Network and IT Infrastructure Services for the IoT Store

Gaël Fromentoux and Nathalie Omnès(✉)

Orange Labs, 2 avenue Pierre Marzin, 22 300 Lannion, France
{gael.fromentoux,nathalie.omnes}@orange.com

Abstract. IoT, Internet of Things, is a major revolution dragging along new requirements that impact the network & IT infrastructure under development. Actually, the network infrastructure is evolving to embed virtualization techniques to gain in flexibility. For this purpose, new architectures are drawn-up such as the one proposed by the ETSI NFV. In this article, we first highlight a new business model: the IoT store. We then show how it benefits from the network & IT infrastructure services. After presenting the main actors of this business model, we actually provide the overview of an NFV-based architecture that fulfills new IoT requirements. We thus show that the move towards a network & IT infrastructure benefiting of Cloud and virtualization solutions can highly serve the IoT deployment.

Keywords: Infrastructure · Network · IT · IoT · Cloud · NFV · Business model · Store

1 Introduction

While the availability of mature IT virtualization techniques has led the IT infrastructure to successfully evolve to the Cloud, the network infrastructure still has to find its way to virtualization. This trend is on its way, in particular thanks to NFV (Network Function Virtualization), currently under standardization by the ETSI, but also with solutions put forward by vendors. Hence the evolution towards a new digital network & IT infrastructure is a revolution that has begun.

IoT, Internet of Things, is another major revolution. Billions of connected objects are upcoming, covering numerous areas ranging from health to entertainment, for example with pointless objects [1]. As a matter of fact, IoT encompasses a large variety of connected "things", including IoO (Internet of Objects) and its passive objects, M2M (Machine to Machine) and smart communicating devices / connected objects. These billions of objects drag along new requirements impacting the network & IT infrastructure under definition [2].

In this paper, we investigate how the network & IT infrastructure can fulfill some requirements issued from IoT.

The paper is organized as follow: the IoT store's business model is depicted in the Sect. 2. In the Sect. 3, we present how to move forward to offer an infrastructure service on line with IoT needs. The Sect. 4 then presents the actors and general architecture, while the Sect. 5 presents the architecture into more details. We finally conclude in the Sect. 6.

R. Giaffreda et al. (Eds.): IoT360 2014, Part I, LNICST 150, pp. 289–296, 2015.
DOI: 10.1007/978-3-319-19656-5_41

2 IoT Store Business Model

The application store business model, which relies on a multitude of web designers and developers, emerged thanks to the application of DIY (Do It Yourself) to web technologies. With the open hardware revolution, DIY now applies to the electronic field. By bringing a disruption into hardware conception, open hardware does not only lead to inventiveness, it also paves the way to the creation of many connected objects and start-ups. Hence the IoT store business model may emerge as a double-sided business, benefiting on one side of the multitude of connected objects' inventors, and on the other side of the relationship with the customers [3, 6].

The IoT store also benefits to connected objects' inventors by offering them a window display and by simplifying the distribution of their products. The IoT store manager should further provide inventors with a large customer basis so that their invention has a real opportunity to be widely exposed and adopted.

The IoT store benefits to consumers, by helping them into finding a way through the boiling universe of connected objects. In particular, connected objects shall get through a test phase so that only the reliable ones are published on the store. Billing, research and recommendation functions must also be implemented within the store to allow the consumers to buy objects and to let them be guided to new experiences or usages.

Thanks to all these elements, the IoT store business model becomes as safe as the application store business model, and multiple actors are enticed to grasp this opportunity. Please note that the main elements of this business are depicted within white rectangles in the following Fig. 1.

3 Towards Network and IT Infrastructure Services for IoT

Unlike web applications, connected objects have numerous and specific needs, while the related standards or technical trends are not clear yet. In particular, there are many possible access technologies, including 6LowPan, ZigBee and BLE (Bluetooth Low Energy), and none of them clearly appears currently as the sole possible answer. Furthermore, strong access control and authentication on the one hand and privacy and safety on the other hand are key issues, as stated by Vint Cerf [5], that must be addressed for the general public to gain confidence in connected objects and the associated data processing. Consider for example a connected lock letting authorized users to get into your home even when you are away. The corresponding requirements are very stringent and require a rigorous technical answer!

