2

Internet of Things Strategic Research Roadmap

Dr. Ovidiu Vermesan[1], Dr. Peter Friess[2], Patrick Guillemin[3], Sergio Gusmeroli[4], Harald Sundmaeker[5], Dr. Alessandro Bassi[6], Ignacio Soler Jubert[7], Dr. Margaretha Mazura[8], Dr. Mark Harrison[9], Dr. Markus Eisenhauer[10], Dr. Pat Doody[11]

[1]*SINTEF, Norway*
[2]*European Commission, Belgium*
[3]*ETSI, France*
[4]*TXT e-solutions, Italy*
[5]*ATB GmbH, Germany*
[6]*IoT-A Project, France*
[7]*ATOS Origin, Spain*
[8]*EMF, UK*
[9]*Institute of Manufacturing, University of Cambridge, UK*
[10]*Fraunhofer FIT, Germany*
[11]*Centre for Innovation in Distributed Systems, Institute of Technology, Ireland*

> "*What most people need to learn in life is how to love people and use things instead of using people and loving things.*"

> "*It is not because things are difficult that we do not dare, it is because we do not dare that things are difficult.*"
>
> ***Seneca***

> "*All things appear and disappear because of the concurrence of causes and conditions. Nothing ever exists entirely alone; everything is in relation to everything else.*"
>
> ***Hindu Prince Gautama Siddharta***

2.1 Internet of Things Conceptual Framework

Internet of Things (IoT) is an integrated part of Future Internet including existing and evolving Internet and network developments and could be conceptually defined as 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, use intelligent interfaces, and are seamlessly integrated into the information network.

In the IoT, "smart things/objects" are expected to become active participants in business, information and social processes where they are enabled to interact and communicate among them-selves and with the environment by exchanging data and information "sensed" about the environment, while reacting autonomously to the "real/physical world" events and influencing it by running processes that trigger actions and create services with or without direct human intervention.

Services will be able to interact with these "smart things/objects" using standard interfaces that will provide the necessary link via the Internet, to query and change their state and retrieve any information associated with them, taking into account security and privacy issues [1].

The IERC definition aims to coin the IoT paradigm and concept by unifying the different statements and many visions referred to as a "Things," "Internet," "Semantic," "Object Identification" oriented definitions of Internet of Things promoted by individuals and organisations around the world.

This enables a common vision for the deployment of independent federated services and applications, characterized by a high degree of autonomous data capture, event transfer, network connectivity and interoperability.

2.2 Internet of Things Vision

The vision of Future Internet based on standard communication protocols considers the merging of computer networks, Internet of Things (IoT), Internet of People (IoP), Internet of Energy (IoE), Internet of Media (IoM), and Internet of Services (IoS), into a common global IT platform of seamless networks and networked "smart things/objects".

IoE is defined as a dynamic network infrastructure that interconnects the energy network with the Internet allowing units of energy (locally generated, stored, and forwarded) to be dispatched when and where it is needed. The related information/data will follow the energy flows thus implementing the necessary information exchange together with the energy transfer.

IoS is denoting a software based component that will be delivered via different networks and Internet. Research on SOA, Web/enterprise 3.0/X.0, enterprise interoperability, service Web, grid services and semantic Web will address important bits of the IoS puzzle, while improving cooperation between service providers and consumers.

IoM will address the challenges in scalable video coding and 3D video processing, dynamically adapted to the network conditions that will give rise to innovative applications such as massive multiplayer mobile games, digital cinema and in virtual worlds placing new types of traffic demands on mobile network architectures.

IoP interconnects growing population of users while promoting their continuous empowerment, preserving their control over their online activities and sustaining free exchanges of ideas. The IoP also provides means to facilitate everyday life of people, communities, organizations, allowing at the same time the creation of any type of business and breaking the barriers between information producer and information consumer (emergence of prosumers).

IoT together with the other emerging Internet developments such as Internet of Energy, Media, People, Services, Business/Enterprises are the backbone of the digital economy, the digital society and the foundation for the future knowledge based economy and innovation society. IoT developments show that we will have 16 billion connected devices by the year 2020 [1], which will average out to six devices per person on earth and to many more per person in digital societies. Devices like smart phones and machine to machine or thing to thing communication will be the main drivers for further IoT development.

By 2015, wirelessly networked sensors in everything we own will form a new Web. But it will only be of value if the “terabyte torrent” of data it generates can be collected, analyzed and interpreted [6].

The first direct consequence of the IoT is the generation of huge quantities of data, where every physical or virtual object connected to the IoT may have a digital twin in the cloud, which could be generating regular updates. As a result, consumer IoT related messaging volumes could easily reach between 1.000 and 10.000 per person per day [2].

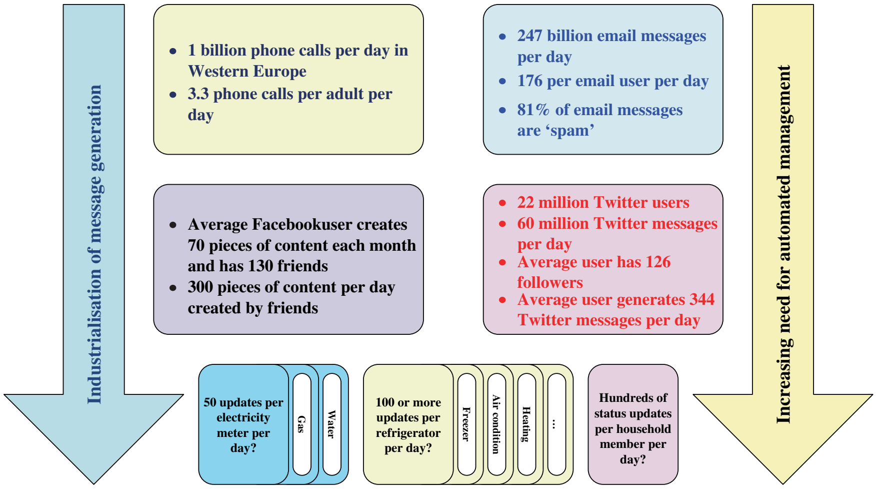
Industrialisation of message generation
1 billion phone calls per day in Western Europe
3.3 phone calls per adult per day
247 billion email messages per day
176 per email user per day
81% of email messages are 'spam'
Increasing need for automated management
Average Facebookuser creates 70 pieces of content each month and has 130 friends
300 pieces of content per day created by friends
22 million Twitter users
60 million Twitter messages per day
Average user has 126 followers
Average user generates 344 Twitter messages per day
50 updates per electricity meter per day?
Gas
Water
100 or more updates per refrigerator per day?
Freezer
Air condition
Heating
...
Hundreds of status updates per household member per day?

Fig. 2.1 The industrialisation of message generation [1].

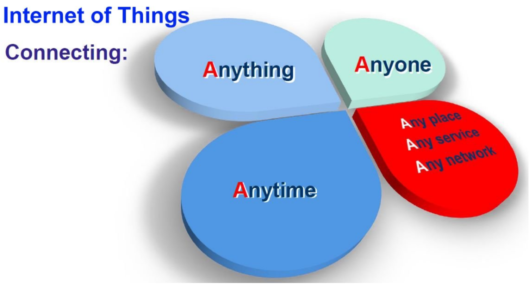

Fig. 2.2 Internet of things — 6A connectivity.

The IoT contribution is in the increased value of information created by the number of interconnections among things and the transformation of the processed information into knowledge for the benefit of mankind and society.

The Internet of Things could allow people and things to be connected Anytime, Anyplace, with Anything and Anyone, ideally using Any path/network and **A**ny service. This is stated as well in the ITU vision of the IoT, according to which: "From anytime, anyplace connectivity for anyone, we will now have connectivity for anything" [4].

The vision of what exactly the Internet of Things will be, and what will be its final architecture, are still diverging.

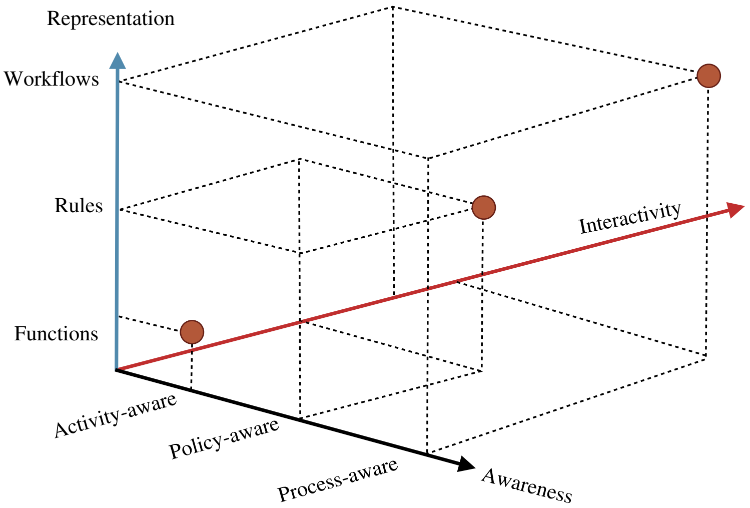

Fig. 2.3 Smart object dimensions: activity, policy and process aware [12].

