University Of Pisa

Department Of Computer Science

Ph.D. Thesis Proposal

Cloud Computing and the Internet of Things: Service Architectures for Data Analysis and Management.

Marco Distefano

Supervisor
Prof. Massimo Coppola

October 2015

Contents

1 Introduction

This document presents my PhD thesis proposal that concludes my first year as PhD student on Computer Science Department of University of Pisa.

The document is organized as follow. In Section 2 we introduce the Cloud Computing paradigm giving a detailed definition, explaining the main features of the paradigm and listing the service and the deployment models. This section continues with the introduction of Internet of Things paradigm by different perspectives along with some application domains. Section 3 presents a scenario in which Cloud Computing and Internet of Things converge. This is presented along some motivations and benefits for their integration. Moreover, the Section also presents the state of the art of this convergence and present some works on the areas that have been most covered by the community. Finally Section 4 gives a summary of the main open issues that regards the convergence of Cloud and IoT according to the principal contributions of the state of the art. In that section is also sketched a service architecture which aim is twofold. On the one hand it addresses most of the aforementioned issues. On the other hand, we believe that it could meet the typical requirements of IoT services and users. We will end Section 4 with the activities planned aimed at defining, refining and evaluating this service architecture, in order to face all the issues related to Cloud and IoT convergence.

2 Background

2.1 Cloud Computing

Cloud Computing is one of the most popular and interesting computational paradigms, due to its several benefits, that have been explored in the latter years. Although many definitions have been proposed in academia and industry, the one that has been generally accepted by the community is the one that has been formally proposed by the National Institute of Standards and Technology (NIST) [30]:

> *"Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."[30]*

From this definition is possible to extract some peculiar characteristics that emerge from this paradigm.

On-Demand self-service
Cloud services give to a customer an instantaneous access, in his desired timeslot,to the computing resources that he need (e.g. CPU time, storage space, network access etc.) in an automatic and self-serve fashion without requiring any human interaction with the provider of resources.

Broad network access
The resources requested by customers are delivered through the network (e.g. Internet) and are used by several client applications with heterogeneous platforms (such as mobile devices, laptop, workstation etc.) requiring standard protocols and mechanism to access them.

Resource pooling
The computing resources of a cloud service provider are 'pooled' together to serve multiple customers in a multi-tenant way using different physical and virtual resources that are dynamically assigned to satisfy the user demand. This pool-based model has the aim to render 'invisible' the resources to consumers who do not have control or knowledge over the location, formation, and originalities of these resources (e.g. CPU, database etc.).

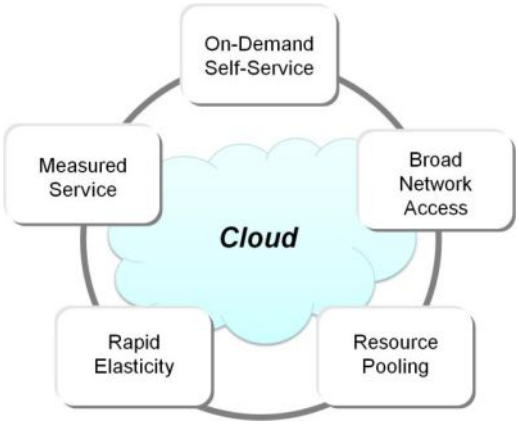

Figure 1: Cloud Computing characteristics

Rapid elasticity
The capabilities of a service provisioned by cloud provider can be elastically deployed, assigned and released to scale up whenever the consumers want and released once they finish to scale down. In this way the resources appear to be unlimited and can be allocated in any quantity at any time.

Measured service
Although computing resources are shared in a multi-tenant way, the underlying infrastructure is able to measure the usage of these resources of each consumer by using appropriate mechanisms in order to give a pay-per-use model to its costumers.

2.1.1 Service models

Considering the services that can be offered by a Cloud provider, we can find three different service models each of them differs from other for the control given to the user on the resources allocated to him, the general functionalities and the architectural layer offered [20].

Software-as-a-Service (SaaS)
In the SaaS model Cloud consumers release their applications to the chosen provider that provide an hosting environment which can be accessed through networks. In this way, the customers do not have control over the entire infrastructure and its management that is completely in charge to the provider.

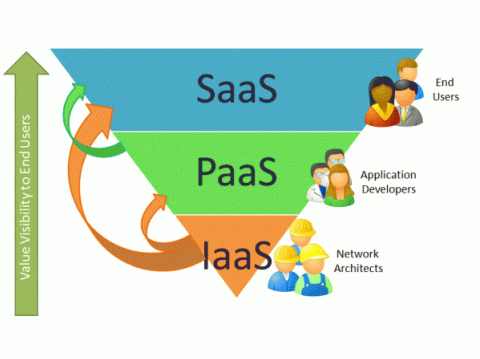

Figure 2: Cloud Computing Service Models

Platform-as-a-Service (PaaS)
The PaaS model consists in a development platform that supports all the software life cycle providing to customers a complete environment to develop his proper services or applications.

Infrastructure-as-a-Service (IaaS)
In the IaaS model, Cloud customers can use directly the IT infrastructure to manage all the software stack. Through the virtualization technology the provider offer all the capabilities of his infrastructure, from processing to storage and network resources.

Moreover, in the latter years, the new definition of Everything-as-a-Service (XaaS)[12] is becoming even more relevant and widely accepted by the community. This definition, that resumes the more important aim of Cloud Computing, also highlights the fundamental role of delivering services through this computational paradigm.

2.1.2 Deployment models

From given NIST definition of Cloud Computing [30] we can categorize a Cloud infrastructure through its deployment models.

Private Cloud
A private cloud infrastructure is provisioned for a single entity or organization that gives the services running in it to its clients or employees. Such type of Cloud infrastructure is managed by the organization itself or by a third part that assures the exclusively use of the resources.

Community Cloud
The community model involves customers from different organization that share a common goal in the usage of a Cloud infrastructure. A community cloud may be owned and managed by one or more of the organization involved in the community or, like a private cloud, can delivered by a third party.

