3

Internet of Things beyond the Hype: Research, Innovation and Deployment

Ovidiu Vermesan[1], Peter Friess[2], Patrick Guillemin[3], Raffaele Giaffreda[4], Hanne Grindvoll[1], Markus Eisenhauer[5], Martin Serrano[6], Klaus Moessner[7], Maurizio Spirito[8], Lars-Cyril Blystad[1] and Elias Z. Tragos[9]

[1]SINTEF, Norway
[2]European Commission, Belgium
[3]ETSI, France
[4]CREATE-NET, Italy
[5]Fraunhofer FIT, Germany
[6]National University of Ireland Galway, Ireland
[7]University of Surrey, UK
[8]ISMB, Italy
[9]FORTH, Greece

"There's a way to do it better. Find it." Thomas Edison

3.1 Internet of Things Vision

Internet of Things (IoT) is a concept and a paradigm that considers pervasive presence in the environment of a variety of things/objects that through wireless and wired connections and unique addressing schemes are able to interact with each other and cooperate with other things/objects to create new applications/services and reach common goals. In this context the research and development challenges to create a smart world are enormous. A world where the real, digital and the virtual are converging to create smart environments that make energy, transport, cities and many other areas more intelligent. The goal of the Internet of Things is to enable things to be connected anytime, anyplace, with anything and anyone ideally using any path/network and any service. Internet of Things is a new revolution of the Internet. Objects

make themselves recognizable and they obtain intelligence by making or enabling context related decisions thanks to the fact that they can communicate information about themselves and they can access information that has been aggregated by other things, or they can be components of complex services [71].

The various layers of the IoT value chain cover several distinct product or service categories. Sensors provide much of the data gathering, actuators act, radios/communications chips provide the underlying connectivity, microcontrollers provide the processing of that data, modules combine the radio, sensor and microcontroller, combine it with storage, and make it "insertable" into a device. Platform software provides the underlying management and billing capabilities of an IoT network, while application software presents all the information gathered in a usable and analysable format for end users. The underlying telecom infrastructure (usually wireless spectrum) provides the means of transporting the data while a service infrastructure needs to be created for the tasks of designing, installing, monitoring and servicing the IoT deployment. Companies will compete at one layer of the IoT value chain, while many will create solutions from multiple layers and functionally compete in a more vertically integrated fashion. [42].

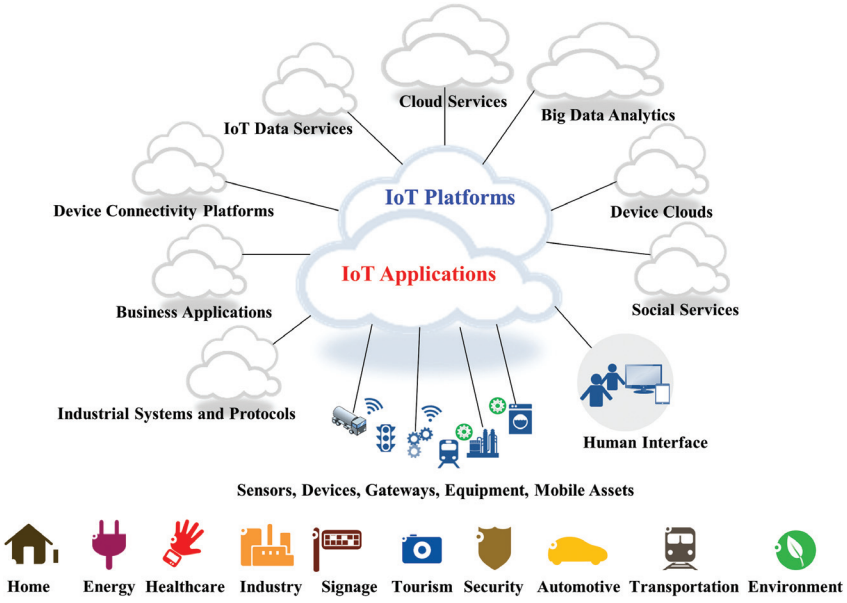

Figure 3.1 Internet of Things Integration.

The Internet of Things makes use of synergies that are generated by the convergence of Consumer, Business and Industrial Internet. The convergence creates the open, global network connecting people, data, and things. This convergence leverages the cloud to connect intelligent things that sense and transmit a broad array of data, helping creating services that would not be obvious without this level of connectivity and analytical intelligence. The use of platforms is being driven by transformative technologies such as cloud, things, and mobile. The Internet of Things and Services makes it possible to create networks incorporating the entire manufacturing process that convert factories into a smart environment. The cloud enables a global infrastructure to generate new services, allowing anyone to create content and applications for global users. Networks of things connect things globally and maintain their identity online. Mobile networks allow connection to this global infrastructure anytime, anywhere. The result is a globally accessible network of things, users, and consumers, who are available to create businesses, contribute content, generate and purchase new services.

Platforms also rely on the power of network effects, as they allow more things, they become more valuable to the other things and to users that make use of the services generated. The success of a platform strategy for IoT can be determined by connection, attractiveness and knowledge/information/data flow.

The Alliance for Internet of Things Innovation (AIOTI) was recently initiated by the European Commission in order to develop and support the dialogue and interaction among the Internet of Things (IoT) various players. The overall goal of the establishment of the AIOTI is the creation of a dynamic European IoT ecosystem to unleash the potentials of the IoT.

The AIOTI will assist the European Commission in the preparation of future IoT research as well as innovation and standardisation policies. It is also going to play an essential role in the designing of IoT Large Scale Pilots, which will be funded by the Horizon 2020 Research and Innovation Programme. The members of AIOTI will jointly work on the creation of a dynamic European IoT ecosystem. This ecosystem is going to build on the work of the IoT Research Cluster (IERC) and spill over innovation across industries and business sectors of IoT transforming ideas to IoT solutions.

The European Commission (EC) considers that IoT will be pivotal in enabling the digital single market, through new products and services. The IoT, big data, cloud computing and their related business models will be the three most important drivers of the digital economy, and in this context it is

fundamental for a fully functional single market in Europe to address aspects of ownership, access, privacy and data flow – the new production factor.

New generations of networks, IoT and cloud computing are also vectors of industrial strategy. The IoT stakeholders are creating a new ecosystem that cuts across vertical areas, in convergence between the physical and digital words. It combines connectivity, data generation, processing and analytics, with actuation and new interfaces, resulting in new products and services based on platforms and software and apps.

Internet of Things developments implies that the environments, cities, buildings, vehicles, clothing, portable devices and other objects have more and more information associated with them and/or the ability to sense, communicate, network and produce new information. In addition the network technologies have to cope with the new challenges such as very high data rates, dense crowds of users, low latency, low energy, low cost and a massive number of devices. Wireless connectivity anywhere, anytime and between every-body and every-thing (smart houses, vehicles, cities, offices etc.) is gaining momentum, rendering our daily lives easier and more efficient. This momentum will continue to rise, resulting in the need to enable wireless connections between people, machines, communities, physical things, processes, content etc. anytime, in flexible, reliable and secure ways. The air interfaces for 2G, 3G, and 4G were all designed for specific use cases with certain KPIs in mind (throughput, capacity, dropped/blocked call rates etc.). However, the emerging trend of connecting everything to the Internet (IoT and Internet of Vehicles, IoV) brings up the need to go beyond such an approach. The inclusion of the above mentioned use cases pose new challenges due to the broader range of service and device classes, ranging from IoT to short range Mobile Broadband (MBB) communications (e.g. WiFi) and from high-end smartphone to low-end sensor. Furthermore, each service type/device class has more stringent requirements than ever (e.g. air interface latency in the order of 1ms) and some of these requirements are conflicting (e.g. to support very low latencies, energy and resource efficiency may not be optimal). So, the challenge is not only to increase the user rates or the capacity (as has always been so far) but also to master the heterogeneity and the trade-off between the conflicting requirements as presented in Figure 3.2 [3].

As the Internet of Things becomes established in smart factories, both the volume and the level of detail of the corporate data generated will increase. Moreover, business models will no longer involve just one company, but will instead comprise highly dynamic networks of companies and completely new value chains. Data will be generated and transmitted autonomously by

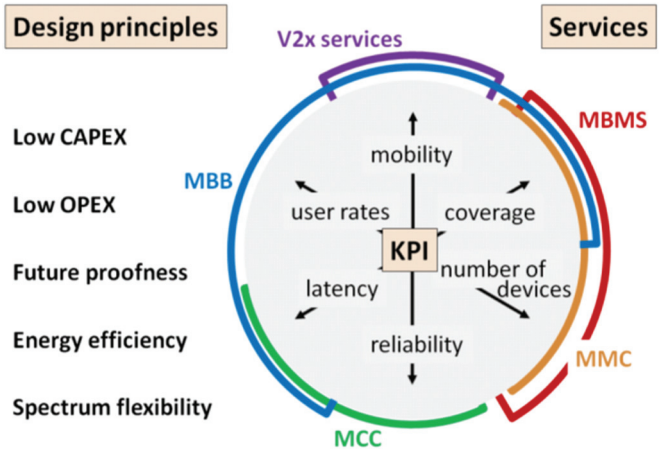

Figure 3.2 Design principles, services and related KPIs [3].

smart machines and these data will inevitably cross company boundaries. A number of specific dangers are associated with this new context – for example, data that were initially generated and exchanged in order to coordinate manufacturing and logistics activities between different companies could, if read in conjunction with other data, suddenly provide third parties with highly sensitive information about one of the partner companies that might, for example, give them an insight into its business strategies. New instruments will be required if companies wish to pursue the conventional strategy of keeping such knowledge secret in order to protect their competitive advantage. New, regulated business models will also be necessary – the raw data that are generated may contain information that is valuable to third parties and companies may therefore wish to make a charge for sharing them. Innovative business models like this will also require legal safeguards (predominantly in the shape of contracts) in order to ensure that the value added created is shared out fairly, e.g. through the use of dynamic pricing models [56].

3.1.1 Internet of Things Common Definition

The IoT is a key enabling technology for digital businesses. Approximately 3.9 billion connected things were in use in 2014 and this figure is expected to rise to 25 billion by 2020. Gartner's top 10 strategy technology trends [55] cover three themes: the merging of the real and virtual worlds, the advent of intelligence everywhere, and the technology impact of the digital business shift.

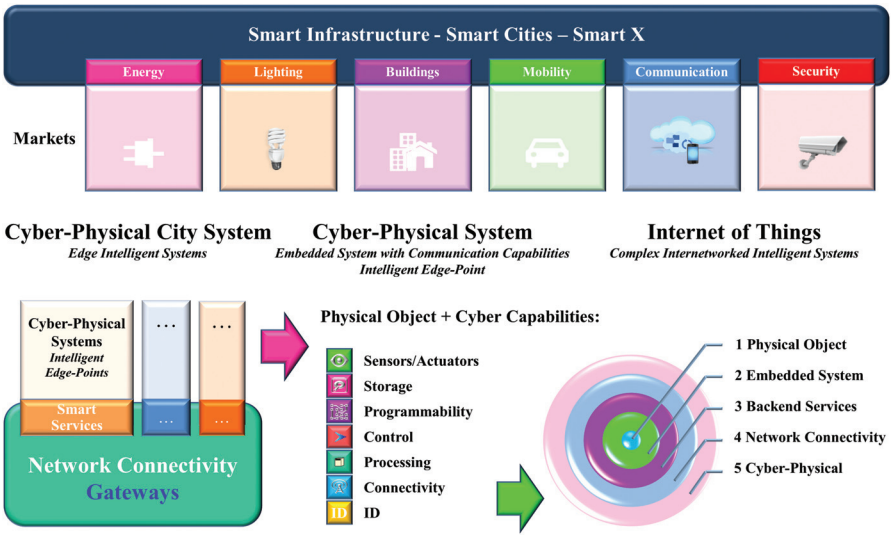

Figure 3.3 Cyber-physical sytems as building blocks of IoT applications.

The traditional distinction between network and device is starting to blur as the functionalities of the two become indistinguishable. Shifting the focus from the IoT network to the devices costs less, scales more gracefully, and leads to immediate revenues.

The systemic nature of innovation requires the need for coordination stakeholders, systems and services in interaction-intensive environments with a permanent and seamless mix of online and real-world experiences and offerings, as the IoT will consist of countless cyber-physical systems (CPS). The overlay of virtual and physical will be enabled by layered and augmented reality interfaces for interconnected things, smartphones, wearables, industrial equipment, which will exchange continuous data via edge sensor/actuator networks and context-aware applications using ubiquitous connectivity and computing by integrating technologies such as cloud edge cloud/fog and mobile. In this context the IoT applications will have real time access to intelligence about virtual and physical processes and events by open, linked and smart data.

Gartner [54, 55] identifies that the combination of data streams and services created by digitizing everything creates four basic usage models:

- Manage
- Monetize

- Operate
- Extend.

These can be applied to people, things, information, and places, and therefore the so called "Internet of Things" will be succeeded by the "Internet of Everything."

In this context the notion of network convergence using IP is fundamental and relies on the use of a common multi-service IP network supporting a wide range of applications and services.

Figure 3.4 The top 10 strategic technology trends for 2015 [55].

The Internet of Things is not a single technology, it's a concept in which most new things are connected and enabled such as street lights being networked and things like embedded sensors, image recognition functionality, augmented reality, near field communication are integrated into situational decision support, asset management and new services. These bring many business opportunities and add to the complexity of IT [52].

To accommodate the diversity of the IoT, there is a heterogeneous mix of communication technologies, which need to be adapted in order to address the needs of IoT applications such as energy efficiency, security, and reliability. In this context, it is possible that the level of diversity will be scaled to a number a manageable connectivity technologies that address the needs of the IoT applications, are adopted by the market, they have already proved to be serviceable, supported by a strong technology alliance.

The Internet of Things provides solutions based on the integration of information technology, which refers to hardware and software used to store, retrieve, and process data and communications technology which includes electronic systems used for communication between individuals or groups. The rapid convergence of information and communications technology is taking place at three layers of technology innovation: the cloud, data and communication pipes/networks and device [44].

IoT will rearrange the tech landscape, again. IoT has key attributes that distinguish it from the "regular" Internet, as captured by the S-E-N-S-E framework presented in Figure 3.5. These attributes may tilt the direction of technology development and adoption, with significant implications for Tech companies, much like the transition from the fixed to the mobile Internet shifted the centre of gravity among the different actors in the value chain.

S-E-N-S-E	What the Internet of Things does	How it differs from the Internet
Sensing	*Leverages sensors attached to things (e.g. temperature, pressure, acceleration)*	*More data is generated by things with sensors than by people*
Efficient	*Adds intelligence to manual processes (e.g. reduce power usage on hot days)*	*Extends the Internet's productivity gains to things, not just people*
Networked	*Connects objects to the network (e.g. thermostats, vehicles, watches)*	*Some of the intelligence shifts from the cloud to the network's edge ("fog" computing)*
Specialized	*Customizes technology and process to specific verticals (e.g. healthcare, retail, oil)*	*Unlike the broad horizontal reach of PCs and smartphones, the IoT is very fragmented*
Everywhere	*Deployed pervasively (e.g. on the human body, in cars, homes, cities, factories)*	*Ubiquitous presence, resulting in an order of magnitude more devices and even greater security concerns*

Figure 3.5 Making S-E-N-S-E of the Internet of Things (Source: Goldman Sachs Global Investment Research).

The synergy of the access and potential data exchange opens huge new possibilities for IoT applications. Already over 50% of Internet connections are between or with things.

By 2020, over 30 billion connected things, with over 200 billion with intermittent connections are forecast. Key technologies here include embedded sensors, image recognition and NFC. By 2015, in more than 70% of enterprises, a single executable will oversee all Internet connected things. This becomes the Internet of Everything [53].

As a result of this convergence, the IoT applications require that classical industries are adapting and the technology will create opportunities for new industries to emerge and to deliver enriched and new user experiences and services.

In addition, to be able to handle the sheer number of things and objects that will be connected in the IoT, cognitive technologies and contextual intelligence are crucial. This also applies for the development of context aware applications that need to be reaching to the edges of the network through smart devices that are incorporated into our everyday life.

The Internet is not only a network of computers, but it has evolved into a network of devices of all types and sizes, vehicles, smartphones, home appliances, toys, cameras, medical instruments and industrial systems, all connected, all communicating and sharing information all the time.

The Internet of Things had until recently different means at different levels of abstractions through the value chain, from lower level semiconductor through the service providers.

The Internet of Things is a "global concept" and requires a common definition. Considering the wide background and required technologies, from sensing device, communication subsystem, data aggregation and pre-processing to the object instantiation and finally service provision, generating an unambiguous definition of the "Internet of Things" is non-trivial.

The IERC is actively involved in ITU-T Study Group 13, which leads the work of the International Telecommunications Union (ITU) on standards for next generation networks (NGN) and future networks and has been part of the team which has formulated the following definition [67]: "***Internet of things (IoT)****: A 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. NOTE 1 – Through the exploitation of identification, data capture, processing and communication capabilities, the IoT makes full use of things to offer services to all kinds of applications, whilst ensuring*

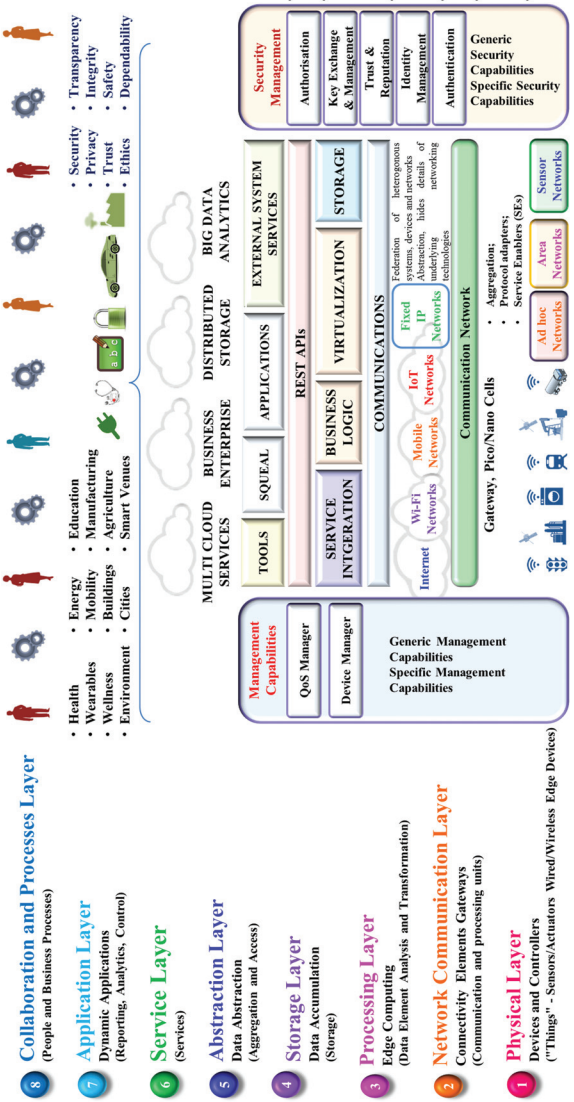

Figure 3.6 IoT Architectural View.

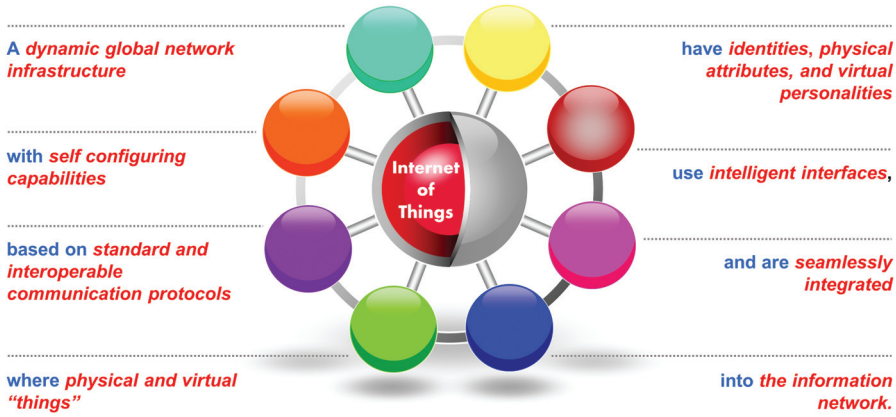

Figure 3.7 IoT Definition [70].

that security and privacy requirements are fulfilled. NOTE 2 – From a broader perspective, the IoT can be perceived as a vision with technological and societal implications."

The IERC definition [70] states that IoT is *"A dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols where physical and virtual "things" have identities, physical attributes, and virtual personalities and use intelligent interfaces, and are seamlessly integrated into the information network."*.

3.2 IoT Strategic Research and Innovation Directions

The development of enabling technologies such as nanoelectronics, communications, sensors, smart phones, embedded systems, cloud networking, network virtualization and software will be essential to provide to things the capability to be connected all the time everywhere. This will also support important future IoT product innovations affecting many different industrial sectors. Some of these technologies such as embedded or cyber-physical systems form the edges of the "Internet of Things" bridging the gap between cyber space and the physical world of real "things", and are crucial in enabling the "Internet of Things" to deliver on its vision and become part of bigger systems in a world of "systems of systems".

The final report of the Key Enabling Technologies (KET), of the High-Level Expert Group [45] identified the enabling technologies, crucial to many of the existing and future value chains of the European economy:

- Nanotechnologies
- Micro and Nano electronics
- Photonics
- Biotechnology
- Advanced Materials
- Advanced Manufacturing Systems

As such, IoT creates intelligent applications that are based on the supporting KET's identified, as IoT applications address smart environments either physical or at cyber-space level, and in real time.

To this list of key enablers, we can add the global deployment of IPv6 across the World enabling a global and ubiquitous addressing of any communicating smart thing.

From a technology perspective, the continuous increase in the integration density proposed by Moore's Law was made possible by a dimensional scaling: in reducing the critical dimensions while keeping the electrical field constant, one obtained at the same time a higher speed and a reduced power consumption of a digital MOS circuit: these two parameters became driving forces of the microelectronics industry along with the integration density.

The International Technology Roadmap for Semiconductors has emphasized in its early editions the "miniaturization" and its associated benefits in terms of performances, the traditional parameters in Moore's Law. This trend for increased performances will continue, while performance can always be traded against power depending on the individual application, sustained by the incorporation into devices of new materials, and the application of new transistor concepts. This direction for further progress is labelled "More Moore".

The second trend is characterized by functional diversification of semiconductor-based devices. These non-digital functionalities do contribute to the miniaturization of electronic systems, although they do not necessarily scale at the same rate as the one that describes the development of digital functionality. Consequently, in view of added functionality, this trend may be designated "More-than-Moore" [48].

Mobile data traffic is projected to double each year between now and 2015 and mobile operators will find it increasingly difficult to provide the

bandwidth requested by customers. In many countries there is no additional spectrum that can be assigned and the spectral efficiency of mobile networks is reaching its physical limits. Proposed solutions are the seamless integration of existing Wi-Fi networks into the mobile ecosystem. This will have a direct impact on Internet of Things ecosystems. The chips designed to accomplish this integration are known as "multicom" chips. Wi-Fi and baseband communications are expected to converge and the architecture of mobile devices is likely to change and the baseband chip is expected to take control of the routing so the connectivity components are connected to the baseband or integrated in a single silicon package. As a result of this architecture change, an increasing share of the integration work is likely done by baseband manufacturers (ultra -low power solutions) rather than by handset producers.

Today many European projects and initiatives address Internet of Things technologies and knowledge. Given the fact that these topics can be highly diverse and specialized, there is a strong need for integration of the individual results. Knowledge integration, in this context is conceptualized as the process through which disparate, specialized knowledge located in multiple projects across Europe is combined, applied and assimilated.

The Strategic Research and Innovation Agenda (SRIA) is the result of a discussion involving the projects and stakeholders involved in the IERC activities, which gather the major players of the European ICT landscape addressing IoT technology priorities that are crucial for the competitiveness of European industry.

IERC Strategic Research and Innovation Agenda covers the important issues and challenges for the Internet of Things technology. It provides the vision and the roadmap for coordinating and rationalizing current and future research and development efforts in this field, by addressing the different enabling technologies covered by the Internet of Things concept and paradigm.

