RECyT
Year 24 / Nº 38 / 2022 / 20–27
DOI: https://doi.org/10.36995/j.recyt.2022.38.003

An IoT architecture for smart cities based on the Fiware platform

Una arquitectura IoT para ciudades inteligentes basada en la plataforma Fiware

Dalia M. Berbes Villalón[1, *], Laura Sánchez Jiménez[1], Manuel de la Iglesia Campos[1], María E. Díaz Aguirre[1], Tatiana Delgado Fernández[1, 2]

1- Universidad Tecnológica de La Habana "José Antonio Echeverría". Cuba; 2- Unión de Informáticos de Cuba. Cuba.
* E-mail: dmberbes@gmail.com

Received: 20/08/2021; Accepted: 20/01/2022

Abstract

The Internet of Things (IoT) is a concept that has been gaining considerable popularity today. It attempts to represent everyday things that are connected to the internet, but in reality it is much more than that. The overall aim is to interconnect the physical with the digital world, as the physical world is measured by sensors which translates into actionable data, and also the data can be translated into commands to be executed by actuators.
Currently, the number of designed IoT architectures has increased considerably as a result of different approaches, standards and use cases. This leads to difficulties in understanding, selecting and using these architectures. In this work, an IoT architecture based on the FIWARE platform is proposed with the aim of facilitating the development of smart cities. With the proposal made, it was possible to integrate the main elements to be considered in this technology, thus offering a basis that serves as a guide, both for developing IoT systems and for creating more specific architectures that respond to the particular characteristics of a given application.

Keywords: IoT architecture, FIWARE, Internet of things, IoT.

Resumen

Internet de las Cosas (IoT) es un concepto que ha estado ganando considerable popularidad en la actualidad. Intenta representar cosas cotidianas que se conectan a Internet, pero en realidad se trata de mucho más que eso. El objetivo general es interconectar lo físico con el mundo digital, dado que, el mundo físico se mide con sensores lo cual se traduce en datos procesables, y también los datos pueden traducirse en comandos para ser ejecutados por actuadores.
En la actualidad, el número de arquitecturas IoT diseñadas ha aumentado considerablemente como resultado de diferentes enfoques, estándares y casos de uso. Esto lleva a dificultades para comprender, seleccionar y usar estas arquitecturas. En este trabajo se propone una arquitectura IoT basada en la plataforma FIWARE con el objetivo de facilitar el desarrollo de ciudades inteligentes. Con la propuesta realizada se logró integrar los principales elementos a tener en cuenta en esta tecnología ofreciendo así una base que sirve de guía, tanto para desarrollar sistemas IoT, como para realizar arquitecturas más específicas que respondan a características particulares de determinada aplicación.

Palabras clave: Arquitectura IoT, FIWARE, Internet de las cosas, IoT.

Introduction

For about 30 years, the idea of making everyday objects a little more interactive, such as the smart home, also known as the house of tomorrow, has been in the works (Guth et al., 2018).

The Internet of Things (IoT) empowers objects that were formerly connected through closed loops, such as communicators, cameras, sensors, and so on, and allows them to communicate globally through the use of the network of networks. The IoT vision describes a future in which many of the objects are interconnected through a global network. They collect and share data about themselves and their environment to enable monitoring, analysis, optimisation and control. Until recently this was merely a vision, but in recent times, it has slowly become a reality (Firouzi, Farahani, Weinberger, DePace, & Aliee, 2020).

Through the Internet of Things, objects recognise themselves and obtain intelligent behaviour by making related decisions about the information they can

communicate about themselves (Zeinab & Elmustafa, 2017). In this way, smart objects that intervene within an IoT architecture, or IoT system, can produce contextual information in large quantities, which is why the use of specialised platforms with standards and protocols for handling and processing this information on a large scale is currently required, with the aim of creating and deploying smart and manageable IoT applications (Miorandi, Sicari, De Pellegrini, & Chlamtac, 2012).

IoT architectures have been widely addressed in the literature. There is a group of architectures based on physical gateways, for example, in (Hernández, Calderón, & Fernández, 2021) where an IoT M2M (machine to machine) architecture for real-time environmental monitoring is addressed, while others are based on layers that include middleware for data processing (Ochoa Duarte, Cangrejo Aljure, & Delgado, 2018; Sobin, 2020).