Public Cloud
A public cloud is a cloud infrastructure provisioned for open use. A provider of a public cloud offers all the services and the resources to anyone ask them in a pay-per-use model.

Hybrid Cloud
In an Hybrid Cloud the infrastructure is a composition of two or more

distinct infrastructure with different deployment models. The different infrastructures involved in an hybrid cloud are bound together with standardized or proprietary technology that enables the portability of data and applications.

In this context, the Cloud Computing paradigm offers a wide set of choices to who would like to exploit the benefits in using such type of infrastructures.

However, in the latter years, many of the Cloud services providers has faced the problem to meet the expectations of all their customers that require specific Quality of Service (QoS) parameters. To face this issue, the research community have also explored a new model for organizing the Cloud infrastructures in a federated way [16]. The new concepts of *Inter-Clouds* and *Cloud Federations* have become very popular and are seen as the better way to offers many benefits to customers, like the mitigation of the vendor lock-in problem (the customer is often tightly-coupled to a single cloud provider), an improved reliability and a geographic distribution that can overcome issues of compliance with laws and regulations.

2.2 Internet Of Things

The term Internet of Things (IoT), first introduced by Kevin Ashton in 1998, refers to an emerging paradigm that consists in a new Internet-based information service architecture [35]. In IoT, "*things*" refer to objects and devices connected each other to form much larger systems enabling new ubiquitous and pervasive computing scenarios.

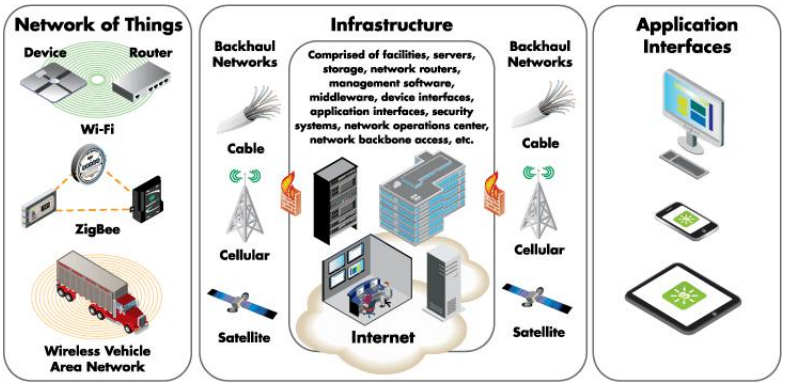

Figure 3: The Internet Of Things

According to European Research Cluster on the Internet Of Things [1] the objects and devices involved in this emerging paradigm are generally characterized as real world and small things that are involved in several business, information and social processes [34]. Indeed, there isn't a real convergence in the definitions of Internet Of Things in the research community due to the fact that exist different visions of the same paradigm. In fact, as highlighted by Atzori et al. [10] there are at least three different perspectives to give a definition of IoT paradigm.

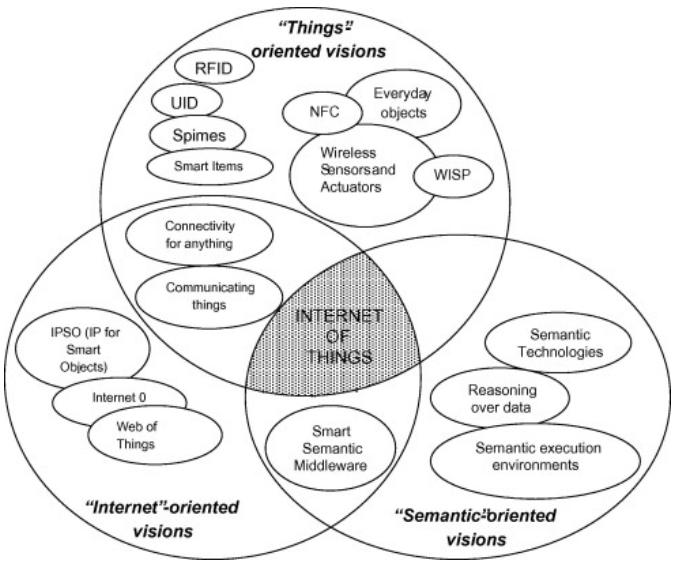

Figure 4: The three perspective of IoT [10]

The first derives from a "*Things*"-oriented perspective in which the focus is in the devices involved that can be RFID devices, wireless sensors and actuators or smart objects of everyday life. Another perspective is a "*Internet*"-oriented vision that poses the focus on the enabling technologies that make possible the communication of the objects involved in a network oriented vision. A third perspective in the IoT vision has a more "*Semantic*" approach. Considered that the number of *things* connected together are growing every day exponentially is crucial to face issues related to how to store, manage and represent the data produced by the Internet of Things systems.

[1] http://www.internet-of-things-research.eu/

2.2.1 Applications of IoT

The collection and the transmission of data from the devices, machines and sensors involved in the Internet of Things and the communication between them lead to have several application domains and an unprecedented flexibility in their variety. Such a variety can be classified into at least four application domains: Personal and Home, Enterprise, Utilities and Mobile [23].

Figure 5: IoT application domains [23]

In the context of personal and home domain, for example, various applications for controlling homes and buildings equipment such as air conditioner, refrigerators, washing machine etc., can allow better home and energy management [9, 19]. Moreover, ubiquitous healthcare [10] has been envisioned through IoT systems that give a perfect platform to enabling this vision, for example, using body area sensors and an IoT backend to upload data to servers. An extension of the body area sensors has been developed for creating a home monitoring system for aged-care that allows the monitoring of the elderly patients by doctors directly in their homes reducing hospitalization cost [29, 32].

In the enterprise domain sensors have been an integral part of the factory mainly used for security, automation, climate control etc. The advent of Internet Of Things can replace the old sensors with wireless systems that give the flexibility to make changes to the settings when required. Moreover, a growing attention in the latter years is focused on the Smart Environment IoT in which can be possible identify many applications and use-cases.

These applications can be related to emergency services, traffic management, infrastructure monitoring etc.[28].