Many other technologies are converging to support and enable IoT applications. These technologies are summarised as:

- IoT architecture
- Identification
- Communication
- Networks technology
- Network discovery
- Software and algorithms

- Hardware technology
- Data and signal processing
- Discovery and search engine
- Network management
- Power and energy storage
- Security, trust, dependability and privacy
- Interoperability
- Standardization

The Strategic Research and Innovation Agenda is developed with the support of a European-led community of interrelated projects and their stakeholders, dedicated to the innovation, creation, development and use of the Internet of Things technology.

Since the release of the first version of the Strategic Research and Innovation Agenda, we have witnessed active research on several IoT topics. On the one hand this research filled several of the gaps originally identified in the Strategic Research and Innovation Agenda, whilst on the other it created new challenges and research questions. Recent advances in areas such as cloud computing, cyber-physical systems, autonomic computing, and social networks have changed the scope of the Internet of Thing's convergence even more so. The Cluster has a goal to provide an updated document each year that records the relevant changes and illustrates emerging challenges. The updated release of this Strategic Research and Innovation Agenda builds incrementally on previous versions [70, 71, 92, 93] and highlights the main research topics that are associated with the development of IoT enabling technologies, infrastructures and applications with an outlook towards 2020 [82].

The research items introduced will pave the way for innovative applications and services that address the major economic and societal challenges underlined in the EU 2020 Digital Agenda [83].

The IERC Strategic Research and Innovation Agenda is developed incrementally based on its previous versions and focus on the new challenges being identified in the last period.

The updated release of the Strategic Research and Innovation Agenda is highlighting the main research topics that are associated with the development of IoT infrastructures and applications, with an outlook towards 2020 [82].

The timeline of the Internet of Things Strategic Research and Innovation Agenda covers the current decade with respect to research and the following years with respect to implementation of the research results. Of course,

as the Internet and its current key applications show, we anticipate unexpected trends will emerge leading to unforeseen and unexpected development paths.

The Cluster has involved experts working in industry, research and academia to provide their vision on IoT research challenges, enabling technologies and the key applications, which are expected to arise from the current vision of the Internet of Things.

The IoT Strategic Research and Innovation Agenda covers in a logical manner the vision, the technological trends, the applications, the technology enablers, the research agenda, timelines, priorities, and finally summarises in two tables the future technological developments and research needs.

The field of the Internet of Things is based on the paradigm of supporting the IP protocol to all edges of the Internet and on the fact that at the edge of the network many (very) small devices are still unable to support IP protocol stacks. This means that solutions centred on minimum Internet of Things devices are considered as an additional Internet of Things paradigm *without IP to all access edges*, due to their importance for the development of the field.

3.2.1 IoT Applications and Deployment Scenarios

The IERC vision is that "the major objectives for IoT are the creation of smart environments/spaces and self-aware things (for example: smart transport, products, cities, buildings, rural areas, energy, health, living, etc.) for climate, food, energy, mobility, digital society and health applications" [70].

The outlook for the future is the emerging of a network of interconnected uniquely identifiable objects and their virtual representations in an Internet alike structure that is positioned over a network of interconnected computers allowing for the creation of a new platform for economic growth.

Smart is the new green as defined by Frost & Sullivan [49] and the green products and services will be replaced by smart products and services. Smart products have a real business case, can typically provide energy and efficiency savings of up to 30 per cent, and generally deliver a two- to three-year return on investment. This trend will help the deployment of Internet of Things applications and the creation of smart environments and spaces.

At the city level, the integration of technology and quicker data analysis will lead to a more coordinated and effective civil response to security

and safety (law enforcement and blue light services); higher demand for outsourcing security capabilities.

At the building level, security technology will be integrated into systems and deliver a return on investment to the end-user through leveraging the technology in multiple applications (HR and time and attendance, customer behaviour in retail applications etc.).

There will be an increase in the development of "Smart" vehicles which have low (and possibly zero) emissions. They will also be connected to infrastructure. Additionally, auto manufacturers will adopt more use of "Smart" materials.

The key focus will be to make the city smarter by optimizing resources, feeding its inhabitants by urban farming, reducing traffic congestion, providing more services to allow for faster travel between home and various destinations, and increasing accessibility for essential services. It will become essential to have intelligent security systems to be implemented at key junctions in the city. Various types of sensors will have to be used to make this a reality. Sensors are moving from "smart" to "intelligent".

Figure 3.8 IoT applications for integration of different vertical sectors.

Wastewater treatment plants will evolve into bio-refineries. New, innovative wastewater treatment processes will enable water recovery to help close the growing gap between water supply and demand.

Self-sensing controls and devices will mark new innovations in the Building Technologies space. Customers will demand more automated, self-controlled solutions with built in fault detection and diagnostic capabilities.

Development of smart implantable chips that can monitor and report individual health status periodically will see rapid growth.

Smart pumps and smart appliances/devices are expected to be significant contributors towards efficiency improvement. Process equipment with in built "smartness" to self-assess and generate reports on their performance, enabling efficient asset management, will be adopted.

The Industrial Internet starts with embedding sensors and other advanced instrumentation in an array of machines from the simple to the highly complex. This allows the collection and analysis of an enormous amount of data, which can be used to improve machine performance, and inevitably the efficiency of the systems and networks that link them. Even the data itself can become "intelligent," instantly knowing which users it needs to reach.

Consumer IoT is essentially wireless, while the industrial IoT has to deal with an installed base of millions of devices that could potentially become part of this network (many legacy systems installed before IP deployment). These industrial objects are linked by wires that provides the reliable communications needed. The industrial IoT has to consider the legacy using specialised protocols, including Lonworks, DeviceNet, Profibus and CAN and they will be connected into this new network of networks through gateways.

The automation and management of asset-intensive enterprises will be transformed by the rise of the IoT, Industry 4.0, or simply Industrial Internet. Compared with the Internet revolution, many product and asset management solutions have laboured under high costs and poor connectivity and performance. This is now changing. New high-performance systems that can support both Internet and Cloud connectivity as well as predictive asset management are reaching the market. New cloud computing models, analytics, and aggregation technologies enable broader and low cost application of analytics across these much more transparent assets. These developments have the potential to radically transform products, channels, and company business models. This will create disruptions in the business and opportunities for all types of organizations – OEMs, technology

suppliers, system integrators, and global consultancies. There may be the opportunity to overturn established business models, with a view toward answering customer pain points and also growing the market in segments that cannot be served economically with today's offerings. Mobility, local diagnostics, and remote asset monitoring are important components of these new solutions, as all market participants need ubiquitous access to their assets, applications, and customers. Real-time mobile applications support EAM, MRO, inventory management, inspections, workforce management, shop floor interactions, facilities management, field service automation, fleet management, sales and marketing, machine-to-machine (M2M), and many others [57].

In this context the concept of Internet of Energy requires web based architectures to readily guarantee information delivery on demand and to change the traditional power system into a networked Smart Grid that is largely automated, by applying greater intelligence to operate, enforce policies, monitor and self-heal when necessary. This requires the integration and interfacing of the power grid to the network of data represented by the Internet, embracing energy generation, transmission, delivery, substations, distribution control, metering and billing, diagnostics, and information systems to work seamlessly and consistently.

The concept enables the ability to produce, store and efficiently use energy, while balancing the supply/demand by using a cognitive Internet of Energy that harmonizes the energy grid by processing the data, information and knowledge via the Internet. The Internet of Energy concept leverages on the information highway provided by the Internet to link devices and services with the distributed smart energy grid that is the highway for renewable energy resources allowing stakeholders to use green technologies and sell excess energy back to the utility. The concept has the energy management element in the centre of the communication and exchange of data and energy.

The Smart-X environments are implemented using CPS building blocks integrated into Internet of X applications connected through the Internet and enabling seamless and secure interactions and cooperation of intelligent embedded systems over heterogeneous communication infrastructures.

It is expected that this "development of smart entities will encourage development of the novel technologies needed to address the emerging challenges of public health, aging population, environmental protection and climate change, conservation of energy and scarce materials, enhancements to safety and security and the continuation and growth of economic prosperity." The IoT applications are further linked with Green ICT, as the IoT will drive energy-efficient

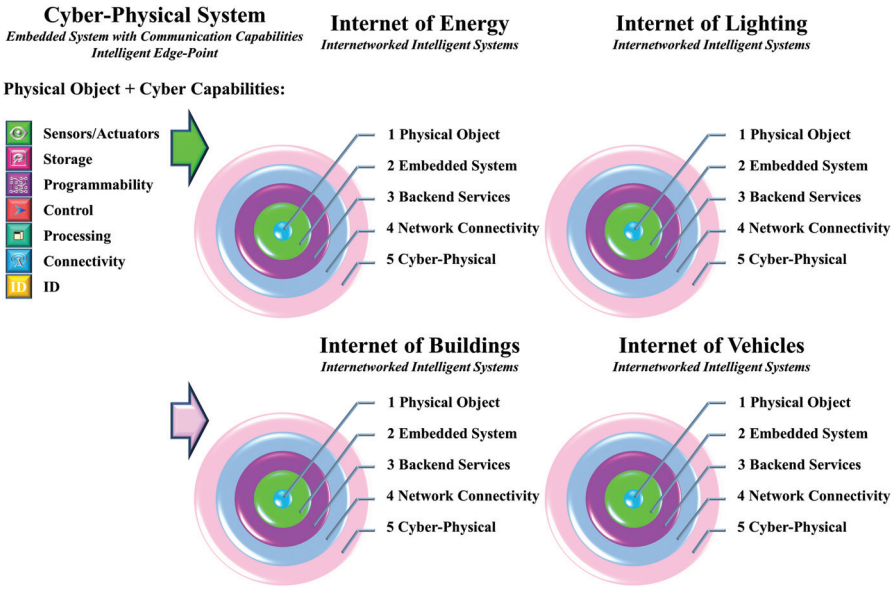

Figure 3.9 CPS building blocks for Internet of X applications.

applications such as smart grid, connected electric cars, energy-efficient buildings, thus eventually helping in building green intelligent cities.

3.3 IoT Smart-X Applications

The IoT applications are addressing the societal needs and the advancements to enabling technologies such as nanoelectronics and cyber-physical systems continue to be challenged by a variety of technical (i.e., scientific and engineering), institutional, and economical issues.

The list is focusing to the applications chosen by the IERC as priorities for the next years and it provides the research challenges for these applications. While the applications themselves might be different, the research challenges are often the same or similar.

3.3.1 Wearables

Wearables are integrating key technologies (e.g. nanoelectronics, organic electronics, sensing, actuating, communication, low power computing, visualisation and embedded software) into intelligent systems to bring new functionalities into clothes, fabrics, patches, watches and other body-mounted devices.

Figure 3.10 Smart wristbands and watches – connected IoT devices.

These intelligent edge devices are more and more part of integrated IoT solutions and assist humans in monitoring, situational awareness and decision making. They can provide actuating functions for fully automated closed-loop solutions that are used in healthcare, well-being, safety, security, infotainment applications and connected with smart buildings, energy, lighting, mobility or smart cities IoT applications. With more than 35 million connected wearable devices in use by the end of 2014, developers are pushing the technological integration into IoT applications looking for the innovation opportunities in different domains. Today, Over 75% of consumers with wearable devices stop using them within 6 months. The challenge for developers is to leverage actionable data to create apps that are seamlessly integrated into everyday life and integrate them with other IoT applications.

Creating a seamless user experience is essential for wearable application success. Leveraging tools to implement gesture-centric interfaces will allow users to make the most of limited surfaces of the wearables. The integration into common IoT platforms where developers can access data gathered from wearable devices is essential recombining datasets to develop applications for specific use cases. The industrial sector offers many opportunities for developers with the augmented reality headsets needed to be used to integrate wearables for solving real problems in the industrial sector.

The market for wearable computing is expected to grow six-fold, from 46 million units in 2014 to 285 million units in 2018 [51]. Wearable computing applications include everything from fitness trackers, health monitors, smart

watches that provide new ways to interact with and utilize your smartphone, to augmented reality glasses wearable computing device.

Fitness tracking is the biggest application today and this opens the opportunities for watches that are capable of tracking blood pressure, glucose, temperature, pulse rate and other vital parameters measured every few seconds for a long period of time to be integrated in new kinds of healthcare applications. Glasses for augmented reality can be another future wearable application.

3.3.2 Smart Health, Wellness and Ageing Well

The market for health monitoring devices is currently characterised by application-specific solutions that are mutually non-interoperable and are made up of diverse architectures. While individual products are designed to cost targets, the long-term goal of achieving lower technology costs across current and future sectors will inevitably be very challenging unless a more coherent approach is used. The IoT can be used in clinical care where hospitalized patients whose physiological status requires close attention can be constantly monitored using IoT -driven, non-invasive monitoring. This requires sensors to collect comprehensive physiological information and uses gateways and the cloud to analyse and store the information and then send the analysed data wirelessly to caregivers for further analysis and review. These techniques improve the quality of care through constant attention and lower the cost of care by eliminating the need for a caregiver to actively engage in data collection and analysis. In addition the technology can be used for remote monitoring using small, wireless solutions connected through the IoT. These solutions can be used to securely capture patient health data from a variety of sensors, apply complex algorithms to analyse the data and then share it through wireless connectivity with medical professionals who can make appropriate health recommendations.

The links between the many applications in health monitoring are:

- Applications require the gathering of data from sensors.
- Applications must support user interfaces and displays.
- Applications require network connectivity for access to infrastructural services.
- Applications have in-use requirements such as low power, robustness, durability, accuracy and reliability.

IoT applications are pushing the development of platforms for implementing ambient assisted living (AAL) systems that will offer services in the areas

of assistance to carry out daily activities, health and activity monitoring, enhancing safety and security, getting access to medical and emergency systems, and facilitating rapid health support.

The main objective is to enhance life quality for people who need permanent support or monitoring, to decrease barriers for monitoring important health parameters, to avoid unnecessary healthcare costs and efforts, and to provide the right medical support at the right time.

The IoT plays an important role in healthcare applications, from managing chronic diseases at one end of the spectrum to preventing disease at the other.

Challenges exist in the overall cyber-physical infrastructure (e.g., hardware, connectivity, software development and communications), specialized processes at the intersection of control and sensing, sensor fusion and decision making, security, and the compositionality of cyber-physical systems. Proprietary medical devices in general were not designed for interoperation with other medical devices or computational systems, necessitating advancements in networking and distributed communication within cyber-physical architectures. Interoperability and closed loop systems appears to be the key for success. System security will be critical as communication of individual patient data is communicated over cyber-physical networks. In addition, validating data acquired from patients using new cyber-physical technologies against existing gold standard data acquisition methods will be a challenge. Cyber-physical technologies will also need to be designed to operate with minimal patient training or cooperation [91].

New and innovative technologies are needed to cope with the trends on wired, wireless, high-speed interfaces, miniaturization and modular design approaches for products having multiple technologies integrated.

IoT applications have a market potential for electronic health services and connected telecommunication industry with the possibility of building ecosystems in different application areas. Medical expenditures are in the range of 10% of the European gross domestic product. The market segment of telemedicine, one of lead markets of the future will have growth rates of more than 19%.

The smart living environments at home, at work, in public spaces should be based upon integrated systems of a range of IoT-based technologies and services with user-friendly configuration and management of connected technologies for indoors and outdoors.

These systems can provide seamless services and handle flexible connectivity while users are switching contexts and moving in their living

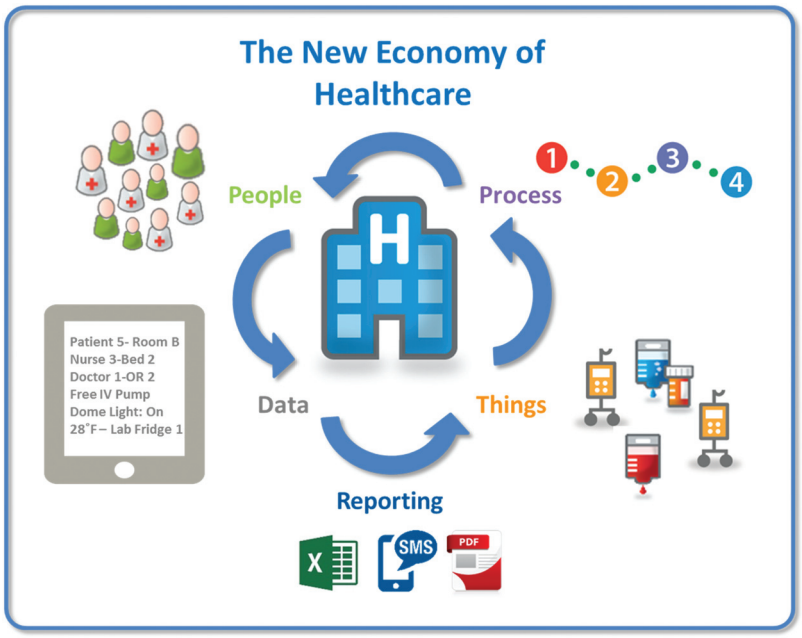

Figure 3.11 Internet of Everything and the new economy of healthcare [81].

environments and be integrated with other application domains such as energy, transport, or smart cities. The advanced IoT technologies, using and extending available open service platforms, standardised ontologies and open standardised APIs can offer many of such smart environment developments.

These IoT technologies can propose user-centric multi-disciplinary solutions that take into account the specific requirements for accessibility, usability, cost efficiency, personalisation and adaptation arising from the application requirements.

3.3.3 Smart Homes and Buildings

The rise of Wi-Fi's role in home automation has primarily come about due to the networked nature of deployed electronics where electronic devices (TVs and AV receivers, mobile devices, etc.) have started becoming part of the home IP network and due the increasing rate of adoption of mobile computing devices (smartphones, tablets, etc.).

Several organizations are working to equip homes with technology that enables the occupants to use a single device to control all electronic devices

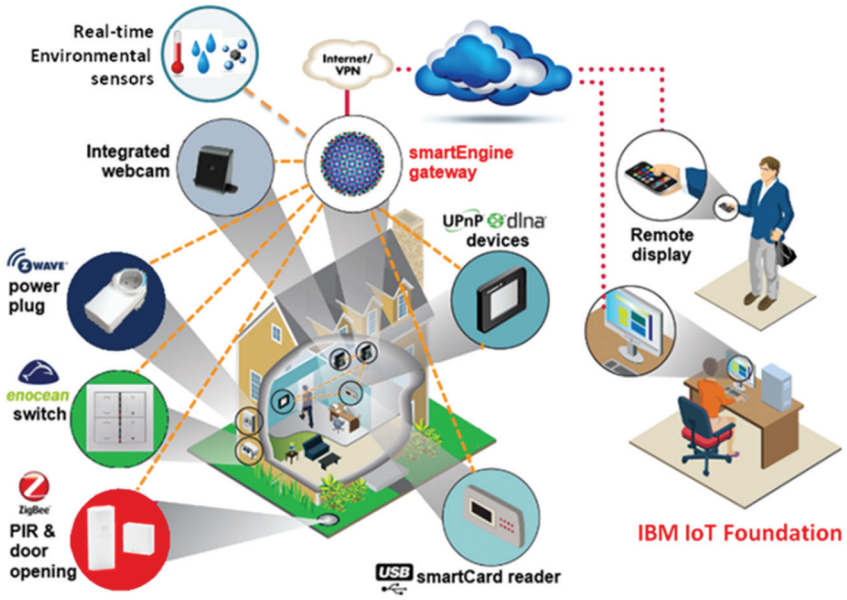

Figure 3.12 Home equipment and appliances [78].

and appliances. The solutions focus primarily on environmental monitoring, energy management, assisted living, comfort, and convenience. The solutions are based on open platforms that employ a network of intelligent sensors to provide information about the state of the home. These sensors monitor systems such as energy generation and metering; heating, ventilation, and air conditioning (HVAC); lighting; security; and environmental key performance indicators. The information is processed and made available through a number of access methods such as touch screens, mobile phones, and 3–D browsers [117]. The networking aspects are bringing online streaming services or network playback, while becoming a mean to control of the device functionality over the network. At the same time mobile devices ensure that consumers have access to a portable 'controller' for the electronics connected to the network. Both types of devices can be used as gateways for IoT applications. In this context many companies are considering building platforms that integrate the building automation with entertainment, healthcare monitoring, energy monitoring and wireless sensor monitoring in the home and building environments.

IoT applications using sensors to collect information about operating conditions combined with cloud hosted analytics software that analyse disparate

data points will help facility managers become far more proactive about managing buildings at peak efficiency.

Issues of building ownership (i.e., building owner, manager, or occupants) challenge integration with questions such as who pays initial system cost and who collects the benefits over time. A lack of collaboration between the subsectors of the building industry slows new technology adoption and can prevent new buildings from achieving energy, economic and environmental performance targets.

Integration of cyber physical systems both within the building and with external entities, such as the electrical grid, will require stakeholder cooperation to achieve true interoperability. As in all sectors, maintaining security will be a critical challenge to overcome [91].

Within this field of research the exploitation of the potential of wireless sensor networks (WSNs) to facilitate intelligent energy management in buildings, which increases occupant comfort while reducing energy demand, is highly relevant. In addition to the obvious economic and environmental gains from the introduction of such intelligent energy management in buildings other positive effects will be achieved. Not least of which is the simplification of building control; as placing monitoring, information feedback equipment and control capabilities in a single location will make a buildings' energy management system easier to handle for the building owners, building managers, maintenance crews and other users of the building.

Using the Internet together with energy management systems also offers an opportunity to access a buildings' energy information and control systems from a laptop or a Smartphone placed anywhere in the world. This has a huge potential for providing the managers, owners and inhabitants of buildings with energy consumption feedback and the ability to act on that information.

The perceived evolution of building system architectures includes an adaptation level that will dynamically feed the automation level with control logic, i.e. rules. Further, in the IoT approach, the management level has also to be made available transversally as configuration; discovery and monitoring services must be made accessible to all levels. Algorithms and rules have also to be considered as Web resources in a similar way as for sensors and actuators. The repartition of roles for a classical building automation system to the new web of things enabled architecture is different and in this context, future works will have to be carried on to find solutions to minimize the transfer of data and the distribution of algorithms [46].

In the context of the future 'Internet of Things', Intelligent Building Management Systems can be considered part of a much larger information

system. This system is used by facilities managers in buildings to manage energy use and energy procurement and to maintain buildings systems. It is based on the infrastructure of the existing Intranets and the Internet, and therefore utilises the same standards as other IT devices. Within this context reductions in the cost and reliability of WSNs are transforming building automation, by making the maintenance of energy efficient healthy productive work spaces in buildings increasingly cost effective [80].

3.3.4 Smart Energy

There is increasing public awareness about the changing paradigm of our policy in energy supply, consumption and infrastructure. For several reasons our future energy supply should no longer be based on fossil resources. Neither is nuclear energy a future proof option. In consequence future energy supply needs to be based largely on various renewable resources. Increasingly focus must be directed to our energy consumption behaviour. Because of its volatile nature such supply demands an intelligent and flexible electrical grid which is able to react to power fluctuations by controlling electrical energy sources (generation, storage) and sinks (load, storage) and by suitable reconfiguration. Such functions will be based on networked intelligent devices (appliances, micro-generation equipment, infrastructure, consumer products) and grid infrastructure elements, largely based on IoT concepts. Although this ideally requires insight into the instantaneous energy consumption of individual loads (e.g. devices, appliances or industrial equipment) information about energy usage on a per-customer level is a suitable first approach.

Future energy grids are characterized by a high number of distributed small and medium sized energy sources and power plants which may be combined virtually ad hoc to virtual power plants; moreover in the case of energy outages or disasters certain areas may be isolated from the grid and supplied from within by internal energy sources such as photovoltaics on the roofs, block heat and power plants or energy storages of a residential area ("islanding").

A grand challenge for enabling technologies such as cyber-physical systems is the design and deployment of an energy system infrastructure that is able to provide blackout free electricity generation and distribution, is flexible enough to allow heterogeneous energy supply to or withdrawal from the grid, and is impervious to accidental or intentional manipulations. Integration of cyber-physical systems engineering and technology to the existing electric grid and other utility systems is a challenge. The increased system complexity

Figure 3.13 Smart Energy Concept [75].

poses technical challenges that must be considered as the system is operated in ways that were not intended when the infrastructure was originally built. As technologies and systems are incorporated, security remains a paramount concern to lower system vulnerability and protect stakeholder data [91]. These challenges will need to be address as well by the IoT applications that integrate heterogeneous cyber-physical systems.

