Smart Governance of Heterogeneous Internet of Things for Smart Cities

Aqeel Kazmi
Insight Centre for Data Analytics
National University of Ireland Galway
Galway, Ireland
aqeel.kazmi@insight-centre.org

Martin Serrano
Insight Centre for Data Analytics
National University of Ireland Galway
Galway, Ireland
martin.serrano@insight-centre.org

Angelos Lenis
Upwork
Mountain View
California, United States
lenis.angelos@gmail.com

***Abstract*—The Internet of Things (IoT) is a fast-emerging technology which aims to address the societal challenges faced by the modern cities. IoT can be underpinned in a wide range of Smart City applications including (but not limited to) holistic urban planning, tracking of city wide services, enhancing public transportation, while reducing traffic congestion, keeping citizens safe, enabling sustainable economic growth, and improving quality of life of citizens. IoT has been growing rapidly in different domains, which led to the development of numerous IoT platforms, standards, and protocols, etc. Today, within a Smart City, different types of IoT systems and applications are deployed which operate independently. There is a need to enable city authorities and application developers to see IoT systems as part of an integrated whole, allowing optimal use of existing infrastructure and achieving more than what these independent systems can do in isolation. Furthermore, with the arrival of European Union's General Data Protection Regulation (GDPR), the governance of diverse IoT resources has become a critical requirement. This paper presents a smart governance methodology designed for managing heterogeneous IoT systems. The proposed approach facilitates the semantic interoperability of IoT infrastructure deployed across various domains in Smart Cities and enables integrated governance (and management) of IoT systems and their resources.**

***Index Terms*—Internet of Things; Smart Cities ; Data Governance; Data Policies**

I. Introduction

Smart Cities represent the ultimate urban development vision of modern cities. A Smart City uses ICT infrastructure to efficiently manage the city-wide resources and citizen-centric services. The Smart Cities are increasingly seeking ICT-driven solutions to plan and monitor their sustainable interventions on the urban environment. Such interventions include the development, deployment and operation of IoT-based smart city services. The IoT paradigm is expected to benefit and improve the intelligence of the cities by promoting the interaction between the citizens and the environment. Cities are gradually deploying IoT infrastructures and applications. These infrastructures span across different IoT and communication technologies (e.g., Wireless Sensor Networks (WSNs), Radio-Frequency Identification (RFID), Cameras, smart meters [1], actuators, broadband networks, open data set portals) and target different applications areas such as smart energy, waste, traffic, mobility, healthcare, active and healthy ageing, ambient-assisted living, etc.

Currently, IoT-based Smart City applications operate in isolation e.g. they are developed and managed independently. Typically, an IoT application/system collects high volumes of data streams from a plethora of underlying sensing devices. The design of sophisticated IoT applications must harness an IoT platform. An IoT platform is a software system that is used to collect data streams from sensors, provide monitoring capability, and in some cases control the IoT devices. Nowadays, there is a large number of IoT platforms, which empower the data measurement, processing, and actuation tasks, including platforms that emphasize the integration of BigData functionalities for Smart Cities [2]), and platforms that support the integration with Cyber-Physical Systems (CPS) as a means of supporting actuation tasks [3]. The development and deployment of these IoT systems and platforms, typically managed independently, tend to form vertical fragmented application silos, which are very difficult to manage in an integrated way. As a result, this fragmented IoT landscape requires the city authorities and application developers to deal with diverse set of IoT platforms, devices and data models.

The ability to plan, monitor and govern IoT based infrastructures and services regardless of the technology platform that empowers them is a key enabler for structuring and organizing city-wide interventions. City authorities (and administrators) should be able to manage and govern diverse IoT systems and data sources from a single entry point. In this paper, we present integrated and smart governance methodology designed for managing and monitoring diverse IoT devices and services that are made available through diverse IoT platforms. This approach is developed as a part of the VITAL-OS [4] project. VITAL-OS is an IoT operating system for Smart Cities that facilitates access and control of the IoT infrastructure, resources and sensor networks, with abstraction and tools that can additionally be used by developers to create new applications utilizing available IoT resources to empower citizens. One of the core characteristics of this platform is its integrated Management and Governance layer, which aims at providing functionalities for governing diverse IoT systems and services, in a unified way, thereby facilitating the city-wide planning and monitoring of relevant interventions. Despite the importance of integrated governance and management of city-wide IoT infrastructure, most of the existing IoT platforms do not provide relevant functionalities and therefore VITAL-OS aspires to be a pioneer in this respect.

