3

Internet of Things Cognitive Transformation Technology Research Trends and Applications

Ovidiu Vermesan[1], Markus Eisenhauer[2], Harald Sundmaeker[3], Patrick Guillemin[4], Martin Serrano[5], Elias Z. Tragos[5], Javier Valiño[6], Arthur van derWees[7], Alex Gluhak[8] and Roy Bahr[1]

[1]SINTEF, Norway
[2]Fraunhofer FIT, Germany
[3]ATB Institute for Applied Systems Technology Bremen, Germany
[4]ETSI, France
[5]Insight Centre for Data Analytics, NUI Galway, Ireland
[6]Atos, Spain
[7]Arthur's Legal B.V., The Netherlands
[8]Digital Catapult, UK

Abstract

The Internet of Things (IoT) is changing how industrial and consumer markets are developing. Robotic devices, drones and autonomous vehicles, blockchains, augmented and virtual reality, digital assistants and machine learning (artificial intelligence or AI) are the technologies that will provide the next phase of development of IoT applications. The combination of these disciplines makes possible the development of autonomous systems combining robotics and machine learning for designing similar systems. This new hyperconnected world offers many benefits to businesses and consumers, and the processed data produced by hyperconnectivity allows stakeholders in the IoT value network ecosystems to make smarter decisions and provide better customer experience.

3.1 Internet of Things Evolving Vision

IoT technologies and applications are creating fundamental changes in individuals' and society's view of how technologies and businesses work in the world. The IoT has changed the way that connected vehicles work, facilitating the functionalities with automated procedures. The IoT connects vehicle to vehicle, assisting with collision avoidance and vehicle to infrastructure, preventing unscheduled lane departure and automating toll collection. Vehicles are manufactured in a way that facilitates the employment of IoT technologies, with autonomous driving technology and features integrated into the vehicle, e.g. automatic and responsive cruise control based on recognizing and responding to traffic signs and communication with the infrastructure of the city (i.e., traffic lights, buildings, etc.). Maintaining digitally-connected lifestyles is supported by IoT technologies that are improving the physical driving experience, and make it more enjoyable by integrating it with new "mobility as a service" concepts and business models.

Citizen-centric IoT open environments require new technological trends and challenges to be tackled. In this context, future developments are likely to require new businesses, business models and investment opportunities, new IoT architectures and new concepts and tools to be integrated into the design and development of open IoT platforms. This becomes evident in scenarios where IoT infrastructures and services intersect with intelligent buildings that automatically optimize their HVAC and lighting systems for occupancy and reduced energy usage. Other examples include heavy machinery that predicts internal part failure and schedules its own maintenance or robotic and autonomous system technologies that deliver advanced functionality.

IoT is the result of heterogeneous technologies used to sense, collect, act, process, infer, transmit, notify, manage and store data. IoT includes also the combination of advanced sensing/actuating, communication, and local and distributed processing, which takes the original vision of the IoT to a wholly different level, opening up completely new classes of opportunities for IoT with many research challenges to be addressed spanning several research areas.

3.1.1 IoT Common Definition

IoT is transforming the everyday physical objects in the surrounding environment into ecosystems of information that enrich people's lives. IoT is bridging the gap between the physical and the digital or virtual worlds,

facilitating the convergence of advances in miniaturization, wireless connectivity, increased data-storage capacity and batteries. IoT is a set of key enabling technologies for digital businesses and one of the main drivers contributing to transforming the Internet and improving decision-making capacity via its augmented intelligence. People will engage with IoT applications using all their senses: touch and feel, sight, sound, smell and taste, individually or in combination. Success in developing value-added capabilities around IoT requires a broad approach that includes expertise in sensing/actuating, connectivity, edge computing, machine learning, networked systems, human-computer interaction, security and privacy. IoT technologies are deployed in different sectors, from agriculture in rural areas to health and wellness, smart home and Smart-X applications in cities.

The IoT is bridging the gap between the virtual, digital and physical worlds by bringing together people, processes, data and things while generating knowledge through IoT applications and platforms. IoT achieves this addressing security, privacy and trust issues across these dimensions in an era where technology, computing power, connectivity, network capacity and the number and types of smart devices are all expected to increase. In this context, IoT is driving the digital transformation as presented in Figure 3.1.

Smart IoT applications with sensing and actuation embedded in "things" are creating smart environments based on hyperconnectivity; the high density of sensing and actuation coverage allows a qualitative change in the

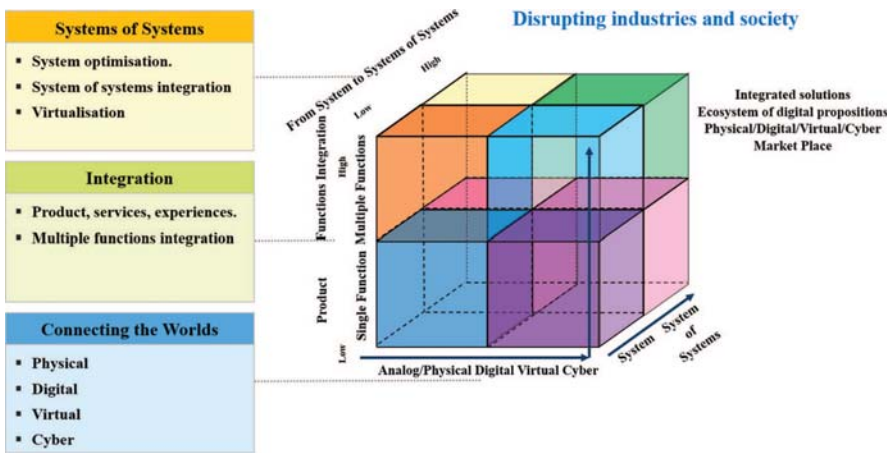

Figure 3.1 The pathway of IoT digital transformation.

way people interact with the intelligent environment cyberspaces, from using appliances at home to caring for patients or elderly persons. The massive deployment of IoT devices creates systems of systems that synergistically interact to form totally new and unpredictable services, providing an unprecedented economic impact that offers multiple opportunities. The potential of the IoT is underexploited; the physical and the intelligent are largely disconnected, requiring a lot of manual effort to find, integrate and use information in a meaningful way. IoT and its advances in intelligent spaces can be categorized with the key technologies at the core of the Internet.

Intelligent spaces are created and enriched by the IoT, in which the traditional distinction between network and device is starting to blur as the functionalities of the two become indistinguishable. With the growing number of IoT deployments, the spectrum of edge devices, short- and long-range radios, infrastructure components from edge computing and cloud storage, as well as networks are increasing in volume, bringing IoT components within reach of a larger pool of potential adopters. In this context, the development of concepts, technologies and solutions to address the perceived security exposure that IoT represents with respect to information technology (IT)/operational technology (OT), is a high priority across several industrial domains, (e.g., manufacturing, automotive, energy, etc.). In Figure 3.2, which will redefine the landscape of business environment.

The IoT as a "global concept" requires a common high-level definition. It has different meanings at different levels of abstraction through the value chain, from lower level semiconductor aspects to service providers. IoT is a paradigm with different visions, and involves multidisciplinary activities.

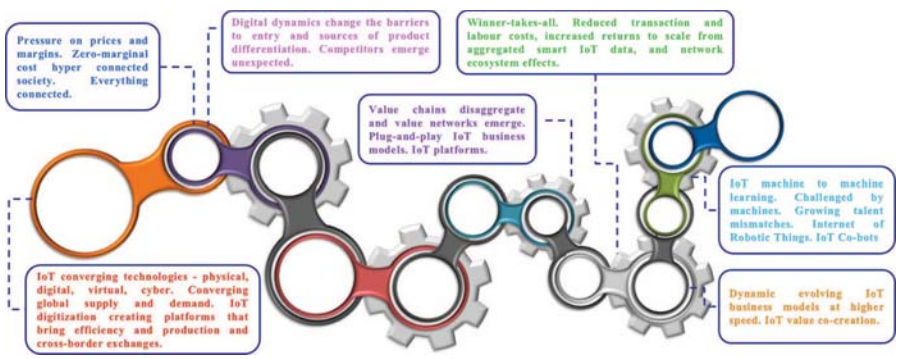

Figure 3.2 The dynamics of IoT digital age.

Considering the wide background and the number of required technologies, from sensing devices, communication subsystems, data aggregation and pre-processing to object instantiation and finally service provision, it is clear that generating an unambiguous definition of the "IoT" 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 formulated the following definition [10]. "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 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 [9] 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."

3.1.2 IoT Cognitive Transformation

IoT technologies are creating the next generation of smart homes/buildings, smart vehicles and smart manufacturing applications by providing intelligent automation, predictive analytics and proactive intervention. Artificial intelligence (AI) or advanced Machine Learning (ML) is integrated into the different components of IoT architecture layers as part of the complex IoT platforms. These components are composed of many technologies and techniques, (e.g., deep learning, neural networks and Natural Language Processing – NLP). These techniques move beyond traditional rule-based algorithms to create autonomous IoT systems that understand, learn, predict, adapt and operate autonomously and give rise to a spectrum of intelligent implementations, including physical devices, (e.g., robots, autonomous vehicles, consumer electronics) as well as applications and services, (e.g., virtual personal assistants, smart advisors). In this context, the IoT implementations deliver a new class of intelligent applications and things and provide embedded intelligence for a wide range of mesh devices, software platforms and service solutions.

In the IoT world, AI will further enhance the capabilities of concepts such as digital twins, where a dynamic software model is formed of a physical thing or system that relies on sensor data to understand its state, respond to changes, improve operations and add value. Digital twins include a combination of metadata, (e.g., classification, composition and structure), condition or state, (e.g., location and temperature), event data, (e.g., time series) and analytics, (e.g., algorithms and rules) and are used by AI algorithms to model, simulate and predict.

The elements behind the IoT "neuromorphic" structure are illustrated in Figure 3.3.

The cognitive transformation of IoT applications allows the use of optimized solutions for individual applications and the integration of immersive technologies, i.e., virtual reality (VR) and augmented reality (AR); concepts that transform the way individuals and robotic things interact with one another and with IoT platform systems. In this context, VR and AR capabilities are merging with the digital mesh to form a seamless system of intelligent devices capable of orchestrating a flow of information that is delivered to the user as hyper-personalized, hyperconnected and to relevant applications and services. Integration across multiple industrial domains and environments extend immersive applications beyond closed-loop experiences to collaborative cyberspaces of heterogeneous interactive devices and humans. Smart spaces (i.e., rooms, manufacturing floors, and mobility areas) become active with things. Their mesh interconnection will appear and work in conjunction with immersive virtual worlds in a collaborative manner. Cognitive IoT technologies allow embedding intelligence into systems and processes, enabling

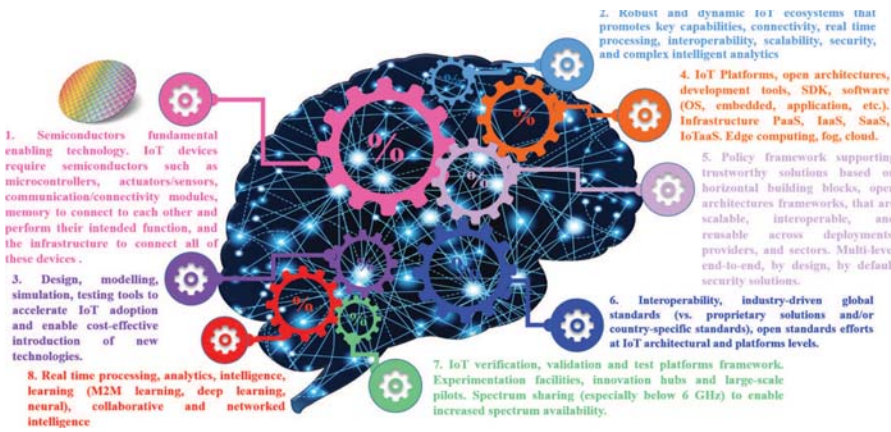

Figure 3.3 IoT "neuromorphic" structure.

the digital mesh to expand the set of endpoints that people and things use to access applications and information or to interact with other people and things. As the device mesh evolves, connection models expand and greater cooperative interaction between devices emerges, creating the foundation for a new continuous and ambient digital experience.

The information exchanged by IoT applications is managed by IoT platforms using cognitive systems with new components addressing the information systems, customer experience, analytics, intelligence and business ecosystems in order to generate new and better services and use cases in the digital business environment.

The cognitive IoT capabilities at the edge integrate the functions of the intelligent digital mesh and related digital technology platforms and application architectures at the cloud level, while increasing the demand for end-to-end security solutions. In addition to the use of established security technologies, it is critical to monitor user and entity behaviour in various IoT scenarios. IoT edge is the new frontier for security solutions creating new vulnerability areas that require new remediation tools and processes that must be embedded into IoT platforms.

The use of artificial intelligence, swarm intelligence and cognitive technologies together with deep learning techniques for optimizing the IoT services provided by IoT applications in smart environments and collaboration spaces, creates new solutions and brings new challenges and opportunities. AI is an increasingly important factor in the development and use of IoT technologies. While focusing on technology it is important to address ethical considerations with respect to deployment and design: ensuring the interpretability of IoT applications and solutions based on AI systems, empowering the consumer, considering responsibility in the deployment of IoT technologies and applications based on AI systems, ensuring accountability and creating a social and economic environment that is formed through the open participation of different stakeholders in the IoT ecosystems.

There are many factors contributing to the challenges faced by stakeholders in the development of IoT technologies based on cognitive capabilities and AI, (i.e., autonomous vehicles, internet of robotic things, digital assistants, etc.), including:

- Decision-making that is based on transparency and “interpretability”. When using IoT technologies based on artificial intelligence for performing tasks ranging from self-driving vehicles to managing parking lots or healthcare journals, there is a need for a robust and clear basis for

the decisions made by an AI agent. Transparency around algorithmic decisions is in many cases limited by technical secrecy or literacy. Machine learning creates further challenges as the internal decision logic of the model is not understandable even for the developers, and even if the learning algorithm is open and transparent, the model it produces may not be. IoT applications involving autonomous systems need to understand why a self-driving vehicle chooses to take specific actions and need to be able to determine liability in the case of an accident.