Given the large number of aspects related to IoT, it is necessary to find a way to integrate those that are most important to ensure the proper functioning of any IoT solution.

In the search for such integration, several IoT architectures were analysed. As part of the framework of the project "Experimentation of smart cities in Old Havana", the evaluation of some of these IoT architectures was carried out, considering the fulfilment of certain requirements, the most important of them being OpenSource and free.

The main objective of this work is to propose an IoT architecture that allows the development of smart cities taking into account the aforementioned requirements. The proposal aims to integrate the main elements to be taken into account in this technology, as well as to manage the interaction between producers and consumers of context within the framework of the Internet of Things, both to develop IoT systems and to create more specific architectures that respond to the particular characteristics of a given application.

Materials and Methods

The following methodology was used to propose the IoT architecture:

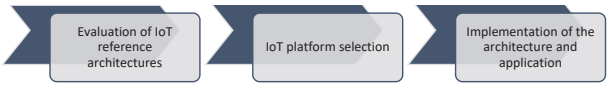


Figure 1: Methodology for proposing the IoT architecture.

Figure 1 shows the methodology for proposing the IoT architecture.

To evaluate the architectures, a Google Scholar literature search of secondary sources (reviews and surveys) was performed in order to more quickly evaluate the regularities of IoT architectures. Other references used in previous studies were also incorporated.

The selection of the IoT platform was conditioned by a previous study to select a platform that could access heterogeneous devices such as sensors, actuators and RFID tags and provide their data to the application layer.

As a result of these two stages, the implementation of the IoT architecture and application for smart cities is carried out including two aspects related to data modelling and platform performance evaluation.

Theoretical framework

IoT architecture

There is currently no single universally adopted definition for IoT architecture. Different proposals have emerged during its development among which we can find: the 3-layer architecture, the 5-layer architecture, the cloud architecture, the fog architecture and the edge computing architecture among many others. Despite the large number of proposed solutions it is possible to generate a general framework to understand the main layers that make up IoT (Hou et al., 2016; Vélez, 2019; Wu, Lu, Ling, Sun, & Du, 2010).

Figure 2 shows the ITU (International Telecommunication Union) reference model for an IoT architecture (ITU, 2012), where:

- The application layer: is responsible for delivering specific services and applications to the end user. This layer can be understood as the convergence between IoT and industrial and intellectual needs, defining specific applications such as smart homes, smart cities, smart transportation, among many others.
- The service and application support layer: The service and application support layer consists of the following two groups of capabilities:
  - Generic support capabilities: these are common capabilities that can be used in different IoT applications, such as data processing or data storage. These capabilities can also be used by other specific capabilities to, for example, create other specific capabilities.
  - Specific support capabilities: These are capabilities to address the particular needs of different applications. In reality, they can consist of several groups of precise capabilities that provide different functions to support different IoT applications.
- The network layer: This is the core layer of IoT. Its main function is to transmit and process the information obtained by the sensing layer. This layer is also responsible for interconnecting other networks of smart devices, network elements and servers.
- The device layer: This is the sensory layer of IoT where "the things" identify their surroundings, collect

information from the physical world and interact with it. This layer is composed of cameras, GPS, sensors, terminals, RFID tags and actuators which convert all the information into electrical signals which are easier to transmit for further analysis.

- The security layer: It is responsible for providing a higher level of security to the solution. Orion does not provide native authentication or any authorisation mechanism to enforce access control. However, authentication/authorisation can be achieved with the access control framework provided by FIWARE GE (FIWARE-Foundation, 2021b). More specifically, secure access to components in the architecture of any FIWARE-based solution can be implemented using the generic enablers (FIWARE-Foundation, 2021a):
  - Keyrock Identity Management Generic Enabler: provides support for OAuth2-based secure and private user and device authentication, user profile management, privacy-preserving personal data disposition, single sign-on (SSO), and identity federation across multiple management domains.
  - Wilma's generic proxy enabler provides support for proxy functions within OAuth2-based authentication schemes. It also implements PEP functions within an XACML-based access control scheme.
  - AuthZForce PDP / PAP Generic Enabler provides support for PDP / PAP functions within an access control scheme based on the XACML standard.

