SAT-IoT: An Architectural Model for a High-Performance Fog/Edge/Cloud IoT Platform

Miguel Angel López Peña
Innovation and Development Department.
Sistemas Avanzados de Tecnología, S.A. (SATEC)
Madrid, Spain
miguelangel.lopez@satec.es

Isabel Muñoz Fernández
Departamento de Sistemas Informáticos E.T.S.I.S.I.
Technical University of Madrid
Madrid, Spain
isabel.munoz@upm.es

***Abstract*—Current new IoT standards do not detail enough some important and emergent aspects as the Fog/Edge computing support, the IoT computation topology management or the IoT visualization systems. This work defines three new concepts: a) the paradigm of edge/cloud computing transparency that lets the computation nodes change dynamically without administrator intervention; b) the IoT computing topology management that gives an IoT system global view, from the hardware and communication infrastructures to the software deployed on them, and c) the automation and integration of IoT visualization systems for real time data visualization, current IoT topology and current paths of data flows. It is also defined a new architectural model that includes these concepts and covers other IoT demands, like security safeguard services based on Blockchain. This architectural model definition is taken as the basis for developing a new advanced IoT platform referred as SAT-IoT.**

Keywords—Internet of Things (IoT), Fog Computing, Edge Computing, Cloud Computing, IoT Platform, IoT Architectural Reference Models, Edge/Cloud Computing Location Transparency, Distributed Computing, IoT Visualization, IoT Topology Management, IT/IoT Automation, Blockchain in IoT.

I. Introduction

The International Telecommunication Union (ITU) defines the Internet of Things (IoT) as "global infrastructure for the Information Society, enabling advanced services by interconnecting (physical and virtual) things based on, existing and evolving, interoperable information and communication technologies" [1].

This challenging architecture requires the definition of an IoT formal framework that integrating the involved technologies, systems and devices [2]. The standardization of IoT platforms is in progress; there are published standards that already describe a Reference Model for the architecture and functionalities of IoT Platforms [3] [4]. In general, these reference models define the structure of an IoT platform as a set of logical entities such as: Business & External Application, Services & IoT Application, IoT Network & Gateways, Devices and Physical Layer [5] [6] [7]. These reference models also describe functionalities such as: Connectivity, Device management, Data Access and Databases, Data Processing and Management of Actions, Data Analytics, External interfaces including Human-Machine Interface (HMI), etc.

In addition to the IoT concept, Fog/Edge computing is a new technological paradigm pursuing the process of data near its sources in order to reduce latencies and save bandwidth [8][9]. Nowadays most authors accept that Fog/Edge computing features should also be included in the definition of the new IoT architectures [10] [11] [12] [13] [14].

From our point of view, the IoT platform standards do not detail enough some important and emergent aspects as the Fog/Edge computing support, the IoT computation topology management (mainly for industrial and Smart cities environments), the visualization systems integrated in the platform (not only in the applications) and audit services for IoT based in Blockchain or Distributed Ledgers.

This work presents a set of contributions to the IoT architectural reference models defined in current standards, in order to integrate the following concepts: 1) the paradigm of edge/cloud computing transparency, 2) the IoT computing topology management, and 3) the automation and integration of IoT visualization systems. In addition, it is proposed to include some new support systems demanded by the IoT market such as IT automation systems and the embedded regulation/audit services.

As a result, we propose a whole extended architectural reference model that is being used as the design and implementation basis of a new IoT platform (called SAT-IoT).

In the next section, we define the IoT framework concepts that extend the reference models. Then, we present a whole IoT architectural model in terms of entities and systems with their functionalities and mutual relationships.

II. new IoT Framework Concepts

A. *Paradigm of Edge/Cloud Computing Location Transparency*

In order to improve the performance of an IoT system, the Edge Computing model aims to process the massive data generated from different IoT devices at their zone edge nodes. Only the processing results are transmitted to the cloud infrastructure or to the IoT devices, reducing the bandwidth consumption, the response latency and/or the storage needed [15]. For example, consider an IoT system that uses the hybrid network of Fig.1. Since edge nodes X and Y are not connected to each other, any application that processes data from zones X and Y will be run in node Mid1, in order to be as near as possible to both edge nodes.