The information from the sensor networks in the utilities domain are already being used by utility companies for management of resources to optimize costs and profits. The smart metering and the smart grid are another interesting IoT applications and through it, for example, is possible to achieve efficient energy consumption by monitoring the electricity points and using these data to change the way of how the electricity is consumed. The monitoring of water network is another crucial application that is being addressed using IoT. The monitoring of water parameters through sensor networks allows to ensure high quality supply and avoids accidental contamination among storm water drains, drinking water and sewage disposal.

Another important application in the utilities domain is the Video based IoT which supports surveillance systems. These type of applications integrates video, infrared, microphones and network technologies for helping to track targets, identify suspicious activities and monitor unauthorized access.

Another domain of IoT application involves moving *things*. The mobile domain can include smart transportation and smart logistics. The IoT can allow to use existing sensor network to give dynamic traffic information that can use for example to allow better planning and improve scheduling on freight movement or collect data for urban traffic control.

3 IoT and Cloud Convergence

How we explained the two concepts of Cloud Computing and Internet of Things have seen an independent evolution in the latter years. However, many actors both from the research community and from industry have seen an interesting convergence in these paradigms. Several advantages deriving from the integration of IoT systems and Cloud services and infrastructures have been identified [14]. IoT systems can have many benefits from the virtually unlimited capabilities that Cloud Computing can offer, for example, to compensate the technological constraints (e.g., storage, processing, energy) of IoT devices.

This vision highlights that Cloud and IoT have many complementary characteristics arising from the different proposals in literature. As the research community has envisioned, the Cloud can act as intermediate layer between the *things* and the applications hiding all the complexity of the resources management and the functionalities necessary to implement the latter. This intermediate layer will impact future application development,

where information gathering, processing, and transmission will produce new challenges to be addressed [18].

3.1 Motivations

The convergence between Internet Of Things and Cloud Computing reveals a new paradigm that seems to be promising named in the literature in various way such as Cloud Of Things [8] or CloudIoT [14]. The number of Internet of Things devices connected to Internet is growing exponential and, since 2011, has already exceeded the number of people on Earth. They have already reached the 9 billion and are expected to grow more rapidly in the next years until reach the 24 billion in 2020 [23]. Besides the growing number of IoT systems, other aspects reveal several motivations on its integration between IoT and Cloud Computing infrastructures that will be shown in this section.

Storing data locally and temporarily will not be possible anymore and there is going to be even more a need of storage space. Moreover, this huge amount of data can't be processed locally in the devices and the need of computational capacity is growing.

Typically the IoT services are provided as isolated vertical solution in which all component of the applications are tightly coupled to the specific context of application. Bringing IoT services in the Cloud can ease the delivery and the deployment of them by leveraging all the flexibility of Cloud models. In this context, the Cloud Computing facilitates applications de-

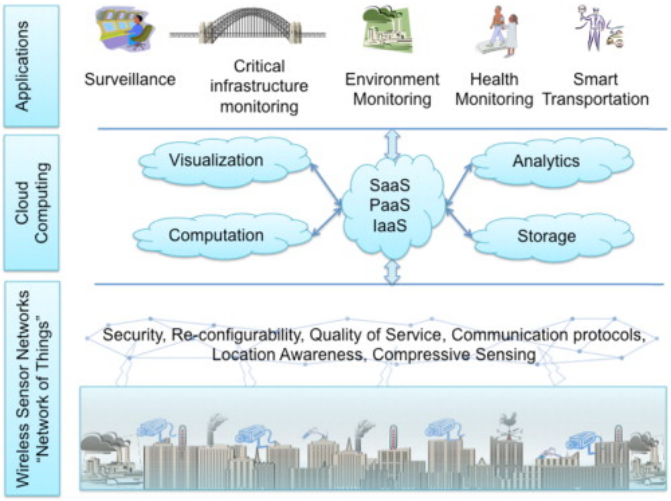

Figure 6: Cloud as a middleware in IoT paradigm [23]

velopment make possible an abstract vision of the IoT systems and offers its services to meet need to decouple the applications from the specific context.

Internet of Things can provide also a platform for the Smart Cities services that are been envisioned in the latter years. Through these platforms can be possible acquiring information from different heterogeneous sensing devices, accessing all kinds of geo-location and IoT technologies, and exposing data extracted from them in a uniform way. Several proposed solution suggest to use Cloud architectures to discover sensors and actuators, to enable their connection and interaction and to create platforms that are able to support ubiquitous connectivity and real-time applications for smart cities[11, 33, 31].

Another scenario in which Cloud and Internet of Things can participate in a coordinated manner to provide better services is the Smart Energy. To provide intelligent management of energy distribution and consumption in a local or a wide environment, the computing tasks that collect data from different sensing nodes attached to the network can be offloaded to a Cloud to exploit its computational capabilities for taking more complex and comprehensive decisions about the energy usage.

These examples, of course, not cover all those aspects in which can be a cooperation between Cloud and Internet of Things but, in all these cases, Internet of Things systems can have many benefits from the usage of an "*unlimited*" computational capacity allowing scalability in their applications. Also, elasticity that a Cloud infrastructure provides can face scenarios in which there is a peak of the demand of resource usage from an IoT system or these resources can be released because the demand is poor. Finally, in each of these scenarios, the pay-per-use model has a crucial role reducing the deployment cost of these infrastructures.

3.2 State of Art

Although this new paradigm can allow that Cloud and IoT work together to satisfy the needs explained and can bring new business models, their integration bears a lot of unsolved issues.

3.2.1 Service Delivery and Development

As we seen, a Cloud infrastructure can ease the development and delivery of IoT application through its service models. Leveraging PaaS-like models as Li et al. have proposed [27] can represent a generic solution for easing the development and the deployment of IoT applications. In contrast, this

moves some IoT challenges in the Cloud scenario. For instance, management of highly heterogeneous devices as well as the interaction with them have to be addressed in the Cloud on each different architectural and service level.

Through the Sensor-Cloud infrastructure, Yuriyama and Kushida [36], have proposed a solution to allow the management of physical sensors by connecting them to the Cloud. Sensor-Cloud abstracts the physical sensor in a virtualized environment, grouping them for group configuration and management, allowing user to share the capabilities of his sensors without worrying about the specific details. This solution can overcome the problem to interface an application with different kind of sensors but it only focuses in managing and configuring sensors via cloud leaving out issues related to data collected.

