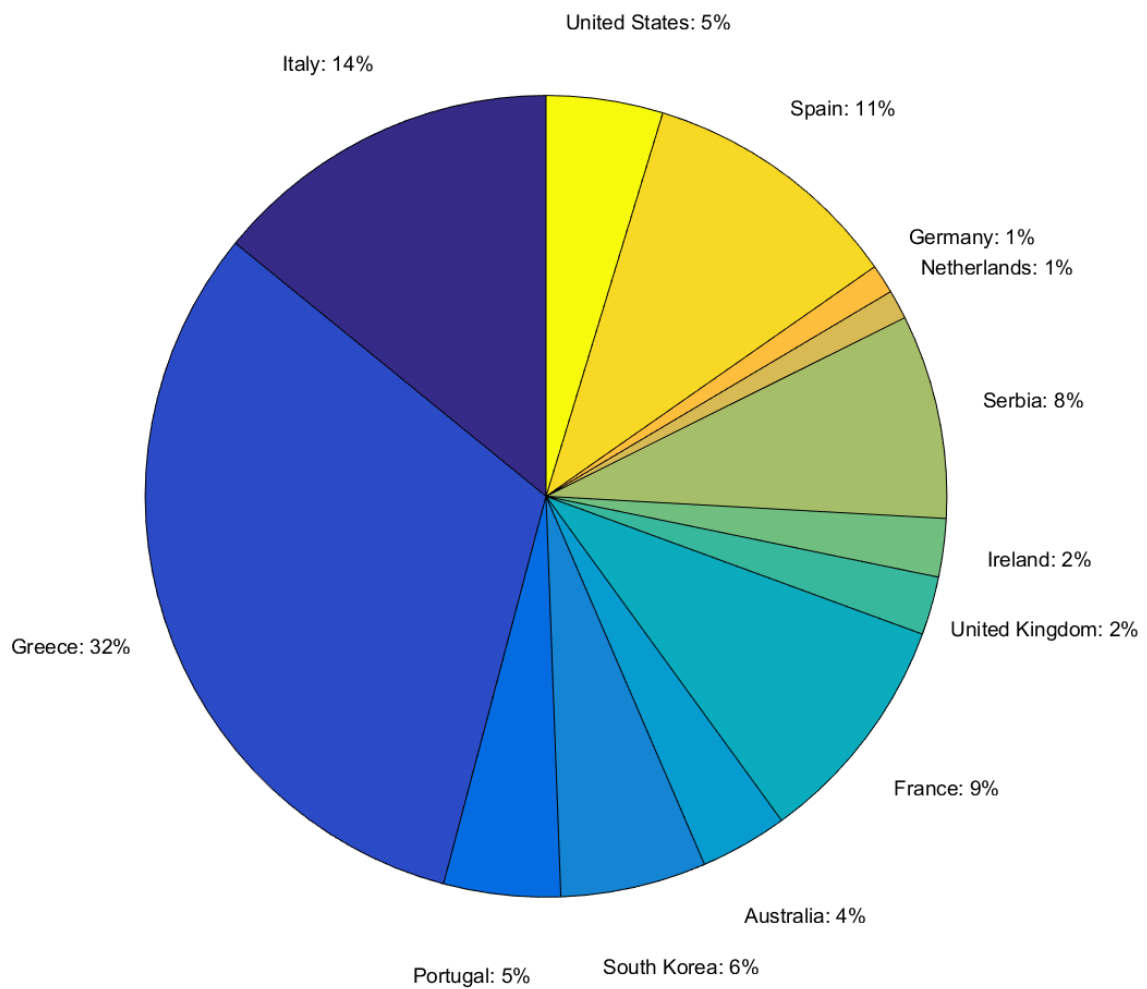
Number of queries per IP without localhost			
Average	Standard Deviation	Max	Min
3481.9765	11288.9144	66694	1

The duration of the experiment, considering the dates when the first and the last calls were performed, we find an average of 11.5 days, with a high standard deviation, probably due to experiments that only need to perform specific queries to get historical data, and experiments accessing the platform continuously.

Finally, if we analyse the location of the IPs we are receiving requests, we can find queries from 13 different countries. As shown in Figure 47, the country with most different IP sources was Greece, followed by Italy and Spain. As expected, the country distribution follows a similar distribution as the countries from selected experiments in the Open-Calls.

### Conclusions

We can conclude through the analysis carried out in this section that the platform is suitable enough to provide semantic and agnostically access to multiple testbeds. As shown in the multiple graphs within this section, the platform supported a huge number of calls throughout the two months analysed, from mid-January to mid-March. Furthermore, thanks to the continuous improvement of the platform during the project lifetime, most of the calls (up to 90% of them) are processed in less than 3 and 4 seconds, depending if they are readings or writings, respectively.



*Figure 47. Countries accessing the platform based on the IPs geolocation.*

## 6 PRIVACY PROTECTION AND ITS IMPLICATIONS FOR FIESTA-IOT

The FIESTA-IoT project was designed as an experimental platform with the main objective to support/serve multiple pan-European experimental facilities where the first objective is to have a common virtual place where to share sensors data. Other functionalities, such as authentication and verification were also implemented to provide a reliable access control mechanism.

However, the objective of the FIESTA-IoT architecture design was not to address the personal data concerns in regards to the new GDPR, as it was not released at the time of platform design. In that sense, considering this new regulation, any system or platform, service or data infrastructure that is prone to process personal data, is compromised to have some minimal services that guarantee the preservation of privacy, the accessibility to the data and the traceability mechanism to have control where, when and how the data is being used.

This section presents the necessary modifications that have been initially foreseen to better align the FIESTA-IoT Platform with the requirements of the new GDPR. The objective of these modifications is to pave the way towards a fully-compliant Platform so further additions might be required after initial assessment of the proposed upgrade.

On the other hand, we have also introduced in this section the Privacy Dashboard component, which address the authorisation mechanisms that some of the FIESTA-IoT testbeds requested. These mechanisms aims at providing a way of authorising only specific experimenters to certain datasets.

The section is distributed as follows. Firstly, the FIESTA-IoT technical assessment is described, including all the functionalities needed based on the FIESTA-IoT Data Protection Impact Assessment. Secondly, the description of the modifications performed on top of the platform are presented, as well as the data model changes required. Finally, the new Privacy Dashboard component is described in detail.

### 6.1 FIESTA-IoT Technical Assessment

A global vision of the FIESTA-IoT platform architecture is provided in the figure 3 showing also the interactions between the different components that form the FIESTA-IoT framework. We also hint the two main roles that can be undertaken by external users: testbed administrator and experimenter. In addition to this, there are various components marked with a web-browser-like icon, only meaning that the component is integrated within the FIESTA-IoT Web Portal.

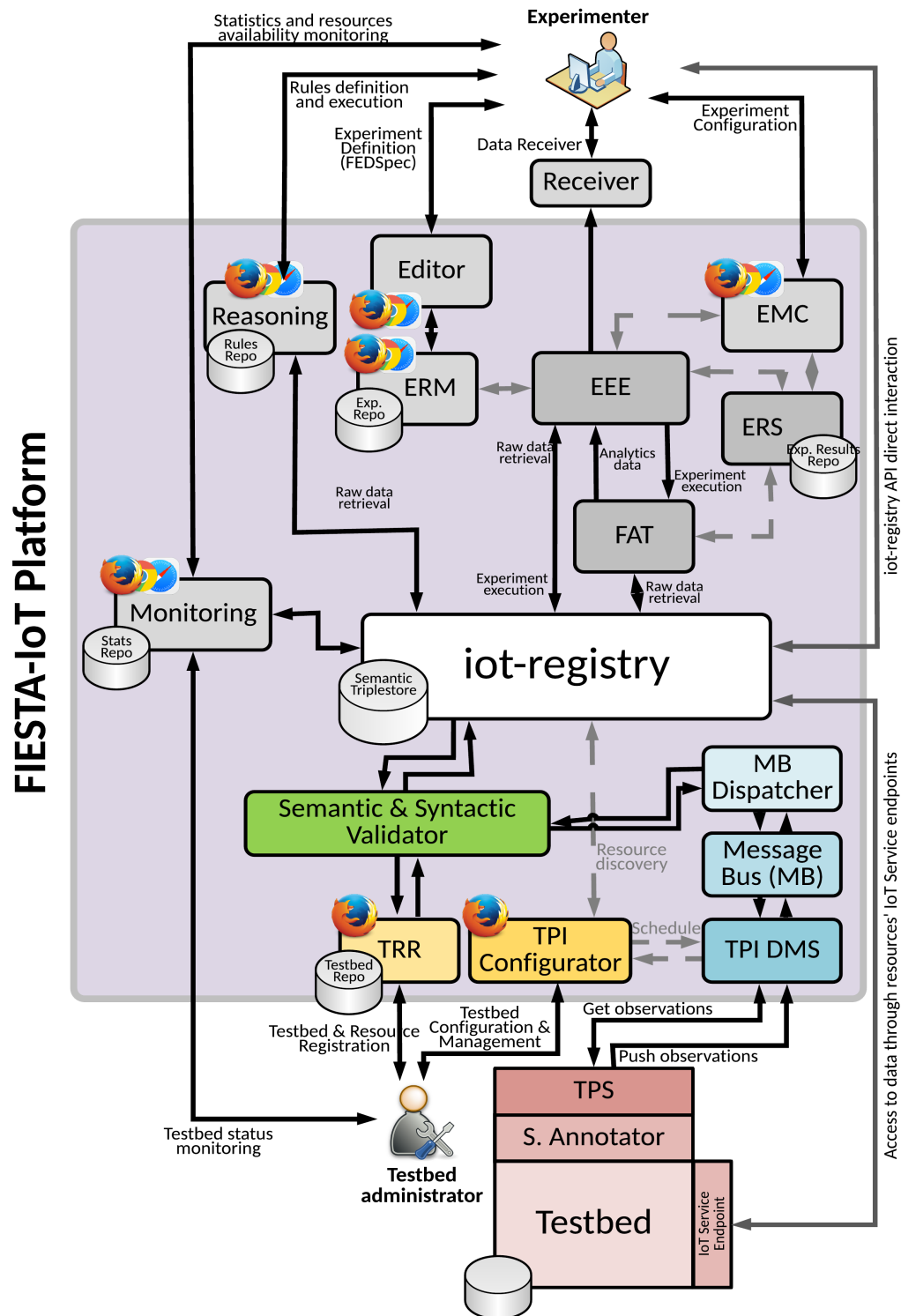


Figure 48. FIESTA-IoT Architecture with Security - Current Version.



Table 17 summarize the FIESTA-IoT identified functionalities as result of the Data Protection Impact Assessment (DPIA) activity and the FIESTA-IoT desirable performance towards GDPR compliance:

*Table 17. FIESTA-IoT identified functionalities from DPIA.*

FIESTA-IoT identified functionalities	FIESTA-IoT Status
A) Data Privacy	- FIESTA-IoT making use of Policies for defining what is the accessibility level to overall testbed and sensor data.
B) Data Encryption	<ul style="list-style-type: none"> <li>- FIESTA-IoT enabling encryption at different levels to preserve users's data privacy.</li> <li>- FIESTA-IoT enabling endpoints URL encryption and decryption in the IoT registry component.</li> <li>- For data encryption, if some component need to use, you should reuse FIESTA-IoT utils api for encrypt/decrypt function currently done with Endpoint URL.</li> </ul>
C) Protect Testbed Data	<ul style="list-style-type: none"> <li>- FIESTA-IoT implementing endpoint data protection using privacy component.</li> <li>- FIESTA protecting Data History by means of the SPARQL Query endpoints.*</li> </ul>
D) Logs Accessibility Information	<ul style="list-style-type: none"> <li>- FIESTA-IoT using gray logs for system logs about the components</li> <li>- FIESTA-IoT enabling Data Logs at the level of end points and sparql queries*</li> </ul>

We now present a brief outline of each component along with its functionality.