The remainder of the article is structured as follows. Section II discusses IoT-related standards for smart city applications, including reference architectures and interoperability related efforts. It also positions the VITAL-OS platform within the interoperability related standardisation efforts. In addition, it presents the architecture and main components of VITAL-OS and discuss its key functionalities in terms of integrating heterogeneous IoT systems. In Section III the development of the smart Governance methodology of VITAL-OS is discussed. In Section IV VITAL-OS use cases and platform evaluation is discussed. The article end-up with a concluding paragraph, which highlights the key contributions of work presented in this paper.

II. IoT Deployments and Challenges

The development of IoT applications or systems is a complex process which typically involves the following steps. In the first step, multifarious set of IoT devices, including sensors, smart meters, actuators are deployed for sensing, measuring, and controlling indoor and outdoor environments. Thereafter, different platforms are used to access the capabilities or operations of these infrastructures. Finally, the development and deployment of applications are carried out for managing or creating services for Smart City users and residents. Despite the growing number of IoT deployments in the Smart City, the majority of IoT applications tend to be self-contained, thereby forming application silos.

In majority of cases, the deployment of IoT infrastructures is carried out focusing a particular domain or application within the Smart City. So the whole city-wide IoT infrastructure consists of IoT devices from a diverse range of domains e.g. healthcare, transportation, mobility, environmental, waste, energy, etc. Majority of these devices do not only use different communication technologies but also different standards and architectures. Interoperability among IoT devices at the device level is still a key challenge.

Similarly, most of the existing IoT platforms for Smart Cities focus on support for vertical applications, without any support for cross-domain interoperability. This is for example the case with all cloud-based IoT platforms provided by major IT vendors. They provide scalability and quality of service, yet they lack features for semantic interoperability across IoT deployments. Similarly, community IoT platforms such as the FIWARE (https://www.fiware.org/tag/iot/) provide open APIs for deploying IoT applications in Smart Cities, yet they also lack semantic interoperability features. On the other hand, the open source OpenIoT platform provides mechanisms for semantic interoperability of diverse IoT data streams [5], yet it does not address the semantics of Smart City applications. During the last two years, there are also initiatives emphasizing on the semantic interoperability of diverse IoT deployments, such as the EU's H2020 Symbiote [6], InterIoT [7] and Big-IoT [8] projects. Nevertheless, these initiatives are not exclusively focused on Smart Cities, while their developments are still in their infancy.

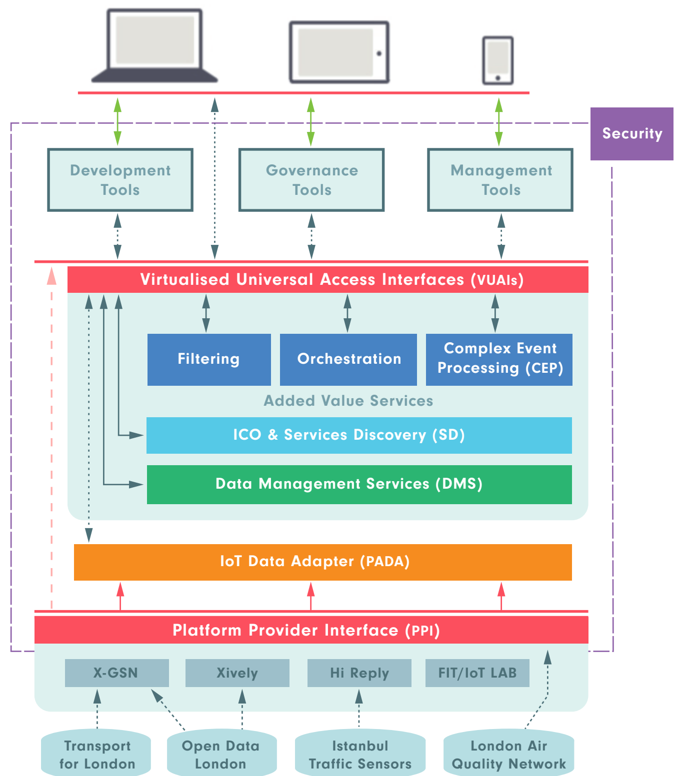

Fig. 1. High-level overview of VITAL-OS architecture.

Moreover, the vast majority of cities have deployed the various applications without a very well structured plan, which has resulted in further fragmentation of the data. This domain-specific fragmentation of IoT systems should be alleviated in order to allow cities to exchange information across independent systems and correlate operations across domains. This could enable a new wave of cross-context cross-vertical applications, which will provide added-value to citizens and new business opportunities for Smart City solution providers. Furthermore, the management and governance of diverse IoT infrastructure from a single point is a must. The governance of IoT resources must be designed in a way that allows the adoption of different legislations and constraints set by city authorities.