But the previous model is not well suited to applications in which the location of devices can change, the volume of data received in each edge node varies dynamically, or the processing needs data from different geographical zones. An example of this kind of scenario is a smart city car route planner, that calculates routes with information received from the cars connected.

978-1-5386-4980-0/19/$31.00 ©2019 IEEE

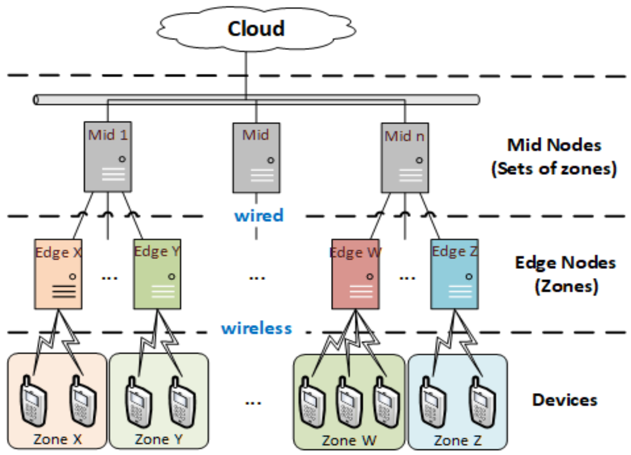


Fig. 1. Example of IoT hybrid network for mobile devices.

In an IoT Model, we define the Edge/Cloud Computing Location Transparency as a computational property of the system in which data to be shared in different zones can be processed in any edge node, mid node or in the cloud, looking for the optimization of response latency, bandwidth consumption, storage, etc. Furthermore, the selection of the computation nodes might change dynamically according to the conditions of the system (shared data, application requests, data volume, or any other relevant one).

Some target scenarios to apply this paradigm are: Smart cities (traffic monitoring, route planning), connected factories (with distributed zones like administration, manufacturing lines, logistics, etc.) or connected renewable energy plants (solar, wind, etc.).

B. *IoT Computing Topology Management*

In scenarios like Industrial IoT and Smart Cities, wireless networks complement wired networks to form a hybrid network [16]. These hybrid networks (Fig.1) include: the cloud, edge nodes and mid nodes. Mid nodes are connected to the cloud and to each other in a mesh network. Edge nodes receive data from wireless devices located in the same geographical zone. Groups of edge nodes are connected to a mid-node. Edge nodes are not connected to each other.

In this kind of scenarios where the hybrid network is defined and deployed ad-hoc, it is necessary a service to manage the IoT network topology. In addition, this topology administration service will facilitate the dynamic deploy of IoT distributed applications, the interconnection of devices to the IoT platform, and the data exchange among platform network nodes.

In summary, the topology administration service provides a global view of the IoT system from the hardware and communication infrastructures to the software deployed on them.

C. *Automation and Integration of IoT Visualization Systems*

Embedded functionalities of current IoT standards do not include the visualization of the IoT topology and its data flow paths. The data visualization service is only considered as part of the applications or included in external support services.

Including the "Edge/Cloud Computing Location Transparency" and the "Topology Management" entities in IoT system models requires a new visualization service, not only for data visualization, but also to show the current IoT topology and the paths of the data flows.

We define the concept of Automation and Integration of IoT Visualization System as a kind of system embedded in the IoT platform that is able to show automatically two basic dashboards: a) a system dashboard with the deployed IoT topology (nodes, links, their features and the consumption of their internal resources like memory, bandwidth, storage, etc.) and the data flow paths of the topology (data flows and their volume, for instance); and b) an IoT raw data dashboard to continuously show the data received in the platform from the configured and connected devices.