- The accuracy and quality of the data that are used by the learning algorithm influence the decisions of an IoT application involving autonomous or robotic vehicles. In these safety-critical and mission-critical applications reliable data are crucial and the use and processing of data from reliable sources is an important element in maintaining confidence and trust in the technology.
- Safety and security are critical for IoT technologies integrated with autonomous systems and AI. Cognitive techniques and AI agents are used to learn about and interact with smart environments, and they must detect unpredictable and harmful behaviour, including indifference to the impact of their actions that can be interpreted as a form of "hacking". In this context, the actions of an AI agent may be limited by how it learns from its environment, how the learning is reinforced and how the exploration/exploitation dilemma is addressed. IoT autonomous systems are exposed to malicious actors trying to manipulate the algorithm by using "adversarial learning" mechanisms to influence the training data for abnormal traffic detection, and this demonstrates that safety and security considerations must be taken into account in the debate around transparency of algorithmic decisions.
- Accountability is another factor that must be considered for IoT autonomous systems based on cognitive and AI technologies where things learn on their own, and humans have less control. Machine learning can create situations that bring into question who is accountable: the producer of the individual thing, the service provider, the fleet manager, the developers/programmers, the collaborative network, etc. The advancement of IoT technologies, requires the issue to be addressed, as flaws in algorithms may result in collateral damages, and there is a need for clarification with regard to liability on the part of the manufacturer, operator and programmer. Cognitive and AI techniques introduce another dimension, as the training data, rather than the algorithm itself, could be the problem.

- The social and economic impacts of IoT technologies based on AI and cognitive solutions are reflected in economic changes through increases in productivity, since robotic things are able to perform new tasks, e.g., self-driving vehicles, networked robotic things or smart assistants to support people in their tasks. This will affect the stakeholders involved in various ways, and create different outcomes for labour markets and society as a whole. IoT autonomous systems improve efficiency and generate cheaper products, create new jobs or increase the demand for certain existing ones, while unskilled and low-paying jobs are more likely to disappear. IoT technologies will have an impact on highly-skilled jobs that rely extensively on routine cognitive tasks. IoT autonomous systems challenge the division of labour on a global scale, and companies may choose to automate their operations locally instead of outsourcing. These developments could increase the digital divide and lead to technological distrust.
- Governance of IoT autonomous systems based on AI and cognitive solutions requires new ways of thinking as these technologies are developed across ecosystems that intersect with topics addressed by the Internet, IoT, AI, robotics governance and policy. Privacy and data laws are experiencing a fundamental paradigm shift as processes are running in parallel with regulations that are adopted or interpreted in different ways. Ensuring a coherent approach in the regulatory space is important, to ensure that the benefits of global IoT technologies, including AI, machine learning, robotics, etc., are realized.

From the point of view of market-based approaches to regulation, all stakeholders should engage to manage the IoT technology's economic and social impact. The social impact of autonomous IoT systems based on cognitive and AI techniques cannot possibly be addressed by governing the technology, and requires efforts to govern the impact of the technology in various applications and domains.

3.2 IoT Strategic Research and Innovation Directions

The IERC brings together EU-funded projects with the aim of defining a common vision for IoT technology and addressing European research challenges. The rationale is to leverage the large potential for IoT-based capabilities and promote the use of the results of existing projects to encourage the convergence of ongoing work; ultimately, the endpoints are to tackle the most

important deployment issues, transfer research and knowledge to products and services, and apply these to real IoT applications.

The objectives of IERC are to provide information on research and innovation trends, and to present the state of the art in terms of IoT technology and societal analysis, to apply developments to IoT-funded projects and to market applications and EU policies. The final goal is to test and develop innovative and interoperable IoT solutions in areas of industrial and public interest. The IERC objectives are addressed as an IoT continuum of research, innovation, development, deployment, and adoption.

The IERC launches every year the Strategic Research and Innovation Agenda (SRIA), which is the outcome of discussion involving the projects and stakeholders involved in IERC activities. As such, it brings together the major players of the European landscape to address IoT technology priorities that are essential to the competitiveness of European industry. The SRIA covers the important issues and challenges relating to IoT technology. It provides the vision and roadmap for coordinating and rationalizing current and future research and development efforts in this field, by addressing the different enabling technologies covered by the concept and paradigm of the IoT.

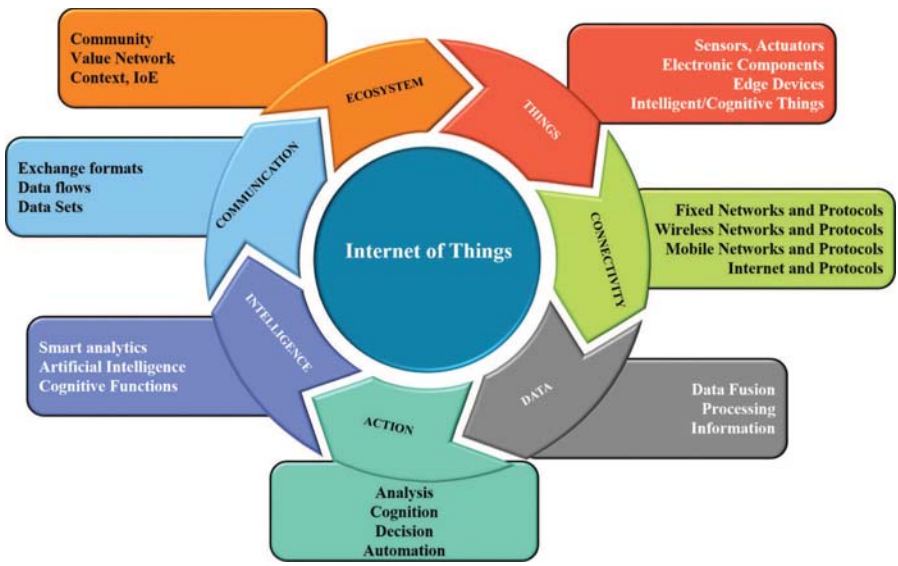

Figure 3.4 IoT components as part of research, innovation, deployment.

Enabled by the activities of the IERC, IoT is bridging physical, digital, virtual, and human spheres through networks, connected processes, and data, and turning them into knowledge and action, so that everything is connected in a large, distributed network. New technological trends bring intelligence and cognition to IoT technologies, protocols, standards, architecture, data acquisition, and analysis, all with a societal, industrial, business, and/or human purpose in mind. The IoT technological trends are presented in the context of integration; hyperconnectivity; digital transformation; and actionable data, information, and knowledge.

IoT developments address highly distributed and hyperconnected IoT applications that use computing platforms, storage, and networking services between edge devices and edge computing and the cloud; these applications drive the growth of new as-a-service business models. Distributed and federated heterogenous IoT platforms at the edge and the cloud as presented in Figure 3.5 require new distributed architectural models to address the future IoT implementations.

The development and deployment of more complex and scalable IoT solutions will result in technological diversification. This will create new challenges for the IoT architecture and open platforms in addressing the complex and cooperative work needed to develop, adopt, and maintain an effective cross-industry technology reference architecture that will allow for true interoperability and ease of deployment. New technological developments in consumers' use of AI-driven IoT opens a new era for IoT; it will be a shift from two-dimensional interfaces for 2D experiences, by using 3D interfaces to generate 3D experiences. In those 3D experiences, things will

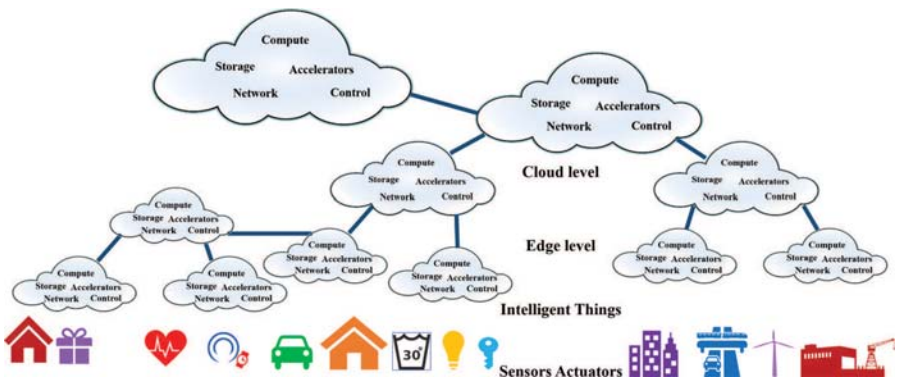

Figure 3.5 Distributed and federated heterogenous IoT platforms at the edge and cloud.

interact with a digital service that takes into account the real-time smart environment and creates a physical result, for example sending a vehicle or robot to a requested location. IoT applications aim to present a single view of data. The convergence of physical, digital, and virtual worlds across multiple channels has created opportunities to measure and influence the product, service and experience beyond traditional value chains, and how stakeholders manage value co-creation.

End-to-end distributed security requires new models and mechanisms to deal with the increased challenges posed by hyperconnectivity. In this context, blockchain technology could be considered the 'missing link' needed to address scalability, privacy, and reliability concerns with respect to IoT technologies and applications. Blockchain technology offers capabilities for tracking a vast number of connected devices; indeed, it can enable coordination and the processing of transactions between devices. The decentralized approach provided by the technology eliminates single points of failure, and thus creates a more resilient device ecosystem. Additionally, the cryptographic algorithms used by blockchain could allow the stronger protection of private consumer data.

The IERC will work to provide a framework that supports the convergence of IoT architecture approaches; it will do so while considering the vertical definition of the architectural layers, end-to-end security, and horizontal interoperability. IoT technology is deployed globally, and supporting the activities of common and unified reference architecture would increase coherence among various IoT platforms. The establishment of a common architectural approach, however, will require a focus on the reference model, specifications, requirements, features, and functionality. These issues will be particularly important in preparing future IoT LSPs, although time schedules might be difficult to synchronize.

The SRIA is developed with the support of a European-led community of interrelated projects and their stakeholders, all of whom are dedicated to the innovation, creation, development, and use of IoT technology.

Since the release of the first version of the SRIA, we have witnessed active research on several IoT topics. On one hand, that research fills several of the gaps originally identified in the SRIA; on the other hand, it creates new challenges and research questions. Recent advances in areas such as cloud computing, cyber-physical systems, robotics, autonomic computing, and social networks have changed even more the scope of convergence in the IoT. The Cluster has the goal of providing an updated document each year that records relevant changes and illustrates emerging challenges.

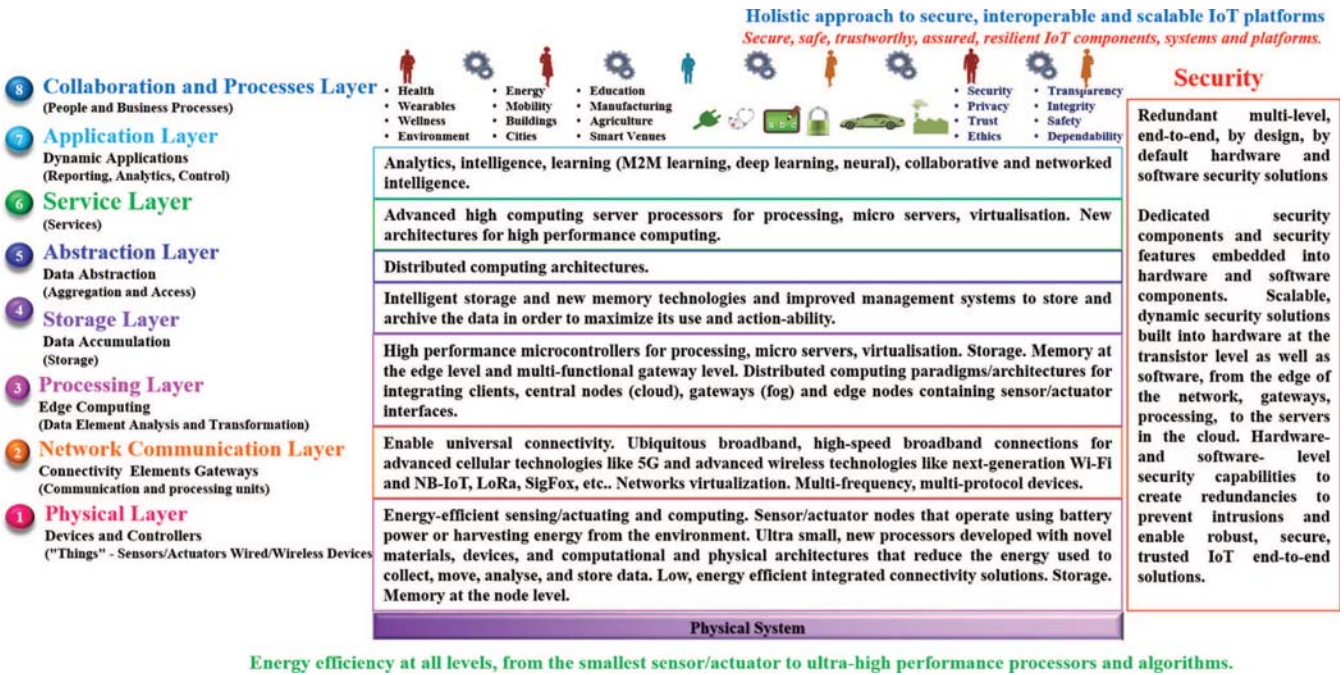

Figure 3.6 IoT Research topics addressed at different IoT architectural layers.

Updated releases of this SRIA build incrementally on previous versions [9, 11, 37] and highlight the main research topics associated with the development of IoT-enabling technologies, infrastructure, and applications [1].

The research activities include the IoT European Platforms Initiative (IoT-EPI) program that includes the research and innovation consortia that are working together to deliver an IoT extended into a web of platforms for connected devices and objects. The platforms support smart environments, businesses, services and persons with dynamic and adaptive configuration capabilities. The goal is to overcome the fragmentation of vertically-oriented closed systems, architectures and application areas and move towards open systems and platforms that support multiple applications. IoT-EPI is funded by the European Commission (EC) with EUR 50 million over three years (2016–2018) [16].

The research and innovation items addressed and discussed in the task forces of the IoT–EPI program, the IERC activity chains, and the AIOTI working groups for the basis of the IERC SRIA address the roadmap of IoT technologies and applications; this is done in line with the major economic and societal challenges underscored by the EU 2020 Digital Agenda [36].