A. *VITAL-OS*

The VITAL-OS approach lays out an important step in overcoming the interoperability issues. The methodology has designed and implemented a novel paradigm for the virtualized integrated development and deployment of IoT applications for smart cities, notably applications that leverage data and services from multiple IoT systems (i.e. IoT platforms and applications). This paradigm is empowered by the VITAL-OS platform. Figure 1 provides an overview and illustrates the main building blocks of VITAL-OS architecture. Due to the complexity of the goal, and avoiding to reinvent the wheel, VITAL-OS architecture has taken into account the work performed in the scope of the FP7 IoT-A project and their IoT-A Reference Model (ARM).

The VITAL-OS platform in its nature is a service oriented distributed system that consists of various loosely coupled components. At the lowest layer of VITAL-OS architecture, various IoT systems (including IoT platforms and IoT applications, data sources) deployed in urban environments reside. These systems are virtualized and integrated as part of the VITAL-OS platform. The next layer is the Platform Provider Interfaces (PPI) that enables access to data and services of the underlying IoT systems in a secure and authenticated way. Its role is to access the low-level capabilities of the IoT systems and accordingly to transform the acquired data and metadata into VITAL-OS data model for storage. The IoT Data Adaptor keeps track of registered PPIs, pulls data from IoT systems and stores it into the VITAL-OS Data Management System (DMS). The DMS is a platform agnostic data management system that offers a wide range of services to higher level applications. VITAL-OS platform also provides various added value components such as Service Discovery component for discovering the IoT resources (e.g. data, sensors, systems, services, etc.), Filtering component to filter or reduce reducing the information associated with individual data streams persisted in the DMS, and Complex Event Processing (CEP) for processing of data streams stemmed from multiple sources in order to identify patterns and/or infer events. The Orchestrator is a Business Process Management (BPM) component that combines and manages multiple services in order to deliver new added-value services. Finally, the platform provides Smart City tools to allow the development of cross-platform and cross-context applications via the Development tools, and integrated management and governance of diverse IoT resources via the Management and Governance tools respectively. Further details on the VITAL-OS platform and its components can be found elsewhere [4].

B. VITAL-OS Deployment Roles

From a deployment perspective, the various components of the VITAL-OS architecture may be deployed and operated by different business roles and stakeholders of the VITAL-OS ecosystem. In particular, VITAL-OS considers the following roles:

- **End-Users**: Different types of end-users can access the VITAL-OS platform in different ways: A) Citizens and Businesses are likely to use operational-level applications that visualize data and information flowing through the VITAL-OS platform; B) City authorities are likely to use management and strategic level applications boosting their decision making. The latter are likely to be customized based on the projects Management and Governance tools.
- **VITAL-OS Smart City Services Providers**: Smart city services providers are likely to deploy and operate a cloud infrastructure, which shall be hosting the VITAL-OS platform. At the same time, service providers can provide the added-value functionalities of the platform (e.g., discovery, CEP) over this cloud infrastructure. Moreover, they can use the Management and Governance tools of VITAL-OS as a means of monitoring the IoT services that they offer to end-users. Note that VITAL-OS Smart City services providers establish SLAs (Service Level Agreements) with providers of legacy IoT platforms and/or providers of legacy IoT applications in order to use their data.
- **Smart City Solution Providers and Integrators**: Smart city solution integrators are likely to deploy and operate the VITAL-OS platform agnostic data management layer, as part of the implementation/integration of an integrated multi-platform IoT solution for smart cities. Furthermore, solution providers and integrators are the prominent users of the development tools of the project, as part of their effort to reduce the time and resources needed to develop VITAL-OS based applications.
- **Smart City IoT Platform and Applications Providers**: At the technical level, IoT platforms and applications providers are likely to implement a PPI over their platform/application in order to make it compliant to the VITAL-OS platform. At the business level, IoT platform and/or application providers need to establish SLAs with the providers of the VITAL-OS infrastructures and services.

The deployers, operators and administrators (e.g. city authorities) of IoT infrastructure can configure, manage and customize the installation of VITAL-OS platform as well as the integrated IoT resources. This functionality is enabled via the smart Governance and Management components. In VITAL-OS, the smart Governance and Management of diverse IoT deployments is achieved by providing 1) a common data model for IoT resources [9]; 2) the specification and implementation of techniques and best practices for accessing IoT resources, through diverse platforms, architectures and application silos; 3) the specification and implementation of interfaces (called Virtualized Unified Access Interfaces (VUAIs)) for accessing sensor data and functionalities in a virtualized way e.g. regardless of the underlying platforms or silo application to which the sensor/device belongs; and 4) consideration on the security, privacy, legal and business issues (including SLA issues) associated with access and integration of sensors and sensor data residing in multiple silos based on different disjoint architectures or platforms.