A future network of networks could be laid out as public/private infrastructures and dynamically extended and improved by edge points created by the "things" connecting to one another. In fact, in the IoT communications could take place not only between things but also between people and their environment.

The vision of an Internet of Things built from smart things/objects needs to address issues related to system architecture, design and development, integrated management, business models and human involvement. This vision will have to take into account the integration of legacy systems and communications. Topics like the right balance for the distribution of functionality between smart things and the supporting infrastructure, modelling and representation of smart objects' intelligence, and programming models, are important elements that can be addressed by classifying smart object/things types as: *Activity-aware objects*, *policy-aware objects*, and *process-aware objects* [12]. These types represent specific combinations of three design dimensions with the aim to highlight the interdependence between design decisions and explore how smart objects can cooperate to form an "Internet of smart objects."

For instance, in [12] a vision of an IoT built by smart objects, able to sense, interprets, and react to external events is proposed. Within this vision, by capturing and interpreting user actions, smart items will be able to perceive and instruct their environment, to analyse their observations and to communicate with other objects and the Internet. This new Internet will co-exist and be intimately bound up with the Internet of information and services [13].

Utilizing real world knowledge on the networking levels, as well on service level will enable optimizing systems towards higher performance, better user experiences, as well as toward more energy efficiency.

Addressing elements such as Convergence, Content, Collections (Repositories), Computing, Communication, and Connectivity is likely to be instrumental in order to allow seamless interconnection between people and things and/or between things and things. The Internet of Things could imply a symbiotic interaction between the real/physical, world, and the digital/virtual world: physical entities have digital counterparts and virtual representation; things become context aware and they can sense, communicate, interact, exchange data, information and knowledge. 'Things' can only become context aware, sense, communicate, interact, exchange data, information and knowledge if they are suitably equipped with appropriate object-connected technologies; unless of course they are human 'things' or other entities with these intrinsic capabilities. In this vision, through the use of intelligent decision-making algorithms in software applications, appropriate rapid responses can be given to physical phenomena, based on the very latest information collected about physical entities and consideration of patterns in the historical data, either for the same entity or for similar entities. These create new opportunities to meet business requirements, create new services based on real time physical world data, gain insights into complex processes and relationships, handle incidents, address environmental degradation (for example pollution, disaster, tsunami, global warming), monitor human activities (health, movements, etc.), improve infrastructure integrity (energy, transport, etc.), and address energy efficiency issues (smart energy metering in buildings, efficient consumption by vehicles, etc.).

Everything from individuals, groups, communities, objects, products, data, services, processes could use the communication fabric provided by the smart things/objects. Connectivity will become in the IoT a kind of commodity, available to all at a very low cost and not owned by any private entity. In this context, there will be the need to create the right situation-aware development environment for stimulating the creation of services and proper intelligent middleware to understand and interpret the information, to ensure protection from fraud and malicious attack (that will inevitably grow as Internet becomes more and more used) and to guarantee privacy.

Capturing real world data, information and knowledge and events is becoming increasingly easier with sensor networks, social media sharing, location based services, and emerging IoT applications. The knowledge capturing and using is done in many cases at application level and the networks are mainly agnostic about what is happening around the terminals connected to the Internet.

Internet connectable consumer household devices will increase significantly in the next decade, with the computer network equipment that accounts for the majority of household devices, at about 75% in 2010, and declining to 25% by 2020 [1].

Embedding real world information into networks, services and applications is one of the aims of IoT technology by using enabling technologies like wireless sensor and actuator networks, IoT devices, ubiquitous device assemblies and RFID. These autonomous systems will "naturally" network with each other, with the environment, and the network infrastructure itself. New principles for self- properties, analysis of emerging behaviour, service platform approaches, new enabling technologies, as well as Web technology-based ideas will form the basis for this new "cognitive" behaviour.

Under this vision and making use of intelligence in the supporting network infrastructure, things will be able to autonomously manage their transportation, implement fully automated processes and thus optimise logistics; they have to be able to harvest the energy they need; they will configure themselves when exposed to a new environment, and show an "intelligent/cognitive" behaviour when faced with other things and deal seamlessly with unforeseen circumstances; and, finally, they might manage their own disassembly and recycling, helping to preserve the environment, at the end of their lifecycle.

The Internet of Things infrastructure allows combinations of smart objects (i.e., wireless sensors, mobile robots, etc.), sensor network technologies, and human beings, using different but interoperable communication protocols and realises a dynamic multimodal/heterogeneous network that can be deployed also in inaccessible, or remote spaces (oil platforms, mines, forests, tunnels, pipes, etc.) or in cases of emergencies or hazardous situations (earthquakes, fire, floods, radiation areas, etc.). In this infrastructure, these different entities or "things" discover and explore each other and learn to take advantage of each

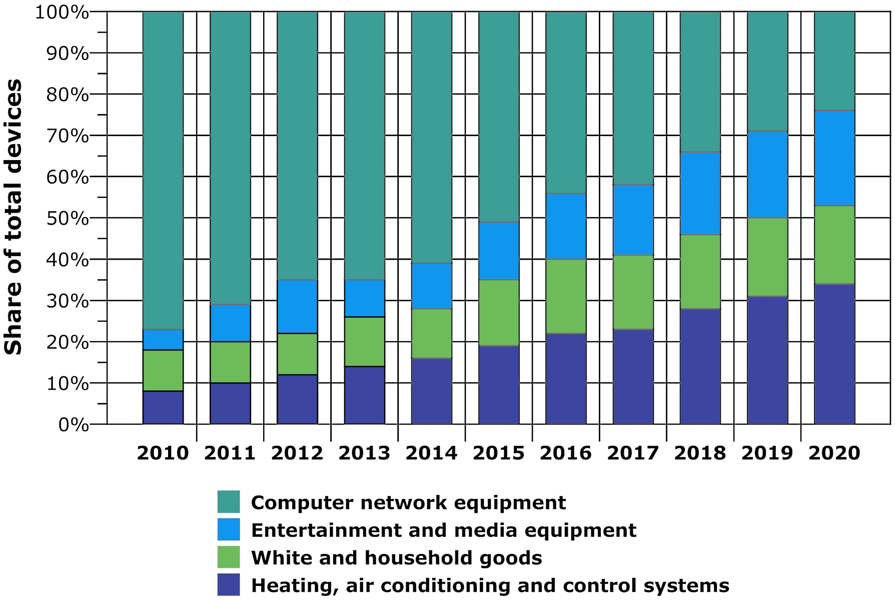

Fig. 2.4 Share of Internet-connectable consumer household devices by type, worldwide, 2010–2020 [1].

other's data by pooling of resources and dramatically enhancing the scope and reliability of the resulting services.

IoT is included by the US National Intelligence Council in the list of six "Disruptive Civil Technologies" with potential impacts on US [3]. NIC considers that "by 2025 Internet nodes may reside in everyday things — food packages, furniture, paper documents, and more." It describes future opportunities that will arise, starting from the idea that "popular demand combined with technology advances could drive widespread diffusion of an Internet of Things (IoT) that could, like the present Internet, contribute invaluably to economic development." The possible threats deriving from a widespread adoption of such a technology are also presented. It is discussed that "to the extent that everyday objects become information security risks, the IoT could distribute those risks far more widely than the Internet has to date."

The concept of Internet of Things is based on many enabling technologies that form the backbone of this new paradigm and for many people is rather abstract. In this context an interesting blog discussion started in 2010, that presents opinions on what the Internet of Things is not [6]. Based on the author's opinion the IoT is not:

- Ubiquitous/pervasive computing: Although the miniaturization of computing devices and the ubiquitous services derived from their data is probably a requirement for the IoT, pervasive computing is NOT the Internet of Things. Ubiquitous computing doesn't imply the use of objects, nor does it require an Internet infrastructure.
- The Internet Protocol: The Internet can be used globally because clients and servers use the same protocol for communication: however many objects in the Internet of Things will not be able to run an Internet Protocol.
- Communication technologies: As this represents only a partial functional requirement in the Internet of Things similar to the role of communication technology in the Internet and equalling communication technologies such as WiFi, Bluetooth, ZigBee, 6LoWPAN, ISA 100, WirelessHart/802.15.4, 18000-7, LTE to the Internet of Things is too simplistic. However, we can say that these technologies certainly might be part of Internet of Things.
- Embedded devices: RFID or wireless sensor networks (WSN), may be part of the Internet of Things, but as stand alone applications (intranets) they miss the back-end information infrastructures necessary to create new services. The IoT has come to mean much more that just networked RFID systems. While RFID systems have at least certain standardized information architectures to which all the Internet community could refer, global WSN infrastructures have not yet been standardized.
- Applications: A common misuse of the Internet of Things, very related with the pervasive computing issue and just as Google or Facebook could not be used in the early 90's to describe the possibilities offered by Internet or WWW. It is arguably to use Internet application and services to describe the Internet itself, but it is even more illogical to refer to small applications that would have no real impact on a global Internet.