FIESTA-IoT Component	DPIA & Coding Implication(s)
<b>OpenAM.</b> Even though it does not explicitly appear in the figure, this component is in charge of protecting the FIESTA-IoT Platform provided services, by ensuring that authenticated users only have secure access to the applications and services that are deployed and available via the	- Encryption one way PASSWORD

<p>Web Portal, the Experiment-as-a-Service (EaaS) APIs and the Graphical User Interfaces (GUIs) provided by FIESTA-IoT. The FIESTA-IoT Security Framework book covers all the features supported by this security framework.</p>	
<p><b>iot-registry.</b></p> <p>This component is the cornerstone of the FIESTA-IoT platform. It is the module in charge of handling the semantic information that flows across the FIESTA-IoT platform. Basically, it undertakes the control of the triple-store and internally holds the overall semantic meta-repository.</p>	<ul style="list-style-type: none"> <li>- Protect endpoint data by IoT-Registry + Privacy component</li> <li>- FIESTA-IoT enabling endpoints URL encryption and decryption in the IoT registry component.</li> <li>- Sensor history data of a testbed can be config accessed or not via sparql endpoint</li> <li>- implement query endpoint can be filterby testbedID and sensorID</li> <li>- System general logs to GrayLogs</li> <li>- Endpoint sensor data access logs done by Privacy-Policy component (DONE) using API from IoT-Registry</li> </ul>
<p><b>Experiment Registry Management (ERM).</b></p> <p>It is the registry where all the experiments are stored. The Experiment Execution Engine and the Experiment Management Console use the ERM APIs to read the information stored about the experiment and take actions accordingly.</p>	<ul style="list-style-type: none"> <li>- System general logs to GrayLogs</li> <li>- Endpoint sensor data access logs done by Privacy-Policy component</li> </ul>
<p><b>Experiment Management Console (EMC).</b></p> <p>It is the User Interface (UI) to the Experiment Execution Engine (EEE). Using this an experimenter can control the execution of the FISMOs beyond what is specified via FEDSpec. Using EMC an experimenter can also know other related information about the experiment that he provided in the FEDSpec.</p>	<ul style="list-style-type: none"> <li>- System general logs to GrayLogs</li> <li>- Endpoint sensor data access logs done by Privacy-Policy component</li> </ul>
<p><b>Experiment Execution Engine (EEE).</b></p> <p>The EEE is the engine that executes the experimenter's need on the IoT-Registry at a specified schedule. It defines a set of services/APIs that are essential for the execution of the experiment. The EMC uses EEE APIs to provide experimenters the execution related information.</p>	<ul style="list-style-type: none"> <li>- System general logs to GrayLogs</li> <li>- Endpoint sensor data access logs done by Privacy-Policy component</li> </ul>

<p><b>Semantic &amp; Syntactic Validator.</b></p> <p>In order to make sure that all the information injected into the iot-registry is 100% compliant with the semantic data model defined in the FIESTA-IoT ontology [1], this component carries out, as its name hints, the corresponding operation, namely by filtering out every erroneous resource description or observation. Nonetheless, this component is part of the core of the platform and externals will never interact with it.</p>	<ul style="list-style-type: none"> <li>- System general logs to GrayLogs</li> <li>- Endpoint sensor data access logs done by Privacy-Policy component</li> </ul>
<p><b>Testbed and Resource Registration (TRR).</b></p> <p>A graphical user interface that provides the means, for testbed administrators, to register their testbed(s) and resource(s).</p>	<ul style="list-style-type: none"> <li>- System general logs to GrayLogs</li> <li>- Endpoint sensor data access logs done by Privacy-Policy component</li> </ul>
<p><b>Testbed Provider Interface (TPI) Configurator.</b></p> <p>It is another UI to be used by testbed administrators. In this case, the testbed administrator can manage his underlying resources and schedule the way FIESTA-IoT platform would interact with his testbed.</p>	<ul style="list-style-type: none"> <li>- System general logs to GrayLogs</li> <li>- Endpoint sensor data access logs done by Privacy-Policy component</li> </ul>
<p><b>TPI Data Management Services (DMS) module.</b></p> <p>It is a component that defines a set of services that allows the FIESTA-IoT platform to collect information (i.e. observations) from the testbeds.</p>	<ul style="list-style-type: none"> <li>- System general logs to GrayLogs</li> <li>- Endpoint sensor data access logs done by Privacy-Policy component</li> </ul>
<p><b>Message Bus (MB).</b></p> <p>This component acts as an entry point for the observations harvested from testbeds.</p>	<ul style="list-style-type: none"> <li>- System general logs to GrayLogs</li> <li>- Endpoint sensor data access logs done by Privacy-Policy component</li> </ul>
<p><b>MB Dispatcher.</b></p> <p>This component collects messages from the MB and forwards them to the iot-registry.</p>	<ul style="list-style-type: none"> <li>- System general logs to GrayLogs</li> <li>- Endpoint sensor data access logs done by Privacy-Policy component</li> </ul>
<p><b>Testbed Provider Services (TPS).</b></p> <p>It is the set of APIs used to setup interactions between a testbed and the</p>	<ul style="list-style-type: none"> <li>- System general logs to GrayLogs</li> <li>- Endpoint sensor data access logs done by Privacy-Policy component</li> </ul>

<p>FIESTA-IoT platform. This set of APIs exclusively focuses on the measurements/observations domain. Namely, we have defined the mechanisms to push/pull measurements/observations from testbeds. Note that, the TPS currently only holds the definition of the API; the actual implementation of the API has to be done by the testbed admin.</p>	
<p><b>Semantic Annotator.</b></p> <p>Usually, testbeds have their own data sets, defined either in a proprietary format or using standard solutions (e.g. FIWARE, OneM2M, etc.). Nonetheless, FIESTA-IoT platform only accepts FIESTA-IoT compliant documents. So, a translation between these two realms must be done. It is up to the testbed providers to implement a semantic annotator that takes their legacy format as input, and provides FIESTA-IoT compliant semantically annotated data to the TPS.</p>	<ul style="list-style-type: none"> <li>- System general logs to GrayLogs</li> <li>- Endpoint sensor data access logs done by Privacy-Policy component</li> </ul>
<p><b>IoT Service Endpoint (optional).</b></p> <p>A URL that exposes a service, e.g. the last observation gathered by a particular sensor. Testbeds might include an endpoint as a part of their resource descriptions.</p>	
<p><b>Monitoring</b></p> <p>Testbed monitoring provides tooling to be able to track testbed data activity; users therefore are able to interact with testbeds.</p>	<ul style="list-style-type: none"> <li>- System general logs to GrayLogs</li> <li>- Endpoint sensor data access logs done by Privacy-Policy component</li> </ul>
<p><b>Reasoning engine</b></p> <p>The FIESTA-IoT Reasoning component is an implementation of a semantic reasoner to work on top of the FIESTA-IoT platform. A semantic reasoning engine is a rule-based engine that is able to infer logical consequences from a set of IoT measurements. In doing so, the FIESTA-IoT Reasoner simplifies the creation of rules, which are generated and stored in a rule repository. This component provides a set of API services and a User Interface (UI) for experimenters, making it easy to</p>	<ul style="list-style-type: none"> <li>- System general logs to GrayLogs</li> <li>- Endpoint sensor data access logs done by Privacy-Policy component</li> </ul>

design and execute rules base on the Apache Jena open source framework.	
<b>Experiment Result Storage (ERS)</b>	<ul style="list-style-type: none"> <li>- System general logs to GrayLogs</li> <li>- Endpoint sensor data access logs done by Privacy-Policy component</li> </ul>
<b>FIESTA-IoT Analytics Tool (FAT)</b> FIESTA-IoT Analytics Tool (FAT) is a component that provides open access data analytics tools for data consumers as a web service.	<ul style="list-style-type: none"> <li>- System general logs to GrayLogs</li> <li>- Endpoint sensor data access logs done by Privacy-Policy component</li> </ul>

Moreover, there are a couple of components that are to be implemented at testbed level in order to be fully compliant with the FIESTA-IoT framework:

FIESTA-IoT Component	DPIA & Coding Implication(s)
<b>Privacy Component</b> Privacy and Policy component provide set of services and UI for testbed that easy configure their data access policy and privacy so that FIESTA system easy to protect testbed data.	<ul style="list-style-type: none"> <li>- System general logs to GrayLogs</li> <li>- Endpoint sensor data access logs done by Privacy-Policy component</li> <li>- History sensor data access logs via sparql endpoint NOT done by Privacy-Policy component</li> <li>- Sensor information of a testbed can be config explored or not ?</li> <li>- Sensor meta of a testbed can be config accessed or not ?</li> <li>- Sensor data of a testbed can be config accessed or not</li> <li>- Sensor history data of a testbed can be config accessed or not via sparql endpoint</li> <li>- Protect endpoint data by IoT-Registry + Privacy component</li> <li>- Protect history data by IoT-Registry + Privacy component</li> </ul>
<b>Data Encrypt/Decrypt Component</b> Encrypt/Decrypt component is a set of services with responsibility for encrypt/decrypt testbed data and FIESTA personal data.	<ul style="list-style-type: none"> <li>- Provide centralize data encrypt/decrypt services</li> <li>- Testbed data (endpoint URL)</li> <li>- Personal data</li> <li>- Using AES/CBC/PKCS5Padding (Can be reuse iot-registry or implement new )</li> <li>- For personal data and testbed data management/delete Mechanism</li> <li>- At the moment for delete and owner data management, iot-registry not check the owner data permission.</li> </ul>

### 6.1.1 FIESTA-IoT Web Portal

A common entry point for all the UIs of the available components that form the FIESTA-IoT platform<sup>10</sup>. The first step is to authenticate yourself via FIESTA-IoT's OpenAM portal as shown in Figure 49 (you will be automatically redirected). Once you go across this authentication process, you will get access to all the features provided through this user interface, according to your user role.



Figure 49. FIESTA-IoT Login portal.

FIESTA-IoT Component	DPIA & UI Implication(s)
<b>FIESTA-IoT Web Portal</b> Through this portal, whose main view is shown in figure, you are able to perform most of the operations addressed in this document. We can observe the separation between the two main roles in the menu, since the experimenters and the testbed providers have access to different features.	<ul style="list-style-type: none"> <li>- Privacy, policy (T&amp;C pages)</li> <li>- Captcha system for double protection</li> <li>- System general logs to GrayLogs</li> <li>- Endpoint sensor data access logs done by Privacy-Policy component</li> </ul>

Logging system:

- Currently using GrayLog (need to define what's information should be log and can be query).
- Can be defined more fields (user\_id, access time, location, ip, etc.)

<sup>10</sup> <https://platform.fiesta-iot.eu/portalui>



## 6.2 FIESTA-IoT Platform V1.5 (GDPR compliance)

The global vision of the FIESTA-IoT platform architecture towards GDPR compliance following the DPIA is provided in the Figure 49 and described as follow:

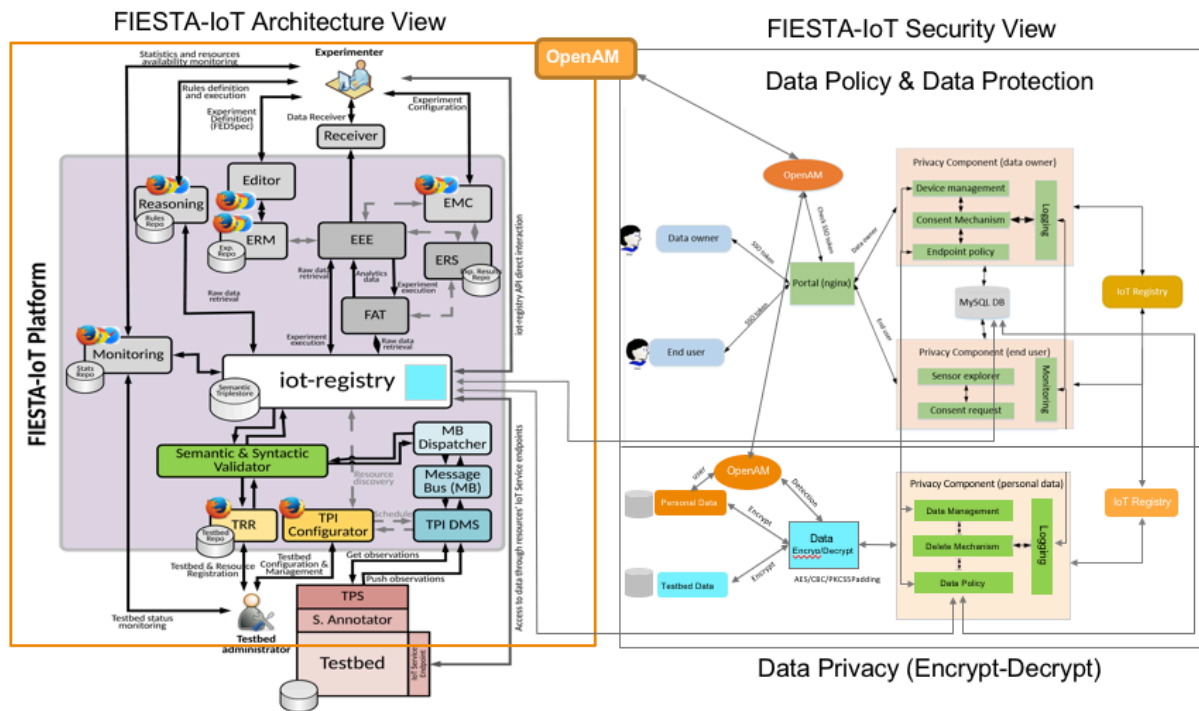


Figure 50. FIESTA-IoT Architecture GDPR Compliance – 1.5 Version.