These stringent requirements will turn into the advantage of the actor that will combine the IoT store business model with the appropriate network service in terms of cost, QoS, connectivity and security. For instance, the IoT store itself cannot prevent customers from pervasive monitoring of the data received and emitted by their objects. However, that is the job of the network & IT infrastructure. The services developed over the network & IT infrastructure may encompass for example secured network links for exchanging information with connected objects, data storage within a cloud, gateways to link the IoT objects to the web or the secured access to the connected objects.

The main lines of this new business model are depicted on the following Fig. 1. The white rectangles correspond to the IoT store business model, while the grey ones are specific to the IoT store enriched with infrastructure services. Thanks to this business model, the store manager can win new business partners.

As depicted in the Figure, the key partners are a crowd of inventors, object designers and start-ups. The first need to fulfill is to provide a large customer basis to the IoT inventors. This is capital but however far from enough. Actually, it is necessary to provide inventors and consumers a common framework encompassing all the required functions and interfaces needed over the network & IT infrastructure (e.g. IP gateways, signaling gateways, authentication schemes, cloud resources). It is indeed the abilities to connect objects, but also to authenticate and associate with all involved actors the right bunch of objects, to bill, to provide secured network connections and advanced services which are keys for the success of the IoT store.

The value propositions are firstly to ease connected objects' distribution and advertizing for inventors and secondly to help consumers to step into the IoT through a trusted store. The customer relationship is indeed achieved through stores, online or not. The customer segments are very wide, as connected objects are likely to concern all mankind, from youth to elderly, at work, at home and on leisure time. The source of income for the IoT store actor is a percentage on all sales. Note there is also an indirect income linked to the actor's brand. Finally, the cost revenue must be kept very low, for the ARPO (Average Revenue Per Object) will be very low, if not nonexistent. This can be achieved with the dynamic sharing of network & IT resources thanks to virtualization. Furthermore, for this business model to be fully effective, API (Application Programmable Interface) must be designed and carefully opened.

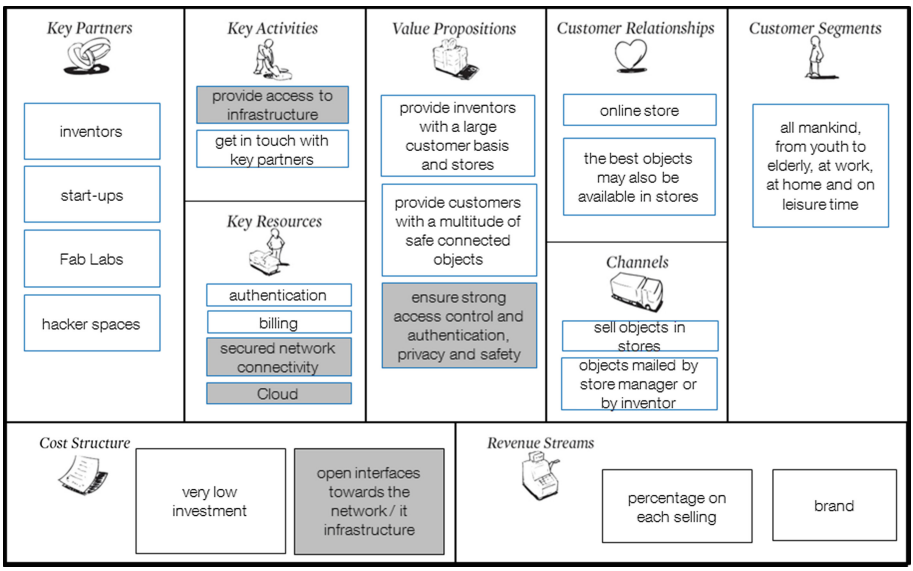

Fig. 1. Infrastructure service IoT store: a new business model

If we keep in mind that there will soon be billions of connected objects offered by multiple actors of different kind and for multiple different applications, there are a lot of challenges ahead!

The connected lock example highlights for example the need to make the distinction between different types of actors: the **owner** will have the right to deliver permanent or temporary access to a list of beneficiaries, a **user** will only have the right to unlock the door, while the **store manager** may have the right to remove all rights for unlocking the door. The related digital rights will have to be stored securely in a referential. Yet this digital rights inventory implies referencing connected objects thanks to metadata. This raises in particular the issue of identifying connected objects, issue that is not solved yet to our knowledge.