In the vision of the Cluster these technologies are part of Internet of Things and are enablers of implementing the concept of Internet of Things in different applications. The IERC strategic research agenda is addressing

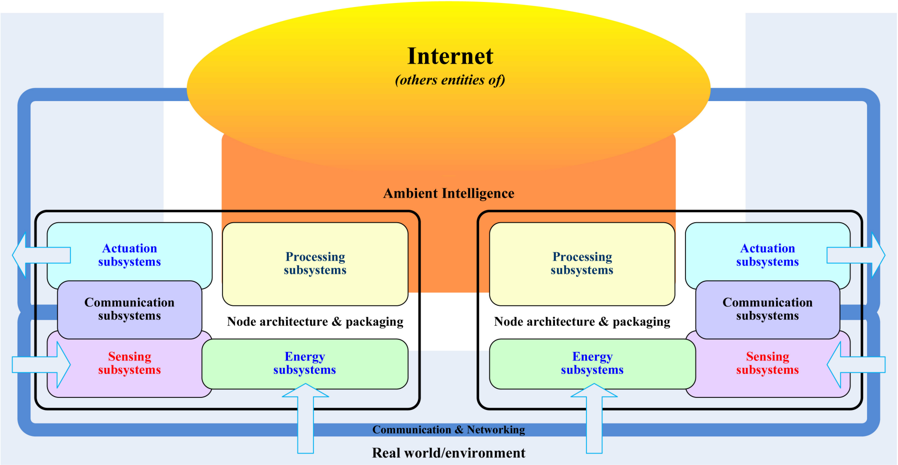

Fig. 2.5 Object connected to Internet of Things and their three main challenging domains: Technologies — Communication — Intelligence [15].

these challenges, considering and integrating the different point of views and differentiating between the Internet of Things from the other concepts and trying to identify the research needs for the implementation and deployment of IoT applications.

The interface between the real and digital worlds requires the capacity for the digital world to sense the real world and act on it. This implies the convergence of at least three domains: Technologies (nanoelectronics, sensors, actuators, embedded systems, cloud computing, software, etc.), Communication and Intelligence [15].

At the conceptual level the IoT technology represents the "middleware" between the implementation of the "grand challenges" such as climate change, energy efficiency, mobility, digital society, health at the global level and enabling technologies such as nanoelectronics, communications, sensors, smart phones, embedded systems, cloud computing and software technologies. These challenges will give rise to new products, new services, new interfaces and new applications. The "grand challenges" may also give rise to smart environments and smart spaces.

2.3 Technological Trends

Advances in wireless networking technology and the greater standardization of communications protocols make it possible to collect data from sensors and wireless identifiable devices almost anywhere at any time. Miniaturized silicon chips are designed with new capabilities, while costs, following the Moore's Law, are falling. Massive increases in storage and computing power, some of it available via cloud computing, make number crunching possible at very large scale and at a high volume, low cost.

It is possible to identify, for the years to come, a number of distinct macro-trends that will shape the future of ICT.

- First, the explosion in the volumes of data collected, exchanged and stored by IoT interconnected objects will require novel methods and mechanisms to find, fetch, and transmit data. This will not happen unless the energy required to operate these devices is dramatically decreased or we discover novel energy harvesting techniques. Today, many data centres have already reached their maximum level of energy consumption, and the acquisition of new devices can only follow the replacement of old ones, as it is not possible to increase energy consumption.
- Second, research is looking for ultra low power autonomic devices and systems from the tiniest smart dust to the huge data centres that will self-harvest the energy they need.
- Third, miniaturisation of devices is also taking place at a lightning speed, and the objective of a single-electron transistor, which seems to be (depending on new discoveries in physics) the ultimate limit, is getting closer.
- Fourth, the trend is towards the autonomous and responsible behaviour of resources. The ever growing complexity of systems, possibly including mobile devices, will be unmanageable, and will hamper the creation of new services and applications, unless the systems will show "self-*" functionality, such as self-management, self-healing and self-configuration.

The key to addressing these macro-trends by IoT is research and development, which drives the innovation cycle by exploiting the results to bring beneficial new technologies to the market and therefore into industrial applications.

IoT research and development is becoming more complex, due to the already highly advanced level of technology, the global, intersectoral and inter-disciplinary collaboration needed and the ever increasing demands of society

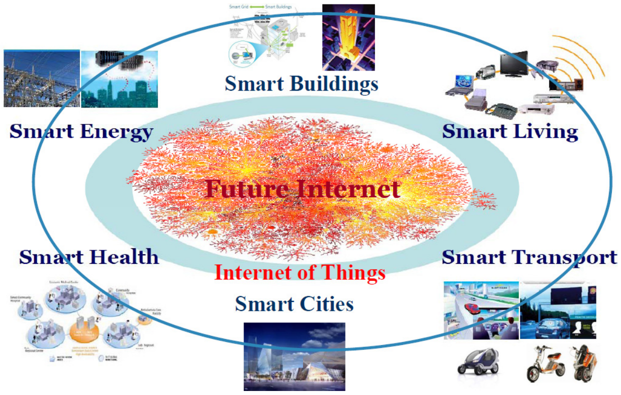

Fig. 2.6 IoT and smart environments creation.

and the economic global marketplace. Development of certain enabling technologies such as nanoelectronics, communications, sensors, smart phones, embedded systems, cloud computing and software technologies will be essential to support important future IoT product innovations affecting the different industrial sectors. In addition, systems and network infrastructure (Future Internet) are becoming critical due to the fast growth and advanced nature of communication services as well as the integration with the healthcare systems, transport, energy efficient buildings, smart grid, smart cities, and electric vehicles initiatives.

The focus of IoT research and development projects is on producing concrete results for several industries, which can then be further developed or exploited directly in creating smart environments/spaces and self-aware products/processes for the benefit of society.

2.4 IoT Applications

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. The concept is illustrated in Figure 2.6.

The developments in smart entities will also encourage the development of the novel technologies needed to address the emerging challenges of public health, aging population, environmental protection and climate change, the conservation of energy and scarce materials, enhancements to safety and security and the continuation and growth of economic prosperity. These challenges will be addressed by:

- Providing reliable, intelligent, self-managed, context aware and adaptable network technology, network discovery, and network management.
- Refining the interaction between hardware, software, algorithms as well as the development of smart interfaces among things (smart machine to machine, things to things interfaces) and smart human-machine/things interfaces, thus enabling smart and mobile software.
- Embedding smart functionality through further developments in the area of nanoelectronics, sensors, actuators, antennas, storage, energy sources, embedded systems and sensor networks.
- Developments across disciplines to address the multi functional, multi-domain communications, information and signal processing technology, identification technology, and discovery and search engine technologies.
- Developing novel techniques and concepts to improve the existing security, privacy and business safety technologies in order to adapt to new technological and societal challenges.
- Enhancing standardisation, interoperability, validation and modularisation of the IoT technologies and solutions.
- Defining new governance principles that address the technology developments and allow for business development and free access to knowledge in line with global needs while maintaining respect for privacy, security and safety.

In this context Internet of Things applications are linked with the Green computing or Green ICT which is defined as “the study and practice of designing, manufacturing, using, and disposing of computers, servers, and associated subsystem — such as monitors, printers, storage devices, and networking and communications systems — efficiently and effectively with minimal or no impact on the environment” [8].

In the future most edge-connecting object-connected devices will have some form of wireless connectivity and the Internet of Things will drive energy efficient applications such as the power grid, or smart grid, connected electric vehicles, energy efficient buildings and will contribute to major savings in fuel consumption and hence carbon emissions. The Internet of Things technologies will allow greening of ICT by CO_2 reduction of infrastructure and products in ICT industry and greening by ICT applications by CO_2 reduction through convergence with ICT in other industries and industrial sectors. Internet of Things provides the technology and solutions that make full use of the integrated technologies of the communications networks and Internet technologies to build future oriented green intelligent cities, that provides a wide variety of interactive and control methods for the system of urban information and further support for building comprehensive systems for the development of urban ecology.

2.5 Technology Enablers

2.5.1 Energy

Energy issues, in all its phases, from harvesting to conservation and usage, are central to the development of the IoT. There is a need to research and develop solutions in this area (nanoelectronics, semiconductor, sensor technology, micro systems integration) having as an objective ultra low power devices, as current devices seem inadequate considering the processing power needed and energy limitations of the future. Using "More Than Moore's" technologies, that focus on system integration, will increase efficiency of current systems, and will provide a number of solutions for the future needs.

2.5.2 Intelligence

Capabilities such as self-awareness, context awareness and inter-machine communication are considered a high priority for the IoT. Integration of memory and processing power, and the ability to withstand harsh environments are also a high priority, as are the best possible security techniques. More specifically, the provision of security at physical layer, exploiting the characteristics of wireless channels, represents the envisioned low-complexity solution also addressing the scalability issues raised by large-scale deployments of smart "things". Transistor density is bound to grow, following Moore's Law, allowing therefore more "intelligent" electronics with increased on chip processing and memory capabilities. Novel cognitive approaches that leverage opportunistically on the time dependent available heterogeneous network resources can be adopted to support seamless continuous access to the information network as well as handle intermittent network connectivity in harsh and/or mobile environments. "Intelligent" approaches to knowledge discovery and device control will also be important research challenges.