The main advantage of this integrated visualization system is that any IoT deployment could be verified even before the development of IoT applications. This occurs because, once the topology is deployed and the devices are connected, the platform would be able to show the topology (as defined in the topology management system) and the results of the internal monitoring of the IoT system.

III. SAT-IoT Architectural Model

Once the current standards have been analyzed, and we have defined the new concepts to include as part of an IoT Platform, we propose a new IoT architectural model with the following entities and elements: A) Physical Layer, B) Smart Device Entity, C) IoT Data Flow Collector Entity, D) IoT Data Flow Dynamic Routing Entity, E) IoT Topology Management Entity, F) IoT Visualization Entity, G) IoT Cloud Entity, H) Platform Access Entity, I) Security and Privacy and J) Embedded IoT Applications. Fig. 2 shows the architecture model with these entities, their internal systems, functionalities and interrelationships. Entities D) E) F) and H) are new, while the rest are extracted from the standards [3] [4] with some modifications.

The new architecture model will be used as a basis for the SAT-IoT Platform design and development.

In the next sections, we describe the entities of this architecture model.

A. *Physical Layer*

The physical layer in [3] or “infrastructures and communications” and “sensor networks” layers in [4] define the set of the basic physical devices, sensors and actuators in the real IoT scenarios (real world things).

In this architectural model, physical layer devices have neither processing capabilities nor intelligence. They can only get data or act in a very basic way, and they are connected/communicated through a data network. In view of this definition, we do not consider the physical layer as a part of the platform, but the layer over which the SAT-IoT platform manages, actuates and receives data.

B. *Smart Device Entity*

Physical devices have evolved significantly in terms of computational intelligence and data storage capacity, and the term "Smart Devices" has emerged [17]. Smart devices are widely used and integrated in different real IoT scenarios, and this is why the SAT-IoT platform includes an entity called "Smart Device Entity" at the bottom of the platform.