Within the IoT ecosystem, IoT platforms are considered the most critical component. Any IoT device must connect to other IoT devices and applications to transfer information using standard internet protocols. The gap between device sensors and data networks is bridged by IoT platforms. These platforms connect the data generated by the myriad sensors and provide information using applications to make sense of the vast amount of data generated.

In any smart solution there is a need to collect, manage and process contextual information to inform external actors, enabling them to act and thus alter or enrich the current context.

A complete solution for Internet of Things applications requires different software, hardware and communication technologies working in an integrated way. A view of the system architecture will give an insight into the correlation of functions between hardware and software components.

Different architectures for the Internet of Things have been proposed by different researchers. The three-layer architecture defines the main idea of the Internet of Things.

1. The transport layer transfers the sensor data from the sensing layer to the processing layer and vice versa through networks such as: wireless, 3G, LAN, Bluetooth, RFID and NFC.
2. The processing layer is also known as the middleware layer. It stores, analyses and processes large amounts of data coming from the transport layer. It can manage and provide a diverse set of services to the lower layers. It employs many technologies such as databases, cloud computing and Big Data processing modules.
3. The enterprise layer manages the entire IoT system, including applications, business and revenue models, and user privacy.

Another representation would be using a 4-layer architecture (Sikder, Petracca, Aksu, Jaeger, & Uluagac, 2018). In this there is a further level of detail where the data transport protocol is represented as an additional layer.

1. Detection layer: The main objective of sensing layer is to identify any phenomena in the peripheral of the devices and obtain data.
2. Network layer: The network layer acts as a communication channel to transfer data, collected in the

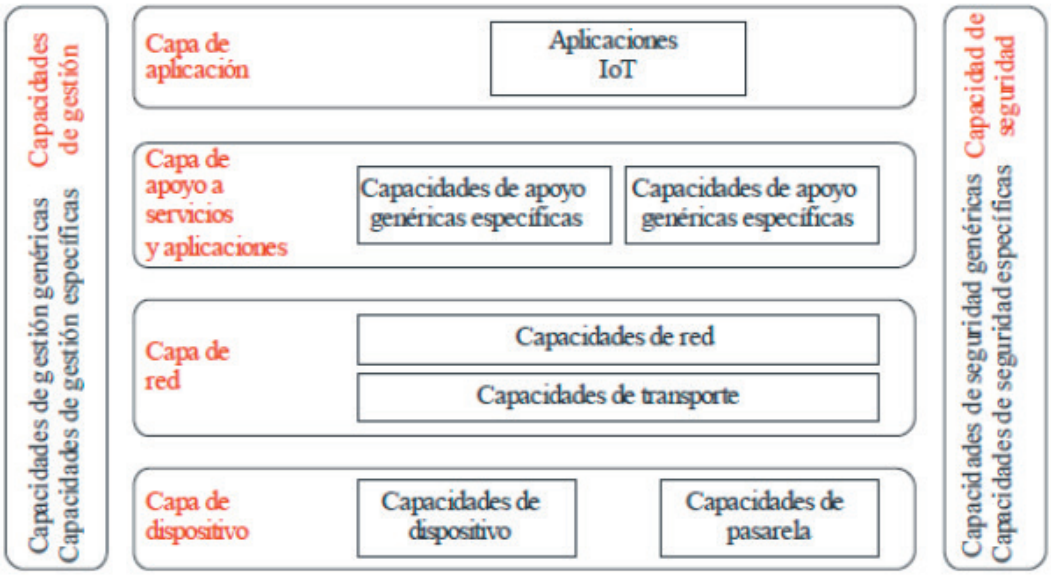


Figure 2: ITU IoT reference model (ITU, 2012).

sensing layer, to other connected devices. The network layer is implemented using various communication technologies (e.g. Wi-Fi, Bluetooth, Zigbee, Z-Wave, LoRa, cellular network, etc.).