2.5.3 Communication

New smart antennas (fractal antennas, adaptive antennas, receptive directional antennas, plasma antennas), that can be embedded in the objects and made of new materials are the communication means that will enable new advanced communications systems on chip, which when combined with new protocols optimized across the Physical (PHY), Media Access Control (MAC) and the Network (NWK) layers will enable the development of different Application Programming Interfaces (APIs) to be used for different applications. Modulation schemes, transmission rates, and transmission speed are also important issues to be tackled. New advanced solutions need to be defined to effectively support mobility of billions of smart things, possibly equipped with multiple heterogeneous network resources. Last but not least, network virtualisation techniques are key to the ensure an evolutionary path for the deployment of IoT applications with assured Quality of Service (QoS).

2.5.4 Integration

Integration of wireless identification technologies (like Radio Frequency Identification — RFID) into packaging, or, preferably, into products themselves will allow for significant cost savings, increased eco-friendliness of products and enable a new dimension of product self-awareness for the benefit of consumers. Integration requires addressing the need for heterogeneous systems that have sensing, acting, communication, cognitive, processing and adaptability features and includes sensors, actuators, nanoelectronics circuits, embedded systems, algorithms, and software embedded in things and objects.

2.5.5 Dependability

Dependability of IoT systems is of paramount importance; therefore the IoT network infrastructure must ensure reliability security and privacy by supporting individual authentication of billions of heterogeneous devices using heterogeneous communication technologies across different administrative domains. Reliable energy-efficient communication protocols must also be designed to ensure dependability.

2.5.6 Semantic Technologies and IoT

IoT requires devices and applications that can easily connect and exchange information in an ad-hoc fashion with other systems. This will require devices and services to express needs and capabilities in formalised ways. To facilitate the interoperability in the IoT further research into semantic technologies is needed. Examples of challenges are large-scale distributed ontologies, new approaches to semantic web services, rule engines and approaches for hybrid reasoning over large heterogeneous data and fact bases, semantic-based discovery of devices and semantically driven code generation for device interfaces.

2.5.7 Resource-constrained Scenarios for Business Based IoT

IoT implies that even the smallest device or sensor could be connected to the network. Research in wireless sensor networks has already resulted in promising solutions, tools and operating systems that can run on very small and resource-constrained devices. These solutions need to be evaluated in real large-scale industrial applications in order to illustrate business-based scenarios for IoT.

2.5.8 Modelling and Design

The design of large-scale IoT systems is challenging due to the large number of heterogeneous components involved and due to the complex iterations among devices introduced by cooperative and distributed approaches. To cope with this issue, innovative models and design frameworks need to be devised; for example, inspired by co-simulation methods for large systems of systems and hardware-in-the-loop approaches.

2.5.9 Validation and Interoperability

Standardisation is a must but it is not enough. It is a known fact that, even if following the same standard, two different devices might not be interoperable.

This is a major showstopper for wide adoption of IoT technologies. Due to the complex and diverse nature of IoT technologies only one interoperability solution may not be possible and integration is therefore required. Future tags and devices must integrate different communication schemes, allow different architectures, centralised or distributed, and be able to communicate with other networks. Interoperability of IoT technologies will always be a complex topic which requires research effort to address the new challenges raised. This for instance might be achieved by increased embedded intelligence and different radio access technologies sometimes even with cognitive capabilities. All these new emerging features together with the necessary intercommunication between different technologies will raise even more complexity in testing and validation and therefore common methodologies and approaches are necessary to validate and ensure interoperability in a coherent and cost effective way. The efforts necessary in achieving success in this area must not be underestimated as the results will serve to really exploit IoT research results by successful worldwide interoperable deployments. One of key success factor of GSM/UMTS/LTE technologies is that the specifications were developed together with the conformity and interoperability testing standards which included machine readable tests written in high level testing languages (like TTCN).

2.5.10 Standards

Clearly, open standards are key enablers for the success of wireless communication technologies (like RFID or GSM), and, in general, for any kind of Machine-to-Machine communication (M2M). Without global recognised standards (such as, the TCP/IP protocol suite or GSM/UMTS/LTE) the expansion of RFID and M2M solutions to the Internet of Things cannot reach a global scale. The need for faster setting of interoperable standards has been recognised an important element for IoT applications deployment. Clarification on the requirements for a unique global identification, naming and resolver is needed. Lack of convergence of the definition of common reference models, reference architecture for the Future Networks, Future Internet and IoT and integration of legacy systems and networks is a challanges that has to be addressed in the future.

2.5.11 Manufacturing

Last but certainly not least, manufacturing challenges must be convincingly solved. Costs must be lowered to less than one cent per passive RFID tag, and production must reach extremely high volumes, while the whole production process must have a very limited impact on the environment, be based on strategies for reuse and recycling considering the overall life-cycle of digital devices and other products that might be tagged or sensor-enabled.

2.6 Internet of Things Research Agenda, Timelines and Priorities

2.6.1 Identification Technology

Further research is needed in the development, convergence and interoperability of technologies for identification and authentication that can operate at a global scale. This includes the management of unique identities for physical objects and devices, and handling of multiple identifiers for people and locations and possible cross-referencing among different identifiers for the same entity and with associated authentication credentials. The IoT will include a very large number of nodes, each of which will produce content that should be retrievable by any authorized user regardless of its or if is a person of his/her position.

New effective addressing policies mobility management are required and frameworks are needed for reliable and consistent encoding and decoding of identifiers, irrespective of which data carrier technology that is used (e.g., whether linear or 2-D barcode, RFID, memory button or other technologies), including those that may be developed in the future. For some applications, it may be necessary to use encrypted identifiers and pseudonym schemes in order to protect privacy or ensure security. Identifiers play a critical role for retrieval of information from repositories and for lookup in global directory lookup services and discovery services, to discover the availability and find addresses of distributed resources.

It is vital that identification technology can support various existing and future identifier schemes and can also interoperate with identifier structures already used in the existing Internet and World Wide Web, such as Uniform Resource Identifiers (URIs).

Further research is needed in development of new technologies that address the global ID schemes, identity management, identity encoding/ encryption, pseudonymity, (revocable) anonymity, authentication of parties, repository management using identification, authentication and addressing schemes, and the creation of global directory lookup services and discovery services for Internet of Things applications with various unique identifier schemes.

2.6.2 Internet of Things Architecture Technology

The Internet of Things needs an open architecture to maximise interoperability among heterogeneous systems and distributed resources including providers and consumers of information and services, whether they be human beings, software, smart objects or devices. Architecture standards should consist of well-defined abstract data models, interfaces and protocols, together with concrete bindings to neutral technologies (such as XML, web services etc.) in order to support the widest possible variety of operating systems and programming languages.

The architecture should have well-defined and granular layers, in order to foster a competitive marketplace of solutions, without locking any users into using a monolithic stack from a single solution provider. Like the Internet, the IoT architecture should be designed to be resilient to disruption of the physical network and should also anticipate that many of the nodes will be mobile, may have intermittent connectivity and may use various communication protocols at different times to connect to the IoT.

IoT nodes may need to dynamically and autonomously form peer networks with other nodes, whether local or remote, and this should be supported through a decentralised, distributed approach to the architecture, with support for semantic search, discovery and peer networking. Anticipating the vast volumes of data that may be generated, it is important that the architecture also includes mechanisms for moving intelligence and capabilities for filtering, pattern recognition, machine learning and decision-making towards the very edges of the network to enable distributed and decentralised processing of the information, either close to where data is generated or remotely in the cloud. The architectural design will also need to enable the processing, routing, storage and retrieval of events and allow for disconnected operations (e.g., where network connectivity might only be intermittent). Effective caching, pre-positioning and synchronisation of requests, updates and data flows need to be an integral feature of the architecture. By developing and defining the architecture in terms of open standards, we can expect increased participation from solution providers of all sizes and a competitive marketplace that benefits end users.

In summary, the following issues have to be addressed:

- Distributed open architecture with end to end characteristics, interoperability of heterogeneous systems, neutral access, clear layering and resilience to physical network disruption.
- Decentralized autonomic architectures based on peering of nodes.
- Architectures moving intelligence at the very edge of the networks, up to users' terminals and things.
- Cloud computing technology, event-driven architectures, disconnected operations and synchronization.
- Use of market mechanisms for increased competition and participation.

2.6.3 Communication Technology

Billions of connected devices are pushing current communication technologies, networks and services approaches to their limits and require new technological investigations. Research is required in the field of Internet architecture evolution, wireless system access architectures, protocols, device technologies, service oriented architecture able to support dynamically changing environments, security and privacy. Research is required in the field of dedicated applications integrating these technologies within complete end-to-end systems.