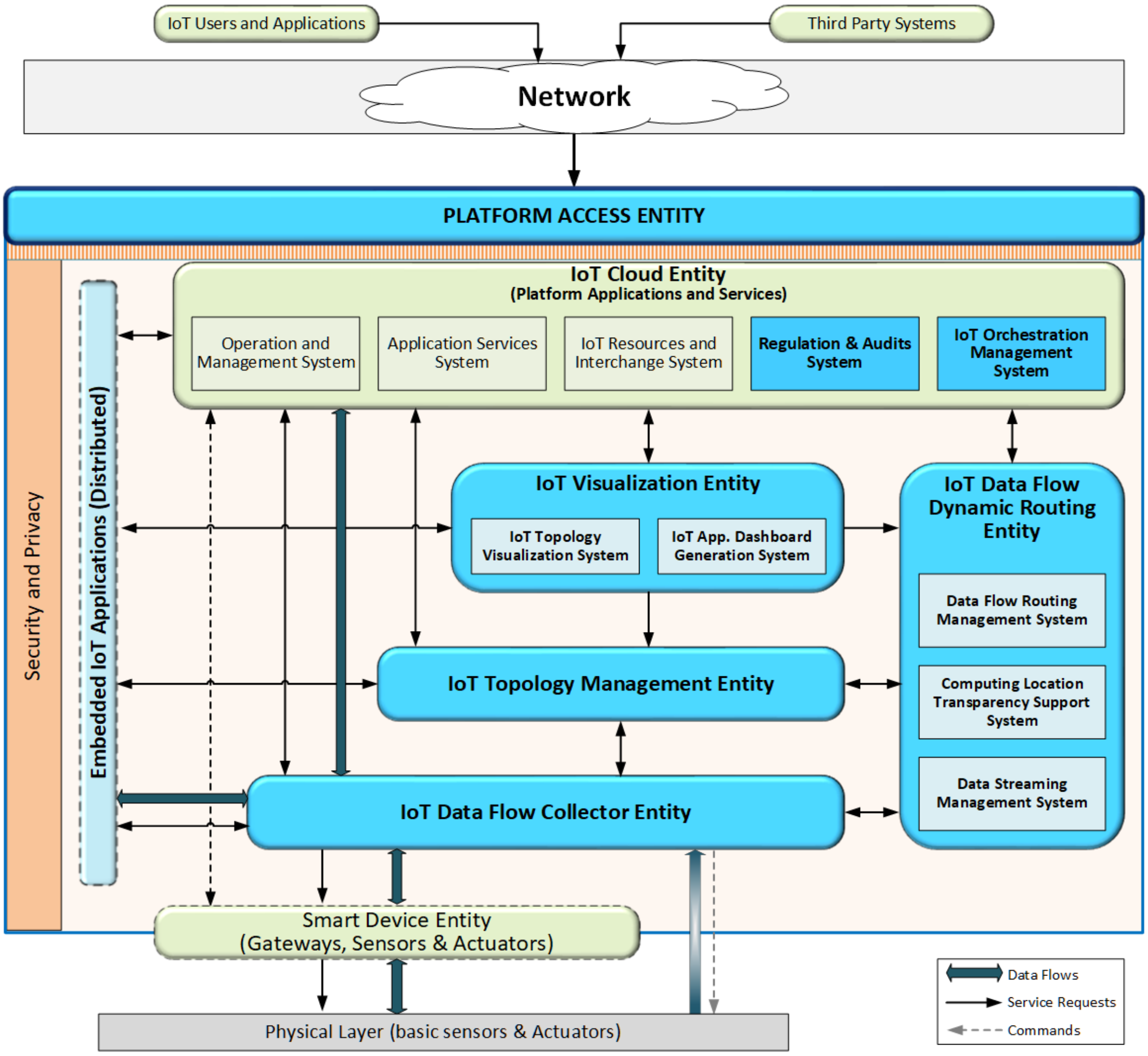

IoT Users and Applications
Third Party Systems
Network
PLATFORM ACCESS ENTITY
Security and Privacy
Embedded IoT Applications (Distributed)
IoT Cloud Entity
(Platform Applications and Services)
Operation and Management System
Application Services System
IoT Resources and Interchange System
Regulation & Audits System
IoT Orchestration Management System
IoT Visualization Entity
IoT Topology Visualization System
IoT App. Dashboard Generation System
IoT Data Flow Dynamic Routing Entity
Data Flow Routing Management System
Computing Location Transparency Support System
Data Streaming Management System
IoT Topology Management Entity
IoT Data Flow Collector Entity
Smart Device Entity
(Gateways, Sensors & Actuators)
Physical Layer (basic sensors & Actuators)
Data Flows
Service Requests
Commands

Fig. 2. SAT-IoT Architectural Model.

The entity "Smart Devices" in SAT-IoT is a combination of “Device Entity” and “Gateway Entity” from ISO/IEC 30141, This suggests its future implementation and functional running, not only in smart devices but also in other network appliances, such as physical gateways or hubs, routers, servers, etc. (typically installed in the network edge).

The functionalities defined in this entity are offered by the high-level function interface provided by the smart device, and the additional software.

Besides the typical IoT gateway functionalities [3] [18], the Smart Device Entity also includes the following functionalities:

- Device Access (Input/Output): High-level input and output operations, register read/write operations or memory operations inside the device. These functionalities also include the automatic data sending to the platform as messages under MQTT Protocol, abstracting the platform from local interconnections and buses (MODBUS, OPC, CANBUS, Serial, etc.).
- Device communications (Interconnection): They are the access network configuration Services. These services use the functions implemented by the devices to set the parameters needed to connect the device to the network through interfaces and technologies like GPRS, 4/5G LPWAN, etc.
- Other functionalities: access to functions and services directly offered by the specific smart devices.

C. *IoT Data Flow Collector Entity*

The IoT Data Flow Collector Entity is in charge of interconnecting devices (smart devices or simple devices) to the SAT-IoT platform.