Apart from the mere research works, the panorama in the area of services delivery and development in IoT field is very complex and provides solutions both from the open source world that from the closed ambit of the industry.

From the open source side we can cite OpenIoT project [5] in the EU or Open Source IoT Cloud project [3] in the US. Both the latters projects have the aim to provide a middleware that facilitate the configuration and the deployment of algorithms for collection and filtering messages from the *things*.

Even the industry has proposed its solutions. Such commercial system, like Xively (formerly COSM) [7], ThingSpeak [2] and Open.Sen.se [6], provide tool for collecting data from *things* and to store them on the Cloud

Table 1: Platform, services and research projects

	Proprietary Things	Open Things	Private Cloud	Public Cloud	Free	Open Source	Application API	Ready To Use
IoTCloud	✓	✓	n/a	n/a	✓	✓	✓	✓
OpenIoT	✓	✓	✓	✓	✓	✓	✓	✓
Open.Sen.se	✓	✓	✓		✓		✓	✓
Xively	✓	✓	✓		✓		✓	✓
ThingSpeak	✓	✓	✓		✓		✓	✓
NimBits	✓	✓	✓		partly	n/a	✓	✓

offered by service provider.

Moreover, the industry has brought his contribution providing also open source solutions. Through these, we can mention the open source project NimBits [4] that provides a set of software to be installed in a private or public Cloud (Google App Engine) to create a PaaS service to collect data from devices and trigger action when specific conditions are verified.

3.2.2 Data Storage

As highlighted previously, with an estimated number of tens billions of devices that will be connected to Internet in the next years, specific attention must be give to storage, access and processing of the huge amount of data that IoT devices will produce. This bring the problems that have to be faced in the scenario of Big Data in which the IoT is a principal actor. It is clear that from a data centric perspective, the IoT asks to the Cloud more rental storage space, uniform treatment of heterogeneous data, scalability of applications, distributed processing and real-time analytics.

Considering the data storage perspective, the ubiquitous sensors, RFID readers, wireless sensor network devices and the other items involved in the IoT systems generate data very fast and the solutions of data storing must be able to store massive data efficiently and support horizontal scaling. In addition to this, the data collected from the variety of *things* involved consist of various structured and unstructured data and the components which have the responsibility to store them must have the ability to deal with heterogeneous data sources.

To overcome these issue Jiang et al. [25] have proposed a data storage framework that solves the problems to store structured and unstructured data collected from different sources. This proposed approach combines different types of databases (DBMS for structured data and file repository for unstructured) and provides an unified interface to store and access them. The databases that this solution supports are MySql, MongoDB and authors have improved Hadoop platform to realize a distributed file repository which supports version management and multitenant data isolation.

A similar solution to the previous one have been proposed by Fazio et al. [21]. In this work, they have proposed a Cloud storage solution that provides data access and query capabilities to several heterogeneous data sources from the scenario of the environment monitoring. They distinguish the data collected from the sensors in two category: *Documents*, retrieved from the measurements of physical or composed phenomena performed by

sensing devices, and *Objects*, that consist on multimedia contents retrieved from information content processing devices (video, audio, images etc.). The storage system they proposed integrates Document-Oriented Storage System (DO-SS), like MongoDB or Cassandra, for the measurement data and Object-Oriented Storage System (OO-SS), like AWS S3 or SWIFT, for the multimedia objects and their metadata. For the integration they refer to two specific Sensor Web Enablement (SWE) standards (Sensor Observation Service, SOS, and Sensor Alert Service, SAS) defined from Open Geospatial Consortium (OGE) to enable sensor web discovery and exchanging and processing sensing information [15].

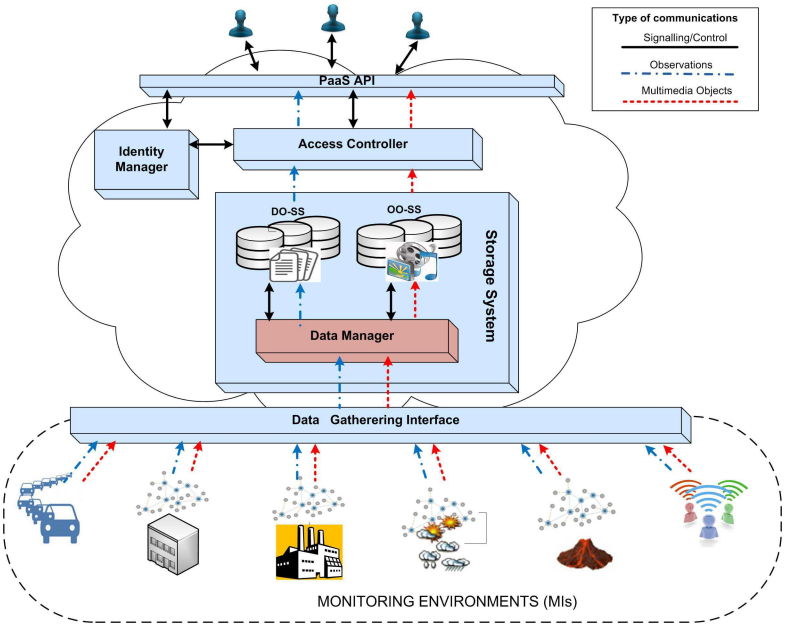

Figure 7: Cloud Storage System [21]

3.2.3 Security, Privacy and Identity Protection

Besides data and resources, the Cloud of Things has to deal with its impact in the business and its consequences. This will create more business opportunities and is making itself more attractive for the attackers. In this terms, security, privacy and identity protection will be major concerns in this area. The two principal components of Cloud Of Things - IoT devices (RFID, WSN etc.) and Cloud infrastructures - are vulnerable to many kind

of attacks or theft actions like, for example, disabling network availability, pushing erroneous data into the network or accessing personal information. In many cases, using cryptographic protocols can ensure data confidentiality, integrity and authenticity. However, encryption cannot ensure protection against insiders malicious attacks [23] and can be hard to implement on computational-constrained devices where no high level intelligence can be enable (specially RFID passive devices) [26]. Another issue regards the updates that are necessary on IoT devices. These is often made through remote wireless reprogramming of all the devices in the network that exploits reprogramming protocols that distribute the new code. Most of such protocols are based on the data dissemination protocol Deluge [17] in which the security on data dissemination is hard to achieve with low overhead on thin devices.