3. Data processing layer: The data processing layer consists of the main data processing unit of the Internet of Things devices. It takes the data collected in the sensing layer and analyses it to make decisions based on the result. This layer can share the result of data processing with other connected devices through the network layer.

4. Application layer: The application layer implements and presents the results of the data processing layer. The application layer is a user-centric layer that executes various tasks for users.

Other authors have approached IoT architectures from this layered perspective, for example, in Figure 3, a three- to five-layer architecture is shown (Sobin, 2020).

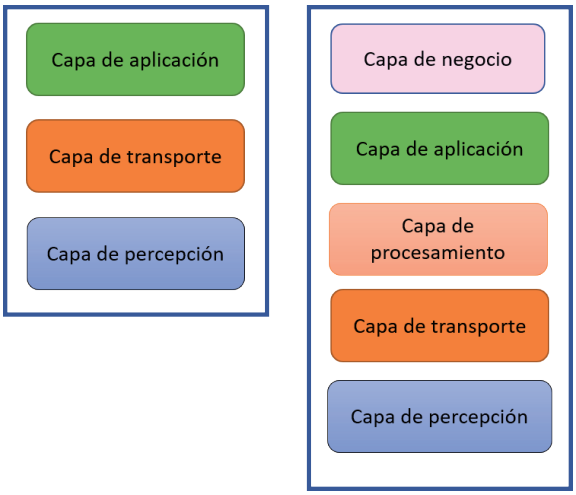


Figure 3: Three- and five-layer IoT architecture. Source: adapted from (Sobin, 2020).

In the sensing layer, the Internet of Things is implemented with different types of sensors: RFID, temperature sensor, proximity sensor, etc. Each sensor is a source of information that captures content. The transport layer integrates various wireless and wired networks for a transmission of the information that is regularly collected from the sensor nodes. Another layer is the application layer that collects, processes and analyses the necessary data. While the business or enterprise layer and the processing layer have the same functions as described for such layers in the reference architectures presented above.

IoT platforms

IoT platforms are considered the most critical component of the IoT ecosystem. The gap between device sensors and data networks is bridged by IoT platforms. These connect sensor-generated data and provide information using IoT applications to make sense of the vast amount of data generated by the myriad sensors (Moura, Ceotto, Gonzalez, & Toledo, 2018). Achieving interoperability between different IoT systems is an important requirement, in order to make everything truly interconnected. Management is essential due to the number of elements involved in any IoT implementation.

IoT platforms facilitate connectivity between IoT systems. These platforms facilitate communication, data flow, device management and application functionality.

The proposed architecture for the development of an innovative smart city prototype, which demonstrates the feasibility of using the FIWARE platform architecture, makes use of the FIWARE platform components to design and implement smart applications that interact with an information capture layer in a context.

The main components of FIWARE are shown below in Figure 4.

Figure 4: Basic components of the FIWARE IoT platform.

The selection of FIWARE was conditioned by a previous study carried out by the team to select an IoT platform that would allow accessing heterogeneous devices such as sensors, actuators and RFID tags and supplying their data to the application layer, considering the following requirements:

- To be OpenSource and free.
- Not relying on global public clouds; allowing the use of private clouds and/or fog nodes.
- Highly scalable, contemplating the use of containers.
- Enable semantic interoperability.
- Easy to use by developers.
- Feasible for smart cities and industrial environments.

Results and discussion

In order to instantiate this architecture in a specific case, an application was designed and implemented to monitor temperature and relative humidity values over time within an institution. Based on the proposed architectures studied, the proposal for the prototype is a 3-layer architecture. Figure 5 shows a representation of the proposed architecture.