This interconnection entity behaves as an IoT platform gateway. It is independent of the physical devices and their field protocols, providing the common entry point to receive IoT data from devices installed in the IoT system.

The IoT Data Flow Collector Entity is designed to be implemented, deployed and run in any network place. But it will be especially useful when deployed in edge nodes, because it works together with the IoT Flows Dynamic Router Entity (described below) in order to support Edge Computing and Edge/Cloud location transparency.

Therefore, the most important functionalities provided by the IoT Data Flow Collector Entity are the following:

- IoT Data gathering.
- Temporary data storage (for edge computing and location transparency).
- Data flows streaming to any internal or external application or service.
- Data Streaming to the platform global database (normally deployed in the cloud).
- Data pre-processing (data filtering, aggregation, measure error management, etc.)
- Execution of local services as microservices of a distributed application.

D. *IoT Data Flow Dynamic Routing Entity*

The IoT Data Flow Dynamic Routing Entity is one of the most important entities in the SAT-IoT architecture model because it supports the Edge/Cloud Computing Location Transparency model.

The IoT Data Flow Dynamic Routing is a key entity that manages dynamically data flows between processing nodes (cloud nodes, edge nodes and even smart devices). In addition, this entity includes a distributed temporary data storage system to support data streaming services and local processing services.

The IoT Data Flow Dynamic Routing Entity includes three main systems:

- **Data Streaming Management System:** it provides the mechanisms to transfer IoT data flows directly from nodes with local storage (for example edge nodes or smart devices) to other internal or external services and applications that request them (with a publish/subscribe model).
- **Computing Location Transparency Support System:** This system decides, in real time, the optimum node where a certain data flow must be processed. The optimum node election for a data flow is decided by an algorithm that uses IT resource optimization techniques, graph theory (based on the topology graph definition) and machine learning mechanisms, to predict the needs of the system in the short term. The prediction considers relevant current metrics of the system, as the hardware and software resources used, the data links bandwidth consumption, the application latencies, the zone structure of the topology or the data flows already involved in each node. The Computing Location Transparency Support System algorithm is part of the research work in the RECAP H2020 European Project[1] and its implementation will be integrated in the SAT-IoT platform.
- **Data Flow Routing Management System:** This system is responsible for setting the routing of a data flow to the optimum computation node, after inquiring about the best computation node for the data flow to the Computing Location Transparency Support System.

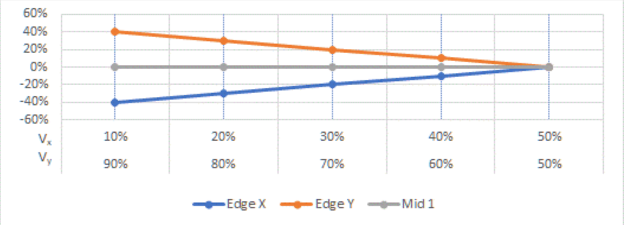


Fig. 3. Data Flow Dynamic Routing: preliminary tests.

It is important to note that, in the latter two systems (Computing Location Transparency Support System and Data Flow Routing Management System), the IoT Data Flow Dynamic Routing Entity needs to ask for the topology and its current performance to the IoT Topology Management Entity, and for the current data flows to the IoT Data Flow Collector Entity.

Fig. 3 shows the results of some preliminary tests performed on a test topology (Fig. 1) that demonstrate the savings or extra costs of bandwidth consumption due to the selection of different nodes when the amount of information shared by each node changes.