In the Internet of Things the following topics related to communication technology have to be considered:

- Communication to enable information exchange between "smart things/objects" and gateways between those "smart things/objects" and Internet.
- Communication with sensors for capturing and representing the physical world in the digital world.
- Communication with actuators to perform actions in the physical world triggered in the digital world.

- Communication with distributed storage units for data collection from sensors, identification and tracking systems.
- Communication for interaction with humans in the physical world.
- Communication and processing to provide data mining and services.
- Communication for physical world localization and tracking.
- Communication for identification to provide unique physical object identification in the digital world.

In the IoT the range of connectivity options will increase exponentially and the challenges of scalability, interoperability and ensuring return on investment for network operators will remain.

In this context the communication needs will change and new radio and service architectures will be required to cater for the connectivity demands of emerging devices. The frequency spectrum allocation and spectrum masks will have to be adapted to the new bandwidth and channel requirements. New communications paradigms that use opportunistically the communication resources available at any given time will have to be adopted to provide seamless connectivity. Approaches based on the use of multiple radio bearers or inspired by cognitive radio technologies will have to be pursued to provide dependability, especially in harsh environments. Issues to be addressed:

Issues to be addressed:

- Internet of Things energy efficient communication multi frequency protocols, communication spectrum and frequency allocation.
- New efficient multiuser detection schemes.
- Software defined radios to remove need for hardware upgrades when new protocols emerge.
- Cognitive radio approaches tailored to low-power IoT devices
- Opportunistic communications paradigms
- Multi-radio wireless communications
- Reliable energy-efficient communication protocols to ensure dependability (e. g. in harsh environments)
- Connectionless communications, even beyond IP.
- High performance, scalable algorithms and protocols.

2.6.4 Network Technology

The evolution and pervasiveness of present communication technologies has promised to revolutionize the way humans interact with their environment. The Internet of Things is born from this vision in which objects form an integral part of the communication infrastructures that wire today's world. For this vision to be realized, the Internet of Things architecture needs to be built on top of a network structure that integrates wired and wireless technologies in a transparent and seamless way. Wireless network technologies have gained more focus due to their ability to provide unobtrusive wire-free communication. They have also become the leading area of research when combined with data collecting technologies used for environmental and object monitoring.

In this regard, wireless sensor networks promise low power, low cost object monitoring and networking, constituting a fundamental technology for the evolution towards a truly embedded and autonomous Internet of Things. Design objectives of the proposed solutions are energy efficiency, scalability since the number of nodes can be very high, reliability, and robustness and self healing.

Integration of sensing technologies into passive RFID tags allows new applications into the IoT context. Intel Labs [10] is involved in research and development focused on wireless identification and sensing platforms where the tags are powered and read by standard RFID readers, harvesting the power from the reader's querying signal. The wireless identification and sensing platforms have been used to measure quantities in a certain environment, such as light, temperature, acceleration, strain, and liquid level.

In Internet of Things scenarios, distributed (pre-)processing of sensor data is required in order to handle a massive amount of measurement data. Therefore, the communication network needs to support an intelligent distribution of (pre-)processing power, considering the status of the power supply of the involved (mostly embedded) devices, the energetic transport cost, as well as the processing power available at each device. The data exchange itself can be optimized by using and developing energy-efficient protocols that require a smaller number of bits to exchange for given information and that require less processing power for the data evaluation on a device level; an example for such a protocol is Binary XML [14].

Auto configuration and network service assembling is an important area since Internet of Things requires highly dynamic and flexible network domains. The handling of such systems is just feasible if the network configuration is automated and adaptable to the actual situation [14].

Research is needed on:

- Networks exploiting: On-chip technology considering on chip communication architectures for dynamic configurations design time parameterized architecture with a dynamic routing scheme and a variable number of allowed virtual connections at each output.
- Scalable communication infrastructure on chip to dynamically support the communication among circuit modules based on varying workloads and/or changing constraints.
- Power aware networks that turn on and off the links in response to bursts and dips of traffic on demand.
- Network virtualisation.
- Adaptability and evolvability to heterogeneous environments, content, context/situation, and application needs (vehicular, ambient/domestic, industrial, etc.).
- Solutions to effectively support mobility of billions of smart things
- Solutions to effectively support connectivity of (possible mobile) smart things equipped with multiple heterogeneous network resources
- Cross-cutting challenge covering Network foundation as well as Internet by and for People, Internet of Services, Internet of Contents and Knowledge, and Internet of Things.

IP provides today the protocol for implementing IoT applications. More research is required for IP technology and eventually the development of different post IP protocols optimized for IoT, compatible and interoperable with the exiting IP technologies.

Issues to be addressed:

- Network technologies (fixed, wireless, mobile etc.).
- Ad-hoc, wireless sensor networks.
- Autonomic computing and networking.
- Opportunistic networking

- Development of the infrastructure for "Network of Networks" capable of supporting dynamically small area and scale free connections and characteristics (typical social communities).
- Password and identity distribution mechanisms at the network level.
- Security and privacy of heterogeneous devices using heterogeneous communication technologies across different administrative domains.
- Anonymous networking.
- IP and post IP technologies.
- Traffic modelling and estimation to ensure efficient communication, load balance and end-to-end Quality of Service.
- Multipath, multi-constraint routing algorithms to enable load balancing among resources constrained intermediate nodes.

2.6.5 Software, Services and Algorithms

Only with appropriate software will it be possible that the Internet of Things comes to life as imagined, as an integral part of the Future Internet. It is through software that novel applications and interactions are realized, and that the network with all its resources, devices and distributed services becomes manageable. For manageability, the need for some sort of self-configuration and auto-recovery after failures is foreseen. The IoT is based on the coexistence of many heterogeneous set of things, which individually provide specific functions accessible through its communication protocol. The use of an abstraction layer capable of harmonizing the access to the different devices with a common language and procedure is a common trend in IoT applications. There are devices that offer discoverable web services on an IP network, while there are many other devices without such services that need the introduction of a wrapping layer, consisting of an interface and a communication sub-layers. The interface provides the web interface and is responsible for the management of all the in/out messaging operations involved in the communication with the real/physical world. The communication sub-layer implements the logic behind the web service methods and translates these methods into a set of device specific commands to communicate with the real/physical tagged objects.

Services play a key role: they provide a good way to encapsulate functionality (e.g., abstracting from underlying heterogeneous hardware or implementation details), they can be orchestrated to create new, higher-level functionality, and they can be deployed and executed in remote locations, in-situ on an embedded device if necessary. Such distribution execution of service logic, sometimes also called distributed intelligence, will be the key in order to deal with the expected scalability challenges. The middleware is defined as a software layer or a set of sub-layers interposed between the technological and the application levels. The middleware architectures proposed in many projects for the IoT often follow the Service Oriented Architecture (SOA) approach. The adoption of the SOA principles allows for decomposing complex systems into applications consisting of an ecosystem of simpler and with well defined components. The use of common interfaces and standard protocols is common in such systems. However typical SOAs fail to provide the loose coupling and proper separation between types and instances that are needed in domains that involve "things" (e.g. home automation). For instance two light appliances may offer the same type of service (turning light on and off) but different actual services, if only because they are located in different rooms. These loose coupling and proper separation between types and instances are however well known in Component Based Software Engineering (CBSE) approaches.

Tools to support the challenging design of large-scale IoT systems need to be developed as well. Such tools need to cope with the large number of heterogeneous components involved and with the complex iterations among devices introduced by cooperative and distributed approaches. Innovative models and design frameworks need to be devised to support such tools (e.g., inspired by co-simulation methods for large systems of systems and hardware-in-the-loop approaches).

Issues to be addressed include:

- Service discovery and composition.
- Service management.
- Object abstraction.
- Semantic interoperability, semantic sensor web etc.
- Data sharing, propagation and collaboration.
- Autonomous agents.
- Human-machine interaction.

- Self management techniques to overcome increasing complexities and save energy.
- Distributed self adaptive software for self optimization, self configuration, self healing.
- Lightweight and open middleware based on interacting components/modules abstracting resource and network functions.
- Energy efficient micro operating systems.
- Software for virtualisation.
- Service composition.
- Language for object interaction.
- Bio-inspired algorithms (e.g., self organization) and solutions based on game theory (to overcome the risks of tragedy of commons and reaction to malicious nodes).
- Algorithms for optimal assignment of resources in pervasive and dynamic environments.
- Modelling and design tools for IoT objects and systems
- Mathematical models and algorithms for inventory management, production scheduling, and data mining.

2.6.6 Cloud Computing

In its broadest form, a ‘cloud’ can be defined as “an elastic execution environment of resources involving multiple stakeholders and providing a metered service at multiple granularities for a specified level of quality (of service).” [9].