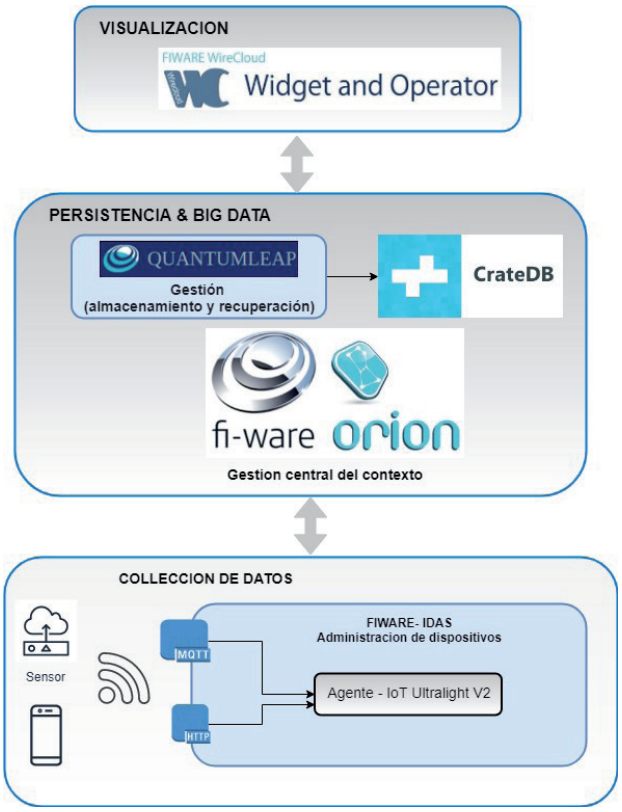


Figure 5: IoT solution architecture based on FIWARE.

The main components of the proposed architecture are explained below:

1. Data collection: The sensors located in the data capture layer allow consuming and generating new data sets updated in real time, the IoT agent allows unifying the data captured through different communication protocols and sending them to the context manager.
2. Persistence and Big Data: The persistence layer is responsible for persisting measurements and generating a history using notifications that alert on new changes that need to be stored.
3. Visualisation: Finally, the visualisation layer allows the analysis of the data, generating new information that will be used in decision making.

The diagram in figure 6 shows the flow of the captured data. The FIWARE air quality model AirqualityObserved, adapted to the needs of the experiment, is chosen as the data model. A set of entities with the Air Quality data model and Device model are created in Orion Context Broker. This in turn notifies the FIWARE QuantumLeap service, which interprets the data model and transforms it into records in the CrateDB database (Crate.io., 2021). For visualisation and decision making, it is proposed to use an application that acts as a Mashup; for example, platforms such as WireCloud (CoNWeT-Lab-(UPM), 2013) or Microsoft Power Bi (Microsoft, 2021) can be used.

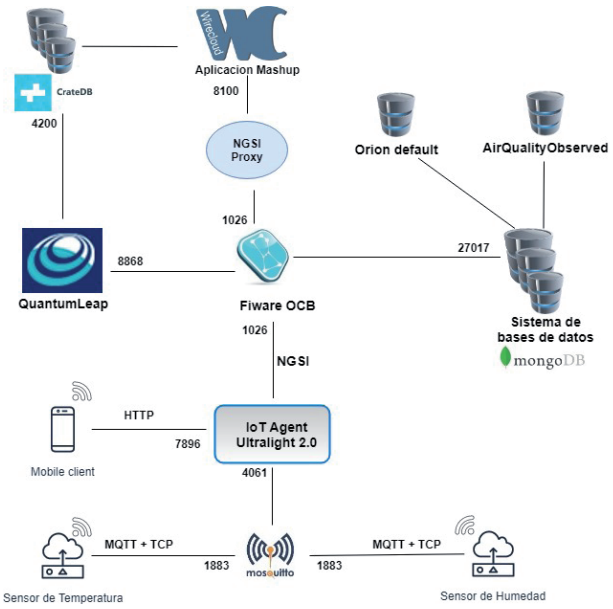


Figure 6: Data flow based on the proposed IoT architecture.

For the implementation of this prototype, a simulation of temperature and relative humidity sensors was used to measure the climatic conditions that influence the observed air quality. For the geolocation of the devices, the coordinates of a coordinate sensor sent from a mobile application are obtained.