E. *IoT Topology Management Entity*

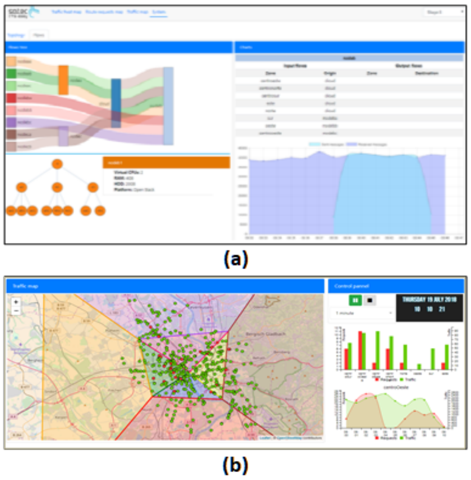
The IoT Topology Management Entity enables the definition of the network topology of every IoT system deployed by the platform. This entity describes each IoT topology as a graph [19] of computing nodes and links between them, and it includes a variety of attributes like node features (CPU, Memory, etc.), data link features (bandwidth), node geolocation (if available), use of resources (hardware and communication metrics), etc.

This entity manages dynamically the IoT hardware topologies. It enables updating the logical structure of the topologies at any time and it includes a monitoring system that continuously provides the status of nodes and links in terms of performance metrics (consumption of CPU, memory, storage, bandwidth, etc., and also data flows crossing the network).

The three main functions of the Topology Management Entity are:

- IoT Topology Definition: It enables the modelling of the IoT architecture as an enhanced graph in which nodes are the hardware elements with processing capabilities, defined with all their attributes (type, CPU, Memory, location, etc.), and edges are the data links and their corresponding attributes.
- Topology Management: It is a set of services to consult and modify the IoT topology definition in order to maintain the coherence between the physical installations and their definition in the platform. It supports the model of Edge/Cloud Computing Location Transparency offered by the platform.
- Topology Monitoring: It continuously gathers and stores metrics of each node and edge. It also provides these metrics to other internal systems (IoT Topology Visualization System or Embedded Applications) and external systems (third party applications and systems).

[1] http://www.recap-project.eu


(a)

(b)

Fig. 4. Visualization Entity: (a) System view (b) Application view.

F. IoT Visualization Entity

The IoT Visualization is an innovative entity that supports the automatic visualization of IoT systems deployed in the SAT-IoT platform.

This entity manages two complementary views of the IoT system: the IoT system view and the IoT data view (Fig. 4). The System view is focused on the IoT topology and the IoT data flow paths; the IoT data view is focused on the groups of data the system receives from devices (normally to be treated by applications).

The IoT Visualization Entity provides two independent internal systems:

- **IoT Topology Visualization System (Fig. 4a):** It interacts with the IoT Topology Management Entity to get all available system information, and automatically generates a dashboard that shows the IoT topology defined in the platform and the main features of its components (server nodes and links). In addition, it shows the data flow paths in the topology (number of messages and total size of them, for instance).
- **IoT Application Dashboard Generation System (Fig. 4b):** It provides functions for configuration and visualization. The configuration functionality provides a graphical user interface that enables the selection of predefined dashboard templates and the configuration of new ones, the visualization of all data types received in the platform from devices, and the matching between data types and template elements in which they will be shown. The visualization functionalities include the automatic dashboard generation with the settings defined before presenting it in a Web browser, and a set of controls over the graphical elements of the dashboard.

G. IoT Cloud Entity

The IoT Cloud Entity represents the highest-level applications and services that the IoT platform provides to external systems, users and applications. It is implemented in the cloud to offer a wide coverage.

The SAT-IoT Cloud Entity provides the three systems described in ISO/IEC 30141 [3] (Operation and Management System, Application Services System and IoT Resources and Interchange System), and includes two new systems that complete the entity:

- **Regulations and Audit System:** current IoT systems demand a lightweight, scalable, and distributed security and privacy safeguard [20]. The SAT-IoT platform provides some basic functions implemented with Blockchain (or other distributed ledgers) to secure specific sets of data. This allows the reliable retrieval of those sets of data and their analysis in processes of regulation compliance auditing (insurance, regulatory compliance, quality control, maintenance, etc.). These functions could also be integrated with data protection tools for encryption and anonymization purposes.
- **IoT Orchestration Management System:** SAT-IoT is a distributed platform that supports the development of distributed IoT applications. Therefore, it provides an IoT automation system that facilitates both the infrastructure definition and the system deployment (real or virtual servers and their configurations, links, connections, etc.). This system integrates software orchestration tools to deploy services and applications all over the IoT computing infrastructure. These tools are very suitable for the deployment of applications built as microservice architectures and encapsulated in containers by using container management tools as Rancher[2] and Kubernetes[3].