Therefore one or several IoT referential will have to be created, allowing the IoT store actor to identify, localize, characterize and group connected objects according to different points of view and types of actors. These referentials must in particular map objects, actors and rights related to each object. Managing and delivering access rights to a huge range of objects of various types is challenging, and so is managing access rights to billions of objects. The data stored in the IoT referentials also allows the objects' owners and users to have an overview of all the objects they are related to on a single web page, through a single interface. By providing the objects' location and state, it can further be used for managing the objects' end of life.

Another distinctive feature of connected objects is their huge diversity. They rely on different sources of energy, including none. They are connected to different types of access networks, including very low range connections. Some of them are connected by intermittence, either to preserve their battery or because they are intended to connect to an intermediate device that will provide them with the access to the service. This is for example the case of a NFC tag exchanging information with a smartphone. Hence a lot of basic connected objects will need to rely on a gateway to send and receive data.

4 Actors and General Architecture

As we have seen in the previous section, each connected object may be linked to different actors, including in particular its owner, its user and its manager. Each of these actors is interested by different kinds of information on the object. Consider for example an anemometer placed close to a kite surf spot and fed by a windmill. This anemometer thus provides wind information when the windmill can provide enough energy. Yet, when an anemometer does not provide any information, the owner may be interested by knowing whether it is because there is no wind or because the anemometer has broken down, while the users are only concerned by having access to the wind information. Furthermore, providing an overview of all available anemometers on a given geographical area and keeping an up-to-date inventory of them is an issue to address. More generally, managing any fleet of objects and providing its owner with exploitation information is a service that should be widely developed. For performing this, the store manager needs to build an IoT referential, including all metadata related to the object and in particular: an identification of each object, of each actor linked to the object and all access rights to each of these objects.

The main actors are depicted in the following figure. They include on the one side the object **user** that actually uses the object and the object **owner** that buys and maintains the object, both depicted on the left-hand lower corner of the figure. On the other side, the **inventor** specifies, designs and possibly markets connected objects. As an intermediate between these two actors lies the **store manager**, responsible for delivering, advertising and marketing applications and services related to IoT. To achieve these actions, the store manager relies on a convergent and virtualized network & IT infrastructure. IoTaaS services are provided on top of this virtualized infrastructure, providing on the fly resources such as applicative gateways and including also an IoT referential, matching objects, actors and access rights (Fig. 2).