The components of the IoT prototype are:

- Hardware: There are three sensors. The temperature and humidity sensors, to acquire data from the environment, communicate via the MQTT protocol, and the GPS sensor sends the coordinate data via the HTTP protocol.
- Software: The FIWARE platform and a set of generic enablers (Generic Enablers) are installed, which will allow the correct operation of the entire system, from the capture of environmental data to their visualisation and analysis. The IoT Ultralight agent is the Generic Enabler to establish communication between the sensors and the platform; this agent allows both communication from the devices to the platform sending measurements (Northbound Traffic), and communication from the platform to the actuator devices that receive a command and change their state (Southbound Traffic). For this solution, only Northbound Traffic communication is implemented. This agent has the ability to recognise two communication protocols: HTTP and MQTT. The Ultralight IoT agent will receive, through the HTTP protocol, the coordinates sent by a mobile application, captured by the GPS sensor of a mobile phone. For communication via MQTT, another software component, a mediator, Mosquitto MQTT-Broker or RabbitMQ, is required. Mosquitto is used in the implementation of the solution, as there is better documentation and examples with the FIWARE platform. For the interception of new readings and

historical storage of captured values, QuantomLeap is used with CrateDB, a distributed SQL database that simplifies the storage and analysis of large amounts of machine data in real time.

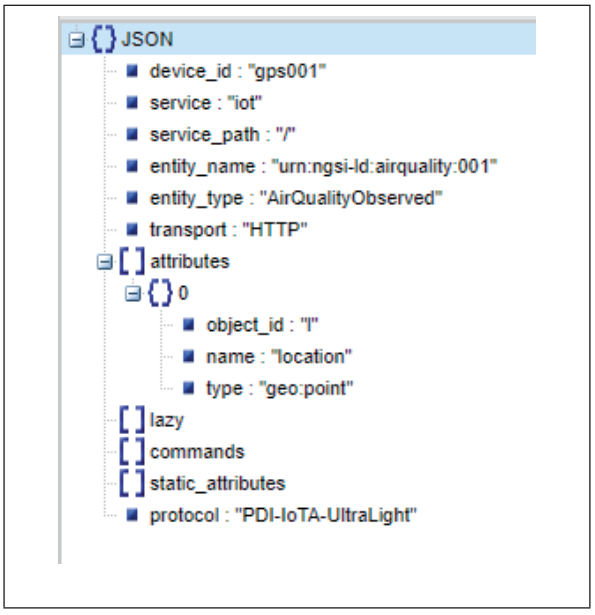
- User interface: Using a web interface of a business intelligence platform (Power BI + Bing) the collected data is displayed on a map.

The data models that are adapted to the prototype are: Devices and Environment.

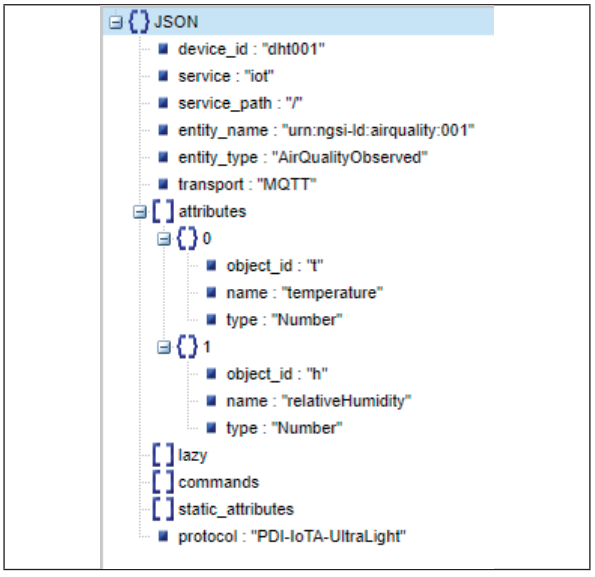
Data Model: Devices

This data model allows representing devices of different nature (IoT, mobiles, laptops, etc.).

Figure 7 A shows the entity that represents the device that measures geo-location, and figure 7 B shows an entity that represents the device that measures temperature and relative humidity levels.



A



B

Figure 7: Entities representing devices.