The IoT European Large-Scale Pilots Programme [17] includes the innovation consortia that are collaborating to foster the deployment of IoT solutions in Europe through integration of advanced IoT technologies across the value chain, demonstration of multiple IoT applications at scale and in a usage context, and as close as possible to operational conditions.

The programme projects are targeted and goal driven initiatives that propose IoT approaches to specific real-life industrial/societal challenges. They are autonomous entities that involve stakeholders from supply side to demand side, and contain all the technological and innovation elements, the tasks related to the use, application and deployment as well as the development, testing and integration activities.

The scope of IoT European Large-Scale Pilots Programme is to foster the deployment of IoT solutions in Europe through integration of advanced IoT technologies across the value chain, demonstration of multiple IoT applications at scale and in a usage context, and as close as possible to operational conditions. Specific Pilot considerations include:

- Mapping of pilot architecture approaches with validated IoT reference architectures such as IoT-A enabling interoperability across use cases;
- Contribution to strategic activity groups that were defined during the LSP kick-off meeting to foster coherent implementation of the different LSPs.

- Contribution to clustering their results of horizontal nature (interoperability approach, standards, security and privacy approaches, business validation and sustainability, methodologies, metrics, etc.).

IoT European Large-Scale Pilots Programme includes projects addressing the IoT applications based on European relevance, technology readiness and socio-economic interest in Europe. The IoT Large-Scale Pilots projects overview is illustrated in Figure 3.7. IoT European Large-Scale Pilots Programme is funded by the European Commission (EC) with EUR 100 million over three years (2017–2019) [17].

The IERC SRIA 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 SRIA highlights the main research topics associated with the development of IoT infrastructures and applications, and it offers an outlook towards 2020 [1].

The timeline of the IERC IoT SRIA covers the current decade (with respect to research), as well as the years that follow (with respect to implementing the research results). As the Internet and its current key applications show, it is anticipated that unexpected trends will emerge that will in turn lead to new and unforeseen development paths.

The IERC has involved experts who work in industry, research, and academia, who provide their vision regarding IoT research challenges, enabling technologies, and key applications that are expected to arise from the current vision for the IoT.

The multidisciplinary nature of IoT technologies and applications reflects in the IoT digital holistic view adapted from [34].

Figure 3.7 IoT European large-scale pilots programme.

The IoT is creating new opportunities and providing competitive advantages for businesses in both current and new markets. IoT-enabling technologies have changed the things that are connected to the Internet, especially with the emergence of tactile Internet and mobile moments (i.e. the moments in which a person or an intelligent device pulls out a device to receive context-aware service in real time). Such technology has been integrated into connected devices, which range from home appliances and automobiles to wearables and virtual assistants.

The IERC SRIA addresses these IoT technologies and covers in a logical manner the vision, technological trends, applications, technological enablers, research agendas, timelines, and priorities, and finally summarizes in two tables future technological developments and research needs.

3.2.1 IoT Research Directions and Challenges

The IoT technologies and applications will bring fundamental changes in individuals' and society's views of how technology and business work in the world. A citizen-centric IoT environment requires tackling new technological trends and challenges. This has an important impact on the research activities that need to be accelerated without compromising the thoroughness, rigorous testing and needed time required for commercialisation.

The integration of billions of "things" in the environment and the functions provided by these things (such as sensing/actuating, interacting and cooperating with each other to enable optimal and efficient services) bring tangible benefits to the environment, economy, citizens and society as a whole and new research challenges. IoT devices involved in IoT applications are very diverse and heterogeneous in terms of resource capabilities, mobility, complexity, communication technologies and lifespan. New research is needed in areas like IoT architecture, communication, naming, discovery, programming models, data and network management, power and energy storage and harvesting, security, trust and privacy. Current Internet approaches are not sufficient to solve these issues, and they need to be revised in order to address the complex requirements imposed by the convergence of industrial, business and consumer IoT. This opens the path for the development of intelligent algorithms, novel network paradigms and new services.

Towards using IoT across industrial sectors, a knowledge-centric network, context awareness, the traffic characterisation, monitoring and optimisation, and the modelling and simulation of large-scale IoT scenarios must be addressed for real-life full-scale deployments, testbeds, prototypes and practical systems.

In Europe, a new dynamic and connected engine for research and innovation is needed in the area of IoT in order to maintain Europe's global edge in IoT research and its innovative spirit and generate new jobs and sustainable economic growth. In this context, an overview of IoT research topics for the coming years is presented below.

A hyperconnected society is converging with a consumer-industrial-business Internet that is based on hyperconnected IoT environments. The latter require new IoT systems architectures that are integrated with network architecture (a knowledge-centric network for IoT), a system design and horizontal interoperable platforms that manage things that are digital, automated and connected, functioning in real time, having remote access and being controlled based on Internet-enabled tools.

Research is not disconnected of development. Thus, the IoT research topics should address technologies that bring benefits, value, context and efficient implementation in different use cases and examples across various applications and industries. The value cycle and the areas targeted by the research activities are presented in Figure 3.8.

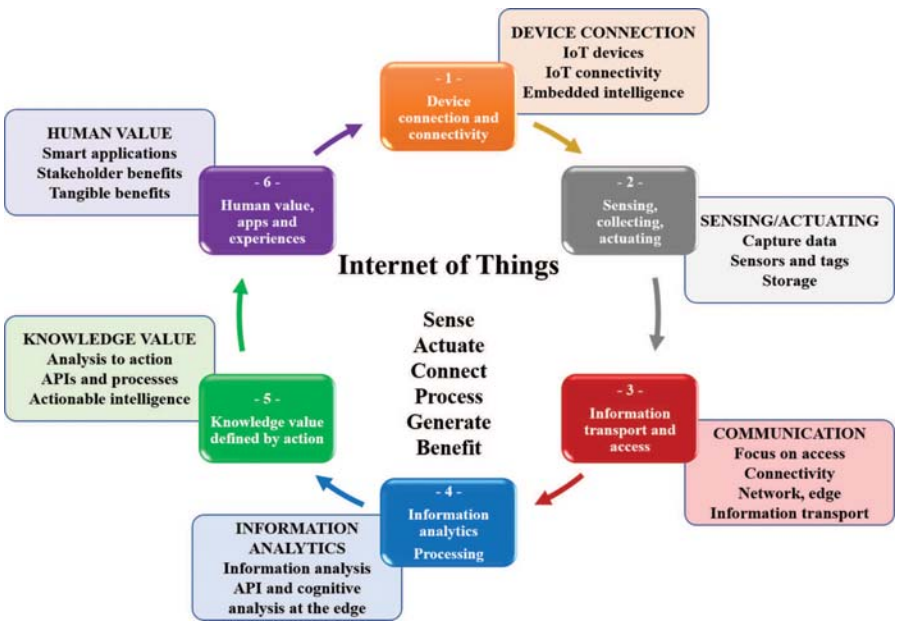

Figure 3.8 IoT value and benefit paradigm.

The shift toward contextual computing, where the intelligent nodes can sense the objective and subjective aspects of a given situation, will augment the ability of edge intelligent "things" to perceive and act in the moment, based on where they are, who they are with, and accumulated experiences. The use of contextual computing in IoT space by combinations of hardware, software, networks, and services that use deep understanding of the intelligent "things" to create costumed, relevant actions that the "things" extend the development of IoT platforms based on new distributed architectures.

The Contextual Internet of Things is the integration of IoT with parallel and opportunistic computing capabilities, neuromorphic and contextual computing (combinations of hardware, software, networks and services) for creating new user experiences and generating tasks on the fly (such as opportunistic IoT applications using data sharing, forming opportunistic networks, on-demand community contextual formation, etc.). Research addressing the context awareness of IoT should include optimal solutions to create and facilitate decentralised opportunistic interactions among humans, IoT networks and the participatory mobile machines. Research should focus on the field of cross-sectorial IoT applications that anticipate human and machine behaviours and human emotions, absorb the social graph, interpret intentions, and provide guidance and support.

The Tactile Internet of Things is based on human-centric sensing/actuating, augmented reality and new IoT network capabilities, including the dynamic mobility of the IoT spatiotemporal systems and data management (personal data, which is consumer-driven, and process data, which is enterprise-driven in a pervasive way). Augmented reality includes 3D visualisation, software robots virtually embedded in things and back-end data systems that enable real-time info and actions. Applications and web browsers are the preferred modes of communication between an IoT device and a smartphone and are challenged by a number of trends and emerging technologies. Messaging platforms for things and developments beyond application program interfaces (APIs) for virtual robots and virtual personal assistants (VPAs) are integrated with things for the post-app era that integrate algorithms at the edge.

The Internet of Mobile Things (IoMT), the Internet of Autonomous Things (IoAT) and the Internet of Robotic Things (IoRT) require research into the area of seamless platform integration, context-based cognitive network integration, new mobile sensor–actuator network paradigms, things identification (addressing and naming in IoT) and dynamic-things discoverability. Research is needed on programmability and communication of multiple heterogeneous mobile, autonomous and robotic things for

cooperation, coordination, configuration, exchange of information, security, safety and protection. In addition, research should focus on IoT heterogeneous parallel processing and communication and dynamic systems based on parallelism and concurrency, as well as dynamic maintainability, self-healing and self-repair of resources, changing the resource state, (re-)configuration and context-based IoT systems for service implementation and integration with IoT network service composition.

IoT dynamic collaborative ecosystems are the extension beyond artificial intelligence, where every mobile thing in an IoT application is able to store and analyse its own usage data and then communicate that data smartly to other connected things and make collaborative decisions. When there is a collective networked artificial intelligence and IoT dynamic collaborative ecosystem, the things have the ability to sense, interpret, control, actuate, communicate and negotiate. Networked collaborative artificial intelligence uses natural-language processing and integrated bots (software robots) to interact with users based on deep-learning pattern recognition (vison, speech, smell, sound, etc.), convolutional neural networks and brain-inspired neuromorphic algorithms for parallel processing and communication. This requires developments in the area of dynamic and mobile machine-to-machine learning (beyond basic machine learning) and real-time coordination among mobile-sensing and actuation platforms for coordinated planning. The integration of IoT operating systems and distributed event-stream processing for real-time data analysis is based on distributed stream-computing platforms.

Research onto IoT swarm-based cognition, intelligence and continuous active learning, could lead to the development of IoT programming models through digitisation and automation of the multitudes of heterogeneous things.

Research is needed on IoT horizontal platform integration for providing edge device control and operations, communications, device monitoring and management, security, firmware updates, IoT data acquisition, transformation and management, IoT application development, event-driven logic, application programming, visualisation, analytics and adapters to connect to enterprise systems. Research should also focus on IoT virtual space, mapping and mobility prediction, and virtual deployment for optimising the kinds of mobile things with sensing/actuating capabilities to install, which protocols to use, which types of IoT platforms can send messages directly to each other and which messages need to be routed through gateways or other IoT platforms. Research is also needed on dynamic sensor–actuator fusion and virtual sensing/actuating.

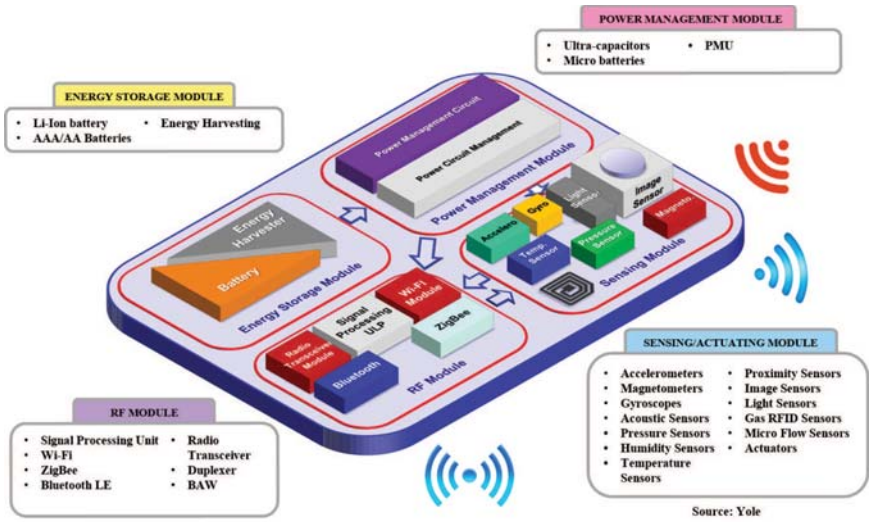

Figure 3.9 IoT sensors/actuators map [12].

Research in the area of sensors/actuators and electronic components that need to integrate multiple function as presented in Figure 3.9.

IoT devices require integrated electronic component solutions that contain sensors/actuators, processing and communication capabilities. These IoT devices make sensing ubiquitous at a very low cost, resulting in extremely strong price pressure on electronic component manufacturers. The research and development in the area of electronic components covers the IoT layered architecture as presented in Figure 3.10.

Additionally, IoT lacks solutions for dynamic context, traffic characterisation- and location-based data processing, storage, processing, virtualisation and visualisation for mobile-edge computing, analytics at the edge (device and gateway level) considering optimal data capture, communication, storage and representation. Moreover, additional work needs to be done in the area of mobile edge-distributed micro IoT clouds based on mobility patterns where data is sent from the same mobile thing to multiple micro IoT clouds. The data needs to be kept synchronised for the purpose of later retrieval and analysis. Research also should focus on how this representation can be extended to data sent from multiple related mobile things.