### 6.2.1 FIESTA-IoT Security View

The security requirements identified in the initial FIESTA-IoT specification (from Deliverable D2.1), defines the features and functionality that the FIESTA-IoT security framework must achieve. Note, from this point forward we define the FIESTA-IoT security framework to be the components and technologies that work together to secure the FIESTA-IoT architecture and the data protection mechanisms. By design the work to secure the FIESTA-IoT architecture is closely related to the majority of architectural components and testbed resources. Such elements must be secured in order that only authorized FIESTA-IoT users can access and utilize them. In the new version not only architectural component must be protected but also data offering privacy and protection to collected and personal data.

#### Data Policy & Data Protection

The way FIESTA-IoT architecture protect the data resources provided by the testbeds in the FIESTA-IoT federation is by using Authentication and Authorization as the most important security mechanisms for this purpose. Additionally, a policy system has been integrated to improve the endpoints data by means of controlling the accessibility to data endpoints and associate them to rules that are for the different roles users have/may have in FIESTA-IoT.

Besides enabling access control to endpoints provided by the testbed to gather sensor data directly from it, FIESTA-IoT has to also extend this policies to restrict access to its

own semantic database, known as IoT-Registry. In order to enable a bigger grade of granularity to the policies that can be applied to data stored in IoT-Registry, it is required to include a new modify component, that will be closely bound to the policy component for endpoints' access control, and adapt the IoT-Registry to guarantee that the result sets from SPARQL requests complies with the permissions set by testbeds owners.

In this sense the internal structure of the IoT-Registry has to be modified. As we have explained in previous deliverables (FIESTA-IoT D4.1, 2015) and (FIESTA-IoT D4.2, 2017), IoT-Registry triple store database (TDB) was divided mainly in two named graphs, one for resources and another for observations. The latter was also subdivided in time-based subgraphs storing observations produced during a period of time and enabling limiting the time scope of the SPARQL request.

As FIESTA-IoT wants to restrict access to the information linked to a sensor, both its description and its observations, the former organization makes it mandatory to analyse/modified every SPARQL sentence, a task that is neither easy nor performance-wise optimal, as the cases are almost infinite. Therefore, we propose a new organization where IoT-Registry's TDB is organized in multiple graphs, each storing information of a specific sensor. Figure 51 shows the foreseen structure.

IoT-Registry TDB

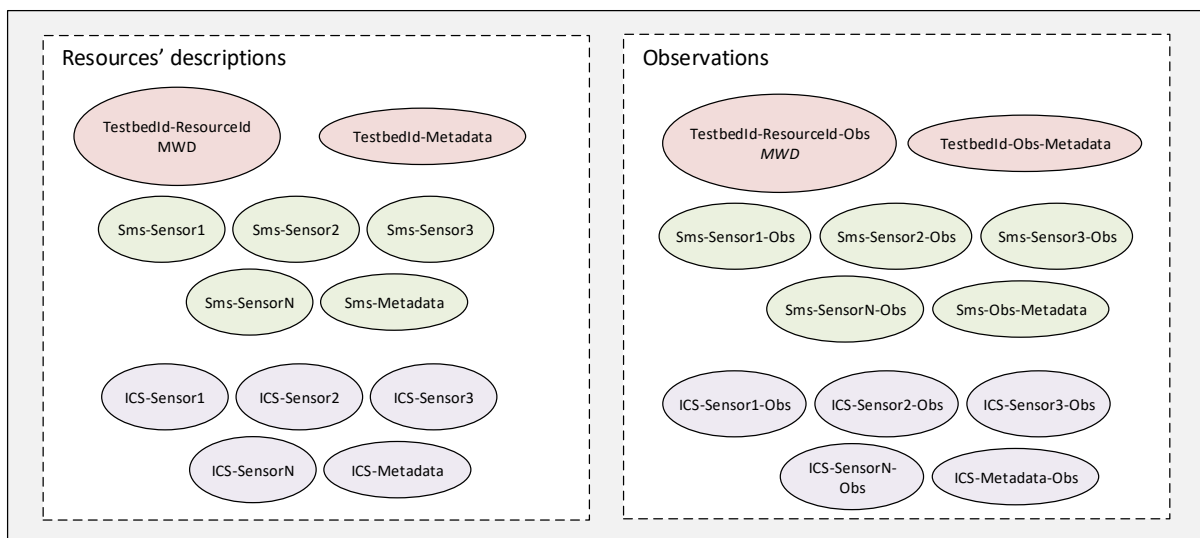
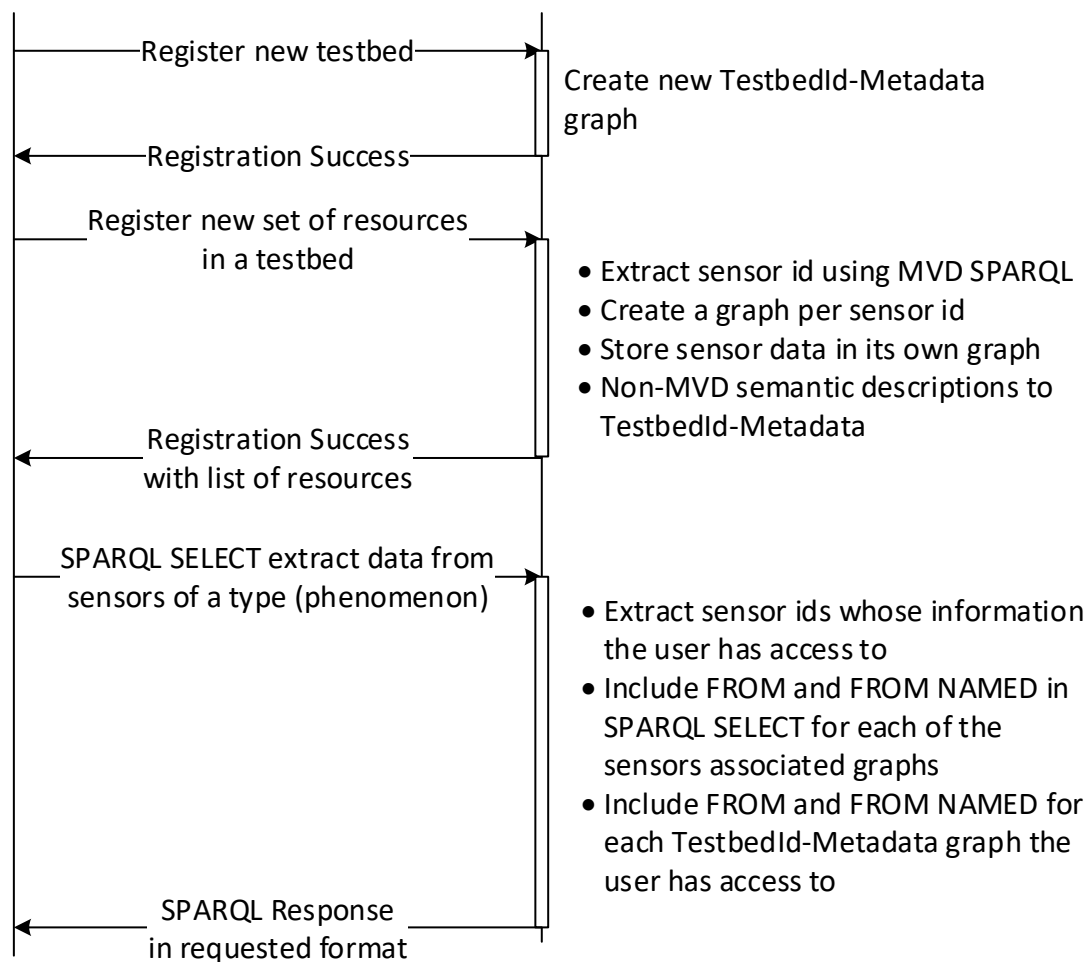


Figure 51. IoT-Registry new TDB structure

As semantic information can be of different nature, so although FIESTA-IoT defines its own ontology, a testbed is free to extend the relationships between semantic entities. However, FIESTA-IoT has considered that a semantic description (resource or observation) to be valid and stored in IoT-Registry has to include a minimum set of data and relations. We named this information the minimum valid document (MVD) and can be extracted by applying a SELECT SPARQL sentence on the semantic document provided by the testbed. Our approach consists on storing the MVD for each sensor on its own graph (for instance named as TestbedID-SensorID), while the rest of information is considered metadata (for instance named as TestbedID-Metadate) and will be stored in a common graph shared by all sensors on a testbed. The same applies for observations produced by sensors, that is, all the MVD for observations

from the same sensor will be stored in a graph (named as TestbedID-SensorID-obs) while the metadata will be stored in a shared graph.

This approach makes it easy to delete or restrict access to the information of a sensor or set of sensors, as the SPARQL sentence will be only tackle the desired graphs. This way there is no need to analyze/modify the original SPARQL sentence from the experimenter. The policy component will provide a list of sensors the experimenter has access to, and extending the SPARQL sentence using FROM <graph> clauses we will be able to limit the request to only the allowed graphs.



*Figure 52. Restricting access to IoT-Registry information*

Figure 52 shows the way a testbed registers its sensors and how an experimenter access the semantic description of a set of sensors. A more detailed description of the SPARQL execution can be seen in Figure 53.

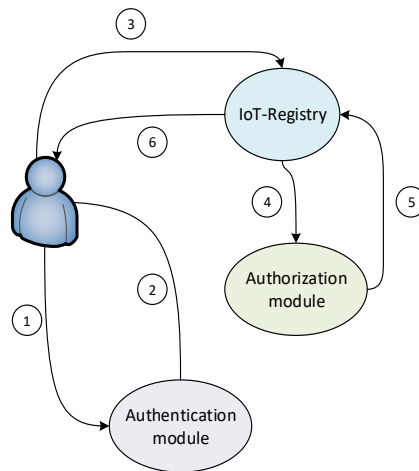


Figure 53. SPARQL request procedure

After retrieving its authentication token issued by OpenAM module, the experimenter is able to access IoT-Registry SPARQL endpoint and post a request. The SPARQL sent to IoT-Registry is:

```

PREFIX rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#>
PREFIX iot-lite: <http://purl.oclc.org/NET/UNIS/fiware/iot-lite#>
PREFIX m3-lite: <http://purl.org/iot/vocab/m3-lite#>

SELECT DISTINCT ?sensor
WHERE {
  ?sensor iot-lite:hasQuantityKind/rdf:type ?phenomenon
  VALUE ?phenomenon {m3-lite:Temperature m3-lite:Illuminance}
}
LIMIT 30
  
```

Upon reception, the IoT-Registry will ask the Authorization module (access policies) for the list of allowed sensors for the user id linked to the experimenter. Suppose the experimenter only has access to Sms-Sensor1 and ICS-Sensor1 from Figure 51. IoT-Registry includes the FROM clauses in the original SPARQL. The final SPARQL that is run by IoT-Registry's engine is:

```

PREFIX rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#>
PREFIX iot-lite: <http://purl.oclc.org/NET/UNIS/fiware/iot-lite#>
PREFIX m3-lite: <http://purl.org/iot/vocab/m3-lite#>

SELECT DISTINCT ?sensor
FROM NAMED <Sms-Sensor1>
FROM <Sms-Sensor1>
FROM NAMED <Sms-Metadata>
FROM <Sms-Metadata>
FROM NAMED <ICS-Sensor1>
FROM <ICS-Sensor1>
FROM NAMED <ICS-Metadata>
FROM <ICS-Metadata>
WHERE {
  ?sensor iot-lite:hasQuantityKind/rdf:type ?phenomenon
  VALUE ?phenomenon {m3-lite:Temperature m3-lite:Illuminance}
}
LIMIT 30
  
```

As the experimenter only has Access to Sms-Sensor1 and ICS-Sensor1, the graphs bound to any other sensor are not included. The request is only restricted to the graphs the user has access to. These restrictions are established by testbed owner or the FIESTA-IoT administrators.

### *Data Privacy View*

In current protection systems and under the regulatory framework (law) there is no standard approach to offer personal data privacy. In FIESTA-IoT the architecture do encrypt and decrypt the personal data, likewise there is no way to identify the data protection mechanism. Nevertheless, in this process at the testbeds side we are proposing to use encrypting algorithms and crypto messages to ensure the preservation of the data privacy.

## **6.2.2 FIESTA-IoT Data Model View**

The motivation to extend a data model is generated from the need to a) be more structured, b) contain more information than before, and c) describe certain concepts that were not described and that are relevant to contextualise the information or simply for offering better organisation to the information contained in the data model.