The developing Smart Grid is expected to implement a new concept of transmission network which is able to efficiently route the energy which is produced from both concentrated and distributed plants to the final user with high security and quality of supply standards. Therefore the Smart Grid is expected to be the implementation of a kind of "Internet" in which the energy packet is managed similarly to the data packet – across routers and gateways which autonomously can decide the best pathway for the packet to reach its destination with the best integrity levels. In this respect the "Internet of Energy" concept is defined as a network infrastructure based on standard and interoperable communication transceivers, gateways and protocols that will allow a real time balance between the local and the global generation and storage capability with the energy demand. This will also allow a high level of consumer awareness and involvement.

The Internet of Energy (IoE) provides an innovative concept for power distribution, energy storage, grid monitoring and communication. It will allow units of energy to be transferred when and where it is needed. Power

consumption monitoring will be performed on all levels, from local individual devices up to national and international level [110]. In the long run electro mobility will become another important element of smart power grids. Electric vehicles (EVs) might act as a power load as well as moveable energy storage linked as IoT elements to the energy information grid (smart grid). IoT enabled smart grid control may need to consider energy demand and offerings in the residential areas and along the major roads based on traffic forecast. EVs will be able to act as sink or source of energy based on their charge status, usage schedule and energy price which again may depend on abundance of (renewable) energy in the grid. This is the touch point from where the following telematics IoT scenarios will merge with smart grid IoT.

Latencies are critical when talking about electrical control loops. Even though not being a critical feature, low energy dissipation should be mandatory. In order to facilitate interaction between different vendors' products the technology should be based on a standardized communication protocol stack. When dealing with a critical part of the public infrastructure, data security is of the highest importance. In order to satisfy the extremely high requirements on reliability of energy grids, the components as well as their interaction must feature the highest reliability performance.

Many IoT applications will go beyond one industrial sector. Energy, mobility and home/buildings sectors will share data through energy gateways that will control the transfer of energy and information.

Sophisticated and flexible data filtering, data mining and processing procedures and systems will become necessary in order to handle the high amount of raw data provided by billions of data sources. System and data models need to support the design of flexible systems which guarantee a reliable and secure real-time operation.

3.3.5 Smart Mobility and Transport

The connection of vehicles to the Internet gives rise to a wealth of new possibilities and applications which bring new functionalities to the individuals and/or the making of transport easier and safer. In this context the concept of Internet of Vehicles (IoV) [110] connected with the concept of Internet of Energy (IoE) represent future trends for smart transportation and mobility applications.

At the same time creating new mobile ecosystems based on trust, security and convenience to mobile/contactless services and transportation applications will ensure security, mobility and convenience to consumer-centric transactions and services.

Representing human behaviour in the design, development, and operation of cyber physical systems in autonomous vehicles is a challenge. Incorporating human-in-the-loop considerations is critical to safety, dependability, and predictability. There is currently limited understanding of how driver behaviour will be affected by adaptive traffic control cyber physical systems. In addition, it is difficult to account for the stochastic effects of the human driver in a mixed traffic environment (i.e., human and autonomous vehicle drivers) such as that found in traffic control cyber physical systems. Increasing integration calls for security measures that are not physical, but more logical while still ensuring there will be no security compromise. As cyber physical systems become more complex and interactions between components increases, safety and security will continue to be of paramount importance [91]. All these elements are of the paramount importance for the IoT ecosystems developed based on these enabling technologies.

Self-driving vehicles today are in the prototype phase and the idea is becoming just another technology on the computing industry's parts list. By using automotive vision chips that can be used to help vehicles understand the environment around them by detecting pedestrians, traffic lights, collisions, drowsy drivers, and road lane markings. Those tasks initially are more the sort of thing that would help a driver in unusual circumstances rather than take over full time. But they're a significant step in the gradual shift toward the computer-controlled vehicles that Google, Volvo, and other companies are working on [88]. The image below shows a footage of what the on-board Google Car's computer "sees" and how it detects other vehicles, pedestrians, and traffic lights [86].

These scenarios are, not independent from each other and show their full potential when combined and used for different applications.

Technical elements of such systems are smart phones and smart vehicle on-board units which acquire information from the user (e.g. position, destination and schedule) and from on board systems (e.g. vehicle status, position, energy usage profile, driving profile). They interact with external systems (e.g. traffic control systems, parking management, vehicle sharing managements, electric vehicle charging infrastructure). Moreover they need to initiate and perform the related payment procedures.

The concept of Internet of Vehicles (IoV) is the next step for future smart transportation and mobility applications and requires creating new mobile ecosystems based on trust, security and convenience to mobile/contactless services and transportation applications in order to ensure security, mobility and convenience to consumer-centric transactions and services.

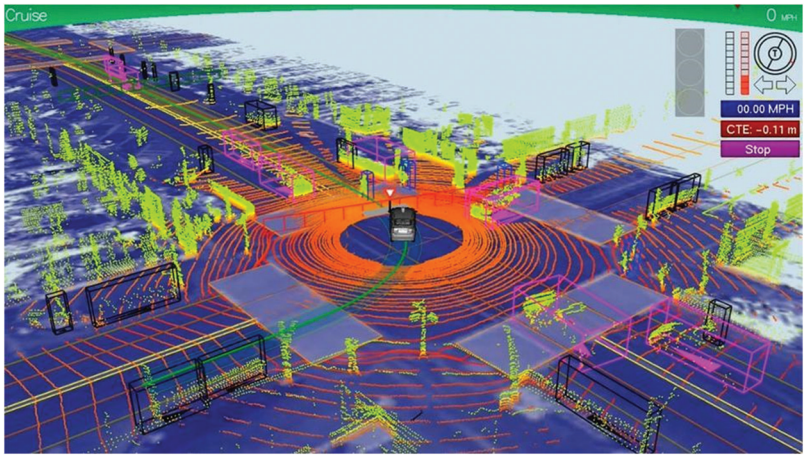

Figure 3.14 Google vehicle vision [86].

Smart sensors in the road and traffic control infrastructures need to collect information about road and traffic status, weather conditions, etc. This requires robust sensors (and actuators) which are able to reliably deliver information to the systems mentioned above. Such reliable communication needs to be based on M2M communication protocols which consider the timing, safety, and security constraints. The expected high amount of data will require sophisticated data mining strategies. Overall optimisation of traffic flow and energy usage may be achieved by collective organisation among the individual vehicles.

When dealing with information related to individuals' positions, destinations, schedules, and user habits, privacy concerns gain highest priority. They even might become road blockers for such technologies. Consequently not only secure communication paths but also procedures which guarantee anonymity and de-personalization of sensible data are of interest.

Connectivity will revolutionize the environment and economics of vehicles in the future: first through connection among vehicles and intelligent infrastructures, second through the emergence of an ecosystem of services around smarter and more autonomous vehicles.

In this context the successful deployment of safe and autonomous vehicles (SAE[1] international level 5, full automation) in different use case scenarios, using local and distributed information and intelligence is an important

[1]Society of Automotive Engineers, J3016 standard.

achievement. This is based on real-time reliable platforms managing mixed mission and safety critical vehicle services, advanced sensors/actuators, navigation and cognitive decision-making technology, interconnectivity between vehicles (V2V) and vehicle to infrastructure (V2I) communication. There is a need to demonstrate in real life environments (i.e. highways, congested urban environment, and/or dedicated lanes), mixing autonomous connected vehicles and legacy vehicles the functionalities in order to evaluate and demonstrate dependability, robustness and resilience of the technology over longer period of time and under a large variety of conditions.

The introduction of the autonomous vehicles will enable the development of service ecosystems around vehicles and multi-modal mobility, considering that the vehicle includes multiple embedded information sources around which information services may be constructed. The information may be used for other services (i.e. maintenance, personalised insurance, vehicle behaviour monitoring and diagnostic, security and autonomous cruise, etc.).

The emergence of these services will be supported by open service platforms that communicate and exchange information with the vehicle embedded information sources and to vehicle surrounding information, with the goal of providing personalised services to drivers. Possible barriers to the deployment of autonomous vehicles and ecosystems are the robustness sensing/actuating the environment, overall user acceptance, the economic, ethical, legal and regulatory issues.

3.3.6 Smart Manufacturing and Industrial Internet of Things

The role of the Internet of Things is becoming more prominent in enabling access to devices and machines, which in manufacturing systems, were hidden in well-designed silos. This evolution will allow the IT to penetrate further the digitized manufacturing systems. The IoT will connect the factory to a whole new range of applications, which run around the production. This could range from connecting the factory to the smart grid, sharing the production facility as a service or allowing more agility and flexibility within the production systems themselves. In this sense, the production system could be considered one of the many Internets of Things (IoT), where a new ecosystem for smarter and more efficient production could be defined.

The first evolutionary step towards a shared smart factory could be demonstrated by enabling access to today's external stakeholders in order to interact with an IoT-enabled manufacturing system. These stakeholders could include the suppliers of the productions tools (e.g. machines, robots),

as well as the production logistics (e.g. material flow, supply chain management), and maintenance and re-tooling actors. An IoT-based architecture that challenges the hierarchical and closed factory automation pyramid, by allowing the above-mentioned stakeholders to run their services in multiple tier flat production system is proposed in [186]. This means that the services and applications of tomorrow do not need to be defined in an intertwined and strictly linked manner to the physical system, but rather run as services in a shared physical world. The room for innovation in the application space could be increased in the same degree of magnitude as this has been the case for embedded applications or Apps, which have exploded since the arrival of smart phones (i.e. the provision of a clear and well standardized interface to the embedded hardware of a mobile phone to be accessed by all types of Apps).

Enterprises are making use of the huge amount of data available, business analytics, cloud services, enterprise mobility and many others to improve the way businesses are being conducted. These technologies include big data and business analytics software, cloud services, embedded technology, sensor networks/sensing technology, RFID, GPS, M2M, mobility, security and ID recognition technology, wireless network and standardisation.

One key enabler to this ICT-driven smart and agile manufacturing lies in the way we manage and access the physical world, where the sensors, the actuators, and also the production unit should be accessed, and managed in the same or at least similar IoT standard interfaces and technologies. These devices are then providing their services in a well-structured manner, and can be managed and orchestrated for a multitude of applications running in parallel.

The convergence of microelectronics and micromechanical parts within a sensing device, the ubiquity of communications, the rise of micro-robotics, the customization made possible by software will significantly change the world of manufacturing. In addition, broader pervasiveness of telecommunications in many environments is one of the reasons why these environments take the shape of ecosystems.

Some of the main challenges associated with the implementation of cyber-physical systems in include affordability, network integration, and the interoperability of engineering systems.

Most companies have a difficult time justifying risky, expensive, and uncertain investments for smart manufacturing across the company and factory level. Changes to the structure, organization, and culture of manufacturing

occur slowly, which hinders technology integration. Pre-digital age control systems are infrequently replaced because they are still serviceable. Retrofitting these existing plants with cyber-physical systems is difficult and expensive. The lack of a standard industry approach to production management results in customized software or use of a manual approach. There is also a need for a unifying theory of non-homogeneous control and communication systems [91].

3.3.7 Smart Cities

A smart city is defined as a city that monitors and integrates conditions of all of its critical infrastructures, including roads, bridges, tunnels, rail/subways, airports, seaports, communications, water, power, even major buildings, can better optimize its resources, plan its preventive maintenance activities, and monitor security aspects while maximizing services to its citizens. Emergency response management to both natural as well as man-made challenges to the system can be focused and rapid. With advanced monitoring systems and built-in smart sensors, data can be collected and evaluated in real time, enhancing city management's decision-making. For example, resources can be committed prior to a water main break, salt spreading crews dispatched only when a specific bridge has icing conditions, and use of inspectors reduced by knowing condition of life of all structures. In the long term Smart Cities vision, systems and structures will monitor their own conditions and carry out self-repair, as needed. The physical environment, air, water, and surrounding green spaces will be monitored in non-obtrusive ways for optimal quality, thus creating an enhanced living and working environment that is clean, efficient, and secure and that offers these advantages within the framework of the most effective use of all resources [89].

There are a number of key elements needed to form a Smart City, and some of these are smart society, smart buildings, smart energy, smart lighting, smart mobility, smart water management etc. ICT forms the basic infrastructure; varying from sensors, actuators and electronic systems to software, Data, Internet and Cloud, Edge/fog and Mobile Edge computing. ICT is applied to improve these systems of systems building up a Smart City, making them autonomous and interoperable, secure and trusted. The interaction of the systems and the connectivity strongly depend on the communication gateway connecting the edge element data from sensors, actuators, and electronic systems to the Internet, managing- and control systems and decision programs. The communication gateway is a key enabler for the interconnection of

systems in many applications such as Internet of Energy (IoE), Internet of Vehicles (IoV), Internet of Buildings (IoB) and Internet of Lighting (IoL). It is obvious with all the new systems and demand of interoperability that these communication gateways need more functionality, processing capacity, storage possibility, seamless connectivity, and more communication protocols embedded. At the same time the gateway must assure a higher level of security, interoperability and communication with devices across various verticals, such as energy, mobility and buildings.

An illustrative example is depicted in Figure 3.15 [76]. The Smart City is not only the integration and interconnection of intelligent applications, but also a people-centric and sustainable innovation model that is using communication and information technology and takes advantage of the open innovation ecology of the city and the new technologies such as IoT, cloud computing, smart data, and man-machine interaction.

A smart city is a developed urban area that creates sustainable economic development and high quality of life by excelling in multiple key areas: economy, mobility, environment, people, living, and government [105].

3.3.7.1 Large Scale Pilots and Ecosystem for Smart Cities

As main areas of application, smarter cities plays a relevant role, not only because the impact in re-using and re-purposing technology that is necessary (the number of deployed sensors) but also the increasing demand of new services (by citizens). IoT applications are currently based on multiple

Figure 3.15 Smart City Concept [76].

architectures, technology standards and seamless software platforms, which have led to a highly fragmented IoT landscape. This fragmentation impacts directly the area of smart cities, which typically comprise several technological silos (i.e. IoT systems that have been developed and deployed independently for smart homes, smart industrial automation, smart transport, and smart buildings etc.).

A radical shift in the development, deployment and operation of IoT applications for smart cities, through introducing an abstract virtualized digital layer that operate across multiple IoT architectures, platforms (e.g. FI-WARE) and business contexts is required. Smart cities soon will face up the need for an integrated solution(s) (SmartCity-OS) that globally can monitor, visualise and control the uncountable integrated number of operations executed by diverse (and every day increasing) services platforms using the sensor technology deployed in the cities. Eventually this OS will be a blueprint across cities providing adaptive tools and generating the integration of other IoT systems and business opportunities.

Additional pointers to highlight are the quality of IoT Data and the numerous IoT Data source provisioning and the inherent need to generate

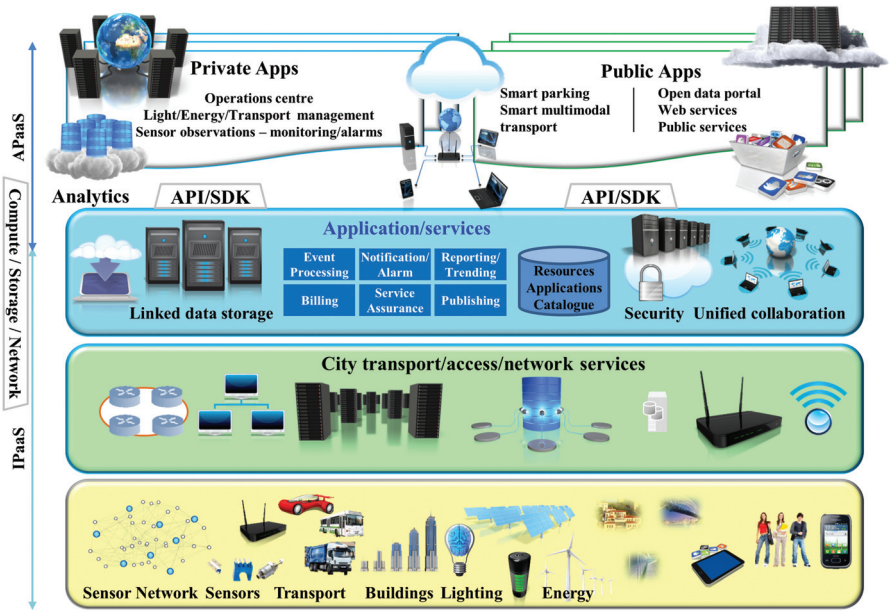

Figure 3.16 Smart City Multi-layered architecture.

semantic-driven business platforms, the reason to emphasize them is to address the emergent need for enabling business-driven IoT ecosystems and the generation of functionalities for Operating across multiple IoT architectures, platforms and business contexts, enable re(use) of Data for Smart Applications, and enable a more connected/integrated approach to smart city applications development.

There is a large way in the run towards integrated Internet of Things technological support and scientific progression towards interoperable connected objects, linked sensor data, pay-as-you-go IoT services and utility-driven privacy. Likewise the main areas to focus from a research perspective are, but not limited to, IoT architecture, systems and applications. The developments of IoT data modelling and schema representations, intra-domain and CPS extensions allow more robustness and extensible software platforms with embedded software and applications enabling Systems of Systems, peer-to-peer systems and applications.

An IoT large Scale Pilot is a fully designed, implemented and deployed ecosystem, such that all the players are inter-related: Technology Designers and Manufacturing, Software Designers and Developers, Research Institutions and Universities, Large Industries alike SME's, Alliance and standardization organisations, City Councils and Policy Makers and Citizen Organisations, share the same common objective which is sustainability. IoT Sustainability implies to have all the technology elements and services connected in the form of data interactions producing results.

3.3.7.2 Role of Institutions and Citizens in the Global IoT

The citizens play a protagonist role in the IoT Large Scale Pilot, particularly if the LSP is focused on Smart City applications. The role citizens can play are, but not limited to, Active elements in the system as data providers, Validation of the deployed infrastructure, Testers of the implemented solutions and services, Adaptability test about Robustness and Extensible software and last but not least Improvements and feedback on software solutions.

As main other areas of application, smart retail play a relevant role, not only because the impact in technology that is necessary (the number of deployed sensors) but also the increasing demand of new services (M2M and by citizens H2M). IoT applications are currently based on multiple architectures, technology standards and seamless software platforms, which have led to a highly fragmented IoT landscape. This fragmentation impacts directly the area of smart cities, which typically comprise several technological silos (i.e.

IoT systems that have been developed and deployed independently for smart homes, smart industrial automation, smart transport, and smart buildings etc.).

Excelling in these key areas can be done so through strong human capital, social capital, and/or ICT infrastructure. With the introduction of IoT a city will act more like a living organism, a city that can respond to citizen's needs.

In this context there are numerous important research challenges for smarty city IoT applications:

- Overcoming traditional silo based organization of the cities, with each utility responsible for their own closed world. Although not technological this is one of the main barriers.
- Creating algorithms and schemes to describe information created by sensors in different applications to enable useful exchange of information between different city services.
- Mechanisms for cost efficient deployment and even more important maintenance of such installations, including energy scavenging.
- Ensuring reliable readings from a plethora of sensors and efficient calibration of a large number of sensors deployed everywhere from lampposts to waste bins.
- Low energy protocols and algorithms.
- Algorithms for analysis and processing of data acquired in the city and making "sense" out of it.
- IoT large scale deployment and integration.

3.3.8 Smart Farming and Food Security

Food and fresh water are the most important natural resources in the world. Organic food produced without addition of certain chemical substances and according to strict rules, or food produced in certain geographical areas will be particularly valued. Similarly, fresh water from mountain springs is already highly valued. Using IoT in such scenarios to secure tracking of food or water from the production place to the consumer is one of the important topics.

The development of sensors, robots and sensor networks combined with procedures to link variables to appropriate farming management actions has open the opportunities for IoT applications in agriculture. The wired/wireless sensors, integrated into a IoT system can gather all the individual data needed for monitoring, control and treatment on (large scale) farms located in a particular region. This provides a mechanism of exchanging information in efficient ways enabling the execution of autonomously interventions in different agriculture sub-sectors (e.g. arable crops, livestock and horticulture).

IoT technology allows the monitoring and control of the plant and animal products during the whole life cycle from farm to fork. The challenge will be in the future to design architectures and implement algorithms that will support each object for optimal behaviour, according to its role in the Smart Farming system and in the food chain, lowering ecological footprint and economical costs and increasing food security.

The set of technologies used in smart farming is complex, to reflect the complexity of activities run by farmers, growers, and other sector stakeholders.

A recent report [85] on smart farming defines seven applications:

- Fleet management – tracking of farm vehicles
- Arable farming, large and small field farming
- Livestock monitoring
- Indoor farming – greenhouses and stables
- Fish farming
- Forestry
- Storage monitoring – water tanks, fuel tanks

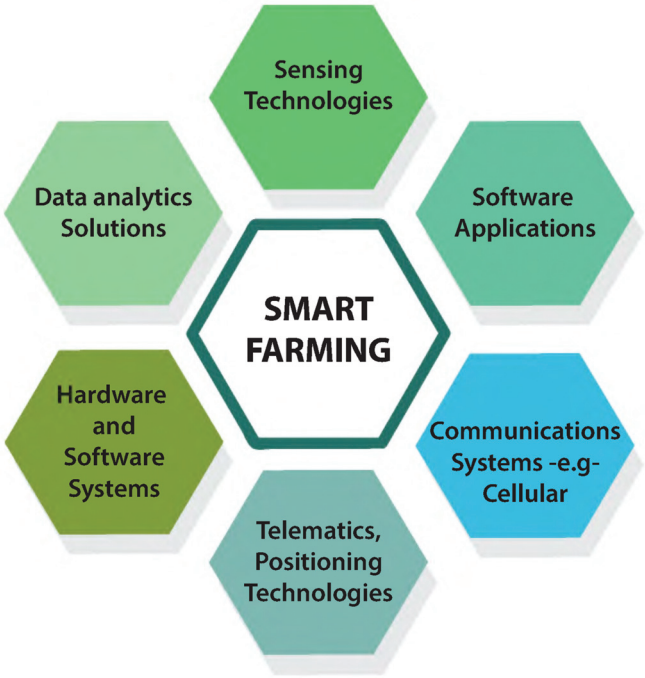

Figure 3.17 Different types of technologies involved in smart farming [85].

The report says that smart farming will allow farmers and growers to improve productivity and reduce waste, ranging from the quantity of fertiliser used to the number of journeys made by farm vehicles.

However, the complexity of smart farming is also reflected into the ecosystem of players. They can be classified in the following way:

- Technology providers – these include providers of wireless connectivity, sensors, M2M solutions, decision support systems at the back office, big data analytical systems, geo-mapping applications, smartphone apps.
- Providers of agricultural equipment and machinery (combines, tractors, robots), farm buildings, as well as providers of specialist products (e.g. seeds, feeds) and expertise in crop management and animal husbandry.
- Customers: farmers, farming associations and cooperatives.
- Influencers – those that set prices, influence the market into which farmers and growers sell their products.

The range of stakeholders in agriculture is broad, ranging from big business, finance, engineering, chemical companies, food retailers to industry associations and groupings through small suppliers of expertise in all the specialist areas of farming.

The end users of precision farming solutions include not only the growers but also farm managers, users of back office IT systems. Not to be forgotten is the role of the veterinary in understanding animal health. Also to be considered are farmers co-operatives, which can help smaller farmers with advice and funding.

The report concludes that the farming industry must embrace the IoT if it is to feed the 9.6 billion global population expected by 2050.

3.4 Future Internet Support for IoT

There are a number of challenges that the Future Internet community will need to address to adequately support the envisaged evolution of the Internet of Things. First we need to position these challenges within a 5–10 year timeline, and then introduce the technology enablers required to support the vision for future IoT-based applications and services. The following sections are reflecting three macro-challenges. One dedicated to the implications of having billions of connected "things" by 2020. The next one looking at what it takes to duly manage these connected devices in order to ensure dependable and robust services. The last one, more longer term oriented, will shed some light

on what is required to usefully interpret the wealth of IoT harvested data and produce meaningful knowledge.

3.4.1 Macro-Challenges for Supporting IoT Evolution

As mentioned in the introduction, three macro-challenges have been identified as a suitable means to convey the main implications for the Future Internet, derived from the evolution of IoT.

The first one relates to the already ongoing trend of having more and more devices and more generically "objects/things" connected to the Internet. Forecasts vary in numbers according to who made the predictions and what those predictions entailed. There is however no disagreement on the fact that there will be billions of connected objects by 2020. The sheer scale of connected devices and the type of traffic these generate (compared to human's devices) will have substantial implications on the Internet as we know it today.