A context-based end-to-end security framework for heterogeneous devices should be explored for various environments (e.g., operational and information technology security convergence) and applications. For example,

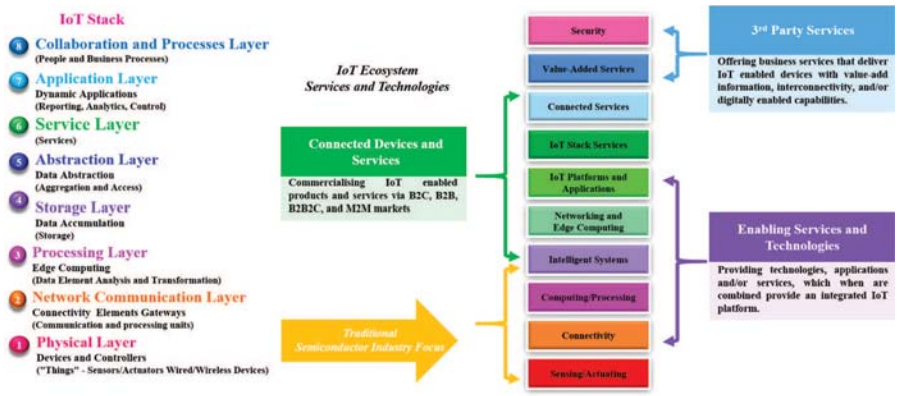

Figure 3.10 IoT electronic devices across the architecture layers.

there is a need for protecting IoT devices and platforms from information cyberattacks and physical tampering by encrypting the communications, as well as addressing new challenges, such as impersonating "things" or denial-of-sleep attacks for batteries. The security framework should be built on real-time business processes and include methods for protecting personal safety and privacy. New artificial intelligence IoT algorithms could be combined with machine-to-machine learning and swarm intelligence to provide new platforms that can identify cyberattacks. Blockchain technology offers capabilities for tracking a vast number of connected devices. It can enable coordination and processing of transactions between devices. The decentralized approach provided by the technology eliminates single points of failure, and thus creates a more resilient device ecosystem.

Data protection in a future IoT landscape with millions of devices continuously monitoring the everyday lives of people is quite challenging. Various attempts have been performed for creating IoT architectures under the concept of privacy by design [30], but still research should be done on creating strong privacy enhancing techniques at the edge, enabling users to have full control over their data in a dynamic way. Research in this area has also to follow the new regulation for data protection of the EU [29].

Heterogeneous networks that combine diverse technical features and low operational cost for various IoT applications should be examined. They can be a mix of short and wide-area networks, offering combined coverage with both high and low bandwidth, achieving good battery life, utilizing lightweight hardware, requiring low operating cost, having high-connection density. When applications request it, the heterogeneous networks should be

able to offer high bandwidth, low-latency, high-data rates and a large volume of data, especially in critical applications.

Standardisation and solutions are needed for designing products to support multiple IoT standards or ecosystems and research on new standards and related APIs.

Summarizing, although huge efforts have been made within the IERC community for the design and development of IoT technologies, the always changing IoT landscape and the introduction of new requirements and technologies creates new challenges or raises the need to revisit existing well-acknowledged solutions. Thus, below we list the main open research challenges for the future of IoT:

- IoT architectures considering the requirements of distributed intelligence at the edge, cognition, artificial intelligence, context awareness, tactile applications, heterogeneous devices, end-to-end security, privacy and reliability.
- IoT systems architectures integrated with network architecture forming a knowledge-centric network for IoT.
- Intelligence and context awareness at the IoT edge, using advanced distributed predictive analytics.
- IoT applications that anticipate human and machine behaviours for social support.
- Tactile Internet of Things applications and supportive technologies.
- Augmented reality and virtual reality IoT applications.
- Autonomics in IoT towards the Internet of Autonomous Things.
- Inclusion of robotics in the IoT towards the Internet of Robotic Things.
- Artificial intelligence and machine learning mechanisms for automating IoT processes.
- Distributed IoT systems using securely interconnected and synchronized mobile edge IoT clouds.
- Stronger distributed and end-to-end holistic security solutions for IoT, addressing also key aspects of remotely controlling IoT devices for launching DDoS attacks.
- Stronger privacy solutions, considering the new General Data Protection Regulation (GDPR) [29] for protecting the users' personal data from unauthorized access, employing protective measures (such as PETs) as closer to the user as possible.
- Cross-layer optimization of networking, analytics, security, communication and intelligence.

- IoT-specific heterogeneous networking technologies that consider the diverse requirements of IoT applications, mobile IoT devices, delay tolerant networks, energy consumption, bidirectional communication interfaces that dynamically change characteristics to adapt to application needs, dynamic spectrum access for wireless devices, and multi-radio IoT devices.
- Adaptation of software defined radio and software defined networking technologies in the IoT.

3.3 IoT Smart Environments and Applications

The IoT applications are addressing the societal needs. However, 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.

IoT technologies and applications are driving digital transformation through gathering massive amount of data, rapid deployment of decisions, predictive maintenance and advanced diagnostics, AI and robotic things used in different applications and domains. The IoT applications are expanding from addressing one industrial sector to develop solutions across sectors. Figure 3.11 illustrate the connections between various domains with stronger links when developers are likely to target more verticals.

3.3.1 IoT Use Cases and Applications

As part of the IERC vision, "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" [9].

There has been a swift acceleration in the evolution of connected devices, in terms of both scale and scope, and a greater focus on interoperability. Hyperconnectivity is supported by rapid developments in various communication technologies, including Wi-Fi, Bluetooth, low-power Wi-Fi, Wi-Max, Ethernet, long-term evolution (LTE), and Li-Fi (using light as a medium of communication between the different parts of a typical network including sensors). The hyperconnected and wireless 5G future, which will feature billions of interconnected wireless devices, will require new ways of sharing the spectrum dynamically, using dynamic spectrum access solutions (DSA)

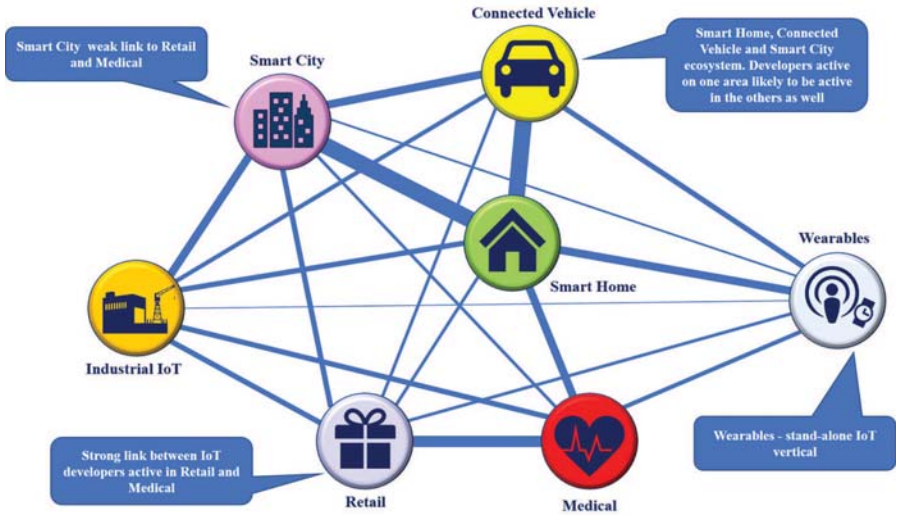

Figure 3.11 IoT connecting people, cities, vehicles, industrial IoT, retail, medical, homes. *Source:* VisionMobile 2015.

for low-band, mid-band, and high-band spectrums that will be available for various IoT applications and requirements.

Wireless dedicated IoT communication technologies-such as 3GPP's narrowband NB-IoT, LoRaWAN, or Sigfox-have been deployed in various IoT applications. In this context, standardization and interoperability are critical, as developers, end users, and business decision-makers need to consider more than 36 wireless connectivity solutions and protocols for their applications as presented in Figure 3.12.

The digital economy is based on three pillars: supporting infrastructure (e.g. hardware, software, telecoms, networks), e-business (i.e. processes that an organization conducts over computer-mediated networks) and e-commerce (i.e. the transfer of goods online) [20]. In this new digital environment, IoT software is distributed across cloud services, edge devices, and gateways. New IoT solutions are built on microservices (i.e. application-built modular services, with each component supporting a specific business goal and using a defined interface to communicate with other modules) and containers (i.e. lightweight virtualization) that are deployed and work across this distributed architecture. Machine learning, edge computing, and cloud services, together with AI algorithms, will be used in conjunction with data collected from IoT edge devices.

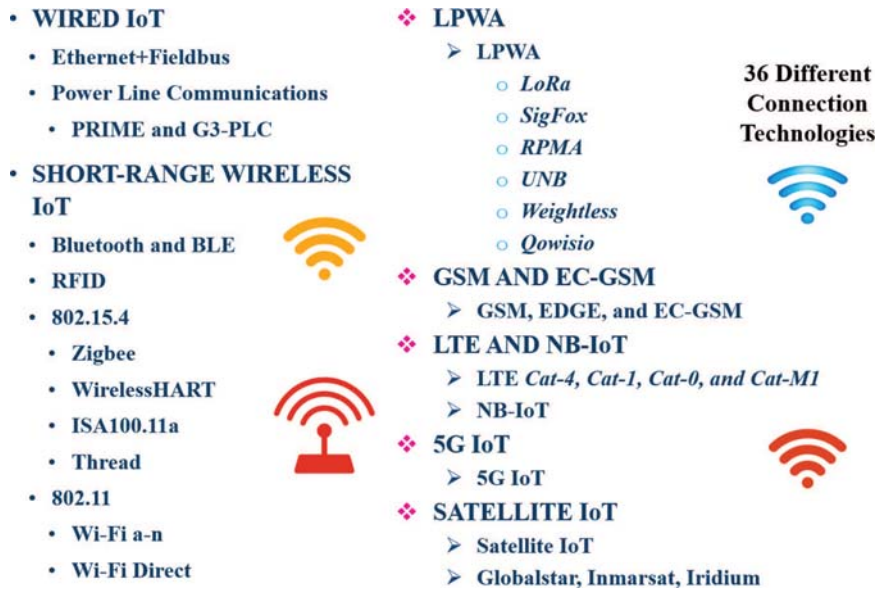

Figure 3.12 IoT Communication technologies.

3.3.2 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. The IoT device producers consider that the wearable devices are one of the exciting new markets expected to see the biggest growth over the next few years. The diversity of wearable devices means that the producers will employ 3G or 4G connectivity alongside Wi-Fi to be used for high-speed local connectivity. The drive for low power, leads to many devices being designed for the application accessories. These devices connect via Bluetooth^{TM} LE (Low Energy) or BT (Bluetooth) Smart to a smartphone or tablet to employ its user interface or display, or to process and send data to the Internet and the cloud, linking to services and being part of an IoT application. Wearable technology is enabled by low-power microcontrollers or application processors, low-power wireless chips and sensors, such as MEMS (Micro-Electro-Mechanical Systems) based motion devices and other environmental sensors. Next-generation devices see these devices further miniaturized in highly integrated solutions with ever-smaller batteries to

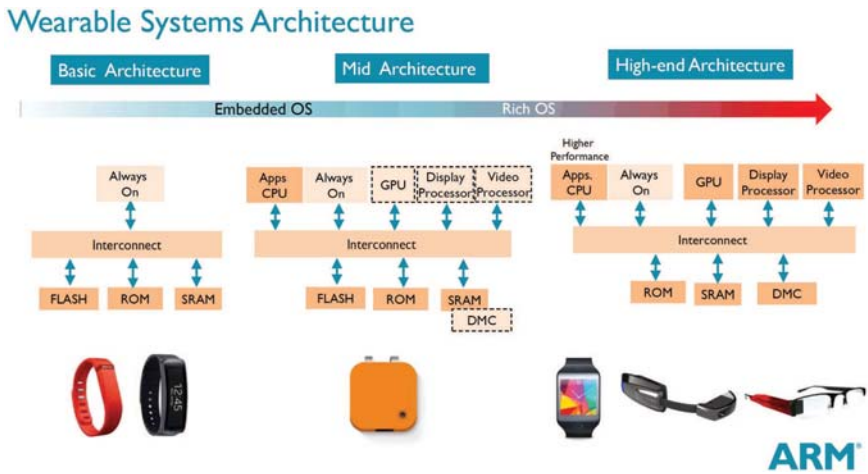

Figure 3.13 Wearables system architecture.

deliver increased functionality in ever-smaller form factors, while high-end products offer increasingly advanced displays and graphics capabilities. In this context, a typical wearables system architecture proposed by companies such as ARM [21] is presented in Figure 3.13.

The global wearable electronics market can be segmented in 5 categories as presented in Figure 3.14 [12]:

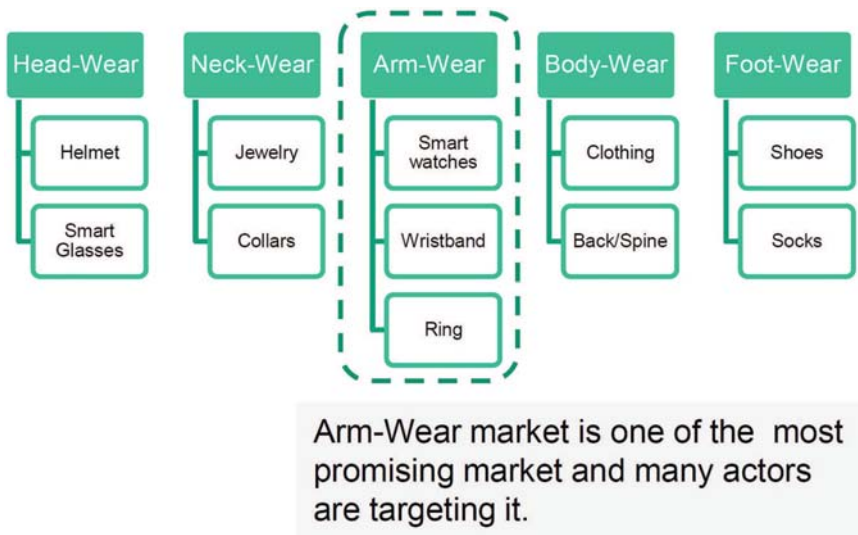

Figure 3.14 Wearable electronic market segmentation [12].

Head-Wear category includes helmet product and vision aid. There's also a category of products for neck-wear, with collars and necklace products that cover up electronics with jewels. Arm-Wear category is the most burgeoning category with multiples devices expected wristband, smartwatches, ring, arm band, etc. Body-Wear products include smart clothing, and devices monitoring back/spine position. The last category concerns foot-wear [12].

CCS Insight expects the wearables market to reach $14 billion by the end of this year and BI Intelligence, Business Insider's research service, expects the wearables market to grow to 162.9 million units by the end of 2020. The healthcare sector is among the top catalysts to push the wearables markets and consumer and professional healthcare trends spur interest in wearable devices. Fitness trackers, are the leading consumer case for wearables as the consumers use wearable devices to record their exercise and health statistics and progress. Hospitals, med-tech companies, pharmaceutical companies, and insurance companies have started to recommend and utilize these devices. One of the major barriers to widespread adoption is accuracy and the manufacturers must ensure that these devices transmit correct data and the users receive accurate progress reports. Privacy concerns are discussed and are not consider as a barrier by early adopters.