In the context of data processing and data re-use and sharing, the FIESTA-IoT data model plays an important role defining the way the data is organised and distributed, and at the same time stored in the FIESTA-IoT platform. The data usually is associated to users ID, using acronyms as references to a person, this practice is not recommended anymore and instead if they are used there is the necessity that the data should not be identified, this requires that the data must be obfuscated or encrypted and thus FIESTA-IoT system equally must be capable to encrypt and decrypt information in order to make it available for the people who correspond to be the owner of the encrypted IDs and thus privacy can be offered.

The main concepts that have been identified as necessary to support data security and privacy are **<Purpose>** as the main feature that defines the reason on how the data is being stored and processed under the identifiers. **<Person>** which defines the individual and the data can be correlated to the individual(s). **<Consent>** that defines the status of the data in order to be share or not according to the decision of the person which is the owner of the data. **<Policy>** the rule or set of rules that are used to associate the data to persons or persons to consents etc. **<Feature of Interest>** is the way to associate the activity in the context of persons with the observations in sensors activity. In the same way the concepts are important and defined, there are also new associations that re necessary to be used and that for their self-descriptive nature are not described but listed as follow: “:forAccessing”, “:requires”, “:givesConsent”, “:owns”, “:for”, “:sets”, “:enables” and “:isAssociatedWith”. Figure 54 represents (in the left hand side of the red dashed line) the extensions that current FIESTA-IoT data model(s) is required in order to support the functionalities for data protection and privacy.

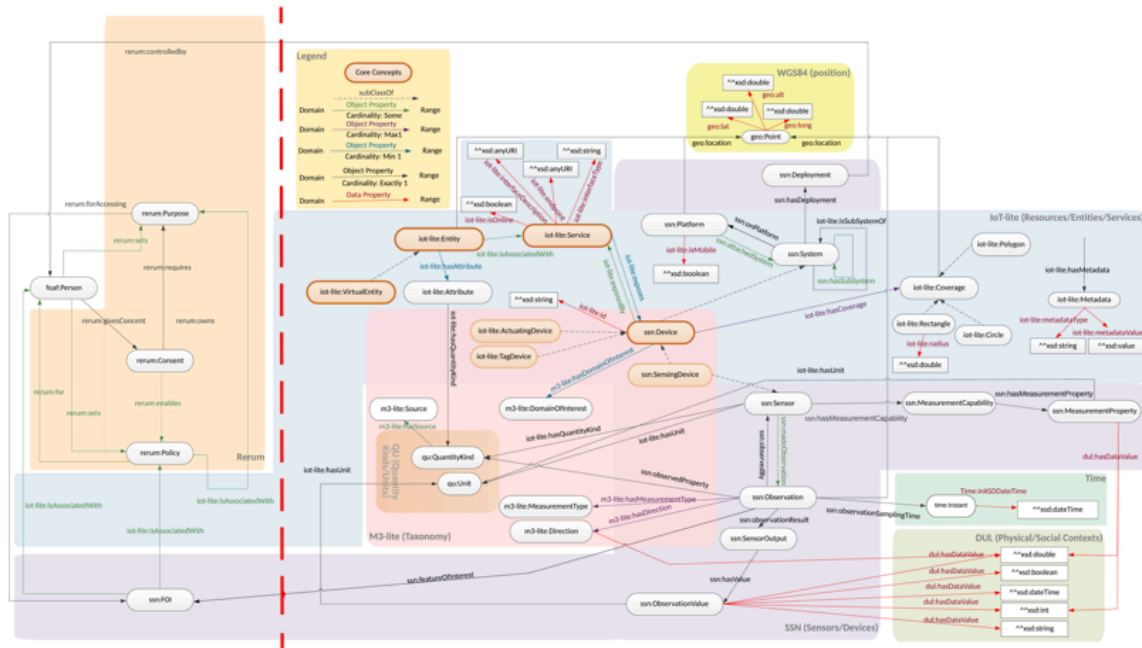


Figure 54. FIESTA-IoT Data Model Extensions for GDPR Compliance Check.

### 6.3 Privacy Dashboard (endpoint privacy policies)

The evaluation process in FIESTA-IoT has been a continuous circular process. The platform tools are updated and they become available for the experimenters to work with them and test them. Then, feedback from the experimenters is evaluated in order to identify required fixes and improvements. After that, the developers work in order to update and improve the tools and give them for the new round of tests.

This process has proved to be very efficient within FIESTA-IoT, allowing for significant improvements been done in the various platform tools. Additionally, this process was also important to identify missing tools that could really extend the functionality of the FIESTA-IoT platform. This is also the case with a new component that was developed in the final months of the project and is related with user privacy. The rest of the paragraphs below describe the platform improvements based on the feedback received from the third-party evaluations, from the internal evaluations and from external comments/suggestions from the Open-Call proposals.

### 6.3.1 Background and motivation

Data access in FIESTA-IoT is controlled by the access policies defined in OpenAM. By default, all users that are registered in the FIESTA-IoT platform have access to all the data that are generated by the integrated testbeds. This means that all the data within the FIESTA-IoT project are open data, publicly available to the registered users. Considering the fact that all data are related to measurements in public spaces for i.e. temperature, humidity, energy consumption, pollution, etc. it seems that this is a reasonable assumption. However, before integrating the testbeds with the FIESTA-IoT platform, the testbed owners were requested to provide the FIESTA-IoT project with their consent to share their data/observations with the experimenters and anyone that



has access to the platform. The testbed owners acknowledged that their data are not sensitive and are open access data and provided their consent.

However, during the project period there were discussions between the project partners and external institutions for integrating additional testbeds (from partners not coming through the Open-Call process). Some testbeds raised concerns about sharing all their data with everyone registered to the platform. They wanted to have control over who has access to their data.

Something similar was also noticed through the Open-Call process, when multiple experimenters wanted to have access to sensitive types of data (which at that point were not available through FIESTA-IoT due to the open access nature of the platform).

Additionally, there is an exponential increase in the interest for privacy protection with respect to sharing data within the EU, which is also proved by the General Data Protection Regulation (GDPR) that comes into effect in May 2018.

The project partners considered all the above and decided to develop a new component that will give full control to the data owners with respect to providing access to their data. This component called Privacy Dashboard (or endpoint privacy policy) was based on the component described in the RERUM project<sup>11</sup>. The main goal of this component is to provide a “one stop shop” to the data owners to be able to see who has access to their data, what types of data they are sharing and change the policies accordingly in a user-friendly way. We have to mention here that with the term “data owner” we refer to the person who owns the data that are being shared through the FIESTA-IoT platform or the person who is the subject of the data.

Finally, before going on to the specifics of the component design, we have to mention that we consider two types of sensors/data within FIESTA-IoT:

- Public sensors/data: the public sensors generate public data that are available to be accessed by all experimenters that are registered to the platform.
- Private sensors/data: The private data are data that can be considered as “sensitive” and the data owner wants to protect the access to these data. Additionally, we consider two types of private sensors:
  - Discoverable: these sensors are private, but the end users can see that they exist and can request access to these data through a consent management system.
  - Hidden: these sensors are private and are also non-discoverable. However, the data owner can create some policies to allow the access of specific users to these data.

### 6.3.2 Component architecture

The overall architecture of the privacy component can be seen in Figure 55. As it is obvious from the figure, the component is basically split in two groups: (i) one group of modules that applies to the data owner and (ii) one group of components that applies to the end user that wants to get access to some data. Both types of users have to be registered to the FIESTA-IoT platform and authenticated to use the system. Thus,

---

<sup>11</sup> <https://ict-rerum.eu/>

logging on to the FIESTA-IoT portal, the portal checks the credentials of the user to see if he is a data owner or an end user to redirect him to the proper web pages.

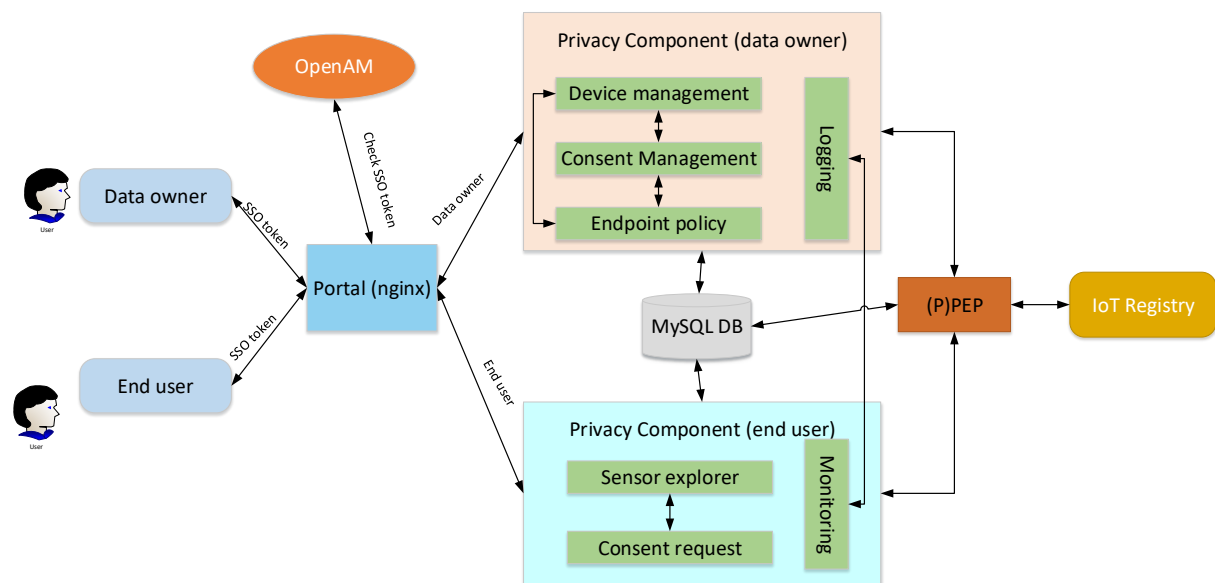


Figure 55. Privacy dashboard overall architecture.

At the data owner side, four main components have been developed:

- **Device management:** this component allows the data owner to check the devices he is sharing and change their nature to make them public, discoverable, hidden, etc.
- **Consent management:** this component allows the data owner to see the number of consent requests that have arrived from end users, check their purpose and either approve them (providing them access to his devices) or reject them (blocking access).
- **Endpoint policy:** this is the main component that allows the data owner to define privacy policies for his data/sensors. The data owner can select policies for all his devices, for multiple devices or one by one. He is also able to define the same policy for all users, multiple users or only one user.
- **Logging:** this component provides information to the data owner regarding the actions of the end users. It provides a user interface, where the data owner can have simple information regarding which end user accessed his data and when.

At the end user side, three main components have been developed:

- **Sensor explorer:** this component provides the functionality to the user to explore the available “discoverable” sensors. It is a user interface, where the user can see the available discoverable sensors, but not their data. The public sensors are not listed in this interface. In order to get access to the data of the discoverable sensors, the end user has to use the consent request component (see below)
- **Consent request:** this component allows the end user to send a request to the data owner to get his consent for accessing data from private-discoverable

sensors. This is a simple form which requests from the end user to state the purpose of accessing the data, so that the data owner can validate if the purpose fits his preferences. These requests are stored in the MySQL data base.

- **Monitoring:** the monitoring component is responsible for monitoring the access of end users to data from private sensors, in order to log this activity and inform the data owner. The activity is stored in the MySQL data base.

As it can be seen from Figure 55, the connection of the end user with the IoT-Registry that has the information for the sensors and the data is controlled by the (P)PEP. The **(P)PEP** is the Privacy Policy Enforcement Point, which is responsible for enforcing the privacy policies defined by the testbed owner. When an end user requests to explore the list of sensors or requests to get access to some data from a sensor, the PPEP checks the policies that are defined by the data owner of that sensor/data and enforces these policies either allowing or blocking the access.

### 6.3.3 User interface

An initial draft implementation of the privacy component was finalised the last months of the project. The component was installed and tested only on the development platform of the project due to the lack of sufficient time to test the component before it is released in the production machine. Additionally, the project did not want to risk changing significantly the functionality of the platform at this critical stage of the project (when almost all experimenters were active).

#### 4.1.3.1 Data owner

The initial screen of the web interface of the data owner can be accessed by the respective menu at the portal. The initial screen is mainly informative, providing some statistics to the data owner and the links for the various actions. The screen can be seen in Figure 56. On the top part there are statistics with respect to the total number of devices the user has registered, the total number of devices he is sharing, the number of users that have access to his data, and the total number of consent requests. Before changing any policies, the user has to sync the endpoint and the users in order to have the latest information. This action performs the respective queries to the IoT-Registry in order to sync this information with the information stored in the MySQL. Then, there are the buttons with links towards setting policies for all endpoints (sensors), for single endpoint, to manage the shared devices, to check the consent requests and to access the logs.