Data model: Environment

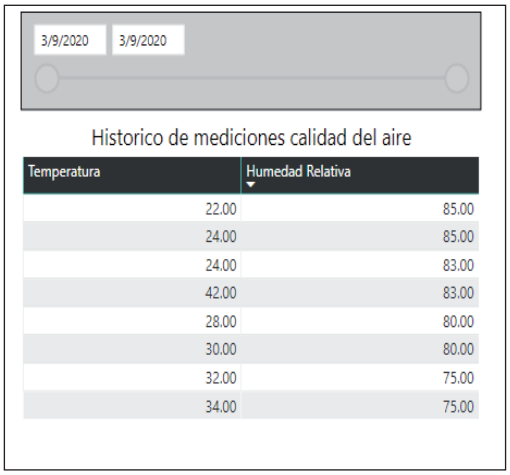
These data models describe the main entities involved with intelligent applications dealing with environmental problems. The main entities identified are:

- AeroAllergenObserved
- AirQualityObserved
- WaterQualityObserved
- NoiseLevelObserved

Because the sensors to be used measure temperature and humidity, the data model that approximates the prototype is AirQualityObserved, as certain climatic conditions have an influence on the observed air quality. It is modelled through a set of weather-related properties already defined by WeatherObserved.

Visualisation of the prototype result

Figure 8 shows an example application with the prototype developed with the IoT architecture for measuring air quality. The Bing platform was used for the presentation on the map of the measurement evaluated at the Technological University of Havana. It is complemented with a table listing the measurements taken, a filter component to determine a time period and a graph to show the behaviour over time of temperatures and relative humidity.



Temperatura	Humedad Relativa
22.00	85.00
24.00	85.00
24.00	83.00
42.00	83.00
28.00	80.00
30.00	80.00
32.00	75.00
34.00	75.00

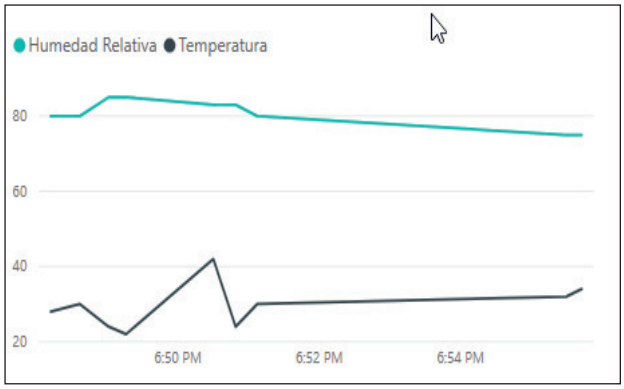


Figure 8: Example of application of the IoT architecture with the air quality prototype.

Each point of interest (in the case of the example, the Technological University of Havana "José Antonio Echevarría") is represented on the map using the captured coordinates and as part of its information, the current temperature and humidity data are shown. The historical values are stored in a database, which facilitates the analysis of the behaviour of the observed variables for each point of interest.

Conclusions

The IoT architecture proposed in this article reaffirms FIWARE as a platform that allows the development of intelligent applications for different application contexts. Its modularity facilitates its adaptation and reuse, both at the architecture level for different IoT applications, as well as for a specific implementation.

The deployment of components and modules independently shows the low coupling of the modules between layers, which allows implementing the functionalities of one of them, without the need to deploy all the remaining layers.

The proposed architecture makes it possible to link general purpose components of the FIWARE platform with layers designed with web services and with layers to obtain context information through sensors.

The results obtained from this prototype demonstrate the viability of the proposed IoT architecture, which serves as a basis for the generation of an API that will be released by the research group in the next stages.

Acknowledgements

This research was supported by the Project "Experimentation of smart cities in Old Havana" (2018-2020), of the National Programme of Science, Technology and Innovation for the Informatisation of Society in Cuba.