H. Platform Access Entity

The Platform Access Entity could be considered more a design element than an entity, because it is defined as a Platform API Gateway [21] on top of the architecture.

This API Gateway is the single entry-point to the SAT-IoT platform which publishes and exposes all the platform services to be used by external users, systems and applications.

The Platform Access Entity also manages and controls the access to services through an authorization and login system based on roles and user profiles.

Therefore, the Platform Access API Gateway, besides abstracting the internal structure of the platform to the external users/applications and simplify its use, provides the following set of cross functionalities and features: publishing of platform APIs for external use (services and groups of services from internal systems and modules of the platform), security policies (authentication, authorization, user management, applications registry, access permissions, etc.), routing (internal routing of messages and requests to different destinations inside the platform), access to sets of data stored and managed by the platform and to service APIs published by the platform for external use.

I. Security and Privacy

Security and privacy must be applied to the whole IoT platform in its different entities due to the distributed

[2] https://rancher.com/

[3] https://kubernetes.io/

architecture of the IoT platform proposed. Therefore, Security and Privacy is not considered as an entity in this design but as a core module that supports the basic functionalities related to secure access to the platform (applications, services, data, etc.).

Typical services provided by this module are: user and role management, access control (authentication, authorization and key management), security policies, data encryption and auditing.

J. *Embedded IoT Applications*

This block represents the embedded IoT applications that can be designed, developed and deployed integrated with the platform. These embedded applications can access to all internal services of the platform, and not only those exposed externally in the API Gateway.

In this way, the platform, the architecture and the embedded applications will be strongly integrated, and internal applications will take advantage of the platform in terms of access to its internal services, application setup functions and/or automated deployment processes.

IV. CONCLUSIONS

This paper defines new concepts for IoT architectures and a reference model that is being implemented in a new IoT Platform named SAT-IoT.

The concept "Edge-Cloud Computing Location transparency" lets computation nodes, in an IoT network topology change dynamically (without administrator intervention) to fulfill the efficiency criteria defined for the IoT system. The "IoT Computing Topology Management" concept integrates the hybrid networks (cloud, edge, devices and their wireless or wired links) as part of the IoT Platforms. This gives an IoT system global view, from the hardware and communication infrastructures to the software deployed on them. The Embedded IoT Visualization System concept offers a mechanism to check the deployment of the new IoT system in the platform.

In summary, the specification of an architectural model that integrates these concepts has been of great help to understand new technical demands in IoT, providing feasible solutions for complex systems as the SAT-IoT Platform.

V. FUTURE WORK

The IoT architectural model presented in this work has been used as an input for the design and development of the SAT-IoT platform. An incremental development life cycle has been started in order to produce some fast prototypes of the platform. It is expected to deliver the first full functional platform at the end of 2019. A vertical application for city traffic monitoring is also being developed, and it will be used for platform test purposes as a general IoT demonstrator.

ACKNOWLEDGMENTS

This work has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 732667 (RECAP. http://www.recap-project.eu).

We thank Pilar Manzano (ETSISI, Technical University of Madrid) for her advice and paper review.

REFERENCES

[1] International Telecomunicaciones Union (ITU), 2012. Recommendation ITU-T Y.4000/Y.2060 (2012), Overview of the Internet of things.

[2] Internet of Things Architecture and Applications: A Survey Tabassum Ara1*, Pritam Gajkumar Shah2 and M. Prabhakar. Indian Journal of Science and Technology, Vol 9(45), DOI: 10.17485/ijst/2016/v9i45/106507, December 2016.