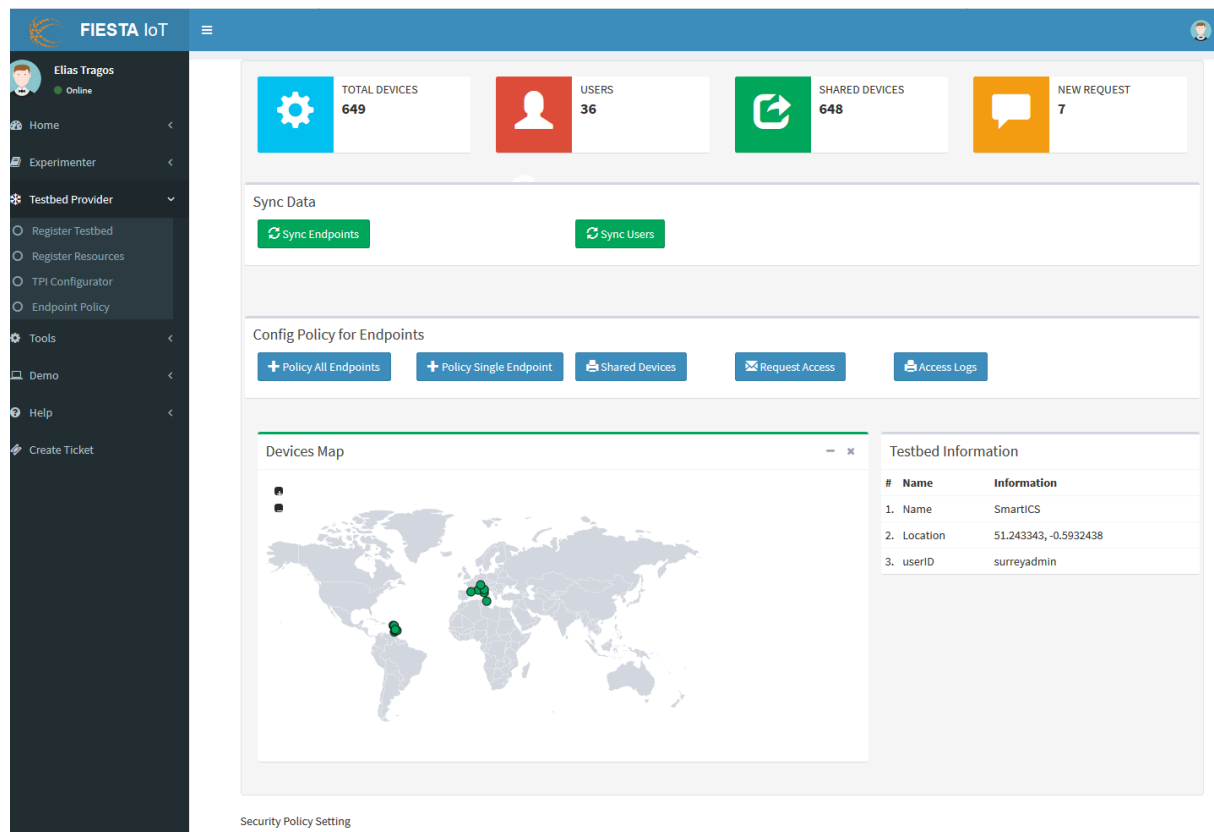


Figure 56. Initial screen of the data owner privacy component.

Figure 57 shows the screen for defining new policies. The data owner can select one or multiple (or all) sensor endpoints and then he can either declare them as “public” or “private”. If the sensors are “public” then they become visible to all end users and they can automatically get access to those data. When the data owner clicks to declare some sensors as “private”, then from the form below he can define the access level of each user to these sensors:

- Visible: this is equal to “discoverable”, which means that the end users can see these sensors to the sensor explorer screen, but do not get access to the data automatically.
- Allow access: Additionally, the data owner can automatically allow access to the sensor to some users, without waiting to get their consent request.
- Disallow access: the data owner can also block access to some user by default.

**Endpoints Policy Config**

**Select Quantity**

-- Select quantity kind --

**Endpoint**

- ☐ http://smart-ics.ee.surrey.ac.uk/fiesta-iot/resource/sc-sics-de-065-light
- ☐ http://smart-ics.ee.surrey.ac.uk/fiesta-iot/resource/sc-sics-de-065-noise
- ☐ http://smart-ics.ee.surrey.ac.uk/fiesta-iot/resource/sc-sics-de-065-humid
- ☐ http://smart-ics.ee.surrey.ac.uk/fiesta-iot/resource/sc-sics-de-065-dust
- ☐ http://smart-ics.ee.surrey.ac.uk/fiesta-iot/resource/sc-sics-de-065-dist
- ☐ http://smart-ics.ee.surrey.ac.uk/fiesta-iot/resource/sc-sics-de-003-dust

**Public** ☐ **Private** ☒

User Id ↑↓	Visible ↑↓	Allow Access ↓↑	Disallow Access ↑↓
ronald.steinke	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
testbed1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
lsanchez-test	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
testbed123	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
dgomez	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
tiago.teixeira	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
mengxuan	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Figure 57. Setting policies per user.

For changing the policies for a single sensor, the data owner can also select the “Policy single endpoint”, which redirects him to the screen shown in Figure 58. Here he can select to edit the policies or view the policies of a single endpoint, as shown in Figure 59.

TOTAL DEVICES  
649

USERS  
36

SHARED DEVICES  
0

NEW REQUEST  
7

Config Policy for Endpoints

+ Policy For All Endpoints
+ Policy For Single Endpoint
Shared Devices
Request Access
Access Logs

Testbed Information

#	Name	Information
1.	Name	SmartICS
2.	Location	51.243343, -0.5932438
3.	userID	surreyadmin

ID	Sensor	Public/Private	
687	http://smart-ics.ee.surrey.ac.uk/fiesta-iot/resource/sc-sics-de-065-light	Private Access	
688	http://smart-ics.ee.surrey.ac.uk/fiesta-iot/resource/sc-sics-de-065-noise	Private Access	
689	http://smart-ics.ee.surrey.ac.uk/fiesta-iot/resource/sc-sics-de-065-humid	Private Access	
690	http://smart-ics.ee.surrey.ac.uk/fiesta-iot/resource/sc-sics-de-065-dust	Private Access	
691	http://smart-ics.ee.surrey.ac.uk/fiesta-iot/resource/sc-sics-de-065-dist	Private Access	
692	http://smart-ics.ee.surrey.ac.uk/fiesta-iot/resource/sc-sics-de-003-dust	Private Access	
693	http://smart-ics.ee.surrey.ac.uk/fiesta-iot/resource/sc-sics-de-003-humid	Private Access	

Figure 58. Single endpoint policy initial screen.

Edit Endpoint Policy
×

ID  
688

Url  
https://platform-dev.fiesta-iot.eu/iot-registry/api/endpoints/5loz6CskJf-5YacPxaJFI92x4dcGVfHH5e4\_Qtl2SgquO7uicpZsVonYqrmLZGcQM\_GeZT7

Sensor Original Id  
http://smart-ics.ee.surrey.ac.uk/fiesta-iot/resource/sc-sics-de-065-noise

Sensor Id  
https://platform-dev.fiesta-iot.eu/iot-registry/api/resources/JpZamUlc17GVaE4kte3t6P8PdWGKAKPJRsZ6oX3nrrT2XnhBgxtlSaQHxVUI8w8E9i0K4B

Testbed Name  
SmartICS

Testbed Id  
49

Public ☐ Private ☒

Config Policy

User Id	Visible	Allow Access	Disallow Access
keti	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
etragos	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
testpolicy	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
flavio	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Figure 59. Setting policies per user for single sensor.

The list of devices that the data owner has shared with some end users can be seen by clicking on the “Shared devices” link. This interface (Figure 60) shows the list and allows the data owner to edit/view the current policies.

The interface displays a dashboard with four summary cards at the top: **TOTAL DEVICES** (649), **USERS** (36), **SHARED DEVICES** (6), and **NEW REQUEST** (7). Below these is a section titled "Config Policy for Endpoints" with five buttons: "+ Policy All Endpoints", "+ Policy Single Endpoint", "Shared Devices" (active), "Request Access", and "Access Logs".

Under "Testbed Information", a table lists details for the SmartICS testbed:

#	Name	Information
1.	Name	SmartICS
2.	Location	51.243343, -0.5932438
3.	userID	surreyadmin

The main section displays a table of shared devices:

ID	Sensor	Public/Private	Actions
687	http://smart-ics.ee.surrey.ac.uk/fiesta-iot/resource/sc-sics-de-065-light	Public Access	[Eye] [Pencil] [X]
688	http://smart-ics.ee.surrey.ac.uk/fiesta-iot/resource/sc-sics-de-065-noise	Public Access	[Eye] [Pencil] [X]
689	http://smart-ics.ee.surrey.ac.uk/fiesta-iot/resource/sc-sics-de-065-humid	Public Access	[Eye] [Pencil] [X]
690	http://smart-ics.ee.surrey.ac.uk/fiesta-iot/resource/sc-sics-de-065-dust	Public Access	[Eye] [Pencil] [X]
691	http://smart-ics.ee.surrey.ac.uk/fiesta-iot/resource/sc-sics-de-065-dist	Public Access	[Eye] [Pencil] [X]
692	http://smart-ics.ee.surrey.ac.uk/fiesta-iot/resource/sc-sics-de-003-dust	Public Access	[Eye] [Pencil] [X]

Showing 1 - 6 of 6 items.

*Figure 60. List of shared devices.*

The consent management console can be accessed by clicking on the “Request access” link. This redirects the data owner to the screen shown in Figure 61. This page shows a list of the consent requests that the data owner has received and his response (reject/accept). By viewing a consent request, the data owner is redirected to the screen in Figure 62, where he can check the content of the request, i.e. the purpose, for which sensor, who made the request, when, etc. Then, by editing the request, the data owner is redirected to the screen in Figure 63, where he can select to approve or reject the request.



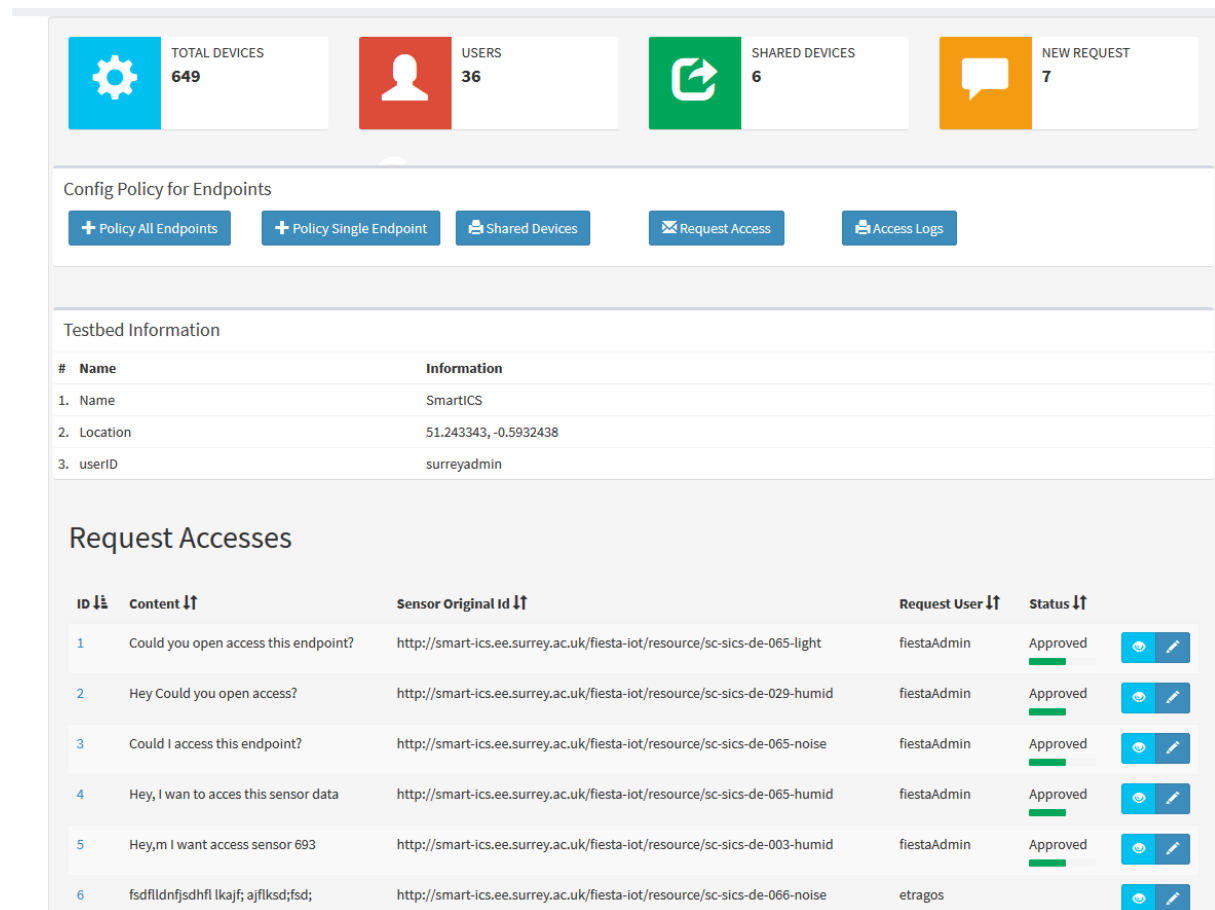


Figure 61. Consent request list.