III. Smart Governance

VITAL-OS enables the integration and orchestration of IoT services and IoT data streams from heterogeneous IoT systems which must be monitored and governed from a single entry point. The need of a governance layer is common to all complex ICT systems, especially when the services offered are of a critical nature; however, IoT systems and their applications in the Smart City domain are not just complex systems that support critical functionality but they also provide processed data and reports that may affect large scale urban planning, policy making, regional or national-level strategic decisions or even legislation. For an IoT system like VITAL-OS, the smart governance layer must offer a number of services to users. It must allow system configuration to meet business requirements and SLAs of underlying IoT resources. It must allow designing and enforcing security policies (e.g. authorization and authentication) from a single entry point. Economize on the resources (and cost) associated with the system deployment, taking into account SLAs with platform providers. It must ensure that application developers and deployers engage with data and services falling in their scope of the smart city application that they are targeting.

A. Component Design

The Management and Governance toolkit in VITAL-OS comprises a set of powerful tools enabling Smart City authorities and services providers to manage and configure/customize the VITAL-OS platform as well as the integrated IoT systems. In Figure 2, high level requirements of the Governance toolkit are displayed in relation to different end-user types. The overall goal of the Governance toolkit is to enable VITAL-OS deployers (e.g. platform administrators and IoT system providers) with the capabilities to manage and configure the VITAL-OS installation as a whole. It provides the tools necessary for elevated users (e.g. municipality administrators) to control the flow of information between VITAL-OS systems and specific applications through high-level policies. Finally, it enforces these policies to applications so that these applications are exposed to the requested subsets of data and services with the desired Quality of Service (QoS) level.

Figure 3 illustrates the design of the Governance module within the VITAL-OS platform as well as its dependencies and interactions with other platform components. The Governance tool is associated with the security component to configure permissions of VITAL-OS modules for specific applications

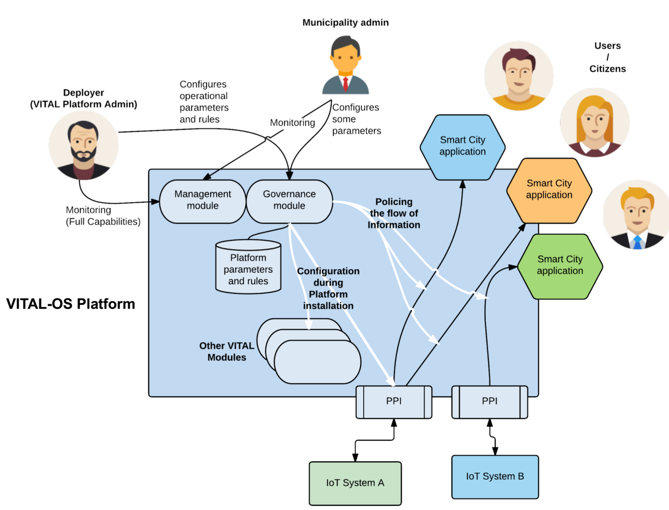

Fig. 2. A high-level overview of Governance Toolkit usage

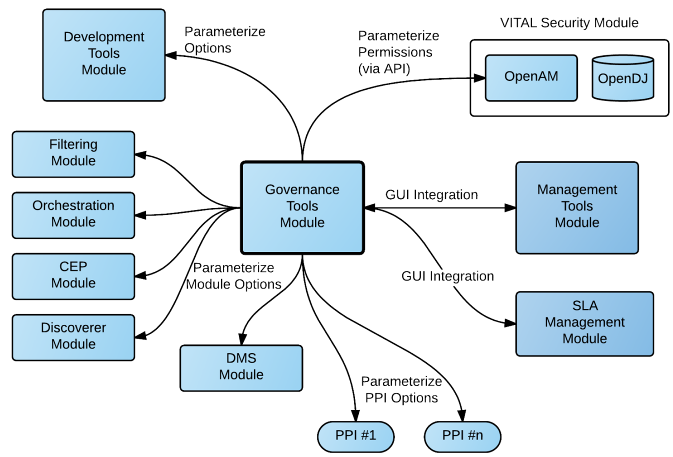

Fig. 3. Design of the Governance toolkit and its interaction with other VITAL-OS modules

(and users). For example, the platform administrator can allow a specific user to access the CEP module while others cannot. The Governance tool is integrated with Management tool [10] in order to allow users to access the Governance tool via the Management GUI (single entry point). Governance module interacts with other VITAL-OS modules e.g. Filtering, Orchestration, CEP, and Discovery for parameterizing their behaviour at the platform or the user level. Finally, the Governance module allows the definition of limitations to specific IoT systems and/or data sources (based on type, location or throughput) at the user level.