Managing objects, and ensuring that they can be seamlessly integrated in different application domains and ensuring that the data they produce can be reliably accessed to sustain dependable services is part of the second macro-challenge identified. There are currently many IoT services being used, though mostly perceived as "best effort" due to the nature of the resources involved (end devices that get out of coverage, out of battery, jammed through interference, need for human intervention for configuring, replacing, maintaining them etc.).

This second macro-challenge is concerned with supporting the "tactile Internet" which by many is already being hailed as the natural evolution of IoT. Sensing substrates and communication infrastructures are getting more tightly geared towards supporting more agile and reactive applications.

Getting billions of objects duly connected and managing these to create a reliable monitoring/actuating substrate only partially caters for the challenges ahead. These challenges cannot be complete without considering how to handle the huge amount of data produced and how to transform it into useful and actionable knowledge. This is indeed the most difficult of the macro-challenges ahead given it is related to intelligent reasoning over the data IoT will produce. The difficulty of this challenge lies in the lack of general purpose machine-learning based solutions that can be re-used to address the wide variety of situations in which similar IoT services and applications could be applied.

The figure below illustrates a visual map of these macro-challenges, together with the associated sub-challenges as illustrated in the next section.

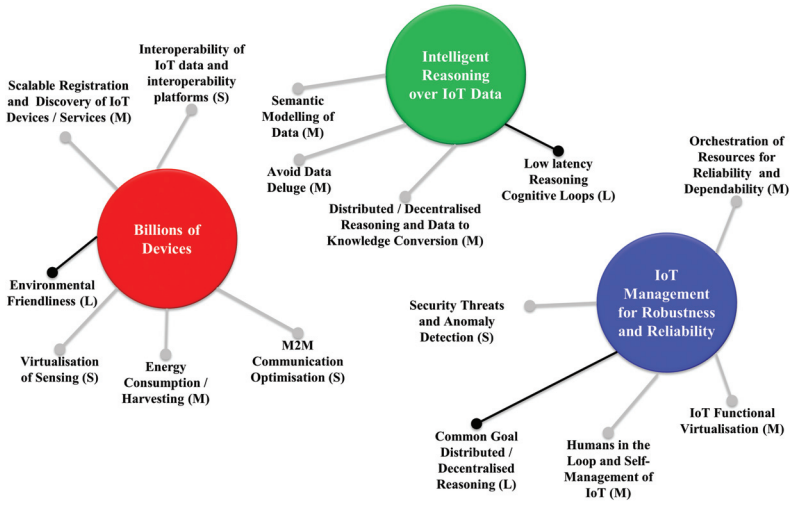

Figure 3.18 Visual map for IoT-related implications of the Future Internet.

The letters S, M and L are there to indicate the Short, Medium or Long term nature of the sub-challenge.

3.4.1.1 Billions of Devices

Scalable registration and discovery of IoT devices/services – As more and more devices get connected, the challenge becomes finding them in a context-aware way. Semantic enrichment of objects description is poised to play a role in facilitating the automated discovery of suitable objects for the purposes of the various applications.

Interoperability of IoT data and interoperability platforms – Besides the common aspects of underlying technologies that have enabled short-range connectivity and the miniaturization of devices that have paved the way towards the success of IoT, current applications have been evolving as a collection of vertical silos often deployed with different standards. To fully unlock the potential of having billions of connected objects, cross-use of data across application domains will be needed. Solutions that foster interoperability and reduce barriers between application silos will therefore have a strong role to play.

Virtualisation of sensing – Following on the need to foster interoperability, virtualization of objects will also be needed to separate real and resource-constrained objects from their virtual counterparts in order to minimising energy consumption, facilitate interaction with applications as well

as address the challenges of scalability and those of empowering single objects with flexible added resources from the "wired and resource intensive world".

M2M communication optimisation – Connected objects have communication requirements that can be substantially different from devices like computers or smart-phones. Short-lived communications in huge numbers and energy consideration will require redesign of communication protocols, especially for the wireless part to minimise the overheads associated with exchanging data between objects and their corresponding clients/gateways.

Energy consumption/harvesting – To ensure long duration and usefulness of connected objects, given also limitations of battery evolution compared to processing power and spectrum efficiency, it will be essential to design hardware and systems that can operate for long time without need for battery replacement/recharging. Integration of energy harvesting techniques also falls in this category.

Environmental friendliness – Billions of devices lasting up to 5–10 years, but very often replaced much earlier, means a lot of waste produced after these devices are no longer operational. Choice of fully recyclable materials fostering sustainability of IoT will be more and more important. Especially after the many IoT deployments will produce sustained need of hardware and services and differentiation between vendors will start including these environmental friendliness factors.

3.4.1.2 IoT Management for Robustness and Reliability

Security threats and anomaly detection – This is a cross-cutting issue as it relates not only to the security of radio communications, but also to the security of IoT-generated data to ensure good levels of trust and privacy. On this front not only solutions that address these issues are needed but also solutions that at a management level can detect attacks and contain them.

Orchestration of resources for reliability and dependability – This challenge relates to the ability of assessing dependencies between sensing, networking and computing resources and how these components contribute to the QoE and reliability of the end-to-end application being supported. Issue of dependability becomes important if one has to leverage on the advantages of the IoT also within mission critical systems and/or simply more dependable services.

IoT function virtualisation – The IoT functionality is currently solely supported by ad-hoc hardware (i.e. communication of sensed-data, domain/sensor specific gateways etc.). IoT function virtualisation will be opening up new

opportunities where hardware ownership will not be necessarily a requirement for producing IoT services.

Common goal distributed/decentralised reasoning – As IoT functionality gets virtualised and distributed besides orchestrating the use of resources there will also be need to coordinate decision-making and achieve conflict resolution for the actuators that are involved in achieving a common goal.

3.4.1.3 Intelligent Reasoning over IoT Data

Semantic modeling of data – As more and more data gets collected through IoT devices, to ensure a more automated selection of the appropriate end devices to be associated with IoT services and applications, IoT data will have to be modeled according to given structures and properly annotated. Semantics help in this respect; so this challenge is part of the broader data interoperability problem though it encompasses besides "finding" the right data also the ability of fostering automated translation between data structures in different ontology domains.

Avoid data deluge – This challenge is about the ability of processing data close to the place where it is generated or on its way to the requesting application. This will help avoid unnecessary use of network resources, as well as reduce the amount of data that have to be processed for analytics purposes. It includes challenges like data aggregation, stream processing, CEP etc.

Distributed/decentralised reasoning and data to knowledge conversion – While the previous challenge is about why we should avoid data deluge, this challenge is about how this can be achieved. IoT is becoming the underlying monitoring fabric of future smart-x applications. Trends suggests there will soon be more devices than we can dedicate attention to, thus getting data across to applications will have to be better managed on the end-to-end delivery path. This requires introduction of new ways for distributed data interpretation which accounts for the locality of data, the need to compress it to meet application requirements (i.e. latency, quality etc.) and network capacity.

Low latency reasoning cognitive loops – This challenge relates to the IoT evolving towards becoming able to support very low-latency reasoning loops. This involves the ability to instantiate data processing instances dynamically and close to data sources, besides addressing redesign of communication protocols for speed.

Humans in the loop and self-management of IoT – The rapidly increasing number of connected objects will not be met by a similarly progress in humans ability to set them up, configure them, manage them etc. This element

of the roadmap relates to the need of solutions that will ensure that devices can be fully operational with simple and little involvement of the users, if need be.

3.4.2 Roadmap and Technology for Addressing These Challenges

IoT is currently positioned at the top of the Gartner hype cycle (the so called "peak of expectations"). The challenge for all the businesses that plan to draw on the wide uptake of this technology, is to ensure that the "through of disillusionment" is somewhat reduced and that the market remains sustained. To achieve this objective one must certainly focus on adoption and user-friendliness. From a technology viewpoint, effort should go to ensuring that the right enablers that support this vision are developed.

3.4.2.1 From Challenges to Technology Solutions

In previous section we split the future IoT challenges under three main categories, one related to dealing with billions of connected things, one related to having to manage these devices and a last one associated with making the most of data these things will produce in other words, how to create useful knowledge.

What is clear is that full mesh connectivity between billions of devices and associate applications will not be achievable, which brings us to the statement that IoT will need increased flexibility in the "communication infrastructure substrate".

This translates into ensuring adequate evolution in the following technology domains: flexible networks for prioritized and M2M-specific communications, edge cloud computing and distributed big-data analytics. Besides these "infrastructure oriented" technologies, also progress in more "IoT specific" domains will be needed: this relates to progress on the "hardware-related" energy harvesting side to ensure more reliable and durable IoT services. Whereas on the "software side" semantic technologies as well as ensuring security and privacy protection solutions need to be reliable and usable to foster wide acceptance.

The remainder of this section sheds more light into the technologies (light boxes in the figures below) that support the highlighted challenges (dark boxes in the figures). As before, we keep the similar structure around the three earlier presented challenges.

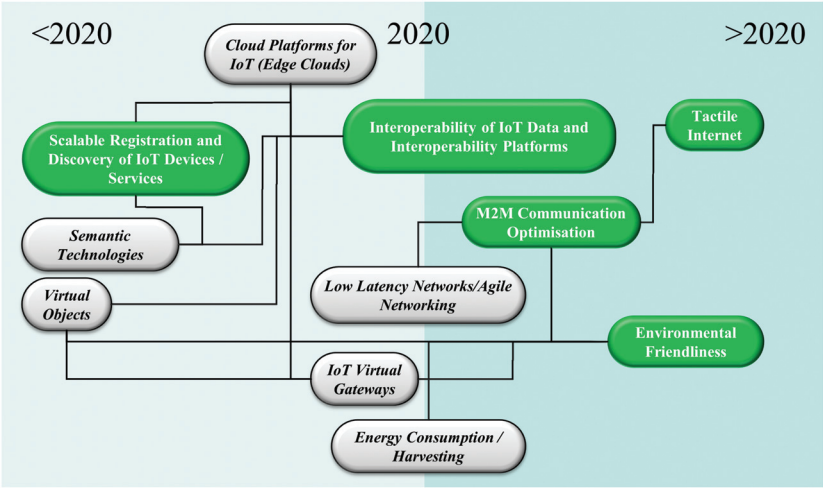

Figure 3.19 Billions of connected devices.

Billions of connected devices, what technology enablers? – Addressing the challenge of billions of connected devices will certainly require some scale-proof technologies for enabling their automated registration, search and discovery, maintenance and management.

This has a lot to do with progress on the semantic technologies front (and subsequent semantic annotation of objects). Through the use of semantics one can design how to automatically relate all devices that e.g. share a similar location, or that can produce a certain type of data, or that are owned by the same person. Moreover progress on the semantic technologies front is also needed to address IoT application silos interoperability problems. In particular this will enable the system's understanding of "what" needs to be done to achieve interoperability between data in separate domains. As far as the "how" is concerned, once it is clear what conversion needs to be applied to the sensed data to make it available for e.g. across application domains. Here comes the role of edge clouds where appropriate algorithms can be instantiated and run to address interoperability issues.

Looking at more "hardware" related issues, progress in the energy harvesting field has many implications on the achievement of the billions devices challenge. It certainly contributes to environmental friendliness as it relies upon renewable energy for the installation of sensing devices at zero energy impact i.e. without connection to power sources. Similarly, the relatively slow advances in battery technologies compared to evolution of

computing capabilities, mean that wireless IoT devices will always be more resource constrained than their wired counterparts. Virtualisation (of sensing) techniques therefore empower wireless devices by adding "always-on" functionality on the "wired side" of the network and breaking functionality from hardware ownership which also contributes to achieving better environmental friendliness as it makes for more efficient (re-)use of hardware resources. This is aligned to leveraging on functionality to the edge of the network, therefore enabling a more sustainable evolution of virtual objects/IoT Virtual Gateway functionality.

With regards to achieving more efficient M2M communications, it is envisaged that progress on the low-latency wireless networks technologies and agile networks management will be needed. This is needed to ensure on the one hand low-overhead for short-lived communications to edge devices (through more agile network management schemes) while on the other hand achieving shorter cognitive loops for sensing-processing-actuating close to the edge, a "must-have" requirement for tactile internet future scenarios.

Management of IoT devices for robustness and reliability – The importance of this challenge stems from IoT becoming more mature and established enabling contextually also support for critical services, or more robust and dependable ones in general.

From a technology viewpoint, there is need for more flexible "infrastructure oriented" technologies to mature. Edge clouds and software networks

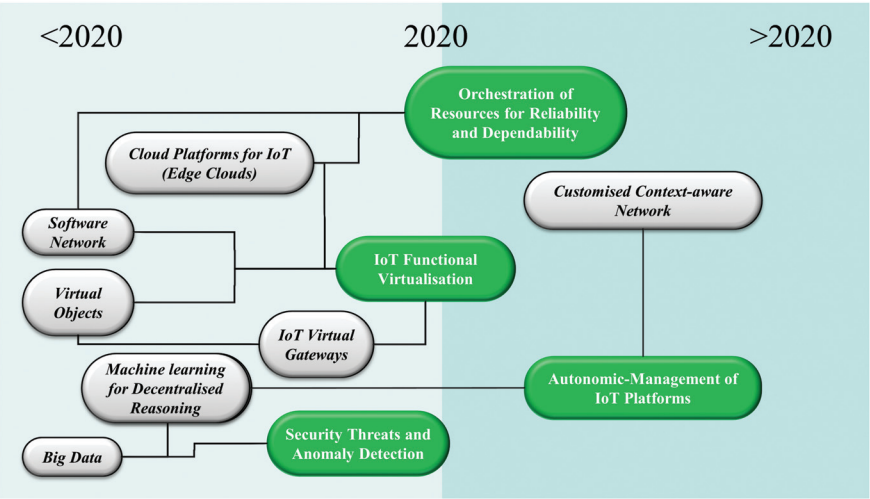

Figure 3.20 Management of IoT for robustness and reliability.

are there to support and complement the constrained nature of devices and have therefore implications on the sub-challenges of virtualizing IoT functionality and orchestrating the use of these "infrastructure technologies" for a more robust IoT. Virtual Objects and Virtual Gateways are also specific IoT technologies, building bricks of virtual IoT functions which can be more robust and resilient to connected objects hardware failures/limited coverage.

With an increase of the number of devices beyond what humans can successfully manage comes the need to rely on cognitive technologies for autonomic management of IoT platforms and for security threats and anomaly detection. Specifically, this is supported by progress in the big-data analytics and leverages on machine learning and decentralized reasoning technologies.

Intelligent reasoning over IoT data – While previous challenges were related to IoT hardware and more infrastructure oriented, this one is about how to best leverage on IoT harvested data, notably to produce the usable and useful knowledge for compelling IoT-based services and applications in many different domains.

Semantic annotation of data is a must to be able to automatically draw "relevance boundaries" amongst available data. Hence, progress on semantic technologies underpins the development of data models that foster and support well-targeted data to knowledge conversions which is key in ensuring wide adoptions (i.e. cognitive systems that take the right decisions through predictive models).

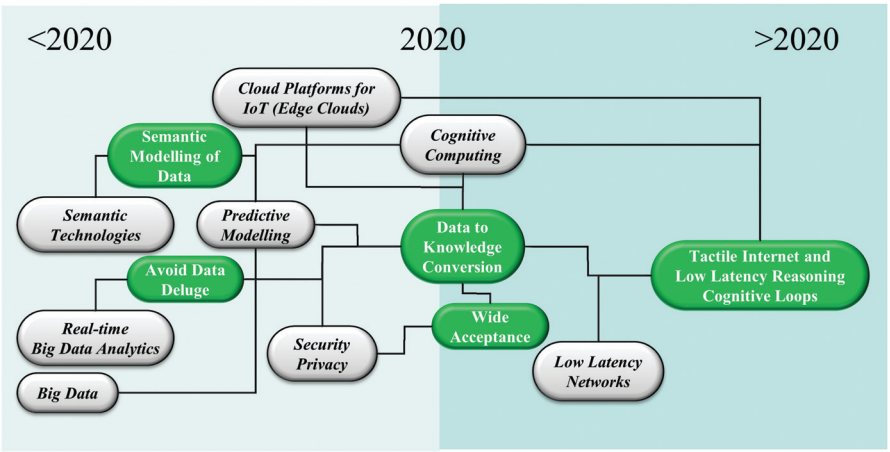

Figure 3.21 Intelligent reasoning over IoT data.

Besides semantic technologies, techniques of cognitive computing are also required. Here we refer to the more and more reliable services that large computing machines such as e.g. IBM Watson will enable. The algorithms for data to knowledge manipulation and for predictive modelling contribute to better quality decisions and wide acceptance. This is also where big-data steps-in, as well as security and privacy by design which are also key to ensure wide acceptance.

On the "data to knowledge conversion" path we illustrated the importance of real-time big-data analytics applied to reduce in size the produced IoT data, and thus lowering IoT impact on communication networks. This is achieved through pre-processing done close to the edge, avoiding data deluge.

Edge clouds and low latency networks, together with well-targeted data to knowledge conversion are the key technologies for achieving fast reasoning loops, which underpin future Tactile Internet scenarios.

3.5 Internet of Things and Related Future Internet Technologies

3.5.1 Cloud and Edge/Fog Computing

Cloud computing has been established as one of the major building blocks of the Future Internet. New technology enablers have progressively fostered virtualisation at different levels and have allowed the various paradigms known as "Applications as a Service", "Platforms as a Service" and "Infrastructure and Networks as a Service". Such trends have greatly helped to reduce cost of ownership and management of associated virtualised resources, lowering the market entry threshold to new players and enabling provisioning of new services. With the virtualisation of objects being the next natural step in this trend, the convergence of cloud computing and Internet of Things will enable unprecedented opportunities in the IoT services arena [112]. Devices send and receive data interacting with the network where the data is transmitted, normalized, and filtered using edge computing/processing then is transferred in data storage units and databases accessible by applications and analytics tools, which process it and provide it to other things and people who will act and collaborate. The IoT layered architecture include the edge intelligence into the edge computing/processing where all the data capture, processing is done at the device level among all the physical sensor/actuators/devices that include controllers based on microprocessors/microcontrollers to compute/process

and wireless modules to communicate. The intelligence at the edge supports devices to use their data sharing and decision-making capabilities to interact and cooperate in order to process the data at the edge, filter it and select/prioritize what is important. This intelligent processing at the edge select the "smart data" that is transferred to the central data stores for further processing in the cloud. This allows including the Edge Cloud for processing data and addressing the challenges of response-time, reliability and security. For real time fast processes, the sensor/actuator edge devices could generate data much faster than the cloud-based apps can process it.

The use of intelligent edge devices require to reduce the amount of data sent to the cloud through quality filtering and aggregation and the integration of more functions into intelligent devices and gateways closer to the edge reduces latency. By moving the intelligence to the edge, the local devices can generate value when there are challenges related to transferring data to the cloud. This will allow as well for protocol consolidation by controlling the various ways devices can communicate with each other.

As part of this convergence, IoT applications (such as sensor-based services) will be delivered on-demand through a cloud environment [113]. This extends beyond the need to virtualize sensor data stores in a scalable fashion. It

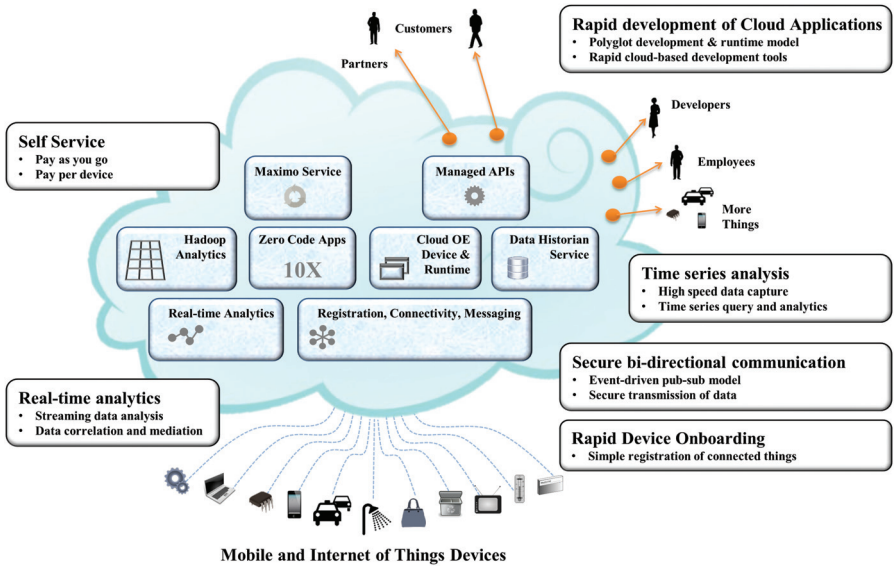

Figure 3.22 Internet of Things Cloud (Source: IBM).

asks for virtualization of Internet-connected objects and their ability to become orchestrated into on-demand services (such as Sensing-as-a-Service).

With the growth of IoT, we're shifting toward a cyber-physical paradigm, where we closely integrate computing and communication with the connected things, including the ability to control their operations. In such systems, many security vulnerabilities and threats come from the interactions between the cyber and physical domains. An approach to holistically integrate security vulnerability analysis and protections in both domains will become increasingly necessary. There is growing demand to secure the rapidly increasing population of connected, and often mobile, things. In contrast to today's networks, where assets under protection are typically inside firewalls and protected with access control devices, many things in the IoT arena will operate in unprotected or highly vulnerable environments (i.e. vehicles, sensors, and medical devices used in homes and embedded on patients). Protecting such things poses additional challenges beyond enterprise networks [60].

Many Internet of Things applications require mobility support and geo-distribution in addition to location awareness and low latency, while the data need to be processed in "real-time" in micro clouds or fog. Micro cloud or Fog computing enables new applications and services applies a different data management and analytics and extends the Cloud Computing paradigm to the edge of the network. Similar to Cloud, Micro Cloud/Edge Cloud/Fog provides data, compute, storage, and application services to end-users.

The Micro Cloud or the Edge Cloud/Fog needs to have the following features in order to efficiently implement the required IoT applications:

- Low latency and location awareness
- Wide-spread geographical distribution
- Mobility
- Very large number of nodes
- Predominant role of wireless access
- Strong presence of streaming and real time applications
- Heterogeneity

The worlds of IT and telecommunications networking are converging bringing with them new possibilities and capabilities that can be deployed into the network. A key transformation has been the ability to run IT based servers at network edge, applying the concepts of cloud computing. This is defined as Mobile Edge computing [69]. Mobile edge computing can be seen as a cloud server running at the edge of a mobile network and performing specific tasks

that could not be achieved with traditional network infrastructure. IoT/M2M gateway and control functions are typical examples, but there are many others. Mobile edge computing is characterized by [69]:

- On-Premises: The Edge is local, meaning that it can run isolated from the rest of the network, while having access to local resources. This becomes particularly important for M2M scenarios, for example when dealing with security or safety systems that need high levels of resilience.
- Proximity: Being close to the source of information, Edge Computing is particularly useful to capture key information for analytics and big data. Edge computing may also have direct access to the devices, which can easily be leveraged by business specific applications.
- Lower latency: As Edge services run close to end devices it considerably reduces latency. This can be utilized to react faster, to improve user experience, or to minimize congestion in other parts of the network.
- Location awareness: When a Network Edge is part of a wireless network, whether it is Wi-Fi or Cellular, a local service can leverage low-level signalling information to determine the location of each connected device. This gives birth to an entire family of business-oriented use cases, including Location Based Services, Analytics, and many more.
- Network context information: Real-time network data (such as radio conditions, network statistics, etc.) can be used by applications and services to offer context-related services that can differentiate the mobile broadband experience and be monetized. New applications can be developed (which will benefit from this real-time network data) to connect mobile subscribers with local points-of-interest, businesses and events.

Mobile Edge computing transforms base stations into intelligent service hubs that are capable of delivering highly personalized services directly from the very edge of the network while providing the best possible performance in mobile networks. Proximity, context, agility and speed can be translated into unique value and revenue generation, and can be exploited by operators and application service providers to create a new value chain [69].

For the future IoT applications it is expected that more of the network intelligence to reside closer to the source. This will push for the rise of Edge Cloud/Fog, Mobile Edge computing architectures, as most data will be too noisy or latency-sensitive or expensive to be transfer to the cloud.