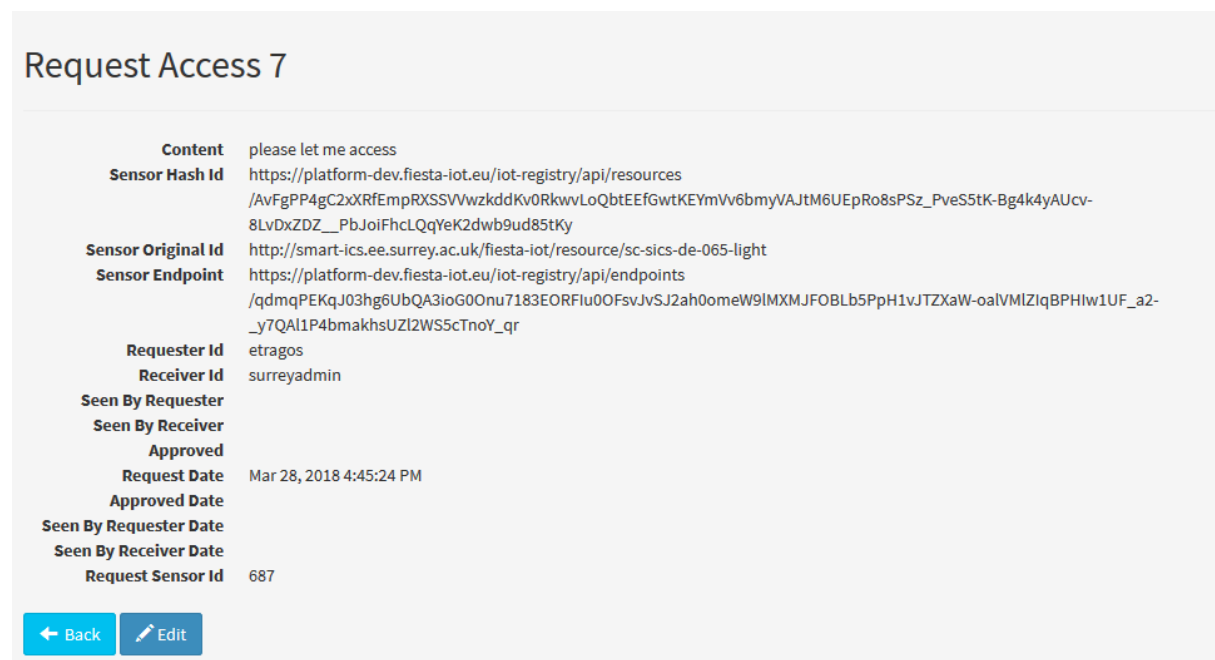


Figure 62. Consent request information.

Create or edit a Request Access

ID  
7

Content  
please let me access

Approved ☐ Rejected ☐

687

Cancel Save

Figure 63. Approve or reject a consent request.

Finally, by clicking on the “Access logs”, the data owner is redirected to the screen in Figure 64, which shows the list of sensors and information of the user id that accessed the sensor and on which date.

TOTAL DEVICES 649

USERS 36

SHARED DEVICES 6

NEW REQUEST 7

Config Policy for Endpoints

+ Policy All Endpoints + Policy Single Endpoint Shared Devices Request Access Access Logs

Testbed Information

#	Name	Information
1.	Name	SmartICS
2.	Location	51.243343, -0.5932438
3.	userID	surreyadmin

Access Logs

ID	User Id	Original Sensor Id	Access Status	Access Time
4	fiestaAdmin	<a href="http://smart-ics.ee.surrey.ac.uk/fiesta-iot/resource/sc-sics-de-065-light">http://smart-ics.ee.surrey.ac.uk/fiesta-iot/resource/sc-sics-de-065-light</a>	SUCCESS	Mar 26, 2018 12:38:51 PM
5	fiestaAdmin	<a href="http://smart-ics.ee.surrey.ac.uk/fiesta-iot/resource/sc-sics-de-029-humid">http://smart-ics.ee.surrey.ac.uk/fiesta-iot/resource/sc-sics-de-029-humid</a>	SUCCESS	Mar 28, 2018 12:56:08 PM
6	fiestaAdmin	<a href="http://smart-ics.ee.surrey.ac.uk/fiesta-iot/resource/sc-sics-de-065-humid">http://smart-ics.ee.surrey.ac.uk/fiesta-iot/resource/sc-sics-de-065-humid</a>	SUCCESS	Mar 28, 2018 2:01:16 PM

Figure 64. Access log list.

#### 4.1.3.2 End user

The end user can select the link “Sensor explorer” on the Experimenter menu of the platform to get the list of sensors that are “Discoverable”. This list is shown in Figure 65. This shows the list of discoverable devices that this user is allowed to see and some information on the quantity kind, the location, etc. Here, the user can click on the edit button to create a new consent request, in order to request access to this device. Then, he is redirected to the screen in Figure 66, where the user in the “Content” box has to specify the purpose for this consent request. As seen in Figure 65, the end user can also see the status of his access to the devices. For example, for the first device with id 687, he has already sent a consent request (with no response yet). For device with id 688, he has sent a request and it was approved, so now he is allowed to access it.

**Sensor Explorers**

Select Quantity  
-- Select quantity kind --

ID	Quantity kind	Unit	Latitude	Longitude	Status	Action
687	Illuminance	MicrowattPerSquareCentimetre	51.243343	-0.5932438	Requested	
688	Sound	Decibel	51.243343	-0.5932438	Requested Approve Access	
689	Humidity	Percent	51.243343	-0.5932438		
690	ChemicalAgentAtmosphericConcentrationDust	MilligramPerCubicMetre	51.243343	-0.5932438		
691	Distance	Centimetre	51.243343	-0.5932438		
692	ChemicalAgentAtmosphericConcentrationDust	MilligramPerCubicMetre	51.243343	-0.5932438		

Showing 1 - 20 of 649 items.

« < 1 2 3 4 5 > »

Figure 65. Sensor explorer initial screen.

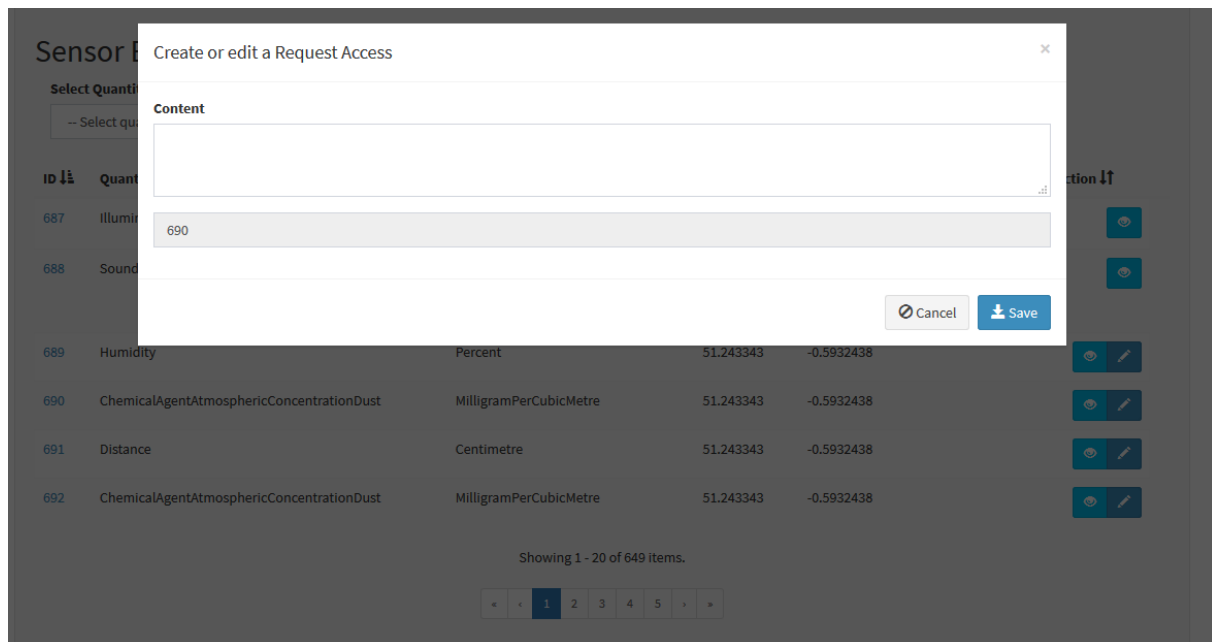


Figure 66. Declaring the purpose for the consent request.

### 6.3.4 Discussion

The privacy component fits perfectly with the requirements and the nature of the FIESTA-IoT project, since it provides full control to the data owners for the data that they share through the FIESTA-IoT platform. The component also respects the specificities and especially the testbed-agnostic nature of the project. This is evident in Figure 65, where the end user only sees the quantity kind/location of the sensors he is allowed to access and not the information regarding which testbed/data owner owns this device.

The initial tests that were performed on the development platform of FIESTA-IoT are very promising. The privacy component works as expected with accurate actions regarding blocking/allowing access of the end users to the data. Additionally, the component does not affect the stability or the responsiveness of the system to the user requests and does not add extra delay to the response.

In general, the component has been evaluated favourably by the project partners in all the tests.

## 7 CONCLUSIONS

This deliverable has presented the analysis of the final version of the platform, including both, the functional and non-functional analysis. Additionally, the deliverable has also included the latest updates from the in-house experiments, already described in detail in the deliverable D5.2 (FIESTA-IoT D5.2, 2017). Finally, this deliverable describes the technical considerations that might be observed to achieve formal alignment with the new GDPR and the new updates performed on the platform based on the feedback received. More precisely, the “privacy content dashboard”, which provides a tool to share sensitive data to the testbeds owners of the FIESTA-IoT platform.

In section 2, we have presented the different updates performed in the in-house experiments. Apart from the in-house experiments update during the third year, we can highlight the integration of the CEMA deployment in New Zealand in the ontology, to analyse crowd behaviour (section 2.1).

The platform functional analysis through the feedback of the external experimenters has been described in section 3. In this section it can be found the publishable summaries submitted by the external experimenters (see section 3.1) and the analysis of the feedback provided by them in section 3.2. Based on the evaluation of the platform, we can see that the feedback from external experimenters have been better in the successive Open-Calls, which shows the improvement of the platform over the time.

Similarly to the analysis of the feedback from experimenters, section 4 describes the publishable summaries of the testbeds that have been integrated into the platform, as well as the analysis of their feedback regarding to its use.

Section 5 presents the non-functional evaluation of the FIESTA-IoT platform, analysing the queries performed against it by both, testbeds and experimenters. This analysis proves the capacity of the platform to support external experimentation over the time.

Finally, section **Error! Reference source not found.** describes in detail the technical considerations that have been initially foreseen to align the current FIESTA-IoT Platform architecture and components with the requirements of the new GDPR. Furthermore, it also describes one of the latest integration performed in the platform: the privacy dashboard, which provides the option of sharing only some of the resources with specific experimenters, along with additional privacy tools.

Based on the analysis presented in this report, we can conclude that the FIESTA-IoT platform is suitable and reliable enough to host external experiments. The platform provides semantic functionalities for data agnostic access from different federated testbeds, independently from the API and ontology from each of them.