Definition of limitation at the platform level (i.e. affecting the operation of the current VITAL-OS platform installation as a whole) is communicated directly to the related PPIs and the IoT Data Adapter module, while limitations at the user level (i.e. limitations that affect a specific user) is communicated to the DMS component. For example, if we need to limit the current installation to sensor data from a specific geographical location, or limit communication to only temperature sensor data, then we need to inform the PPIs installed to retrieve and store only the required data (in DMS). A similar example is the case of limiting the overall throughput imposed to a specific underlying IoT system (for cost reasons); in this case the PPI handles the policing of the overall traffic caused by the underlying platform. On the other hand, when an administrator needs to limit a specific user to a geographical area, or types of sensors then the Governance tool will communicate this information to the Policy (security) module that interacts with the DMS component.

B. Implementation

The implementation of the first design requirement, e.g. add or remove an IoT system in VITAL-OS installation, is realized in a common way. Both IoT systems (PPIs) and internal platform modules share a common vocabulary (VITAL-OS data model) and their capabilities are exposed via a similar interface (VUAI). The Governance module includes a registration tool where an administrator may register new systems, unregister existing ones or simply disable/enable them. The second requirement is to filter the data flow to more specific subsets, enforced in an installation scale. To accomplish this requirement, the Governance module allows the VITAL-OS administrator to set data access boundaries for users based on specific locations and observation types. Location based boundaries limit the flow of information only to a specific geographical area while the observation type boundaries limit observations to specific types. Figure 4 depicts this functionality supported by the Governance module. The selection of a rectangular area on the map entails the capture of the coordinates of the vertices of the polygon. The latitude and longitude are used to update the policy. Data from sensors outside the configured area will not be retrieved from PPIs hence not accessible to specific applications/users. Similarly, the selection and de-selection of observations types is used to obtain the list of observation types for which the 'retrieve' action is allowed.

The Governance tool also supports application federation functionality to allow the runtime configuration of groups of VITAL-OS users in relation to their access to specific IoT systems. Figure 5 shows the access policies configuration UI. It displays 'Advanced_Users' group and options to allow/deny access to available IoT systems. For each system, the administrator can select if the users group is allowed to access it. When pressing 'save', the Governance module will translate this high level definition of 'Group X can access System Y' to low level policies where group ids are associated with specific URL and URIs. This functionality leverages upon endpoint-level policies, enforced by the policy agent. For each registered system there is a policy specifying which groups are allowed to access that system. It is automatically created when the system is registered and it is updated upon the submission of allow/deny configurations. Location based boundaries and observation types boundaries selected on the System Boundaries tab are translated in parameters of the global fine-grained policy applied at PPI level, to all authenticated users, or to a specific group.

IV. Use Cases and Results

The two main VITAL-OS use cases are developed after taking into account the needs of city authorities, citizens, and businesses with regard to available data sources, systems and services in London and Istanbul. The London use case, focused on smarter working, reflects changes in working practices and city networks. The smart traffic management use case, chosen for Istanbul, addresses an issue of key importance in that city. In addition, data sources from other cities are also integrated into the VITAL-OS platform. The PPI implementation for each of the listed IoT system is a Java web application that is deployed in Wildfly application server. VITAL-OS provides PPI implementations for the following four platforms:

- **X-GSN**[1]: X-GSN (eXtended Global Sensor Networks) constitutes an enhanced version of the GSN platform that has been developed as part of the OpenIoT project.
- **Xively**[2]: Xively is a well-known IoT Platform as a Service (PaaS) that enables its users to store their data, query them, and even receive notifications when certain conditions are met.
- **FIT/IoT-Lab**[3]: FIT IoT-LAB is a platform that provides a very large scale infrastructure facility suitable for testing small wireless sensor devices and various communicating objects.

[1]https://github.com/OpenIotOrg/openiot/wiki/X-GSN
[2]https://xively.com
[3]https://www.iot-lab.info