Smartwatches offers as well features as fitness bands that could reduce the demand for fitness trackers in the future. The market for wearable computing is expected to grow six-fold, from 46 million units in 2014 to 285 million units in 2018 [35].

The 2016 Gartner Personal Technologies Study surveyed 9,592 online respondents from Australia, the U.S. and the U.K. between June and August 2016, to gain a better understanding of consumers' attitudes toward wearables, particularly their buying behavior for smartwatches, fitness trackers and virtual reality (VR) glasses. According to the survey, smartwatch adoption is still in the early adopter stage (10 percent), while fitness trackers have reached early mainstream (19 percent). Only 8 percent of consumers have used VR glasses/head-mounted displays (excluding cardboard types). The survey found that people typically purchase smartwatches and fitness trackers for their own use, with 34 percent of fitness trackers and 26 percent of smartwatches given as gifts [19].

The innovations are pushing wearable tech into IoT applications for health care, education, smart cities, smart vehicles. The preferred location for wearables has attracted a lot of focus and preferences are shown in Figure 3.15.

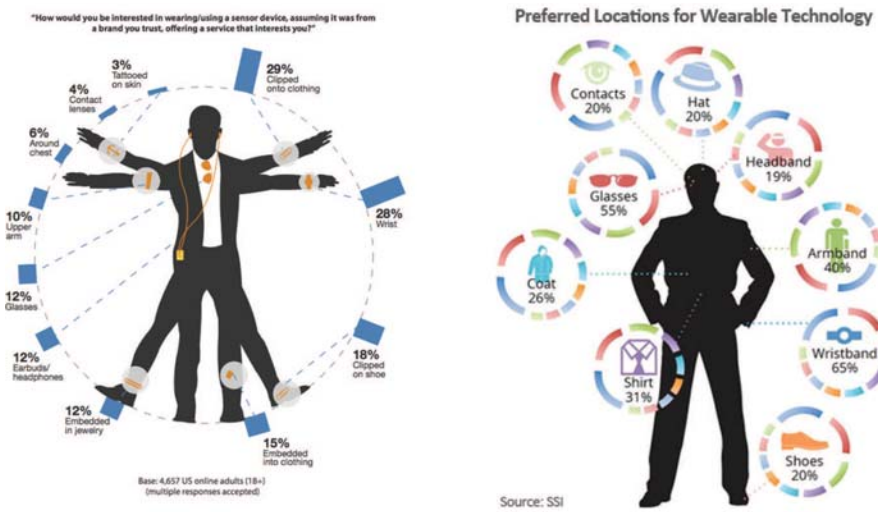

Figure 3.15 Preferred locations for wearable technology.

Source: Google.

The smartwatches will incorporate more sensors, increase functionality and become more autonomous, and they will be untethered from the phone, eschewing Bluetooth connections. The smartwatches will include on board LTE coverage, that allows to call and send texts and connect autonomously to other devices use the device to make payments by swiping the smartwatch at the payment terminal. More computational and communication capabilities more sensors incorporated into smart devices and the smartwatch can act as a hub for other sensors, aggregate and integrate the data from various sensors.

The IoT applications will benefit from the development of wearable technology with integration of virtual and augmented reality features. The virtual information is interfaced to the users using the wearable technology creating ambient AI assistant for coordination and communication and the users will interact with tens different applications to control everything from smart shoes to smart toothbrushes to lightbulbs.

Smart clothing and accessories are integrating seamlessly wearable devices embedded in rings, pendants, sports bras, shoes or clothes including LEDs and colour-changing fabrics. Smart clothing will include many features and different smart solutions are expected on the market in the next years [32, 33]:

- Smart shirt with app, keeping information in 3D showing if too much pressure is put on a certain part of the body, keeping track of your performance, giving information to prevent getting injured while training, with real time feedback
- Health related smart shirt measuring heart rate, breathing rate, sleep monitoring, workout intensity measurements
- Bio sensing silver fibers woven into the shirt
- Clothing to track the number of calories burned
- Clothing to track movement intensity during workout
- Compression fabric that aids in blood circulation and with muscle recovery
- Body monitor sensors – embedded micro sensors throughout the shirt keeping track of temperature, heart beat and heart rate, and the speed and intensity of your workouts
- Shirt able to keep the measured biometrics information by using a small black box woven into the shirt
- Clothing with moisture control and odor control
- Smart shirts can be used in hospitals for monitoring heart beat and breathing in patients
- Baby monitoring – baby garment telling if the baby is sleeping and monitoring the baby's vital signs
- Baby outfit with sensors and a small monitor on it
- Smart socks for baby, monitoring the baby's breath with alert features
- Eco-friendly solar garments as it harnesses the energy of the sun and enables the wearer to charge the owner's phone, music players, and other powered electronic devices
- Adaptive survival clothing that uses moisture and temperature regulation properties of wool to adapt the human body to normal, non-threatening conditions.

The wearable market drivers today are health and fitness smart clothing is used to relay information about fitness and health back to the users. The wearables work well for fitness fans but they still need to reach the everyday consumers since over time, fewer consumers use their wearables daily, which show that the technology isn't becoming habitual or part of the daily routines. In this context, the integration with the IoT digital ecosystem of other products and services is the future trend.

3.3.3 Smart Health, Wellness and Ageing Well

Today, health care stands in a paradigm shift, and new digital solutions require changes in work processes to enable health professionals to spend more time on direct patient contact and treatment. Healthcare and wellness offer unique opportunities for comprehensive IoT implementation. Health care treatments, cost, and availability affect the society and the citizens striving for longer, healthier lives. IoT is an enabler to achieve improved care for patients and providers. It could drive better asset utilization, new revenues, and reduced costs. In addition, it has the potential to change how health care is delivered.

The emergence of Internet of Health (IoH) applications dedicated to citizens health and wellness that spans care, monitoring, diagnostics, medication administration, fitness, etc. will allow the citizens to be more involved with their healthcare. The end-users could access medical records, track the vitals signals with wearable devices, get diagnostic lab tests conducted at home or at the office building, and monitor the health-related habits with Web-based applications on smart mobile devices. Smart Home and welfare technology will merge in integrated services for the benefit of both residents and the municipality. The solutions need to be tailored according to individual needs and evolve as care needs increase. Health information should in future accompany the patient throughout life. IoT systems should be based on patients "and services" needs while confidentiality and privacy are protected. Both the current and future needs for quality-assured information sharing across service levels and business boundaries in the health and care sector, and with other government agencies must implement the new systems.

The IoT technologies offer different solutions for healthcare applications starting from traditional one to wearables and "gadgets" that still need to be develop and tested as listed below:

- Teeth. Toothbrushes that will measure fluoride, remember cavities and discoloration, and notify you of bad breath.
- Eyes. Glasses that will monitor your eyesight and advise correction.
- Hair. Combs that will screen the follicles, report on dandruff density, scan for fungus or lice, and count the hairs (hair loss).
- Bottom. Toilets that will test excrements, both liquid and solid.
- Chest. Airport scanners that will broadcast their results to your phone.
- Body. Clothes that will be intelligent because the fibres will compute, and that will visualize your body language.
- Underbelly. A new field of under wearables that will integrate markers for early detection of cancers or other anomalies.

- Forearms. Shirts that will screen the microbiome on your forearms (40x more than our own cells).
- Neck. Collars that will chemically analyse your sweat.
- Ear. Earphones that will measure your hearing and analyse the emotional level of people you are listening to (sound analysis already allows that!), interesting for total communication (i.e. beyond words and including body language).
- Heart. Pacemakers and stents that will broadcast data to the cardiologist plus ECG
- Nose. Tissues that will examine snot and mucus when you blow your nose.
- Chin. Razors that will plot the surface of the skin looking for acne.
- Lips. Balm that will scan for cold sores.
- Tongue. Tongue scrapers that will screen salivary microbes (the oral microbiome).
- Back. Chairs that will plot your posture and broadcast data for your spine.
- Nails. Nail cutters that will determine the quality of your nails and count the ridges.
- Feet. Step counters.
- Pulse. Heart rate monitors.
- Brain. Headsets that will measure electrical activity in the form of alpha, beta, delta and theta waves.

The World Health Organization (WHO) defines e-Health as: "E-health is the transfer of health resources and health care by electronic means. It encompasses three main areas: The delivery of health information, for health professionals and health consumers, through the Internet and telecommunications; Using the power of IT and e-commerce to improve public health services, e.g. through the education and training of health workers, the use of e-commerce and e-business practices in health systems management. E-health provides a new method for using health resources – such as information, money, and medicines – and in time should help to improve efficient use of these resources. The Internet also provides a new medium for information dissemination, and for interaction and collaboration among institutions, health professionals, health providers and the public."

IoT applications have a market potential for electronic health services and connected telecommunication industry with the possibility of building ecosystems in different application areas.

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 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. IoT technology allows that a variety of functions are controlled with various sensor, hardware, communication, cloud and analytics and integrated, with the living environments allow people with a range of needs to retain their independence. The IoT technology not only overcomes the inconvenience of distance, but also provides people with greater choice and control over the time and the place for monitoring their condition, increasing convenience and making their conditions more manageable. At the same time, it also reduces some of the pressures on clinics and acute hospitals. IoT could make a significant contribution to the management of several chronic conditions, heart failure, hypertension, asthma, diabetes and can be integrated with other living environments domains such as mobility, home/buildings, energy, lighting, cities.

In this context, the IoT applications need to be included into an integrated IoT framework for active and healthy living and sustainable healthcare as presented in Figure 3.16. This need to be implemented using an IoT architecture model for convergence between social and health services, supporting older people and those with long term conditions to live independently and lead fulfilling lives with the national healthcare architecture.

The IoT distributed architecture is built in a modular manner, designed to logically isolate safety critical and non-safety critical systems elements, provide standard open integration points to collaborating systems components, and to take advantage of the principles of service oriented approaches to systems design. Real time and batched event and health metric data are acquired by highly available, resilient and performant modules. The data provided by these modules is then exposed by a series of web services which provide means by which local and remote staff and systems can manage

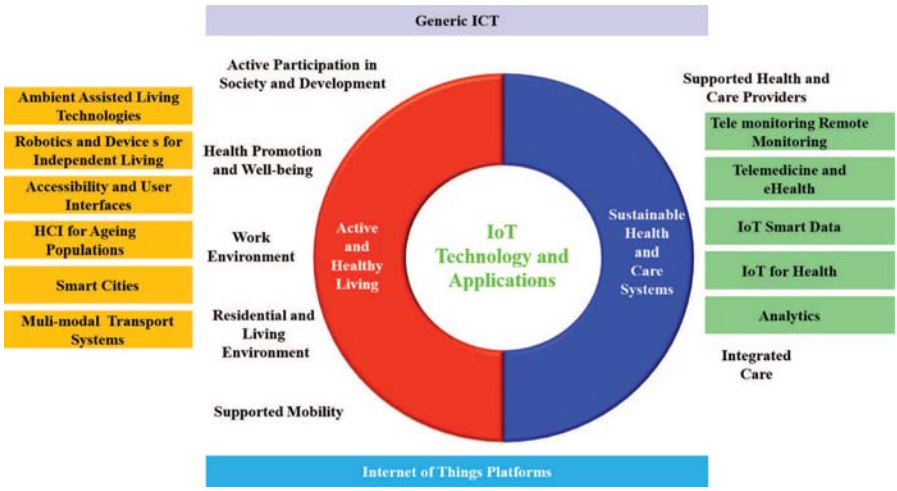

Figure 3.16 Integrated IoT framework for active and healthy living and sustainable healthcare.

the tele monitoring service more effectively. New applications will allow individual user roles to more efficiently deliver tele monitoring services via a single interface. Both applications and services operate in concert on an integrated IoT platform providing data and business logic integration including the services and workflow.

Demographic change, the rising incidence of chronic disease and unmet demand for more personalised care are trends requiring a new, integrated approach to health and social care. Such integration – if brought about in the right manner – has the potential to improve both the quality and the efficiency of care service delivery. Potentially this can be to the benefit of all: beginning with older people in need of care and their family and friends, and including care professionals, service provider organisations, payers and other governance bodies.

There is a need for fundamental shift in the way we think about older people, from dependency and deficit towards independence and well-being. Older people value having choice and control over how they live their lives and interdependence is a central component of older people's well-being. They require comfortable, secure homes, safe neighbourhoods, friendships and opportunities for learning and leisure, the ability to get out and about, an adequate income, good, relevant information and the ability to keep active and healthy. They want to be involved in making decisions about the questions

that affect their lives and the communities in which they live. They also want services to be delivered not as isolated elements, but as joined- up provision, which recognises the collective impact of public services on their lives. Public services have a critical role to play in responding to the agenda for older people.

Within this ongoing change process, advanced IoT technologies provide a major opportunity to realise care integration. At the same time, telecare, telehealth and other IoT applications in this field also remain locked up in segregated silos, reflecting the overall situation. Providing effective and appropriate healthcare to elderly and disable people home is a priority and the use of seamless information and IoT technology at home, in public places, in transport, energy and cities can enable healthcare management to mitigate the future challenges. The use of IoT technologies integrated with other sectors could provide complete and intelligent health management services to elderly home, which provides sustainable healthcare service for elderly people. These new solutions make both the elderly life easier and the healthcare process more effective.

Challenges are the integration of software and hardware to give improved performance of the IoT gateway, provided through various IoT platforms, an enhanced data and network security including down the edge device management for software updates and configuration changes. Successful IoT solutions for elderly people must address:

- Ease-of-use considering that many elderly people aren't comfortable with technology or face issues such as diminished vision or arthritis.
- Non-stigmatizing, "invisible" that cannot be visible and used to further identify and isolate elderly people.
- Privacy and security in order to avoid elderly people to be targets of scams and actions to exploit them or becoming more vulnerable, considering their health situation and health conditions.
- Affordability of IoT technology with devices that are low cost and reliable and can be covered on a fixed income.
- Technology that encourage mutual support and motivators.
- Support and foster independence combing wearables, smart mobility, smart home, smart city applications that help elderly people manage their daily lives to increase the chance they could stay in their homes and move in the city independently for longer, an important factor in both reducing hospitalization costs and fostering self-worth.