## 8 REFERENCES

- Bethencourt, J., Sahai, A., & Waters, B. (2007). Ciphertext-Policy Attribute-Based Encryption. *Security and Privacy*, 321-334.
- Bonomi, F., Milito, R., Zhu, J., & Addepalli, S. (2012). Fog Computing and Its Role in the Internet of Things. *Proceedings of the First Edition*, (pp. 13-16). of the MCC Workshop on Mobile Cloud Computing.
- FIESTA-IoT D2.1. (2015). *FIESTA-IoT Project Deliverable D2.1 - Stakeholders requirements*.
- FIESTA-IoT D2.3. (2016). *FIESTA-IoT Project Deliverable D2.3 - Specification of Experiments, Tools and KPIs*.
- FIESTA-IoT D2.4. (2015). *FIESTA-IoT Project Deliverable D2.4 - FIESTA Meta-Cloud Architecture and Technical Specifications*.
- FIESTA-IoT D3.1. (2016). *FIESTA-IoT Project Deliverable D3.1 - Semantic models for testbeds, interoperability and mobility support and best practices*.
- FIESTA-IoT D3.2. (2016). *FIESTA-IoT Project Deliverable D3.2 - Semantic Models for Testbeds, Interoperability and Mobility Support, and Best Practices*.
- FIESTA-IoT D4.1. (2015). *FIESTA-IoT Project Deliverable D4.1 - EaaS Model Specification and Implementation*.
- FIESTA-IoT D4.2. (2017). *FIESTA-IoT Project Deliverable D4.2 - EaaS Model Specification and Implementation V2*.
- FIESTA-IoT D4.5. (2016). *FIESTA-IoT Project Deliverable D4.5 - Tools and Techniques for Managing Interoperable Data sets*.
- FIESTA-IoT D5.1. (2016). *FIESTA-IoT Project Deliverable D5.1 - Experiment Design and Specification*.
- FIESTA-IoT D5.2. (2017). *FIESTA-IoT Project Deliverable D5.2 - Experiments Implementation, Integration and Evaluation*.
- FIESTA-IoT D5.4. (2018). *FIESTA-IoT Project Deliverable D5.4 - Best Practices for Experiments Design and Conduction*.
- Waters, B. (2011). Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization. *Public Key Cryptography – PKC 2011*, 53-70.
- Wu, F.-J., & Solmaz, G. (June 2018.). CrowdEstimator: Approximating Crowd Sizes with Multi-modal Data for Internet-of-Things Services. *Proceedings of ACM MobiSys'18*. ACM.

## ANNEX I QUESTIONNAIRE FOR EXPERIMENTERS

Experimenters have to fill the questionnaire below to evaluate the tools and resources that served during their experiment development, deployment and execution.

### Starting the experimentation

#### Part I: documentation

#### Q1. Did you use the documentation for experimenters provided on the moodle?

- Yes, I consulted almost all the documents
  - Please, specify the ones you mainly used.....
- Yes, but only some documents
  - Please, specify the ones you mainly used.....
- No, I didn't

#### Q2. Were you able to find the needed information?

- Always
- Most of the time
- Sometimes
- Never

#### Q3. Do you believe that some documentation is missing?

- Yes
  - Please specify.....
- No

#### Q4. How would you rate the quality of the documentation provided to discover the platform?

	EXCELLENT	VERY GOOD	GOOD	FAIR	POOR	N/A
➤ Documentation about FEDSPEC	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
➤ Documentation about APIs	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
➤ Documentation about Ontology	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
➤ Documentation about SPARQL queries	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
➤ Documentation about installing Experiment Data Receiver	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
➤ Experiment Execution process and guidelines	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
➤ Overall documentation in the Project Handbook	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

#### Q5. How would you rate the relevance of the documentation to support you to set up your experimentation?



	EXCELLENT	VERY GOOD	GOOD	FAIR	POOR	N/A
➤ Documentation about FEDSPEC	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
➤ Documentation about APIs	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
➤ Documentation about Ontology	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
➤ Documentation about SPARQL queries	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
➤ Documentation about installing Experiment Data Receiver	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
➤ Experiment Execution process and guidelines	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
➤ Overall documentation in the Project Handbook	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

## Part II: ease of setting up, ease of deployment

	EXCELLENT	VERY GOOD	GOOD	FAIR	POOR	N/A
Q6. How would you rate the FEDSPEC creation process?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Q7. How would you rate the SPARQL Queries creation process?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Q8. How would you rate the integration and deployment process?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Q9. How would you rate the quality and quantity of available data?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Q10. How would you rate the performance of EEE module?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Q11. How would you qualify the quality and relevance of tools that have been made available to you?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Q12. How would you qualify the quality of FIESTA-IoT APIs?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

**Q13. How would you qualify the easy of installing Experiment Data Receiver (Excellent being very easy and Poor being very hard)**

☐ ☐ ☐ ☐ ☐ ☐

**Q14. In case any of the above answers were not Very Good or Excellent, what would you require from the tools to reach such levels?**

*Aspects that prevented the tools made available to you (Experiment Management and Engine, APIs, Available Data, etc.) for running your experiment from getting Excellent or Very Good marks.*

**Q15. Do you prefer to use the API-based solution rather than the experiment portal?**

- Yes
- No

*If Yes, Please specify the reason.....*

**Q16. How much time have you spent in total to integrate the FIESTA-IoT tools in your experiment for having the first experiment prototype working (it counts only the time used to setup the FIESTA-IoT tools such as APIs connector, EMC, Data Receiver setup and so on, without counting effort for visualization tools or set up of external tools):**

	LESS THAN 1 WEEK	LESS THAN 2 WEEKS	LESS THAN 1 MONTH	LESS THAN 2 MONTHS	MORE THAN 2 MONTHS
➤ <b>Novice Level*</b>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
➤ <b>Basic Integration Level</b>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
➤ <b>Full Integration Level</b>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

\* "Novice Level" corresponds to following the instructions in the handbook, "Basic Integration level" corresponds to the first integration of your experiment to Fiesta-IoT, and "Full Integration level" refers to a final integration after necessary fine-tuning of your experiment

## During the experimentation

**Q17. How would you rate your experience of the FIESTA-IoT platform during the experimentation?**

	EXCELLENT	VERY GOOD	GOOD	FAIR	POOR
➤ Availability of the platform	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
➤ Performance of the platform	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
➤ Usability of the portal	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
➤ Performance of the portal	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
➤ Availability of the portal	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

**Q18. In case any of the above answers were not Very Good or Excellent, what would you require from the tools to reach such levels?**

*Aspects that prevented the Platform and Portal from getting Excellent or Very Good marks.*

**Q19. Did you use the FIESTA-IoT support tools during the experimentation?**

	YES	NO
➤ Questions and answers	<input type="checkbox"/>	<input type="checkbox"/>
➤ YouTube video channel	<input type="checkbox"/>	<input type="checkbox"/>
➤ Live chat	<input type="checkbox"/>	<input type="checkbox"/>
➤ Ticketing system	<input type="checkbox"/>	<input type="checkbox"/>

**Q20. How would you rate your experience of the FIESTA-IoT ticketing system during the experimentation?**

	EXCELLENT	VERY GOOD	GOOD	FAIR	POOR
➤ Availability of the ticketing system	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
➤ Performance of the ticketing system	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
➤ Usability of the ticketing system	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
➤ Speed of responses	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
➤ Overall satisfaction of the ticketing system	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

**Q21. Please, give us all comments you may have about your experience during the experimentation**

*To add comments as required.*

## Ending the experiment

	EXCELLENT	VERY GOOD	GOOD	FAIR	POOR
<b>Q22. Overall, how do you qualify your experience on FIESTA-IoT platform?</b>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

### Q23. Are you satisfied with the results you obtained?

- Yes, I'm very satisfied
- Yes, but only partially
  - *Explain the reasons for this partial satisfaction*
- No, I'm not
  - *Explain the reasons for your dissatisfaction*

### Q24. Are you satisfied with the results you obtained?

- Yes, I'm very satisfied
- Yes, but only partially
  - *Explain the reasons for this partial satisfaction*
- No, I'm not
  - *Explain the reasons for your dissatisfaction*

### Q25. What value does having access to the FIESTA-IoT Platform provide for your research?

*To describe the main added-value obtained through the FIESTA-IoT Platform. Optimally, describe the limitations for your research in absence of the offering of the FIESTA-IoT Platform.*

### Q26. Would you be prepared to pay to be part of the FIESTA-IoT beyond the lifetime of the project?

- Yes
  - *Would you pay on a subscription basis, as a one off charge, or in return for activity routed to your testbed?*
- No
  - *Who do you think should pay to maintain the FIESTA-IoT?*

### Q27. Do you intend to continue to be part of the federation beyond the lifetime of the project?

- Yes
- No
- If No, what would attract you to continue?

**Q28. Would you recommend FIESTA-IoT platform to other experimenters?**

- Yes
- No

*Provide summary comments highlighting the strong and weak aspects of experimentation using the FIESTA-IoT Platform.*

## ANNEX II QUESTIONNAIRE FOR TESTBEDS

Testbed Providers have to fill the questionnaire below to evaluate the tools and resources that served during the integration of their testbeds.

### Starting the integration

#### Q01 Did you use the documentation for extensions provided on the Moodle?

- Yes, I consulted almost all the documents
  - Please, specify the ones you mainly used.....
- Yes, but only some documents
  - Please, specify the ones you mainly used.....
- No, I didn't

#### Q02 Were you able to find the needed information?

- Always
- Most of the time
- Sometimes
- Never

#### Q03 Do you believe that some documentation is missing?

- Yes
  - Please specify.....
- No

#### Q04 How would you rate the quality of the documentation provided to integrate the testbed?

	EXCELLENT	VERY GOOD	GOOD	FAIR	POOR	N/A
➤ Documentation about APIs	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
➤ Documentation about Ontology	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
➤ Documentation about annotators	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
➤ Documentation about Annotator as a Service	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
➤ Documentation about Testbed Provider Services	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
➤ Testbed integration process and guidelines	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
➤ Overall documentation in the Project Handbook	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

#### Q05 How would you rate the relevance of the documentation to support you to set up your experimentation?



	EXCELLENT	VERY GOOD	GOOD	FAIR	POOR	N/A
➤ Documentation about APIs	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
➤ Documentation about Ontology	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
➤ Documentation about annotators	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
➤ Documentation about Annotator as a Service	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
➤ Documentation about Testbed Provider Services	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
➤ Testbed integration process and guidelines	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
➤ Overall documentation in the Project Handbook	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

## During the testbed integration

## Part I: ease of setting up, ease of deployment

	EXCELLENT	VERY GOOD	GOOD	FAIR	POOR	N/A
Q06 How would you rate the Certification Portal?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Q07 How would you rate the Annotator-as-a-Service tool?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Q08 How would you rate the Testbed Registration process?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Q09 How would you rate the Resource Registration process?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

**Q10 In case any of the above answers were not Very Good or Excellent, what would you require from the tools to reach such levels?**

*Aspects that prevented Certification Portal, AaaS, Testbed Registration and/or Resource Registration from getting Excellent or Very Good marks.*

**Q11 Do you prefer to use the API-based resource registration rather than the portal-based options (manual, text, file upload)?**

- Yes
- No

*If Yes, please specify the reason.....*

*If No, please specify which of the three options you employed and what made you prefer that one.....*

	EXCELLENT	VERY GOOD	GOOD	FAIR	POOR	N/A
<b>Q12 How would you rate the Testbed Provider Interface Configurator?</b>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<b>Q13 How would you qualify the quality and relevance of tools that have been made available to you?</b>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<b>Q14 How would you qualify the quality of FIESTA-IoT APIs?</b>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

**Q15 In case any of the above answers were not Very Good or Excellent, what would you require from the tools to reach such levels?**

*Aspects that prevented TPI Configurator and/or FIESTA-IoT APIs from getting Excellent or Very Good marks.*

**Q16 How would you rate your experience of the FIESTA-IoT platform during the testbed integration?**

	EXCELLENT	VERY GOOD	GOOD	FAIR	POOR
➤ Availability of the platform	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
➤ Performance of the platform	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
➤ Usability of the portal	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
➤ Performance of the portal	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
➤ Availability of the portal	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

## Part II: support during the integration

**Q17 Did you use the FIESTA-IoT support tools during the testbed integration?**

	YES	NO
➤ Questions and answers	<input type="checkbox"/>	<input type="checkbox"/>
➤ YouTube video channel	<input type="checkbox"/>	<input type="checkbox"/>
➤ Live chat	<input type="checkbox"/>	<input type="checkbox"/>
➤ Ticketing system	<input type="checkbox"/>	<input type="checkbox"/>

**Q18 How would you rate your experience of the FIESTA-IoT ticketing system during the testbed integration?**

	EXCELLENT	VERY GOOD	GOOD	FAIR	POOR
➤ Availability of the ticketing system	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
➤ Performance of the ticketing system	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
➤ Usability of the ticketing system	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
➤ Speed of responses	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
➤ Overall satisfaction of the ticketing system	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

**Q19 Please, give us all comments you may have about your experience during the testbed integration**

*To add comments as required.*

Ending the testbed integration

	EXCELLENT	VERY GOOD	GOOD	FAIR	POOR
<b>Q20 Overall, how do you qualify your experience on FIESTA-IoT platform?</b>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

**Q21 Are you satisfied with the results you obtained?**

- Yes, I'm very satisfied
- Yes, but only partially
  - *Explain the reasons for this partial satisfaction*
- No, I'm not
  - *Explain the reasons for you dissatisfaction*

**Q22 What value does being part of the FIESTA-IoT federation provide for your testbed?**

**Q23 Would you be prepared to pay to be part of the FIESTA-IoT beyond the lifetime of the project?**

- Yes
  - *Would you pay on a subscription basis, as a one off charge, or in return for activity routed to your testbed?*
- No
  - *Who do you think should pay to maintain the FIESTA-IoT?*

**Q24 Do you intend to continue to be part of the federation beyond the lifetime of the project?**

- Yes
- No
- If No, what would attract you to continue?