3.5.2 Federated IoT Data Cloud and Orchestration of Large Scale Services

The rapid evolution of Sensor Technologies, the Semantic Web consolidation and the extensive deployment of Cloud Computing Systems provide a unique opportunity to unify the real and the virtual worlds (Internet of Things). The Internet of Things enables the building of very large infrastructures that for the first time facilitate the information-driven real-time integration of the physical world and computers (Cyber Physical Systems) on a global scale (connecting sensor with systems and systems with the web). At the same time IoT can be considered a flexible middleware technology that abstracts from heterogeneous sensor network technologies to higher-level functionalities to enable interconnected sensor networks and processing of sensor data (Sensor Internet). It is a cornerstone for enabling Semantic Reality.

Cloud computing comprises the computing capacity necessary to run background operations to facilitate the complex IoT data analytics. The vision towards a Global Internet of Things requires not only emergent technologies but heterogeneous IoT system of systems coordinated via Federated services platforms. The deployment of IoT Data Cloud management systems and the orchestration of Large Scale Services are also important to enable a "global" view of the services and IoT infrastructures. In a global Internet of Things, control of sensors or infrastructure became a secondary role as per the Internet of Things services creation mechanisms are focused on providing capabilities and functionality and repurposing services and data rather than configurations and infrastructure adaptation/changes.

The sheer size of global Internet of Things systems pose novel and unique challenges, as it can only be engineered and deployed if a large degree of self-organization and automation capabilities are offered (large-scale deployments). Global internet of Things are built into the system and its constituents, enabling simple deployment (plug-and-play), dynamic (re-)configuration, re-purposing of technology and flexible component and information integration alike tailored information delivery based on user context and needs in a service-oriented way. This requires semantic descriptions of the user needs and contexts, and of the system's constituents, the data streams they produce, their functionalities and their requirements to enable a machine-understandable information space of real-world entities and their dynamic communication processes on a scale that is beyond the current size of the Internet.

IoT is expanding rapidly and is changing the perception of our daily life, not only from a technological perspective but also our personal activities, professional career and also in the way we establish social interactions. IoT is already considered as crucial in the process for designing the Future Internet. It is expected IoT will revolution our perception of the world enabling more smartness to the different external aspects of the human being (cities, industries, agriculture, clothing, fashion, etc.)

Currently Internet of Things not only has planned the model for "global" distributed infrastructures worldwide interconnected but envisioned the creation of distributed applications that rely in non-proprietary technologies (e.g. Web of Things, Internet of Everything, and the Physical Web). The adoption of IoT technology and its immersion in the society is generating high demands for high volumes of data and the capacity for storing, processing and analysing it in real time.

Based on the evolution of sensor technologies and the semantic technologies to unify the real and the virtual worlds this global vision is becoming a reality. It is yet a need for investigating the convergence of systems and technology platforms (e.g. software systems, the semantic web technologies and the Internet). The main objective is for developing flexible IoT middleware solutions/technology which abstracts data from heterogeneous sensor networks and bring this to a higher application-level(s) for enabling extended systems' functionalities and also enable interconnected sensor networks and sensor web data interoperability.

Extensive attention is necessary to focus on the deployment, maintenance and monitoring work on large-scale deployments, big sensor data collection and annotation and investigate data transformation and processing by means of advance stream processing techniques. To this end it is necessary to work on the design principles for device and infrastructure-related architectures, technologies and protocol frameworks for Internet connected heterogeneous devices.

3.5.2.1 IoT Data Analytics

The need for efficient Methods and Algorithms for Big Data, Collection and Transformation following self-Organization and self-Management paradigms still remains as one of the main objectives in the evolution towards Global Internet of Things. Cloud Computing Infrastructures and Management Platforms have evolved but Privacy and Security-Enabled Middleware Platforms are expected research activities in relation to topics that are not limited to Cloud Infrastructures for Data Analytics, Security, Privacy and Trust, Recommender

Systems and Clustering Mechanisms, Federation and Orchestration, Service Configuration and Control, Ontology Engineering and Applied Semantics alike Modelling and Reasoning Techniques.

A major effort on investigating the convergence of software systems, the semantic web and the Internet, heavily focused on the evolution of sensor technologies and the semantic technologies to unify the real and the virtual worlds. Development of flexible IoT middleware technology which abstracts data from heterogeneous sensor networks and bring this to a higher application-level(s) for enabling extended systems' functionalities and also enable interconnected sensor networks and sensor web data interoperability by using the Internet. Extensive work on large-scale deployments, big sensor data collection and annotation is due to come and investigate data transformation and processing by means of advance stream processing techniques query languages and reasoning techniques for the amount of generated data in the city. Design efforts for defining principles for device and infrastructure-related architectures, technologies and protocol frameworks for Internet connected heterogeneous devices.

Based on the evolution of sensor technologies and the semantic technologies it is possible to unify the real and the virtual worlds. There is yet the need for investigating the convergence of systems and technology platforms (e.g. software systems, the semantic web technologies and the Internet). The main objective is for developing flexible IoT middleware solutions/technology which abstracts data from heterogeneous sensor networks and bring this to a higher application-level(s) for enabling extended systems' functionalities and also enable interconnected sensor networks and sensor web data interoperability by using the Internet. Extensively is necessary to focus on the deployment, maintenance and monitoring work on large-scale deployments, big sensor data collection and annotation and investigate data transformation and processing by means of advance stream processing techniques. To this end it is necessary to work on the design principles for device and infrastructure-related architectures, technologies and protocol frameworks for Internet connected heterogeneous devices.

3.5.3 IoT Interoperability and Semantic Technologies

The previous IERC SRIAs have identified the importance of interoperability semantic technologies towards discovering devices, as well as towards achieving semantic interoperability.

Interoperability is defined as the ability of two or more systems or components to exchange data and use information this provides many challenges on how to get the information, to exchange data, and to understand and process the information. There are four basic IoT interoperability layers to be thoroughly tested and validated: technical, syntactical, semantic, and organizational.

- Technical Interoperability is usually associated with hardware/software components, systems and platforms that enable machine-to-machine communication to take place. This kind of interoperability is often centred on (communication) protocols and the infrastructure needed for those protocols to operate.
- Syntactical Interoperability is usually associated with data formats. Certainly, the messages transferred by communication protocols need to have well-defined syntax and encoding, even if it is only in the form of bit-tables. However, many protocols carry data or content, and this can be represented using high-level transfer syntaxes such as HTML, XML or ASN.1.
- Semantic Interoperability is usually associated with the meaning of content and concerns the human rather than machine interpretation of the content. Thus, interoperability on this level means that there is a common understanding between people of the meaning of the content (information) being exchanged.
- Organizational Interoperability is the ability of organizations to effectively communicate and transfer (meaningful) data (information) even though they may be using a variety of different information systems over widely different infrastructures, possibly across different geographic regions and cultures.

Organizational interoperability depends on the former three. Following the definitions and the trends on ICT sector about sensors and sensor data we can add two other dimensions: Static and dynamic interoperability.

- Dynamic interoperability: Two products cannot interoperate if they do not implement the same set of options (“services”). Therefore when specifications are including a broad range of options, this aspect could lead to serious interoperability problem. Solutions to overcome these aspects consist of definition clearly in a clear document the full list options with all conditions (e.g. defined as PICS in ISO 9646 [77]) as well as to define set of profiles. In the latter case, defining profile would help to truly check interoperability between two products in the same family or

from different family if the feature checked belongs to the two groups. We could consider this aspect as

- Static interoperability using approach of the well-known OSI overall test methodology ISO 9646 [77], where there is definition of static conformance review. Conformance testing consists of checking whether an Implementation Under Test (ITU) satisfies all static and dynamic conformance requirements. For the static conformance requirements this means a reviewing process of the options (PICS) delivered with the IUT. This is referred to as the static conformance review. This aspect could appear easy but that represent serious challenge in the IoT field due the broad range of applications.

The solutions that use non-interoperable solutions lead to increase of complexity in communicating and interpreting their data and services. One interesting research is to accept differences and potential non-interoperability for instance between two different protocols but to adapt on the fly. We see also such features in intelligent gateways and middleware. This can be called dynamic interoperability and should be a continuous important research area in particular with the growing complexity and heterogeneity of IoT environments.

The challenges for IoT interoperability are many and there is a need for an interoperability framework to address them in a consistent manner under the IoT architectural model. These challenges require addressing a number of research topics as presented in Table 3.1.

Table 3.1 IoT Interoperability research topics

Challenges	Research Topics
Discovery of objects and Clustering	• Algorithms for data selection and classification • Efficient clustering mechanisms • IoT service management systems
Privacy and Security at Technical and Semantic level	• Access control algorithms and tools • Rules-based systems • IoT systems federation
Quality of Data	• Data filtering and data selection • Data mining • Control and assurance
Reasoning and Analysis	• Taxonomy, modelling, • Probabilistic modelling • Inference, Abstraction and Abduction
Data Management	• Data fusion • Mash-ups processing • Stream processing

There are arguments against using semantics in constrained environments since ontologies and semantic data can add too much overhead in the case of devices with limited resources. However, ontologies are a way to share and agree on a common vocabulary and knowledge; at the same time there are machine-interpretable and represented in interoperable and re-usable forms. There is no need to add semantic metadata in the source, since this could be added to the data at a later stage (e.g. in a gateway that have mere functionalities). The legacy applications can ignore these ontologies or can be extended to work with it.

In IoT applications semantic technologies will have an important role in enabling sharing and re-use of virtual objects as a service through the cloud. The semantic enrichment of virtual object descriptions will realise for IoT what semantic annotation of web pages has enabled in the Semantic Web. Associated semantic-based reasoning will assist IoT users to more independently find the relevant proven virtual objects to improve the performance or the effectiveness of the IoT applications they intend to use.

3.6 Networks and Communication

Present communication technologies span the globe in wireless and wired networks and support global communication by globally-accepted communication standards. The Internet of Things Strategic Research and Innovation Agenda (SRIA) intends to lay the foundations for the Internet of Things to be developed by research through to the end of this decade and for subsequent innovations to be realised even after this research period. Within this timeframe the number of connected devices, their features, their distribution and implied communication requirements will develop; as will the communication infrastructure and the networks being used. Everything will change significantly. Internet of Things devices will be contributing to and strongly driving this development.

Changes will first be embedded in given communication standards and networks and subsequently in the communication and network structures defined by these standards.

3.6.1 Networking Technology

Mobile traffic today is driven by predictable activities such as making calls, receiving email, surfing the web, and watching videos. Over the next 5 to 10 years, billions of IoT devices with less predictable traffic patterns will join

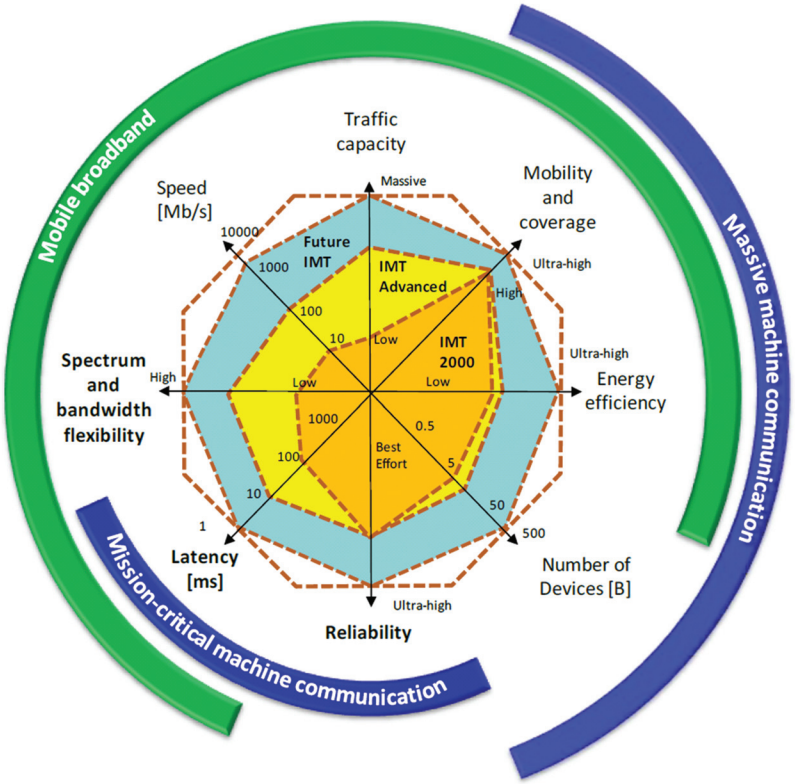

Figure 3.23 Global perspective – 5G capabilities [157].

the network, including vehicles, machine-to-machine (M2M) modules, video surveillance that requires 24-7 bandwidth, or different types of sensors that send out tiny bits of data each day. The rise of cloud computing requires new network strategies for fifth evolution of mobile the 5G, which represents clearly a convergence of network access technologies. The architecture of such network has to integrate the needs for IoT applications and to offer seamless integration. To make the IoT and M2M communication possible there is a need for fast, high-capacity networks.

The capabilities depicted in Figure 3.23 are the following [157]:

- *Traffic capacity* relates to the capability to manage a certain amount of offered traffic per area unit.
- *Mobility/coverage* refers to the capability to provide connectivity in any situation; on the move and when standing still, regardless of user location.

- *Network and device energy efficiency* relates to the energy consumption in both wireless devices and network infrastructure.
- *Massive number of devices* relates to the capability to handle a large number of connected devices per area unit, while preventing that the related control signalling overhead limits the user experience.
- *Reliability* relates to the capability to provide a given service level with very high probability. If reliability is high enough, mission-critical and safety-of-life applications can be supported.
- *Latency* refers to the time the system needs to transport data through its own domain of responsibility.
- *Spectrum and bandwidth flexibility* refers to the flexibility of the system design to handle different spectrum scenarios, and in particular to the capability to handle higher frequencies and wider bandwidths than today.
- *Achievable end user data rate* refers to the maximum data rate a user typically experiences (i.e. the "perceived speed" of the data connection).

The capabilities relate to the use cases for future international mobile telecommunications, as shown through the arches at the edge of the figure.

- Mobile Broadband is the human centric use case for non-limited access to services and data anytime and anywhere.
- Mission-critical machine communication is a use case where communication between machines is required to have an exactly defined behaviour in terms of key KPIs such as guaranteed throughput, latency, etc. Examples are wireless control of industrial manufacturing or production processes, traffic safety applications, etc.
- Massive Machine Communication is a use case mainly characterized by a very large number of connected devices which typically transmit relatively low volume of non-delay-sensitive data. Devices are required to be simple and cheap, and have a very long battery life.

5G networks will deliver 1,000 to 5,000 times more capacity than 3G and 4G networks today and will be made up of cells that support peak rates of between 10 and 100 Gbps. They need to be ultra-low latency, meaning it will take data 1–10 milliseconds to get from one designated point to another, compared to 40–60 milliseconds today. Another goal is to separate communications infrastructure and allow mobile users to move seamlessly between 5G, 4G, and WiFi, which will be fully integrated with the cellular network. Networks will also increasingly become programmable, allowing operators to make changes to the network virtually, without touching the physical infrastructure. The capabilities of Future and previous future

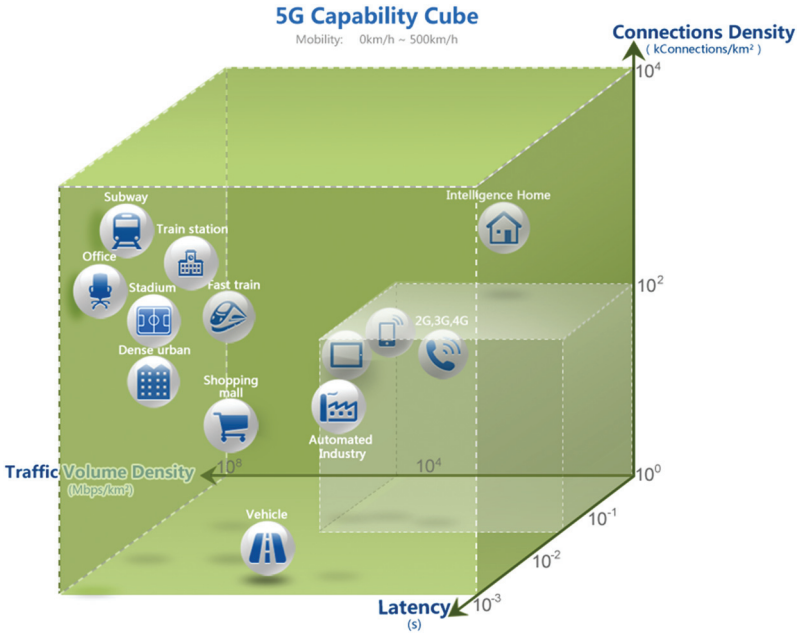

Figure 3.24 5G Capability cube (Source: Ericsson).

international mobile telecommunications systems are depicted in Figure 3.24. Future international mobile telecommunications will encompass all the capabilities of the previous systems. The performance requirements in some scenarios will increase significantly due to new services arising and spreading.

The evolution and pervasiveness of present communication technologies has the potential to grow to unprecedented levels in the near future by including the world of things into the developing Internet of Things. Network users will be humans, machines, things and groups of them.

3.6.2 Communication Technology

The growth in mobile device market is pushing the deployment of Internet of Things applications where these mobile devices (smart phones, tablets, etc. are seen as gateways for wireless sensors and actuators.

Communications technologies for the Future Internet and the Internet of Things will have to avoid such bottlenecks by construction not only for a given status of development, but for the whole path to fully developed and still growing nets.

Many types of Internet of Things devices will be connected to the energy grid all the time; on the other hand a significant subset of Internet of Things devices will have to rely on their own limited energy resources or energy harvesting throughout their lifetime.

The inherent trend to higher complexity of solutions on all levels will be seriously questioned – at least with regard to minimum energy Internet of Things devices and services.

Their communication with the access edges of the Internet of Things network shall be optimized cross domain with their implementation space and it shall be compatible with the correctness of the construction approach.

The next years' M2M associated with the Internet of Things could be SIM-*less*, meaning "wireless, long-range, low-power, low data-rate and without SIM-card". A deep revolution in the landscape of M2M wireless radio communication technologies is taking off. Until now, in the field of M2M, only GPRS, SMS, 3G technologies based on the SIM card principle allowed to pass information over long distances between an object and a remote information system. Once the SIM card is integrated in the sensor, the object becomes communicating. It can be fixed (drinks vending machine, tank, thermostat, energy box, smoke detector, parking meter) or mobile (wagons, containers, heavy vehicles, bicycles). A sensor then records data locally and transmits it automatically via the integrated GSM modem to the remote information system.

Figure 3.25 Communication standards [158].

Innovative wireless communication technologies create new perspectives for IoT applications. Companies such as Sigfox (French IoT operator using its own technology), Weightless (promoted mainly in UK), LoRa (french Cycleo technology acquired by the founder Semtech) are introducing these wireless communication technologies. This new technologies push for the emergence of new attractive and alternative business models for certain IoT applications with subscriptions ranging from 1 € to 20 € per year without cost of data. While these solutions can only transmit a small amount of data per message (dozens or even hundreds of kilobytes per message), they however cover well over 80% of M2M and IoT's needs. Some applications have already rejected the SIM-card GSM approach to precisely focus on SIM-*less*. This is the case for smart meters. Except for market's structural cause, over the next eight years, nearly 200 million residential meters (Water, Gas, Electricity) across the members of the Euro zone countries will be connected and half will be equipped with SIM-*less* technology (and the other half in PLC) [158].

3.7 Data Management

Data management is a crucial aspect in the Internet of Things. When considering a world of objects interconnected and constantly exchanging all types of information, the volume of the generated data and the processes involved in the handling of those data become critical.

In this context there are many technologies and factors involved in the "data management" within the IoT context.

Some of the most relevant concepts which enable us to understand the challenges and opportunities of data management are:

- Data Collection and Analysis
- Big data
- Semantic Sensor Networking
- Virtual Sensors
- Complex Event Processing

Data Collection and Analysis modules or capabilities are the essential components of any IoT platform or system, and they are constantly evolving in order to support more features and provide more capacity to external components (either higher layer applications leveraging on the data stored by the DCA module or other external systems exchanging information for analysis or processing). The DCA module is part of the core layer of any IoT platform.

An example of data management framework for IoT is presented in [73] that incorporates a layered, data-centric, and federated paradigm to join the independent IoT subsystems in an adaptable, flexible, and seamless data network. In this framework, the "Things" layer is composed of all entities and subsystems that can generate data. Raw data, or simple aggregates, are then transported via a communications layer to data repositories. These data repositories are either owned by organizations or public, and they can be located at specialized servers or on the cloud. Organizations or individual users have access to these repositories via query and federation layers that process queries and analysis tasks, decide which repositories hold the needed data, and negotiate participation to acquire the data. In addition, real-time or context-aware queries are handled through the federation layer via a sources layer that seamlessly handles the discovery and engagement of data sources. The whole framework allows a two-way publishing and querying of data. This allows the system to respond to the immediate data and processing requests of the end users and provides archival capabilities for later long-term analysis and exploration of value-added trends.

In the context of IoT, data management systems must summarize data online while providing storage, logging, and auditing facilities for offline analysis. This expands the concept of data management from offline storage, query processing, and transaction management operations into online-offline communication/storage dual operations. The lifecycle of data within an IoT system is illustrated in Figure 3.26, proceeds from data production to aggregation, transfer, optional filtering and pre-processing, and finally to storage and archiving. Querying and analysis are the end points that initiate (request) and consume data production, but data production can be set to be "pushed" to the IoT consuming services. Production, collection, aggregation, filtering, and some basic querying and preliminary processing functionalities are considered online, communication-intensive operations. Intensive pre-processing, long-term storage and archival and in-depth processing/analysis are considered offline storage-intensive operations [73].

The proposed IoT data management framework consists of six stacked layers, two of which include sub-layers and complementary or twin layers. The framework layers map closely to the phases of the IoT data lifecycle with lookup/orchestration considered to be an added process that is not strictly a part of the data lifecycle. The *"Things" Layer* encompasses IoT sensors and smart objects (data production objects), as well as modules for in-network processing and data collection/real-time aggregation (processing,

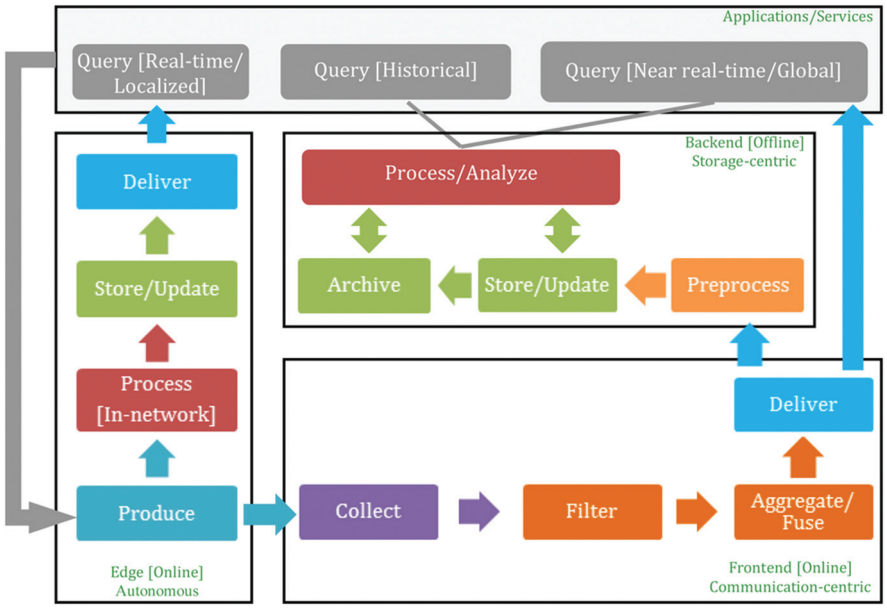

Figure 3.26 IoT data lifecycle and data management [73].

aggregation). The *Communication Layer* provides support for transmission of requests, queries, data, and results (collection and delivery). The *Data/Sources twin layers* respectively handle the discovery and cataloguing of data sources and the storage and indexing of collected data (data storage/archival). The Data Layer also handles data and query processing for local, autonomous data repository sites (filtering, pre-processing, processing).