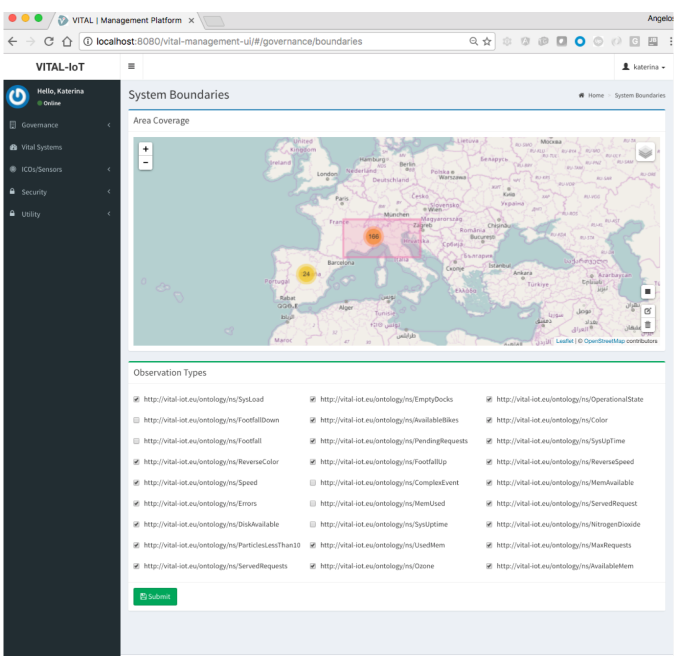

Fig. 4. Defining data boundaries based on location and observation types.

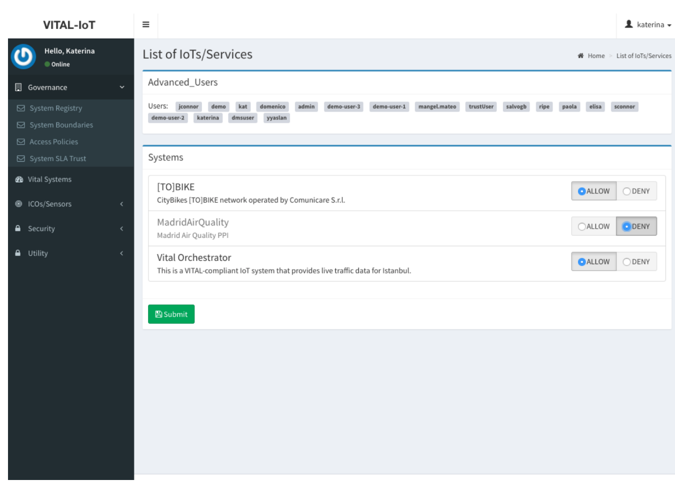

Fig. 5. IoT system access policies based on user group

- **HI Reply**[4]: HI Reply is an IoT platform created by Reply, which incorporates services, devices and middleware for the Internet of Things. HI Reply allows the creation of an ecosystem of objects that are connected.

These integrated IoT systems provide the means for integrating IoT data streams and services to the VITAL-OS platform. In addition to the integration of these platforms, VITAL-OS has implemented PPIs for various open/closed data sources. The Governance tool is the main integration point of all integrated systems and services in the VITAL-OS. While a performance evaluation is not applicable, the Governance tool is evaluated in terms of its transparent interaction with all diverse systems that are integrated in VITAL-OS. It is demonstrated in terms of monitoring and governing the following IoT systems (see Figure 6):

- **HI Reply PPI**: The PPI providing data exposed by Hi Reply, which in turns collects data from the sensors deployed in the city of Istanbul by the Istanbul Metropolitan Municipality (IMM). These include, Remote Traffic Microwave Sensors (RTMS), Bluetooth Sensors, TERRA Detectors, Wireless Magnetic Sensors, Loop Detectors, Electronic Violation Detection Systems (EVDS), and Weather Observation Stations, etc.
- **Camden Footfall PPI**: A PPI implementation that connects to VITAL-OS a footfall data feed (provided by Springboard UK) collected in an hourly basis by small counting devices installed in several locations across Camden town - London.
- **London Bike PPI**: Transport for London (TfL) provides information about bike docking stations in London. This PPI implementation maps docking stations to sensors that measure docks, empty docks, and available bikes.
- **London Air Quality PPI**: Kings College data feed for London Air Quality is connected to VITAL-OS through this PPI. It maps monitoring sites to sensors that observe the level of NO2 in the air.
- **Galway Weather PPI**: This is a VITAL-OS compliant IoT system that provides environmental data from NETATMO sensors, deployed in Insight-Centre NUI Galway.
- **Galway Smart Building PPI**: The smart building system uses a number of wireless sensors based on the TelosB platform. These devices are low-power tiny devices programmed in TinyOS. Over 50 sensors report data about different parameters within the Insight Centre building in NUI Galway.
- **Madrid Air Quality PPI**: PPI for the integrating the air quality data coming from the network of air quality stations distributed throughout the city of Madrid. The information provides data about Nitrogen Dioxide, Ozone and Suspended Dust Particles Smaller than 10 microns.
- **CityBikes PPIs**: A set of three IoT Systems and a wrapper one that connect the CityBikes service in different locations to VITAL-OS.
- **Raspberry PPI**: The system is based on 2 different entities, a gateway and a sensor network which senses the physical environment. The gateway represents the adapter between the VITAL-OS and the SN; it allows IoT Data Adapter to access data produced by the underlying SN and, at the same time, it acts as a sink for the sensors.
- **Arduino PPI**: An IoT system based on an Arduino platform. The implementation is provided as a proof-of-concept to demonstrate the viability of running a lightweight PPI on Arduino which provides temperature and humidity data in the REPLY building, Italy.