3.3.4 Smart Buildings and Architecture

Buildings consume 33% of world energy, this figure grows to 53% of world electricity, and it will continue to grow in the future. As a result, buildings have an important weight in regards to the energy challenge. Today, most commercial buildings are having basic infrastructure to its purpose or costs and many building managers lack basic visibility into the infrastructure they are responsible for.

The current lack of dispatchablility is the fundamental disconnect between the current state in which buildings are passive, "sleeping" untapped assets for operators and building owners, and the future state, in which buildings could act as distributed energy assets, functioning as "shock absorbers" for the grid, opening up new value streams for owners and operators, and, in general, playing an essential role in enabling a more efficient, green, and secure energy system. The current system does not exchange energy data information between assets in buildings and between buildings and the grid. It is comprised of legacy distribution management systems (DMS) that make up the backbone of the utility's grid control and optimization systems, installed distributed energy resources (DER), including PV, fuel cells, and combined heat and power systems, and the ultimate customer-side loads (i.e., the buildings and their equipment, appliances, and devices that ultimately "consume" the energy) [25].

Improving life of the occupants implies many aspects including comfort with light, temperature, air quality, having access to services facilitating life inside the building, adapting the behaviour to the needs of the occupants. There is also a direct economic interest to do it as it is recognized that productivity level is connected to the comfort level.

In this context, IoT is already having a significant impact on the commercial real estate (CRE) industry, helping companies move beyond a focus on cost reduction. IoT applications aim to grow margins and enable features such as dramatically more efficient building operations, enhanced tenant relationships, and new revenue generation opportunities [23].

The different ingredients of IoT, connectivity, control, cloud computing, data analytics, can all contribute to make smarter buildings (offices, industrial, residential, tertiary, hotels, hospitals, etc.):

- Connected to the grid ("smart grid ready")
- Connected to the smart city
- Energy efficient while taking care of the comfort of the occupants
- Adaptable to the changing needs of the occupants over time

Figure 3.17 Smart building implementation [22].

- Providing services for a better life of the occupants
- Easy to maintain during the whole life cycle at minimal cost

The solutions focus primarily on environmental monitoring, energy management, assisted living, comfort, and convenience. Utilizing the IoT platforms in the houses and buildings, heterogeneous equipment empowers the automation of regular activities. Through transforming things into appliances' data which are thoroughly linked by applying the Internet can implement services through web interfaces. 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 uses of the IoT connected with automate building maintenance activities, primarily aiming to realize the benefits of low-hanging fruit such as cost savings and operational efficiency through improved energy management

and reduced personnel costs. The approaches are focusing on developing connected Building Management Systems (BMS) that are progressively more connected and integrated. Different approaches to develop connected BMS are presented in [23] and are categorised as:

- Individual BMS: CRE owners install BMS on a piecemeal basis to automate individual tasks such as elevator or lighting control;5 not surprisingly, owners then must collect and aggregate data from various places.
- Partially integrated BMS: CRE companies are using partially integrated BMS, combining automation of a few activities with a common focus, such as energy management systems. Compared with individual BMS, these systems are more integrated, require less manual intervention, and enable faster decision making. More importantly, CRE owners use these systems to enhance tenant and end-client experience through sustainability initiatives (including to support LEED and other green building certification standards), open Wi-Fi access, and so forth.
- Fully integrated, IoT-enabled BMS: IoT-enabled systems fully integrated BMS, allowing higher-order cost, productivity, and revenue benefits with a deep customer and data focus. It can leverage one infrastructure to operate all building management solutions and require minimal to no manual involvement. Internet protocol or IP-enabled devices can facilitate intelligent decision making by automating point decisions and enhancing strategic insights; this allows data to automatically flow all the way around the Information Value Loop without manual interaction, enabling quick action on the data and creating new value for CRE companies.

In order to improve the technology integration and interoperability the following approaches should be considered [23]:

- Develop advanced mobile computing capabilities: CRE companies will likely benefit from developing a flexible mobile application platform that can integrate new IoT information tracking and capture requirements.
- Use appropriate integration software and platforms: Owners of existing buildings can consider buying specialist software solutions that integrate siloed and disparate building systems and improve interoperability. Likewise, owners of new buildings should consider adopting the latest integrated IoT platforms.
- Use common standards and protocols: Gradual consolidation of different BMS protocols will help develop benchmarks that facilitate full use of

IoT technology. OASIS Open Building Information Exchange is one global industry-wide effort aiming to define standard web protocols for communication between various BMS. Ultimately, players must agree on benchmarks to increase interoperability even among systems used by different industries.

The Internet of Building (IoB) and Building Internet of Things (BIoT) concepts integrates the information from multiple intelligent building management systems and optimise the behaviour of individual buildings as part of a larger information system. The value in IoB is as much in the edge devices and the data collected, exchanged and processed. Collecting, exchanging and processing data from building services and equipment provides a granular view of how each building is performing, allowing the development of building systems that collect, store and analyse data at the edge and in the cloud, providing better operational efficiency and integration with IoT platforms and applications across various sectors.

The implementation of the IoB concept in residential building environments require to integrate the IoT gateway architecture into a flexible data platform that is able to run parallel metering and non-metering applications

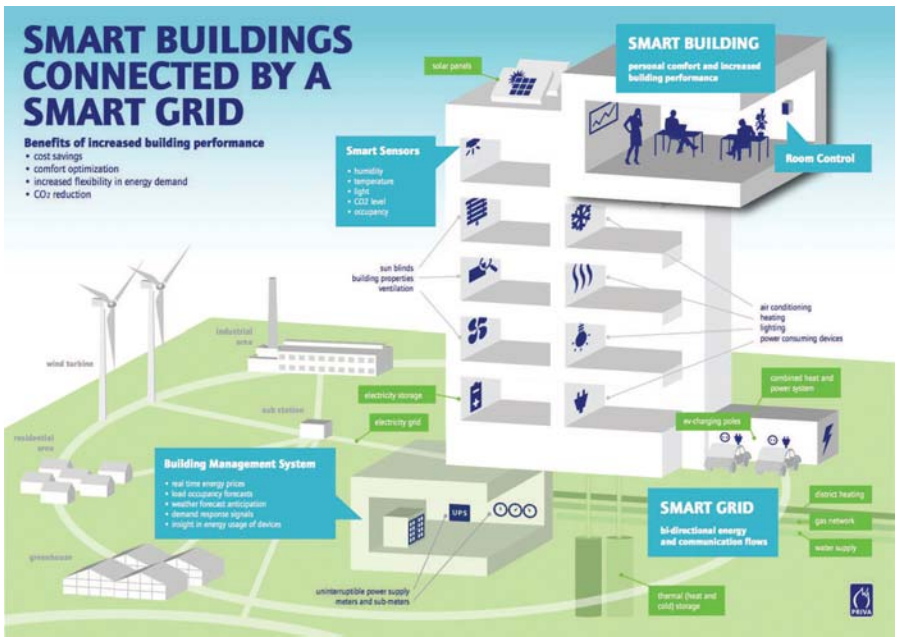

Figure 3.18 Smart Building connected by a Smart Grid [24].

in real-time. An example of such possible implementation for DC drids in residential buildings is shown in Figure 3.19. The solution is able to generate large volumes of granular energy data and behavioural information, and it is able to process these energy and behavioural data locally. It is likely that for the smart energy domain, this solution will evolve into reference residential gateways designs that combines energy management services with other vertical applications in a heterogeneous networking environment.

The future energy economy based on IoT technology need to include open, interoperable transaction-based platforms that facilitates physical transactions of energy, energy-related services, and the financial settlements associated with these transactions and integration with the smart grid (see Figure 3.18), smart city, lighting, mobility applications.

3.3.5 Smart Energy

The energy supply will be largely based on various renewable resources and this source of energy will influence the energy consumption behaviour, demanding 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. The functions

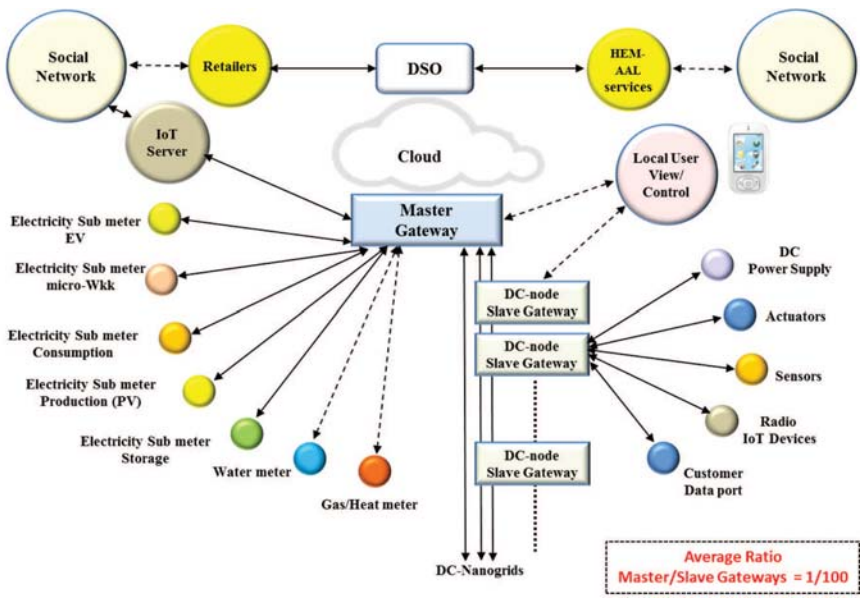

Figure 3.19 IoT concept for residential buildings using the DER DC grid.

are based on networked intelligent devices (appliances, micro-generation equipment, infrastructure, consumer products) and grid infrastructure elements, largely based on IoT concepts.

IoT is expected to facilitate the deployment of new smart energy apps within energy stakeholders' ICT systems (generation and retail companies, grid and market operators, new load aggregators) bringing new options for real-time control strategies across energy asset portfolios for faster reactions to power fluctuations. These new technologies combine both centralised and decentralised approaches integrating all energy generation (generation, storage) and load (demand responsive loads in residential, buildings and industries as well as storage and electrical vehicles) through interconnected real-time energy markets. IoT should also improve the management of asset performance through more accurate estimations of asset health conditions and deployment of fact based preventive maintenance.

These new smart energy apps will largely be based on the networking of IoT intelligent devices embedded within Distributed Energy Resources (DER) spread across the energy system such as consumer appliances, heating and air conditioning, lighting, distributed generation and associated inverters, grid edge and feeder automation, storage and EV charging infrastructures. While energy systems have historically been controlled through single central dispatch strategies with limited information on smart grid edge and consumers behaviours, energy systems are characterized by rapidly growing portfolios of DER structured through several layers of control hierarchies interconnecting the main Grid down to microgrids within industries and communities, nanogrids at building level and picogrids at residential scale.

Most of DER have diffused within end-user premises, new transactive energy (TE) control approaches are required to facilitate their coordination at various scales of the Grid system through real-time pricing strategies. The aggregators and energy supply companies have started to develop new flexibility offers to facilitate DER coordination virtually through ad hoc virtual power plants raising new connectivity, security and data ownership challenges.

Meanwhile climate change has also recently exposed grids to new extreme weather conditions requiring to reconsider grid physical and ICT architectures to allow self-healing during significant disasters while taking advantage of Distributed Generation and storage to island critical grid areas (hospital, large public campus) and maintain safe city areas during emergency weather conditions.

By 2030, the future utility value chain will have transformed significantly. Navigant Research argues that current distribution network operators will have transformed into distribution service orchestrators; they will be responsible for far more than just network operations. Likewise, the current energy supply business – already transitioning to a service-based model – will be fully transformed into an energy service provider (ESP) model. Companies will offer end-to-end energy services that have little in common with today's volume-based approach to revenue generation. The resulting new business models will require new IT infrastructure that relies heavily on the analysis of huge volumes of data. Distribution orchestration platforms will rely on the integration of existing advanced distribution management systems (ADMSs) and DER management software, as well as the incorporation of a market pricing mechanism to reflect the changing value of millions of connected endpoints throughout the day. ESPs will rely on TE platforms that enable prosumers to sell their power into the market, incorporate customer portals to provide in-depth account details, and provide billing and settlement functionality [26].

The high number of distributed small and medium sized energy sources and power plants can be combined virtually ad hoc to virtual power plants. Using this concept, areas of the grid can be isolated from the central 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. Microgrids and Nanogrids either islanded or grid-connected are compounded by several agents of different nature. Consumers, producers and prosumers aim to achieve specific local goals such as reliability, diversification of energy sources, low carbon emission and cost reduction. Small-scale storage is offering flexibility to the electric power system, which can contribute to increase grid security and stability, modifying the electricity generation and load patterns in grid nodes. At the same time, this means an increase in reliability, power quality and renewable energy penetration. Due to the high penetration of renewables, energy storage usage and the wide variation of different resources, electrical grid environment is getting more and more complex. In the energy domain, the proliferation of microgrids for local control of energy sources, integration of renewables and energy storage units requires the integration of communication gateways and distributed cooperative control for bidirectional energy flow. In this context, energy flows will be managed similarly to internet data packets across grid nodes, which autonomously decide the best pathway minimising energy system dispatch costs while guaranteeing its best resiliency.

This is based on the development of Internet of Energy (IoE) concept as network infrastructure based on standard and interoperable communication nodes that allow the end to end real time balance between the local and the central generation, responsive demand and storage. It will allow units of energy to be transferred peer to peer when and where it is needed. For these applications, the IoT gateway is integral component of the micro inverter system and operates between the micro inverters and energy brokers systems and the web-based monitoring and analysis software. A conceptual representation of an integrated energy system based on DER, microgrids where the communication gateways play a key role is presented in Figure 3.20.

The requirements for the IoT technologies and gateways in the energy sector has to be seen in relation with the development of the virtual power plants and novel virtual microgrid architectures. These requirements include microgrid communication infrastructures for microgrid applications such as inter substation communication, substation to building communication, and distributed energy resources. The microgrid information management systems for distribution automation demand side scheduling, distributed generation/control, real time unit embedded system for substations, medium voltage measurement, monitoring and communication system.