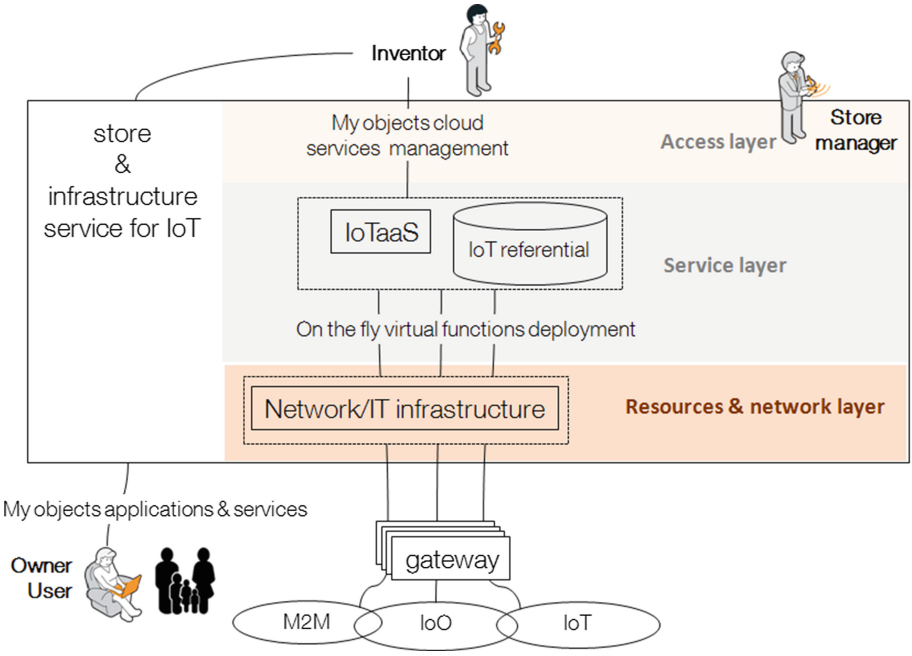

Fig. 2. Actors and general architecture

Thanks to this infrastructure, the store manager can identify and authenticate objects and objects' users and owners. Correlating this authentication to the IoT referential is indeed crucial for respecting strong access control and authentication, privacy and safety, required for the general public to gain confidence in connected objects. Furthermore, the store manager must provide interfaces to the inventors on the one side and to the objects' users and owners on the other side for them to manage the pool of connected objects they are related to, as we are going to depict into more details in the following Sect. 5.

5 Overview of the Network and IT Infrastructure Architecture

In this section, we give an overview of the network & IT architecture for addressing IoT requirements. More precisely, we show how the ETSI NFV architecture framework [4] can be used to support the IoT store.

Having access to a gateway between IoT on one side and service platforms on the other side is a recurrent issue. We have seen we will soon be surrounded by billions of connected objects. We therefore need to build these gateways on a scalable framework, in which one will pay only for what he actually uses. These are part of the founding principles of Cloud services, and hence we believe the answer shall be found in virtualization and Cloud directions. Currently, Cloud services are mature for the IT infrastructure, but not yet for network resources. With NFV, the ETSI currently defines the virtualization applied to network functions. As a matter of fact, some network functions have specific requirements concerning the type of hardware they can be deployed on or else their geographical localization. Pure IT Cloud infrastructures not being able to fulfill these requirements, NFV specifies a general framework to overcome these issues. In particular, the following Fig. 3 depicts 3 new functions specified by the ETSI: the NFV orchestrator, the VNF (Virtual Network Function) manager and the VIM (Virtual Infrastructure Manager).

The **VIM** is responsible for controlling and managing the virtual machines providing computing, storage and network resources.

Then, a **VNF** (Virtual Network Function) is used to support a network function, for example in our case an IoT gateway. The **VNF manager** is responsible for controlling and managing all VNFs. For example, if thousands of connected objects wake up at the same time to upload the information they have collected, the correspond IoT gateway's VNF may need to scale up. This is achieved by the VNF manager that asks the VIM to allocate a new virtual machine to the VNF in order to put up with the new traffic load.

When uploading its collected data, the IoT gateway needs to get in touch with another network function: the data collection. But this data collection also relies on a VNF, made of one or several virtual machines. Hence directing the collected data to the correct location is not straightforward, and needs the specification of a network service: the IoT data collection in our case. This **network service** is controlled and managed by the **NFV orchestrator**. In particular, the orchestrator has a complete knowledge of all deployed IoT gateways and data collectors together with the links between them. It can further create a new gateway when necessary, for example for scalability of localization issues.

Unlike IT resources, the geographical location of network functions is indeed crucial. In particular, the IoT gateway cannot be deployed anywhere in the network, but only in precise and defined locations. The ETSI NFV addresses this issue by allowing specific constraints to be added when requiring a virtual machine, including hardware and localization constraints. Thus NFV can bring an appropriate answer for deploying IoT gateways geographically distributed throughout a territory.

The following Fig. 3 depicts other elements, and in particular a portal to which the objects' owners and users are related. This IoT portal offers several services, within