**Q25 Would you recommend FIESTA-IoT platform to other testbeds?**

- Yes
- No

*As a follow-up of the last question on the previous section, provide summary comments highlighting the strong and weak aspects of the process of integrating your testbed within the FIESTA-IoT Platform.*

Strong aspects of the FIESTA-IoT Platform

*Positive experiences and feedback*

Weak aspects of the FIESTA-IoT Platform

*Issues encountered and hurdles that should be removed if possible.*

Recommendations from improvements of the FIESTA-IoT Platform

*Recommendations if any.*

In order to integrate a testbed within the FIESTA-IoT platform there are a set of well-defined steps/requirements that must be fulfilled. The effort needed to address them from the point of view of the testbed providers, is also key to qualify the FIESTA-IoT platform. Thus, it is indispensable to assess the effort employed in addressing these requirements.

Evaluated requirements are as follows:

- **Ontology and taxonomy adaptation**, which implies the gathering of feedback and subsequent amendment of FIESTA-IoT Ontology and M3-lite taxonomy

- **Annotator development and validation**, which implies the implementation of annotator module and the validation of the resulting annotated testbed resources' descriptions and annotated observations.
- **Testbed Provider Services (TPS) development and validation**, which implies the implementation of the necessary TPS and its interoperability compliance check.
- **Testbed Certification**, which implies the qualification as a certified testbed by applying on the FIESTA-IoT Certification portal.
- **Testbed and Resources registration**, which implies the process of registering the testbed and its devices on the FIESTA-IoT Platform.
- **TPS integration and configuration**, which implies the integration of the TPS into the testbed and the configuration of the schedule at the TPI Configuration UI resulting in the pull/push of observations towards the FIESTA-IoT Platform.

Testbed Providers have to fill the questionnaire below to summarize their experience during the integration of their testbeds.

**Q26 How much time have you spent to complete the ontology and taxonomy adaptation necessary to integrate your testbed in the FIESTA-IoT Platform?**

	LESS THAN 1 WEEK	LESS THAN 2 WEEKS	LESS THAN 1 MONTH	LESS THAN 2 MONTHS	MORE THAN 2 MONTHS
➤ <b>Full Integration Level</b>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

**Q27 How much time have you spent in total to implement the annotator used for your testbed integration in the FIESTA-IoT Platform?**

	LESS THAN 1 WEEK	LESS THAN 2 WEEKS	LESS THAN 1 MONTH	LESS THAN 2 MONTHS	MORE THAN 2 MONTHS
➤ <b>Basic Integration Level</b>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
➤ <b>Full Integration Level</b>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

\* “Basic Integration level” corresponds to the first integration of your testbed to FIESTA-IoT (upon annotator validation), and “Full Integration level” refers to a final integration after necessary fine-tuning of your testbed interfaces

**Q28 How much time have you spent in total to implement the Testbed Provider Service used for your testbed integration in the FIESTA-IoT Platform?**

	LESS THAN 1 WEEK	LESS THAN 2 WEEKS	LESS THAN 1 MONTH	LESS THAN 2 MONTHS	MORE THAN 2 MONTHS
➤ <b>Basic Integration Level</b>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
➤ <b>Full Integration Level</b>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

\* “Basic Integration level” corresponds to the first integration of your testbed to FIESTA-IoT (upon interoperability compliance check), and “Full Integration level” refers to a final integration after necessary fine-tuning of your testbed interfaces

**Q29. How much time have you spent in obtaining the FIESTA-IoT Testbed Certificate?**

	LESS THAN 1 WEEK	LESS THAN 2 WEEKS	LESS THAN 1 MONTH	LESS THAN 2 MONTHS	MORE THAN 2 MONTHS
➤ <b>Full Integration Level</b>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

**Q30. How much time have you spent in total to register your testbed and resources in the FIESTA-IoT Platform?**

	LESS THAN 1 WEEK	LESS THAN 2 WEEKS	LESS THAN 1 MONTH	LESS THAN 2 MONTHS	MORE THAN 2 MONTHS
➤ <b>Basic Integration Level</b>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
➤ <b>Full Integration Level</b>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

\* “Basic Integration level” corresponds to the first integration of your testbed to FIESTA-IoT (upon integration in playground), and “Full Integration level” refers to a final integration after necessary fine-tuning of your testbed interfaces

**Q31. How much time have you spent in total to integrate your TPS in your testbed and configure it using the TPI Configuration UI at the FIESTA-IoT Platform?**

	LESS THAN 1 WEEK	LESS THAN 2 WEEKS	LESS THAN 1 MONTH	LESS THAN 2 MONTHS	MORE THAN 2 MONTHS
➤ <b>Basic Integration Level</b>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
➤ <b>Full Integration Level</b>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

\* “Basic Integration level” corresponds to the first integration of your testbed to FIESTA-IoT (upon integration in playground), and “Full Integration level” refers to a final integration after necessary fine-tuning of your testbed interfaces



## ANNEX III LARGE SCALE EXPERIMENT QUERIES

Noise more than 50 dB(A)
<pre> Prefix ssn: &lt;http://purl.oclc.org/NET/ssnx/ssn#&gt; Prefix iotlite: &lt;http://purl.oclc.org/NET/UNIS/fiware/iot-lite#&gt; Prefix dul: &lt;http://www.loa.istc.cnr.it/ontologies/DUL.owl#&gt; Prefix geo: &lt;http://www.w3.org/2003/01/geo/wgs84_pos#&gt; Prefix time: &lt;http://www.w3.org/2006/time#&gt; Prefix m3-lite: &lt;http://purl.org/iot/vocab/m3-lite#&gt; Prefix xsd: &lt;http://www.w3.org/2001/XMLSchema#&gt; Prefix rdf: &lt;http://www.w3.org/1999/02/22-rdf-syntax-ns#&gt; select ?sensorID (max(?ti) as ?time) ?value ?latitude ?longitude where {     ?o a ssn:Observation.     ?o ssn:observedBy ?sensorID.     ?o ssn:observedProperty ?qkr.     ?qkr rdf:type ?qk.     Values ?qk {m3-lite:Sound m3-lite:SoundPressureLevelAmbient}     ?o ssn:observationSamplingTime ?t.     ?o geo:location ?point.     ?point geo:lat ?latitude.     ?point geo:long ?longitude.     ?t time:inXSDDateTime ?ti.     ?o ssn:observationResult ?or.     ?or ssn:hasValue ?v.     ?v dul:hasDataValue ?value.     FILTER(?value&gt;="50"^^xsd:double)     FILTER(?ti &gt; "%%fromDateTime%"^^xsd:dateTime &amp;&amp; ?ti &lt; "%%toDateTime%"^^xsd:dateTime)     } group by ?sensorID ?time ?value ?latitude ?longitude </pre>

Noise less than 30 dB(A)
<pre> Prefix ssn: &lt;http://purl.oclc.org/NET/ssnx/ssn#&gt; Prefix iotlite: &lt;http://purl.oclc.org/NET/UNIS/fiware/iot-lite#&gt; Prefix dul: &lt;http://www.loa.istc.cnr.it/ontologies/DUL.owl#&gt; Prefix geo: &lt;http://www.w3.org/2003/01/geo/wgs84_pos#&gt; Prefix time: &lt;http://www.w3.org/2006/time#&gt; Prefix m3-lite: &lt;http://purl.org/iot/vocab/m3-lite#&gt; </pre>

```

Prefix xsd: <http://www.w3.org/2001/XMLSchema#>
Prefix rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#>
select ?sensorID (max(?ti) as ?time) ?value ?latitude ?longitude
where {
    ?o a ssn:Observation.
    ?o ssn:observedBy ?sensorID.
    ?o ssn:observedProperty ?qkr.
    ?qkr rdf:type ?qk.
    Values ?qk {m3-lite:Sound m3-lite:SoundPressureLevelAmbient}
    ?o ssn:observationSamplingTime ?t.
    ?o geo:location ?point.
    ?point geo:lat ?latitude.
    ?point geo:long ?longitude.
    ?t time:inXSDDateTime ?ti.
    ?o ssn:observationResult ?or.
    ?or ssn:hasValue ?v.
    ?v dul:hasDataValue ?value.
    FILTER(?value<="30"^^xsd:double)
    FILTER(?ti > "%%fromDateTime%"^^xsd:dateTime && ?ti <
"%%toDateTime%"^^xsd:dateTime)
} group by ?sensorID ?time ?value ?latitude ?longitude

```

### Noise observations for a given bounding box

```

Prefix ssn: <http://purl.oclc.org/NET/ssnx/ssn#>
Prefix iotlite: <http://purl.oclc.org/NET/UNIS/fiware/iot-lite#>
Prefix dul: <http://www.loa.istc.cnr.it/ontologies/DUL.owl#>
Prefix geo: <http://www.w3.org/2003/01/geo/wgs84_pos#>
Prefix time: <http://www.w3.org/2006/time#>
Prefix m3-lite: <http://purl.org/iot/vocab/m3-lite#>
Prefix xsd: <http://www.w3.org/2001/XMLSchema#>
Prefix rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#>
select ?sensorID (max(?ti) as ?time) ?value ?latitude ?longitude
where {
    ?o a ssn:Observation.
    ?o ssn:observedBy ?sensorID.
    ?o ssn:observedProperty ?qkr.
    ?qkr rdf:type ?qk.
    Values ?qk {m3-lite:Sound m3-lite:SoundPressureLevelAmbient}

```

```

?o ssn:observationSamplingTime ?t.
?o geo:location ?point.
?point geo:lat ?latitude.
?point geo:long ?longitude.
?t time:inXSDDateTime ?ti.
?o ssn:observationResult ?or.
?or ssn:hasValue ?v.
?v dul:hasDataValue ?value.
FILTER (
  (xsd:double(?latitude) >= "43.461708"^^xsd:double)
  && (xsd:double(?latitude) <= "43.462898"^^xsd:double)
  && (xsd:double(?longitude) >= "-3.802127"^^xsd:double)
  && (xsd:double(?longitude) <= "-3.796715"^^xsd:double)
)
FILTER(?ti > "%%fromDateTime%"^^xsd:dateTime && ?ti <
"%%toDateTime%"^^xsd:dateTime)
} group by ?sensorID ?time ?value ?latitude ?longitude

```

### Noise observations for a given location

```

Prefix ssn: <http://purl.oclc.org/NET/ssnx/ssn#>
Prefix iotlite: <http://purl.oclc.org/NET/UNIS/fiware/iot-lite#>
Prefix dul: <http://www.loa.istc.cnr.it/ontologies/DUL.owl#>
Prefix geo: <http://www.w3.org/2003/01/geo/wgs84_pos#>
Prefix time: <http://www.w3.org/2006/time#>
Prefix m3-lite: <http://purl.org/iot/vocab/m3-lite#>
Prefix xsd: <http://www.w3.org/2001/XMLSchema#>
select ?sensorID (max(?tim) as ?time) ?val
where {
  ?o a ssn:Observation.
  ?o ssn:observedBy ?sensorID.
  ?o ssn:observedProperty ?qkr.
  ?qkr rdf:type ?qk.
  Values ?qk {m3-lite:Sound m3-lite:SoundPressureLevelAmbient}
  ?o ssn:observationSamplingTime ?t.
  ?o geo:location ?point.
  ?point geo:lat "43.46477E1"^^xsd:double.
  ?point geo:long " -3.8081E0"^^xsd:double.
  ?t time:inXSDDateTime ?ti.

```

```
    ?o ssn:observationResult ?or.  
    ?or ssn:hasValue ?v.  
    ?v dul:hasDataValue ?value.  
    FILTER(?ti > "%%fromDateTime%"^^xsd:dateTime && ?ti <  
    "%%toDateTime%"^^xsd:dateTime)  
  } group by (?sensorID) ?time ?value
```