The *Federation Layer* provides the abstraction and integration of data repositories that is necessary for global query/analysis requests, using meta-data stored in the Data Sources layer to support real-time integration of sources as well as location-centric requests (pre-processing, integration, fusion). The *Query Layer* handles the details of query processing and optimization in cooperation with the *Federation Layer* as well as the complementary *Transactions Layer* (processing, delivery). The Query Layer includes the *Aggregation Sub-Layer*, which handles the aggregation and fusion queries that involve an array of data sources/sites (aggregation/fusion). The *Application/ Analysis Layer* is the requester of data/analysis needs and the consumer of data and analysis results. The layers of the proposed IoT data management framework and their respective functional modules are illustrated in Figure 3.27 [73].

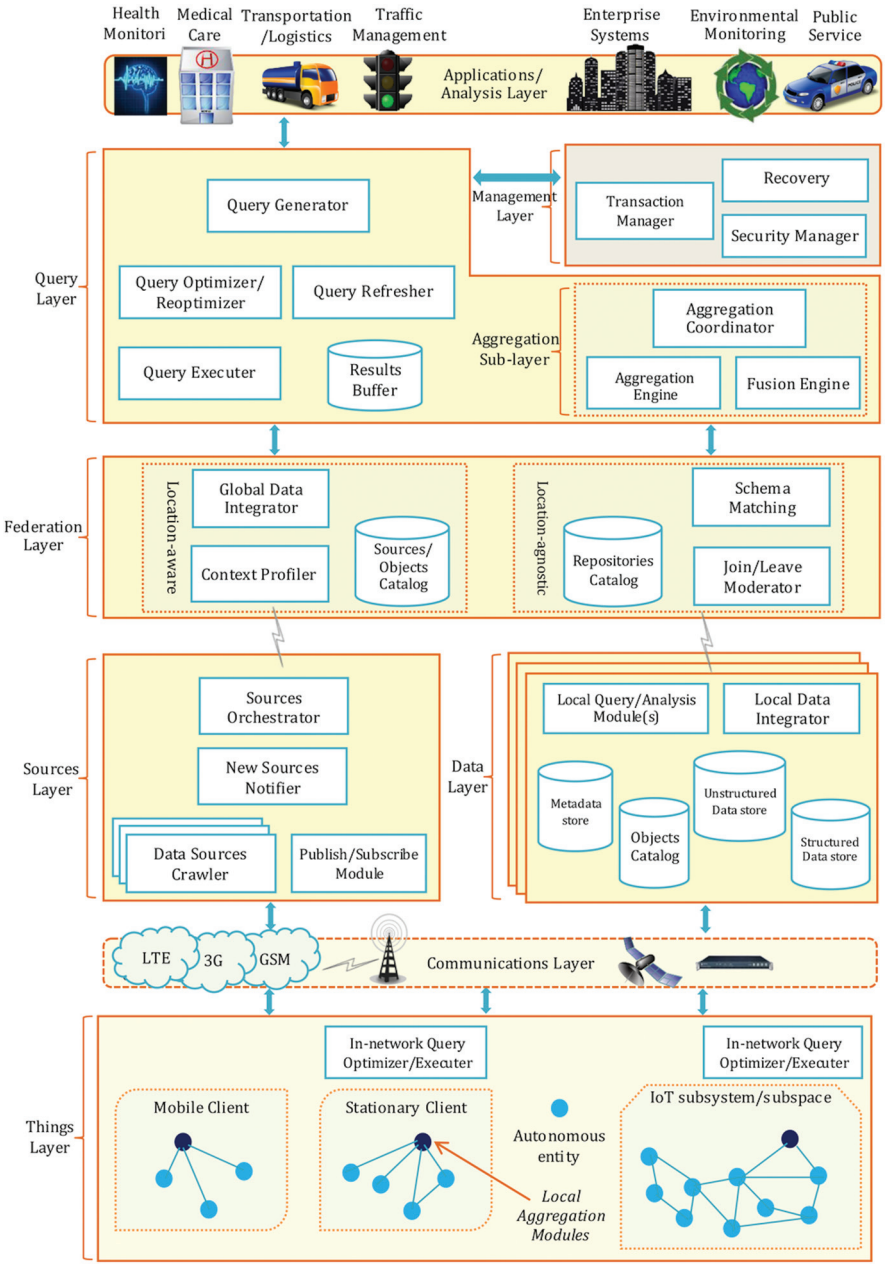

Figure 3.27 IoT data management framework [73].

3.7.1 Smart Data

Smart data is about the processing and analysis of large data repositories, so disproportionately large that it is impossible to treat them with the conventional tools of analytical databases. The machines generate data a lot faster than people can, and their production rates will grow exponentially with Moore's Law. Storing this data is cheap, and it can be mined for valuable information. Examples of this tendency include:

- Web logs
- RFID
- Sensor networks
- Social networks
- Social data (due to the Social data revolution)
- Internet text and documents
- Internet search indexing
- Call detail records
- Astronomy, atmospheric science, genomics, biogeochemical, biological, and other complex and/or interdisciplinary scientific research
- Military surveillance
- Medical records
- Photography archives
- Video archives
- Large scale e-commerce

3.8 A QoS Security Framework for the IoT Architecture

A Quality of Service (QoS) security framework would first and foremost mean that security requirements are met and compliance can be documented.

Security problems inherent with the wireless technologies (Internet, mobile communication networks, and sensor networks) are known and many of them addressed largely so that solutions are on the way. IoT presents new challenges to network and security architects. Specific and more evolved security solutions are required in order to cope with these challenges, which if not addressed may become barriers for the IoT deployment on a broad scale.

This section presents essential security considerations when designing a security framework for the IoT architecture and research aspects to be addressed in the near future. The starting point is a generic IoT architecture integrating physical objects communicating with each other and structured in several layers, suitable for resources-constrained devices. Security aspects are

addressed tailored to constraints of IoT scenarios and characteristics of IoT devices.

The basic components of a QoS security framework are identified, addressing both traditional security problems of communication networks and specific IoT threats. Larger space is dedicated to authentication and access control as important parts of any security chain, and vital for many scenarios in the IP-based IoT. They have their own specificity and have been the focus of recent standardization and certification efforts.

3.8.1 End-to-End Security. The Decentralized Approach.

Large-scale applications and services based on the IoT are increasingly vulnerable to disruption from attack or information theft. Vulnerability is the opportunity for a threat to cause loss and a threat is any potential danger to a resource, originating from anything and/or anyone that has the potential to cause a threat. Common IoT threats are presented in [72] together with requirements to make the IoT secure, involving several technological areas. The thread that is common through all these is the need for end-to-end security.

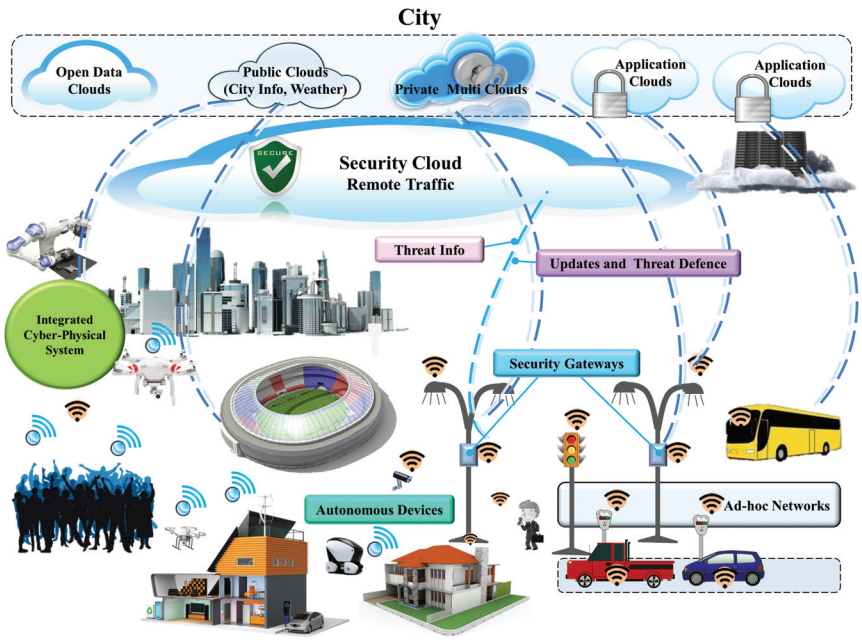

Figure 3.28 Smart City – Multi-layer security framework.

In order to fulfil the end-to-end security principles and IoT inherent requirements, a distributed approach seems to be the most suitable. With this approach, objects are becoming more intelligent, capable of making their own authorization decisions. The adoption of fine-grained authorization mechanisms allows for more flexible resources control and enables tolerance when fronting unknown-risks. In addition, IP security protocol variants for the IoT with public-key-based cryptographic primitives in their protocol design, such as Datagram TLS (DTLS), the HIP Diet EXchange (DEX), and minimal IKEv2, can fulfil the requirements of IoT regarding scalability and interoperability. End-to-end authentication, integrity confidentiality and privacy, are essential.

Important to keep in mind is that all the technologies must be tailored to the constraints of IoT scenarios and characteristics of IoT devices, including limited memory, compute resources, local security, backup connectivity. Thus the employed technologies must reduce the need for expensive cryptographic operations, prevent DoS attacks targeting the security mechanism, improve tolerance to attacks, etc.

3.8.2 Standardization. Certification. Interoperability.

Standardization and certification activities play an important role in securing the IoT, both in terms of enhancing interoperability of IoT devices and adoption of security solutions by the industry. Many of the security solutions are proprietary making it difficult for the IoT devices to communicate with each other in an interoperable manner and in formulation a common and sound security vision in order to standardize security solutions for the IoT. The efforts in the Internet Engineering Task Force (IETF) are making progress exactly in this direction.

3.8.3 Components of a QoS Security Framework

A Quality of Service (QoS) security framework would first and foremost mean that security requirements are met and compliance can be documented.

The basic components of a QoS security framework are:

- Authentication. Implements authentication of users and devices, including identity management in order to ensure authentication, accountability and privacy.
- Authorization. Implements access control on devices and services, in order to ensure data confidentiality and integrity.

- Network. Implements protocols to route and transport control, management and traffic securely over the infrastructure, thus ensuring communication confidentiality and integrity.
- Trust management. Implements remote control, over-the-air update, logging, analytics, in order to document compliance with security requirements and other security related regulations and standards.

3.8.3.1 Authentication

At the core of the security framework for IoT architecture is the authentication component, used to provide and verify the identify information of IoT objects.

According to ISO/IEC 27002, authentication is the act of establishing, or confirming something (or someone) as authentic, i.e., that claims made by, or about the thing are true. Thus, an authentication relationship is initiated based on the identity of the IoT device, whenever the device needs access to the IoT infrastructure.

Some of the traditional authentication technologies in wireless networks, including lightweight public key-based authentication technology, pre-shared key authentication technology, random key pre-distribution authentication technology, the certification based on auxiliary information, the certification based on one-way hash function, can be employed.

However, most of the traditional authentication mechanisms are based on human credentials, such as username and password, token or biometrics, roles in the organizations, etc. For the IoT objects the identity information is different, first and foremost because the process does not involve human intervention. Such information includes RFID, X.509 certificates, MAC address or any other unique hardware based information. However, many devices may have limited memory to store certificates or CPU power to execute the validation operations inherent to such certificates. Near future research much therefore address other credential types.

Another challenge deriving from the IoT devices being usually unattended, is the fact that the equipment is accessible to attacks, targeting exactly the security mechanisms. Accessing the IoT infrastructure with hacked/illegal equipment can create serious damages for the users, such as conflict of interests in addition to the network security issues.

3.8.3.2 Authorization

Authorization is the next component in the security chain, building upon the information provided by the authentication component. Both authentication

and authorization must be in place in order to establish a secure relationship between IoT devices to exchange appropriate information.

According to ISO/IEC 27002, authorization is the process of controlling access and rights to resources.

The state of art and practice for policy mechanisms to manage and control access to consumer and enterprise networks is well advanced so it would only be natural to adopt them for the IoT. The most common scenario is that for a user to have the privileges to access a resource, the user must satisfy certain conditions, such as being assigned certain roles, belonging to certain specific groups, etc.

However, it is clear based on the type of identity information delivered by the authentication component that the traditional role-based access control mechanism (RBAC) is no longer the focus. In the IoT world, the attributes of a node or an IoT object make more sense, so that a fine-grained mechanism such as the attribute-based access control (ABAC) is more suitable.

Although being standard technologies, RBAC and ABAC cannot be applied straightforward to IoT. The challenge with the IoT is that very often there are many different contexts around an IoT identity, so that a centralized solution would not be feasible. The decisions must be made by the IoT objects able to capture local information. Authorization within a central entity would also impact on the scalability of the solution.

A multi context-aware authorization mechanism is necessary. Environment conditions which are captured locally by IoT end-devices may also come into the picture. The authorization component becomes more complex because at any point in time during the authorization process it should be clear: who is requesting the access, who is granting the access, what specific access is being requested, what is the access scope, when is the access requested and granted/denied, what is the access's duration?

A key challenge is therefore the IoT devices capability to capture security-relevant contextual information, such as time, location, state of the environment, etc., and use it to make access decision, when the access requests are issued. More research is needed in this direction.

3.8.3.3 Network

This component encompasses the elements that route and transport endpoint traffic securely over the infrastructure, whether control, management or actual data traffic. There are already established protocols and mechanisms to secure the network infrastructure and affect policy that are well suited to the IoT.

3.8.3.4 Trust Management

This is the component responsible for remote control, over-the-air update, logging of all security-related activities in the IoT environment, producing statistics and document compliance with all security requirements.

As IoT-scale applications and services will scale over multiple administrative domains and involve multiple ownership regimes, there is a need for a trust framework to enable the users of the system to have confidence that the information and services being exchanged can indeed be relied upon. It needs to be able to deal with humans and machines as users, i.e. it needs to convey trust to humans and needs to be robust enough to be used by machines without denial of service.

Trust can only be achieved by building continuous compliance into the IoT infrastructure. By this we mean that embedding techniques into the IoT devices that allow at any point in time to prove (as opposed to only claiming) that the IoT environment complies with the security requirements, the ever-changing laws and regulations related to security and other interoperability requirements inherent to the modern, more complex IoT environments.

3.9 Discussion

In the future the enterprises will make extensive use of IoT technology, and there will be a wide range of products sold into various markets, such as advanced medical devices; factory automation sensors and applications in industrial robotics; sensor motes for increased agricultural yield; and automotive sensors and infrastructure integrity monitoring systems for diverse areas, such as road and railway transportation, water distribution and electrical transmission. By 2020, component costs will have come down to the point that connectivity will become a standard feature, even for processors costing less than $1. This opens up the possibility of connecting just about anything, from the very simple to the very complex, to offer remote control, monitoring and sensing and it is expected that the variety of devices offered to explode [84].

The economic value added at the European and global level is significant across sectors in 2020. The IoT applications are still implemented by the different industrial verticals with a high adoption in manufacturing, healthcare and home/buildings.

IoT will also facilitate new business models based on the real-time data acquired by billions of sensor nodes. This will push for development of

advances sensor, nanoelectronics, computing, and network and cloud technologies and will lead to value creation in utilities, energy, smart building technology, transportation and agriculture.

The IoT's paradigm is based around the idea of connecting things to each other, so it's essential create technology ecosystems and work with other companies that excel at creating IoT devices, gateways, communication/cloud computing platforms, services and applications. As the number of telecommunications providers, device manufacturers, consulting firms, and business software companies supplying IoT services grows, it's easier for enterprises to find the right providers with whom to partner. In order to address the totality of interrelated technologies the IoT technology ecosystem is essential and the enabling technologies will have different roles such as components, products/applications, and support and infrastructure in these ecosystems. The technologies will interact through these roles and impact the IoT technological deployment [50].

IoT ecosystems offer solutions comprising a large system beyond a platform and solve important technical challenges in the different verticals and across verticals. These IoT technology ecosystems are instrumental for the deployment of large pilots and can easily be connected to or build upon the core IoT solutions for different applications in order to expand the system of use and allow new and even unanticipated IoT end uses.

The IoT architecture needs to consider key scenarios, to design for common problems, to appreciate the long term consequences of key decisions in such a way that builds a solid foundation for developing IoT applications, based on specific scenarios and requirements. This is essential for both developing the IoT ecosystems and deploying successfully large IoT application pilots.

If the IoT architecture is not good enough and the software developed is unstable, the development is unable to support existing or future business requirements, and it is difficult to deploy or manage it in a large IoT pilot environment.

One challenge is exchanging the data from and among the things/objects in an interoperable format. This requires creating systems that cross vertical silos and harvest the data across domains, which unleashes useful IoT applications that are user centric, context aware, and are able to create new services by communication across those verticals.

These exchange and processing capabilities are an intrinsic part of the IoT concept and they can be applied to applications in areas such as the Internet of Energy (IoE), the Internet of Lighting (IoL), the Internet of Buildings (IoB), and, in a city context, the Internet of Vehicles (IoV).

The final aim is to create a city-centric ecosystem comprising state-of-the-art and viable technologies which apply the IoT, IoE and IoV concepts to increase the city efficiency by enabling unobtrusive, adaptable and highly usable services at the network-edge, gateway and cloud levels. In this context stimulating the creation of IoT ecosystems (comprising of stakeholders representing the IoT application value-chain: components, chips, sensors, actuators, embedded processing and communication, system integration, middleware, architecture design, software, security, service provision, usage, test, etc.), integrating the future generations of applications, devices, embedded systems and network technologies and other evolving ICT advances, based on open platforms and standardised identifiers, protocols and architectures is of paramount importance. In addition the deployment of IoT Large Scale Pilots to promote the market emergence of IoT and overcome the fragmentation of vertically oriented closed systems, architectures and application areas that address challenges in different application areas by bringing together the technology supply and the application demand sides in real-life settings is the next important step to demonstrate and validate the technology in real environments [50].

Acknowledgments

The IoT European Research Cluster – European Research Cluster on the Internet of Things (IERC) maintains its Strategic Research and Innovation Agenda (SRIA), taking into account its experiences and the results from the on-going exchange among European and international experts.

The present document builds on the 2010, 2011, 2012, 2013 and 2014 Strategic Research and Innovation Agendas and presents the research fields and an updated roadmap on future R&D from 2015 to 2020 and beyond 2020.

The IoT European Research Cluster SRIA is part of a continuous IoT community dialogue supported by the European Commission (EC) DG Connect – Communications Networks, Content and Technology, E1 – Network technologies Unit for the European and international IoT stakeholders. The result is a lively document that is updated every year with expert feedback from on-going and future projects financed by the EC. Many colleagues have assisted over the last few years with their views on the Internet of Things Strategic Research and Innovation agenda document. Their contributions are gratefully acknowledged.

Internet of Things Timelines

Table 3.2 Future Technological Developments

Development	2015–2020	Beyond 2020
Identification Technology	• Identity management • Open framework for the IoT • Soft Identities • Semantics • Privacy awareness	• "Thing/Object DNA" identifier • Context aware identification
Internet of Things Architecture Technology	• Network of networks architectures • IoT reference architecture developments • IoT reference architecture standardization • Adaptive, context based architectures • Self-* properties	• Cognitive architectures • Experimental architectures
Internet of Things Infrastructure	• Cross domain application deployment • Integrated IoT infrastructures • Multi-application infrastructures • Multi provider infrastructures	• Global, general purpose IoT infrastructures • Global discovery mechanism
Internet of Things Applications	• Configurable IoT devices • IoT in food/water production and tracing • IoT in manufacturing industry • IoT in industrial lifelong service and maintenance • IoT device with strong processing and analytics capabilities • Application capable of handling heterogeneous high capability data collection and processing infrastructures	• IoT information open market • Autonomous Vehicles • Internet of Buildings • Internet of Energy • Internet of Vehicles • Internet of Lighting

Communication Technology	• Wide spectrum and spectrum aware protocols • Ultra low power chip sets • On chip antennas • Millimetre wave single chips • Ultra low power single chip radios • Ultra low power system on chip	• Unified protocol over wide spectrum • Multi-functional reconfigurable chips
Network Technology	• Network context awareness • Self-aware and self-organizing networks • Sensor network location transparency • IPv6- enabled scalability	• Network cognition • Self-learning, self-repairing networks • Ubiquitous IPv6-based IoT deployment
Software and algorithms	• Goal oriented software • Distributed intelligence, problem solving • Things-to-Things collaboration environments • IoT complex data analysis • IoT intelligent data visualization • Hybrid IoT and industrial automation systems	• User oriented software • The invisible IoT • Easy-to-deploy IoT SW • Things-to-Humans collaboration • IoT 4 All • User-centric IoT
Hardware	• Smart sensors (bio-chemical) • More sensors and actuators (tiny sensors) • Sensor integration with NFC • Home printable RFID tags	• Nano-technology and new materials
Data and Signal Processing Technology	• Context aware data processing and data responses • Energy, frequency spectrum aware data processing	• Cognitive processing and optimisation

(*Continued*)

Table 3.2 Continued

Development	2015–2020	Beyond 2020
Discovery and Search Engine Technologies	• Automatic route tagging and identification management centres • Semantic discovery of sensors and sensor data	• Cognitive search engines • Autonomous search engines
Power and Energy Storage Technologies	• Energy harvesting (biological, chemical, induction) • Power generation in harsh environments • Energy recycling • Long range wireless power • Wireless power	• Biodegradable batteries • Nano-power processing unit
Security, Privacy & Trust Technologies	• User centric context-aware privacy and privacy policies • Privacy aware data processing • Security and privacy profiles selection based on security and privacy needs • Privacy needs automatic evaluation • Context centric security • Homomorphic Encryption • Searchable Encryption • Protection mechanisms for IoT DoS/DdoS attacks	• Self-adaptive security mechanisms and protocols • Self-managed secure IoT

Material Technology	• SiC, GaN • Improved/new semiconductor manufacturing processes/technologies for higher temperature ranges	• Diamond • Graphene
Interoperability	• Optimized and market proof interoperability approaches used • Interoperability under stress as market grows • Cost of interoperability reduced • Several successful certification programmes in place	• Automated self-adaptable and agile interoperability
Standardisation	• IoT standardization refinement • M2M standardization as part of IoT standardisation • Standards for cross interoperability with heterogeneous networks • IoT data and information sharing	• Standards for autonomic communication protocols

Table 3.3 Internet of Things Research Needs

Research Needs	2015–2020	Beyond 2020
Identification Technology	• Convergence of IP and IDs and addressing scheme • Unique ID • Multiple IDs for specific cases • Extend the ID concept (more than ID number) • Electro Magnetic Identification – EMID	• Multi methods – one ID
IoT Architecture	• Internet (Internet of Things) (global scale applications, global interoperability, many trillions of things)	
Internet of Things Infrastructure	• Application domain-independent abstractions & functionality • Cross-domain integration and management • Large-scale deployment of infrastructure • Context-aware adaptation of operation	• Self-management and configuration
Internet of Things Applications	• IoT information open market • Standardization of APIs • IoT device with strong processing and analytics capabilities • Ad-hoc deployable and configurable networks for industrial use • Mobile IoT applications for IoT industrial operation and service/maintenance • Fully integrated and interacting IoT applications for industrial use	• Building and deployment of public IoT infrastructure with open APIs and underlying business models • Mobile applications with bio-IoT-human interaction

SOA Software Services for IoT	• Quality of Information and IoT service reliability • Highly distributed IoT processes • Semi-automatic process analysis and distribution	• Fully autonomous IoT devices
Internet of Things Architecture Technology	• Code in tags to be executed in the tag or in trusted readers • Global applications Adaptive coverage • Universal authentication of objects • Graceful recovery of tags following power loss • More memory • Less energy consumption • 3-D real time location/position embedded systems	• Intelligent and collaborative functions • Object intelligence • Context awareness • Cooperative position cyber-physical systems
Communication Technology	• Longer range (higher frequencies – tenths of GHz) • Protocols for interoperability • On chip networks and multi standard RF architectures • Multi-protocol chips • Gateway convergence • Hybrid network technologies convergence • 5G developments • Collision-resistant algorithms • Plug and play tags • Self-repairing tags	• Self-configuring, protocol seamless networks

(*Continued*)

Table 3.3 Continued

Research Needs	2015–2020	Beyond 2020
Network Technology	• Grid/Cloud network • Software defined networks • Service based network • Multi authentication • Integrated/universal authentication • Brokering of data through market mechanisms • Scalability enablers • IPv6-based networks for smart cities	• Need based network • Internet of Everything • Robust security based on a combination of ID metrics • Autonomous systems for nonstop information technology service • Global European IPv6-based Internet of Everything