3.2.4 Communication Protocols

The protocols which the sensing devices communicate play a key role both in IoT side that in a complete integration with Cloud infrastructures. Even if the the entities in an IoT scenario can be homogeneous, they can work through different protocols to communicate. The protocols that have been proposed in this area are several (ZigBee, WirelessHart, Bluetooth etc.), none of them has been accepted as a standard. Apart security, already treated in the previous paragraph, the energy consumption is the main consideration for the existing routing protocols mainly for IoT systems that use wirless sensor network technology.

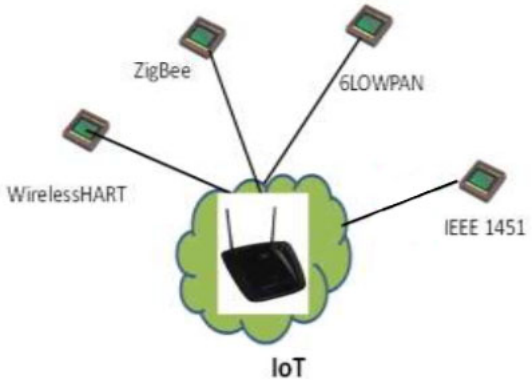

Figure 8: IoT protocols [8]

Although, in the literature can be find existing routing protocols that can work with minor modification in IoT scenario [23], the Internet Engineers Task Force (IETF) Routing Over Low power and Lossy networks (ROLL) working group claims that in such protocols there isn't a complete requirements satisfaction especially in guarantee of low power network connection. Hence, the IETF ROLL group has been proposed a protocol draft that tries faced these requirements to achieve optimization for energy saving, point-to-multipoint traffic patterns, restriction in the frame-size etc. [24].

3.2.5 Fog Computing

In a more abstract vision, the issues arise from the integration of Cloud Computing with the Internet of Things systems bring another paradigm that is *Fog computing*. Fog Computing is a highly virtualized platform that provides compute, storage, and networking services between end devices and traditional Cloud Computing infrastructures that bring the cloud capabilities "*close to the ground*" and then to the *things*. It has been designed to support all these applications involved in IoT that are characterized by strong latency constraints, real-time analysis and processing, requirement for mobility and geo-distribution [13]. Bringing the Cloud at the *edge of the network* implies in several characteristics that make the Fog Computing a non-trivial extension of the Cloud Computing paradigm. The principal characteristics of this paradigm are:

Location awareness and low latency capabilities
This property has been brought by the need to support endpoints with rich services at the edge of the network including application with low latency requirements.

Geographical distribution
In contrast to the centralized Cloud paradigm, the services and applications deployed in the Fog are widely distributed among several geographic positions.

Support for mobility
Many application need to communicate directly with the mobile devices and the Fog allow to decouple host identity from location identity through mobility techniques such as the LISP protocol [1].

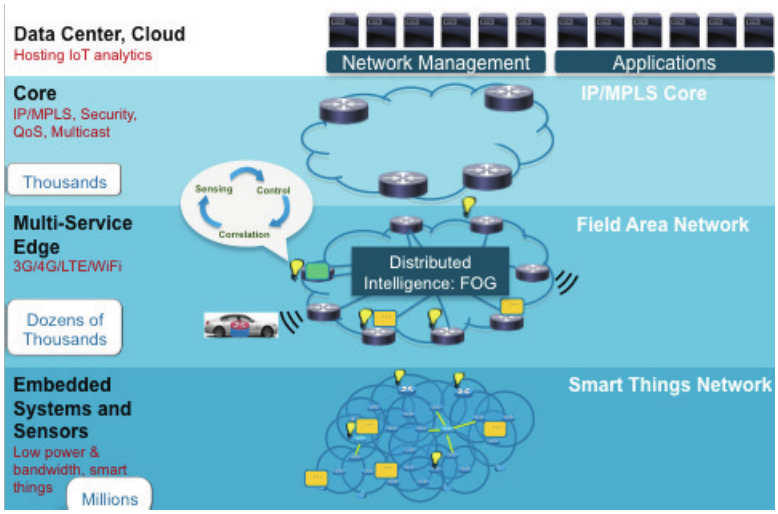

Figure 9: Fog Computing Paradigm [13]

Heterogeneity of resources
Fog nodes come in different form factors, and will be deployed in a wide variety of environments.

Interoperability and federation
In order to support services (such as streaming) requires the cooperation of different providers. Hence, Fog components must be able to interoperate, and services must be federated across domains.

Even though computing, storage and network are resources that characterize both the Cloud that the Fog paradigm, the latter, how we seen, has more specific characteristics that seem to better fit to the requirement of IoT applications. For example, The edge location and location awareness of the fog nodes can better satisfy the need of low latency and the responsiveness of decision processes offloaded to external resources. Moreover, the geographical distribution and the very large number of nodes, in contrast to a centralized Cloud, are characteristics that can be better exploit to support mobility of *things* (through wireless access) for processing their data. However, many applications require both Fog localization, and Cloud globalization, particularly for analysis of Big Data that can require batch processing. Then an interaction between the Fog and the Cloud is often necessary and can bring benefits to the services and applications.

4 Vision and Working Plan

4.1 Main issues summary

As we aforementioned, there is an exponential growth of the connected devices in IoT scenario that produces a proportional growth in the data that have to be stored and processed. Handling the growing of the amount of devices and information produced by them brings the need to have platforms and infrastructures that support different requirements for IoT System. The elastic resource provisioning and the ability to scale are main requirements to deal with this big amount of devices and to face the dynamic nature of IoT systems. Cloud infrastructures can be exploited to ensure such requirements as well as to bring other benefits such as collecting distributed data, remote and real-time data access, pay-per-use model to customers, support for mobility of the devices and ease of delivery and development of the IoT services. Apart these issues briefly summarized, there are some other issues that are important to face in the Cloud and IoT convergence such as security, privacy and reliability in data communication and management of the devices. However, To limit the fields of the research activities we not plan to address these lasts issues.