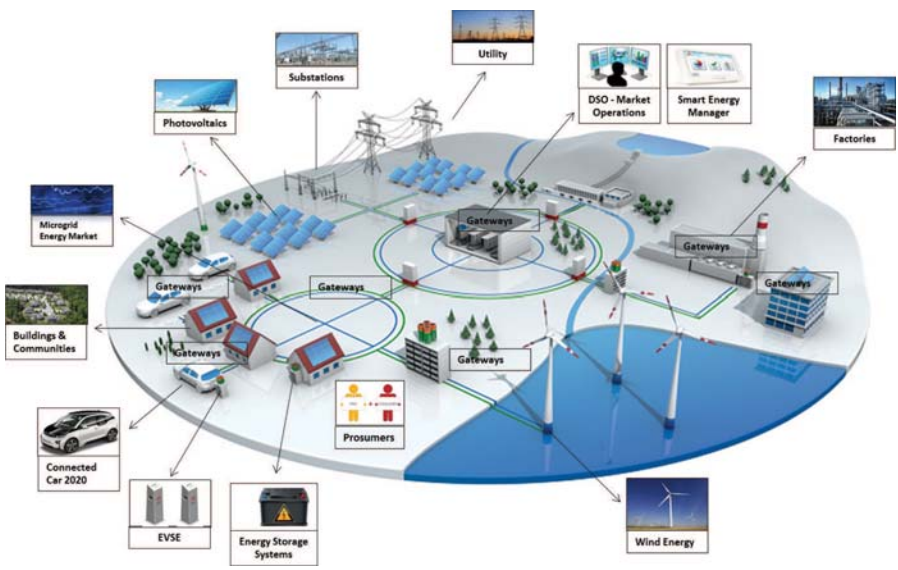

Figure 3.20 IoT technologies and the gateway role in microgrids and nanogrids management systems.

These IoT technologies should combine both centralised and decentralised approaches integrating all energy generation (generation, storage) and load (demand responsive loads in residential, buildings and industries as well as storage and electrical vehicles) through interconnected real-time energy markets. IoT should also improve the management of asset performance through more accurate estimations of asset health conditions and deployment of fact based preventive maintenance.

The IoT technologies deployment will have a significant impact on the energy industry with a shift in business models from energy supply-based to service-based models.

The service-based model of the 2030s means network operators' primary focus is now on end customers and networks are far more dynamic, volatile, and unpredictable [26]:

- The rise of the prosumer means that power flows have become two-way.
- Self-consumption by PV and electricity storage owners significantly changes load curves to evening peaks when solar PV is no longer generating power.
- New, power-hungry appliances such as EVs and heat pumps place significant new demands on network capacity.
- The aggregation of DER into virtual power plants creates dispatchable power connected directly to low voltage networks.
- TE systems encourage rapid switching between the export and import of power from many premises throughout the day.
- DER aggregation and management become a critical component of a distribution service orchestrator's role. Network volatility and dynamism require more active management of low voltage networks, particularly managing the peak consumption periods when customers shift from self-generated consumption to grid-sourced electricity.

The 2030 energy landscape, presented in [26], has the customer in the center of the Energy Cloud (Figure 3.21) with the following characteristics:

- The Energy Cloud is a mature set of technologies. Ubiquitous solar PV and storage create a customer-centric energy value chain where customers' consumption is largely met by self-generated electricity.
- Utility-scale and distributed renewables account for 50%–100% of generation; distributed energy resources (DER) uptake is widespread, accounting for most new build capacity.
- High penetration rates of EVs put a strain on network capacity, which is managed using pricing signals and automatic demand response (DR).

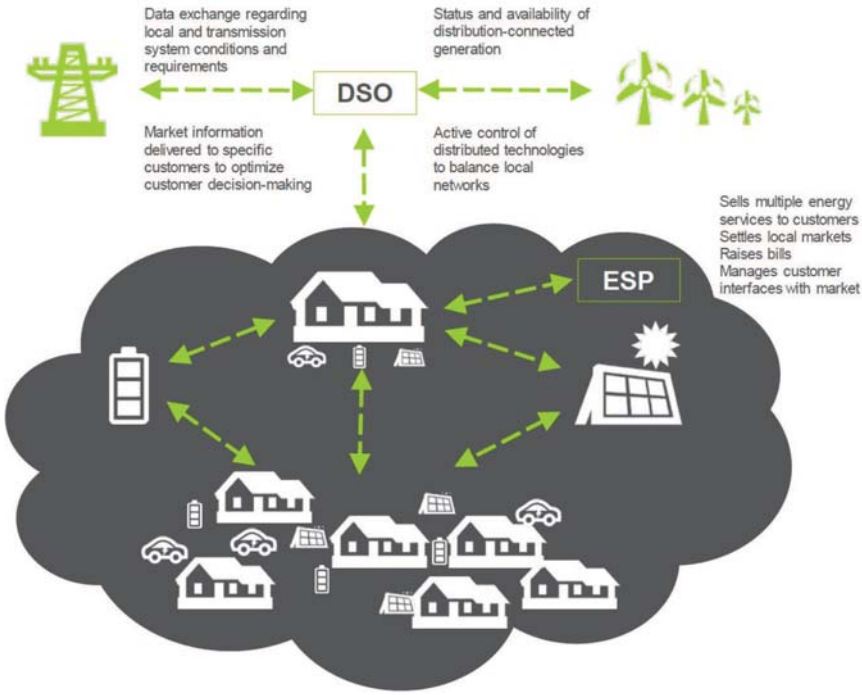

Figure 3.21 Energy cloud 2030 [24].

- Data is as valuable a commodity as electrons. While in 2017 the industry struggled to maximize the value of enterprise data, in 2030 the energy supply chain is fully digitized and its efficient operation is heavily based on analytics-based automation. This automation relies on the huge volumes of data created by technologies within the Energy Cloud.
- The industry has undergone significant digital transformation. Data and artificial intelligence (AI)-based algorithms become important competitive differentiators. Data offers visibility into each prosumer's electricity exports and imports, providing the fundamental basis of the transitive energy market. This data also allows the newly formed distribution service orchestrators to actively manage the dynamic and volatile distribution networks, either through pricing signals or by actively interrupting the power supply.
- Utility business models have transformed from supply- to service-based. Rather than focus purely on the delivery of grid-sourced power, energy service providers (ESPs) offer individualized products and services to

suit their customers' specific needs. These services will include DER sales, maintenance, and aggregation; DR; energy efficiency initiatives; flexible, time-of-use charging; and TE platforms.

- Markets are far more competitive in 2030 compared to 2017. The convergence of the old regulated supply business model and deregulated service-based model creates opportunities for new entrants. Many new service providers have entered the market, exploiting the new value streams from decentralized electricity.
- The smart grid of 2017 has transitioned to a neural grid. The new grid is nearly autonomous and self-healing, leveraging innovations in AI and cyber-physical systems (e.g., IoT, self-driving EVs, and the smart grid).
- Distribution operators have evolved into distribution service orchestrators to manage this neural grid. Advanced platforms incorporate advanced distribution management systems (ADMSs), DER management systems (DERMSs), and pricing signals to manage the more volatile and dynamic grids.
- Two separate, yet complementary technology platforms underpin the market. TE and distribution orchestration platforms enable prosumers to sell self-generated power on open markets and manage the highly volatile and dynamic distribution networks.
- In 2030, prosumers trade their self-generated power on the open market. This is a dramatic change from relying on the subsidies or net metering that supported residential solar PV in 2017. Electricity is bought and sold at market rates and revenue from a TE platform alone totals $6 billion per year. To bring this into the perspective of other disruptive innovators, TE revenue in 2030 is 4 times the size of Uber's 2015 revenue.

3.3.6 Smart Mobility and Transport

Consumer preferences, tightening regulation, and technological breakthroughs add up to a fundamental shift in individual mobility behaviour. Individuals increasingly use multiple modes of transportation to complete their journey, and goods and services are increasingly delivered to (rather than fetched by) consumers. As a result, the traditional business model of car sales will be complemented by a range of diverse on-demand mobility solutions, especially in dense urban environments that proactively discourage private car use. Consumers today use their cars as "all-purpose" vehicles (Figure 3.22), no matter if commuting alone to work or taking the whole family to the beach. In the future, they may want the flexibility to choose the

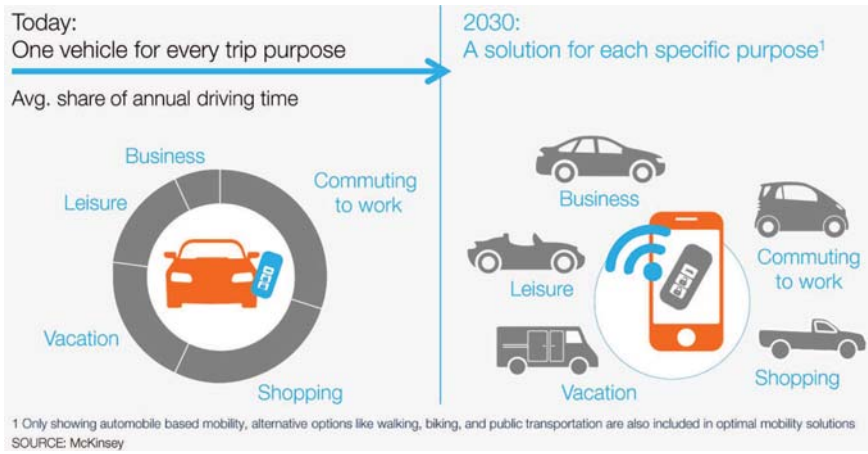

Figure 3.22 Mobility patterns [15].

best solution for a specific purpose, on demand and via their smartphones. We can already observe significant, early signs that the importance of private car ownership is declining and shared mobility is increasing [15].

The connection of vehicles to the Internet offers new possibilities and applications which bring new functionalities to the individuals and/or the making of transport easier and safer. New mobile ecosystems based on trust, security and convenience to mobile/contactless services and transportation applications are created and the developments such as Internet of Vehicles (IoV) [38] are connected with Internet of Energy (IoE) for providing services in an increasingly electrified mobility industry.

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.

Self-driving vehicles today are evolving and the vehicles are equipped with technology that can be used to help 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.

Technical elements of such systems are 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).

In the field of connected autonomous vehicles IoT and sensing technology replace human senses and advances are needed in areas such as [27]:

- Vehicle's location and environment: As there would no longer be active human input for vehicle functions, highly precise and real-time information of a vehicle's location and its surrounding environment will be required (e.g., road signs, pedestrian traffic, curbs, obstacles, traffic rules).
- Prediction and decision algorithms: Advanced concepts based on Artificial Neural Networks (unsupervised/deep learning, machine learning) will be needed to create systems to detect, predict and react to the behaviour of other road users, including other vehicles, pedestrians and animals.
- High accuracy, real time maps: Detailed and complete maps must be available to provide additional and redundant information for the environmental models that vehicles will use for path and trajectory planning.
- Vehicle driver interface: A self-adapting interface with smooth transition of control to/from the driver, mechanisms to keep the driver alert and a flawless ride experience will be instrumental in winning consumer confidence.

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 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 evolutions in the global automotive industry are monitored in order to identify the factors that are driving the change in the automotive ecosystem,

[1]Society of Automotive Engineers, J3016 standard.

the move to new business models such as mobility-as-a-service and the best conditions and the technologies that are supporting the digital transformation. The automotive industry has followed a very linear development path in more than 100 years. The parallel emergence of four megatrends in the last 2 years mobility, automated driving, digital experience and electrification, the industry will be reshaped in the next 10 to 15 years.

The Radar presented in [28] analyzes the transformation via 25 selected indicators in five dimensions: customer interest (e.g. via >10,000 end user interviews), regulation, technology, infrastructure and industry activity.

Figure 3.23 presents the automotive disruption radar globally that indicates the customers' interest in autonomous vehicles and their acceptance of electrical vehicles as an alternative, but a low interest in vehicle to vehicle communication.

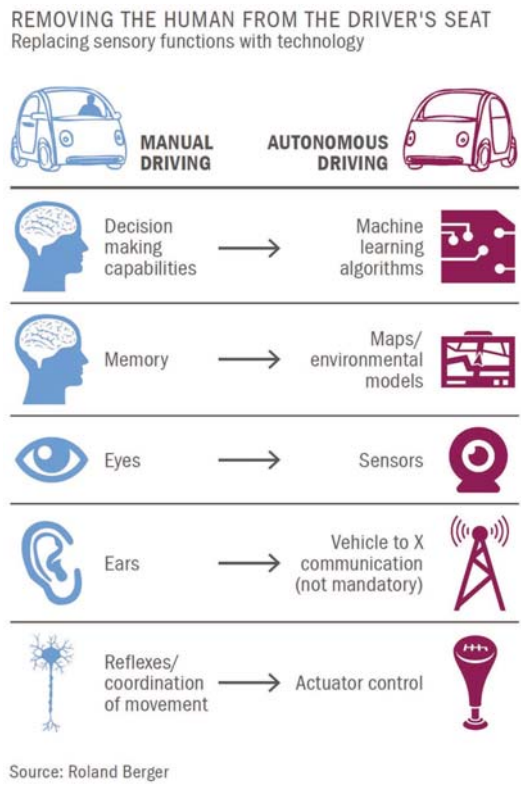

Figure 3.23 Replacing sensory functions with technology [27].