Software and algorithms	• Self-management and control
	• Micro operating systems
	• Context aware business event generation
	• Interoperable ontologies of business events
	• Scalable autonomous software
	• Evolving software
	• Self-reusable software
	• Autonomous things:
	  • Self-configurable
	  • Self-healing
	  • Self-management
	• Platform for object intelligence
		• Self-generating "molecular" software
		• Context aware software

Hardware Devices	• Polymer based memory • Ultra low power EPROM/FRAM • Molecular sensors • Autonomous circuits • Transparent displays • Interacting tags • Collaborative tags • Heterogeneous integration • Self-powering sensors	• Biodegradable circuits • Autonomous "bee" type devices

	• Low cost modular devices • Ultra low power circuits • Electronic paper • Nano power processing units • Silent Tags • Biodegradable antennae	
Hardware Systems, Circuits and Architectures	• Multi-protocol front ends • Ultra low cost chips with security • Collision free air to air protocol • Minimum energy protocols • Multi-band, multi-mode wireless sensor architectures implementations • Adaptive architectures • Reconfigurable wireless systems • Changing and adapting functionalities to the environments • Micro readers with multi standard protocols for reading sensor and actuator data • Distributed memory and processing • Low cost modular devices • Protocols correct by construction	• Heterogeneous architectures • "Fluid" systems, continuously changing and adapting
Data and Signal Processing Technology	• Common sensor ontologies (cross domain) • Distributed energy efficient data processing • Autonomous computing • Tera scale computing • Micro servers • Multi-functional gateways	• Cognitive computing • Cognitive, software-defined gateways

(*Continued*)

Table 3.3 Continued

Research Needs	2015–2020	Beyond 2020
Discovery and Search Engine Technologies	• Scalable Discovery services for connecting things with services while respecting security, privacy and confidentiality • "Search Engine" for Things • IoT Browser • Multiple identities per object • On demand service discovery/integration • Universal authentication	• Cognitive registries
Power and Energy Storage Technologies	• Paper based batteries • Wireless power everywhere, anytime • Photovoltaic cells everywhere • Energy harvesting • Power generation for harsh environments	• Biodegradable batteries
Interoperability	• Dynamic and adaptable interoperability for technical and semantic areas • Open platform for IoT validation	• Self-adaptable and agile interoperability approaches
Security, Privacy & Trust Technologies	• Low cost, secure and high performance identification/authentication devices • Access control and accounting schemes for IoT • General attack detection and recovery/ resilience for IoT • Cyber Security Situation Awareness for IoT • Context based security activation algorithms • Service triggered security • Context-aware devices	• Cognitive security systems • Self-managed secure IoT • Decentralised approaches to privacy by information localisation

	• Object intelligence • Decentralised self-configuring methods for trust establishment • Novel methods to assess trust in people, devices and data • Location privacy preservation • Personal information protection from inference and observation • Trust Negotiation	
Governance (legal aspects)	• Legal framework for transparency of IoT bodies and organizations • Privacy knowledge base and development privacy standards	• Adoption of clear European norms/standards regarding Privacy and Security for IoT
Economic	• Business cases and value chains for IoT • Emergence of IoT in different industrial sectors	• Integrated platforms
Material Technology	• Carbon nanotube • Conducting Polymers and semiconducting polymers and molecules • Modular manufacturing techniques	• Graphene

List of Contributors

Abdur Rahim Biswas, IT, create-net, iCore
Alessandro Bassi, FR, Bassi Consulting, IoT-A
Ali Rezafard, IE, Afilias, EPCglobal Data Discovery JRG
Amine Houyou, DE, SIEMENS, IoT@Work
Antonio Skarmeta, SP, University of Murcia, IoT6
Carlos Agostinho, PT, UNINOVA
Carlo Maria Medaglia, IT, University of Rome 'Sapienza', IoT-A
César Viho, FR, Probe-IT
Claudio Pastrone, IT, ISMB, ebbits, ALMANAC
Daniel Thiemert, UK, University of Reading, HYDRA
David Simplot-Ryl, FR, INRIA/ERCIM, ASPIRE
Elias Tragos, GR, FORTH, RERUM
Eric Mercier, FR, CEA-Leti
Erik Berg, NO, Telenor, IoT-I
Francesco Sottile, IT, ISMB, BUTLER
Franck Le Gall, FR, Inno, PROBE-IT, BUTLER
François Carrez, GB, IoT-I
Frederic Thiesse, CH, University of St. Gallen, Auto-ID Lab
Friedbert Berens, LU, FB Consulting S.à r.l, BUTLER
Gary Steri, IT, EC, JRC
Gianmarco Baldini, IT, EC, JRC
Giuseppe Abreu, DE, Jacobs University Bremen, BUTLER
Ghislain Despesse, FR, CEA-Leti
Harald Sundmaeker, DE, ATB GmbH, SmartAgriFood, CuteLoop
Henri Barthel, BE, GS1 Global
Igor Nai Fovino, IT, EC, JRC
Jan Höller, SE, EAB
Jens-Matthias Bohli, DE, NEC
John Soldatos, GR, Athens Information Technology, ASPIRE, OpenIoT
Jose-Antonio, Jimenez Holgado, ES, TID
Klaus Moessner, UK, UNIS, IoT.est
Kostas Kalaboukas, GR, SingularLogic, EURIDICE
Latif Ladid, LU, UL, IPv6 Forum
Levent Gürgen, FR, CEA-Leti
Luis Muñoz, ES, Universidad De Cantabria
Marco Carugi, IT, ITU-T, ZTE
Marilyn Arndt, FR, Orange

Mario Hoffmann, DE, Fraunhofer-Institute SIT, HYDRA
Markus Eisenhauer, DE, Fraunhofer-FIT, HYDRA, ebbits
Markus Gruber, DE, ALUD
Martin Bauer, DE, NEC, IoT-A
Martin Serrano, IE, OpenIoT, NUI Galway, Insight Centre, OpenIoT, VITAL
Maurizio Spirito, IT, Istituto Superiore Mario Boella, ebbits, ALMANAC
Maarten Botterman, NL, GNKS, SMART-ACTION
Nicolaie L. Fantana, DE, ABB AG
Nikos Kefalakis, GR, Athens Information Technology, OpenIoT
Paolo Medagliani, FR, Thales Communications & Security, CALYPSO
Payam Barnaghi, UK, UNIS, IoT.est
Philippe Cousin, FR, easy global market, PROBE-IT
Raffaele Giaffreda, IT, CNET, iCore
Ricardo Neisse, IT, EC, JRC
Richard Egan, UK, TRT
Rolf Weber, CH, UZH
Sébastien Boissseau, FR, CEA-Leti
Sébastien Ziegler, CH, Mandat International, IoT6
Sergio Gusmeroli, IT, TXT e-solutions,
Stefan Fisher, DE, UZL
Stefano Severi, DE, Jacobs University Bremen, BUTLER
Srdjan Krco, RS, DunavNET, IoT-I, SOCIOTAL
Sönke Nommensen, DE, UZL, SmartSantander
Trevor Peirce, BE, CASAGRAS2
Veronica Gutierrez Polidura, ES, Universidad De Cantabria
Vincent Berg, FR, CEA-Leti
Vlasios Tsiatsis, SE, EAB
Wolfgang König, DE, ALUD
Wolfgang Templ, DE, ALUD

Contributing Projects and Initiatives

ASPIRE, BRIDGE, CASCADAS, CONFIDENCE, CuteLoop, DACAR, ebbits, ARTEMIS, ENIAC, EPoSS, EU-IFM, EURIDICE, GRIFS, HYDRA, IMS2020, Indisputable Key, iSURF, LEAPFROG, PEARS Feasibility, PrimeLife, RACE networkRFID, SMART, StoLPaN, SToP, TraSer, WALTER, IoT-A, IoT@Work, ELLIOT, SPRINT, NEFFICS, IoT-I, CASAGRAS2,

eDiana, OpenIoT, IoT6, iCore PROBE-IT, BUTLER, IoT-est, SmartAgri-Food, ALMANAC, CITYPULSE, COSMOS, CLOUT, RERUM, SMARTIE, SMART-ACTION, SOCIOTAL, VITAL.

List of Abbreviations and Acronyms

Acronym	Meaning
3GPP	3rd Generation Partnership Project
AAL	Ambient Assisted Living
ACID	Atomicity, Consistency, Isolation, Durability
ACL	Access Control List
AMR	Automatic Meter Reading Technology
API	Application Programming Interface
ARM	Architecture Reference Model
AWARENESS	EU FP7 coordination action Self-Awareness in Autonomic Systems
BACnet	Communications protocol for building automation and control networks
BAN	Body Area Network
BDI	Belief-Desire-Intention architecture or approach
Bluetooth	Proprietary short range open wireless technology standard
BPM	Business process modelling
BPMN	Business Process Model and Notation
BUTLER	EU FP7 research project uBiquitous, secUre inTernet of things with Location and contExt-awaReness
CAGR	Compound annual growth rate
CE	Council of Europe
CEN	Comité Européen de Normalisation
CENELEC	Comité Européen de Normalisation Électrotechnique
CEO	Chief executive officer
CEP	Complex Event Processing
CSS	Chirp Spread Spectrum
D1.3	Deliverable 1.3
DATEX-II	Standard for data exchange involving traffic centres
DCA	Data Collection and Analysis
DNS	Domain Name System
DoS/DDOS	Denial of service attack Distributed denial of service attack

EC	European Commission
eCall	eCall – eSafety Support A European Commission funded project, coordinated by ERTICO-ITS Europe
EDA	Event Driven Architecture
EH	Energy harvesting
EMF	Electromagnetic Field
ERTICO-ITS	Multi-sector, public/private partnership for intelligent transport systems and services for Europe
ESOs	European Standards Organisations
ESP	Event Stream Processing
ETSI	European Telecommunications Standards Institute
EU	European Union
Exabytes	10^{18} bytes
FI	Future Internet
FI PPP	Future Internet Public Private Partnership programme
FIA	Future Internet Assembly
FIS 2008	Future Internet Symposium 2008
F-ONS	Federated Object Naming Service
FP7	Framework Programme 7
FTP	File Transfer Protocol
GFC	Global Certification Forum
GreenTouch	Consortium of ICT research experts
GS1	Global Standards Organization
Hadoop	Project developing open-source software for reliable, scalable, distributed computing
IAB	Internet Architecture Board
IBM	International Business Machines Corporation
ICAC	International Conference on Autonomic Computing
ICANN	Internet Corporation for Assigned Name and Numbers
ICT	Information and Communication Technologies
iCore	EU research project Empowering IoT through cognitive technologies
IERC	European Research Cluster for the Internet of Things
IETF	Internet Engineering Task Force
INSPIRE	Infrastructure for Spatial Information in the European Community
IIoT	Industrial Internet of Things
IoB	Internet of Buildings

IoC	Internet of Cities
IoE	Internet of Energy
IoE	Internet of Everything
IoL	Internet of Lighting
IoM	Internet of Media
IoP	Internet of Persons, Internet of People
IoS	Internet of Services
IoT	Internet of Things
IoT6	EU FP7 research project Universal integration of the Internet of Things through an IPv6-based service oriented architecture enabling heterogeneous components interoperability
IoT-A	Internet of Things Architecture
IoT-est	EU ICT FP7 research project Internet of Things environment for service creation and testing
IoT-I	Internet of Things Initiative
IoV	Internet of Vehicles
IP	Internet Protocol
IPSO Alliance	Organization promoting the Internet Protocol (IP) for Smart Object communications
IPv6	Internet Protocol version 6
ISO 19136	Geographic information, Geography Mark-up Language, ISO Standard
IST	Intelligent Transportation System
KNX	Standardized, OSI-based network communications protocol for intelligent buildings
LNCS	Lecture Notes in Computer Science
LOD	Linked Open Data Cloud
LTE	Long Term Evolution
M2M	Machine to Machine
MAC	Media Access Control data communication protocol sub-layer
MAPE-K	Model for autonomic systems: Monitor, Analyse, Plan, Execute in interaction with a Knowledge base
makeSense	EU FP7 research project on Easy Programming of Integrated Wireless Sensors
MB	Megabyte

MIT	Massachusetts Institute of Technology
MPP	Massively parallel processing
NIEHS	National Institute of Environmental Health Sciences
NFC	Near Field Communication
NoSQL	not only SQL – a broad class of database management systems
OASIS	Organisation for the Advancement of Structured Information Standards
OEM	Original equipment manufacturer
OGC	Open Geospatial Consortium
OMG	Object Management Group
OpenIoT	EU FP7 research project Part of the Future Internet public private partnership Open source blueprint for large scale self-organizing cloud environments for IoT applications
Outsmart	EU project Provisioning of urban/regional smart services and business models enabled by the Future Internet
PAN	Personal Area Network
PET	Privacy Enhancing Technologies
Petabytes	10^{15} byte
PHY	Physical layer of the OSI model
PIPES	Public infrastructure for processing and exploring streams
PKI	Public key infrastructure
PPP	Public-private partnership
Probe-IT	EU ICT-FP7 research project Pursuing roadmaps and benchmarks for the Internet of Things
PSI	Public Sector Information
PV	Photo Voltaic
QoI	Quality of Information
RFID	Radio-frequency identification
SASO	IEEE international conferences on Self-Adaptive and Self-Organizing Systems
SDO	Standard Developing Organization
SEAMS	International Symposium on Software Engineering for Adaptive and Self-Managing Systems

SENSEI	EU FP7 research project Integrating the physical with the digital world of the network of the future
SIG	Special Interest Group
SLA	Service-level agreement/Software license agreement
SmartAgriFood	EU ICT FP7 research project Smart Food and Agribusiness: Future Internet for safe and healthy food from farm to fork
SmartSantander	EU ICT FP7 research project Future Internet research and experimentation
SOA	Service Oriented Approach
SON	Self-Organising Networks
SSW	Semantic Sensor Web
SRA	Strategic Research Agenda
SRIA	Strategic Research and Innovation Agenda
SRA2010	Strategic Research Agenda 2010
SWE	Sensor Web Enablement
TC	Technical Committee
TTCN-3	Testing and Test Control Notation version 3
USDL	Unified Service Description Language
UWB	Ultra-wideband
W3C	World Wide Web Consortium
WS& AN	Wireless sensor and actuator networks
WSN	Wireless sensor network
WS-BPEL	Web Services Business Process Execution Language
Zettabytes	10^{21} byte
ZigBee	Low-cost, low-power wireless mesh network standard based on IEEE 802.15.4

Bibliography

[1] NFC Forum, online at http://nfc-forum.org

[2] METIS, Mobile and wireless communications Enablers for the Twenty-twenty (2020) Information Society, online at https://www.metis2020.com/

[3] F. Schaich, B. Sayrac, and M. Schubert. On the Need for a New Air Interface for 5G, *IEEE COMSOC MMTC E-Letter*, Vol. 9, No. 5, September 2014, http://www.comsoc.org/∼mmc

[4] Wemme, L., "NFC: Global Promise and Progress", NFC Forum, 22.01.2014, online at http://nfc-forum.org/wp-content/uploads/2014/01/Omnicard_Wemme_2014_website.pdf
[5] Bluetooth Special Interest Group, online at https://www.bluetooth.org/en-us/members/about-sig
[6] Bluetooth Developer Portal, online at https://developer.bluetooth.org/Pages/default.aspx
[7] Bluetooth, online at http://www.bluetooth.com
[8] ANT+, online at http://www.thisisant.com/
[9] ANT, "Message Protocol and Usage rev.5.0", online at http://www.thisisant.com/developer/resources/downloads#documents_tab
[10] ANT, "FIT2 Fitness Module Datasheet", online at http://www.thisisant.com/developer/resources/downloads#documents_tab
[11] Wi-Fi Alliance, online at http://www.wi-fi.org/
[12] Z-Wave alliance, online at http://www.z-wavealliance.org
[13] Pätz, C., "Smart lighting. How to develop Z-Wave Devices", EE|Times europe LEDLighting, 04.10.2012, online at http://www.ledlighting-eetimes.com/en/how-to-develop-z-wave-devices.html?cmp_id=71&news_id=222908151
[14] KNX, online at http://www.knx.org/knx-en/knx/association
[15] European Editors, "Using Ultra-Low-Power Sub-GHz Wireless for Self-Powered Smart-Home Networks", 12.05.2013, online at http://www.digikey.com/en-US/articles/techzone/2013/dec/using-ultra-low-power-sub-ghz-wireless-for-self-powered-smart-home-networks
[16] HART Communication Foundation, online at http://www.hartcomm.org
[17] Mouser Electronics, "Wireless Mesh Networking – Featured Wireless Mesh Networking Protocols", online at http://no.mouser.com/applications/wireless_mesh_networking_protocols/
[18] IETF, online at https://www.ietf.org
[19] Bormann, C., "6LoWPAN Roadmap and Implementation Guide", 6LoWPAN Working Group, April 2013, http://tools.ietf.org/html/draft-bormann-6lowpan-roadmap-04
[20] Shelby, Z. and Bormann, C., "6LoWPAN: The Wireless Embedded Internet", Wiley, Great Britain, ISBN 9780470747995, 2009, online at http://elektro.upi.edu/pustaka.elektro/Wireless%20Sensor%20Network/6LoWPAN.pdf
[21] WiMAX Forum, online at http://www.wimaxforum.org

[22] A. Passemard, "The Internet of Things Protocol stack – from sensors to business value", online at http://entrepreneurshiptalk.wordpress.com/2014/01/29/the-internet-of-thing-protocol-stack-from-sensors-to-business-value/
[23] EnOcean Alliance, online at http://www.enocean-alliance.org/en/profile/
[24] EnOcean Wireless Standard, online at http://www.enocean.com
[25] EnOcean Alliance, "EnOcean Equipment Profiles (EEP)", Ver. 2.6, December 2013, online at http://www.enocean.com/en/home/
[26] DASH7 Alliance, online at http://www.dash7.org
[27] Maarten Weyn, "Dash7 Alliance Protocol Technical Presentation", December 2013, online at http://www.slideshare.net/MaartenWeyn1/dash7-alliance-protocol-technical-presentation
[28] Visible Assets, Inc., "Rubee Technology", online at http://www.rubee.com/Techno/index.html
[29] Stevens, J., Weich, C., GilChrist, R., "RuBee (IEEE 1902.1) – The Physics Behind, Real-Time, High Security Wireless Asset Visibility Networks in Harsh Environments", online at http://www.rubee.com/White-SEC/RuBee-Security-080610.pdf
[30] RuBee Hardware, online at http://www.rubee.com/page2/Hard/index.html
[31] Foster, A., "A Comparison Between DDS, AMQP, MQTT, JMS, REST and CoAP", Version 1.4, January 2014, online at http://www.prismtech.com/sites/default/files/documents/MessagingComparsionJan2014USROW_vfinal.pdf
[32] Elkstein, M., "Learn REST: A tutorial", online at http://rest.elkstein.org
[33] Jaffey, T., "MQTT and CoAP IoT Protocols.pdf", September 2013, online at https://docs.google.com/document/d/1_kTNkl84o_yoC56dzFfkYHoHuepINP3nDNokycXINXI/edit?usp=sharing&pli=1
[34] Puzanov, O., "IoT Protocol Wars: MQTT vs COAP vs XMPP", online at http://www.iotprimer.com/2013/11/iot-protocol-wars-mqtt-vscoap-vs-xmpp.html
[35] Home Gateway Initiative (HGI), online at www.homegatewayinitiative.org
[36] Artemis IoE project, online at www.artemis-ioe.eu
[37] Casaleggio Associati, "The Evolution of Internet of Things", February 2011, online at http://www.casaleggio.it/pubblicazioni/Focus_internet_of_things_v1.81%20-%20eng.pdf

[38] J. B., Kennedy, "When woman is boss, An interview with Nikola Tesla", in Colliers, January 30, 1926.

[39] M. Weiser, "The Computer for the 21st Century," *Scientific Am.*, Sept., 1991, pp. 94–104; reprinted in *IEEE Pervasive Computing*, Jan.–Mar. 2002, pp. 19–25."

[40] K. Ashton, "That 'Internet of Things' Thing", online at http://www.rfid journal.com/article/view/4986, June 2009

[41] N. Gershenfeld, "When Things Start to Think", Holt Paperbacks, New York, 2000.

[42] Raymond James & Associates, "The Internet of Things – A Study in Hype, Reality, Disruption, and Growth", online at http://sitic.org/wp-content/uploads/The-Internet-of-Things-A-Study-in-Hype-Reality-Disruption-and-Growth.pdf, January 2014.

[43] N. Gershenfeld, R. Krikorian and D. Cohen, *Scientific Am.*, Sept., 2004.

[44] World Economic Forum, "The Global Information Technology Report 2012 – Living in a Hyperconnected World" online at http://www3.weforum.org/docs/Global_IT_Report_2012.pdf

[45] "Key Enabling Technologies", Final Report of the HLG-KET, June 2011.

[46] G. Bovet, A. Ridi and J. Hennebert, "Toward Web Enhanced Building Automation System", in Eds. N. Bessis and C. Dobre – Big Data and Internet of Things: A Roadmap for Smart Environments, ISBN: 978-3-319-05028-7, Studies in Computational Intelligence, Volume 546, 2014 pp. 259–283, online at http://hal.archives-ouvertes.fr/docs/00/97/35/10/PDF/BuildingsWoT.pdf

[47] International Technology Roadmap for Semiconductors, ITRS 2012 Update, online at http://www.itrs.net/Links/2012ITRS/2012Chapters/2012Overview.pdf

[48] W. Arden, M. Brillouët, P. Cogez, M. Graef, et al., "More than Moore" White Paper, online at http://www.itrs.net/Links/2010ITRS/IRC-ITRS-MtM-v2%203.pdf

[49] Frost & Sullivan "Mega Trends: Smart is the New Green" online at http://www.frost.com/prod/servlet/our-services-page.pag?mode=open&sid=230169625

[50] O. Vermesan. The IoT: a concept, a paradigm, and an open global network. *Telit2market International*, Issue 10, February 2015, pp. 120–122, online at http://www.telit2market.com/wp-content/

uploads/2015/02/telit2market_10_15_anniversary_edition.pdf, Accessed 29 May 2015.

[51] Market research group Canalys, online at http://www.canalys.com/

[52] E. Savitz, "Gartner: 10 Critical Tech Trends For The Next Five Years" online at http://www.forbes.com/sites/ericsavitz/2012/10/22/gartner-10-critical-tech-trends-for-the-next-five-years/

[53] E. Savitz, "Gartner: Top 10 Strategic Technology Trends For 2013" online at http://www.forbes.com/sites/ericsavitz/2012/10/23/gartner-top-10-strategic-technology-trends-for-2013/

[54] P. High "Gartner: Top 10 Strategic Technology Trends For 2014" online at http://www.forbes.com/sites/peterhigh/2013/10/14/gartner-top-10-strategic-technology-trends-for-2014/#

[55] Gartner's Top 10 Strategic Technology Trends for 2015, online at http://www.gartner.com/smarterwithgartner/gartners-top-10-strategic-technology-trends-for-2015/

[56] Platform INDUSTRIE 4.0 – Recommendations for implementing the strategic initiative INDUSTRIE 4.0, Final report of the Industrie 4.0 Working Group, online at, http://www.acatech.de/fileadmin/user_upload/Baumstruktur_nach_Website/Acatech/root/de/Material_fuer_Sonderseiten/Industrie_4.0/Final_report__Industrie_4.0_accessible.pdf, 2013

[57] Industrial Internet of Things (IoT) Advisory Service, ARC Advisory Group, online at, http://www.arcweb.com/services/pages/industrial-internet-of-things-service.aspx

[58] rtSOA – A Data Driven, Real Time Service Oriented Architecture for Industrial Manufacturing, online at http://www-db.in.tum.de/research/projects/rtSOA/

[59] P. C. Evans and M. Annunziata, Industrial Internet: Pushing the Boundaries of Minds and Machines, General Electric Co., online at http://files.gereports.com/wp-content/uploads/2012/11/ge-industrial-internet-vision-paper.pdf

[60] Cisco, "Securely Integrating the Cyber and Physical Worlds", online at http://www.cisco.com/web/solutions/trends/tech-radar/securing-the-iot.html

[61] NXT Cities, online at http://www.communicasia.com/wp-content/themes/cmma2014/images/img-nxtcities-large.jpg

[62] NXT Enterprises, online at http://www.communicasia.com/wp-content/themes/cmma2014/images/img-nxtenterprise-large.jpg

[63] NXT Connect, online at http://www.communicasia.com/wp-content/themes/cmma2014/images/img-nxtconnect-large.jpg

[64] H. Bauer, F. Grawert, and S. Schink, Semiconductors for wireless communications: Growth engine of the industry, online at www.mckinsey.com/

[65] L. Fretwell and P. Schottmiller, Cisco Presentation, online at http://www.cisco.com/assets/events/i/nrf-Internet_of_Everything_Whats_the_Art_of_the_Possible_in_Retail.pdf, January 2014.