4.2 Architectural Model

To overcome the issues that arise from the convergence through IoT and Cloud Computing, an efficient solution may be to provide an architecture composed by different layers that exploits multiple cloud infrastructures. This type of architecture allows to have different services for IoT applications deployed on different layers in order to give the right view and knowledge of the particular domain. Having the computational capacity of a cloud infrastructure that can stay close to the devices, or that are in charge to manage a specific subset of them, can brings many benefits to the services that have to deal with them. A cloud infrastructure deployed locally to an IoT system can have location-aware properties that can be exploited to provide service in a more efficient manner. Moreover, stay close to the devices or deal with a restrict number of them can allow to provide an high throughput and a capable bandwidth for guarantee real-time responses. On the other hand, the higher level of such architecture has an overall vision of the devices involved allowing it to have a wide knowledge of the entire infrastructure's domain and to take a more comprehensive decisions leaving to the underlying layers the processes that can be performed locally on a close cloud or those that are more specific to a singles subsets.

A Cloud-IoT architecture that can enable a scenario such the one depicted is showed in fig 10. In this architecture we can identify three major components that are:

- The IoT systems

  In this components we have all the physical objects, machines and devices that can connect to the Internet and produce data or consume services through the network.

- The localized or specialized middleware clouds

  This type of components are geographical distributed cloud infrastructures that serve as a point of liaison between the *things* in the sub-layer and the global centralized cloud. This components can form one of several layers provide different aggregations and different levels of abstractions of IoT Systems in the sub-layers.

- The global cloud

  This is the highest layer that has a global view of all sub-layers. This layer does not handle directly the physical devices but it leverages the middlware clouds as mediators and aggregators.

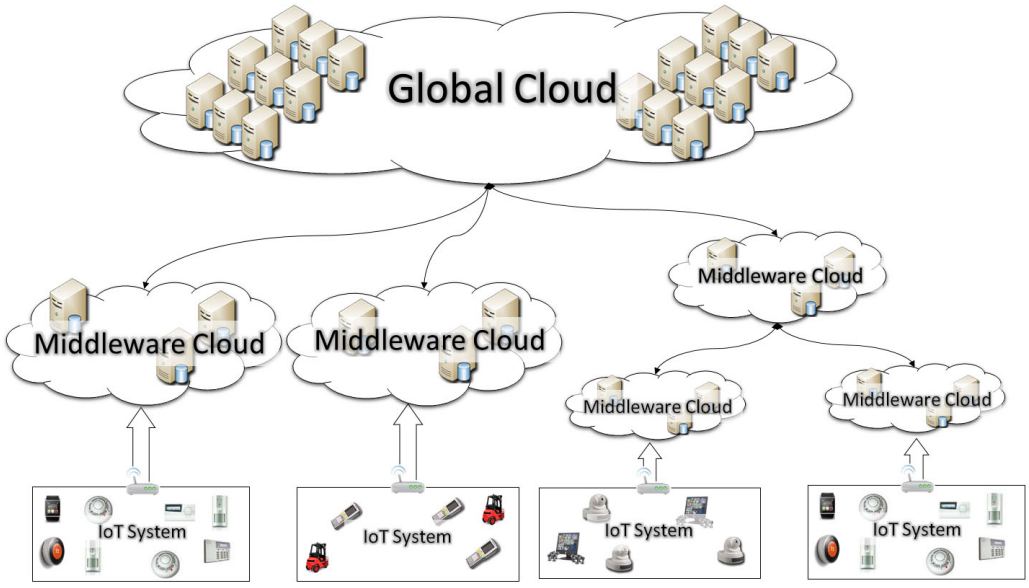

Figure 10: IoT+Cloud hierarchical architecture

Each layer must have the enabling functionalities to provide different kind of services and for this each entity has a different role and different issues that have to be addressed.

This can allow to face problems that is hardly to address using a standard Cloud service deployment. The extremely heterogeneous nature of IoT devices is reflected in their data produced. This data can be noisy or incomplete in many cases, thus, the process of collecting data often need a pre-process phase. The middleware layers of an infrastructure like the one depicted can taking care such pre-process phase in order to aggregate the data collected, for example, to overcome latency problem on the transmission or simply because is useless to collected all the data produced. In other cases the data produced by such simple devices are noisy or incomplete and also need to be pre-processed. Once again, a middleware layer that takes care to perform a cleaning or an enrichment phase enabling a more comprehensive analysis performed in a centralized Cloud.

4.3 Main areas to investigate

Considering the issues that the convergence of Cloud and IoT has highlighted and the architectural model proposed, in the next section we discuss the main interesting areas that have to be further investigate and in which we want to focus the future efforts.

4.3.1 Architectural considerations

The hierarchical service architecture depicted in the previous section needs a further analysis in order to be better modeled. Identify how each component of the architecture can be composed, define their functionalities and responsibilities, modeling the interactions between layers and components and specifies their interfaces are all issues that have to be addressed to give a comprehensive model of this service architecture.

4.3.2 Resource Management and Scheduling

In this context, the allocation of resources is a critical task in each layer and must be addressed considering the particular Quality of Service that a specific layer has to provide. Algorithms that solve commons cloud scheduling problems can suffer from a dimensionality breakdown when the size of the problem grows. Indeed, this problem becomes more challenging in the proposed scenario where Cloud and IoT have to deal with a huge proliferation of the devices and the data that have to be processed.