It is up to debate whether the Internet of Things is related to cloud systems at all: Whilst the Internet of Things will certainly have to deal with issues related to elasticity, reliability and data management etc., there is an implicit assumption that resources in cloud computing are of a type that can host and/or process data — in particular storage and processors that can form a computational unit (a virtual processing platform). However, specialised clouds may e.g., integrate dedicated sensors to provide enhanced capabilities and the issues related to reliability of data streams etc. are principally independent of the type of data source. Though sensors as yet do not pose essential scalability issues, metering of resources will already require some degree of sensor information integration into the cloud. Clouds may furthermore offer vital support to the Internet of Things, in order to deal with a flexible amount of data originating from the diversity of sensors and "smart things/objects." Similarly, cloud concepts for scalability and elasticity may be of interest for the Internet of Things in order to better cope with dynamically scaling data streams [9].

Deployment of 4G and other wireless broadband networks will support new cloud services, and demand for cloud services will drive network deployment. Additional utility services, such as voice recognition and other intelligent interfaces will become a part of cloud service platforms; and standards for cloud interoperability will develop so that data, applications, and environments can be ported between different cloud services [11].

Cloud computing is a building block of the Future Internet and it is expected that the Internet of Things will be the biggest consumer of Cloud. The IoT applications are composed of many detectors and services to manage them and are very dynamic involving rapidly varying data volumes and rates. Clouds provide an elastic facility to manage this variability. Of course a Cloud environment can also provide the services for analysis of the data streams often

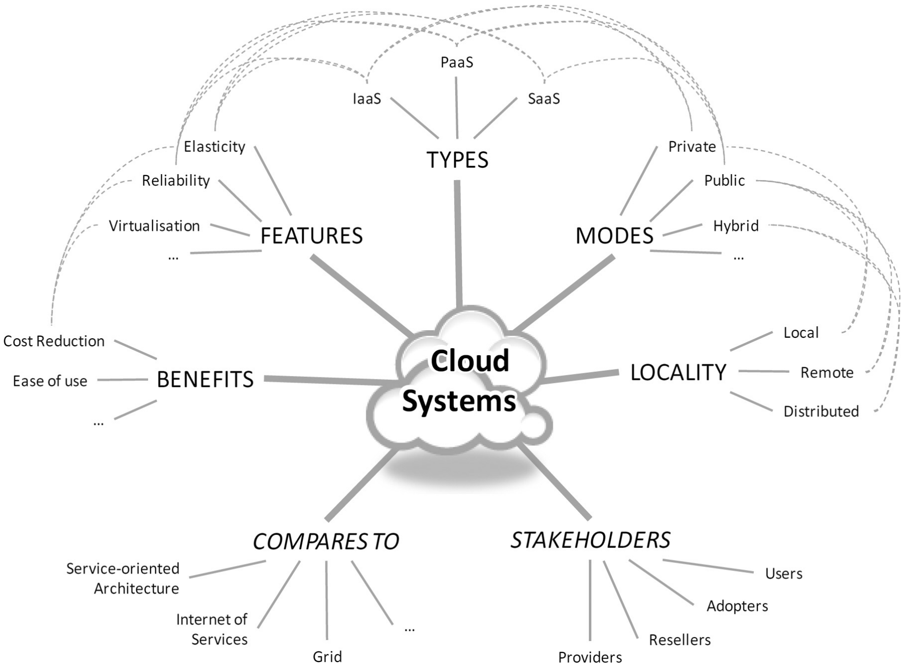

Fig. 2.7 Non-exhaustive view on the main aspects forming a cloud system [9].

associated with synchronous simulation to aid the provision of information to the end-user in an optimal form. The business benefit occurs in applications such as environmental monitoring, healthcare monitoring where the high volumes and rates of data need rapid processing to information for understanding.

2.6.7 Hardware

The developments in the area of IoT will require research for hardware adaptation and parallel processing in ultra low power multi processor system on chip that handle situations not predictable at design time with the capability of self-adaptiveness and self-organization. Research and development is needed in the area of very low power field-programmable gate array hardware where the configuration (or parts of it) is changed dynamically from time to time to introduce changes to the device. Context switching architectures, where a set of configurations are available and the device between switch between them depending on the defined using context.

Important issues are making a full interoperability of interconnected devices possible, providing the hardware with a sufficient degree of smartness by enabling their adaptation and autonomous behaviour, while guaranteeing trust, privacy, and security. In this context the IoT poses several new problems concerning the networking aspects when the things composing the IoT are defined in many cases by low resources in terms of both computation and energy capacity.

Research is needed for ultra low power very large scale integrated (VLSI) circuits containing scalable cognitive hardware systems that are changing the topology mapped on the chip using dedicated algorithms.

Self adaptive networks on chip that analyzes itself during run time and self adapts are required for IoT applications. Such run time adaptive network on chip will adapt the underlying interconnection infrastructure on demand in response to changing communication requirements imposed by an application and context.

Issues to be addressed:

- Nanotechnologies–miniaturization.
- Sensor technologies–embedded sensors, actuators.
- Solutions bridging nano and micro systems.
- Communication–antennas, energy efficient RF front ends.

- Nanoelectronics devices and technologies, self configuration, self optimization, self healing circuit architectures.
- Polymer electronics.
- Embedded systems–micro energy microprocessors/microcontrollers, hardware acceleration.
- Spintronics.
- Low cost, high performance secure identification/authentication devices.
- Low cost manufacturing techniques.
- Tamper-resistant technology, side-channel aware designs.

2.6.8 Data and Signal Processing Technology

By 2020, trillions of networked sensors will be deployed around the planet, in the spaces we inhabit, the systems we use, the devices we carry, and inside our bodies. Sensors are a key enabling technology; with detection, measurement, computation, and communication, they can make passive systems active. Sensors will be used to measure everything from acceleration and location to temperature, energy use, soil chemistry, air pollution, and health conditions. They will help ensure the structural integrity of airplanes, bridges, buildings and other critical infrastructure, and make our living environments more responsive to us. The streams of data they generate will support better management of resources and provide early warnings of significant events, from impending heart attacks to climate change. They will smooth transactions, and increase the visibility and transparency of previously obscure relationships and hidden economies. The information they provide will be actionable, and ultimately, provide us with greater foreknowledge and awareness of things to come [11].

In the context of Internet of Things the devices that are operating at the edge are evolving from embedded systems to cyber physical and web enabled “smart things/objects” that are integrating computation, physical and cognitive processes. Cognitive devices, embedded computers and networks will monitor and control the physical processes, with feedback loops where physical processes affect computations and cognitive processes and contrariwise. This convergence of physical computing and cognitive devices (wireless sensor networks, mobile phones, embedded systems, embedded computers, micro robots etc.) and the Internet will provide new design opportunities and challenges and requires new research that addresses the data and signal processing technology.

A typical features of cyber physical and web enabled "smart things/objects" will be the heterogeneity of device models, communication and cognitive capabilities. This heterogeneity concerns different execution models (synchronous, asynchronous, vs. timed and real-timed), communication models (synchronous vs. asynchronous), and scheduling of real time processes.

Issues to be addressed:

- Semantic interoperability,
- Service discovery,
- Service composition,
- Semantic sensor web,
- Data sharing, propagation and collaboration,
- Autonomous agents,
- Human machine interaction and human machine interfaces.

2.6.9 Discovery and Search Engine Technologies

The Internet of Things will consist of many distributed resources including sensors and actuators, as well as information sources and repositories. It will be necessary to develop technologies for searching and discovering such resources according to their capabilities (e.g., type of sensor/actuator/services offered), their location and/or the information they can provide (e.g., indexed by the unique IDs of objects, transactions etc.). Search and discovery services will be used not only by human operators but also by application software and autonomous smart objects, in order to help gathering complete sets of information from across many organisations and locations. Such services may also serve to discover what ambient infrastructure is available to support smart objects with their needs for transportation and handling, heating/cooling, network communication and data processing. These services play a key role in the mapping between real entities such as physical objects and in the assembly of their digital and virtual counterparts from a multitude of fragments of information owned and provided by different entities. Universal authentication mechanisms will be required, together with granular access control mechanisms that allow owners of resources to restrict who can discover their resources or the association between their resource and a specific entity, such as a uniquely identified physical object.

For efficient search and discovery, metadata and semantic tagging of information will be very important and there are significant challenges in ensuring that the large volumes of automatically generated information can be automatically and reliably accommodated without requiring human intervention. It will also be important that terrestrial mapping data is available and cross-referenced with logical locations such as postcodes and place names and that the search and discovery mechanisms are able to handle criteria involving location geometry concepts, such as spatial overlap and separation.

Issues to be addressed:

- Device discovery, distributed repositories
- Positioning and localisation
- Mapping of real, digital and virtual entities
- Terrestrial mapping data
- Semantic tagging and search
- Universal authentication mechanisms

2.6.10 Relationship Network Management Technologies

With many Internet of Things and applications moving to a distributed seamless architecture the future application manager needs to monitor more than just the infrastructure. The Internet of Things must incorporate traffic and congestion management. This will sense and manage information flows, detect overflow conditions and implement resource reservation for time-critical and life-critical data flows. The network management technologies will need depth visibility to the underlying seamless networks that serves the applications and services and check the processes that run on them, regardless of device, protocol, etc. This will require identifying sudden overloads in service response time and resolving solutions, monitoring IoT and web applications and identify any attacks by hackers, while getting connected remotely and managing all "smart things"/obejects involved in specific applications from remote "emergency" centres.