Furthermore, to evaluate the VITAL-OS platform from users' perspective, 7 stakeholders' workshops have been organized across different cities (London, Istabul, Athens, Turin, Galway, Madrid, and Lille) in Europe. A total of 145 participants (IoT researchers, IoT developers, and city authorities) took part in these workshops. The Management and Governance tool's evaluation has been conducted by providing stakeholders with questionnaires in order to gather feedback on the usability of the tool, the functionalities available, and the options provided for controlling/governing the underlying IoT systems and data sources. Two different questionnaires were administered, one for city authorities and another for technical experts and solution providers. The questionnaires also included questions about the overall assessment and added-value of the VITAL-OS platform with an outlook on whether it could be useful for the participants.

Majority of the participants (both the IoT developers and the city authorities) indicated a positive opinion in terms of VITAL-OS's ability to facilitate IoT platforms integration, to improve the cost-efficiency of smart city deployments, and overall to improve the functionalities offered by Smart City platforms. Figure 7 highlights the feedback provided by city authorities. Another remark is that the majority of end-users (i.e. 45%) perceived the VITAL-OS as a unified system and

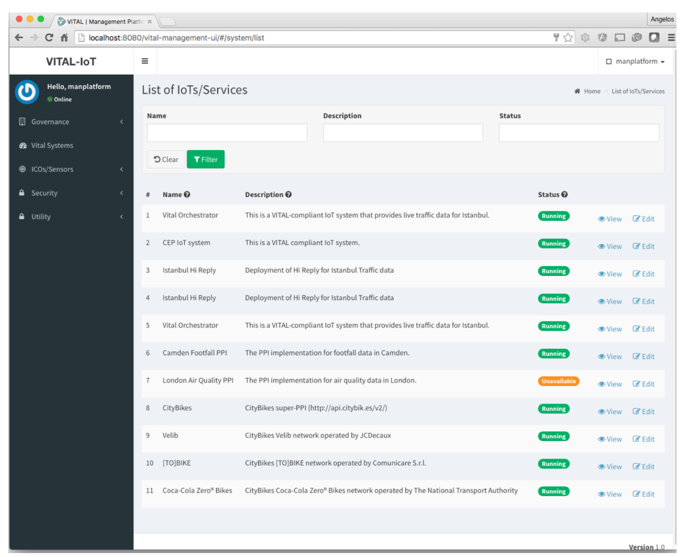

Fig. 6. List of VITAL-OS integrated IoT systems.

[4]https://www.reply.com/en/content/hi-reply

expressed interest in the platform as a whole rather than in individual components. A significant percentage of 22% declared interest in the core middleware and Management and Governance tools of the platform. The questionnaire for IoT solution providers and integrators was different to the questionnaires for the city authorities. The majority of the participants (e.g. IoT developers/integrators) classified the innovation of the VITAL-OS platform as 'good' (53%), a 37% characterized it as 'very good', while a 10% gave the characterization 'acceptable'. Figure 8 highlights the feedback provided by developers and integrators.

V. Conclusion

In this paper, we have presented the VITAL-OS Governance environment for Smart Cities. The smart Governance environment alleviates the challenges that are associated with the governance and management of wide range of heterogeneous IoT systems deployed in Smart Cities. The goal of the module is to provide a range of configuration functionalities, which enable the customization of each VITAL-OS deployment for use within a smart city or region. As a general rule the governance functionalities enforce restrictions on the data and services that can be accessed by specific users, taking into account the users' privileges, the characteristics of the Smart City where the deployment will take place, as well as SLAs with IoT platform and services providers. The goal of these restrictions is to economize on the required resources and costs, but also to ensure stakeholders' control over the smart city operations that can be performed by developers. The Governance tool is evaluated in terms of its monitoring and configuration functionalities to govern diverse IoT systems that are integrated in VITAL-OS. As part of the stakeholders' workshops, the VITAL-OS platform has collected positive feedback regarding the innovation of the platform, the utility of its main functionalities, and the potential of integrating and utilizing the VITAL-OS in the scope of existing Smart City platforms. The discussions during the workshops also raised few technical limitations of VITAL-OS that will be addressed in the future work.