While many advances have been made in this field, many issues still remain unexplored and could be investigated. For example, scheduling approaches should be smart enough to make real-time responses to a changing environment like the one emerged with the convergence of Cloud and Internet of Things. Most of the existing works in scheduling cloud resources are centralized approaches because they consider the scheduling problem as a whole and find an optimal solution offline. These approaches, indeed, often face difficulties for providing a real-time response to environmental changes and there is a need to investigate in how these approaches can be adapted to face such difficulties. Moreover, another interesting challenge in cloud resource scheduling is that the deployment of cloud resources is often distributed with different data centers or at different locations. This is the case of the interconnected cloud infrastructures depicted in figure 10 in which the distributed nature of its architectures can benefit from a distributed or parallel scheduling. This can be not only useful for scheduling cloud resources among different cloud infrastructures, but is also useful for scheduling different kinds of resources in the same cloud. Finally, real-time and distributed process in scheduling algorithms, or also multi-objectives scheduling, can be investigated to provide an efficient manner to deal with the growing amount of data produced by IoT systems.

4.3.3 Inter-Cloud Interoperability and Portability

In the architecture envisioned cloud-to-cloud communication and intercloud interoperability capabilities have a crucial role. Enabling intercloud interoperability allows data exchange and resource sharing among clouds that can stay at the same layer or can interoperate in a hierarchical way across different layers. As we said, Inter-layer cloud interactions can allow sharing of resources and delegation of some activities that need a different view of the domain while intra-layer cloud interactions enable accommodation of unexpected increases in demands and migration of tasks and applications to enhance resource utilization and support mobility.

Apart for data exchange and resource sharing, there are several other motivations for why enabling interoperability and portability capabilities across different cloud infrastructures is important. First, it can ease the deployment and migration of data across different clouds allow to move consumer data in and out of the cloud. Second, it mitigates the vendor lock-in problem that arises using cloud services providing to the customers the flexibility of selecting, mixing, and changing cloud service providers with minimal effort. Finally, it can add elasticity to service outsourcing by allowing customers

and enterprises to easily move some parts of their applications while hosting other parts locally. This also allows customers to spread their outsourced applications and software across multiple cloud providers, not forcing them to necessarily use just one provider.

Although inter-cloud models and cloud federations have been largely investigated in the recent years, many issues remains to be investigated principally when these models have to deal with the integration of Cloud and IoT. The definition of standards and uniform APIs remains a challenge issue as well as stadardisation of data representation and support for portability of applications. In order to promote the possibility of inter-cloud migration of services and application, the definition of performance metrics and thresholds to quantify if a provider has satisfied the SLA contract and whether migration should be triggered can be investigated. Moreover, the definition of protocols and tools that can be used to select the best provider when a migration of a service is triggered has to be further investigated.

4.3.4 Service Level Agreements and Quality of Service

Another key requirement to enable an architectural model like the one exposed is the ability to allocate and control resources to meet Service Level Agreements of the actors involved.

In cloud computing, SLAs are viewed as contractual obligation metrics introduced to define the minimum required service levels and the resolution policies that has to be followed when providers fail to satisfy certain parameters negotiated with the customers. Examples of SLAs include VM availability, CPU performance, bandwidth guarantee, data format, localization of storage and computing resources and level of security assurance.

This requires a further investigation about mechanisms that enable resources usage monitoring and admission control in order to guarantee the fulfillment of contracted SLAs. In order to guarantee the SLAs can be necessary to model protocols and procedures that report resource usage to service providers and customers.

Finally, considering a scenario that is focused to enabling the architecture proposed others issues had to be addressed. Firstly, there isn't a clear split of roles among the layers and we must investigate which layer can be taking care of QoS assurance, SLAs satisfaction or negotiation process. Secondly, existing techniques, for instance from the cloud computing area, are to be revisited for ensuring the integration of SLAs aspects in resource allocation mechanisms, taking into account inter- and intra-layer interoperability.

4.4 Working Plan

In this thesis we plan to investigate the problem of defining in a more concrete way a software architecture such the one abstractly depicted that will be general enough to be exploited by different classes of applications in IoT domain.

This implies a comprehensive analysis of the variety of real IoT application domains, both from the literature and industrial solution. This process will be aimed at determining classes of abstract issues derived from use cases. These classes need to be identified and defined in order to analyze their characteristic requirements. The analysis of these requirements will allow to better understand which features each layers has to provide and how they can be composed. We plan to further progress in the architecture refinement process considering the components associated with layers and defining their characteristics and the interactions among them.

In the refinement process we plan to considers all the the open issues we previously discussed, e.g. scalability, elasticity, resources management, inter-cloud interoperability etc. We will also need to identify, analyze and choose the technological or theoretical tools that are needed to address such issues.

Finally, a phase of evaluation and analysis is needed and can be performed in different ways depending on the available platforms. The possibilities are:

- An experimental evaluation of the architectural model through the exploitation of existing real testbeds. It should be interesting to find companies having a real IoT testbed that are interested in the evaluation of this type software architecture to start a collaboration with them.
- To exploit some existing research testbeds that can be find in literature [22].
- To evaluate the architectural model exploiting some simulation environments, which have to be identified.
- To follow an hybrid approach that combines company or open testbeds with some simulators.

References

[1] an open-source LISP implementation for Linux, Android and OpenWRT. http://lispmob.org/, 2015.

[2] Internet Of Things - ThingSpeak. https://thingspeak.com/, 2015.

[3] IoTCloud: Open source iot cloud project. https://sites.google.com/site/opensourceiotcloud, 2015.

[4] NimBits. http://www.nimbits.com/, 2015.

[5] OpenIoT: Open source cloud solution for the internet of things. http://openiot.eu/, 2015.

[6] Open.Sen.se. http://open.sen.se/, 2015.

[7] Xively: Internet of thing platform connecting devices and app for real-time control and data storage. http://xively.com/, 2015.

[8] Mohammad Aazam, Imran Khan, Aymen Abdullah Alsaffar, and Eui-Nam Huh. Cloud of things: Integrating internet of things and cloud computing and the issues involved. In *Applied Sciences and Technology (IBCAST), 2014 11th International Bhurban Conference on*, pages 414–419. IEEE, 2014.

[9] Ali Ziya Alkar and Umit Buhur. An internet based wireless home automation system for multifunctional devices. *Consumer Electronics, IEEE Transactions on*, 51(4):1169–1174, 2005.