[66] ITU-T, Internet of Things Global Standards Initiative, http://www.itu.int/en/ITU-T/gsi/iot/Pages/default.aspx

[67] International Telecommunication Union – ITU-TY.2060 – (06/2012) – Next Generation Networks – Frameworks and functional architecture models – Overview of the Internet of things.

[68] IEEE-SA – Enabling Consumer Connectivity Through Consensus Building, online at http://standardsinsight.com/ieee_company_detail/consensus-building

[69] Mobile-Edge Computing – Introductory Technical White Paper, 2014, online at https://portal.etsi.org/Portals/0/TBpages/MEC/Docs/Mobile-edge_Computing_-_Introductory_Technical_White_Paper_V1%2018-09-14.pdf

[70] O. Vermesan, P. Friess, P. Guillemin, S. Gusmeroli, et al., "Internet of Things Strategic Research Agenda", Chapter 2 in Internet of Things – Global Technological and Societal Trends, River Publishers, 2011, ISBN 978-87-92329-67-7.

[71] O. Vermesan, P. Friess, P. Guillemin, H. Sundmaeker, et al., "Internet of Things Strategic Research and Innovation Agenda", Chapter 2 in Internet of Things – Converging Technologies for Smart Environments and Integrated Ecosystems, River Publishers, 2013, ISBN 978-87-92982-73-5.

[72] O. Vermesan, P. Friess, P. Guillemin, H. Sundmaeker, et al. Internet of Things Strategic Research and Innovation Agenda. O. Vermesan and P. Friess, Eds. *Internet of Things Applications – From Research and Innovation to Market Deployment*. Alborg, Denmark: The River Publishers, ISBN: 978-87-93102-94-1, 2014, pp. 7–142.

[73] M. Abu-Elkheir, M. Hayajneh and N. Abu Ali. Data Management for the Internet of Things: Design Primitives and Solution. *Sensors*, 13(11): 15582–15612, 2013.

[74] SmartSantander, EU FP7 project, Future Internet Research and Experimentation, online at http://www.smartsantander.eu/

[75] Introducing Fujisawa SST – A town sustainably evolving through living ideas, Panasonic, online at http://panasonic.net/es/fujisawasst/
[76] Foundational Solution of Smart City, online at http://br.fiberhomegroup.com/pt/Enterprise/324/2282.aspx#1
[77] ISO 9646: "Conformance Testing Methodology and Framework".
[78] J. Bloem. InterOperability Testing in the Age of Cloud, Things and DevOps, online at https://www.sogeti.nl/updates/blogs/interoperability-testing-age-cloud-things-and-devops
[79] Internet of Things Concept, online at http://xarxamobal.diba.cat/XGMSV/imatges/actualitat/iot.jpg
[80] H. Grindvoll, O. Vermesan, T. Crosbie, R. Bahr, et al., "A wireless sensor network for intelligent building energy management based on multi communication standards – a case study", ITcon Vol. 17, pg. 43–62, http://www.itcon.org/2012/3
[81] S. Toronidis. Better Operations, Better Operating Rooms, online at http://www.centrak.com/blog.aspx
[82] EU Research & Innovation, "Horizon 2020", The Framework Programme for Research and Innovation, online at http://ec.europa.eu/research/horizon2020/index_en.cfm
[83] Digital Agenda for Europe, European Commission, Digital Agenda 2010–2020 for Europe, online at http://ec.europa.eu/information_society/digital-agenda/index_en.htm
[84] Gartner, 2013, online at http://www.gartner.com/newsroom/id/2636073
[85] Beecham Research Limited. Towards Smart Farming: Agriculture Embracing the IoT Vision, online at http://www.beechamresearch.com/download.aspx?id=40
[86] E. Guizzo. How Google's Self-Driving Car Works. IEEE Spectrum, online at http://spectrum.ieee.org/automaton/robotics/artificial-intelligence/how-google-self-driving-car-works
[87] K. Karimi and G. Atkinson, "What the Internet of Things (IoT) Needs to Become a Reality", White Paper, 2013, online at http://www.freescale.com/files/32bit/doc/white_paper/INTOTHNGSWP.pdf
[88] Freescale vision chip makes self-driving cars a bit more ordinary, online at http://www.cnet.com/news/freescale-vision-chip-makes-self-driving-cars-a-bit-more-ordinary/
[89] R. E. Hall, "The Vision of A Smart City" presented at the 2nd International Life Extension Technology Workshop Paris, France September 28, 2000, online at http://www.crisismanagement.com.cn/

templates/blue/down_list/llzt_zhcs/The%20Vision%20of%20A%20Smart%20City.pdf

[90] EU 2012. The ARTEMIS Embedded Computing Systems Initiative, October 2012 online at http://www.artemis-ju.eu/

[91] Foundations for Innovation in Cyber-Physical Systems, Workshop Report, NIST, 2013, online at http://www.nist.gov/el/upload/CPS-WorkshopReport-1-30-13-Final.pdf

[92] IERC – European Research Cluster on the Internet of Things, "Internet of Things – Pan European Research and Innovation Vision", October, 2011, online at, http://www.theinternetofthings.eu/sites/default/files/Rob%20van%20Kranenburg/IERC_IoT-Pan%20European%20Research%20and%20Innovation%20Vision_2011.pdf

[93] O. Vermesan, P. Friess, G. Woysch, P. Guillemin, S. Gusmeroli, et al., "Europe's IoT Stategic Research Agenda 2012", Chapter 2 in The Internet of Things 2012 New Horizons, Halifax, UK, 2012, ISBN 978-0-9553707-9-3.

[94] SENSEI, EU FP7 project, *D1.4: Business models and Value Creation*, 2010, online at: http://www.ict-sensei.org

[95] IoT-I, Internet of Things Initiative, FP7 EU project, online at http://www.iot-i.eu

[96] Libelium, "50 Sensor Applications for a Smarter World", online at http://www.libelium.com/top_50_iot_sensor_applications_ranking#

[97] OUTSMART, FP7 EU project, part of the Future Internet Private Public Partnership, "OUTSMART – Provisioning of urban/regional smart services and business models enabled by the Future Internet", online at http://www.fi-ppp-outsmart.eu/en-uk/Pages/default.aspx

[98] BUTLER, FP7 EU project, online at http://www.iot-butler.eu/

[99] NXP Semiconductors N.V., "What's Next for Internet-Enabled Smart Lighting?", online at http://www.nxp.com/news/press-releases/2012/05/whats-next-for-internet-enabled-smart-lighting.html

[100] J. Formo, M. Gårdman, and J. Laaksolahti, "Internet of things marries social media", in *Proceedings of the 13th International Conference on MobileHCI,* ACM, New York, NY, USA, pp. 753–755, 2011.

[101] J. G. Breslin, S. Decker, and M. Hauswirth, et. al., "Integrating Social Networks and Sensor Networks", *W3C Workshop on the Future of Social Networking,* Barcelona, 15–16 January 2009.

[102] M. Kirkpatrick, "The Era of Location-as-Platform Has Arrived", *ReadWriteWeb*, January 25, 2010.

[103] F. Calabrese, K. Kloeckl, and C. Ratti (MIT), "WikiCity: Real-Time Location-Sensitive tools for the city", in *IEEE Pervasive Computing*, July–September 2007.

[104] Building smart communities, online at http://www.holyroodconnect .com/tag/smart-cities/

[105] Using Big Data to Create Smart Cities, online at http://informationstr ategyrsm.wordpress.com/2013/10/12/using-big-data-to-create-smart-cities/

[106] N. Maisonneuve, M. Stevens, M. E. Niessen, L. Steels, "NoiseTube: Measuring and mapping noise pollution with mobile phones", in *Information Technologies in Environmental Engineering (ITEE 2009)*, Proceedings of the 4th International ICSC SymposiumThessaloniki, Greece, May 28–29, 2009.

[107] J-S. Lee, B. Hoh, "Sell your experiences: a market mechanism based incentive for participatory sensing", *2010 IEEE International Conference on Pervasive Computing and Communications (PerCom)*, pp. 60–68, March 29, 2010, – April 2, 2010.

[108] R. Herring, A. Hofleitner, S. Amin, T. Nasr, A. Khalek, P. Abbeel, and A. Bayen, "Using Mobile Phones to Forecast Arterial Traffic Through Statistical Learning", *89th Transportation Research Board Annual Meeting,* Washington D.C., January 10–14, 2010.

[109] M. Kranz, L. Roalter, and F. Michahelles, "Things That Twitter: Social Networks and the Internet of Things", in *What can the Internet of Things do for the Citizen (CIoT) Workshop* at *The Eighth International Conference on Pervasive Computing (Pervasive 2010)*, Helsinki, Finland, May 2010.

[110] O. Vermesan, et al., "Internet of Energy – Connecting Energy Anywhere Anytime" in Advanced Microsystems for Automotive Applications 2011: Smart Systems for Electric, Safe and Networked Mobility, Springer, Berlin, 2011, ISBN 978-36-42213-80-9.

[111] W. Colitti, K. Steenhaut, and N. De Caro, "Integrating Wireless Sensor Networks with the Web," Extending the Internet to Low Power and Lossy Networks (IP+ SN 2011), 2011 online at http://hinrg.cs.jhu.edu/joomla/images/stories/IPSN_2011_koliti.pdf

[112] M. M. Hassan, B. Song, and E. Huh, "A framework of sensor-cloud integration opportunities and challenges", in *Proceedings of the 3rd International Conference on Ubiquitous Information Management and Communication,* ICUIMC 2009, Suwon, Korea, January 15–16, pp. 618–626, 2009.

[113] M. Yuriyama and T. Kushida, "Sensor-Cloud Infrastructure – Physical Sensor Management with Virtualized Sensors on Cloud Computing", NBiS 2010: 1–8.

[114] C. Bizer, T. Heath, K. Idehen, and T. Berners-Lee, "Linked Data on the Web", *Proceedings of the 17th International Conference on World Wide Web (WWW'08),* New York, NY, USA, ACM, pp. 1265–1266, 2008.

[115] T. Heath and C. Bizer, "Linked Data: Evolving the Web into a Global Data Space", *Synthesis Lectures on the Semantic Web: Theory and Technology*, 1st edition. Morgan & Claypool, 1:1, 1–136, 2011.

[116] IBM, "An architectural blueprint for autonomic computing", IBM White paper. June 2005.

[117] Connected Devices for Smarter Home Environments, IBM Data Magazine, 2014, online at http://ibmdatamag.com/2014/04/connected-devices-for-smarter-home-environments/

[118] International Conference on Autonomic Computing http://www.autonomic-conference.org/

[119] IEEE International Conferences on Self-Adaptive and Self-Organizing Systems, http://www.saso-conference.org/

[120] International Symposium on Software Engineering for Adaptive and Self-Managing Systems, http://www.seams2012.cs.uvic.ca/

[121] Awareness project, Self-Awareness in Autonomic Systems http://www.aware-project.eu/

[122] M. C. Huebscher, J. A. McCann, "A survey of autonomic computing — degrees, models, and applications", *ACM Computing Surveys (CSUR)*, Volume 40 Issue 3, August 2008.

[123] A. S. Rao, M. P. Georgeff, "BDI Agents: From Theory to Practice", in *Proceedings of The First International Conference on Multi-agent Systems (ICMAS)*, 1995. pp. 312–319.

[124] G. Dimitrakopoulos, P. Demestichas, W. Koenig, *Future Network & Mobile Summit 2010 Conference Proceedings.*

[125] John Naisbit and Patricia Aburdene (1991), *Megatrends 2000*, Avon.

[126] D. C. Luckham, Event Processing for Business: Organizing the Real-Time Enterprise, John Wiley & Sons, 2012.

[127] T. Mitchell, *Machine Learning*, McGraw Hill, 1997.

[128] D. Estrin, "Participatory Sensing: Applications and Architecture, online at http://research.cens.ucla.edu/people/estrin/resources/conferences/2010-Estrin-participatory-sensing-mobisys.pdf O. Etzion, P. Niblett, *Event Processing in Action*, Manning, 2011.

[129] V. J. Hodgem, J. Austin, "A Survey of Outlier Detection Methodologies", *Artificial Intelligence Review*, 22 (2), pages 85–126, 2004.

[130] F. Angiulli, and C. Pizzuti, "Fast outlier detection in high dimensional spaces" in *Proc. European Conf. on Principles of Knowledge Discovery and Data Mining*, 2002.

[131] H. Fan, O. Zaïane, A. Foss, and J. Wu, "Nonparametric outlier detection for efficiently discovering top-n outliers from engineering data", in *Proc. Pacific-Asia Conf. on Knowledge Discovery and Data Mining (PAKDD)*, Singapore, 2006.

[132] A. Ghoting, S. Parthasarathy, and M. Otey, "Fast mining of distance-based outliers in high dimensional spaces", in *Proc. SIAM Int. Conf. on Data Mining (SDM)*, Bethesda, ML, 2006.

[133] G. Box, G. Jenkins, *Time series analysis: forecasting and control*, rev. ed., Oakland, California: Holden-Day, 1976.

[134] J. Hamilton, *Time Series Analysis*, Princeton Univ. Press, 1994.

[135] J. Durbin and S. J. Koopman, *Time Series Analysis by State Space Methods*, Oxford University Press, 2001.

[136] R. O. Duda, P. E. Hart, D. G. Stork, *Pattern Classification, 2nd Edition*, Wiley, 2000.

[137] C. M. Bishop, *Neural Networks for Pattern Recognition*, Oxford University Press, 1995.

[138] C. M. Bishop, *Pattern Recognition and Machine Learning*, Springer, 2006.

[139] M. J. Zaki, "Generating non-redundant association rules", *Proceedings of the sixth ACM SIGKDD international conference on Knowledge discovery and data mining*, 34–43, 2000.

[140] M. J. Zaki, M. Ogihara, "Theoretical foundations of association rules", *3rd ACM SIGMOD Workshop on Research Issues in Data Mining and Knowledge Discovery*, 1998.

[141] N. Pasquier, Y. Bastide, R. Taouil, L. Lakhal, "Discovering Frequent Closed Itemsets for Association Rules", *Proceedings of the 7th International Conference on Database Theory*, (398–416), 1999.

[142] C. M. Kuok, A. Fu, M. H. Wong, "Mining fuzzy association rules in databases", *SIGMOD Rec.* 27, 1 (March 1998), 41–46.

[143] T. Kohonen, *Self-Organizing Maps*, Springer, 2001.

[144] S.-H. Hamed, S. Reza, "TASOM: A New Time Adaptive Self-Organizing Map", *IEEE Transactions on Systems, Man, and Cybernetics—Part B: Cybernetics* 33 (2): 271–282, 2003.

[145] L.J.P. van der Maaten, G.E. Hinton, "Visualizing High-Dimensional Data Using t-SNE", *Journal of Machine Learning Research* 9(Nov): 2579–2605, 2008.

[146] I. Guyon, S. Gunn, M. Nikravesh, and L. Zadeh (Eds), *Feature Extraction, Foundations and Applications*, Springer, 2006.

[147] Y. Bengio, "Learning deep architectures for AI", *Foundations and Trends in Machine Learning*, 2(1):1–12, 2009.

[148] Y. Bengio, Y. LeCun, "Scaling learning algorithms towards AI", *Large Scale Kernel Machines*, MIT Press, 2007.

[149] B. Hammer, T. Villmann, "How to process uncertainty in machine learning?", *ESANN'2007 proceedings – European Symposium on Artificial Neural Networks*, Bruges (Belgium), 2007.

[150] J. Quinonero-Candela, C. Rasmussen, F. Sinz, O. Bousquet, and B. Schölkopf, "Evaluating Predictive Uncertainty Challenge", in *Machine Learning Challenges: Evaluating Predictive Uncertainty, Visual Object Classification, and Recognising Tectual Entailment,* First PASCAL Machine Learning Challenges Workshop (MLCW 2005), Springer, Berlin, Germany, 1–27, 2006.

[151] D. Koller and N. Friedman, *Probabilistic graphical models: principles and techniques*, MIT press, 2009.

[152] M. R. Endsley, "Measurement of situation awareness in dynamic systems", *Human Factors*, 37, 65–84, 1995.

[153] R. Fuller, *Neural Fuzzy System*, Åbo Akademi University, ESF Series A: 443, 1995, 249 pages. [ISBN 951-650-624-0, ISSN 0358-5654].

[154] S. Haykin, *Neural Networks: A Comprehensive Foundation, 2nd edn*., Prentice-Hall, New York (1999).

[155] L. Rabiner, "A Tutorial on Hidden Markov Models and Selected Applications in Speech Recognition," *Proceedings of the IEEE*, vol. 77, no. 2, Feb. 1989.

[156] S.K. Murthy, "Automatic construction of decision trees from data: a multi-disciplinary survey", *Data Mining Knowledge Discovery*, 1998.

[157] ITU towards "IMT for 2020 and beyond."

[158] G. Macaigne. SIM-less networks, the new Eldorado of M2M and Internet of Things, online at http://www.inov360.com/blog/sim-less-networks-the-new-eldorado-of-m2m-and-internet-of-things/

[159] S. Haller and C. Magerkurth, "The Real-time Enterprise: IoT-enabled Business Processes", IETF IAB Workshop on Interconnecting Smart Objects with the Internet, March 2011.

[160] Open Geospatial Consortium, Geospatial and location standards, http://www.opengeospatial.org

[161] M. Botts, G. Percivall, C. Reed, and J. Davidson, "oGC Sensor Web Enablement: Overview and High Level Architecture", *The Open Geospatial Consortium*, 2008, online at http://portal.opengeospatial .org/files/?artifactid=25562

[162] W3C Semantic Sensor Network Incubator Group, Incubator Activity, online at http://www.w3.org/2005/Incubator/ssn/

[163] Logical Neighborhoods, Virtual Sensors and Actuators, online at http://logicalneighbor.sourceforge.net/vs.html

[164] K. M. Chandy and W. R. Schulte, "What is Event Driven Architecture (EDA) and Why Does it Matter?", 2007, online at http://complexevents.com/?p=212, (accessed on: 25.02.2008).

[165] D. Luckham, "What's the Difference Between ESP and CEP?", 2006, online at http://complexevents.com/?p=103, accessed on 15.12.2008.

[166] The CEP Blog, http://www.thecepblog.com/

[167] EnOcean – the Energy Harvesting Wirless Standard for Building Automation and Industrial Automation, online at http://www.enocean .com/en/radio-technology/

[168] IEEE Std 802.15.4$^{\mathrm{TM}}$-2006, Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs), online at http://www.ieee802.org/15/pub/TG4.html

[169] Bluetooth Low Energy (LE) Technology Info Site, online at http://www.bluetooth.com/English/Products/Pages/low_energy.aspx

[170] The Official Bluetooth Technology Info Site, online at http://www .bluetooth.com/

[171] M-G. Di Benedetto and G. Giancola, *Understanding Ultra Wide Band Radio Fundamentals*, Prentice Hall, June 27, 2004.

[172] ISO, International Organization for Standardization (ISO), Identification cards – Contactless integrated circuit(s) cards – Vicinity cards, ISO/IEC 14443, 2003.

[173] N. Pletcher, S. Gambini, and J. Rabaey, "A 52 μW Wake-Up Receiver With 72 dBm Sensitivity Using an Uncertain-IF Architecture", in *IEEE Journal of Solid-State Circuits*, vol. 44, no1, January, pp. 269–280. 2009.

[174] A. Vouilloz, M. Declercq, and C. Dehollain, "A Low-Power CMOS Super-Regenerative Receiver at 1 GHz", in *IEEE Journal of Solid-State Circuits*, vol. 36, no3, March, pp. 440–451, 2001.

[175] J. Ryckaert, A. Geis, L. Bos, G. van der Plas, J. Craninckx, "A 6.1 GS/s 52.8 mW 43 dB DR 80 MHz Bandwidth 2.4 GHz RF Bandpass Σ-Δ ADC in 40 nm CMOS", in *IEEE Radio-Frequency Integrated Circuits Symposium*, 2010.

[176] L. Lolis, C. Bernier, M. Pelissier, D. Dallet, and J.-B. Bégueret, "Bandpass Sampling RX System Design Issues and Architecture Comparison for Low Power RF Standards", *IEEE ISCAS 2010*.

[177] D. Lachartre, "A 550 µW inductorless bandpass quantizer in 65 nm CMOS for 1.4-to-3 GHz digital RF receivers", *VLSI Circuits 2011*, pp. 166–167, 2011.

[178] S. Boisseau and G. Despesse, "Energy Harvesting, Wireless Sensor Networks & Opportunities for Industrial Applications", in *EETimes,* 27th Feb 2012, online at http://www.eetimes.com

[179] J.G. Koomey, S. Berard, M. Sanchez, and H. Wong, "Implications of Historical Trends in the Electrical Efficiency of Computing", in *IEEE Annals of the History of Computing*, vol. 33, no. 3, pp. 46–54, March 2011.

[180] eCall – eSafety Support, online at http://www.esafetysupport.org/en/ecall_toolbox/european_commission/index.html

[181] European Commission, "Smart Grid Mandate, Standardization Mandate to European Standardisation Organisations (ESOs) to support European Smart Grid deployments", M/490 EN, Brussels 1st March, 2011.

[182] Global Certification Forum, online at http://www.globalcertificationforum.org

[183] SENSEI, EU FP7 project, online at http://www.sensei-project.eu

[184] IoT-A, EU FP7 project, online at http://www.iot-a.eu

[185] IoT6, EU FP7 project, online at http://www.iot6.eu

[186] IoT@Work, EU FP7 project, online at https://www.iot-at-work.eu/

[187] Federated Object Naming Service, GS1, online at http://www.gs1.org/gsmp/community/working_groups/gsmp#FONS

[188] Directive 2003/98/EC of the European Parliament and of the Council on the reuse of public sector information, 17 November 2003, online at http://ec.europa.eu/information_society/policy/psi/docs/pdfs/directive/psi_directive_en.pdf

[189] INSPIRE, EU FP7 project, – Infrastructure for Spatial Information in Europe, online at http://inspire.jrc.ec.europa.eu/

[190] H. van der Veer, A. Wiles, "Achiveing Technical Interoperability – the ETSI Approach", ETSI White Paper No.3, 3rd edition, April 2008,

http://www.etsi.org/images/files/ETSIWhitePapers/IOP%20whitepaper%20Edition%203%20final.pdf
[191] Ambient Assisted Living Roadmap, AALIANCE.
[192] Atmel AVR Xmega Micro Controllers, http://it.mouser.com/atmel_xmega/
[193] Worldwide Cellular M2M Modules Forecast, Beecham Research Ltd, August 2010.
[194] Future Internet Assembly Research Roadmap, FIA Research Roadmap Working Group, May 2011.
[195] D. Scholz-Reiter, M.-A. Isenberg, M. Teucke, H. Halfar, "An integrative approach on Autonomous Control and the Internet of Things", 2010.
[196] NIEHS on EMF, http://www.niehs.nih.gov/health/topics/agents/emf/
[197] R.H. Weber/R. Weber, "Internet of Things – Legal Perspectives", Springer, Berlin 2010.
[198] "The Global Wireless M2M Market", Berg Insight, 2010, http://www.berginsight.com/ReportPDF/ProductSheet/bi-gwm2m-ps.pdf
[199] M. Hatton, "Machine-to-Machine (M2M) communication in the Utilities Sector 2010–2020", Machina Research, July 2011.
[200] G. Masson, D. Morche, H. Jacquinot, and P. Vincent, "A 1 nJ/b 3.2–4.7 GHz UWB 50 Mpulses/s Double Quadrature Receiver for Communication and Localization", in *ESSCIRC 2010.*