Issues to be addressed:

- Propagation of memes by things
- Identity, relationship and reputation management
- Traffic modelling and estimation

2.6.11 Power and Energy Storage Technologies

Objects require a digital "self" in order to be part of the Internet of Things. This participation is obtained by combining electronic identification, embedded and wireless communication technologies into the physical objects themselves. Simple digitalization alternatives, such as bar code and passive RFID, do not require an integral power source. More complex alternatives, such as those that provide active communications and object condition monitoring, need batteries to power the electronics.

Energy storage has become one of the most important obstacles to the miniaturization of electronic devices, and today's embedded wireless technologies such as Wireless Sensor Networks and Active RFID suffer from either bulky packaging to support large batteries or from short life times, that will require recharging or replacement of the integrated batteries. In order for the IoT to succeed in providing truly embedded and digital object participation, it is necessary to continue with the research on miniature high-capacity energy storage technologies. A solution that could bypass the shortcomings of energy storage is the harvesting of energy from the environment, which would automatically recharge small batteries contained in the objects.

Energy harvesting is still a very inefficient process that would require a large amount of research. Sources for energy harvesting in embedded devices could include, among others, vibration, solar radiation, thermal energy, etc.

Micro power technologies have emerged as a new technology area that can provide many development opportunities for IoT devices.

Research topics and issues that need to be addressed include:

- Energy harvesting/scavenging for MEMS devices and microsystems

- Electrostatic, piezoelectric and electromagnetic energy conversion schemes
- Thermoelectric systems and micro coolers
- Photovoltaic systems
- Micro fuel cells and micro reactors
- Micro combustion engines for power generation and propulsion
- Materials for energy applications
- Micro power ICs and transducers
- Micro battery technologies
- Energy storage and micro super capacitor technologies

2.6.12 Security and Privacy Technologies

Internet of Things needs to be built in such a way as to ensure an easy and safe user control. Consumers need confidence to fully embrace the Internet of Things in order to enjoy its potential benefits and avoid any risks to their security and privacy.

In the IoT every smart thing/object could be connected to the global Internet and is able to communicate with other smart objects, resulting in new security and privacy problems, e.g., confidentiality, authenticity, and integrity of data sensed and exchanged by 'things/objects'. Privacy of humans and things must be ensured to prevent unauthorized identification and tracking. In this context, the more autonomous and intelligent "things/smart objects" get, problems like the identity and privacy of things emerge, and accountability of things in their acting will have to be considered.

The close interaction of wirelessly interconnected things with the physical world makes it possible to pursue solutions that provide security at physical layer. Such solutions exploit the richness of the wireless channel features to ensure security at the physical layer. Their low-complexity solutions may help addressing at the same time scalability issues in large-scale IoT deployments.

The Internet of Things will challenge the traditional distributed database technology by addressing very large numbers of "things/objects" that handle data, in a global information space. This poses challenges. In this context the information map of the real world of interest is represented across billions of "things," many of which are updating in real-time and a transaction or data change is updated across hundreds or thousands of "things" with differing update policies, opens up for many security challenges and security techniques across multiple policies. In order to prevent the unauthorized use of private information, research is needed in the area of dynamic trust, security, and privacy management.

Issues to be addressed:

- Event-driven agents to enable an intelligent/self aware behaviour of networked devices
- Authentication and data integrity
- Privacy preserving technology for heterogeneous sets of devices
- Models for decentralised authentication and trust
- Energy efficient encryption and data protection technologies
- Security and trust for cloud computing
- Data ownership
- Legal and liability issues
- Repository data management
- Access and use rights, rules to share added value
- Responsibilities, liabilities
- Artificial immune systems solutions for IoT
- Secure, low cost devices
- Integration into, or connection to, privacy-preserving frameworks, with evaluation privacy-preserving effectiveness.
- Privacy Policies management
- Wireless security at physical layer

2.6.13 Standardisation

The Internet of Things will support interactions among many heterogeneous sources of data and many heterogeneous devices through the use of standard interfaces and data models to ensure a high degree of interoperability among diverse systems. Although many different standards may co-exist, the use of ontology based semantic standards will enable mapping and cross-referencing between them, in order to enable information exchange. From an architectural perspective, standards have an important role to play both within an organisation or entity and across organisations; adoption of standards promotes interoperability and allows each organisation or individual to benefit from a competitive marketplace of interoperable technology solutions from multiple providers; when those organisations or individuals which want to share or exchange information, standards allow them to do so efficiently, minimising ambiguity about the interpretation of the information they exchange. Standards regarding frequency spectrum allocation, radiation power levels and communication protocols will ensure that the Internet of Things co-operates with other users of the radio spectrum, including mobile telephony, broadcasting, emergency services etc. These can be expected to develop, as the Internet of Things increases in scale and reach and as additional radio spectrum becomes available through digital switchover etc.

As greater reliance is placed on the Internet of Things as the global infrastructure for generation and gathering of information, it will be essential to ensure that international quality and integrity standards are deployed and further developed, as necessary to ensure that the data can be trusted and also traced to its original authentic sources. In this context a close collaboration among different standardisation Institutions and other world wide Interest Groups and Alliances is mandatory.

Issues to be addressed:

- IoT standardisation
- Ontology based semantic standards
- Spectrum energy communication protocols standards
- Standards for communication within and outside cloud
- International quality/integrity standards for data creation, data traceability

2.7 Future Technological Developments

Development	2011–2015	2015–2020	Beyond 2020
Identification Technology	• Unified framework for unique identifiers • Open framework for the IoT • URIs	• Identity management • Semantics • Privacy-awareness	• “Thing DNA” identifier
Internet of Things Architecture Technology	• IoT architectures developments • IoT architecture in the FI • Network of networks architectures • F-O-T platforms interoperability	• Adaptive, context based architectures • Self-* properties	• Cognitive architectures • Experiential architectures
Communication Technology	• Ultra low power chip sets • On chip antennas • Millimetre wave single chips • Ultra low power single chip radios • Ultra low power system on chip	• Wide spectrum and spectrum aware protocols	• Unified protocol over wide spectrum
Network Technology	• Self aware and self organizing networks • Sensor network location transparency • Delay tolerant networks • Storage networks and power networks • Hybrid networking technologies	• Network context awareness	• Network cognition • Self learning, self repairing networks
Software and algorithms	• Large scale, open semantic software modules • Composable algorithms • Next generation IoT-based social software • Next generation IoT-based enterprise applications	• Goal oriented software • Distributed intelligence, problem solving • Things-to-Things collaboration environments	• User oriented software • The invisible IoT • Easy-to-deploy IoT sw • Things-to-Humans collaboration • IoT 4 All

(Continued)

Development	2011–2015	2015–2020	Beyond 2020
Hardware	• Multi protocol, multi standards readers • More sensors and actuators • Secure, low-cost tags (e.g., Silent Tags) • NFC in mobile phones. Sensor integration with NFC	• Smart sensors (bio-chemical) • More sensors and actuators (tiny sensors)	• Nano-technology and new materials
Data and Signal Processing Technology	• Energy, frequency spectrum aware data processing, • Data processing context adaptable	• Context aware data processing and data responses	• Cognitive processing and optimisation
Discovery and Search Engine Technologies	• Distributed registries, search and discovery mechanisms • Semantic discovery of sensors and sensor data	• Automatic route tagging and identification management centres	• Cognitive search engines • Autonomous search engines
Power and Energy Storage Technologies	• Energy harvesting (energy conversion, photovoltaic) • Printed batteries • Long range wireless power	• Energy harvesting (biological, chemical, induction) • Power generation in harsh environments • Energy recycling • Wireless power	• Biodegradable batteries • Nano-power processing unit
Security and Privacy Technologies	• User centric context-aware privacy and privacy policies • Privacy aware data processing • Virtualisation and anonymisation	• Security and privacy profiles selection based on security and privacy needs • Privacy needs automatic evaluation • Context centric security	• Self adaptive security mechanisms and protocols
Material Technology	• SiC, GaN • Silicon • Improved/new semiconductor manufacturing processes/technologies for higher temperature ranges	• Diamond	
Standardisation	• IoT standardisation • M2M standardisation • Interoperability profiles	• Standards for cross interoperability with heterogeneous networks	• Standards for automatic communication protocols

2.8 Internet of Things Research Needs

Research Needs	2011–2015	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	• Beyond EMID	• Multi methods-one ID
IoT Architecture	• Extranet (Extranet of Things) (partner to partner applications, basic interoperability, billions-of-things)	• Internet (Internet of Things) (global scale applications, global interoperability, many trillions of things)	
SOA Software Services for IoT	• Composed IoT services (IoT Services composed of other Services, single domain, single administrative entity)	• Process IoT services (IoT Services implementing whole processes, multi/ cross domain, multi administrative entities, totally heterogeneous service infrastructures)	
Internet of Things Architecture Technology	• Adaptation of symmetric encryption and public key algorithms from active tags into passive tags • Universal authentication of objects • Graceful recovery of tags following power loss • More memory • Less energy consumption • 3-D real time location/position embedded systems • IoT Governance scheme	• Code in tags to be executed in the tag or in trusted readers. • Global applications • Adaptive coverage • Object intelligence • Context awareness	• Intelligent and collaborative functions
Communication Technology	• Long range (higher frequencies — tenth of GHz)	• On chip networks and multi standard RF architectures	• Self configuring, protocol seamless networks