References

1. **CoNWeT-Lab-(UPM). (2013).** *Welcome to the next-generation application mashup platform aimed at leveraging the long tail of the Internet of Services*. Retrieved from http://conwet.fi.upm.es/wirecloud/
2. **Crate.io. (2021).** *The Scalable SQL Database for Machine Data*. Retrieved from https://crate.io/
3. **Firouzi, F., Farahani, B., Weinberger, M., DePace, G., & Aliee, F. S. (2020).** *Iot fundamentals: Definitions, architectures, challenges, and promises*. In Intelligent Internet of Things (pp. 3-50): Springer.
4. **FIWARE-Foundation. (2021a).** *FIWARE COMPONENTS*. Retrieved from fiware.org/developers/catalogue/
5. **FIWARE-Foundation. (2021b).** *FIWARE: The Open Source Platform for Our Smart Digital Future*. Retrieved from https://www.fiware.org/
6. **Guth, J., Breitenbücher, U., Falkenthal, M., Fremantle, P., Kopp, O., Leymann, F., & Reinfurt, L. (2018).** *A detailed analysis of IoT platform architectures: concepts, similarities, and differences*. In Internet of everything (pp. 81-101): Springer.
7. **Hernández, E. C., Calderón, C. A., & Fernández, T. D. (2021).** *Arquitectura M2M para el monitoreo ambiental en tiempo real.* ITECKNE: Innovación e Investigación en Ingeniería, 18(1), 2-2. Retrieved from https://dialnet.unirioja.es/servlet/articulo?codigo=7966033 issn: 2339-3483.
8. **Hou, L., Zhao, S., Xiong, X., Zheng, K., Chatzimisios, P., Hossain, M. S., & Xiang, W. (2016).** *Internet of things cloud: Architecture and implementation*. IEEE Communications Magazine, 54(12), 32-39. doi:10.1109/MCOM.2016.1600398CM, issn: 0163-6804.
9. **Microsoft. (2021).** *Pase de los datos al conocimiento y la acción con Power BI Desktop*. Retrieved from https://powerbi.microsoft.com/es-es/desktop/
10. **Miorandi, D., Sicari, S., De Pellegrini, F., & Chlamtac, I. (2012).** *Internet of things: Vision, applications and research challenges.* Ad hoc networks, 10(7), 1497-1516. doi:https://doi.org/10.1016/j.adhoc.2012.02.016, issn: 1570-8705.
11. **Moura, R., Ceotto, L., Gonzalez, A., & Toledo, R. (2018).** *Industrial Internet of Things (IIoT) platforms-an evaluation model*. Paper presented at the 2018 International Conference on Computational Science and Computational Intelligence (CSCI). Publisher: IEEE. DOI:10.1109/CSCI46756.2018.00194. Retrieved from: https://ieeexplore.ieee.org/abstract/document/8947823
12. **Ochoa Duarte, A., Cangrejo Aljure, L. D., & Delgado, T. (2018).** *Alternativa Open Source en la implementación de un sistema IoT para la medición de la calidad del aire*. Revista Cubana de Ciencias Informáticas, 12(1), 189-204. issn: 2227-1899.
13. **Sikder, A. K., Petracca, G., Aksu, H., Jaeger, T., & Uluagac, A. S. (2018).** *A survey on sensor-based threats to internet-of-*

things (iot) devices and applications. arXiv preprint arXiv:1802.02041. Retrieved from https://arxiv.org/abs/1802.02041.

14. **Sobin, C. (2020).** *A survey on architecture, protocols and challenges in IoT*. Wireless Personal Communications, 112(3), 1383-1429. doi:https://doi.org/10.1007/s11277-020-07108-5, issn: 1572-834X.
15. **Unión Internacional de Telecomunicaciones (UIT). (2012).** *Recomendación UIT-T Y.2060(06/2012). Descripción general de Internet de los objetos. DOI:11.1002/1000/11559. Retrieved from http://handle.itu.int/11.1002/1000/11559-es?locatt=id:1*
16. **Vélez, A. (2019).** *Arquitecturas de referencia para IoT con trasnferencia segura de información*. Tesis en Especialización De Seguridad Informática), Escuela De Ciencias.
17. **Wu, M., Lu, T.-J., Ling, F.-Y., Sun, J., & Du, H.-Y. (2010).** *Research on the architecture of Internet of Things*. Paper presented at the 2010 3rd international conference on advanced computer theory and engineering (ICACTE). Publisher: IEEE. DOI:10.1109/ICACTE.2010.5579493. Retrieved from: https://ieeexplore.ieee.org/abstract/document/5579493
18. **Zeinab, K. A. M., & Elmustafa, S. A. A. (2017).** *Internet of things applications, challenges and related future technologies*. World Scientific News, 2(67), 126-148. issn: 2392-2192.