[3] ISO/IEC JTC 1/SC 41 - Internet of Things and related: "ISO/IEC 30141. Internet of Things (loT) -- Reference Architecture". 2018. Available: https://www.iso.org/standard/65695.html

[4] CTN 178/SC 1 - INFRAESTRUCTURAS: "UNE 178104:2017. Comprehensive systems for a smart city management. Requirements of interoperability for a Smart City Platform. 2017. Available: https://www.aenor.com/normas-y-libros/buscador-de-normas/une/?c=N0059471

[5] GUTH, Jasmin, et al. Comparison of IoT platform architectures: A field study based on a reference architecture. En Cloudification of the Internet of Things (CIoT). IEEE, 2016. p. 1-6.

[6] ARA, Tabassum; SHAH, Pritam Gajkumar; PRABHAKAR, M. Internet of Things Architecture and Applications: A Survey. Indian Journal of Science and Technology, 2016, vol. 9, no 45.

[7] FREMANTLE, Paul. A reference architecture for the internet of things. WSO2 White paper, 2014.

[8] OFC, "Openfog consortium," accessed on, June 2016. [Online]. Available: http://www.openfogconsortium.org/

[9] HU, Yun Chao, et al. Mobile edge computing—A key technology towards 5G. ETSI white paper, 2015, vol. 11, no 11, p. 1-16.

[10] Fremantle, P., "A Reference Architecture for the Internet of Things," 2015. [Online]. Available: http://wso2.com/wso2 resources/wso2 whitepaper a-reference-architecture-for-the-internet-of-things.pdf

[11] BONOMI, Flavio, et al. Fog computing and its role in the internet of things. En Proceedings of the first edition of the MCC workshop on Mobile cloud computing. ACM, 2012. p. 13-16.

[12] Rafiullah Khan SUK, Rifaqat Zaheer, Shahid Khan. Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges, 10th International Conference on Frontiers of Information Technology, 2012.

[13] YI, Shanhe, et al. Fog computing: Platform and applications. En 2015 Third IEEE Workshop on Hot Topics in Web Systems and Technologies (HotWeb). IEEE, 2015. p. 73-78.

[14] MUNIR, Arslan; KANSAKAR, Prasanna; KHAN, Samee U. IFCIoT: Integrated Fog Cloud IoT: A novel architectural paradigm for the future Internet of Things. IEEE Consumer Electronics Magazine, 2017, vol. 6, no 3, p. 74-82.

[15] AI, Yuan; PENG, Mugen; ZHANG, Kecheng. Edge computing technologies for Internet of Things: a primer. Digital Communications and Networks, 2018, vol. 4, no 2, p. 77-86.

[16] SAUTER, Thilo; JASPERNEITE, Jürgen; BELLO, Lucia Lo. Towards new hybrid networks for industrial automation. En Emerging Technologies & Factory Automation, 2009. ETFA 2009. IEEE Conference on. IEEE, 2009. p. 1-8.

[17] WEISER, Mark. The Computer for the 21 st Century. Scientific american, 1991, vol. 265, no 3, p. 94-105.

[18] CHEN, Hao; JIA, Xueqin; LI, Heng. A brief introduction to IoT gateway. En Communication Technology and Application (ICCTA 2011), IET International Conference on. IET, 2011. p. 610-613.

[19] SCHVANEVELDT, Roger W.; DEARHOLT, D. W.; DURSO, F. T. Graph theoretic foundations of Pathfinder networks. COMP. MATH. APPLIC., 1988, vol. 15, no 4, p. 337-345.

[20] DORRI, Ali, et al. Blockchain for IoT security and privacy: The case study of a smart home. En Pervasive Computing and Communications Workshops (PerCom Workshops), 2017 IEEE International Conference on. IEEE, 2017. p. 618-623.

[21] MONTESI, Fabrizio; WEBER, Janine. Circuit breakers, discovery, and API gateways in microservices. arXiv preprint arXiv:1609.05830, 2016.