[10] Luigi Atzori, Antonio Iera, and Giacomo Morabito. The internet of things: A survey. *Computer networks*, 54(15):2787–2805, 2010.

[11] Pieter Ballon, Julia Glidden, Pavlos Kranas, Andreas Menychtas, Susie Ruston, and Shenja Van Der Graaf. Is there a need for a cloud platform for european smart cities? In *eChallenges e-2011 Conference Proceedings, IIMC International Information Management Corporation*, 2011.

[12] P. Banerjee, R. Friedrich, C. Bash, P. Goldsack, B.A. Huberman, J. Manley, C. Patel, P. Ranganathan, and A. Veitch. Everything as a service: Powering the new information economy. *Computer*, 44(3):36–43, March 2011.

[13] Flavio Bonomi, Rodolfo Milito, Jiang Zhu, and Sateesh Addepalli. Fog computing and its role in the internet of things. In *Proceedings of the first edition of the MCC workshop on Mobile cloud computing*, pages 13–16. ACM, 2012.

[14] Alessio Botta, Walter de Donato, Valerio Persico, and Antonio Pescapé. On the integration of cloud computing and internet of things. In *Future Internet of Things and Cloud (FiCloud), 2014 International Conference on*, pages 23–30. IEEE, 2014.

[15] Mike Botts, George Percivall, Carl Reed, and John Davidson. Ogc® sensor web enablement: Overview and high level architecture. In *GeoSensor networks*, pages 175–190. Springer, 2008.

[16] Rajkumar Buyya, Rajiv Ranjan, and Rodrigo N Calheiros. Intercloud: Utility-oriented federation of cloud computing environments for scaling of application services. In *Algorithms and architectures for parallel processing*, pages 13–31. Springer, 2010.

[17] Adam Chlipala, Jonathan Hui, and Gilman Tolle. Deluge: data dissemination for network reprogramming at scale. *University of California, Berkeley, Tech. Rep*, 2004.

[18] European Commision. *Definition of a research and innovation policy leveraging Cloud Computing and IoT combination.* Tender specification, SMART 2013/0037, 2013.

[19] Mohsen Darianian and Martin Peter Michael. Smart home mobile rfid-based internet-of-things systems and services. In *Advanced Computer Theory and Engineering, 2008. ICACTE'08. International Conference on*, pages 116–120. IEEE, 2008.

[20] Tharam Dillon, Chen Wu, and Elizabeth Chang. Cloud computing: issues and challenges. In *Advanced Information Networking and Applications (AINA), 2010 24th IEEE International Conference on*, pages 27–33. Ieee, 2010.

[21] M Fazio, A Celesti, A Puliafito, and M Villari. Big data storage in the cloud for smart environment monitoring. *Procedia Computer Science*, 52:500–506, 2015.

[22] Alexander Gluhak, Srdjan Krco, Michele Nati, Dennis Pfisterer, Nathalie Mitton, and Tahiry Razafindralambo. A survey on facilities for

experimental internet of things research. *Communications Magazine, IEEE*, 49(11):58–67, 2011.

[23] Jayavardhana Gubbi, Rajkumar Buyya, Slaven Marusic, and Marimuthu Palaniswami. Internet of things (iot): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, 29(7):1645–1660, 2013.

[24] IETF. Routing over low power and lossy networks (roll). `https://datatracker.ietf.org/wg/roll/charter/`, 2015.

[25] Lihong Jiang, Li Da Xu, Hongming Cai, Zuhai Jiang, Fenglin Bu, and Boyi Xu. An iot-oriented data storage framework in cloud computing platform. *Industrial Informatics, IEEE Transactions on*, 10(2):1443–1451, 2014.

[26] Ari Juels. Rfid security and privacy: A research survey. *Selected Areas in Communications, IEEE Journal on*, 24(2):381–394, 2006.

[27] Fei Li, Michael Vögler, Markus Claeßens, and Schahram Dustdar. Efficient and scalable iot service delivery on cloud. In *Cloud Computing (CLOUD), 2013 IEEE Sixth International Conference on*, pages 740–747. IEEE, 2013.

[28] Xu Li, Rongxing Lu, Xiaohui Liang, Xuemin Shen, Jiming Chen, and Xiaodong Lin. Smart community: an internet of things application. *Communications Magazine, IEEE*, 49(11):68–75, 2011.

[29] Haiyan Luo, Haiyan Luo Ci, Dalei Wu, Nicholas Stergiou, and Ka-Chun Siu. A remote markerless human gait tracking for e-healthcare based on content-aware wireless multimedia communications. *Wireless Communications, IEEE*, 17(1):44–50, 2010.

[30] Peter Mell and Tim Grance. The nist definition of cloud computing. *National Institute of Standards and Technology*, 53(6):50, 2009.

[31] Nathalie Mitton, Symeon Papavassiliou, Antonio Puliafito, and Kishor S Trivedi. Combining cloud and sensors in a smart city environment. *EURASIP journal on Wireless Communications and Networking*, 2012(1):1–10, 2012.

[32] Gerhard Nussbaum. People with disabilities: assistive homes and environments. In *Computers Helping People with Special Needs*, pages 457–460. Springer, 2006.

[33] George Suciu, Alexandru Vulpe, Simona Halunga, Octavian Fratu, Gheorghe Todoran, and Victor Suciu. Smart cities built on resilient cloud computing and secure internet of things. In *Control Systems and Computer Science (CSCS), 2013 19th International Conference on*, pages 513–518. IEEE, 2013.

[34] Harald Sundmaeker, Patrick Guillemin, Peter Friess, and Sylvie Woelfflé, editors. *Vision and Challenges for Realising the Internet of Things*. Publications Office of the European Union, Luxembourg, 2010.

[35] Rolf H Weber. Internet of things–need for a new legal environment? *Computer law & security review*, 25(6):522–527, 2009.

[36] Madoka Yuriyama and Takayuki Kushida. Sensor-cloud infrastructure-physical sensor management with virtualized sensors on cloud computing. In *Network-Based Information Systems (NBiS), 2010 13th International Conference on*, pages 1–8. IEEE, 2010.