(*Continued*)

Research Needs	2011–2015	2015–2020	Beyond 2020
	• Protocols for interoperability • Protocols that make tags resilient to power interruption and fault induction. • Collision-resistant algorithms	• Plug and play tags • Self repairing tags	
Network Technology	• Grid/Cloud network • Hybrid networks • Ad hoc network formation • Self organising wireless mesh networks • Multi authentication • Sensor RFID-based systems • Networked RFID-based systems — interface with other networks — hybrid systems/networks	• Service based network • Integrated/universal authentication • Brokering of data through market mechanisms	• Need based network • Internet of **Everything** • Robust security based on a combination of ID metrics • Autonomous systems for non stop information technology service
Software and algorithms	• Self management and control • Micro operating systems • Context aware business event generation • Interoperable ontologies of business events • Scalable autonomous software • Software for coordinated emergence • (Enhanced) Probabilistic and non-probabilistic track and trace algorithms, run directly by individual "things." • Software and data distribution systems	• 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	• Paper thin electronic display with RFID • Ultra low power EPROM/FRAM	• Polymer based memory • Molecular sensors	• Biodegradable antennas • Autonomous "bee" type devices

(*Continued*)

Research Needs	2011–2015	2015–2020	Beyond 2020
	• NEMS • Polymer electronics tags • Antennas on chip • Coil on chip • Ultra low power circuits • Electronic paper • Devices capable of tolerating harsh environments (extreme temperature variation, vibration and shocks conditions and contact with different chemical substances) • Nano power processing units • Silent Tags • Biodegradable antennae	• Autonomous circuits. • Transparent displays • Interacting tags • Collaborative tags • Heterogeneous integration • Self powering sensors • Low cost modular devices	
Hardware Systems, Circuits and Architectures	• Multi protocol front ends • Multi standard mobile readers • Extended range of tags and readers • Transmission speed • Distributed control and databases • Multi-band, multi-mode wireless sensor architectures • Smart systems on tags with sensing and actuating capabilities (temperature, pressure, humidity, display, keypads, actuators, etc.) • Ultra low power chip sets to increase operational range (passive tags) and increased energy life (semi passive, active tags). • Ultra low cost chips with security • Collision free air to air protocol	• 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	• Heterogeneous architectures • “Fluid” systems, continuously changing and adapting
Data and Signal Processing Technology	• Common sensor ontologies (cross domain)	• Autonomous computing	• Cognitive computing

(*Continued*)

Research Needs	2011–2015	2015–2020	Beyond 2020
	• Distributed energy efficient data processing	• Tera scale computing	
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	• Printed batteries • Photovoltaic cells • Super capacitors • Energy conversion devices • Grid power generation • Multiple power sources	• Paper based batteries • Wireless power everywhere, anytime. • Power generation for harsh environments	• Biodegradable batteries
Security and Privacy Technologies	• Adaptation of symmetric encryption and public key algorithms from active tags into passive tags • Low cost, secure and high performance identification/authentication devices	• Context based security activation algorithms • Service triggered security • Context-aware devices • Object intelligence	• Cognitive security systems
Material Technology	• Carbon • Conducting Polymers and semiconducting polymers and molecules • Conductive ink • Flexible substrates • Modular manufacturing techniques	• Carbon nanotube	
Standardisation	• Privacy and security cantered standards • Adoption of standards for “intelligent” IoT devices • Language for object interaction	• Dynamic standards • Adoption of standards for interacting devices	• Evolutionary standards • Adoption of standards for personalised devices

Acknowledgments

The IoT European Research Cluster — European Research Cluster on the Internet of Things (IERC) maintains its Strategic Research Agenda (SRA), taking into account its experiences and the results from the ongoing exchange among European and international experts.

The present document builds on the 2009 Strategic Research Agenda and presents the research fields and an updated roadmap on future R&D until 2015 and beyond 2020.

The IoT European Research Cluster SRA is part of a continuous IoT community dialogue initiated by the European Commission (EC) DG INFSO-D4 Unit for the European and international IoT stakeholders. The result is a lively document that is updated every year with expert feedback from ongoing and future projects within the FP7 Framework Program on Research and Development in Europe.

Many colleagues have assisted over the last few years with their views on the Internet of Things strategic research agenda document. Their ***contributions*** are gratefully acknowledged.

Ali Rezafard, IE, Afilias, EPCglobal Data Discovery JRG
Andras Vilmos, HU, Safepay, StoLPaN
Anthony Furness, UK, AIDC Global Ltd & AIM UK, CASAGRAS, RACE networkRFID
Antonio Manzalini, IT, Telecom Italia, CASCADAS
Carlo Maria Medaglia, IT, University of Rome 'Sapienza', IoT-A
Claudio Pastrone, IT, Istituto Superiore Mario Boella, Pervasive Technologies Research Area, ebbits
Daniel Thiemert, UK, University of Reading, HYDRA
David Simplot-Ryl, FR, INRIA/ERCIM, ASPIRE
Dimitris Kiritsis, CH, EPFL, IMS2020
Florent Frederix, EU, EC, EC
Franck Le Gall, FR, Inno, WALTER
Frederic Thiesse, CH, University of St. Gallen, Auto-ID Lab
Harald Vogt, DE, SAP, SToP
Harald Sundmaeker, DE, ATB GmbH, CuteLoop
Humberto Moran, UK, Friendly Technologies, PEARS Feasibility
John Soldatos, GR, Athens Information Technology, ASPIRE

Karel Wouters, BE, K.U. Leuven, PrimeLife
Kostas Kalaboukas, GR, SingularLogic, EURIDICE
Mario Hoffmann, DE, Fraunhofer-Institute SIT, HYDRA
Mark Harrison, UK, University of Cambridge, Auto-ID Lab, BRIDGE, EPC-global Data Discovery JRG
Markus Eisenhauer, DE, Fraunhofer-FIT, HYDRA, ebbits
Maurizio Spirito, IT, Istituto Superiore Mario Boella, Pervasive Technologies Research Area, ebbits
Maurizio Tomasella, UK, University of Cambridge, Auto-ID Lab, SMART, BRIDGE, Auto-ID Lab
Neeli Prasad, DK, CTIF, University of Aalborg, ASPIRE
Paolo Paganelli, IT, Insiel, EURIDICE
Philippe Cousin, FR, easy global market, Walter, Myfire, Mosquito, EU-China IoT
Stephan Haller, CH, SAP, CoBIS
Wang Wenfeng, CN, CESI/MIIT, CASAGRAS
Zsolt Kemeny, HU, Hungarian Academy of Sciences, TraSer

Contributing Projects and Initiatives

ASPIRE, BRIDGE, CASCADAS, CONFIDENCE, CuteLoop, DACAR, ebbits, ETP, 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.

References

[1] Vision and Challenges for Realising the Internet of Things, European Union 2010, ISBN 9789279150883.

[2] Internet 3.0: The Internet of Things. © Analysys Mason Limited 2010.

[3] National Intelligence Council, Disruptive Civil Technologies — Six Technologies with Potential Impacts on US Interests Out to 2025 — Conference Report CR 2008–07, April 2008, Online: www.dni.gov/nic/NIC_home.html.

[4] ITU Internet Reports, The Internet of Things, November 2005.

[5] A Digital Agenda for Europe, COM (2010) 245, Chapter 2.5.3. Industry-led initiatives for open innovation.

[6] Extracting Value From the Massively Connected World of 2015, Online: www.gartner.com/DisplayDocument?id=476440.

[7] What the Internet of Things is NOT, Online: Technicaltoplus.blogspot.com/2010/03/what-internet-of-things-is-not.html.

[8] S. Murugesan, "Harnessing Green IT: Principles and Practices," IEEE IT Professional, pp. 24–33, January–February 2008.

[9] The future of Cloud Computing, Opportunities for European Cloud Computing beyond 2010 Online: cordis.europa.eu/fp7/ict/ssai/events-20100126-cloud-computing_en.html.

[10] Wireless identification and sensing platform, Online: seattle.intel-research.net/wisp/.

[11] ICT 2020_4 Scenario Stories. Hidden Assumptions and Future Challenges. Ministry of Economic Affairs, The Hague, 2010.

[12] G. Kortuem, F. Kawsar, V. Sundramoorthy, and D. Fitton, "Smart objects as building blocks for the internet of things," *IEEE Internet Computing* pp. 30–37, January/February 2010.

[13] Future internet 2020, Visions of an Industry Expert Group, May 2009.

[14] Future Internet Strategic Research Agenda, Version 1.1, January 2010.

[15] White Paper: Smart Networked Objects & Internet of Things, Les Instituts Carnot, V1.1, January 2011.