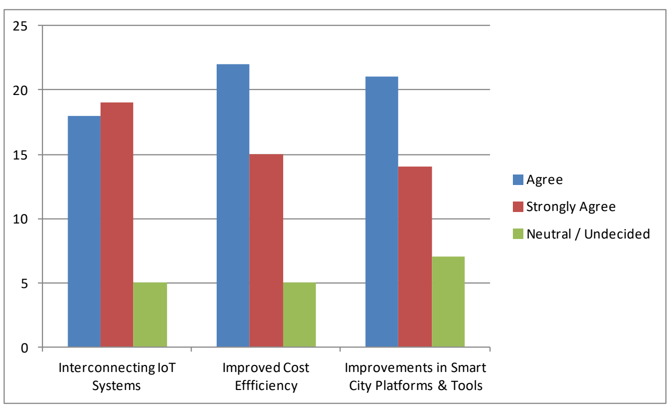

Fig. 7. Opinion of city authorities on VITAL-OS platform.

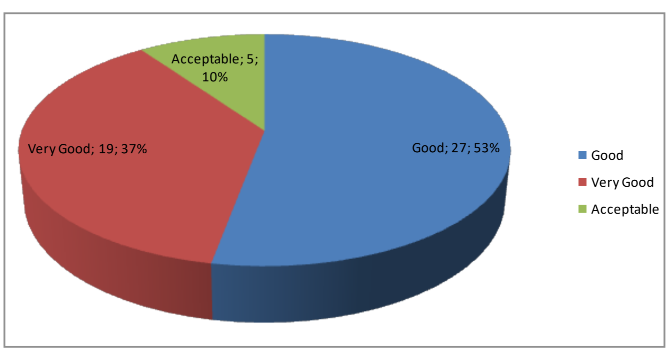

Fig. 8. Opinion of IoT developers and integrators on VITAL-OS platform.

Acknowledgment

The authors acknowledge support from the ICT-2013.1.14 - VITAL-OS project, which is co-funded by the European Commission under the Seventh Framework Program (FP7), grant agreement number 608682. The authors also acknowledge help and contributions from all partners of the VITAL-OS consortium.

References

[1] A. H. Kazmi, M. J. O'Grady, and G. M. P. O'Hare, "Energy management in the smart home," in *Proceedings of the 2013 IEEE 10th International Conference on Ubiquitous Intelligence & Computing and 2013 IEEE 10th International Conference on Autonomic & Trusted Computing*, ser. UIC-ATC '13. Washington, DC, USA: IEEE Computer Society, 2013, pp. 480–486.

[2] J. Soldatos, *The Building Blocks of IoT Analytics: Internet-of-Things Analytics*. River Publishers, 2017.

[3] J. Jin, J. Gubbi, S. Marusic, and M. Palaniswami, "An information framework for creating a smart city through internet of things," *IEEE Internet of Things Journal*, vol. 1, no. 2, pp. 112–121, April 2014.

[4] A. Kazmi, M. Serrano, and J. Soldatos, "Vital-os: An open source iot operating system for smart cities," *IEEE Communications Standards Magazine*, vol. 2, no. 2, pp. 71–77, JUNE 2018.

[5] M. Serrano, N. Kefalakis, J. Soldatos, and M. Hauswirth, *OpenIoT: An Open Source Platform for Enabling Intelligence to the Internet of Things*, 2014.

[6] H. Reinhard, M. Jacoby, and I. P. arko, "Semantic interoperability in iot-based automation infrastructures," *Special Issue: Industrial Internet of Things supporting Factory Automation*, vol. 64, no. 9, pp. 742–749, 2016.

[7] M. Ganzha, M. Paprzycki, W. Pawlowski, P. Szmeja, and K. Wasielewska, "Semantic technologies for the iot - an inter-iot perspective," in *2016 IEEE First International Conference on Internet-of-Things Design and Implementation (IoTDI)*, April 2016, pp. 271–276.

[8] A. Brring, S. Schmid, C. K. Schindhelm, A. Khelil, S. Kbisch, D. Kramer, D. L. Phuoc, J. Mitic, D. Anicic, and E. Teniente, "Enabling iot ecosystems through platform interoperability," *IEEE Software*, vol. 34, no. 1, pp. 54–61, Jan 2017.

[9] A. Kazmi, Z. Jan, A. Zappa, and M. Serrano, "Overcoming the heterogeneity in the internet of things for smart cities," in *Interoperability and Open-Source Solutions for the Internet of Things: Second International Workshop, InterOSS-IoT 2016, Held in Conjunction with IoT 2016, Stuttgart, Germany*, vol. 10218. Springer International Publishing, 2017, pp. 20–35.

[10] A. Kazmi, M. Serrano, A. Lenis, and J. Soldatos, "A qos-aware integrated management of iot deployments in smart cities," in *2017 IEEE 10th Conference on Service-Oriented Computing and Applications (SOCA)*, Nov 2017, pp. 141–146.