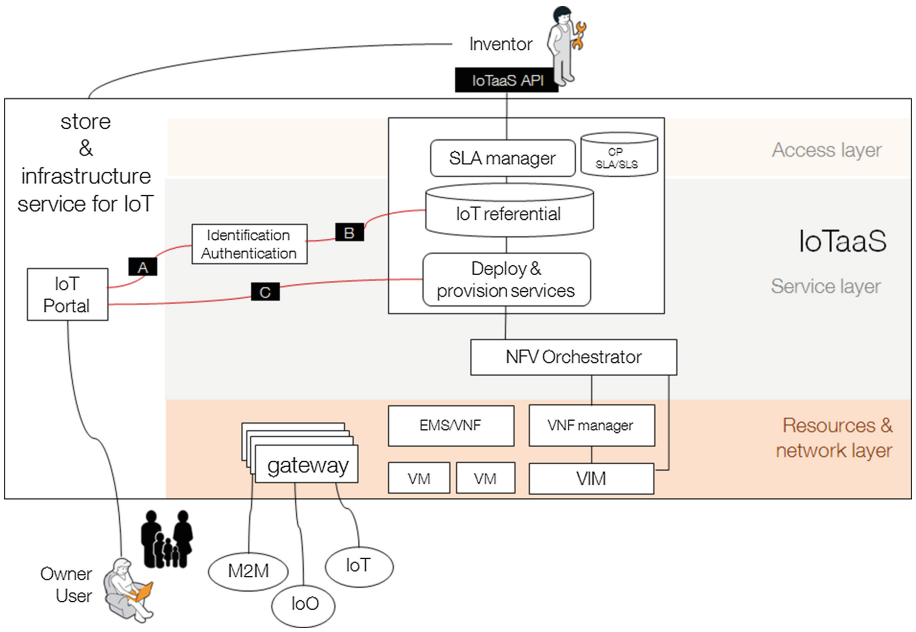

Fig. 3. Overview of the Network and IT Infrastructure Services Architecture

which the IoT dashboard. To build this dashboard, the IoT portal requires the access to the IoT referential. For security and safety issues, this access to the IoT referential must be protected thanks to an identification and authentication function. We thus highlight new interfaces, A and B, depicted in red in the Fig. 3.

The above Figure highlights another new interface, labeled C, between the IoT portal and another function named "deploy & provision services". This function is responsible for interacting with the NFV orchestrator to create new network services or update existing network services for instance in terms of features, topologies, resources. This new interface is restricted to the store manager and does thus not need other actors to authenticate.

The **IoT referential** is also implemented within a VNF, using one or several virtual machines. We have seen this referential must have knowledge concerning all objects, including the **identification,** the **type** of connected object and type of object's authentication. The object's **location**, crucial when deploying IoT gateways, shall be referenced within this IoT referential function. The list of each object's users and owner shall also be stored within the referential. This list must be dynamically updated each time a digital right is either created or removed by the object's owner. This referential shall further be improved by the network & IT infrastructure, which provides in particular location and status information.

Smartphones as widely distributed and smart connected devices are likely to play a particular role, acting as gateways and digital rights repository. The IoT referential can be linked to a push notification server and provide relevant information concerning a

collection of connected objects to the smartphone, including for example the owners' identity and the status of the object (alive, unreachable, low battery…).

More generally, IoT requirements can be fulfilled by dynamically implementing new functions thanks to the NFV framework. This framework indeed offers the key advantage of scalability and cost-efficiency that are vital to address the tsunami of connected objects and their very low ARPO.

6 Conclusion

Modeled on the application store business model, the IoT store is emerging as a double-sided business between the IoT inventors and consumers. The open hardware revolution actually paves the way to the multiplication of IoT inventors. However, connected objects have numerous and specific needs, while the related standards or technical trends are not clear yet. We have thus highlighted an evolution of the store business model, in which the double-sided IoT store business is enriched with network & IT infrastructure services. In particular, we have shown that new functions are required and must be combined: IoT gateways and IoT referential. Because these new functions must be highly scalable and cost-efficient, we suggest relying on the virtualization techniques – see ETSI NFV framework - for their deployment. We have thus provided an overview of this new network & IT infrastructure service architecture. We indeed believe that the IoT stringent requirements will turn into the advantage of the IoT store actor that will be able to offer the appropriate network & IT services in terms of cost, QoS, connectivity, flexibility and security.

References

1. Boujemaa, F., et al.: Internet of things, the newt Wave of Internet, Final synthesis, September 2012
2. Ropert, S.: Internet of Things, Outlook for the top 8 vertical markets, Idate, Septembre 2013
3. Berkers, F., Roelands, M.: Contructing a Multi-Sided Business Model for a Smart Horizontal IoT Service Platform. In: 17th International Conference on Intelligence in Next Generation Networks, October 2013
4. Chiosi, M., et al.: Network Functions Virtualisation – Introductory White Paper, at the "SDN and OpenFlow World Congress", Darmstadt-Germany, 22−24 October 2012
5. http://www.networkworld.com/community/blog/google%E2%80%99s-vint-cerf-defines-internet-things-challenges
6. http://phx.corporate-ir.net/phoenix.zhtml?c=176060&p=irol-newsArticle&ID=1923514&highlight