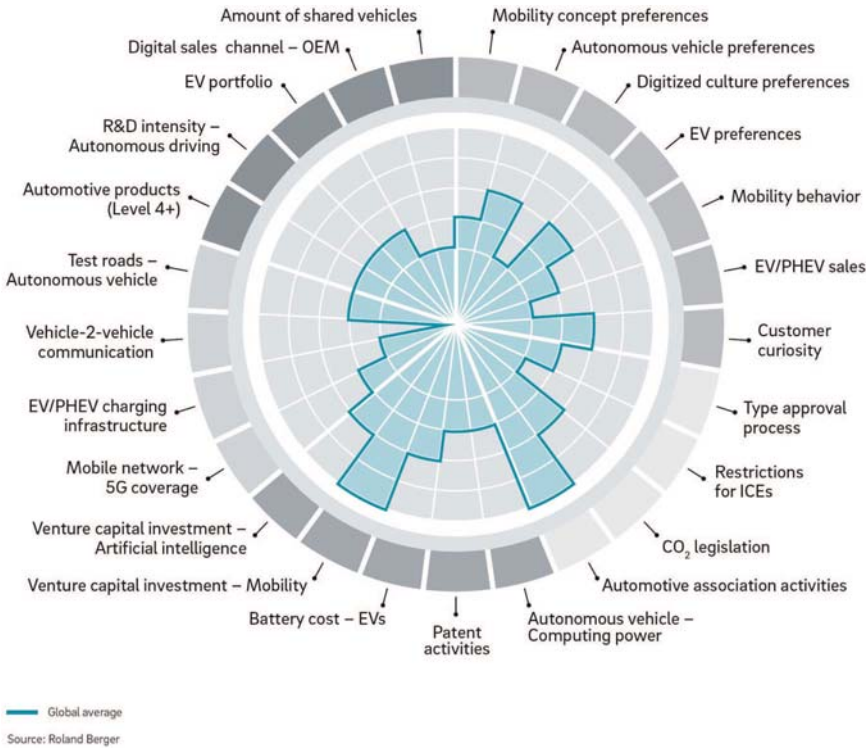

Figure 3.24 Automotive disruption radar globally [28].

3.4 IoT and Related Future Internet Technologies

3.4.1 Edge Computing

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. There are different edge computing paradigms, such as transparent computing and fog computing. The fog computing is focusing on resource allocation in the service level, while transparent computing concentrates on logically splitting the software stack (including OS) from the underlying hardware platform to provide cross-platform and streamed services for a variety of devices. These

differences enable edge computing to support broader IoT applications with various requirements.

As part of this convergence, IoT applications (such as sensor-based services) will be delivered on-demand through a cloud environment [39]. This extends beyond the need to virtualize sensor data stores in a scalable fashion. It asks for virtualization of Internet-connected objects and their ability to become orchestrated into on-demand services (such as Sensing-as-a-Service).

Computing at the edge of the mobile network defines the IoT-enabled customer experiences and require a resilient and robust underlying network infrastructures to drive business success. IoT assets and devices are connected via mobile infrastructure, and cloud services are provided to IoT platforms to deliver real-time and context-based services. Edge computing is using the power of local computing and using different types of edge devices, to provide intelligent services. Data storage, computing and control can be separated and distributed among the connected edge devices (servers, micro servers, gateways, IoT nodes, etc.). Thus, edge computing advantages, such as, improved scalability, local processing, contextual computing and analytics. Interacting with the cloud (see Figure 3.25), edge computing provide scalable services for different type of IoT applications.

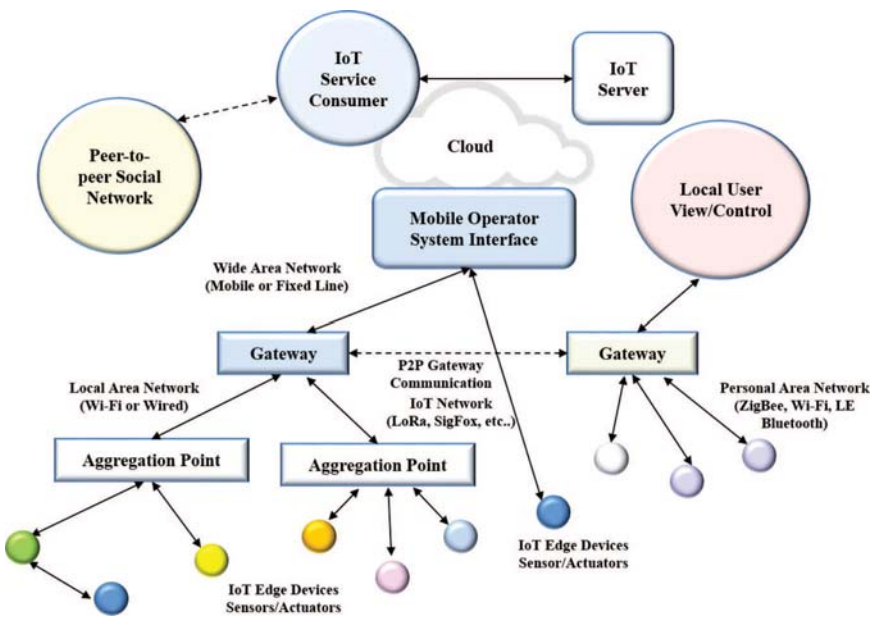

Figure 3.25 IoT centralised and distributed networks – gateway aggregation points.

Data transmission costs and the latency limitations of mobile connectivity pose challenges to many IoT applications that rely on cloud computing. Mobile edge computing will enable businesses to deliver real-time and context-based mobile moments to users of IoT solutions, while managing the cost base for mobile infrastructure. A number of challenges listed below have to be addressed when considering edge-computing implementation [40]:

- Cloud computing and IoT applications are closely connected and improve IoT experiences. IoT applications gain functionality through cloud services, which in turn open access to third-party expertise and up-to-date information.
- Mobile connectivity can create challenges for cloud-enabled IoT environments. Latency affects user experiences, so poor mobile connectivity can limit cloud-computing deployments in the IoT context.
- Mobile edge computing provides real-time network and context information, including location, while giving application developers and business leaders access to cloud computing capabilities and a cloud service environment that's closer to their actual users.
- Mobile edge computing is an important network infrastructure component for blockchain. The continuous replication of "blocks" via devices on this distributed data centre poses a tremendous technological challenge. Mobile edge computing reveals one opportunity to address this challenge.

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. The edge computing technologies for IoT require to address issues such as unstable and intermittent data transmission via wireless and mobile links, efficient distribution and management of data storage and computing, edge computing interfacing with the cloud computing to provide scalable services, and finally mechanisms to secure the IoT applications. In this context, the research challenges in this area are:

- Open distributed edge computing architectures and implementations for IoT
- Modelling and performance analysis for edge computing in IoT
- Heterogenous wireless communication and networking in edge computing for IoT
- Resource allocation and energy efficiency in edge computing for IoT

- QoS and QoE provisioning in edge computing for IoT
- Trust, distributed end-to-end security and privacy issues in edge computing for IoT
- Federation and cross-platform, service supply in transparent computing for IoT

3.4.2 Networks and Communication

It is predicted that low-power short-range networks will dominate wireless IoT connectivity through 2025, far outnumbering connections using wide-area IoT networks [31], while 5G networks will deliver 1,000 to 5,000 times more capacity than 3G and 4G networks today. IoT technologies are extending the known business models and leading to the proliferation of different ones as companies push beyond the data, analytics and intelligence boundaries, while, everything will change significantly. IoT 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.

Network Technology

The development in cloud and mobile edge computing requires 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 and optimise the access to Cloud or mobile edge computing resources. IoT is estimated that will connect 30 billion devices. All these devices are connecting humans, things, information and content, which is changing the performance characteristics of the network. Low latency is becoming crucial (connected vehicles or industrial equipment must react in ms), there is a need to extend network coverage even in non-urban areas, a better indoor coverage is required, ultra-low power as many of the devices will be battery operated is needed and a much higher reliability and robustness is requested.

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 Wi-Fi, which will be fully integrated with the cellular network.

Applications making use of cloud computing, and those using edge computing will have to co-exist and will have to securely share data. The right balance needs to be found between cloud/mobile edge computing to optimize overall network traffic and optimize the latency. Facilitating optimal use of both mobile edge and cloud computing, while bringing the computing processing capabilities to the end user. Local gateways can be involved in this optimization to maximize utility, reliability, and privacy and minimize latency and energy expenditures of the entire networks.

Future networks have to address the interference between the different cells and radiations and develop new management models control roaming, while exploiting the co-existence of the different cells and radio access technologies. New management protocols controlling the user assignment to cells and technology will have to be deployed in the mobile core network for a better efficiency in accessing the network resource. Satellite communications need to be considered as a potential radio access technology, especially in remote areas. With the emerging of safety applications, minimizing the latency and the various protocol translation will benefit to the end to end latency. Densification of the mobile network strongly challenges the connection with the core network. Future networks should however implement cloud utilization mechanisms to maximize the efficiency in terms of latency, security, energy efficiency and accessibility.

In this context, there is a need for higher network flexibility combining Cloud technologies with Software Defined Networks (SDN) and Network Functions Virtualisation (NFV), that will enable network flexibility to integrate new applications and to configure network resources adequately (sharing computing resources, split data traffic, security rules, QoS parameters, mobility, etc.)

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 IoT. Network users will be humans, machines, things and groups of them.

Communication Technology

The communication with the access edges of the IoT network shall be optimized cross domain with their implementation space and it shall be compatible with the correctness of the construction approach. Figure 3.26 IoT communication topologies across the architectural layers used for different configurations in IoT applications.

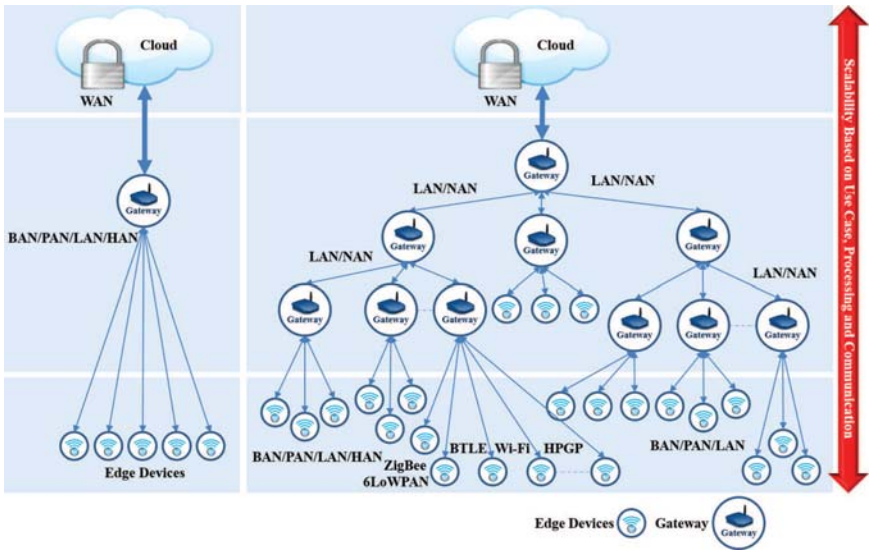

Figure 3.26 IoT Communication topologies across the architectural layers.

These trends require the extension of the spectrum in to the 10–100 GHz and unlicensed band and technologies like WiGig or 802.11ad that are mature enough for massive deployment, can be used for cell backhaul, point-to-point or point-to-multipoint communication. The use of advanced multi-/massive-MIMO technologies have the capability to address both coverage and bandwidth increase, while contributing to optimize the usage of the network resources adequately to real need.

Cisco expects by 2021 that 50% of all IP traffic will be Wi-Fi (30% will be carried by fixed networks and 20% via cellular networks). Parks Associates found that domestic smartphone users reported a 40% increase in their monthly Wi-Fi data consumption last year. Wi-Fi usage as presented in Figure 3.27 increased faster than mobile data usage, with two-thirds of smartphone users consuming more than 3 GB per month [13].

The IEEE's 802.11 (802.11k, 11r and 11v) standards focus on manageability, with features that address chaotic environments (such as transportation hubs) and steering Wi-Fi clients to less-congested, nearby access points (APs) automatically, depending on network conditions, as well as capabilities to better transition from AP to AP and network to network with very rapid handovers. The features of the latest 802.11 standards are shortly described below:

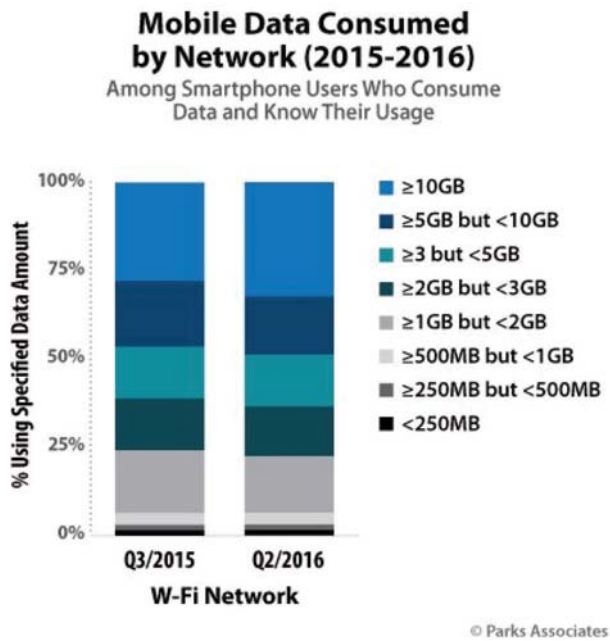

Figure 3.27 Wi-Fi Network – Mobile data consumed by network (2015–2016) [13].

- 802.11k – The 802.11k Assisted Roaming (AR) Roaming allows 11k capable clients to request a neighbor report containing information about known neighbor APs that are candidates for roaming. This feature enables the client to ask one AP about the other APs in the network – a neighbor list – and the client then makes use of that list in order to decide which AP to connect to, rather than sending probe signals.
- 802.11v – This feature enables client steering. A Wi-Fi client and an AP can both do some amount of measuring the signal environment and exchanging information to determine that "next best AP" for the client to connect to as it moves through the network. 802.11v enables an AP to warn and then force a client with a fading signal to disconnect, while providing information about other APs that the client can utilize that may be more lightly loaded or provide better signal strength. This prevents so-called "sticky" clients from being able to cling to a preferred AP that is providing a poor signal or is congested.
- 802.11r – The 802.11r Fast Transition (FT) Roaming uses a new concept for roaming. The initial handshake with the new Access Point (AP)

occurs before client roams to the target AP, called as Fast Transition (FT). In terms of authentication, once a device is authenticated on a Wi-Fi network, 802.11r provides some short-cuts on authentication among APs on the same network – so the network and device aren't basically trading the same "handshake" information back and forth every time a client connects to a new AP within the network. The number of exchanges is reduced, which means the roaming or reconnection time is also reduced, therefore improving the user experience.

The IoT applications will embed the devices in various forms of communication models that will coexist in heterogeneous environments. The models will range from device to device, device to cloud and device to gateway communications that will bring various requirements to the development of electronic components and systems for IoT applications. The first approach considers the case of devices that directly connect and communicate between each another (i.e. using Bluetooth, Z-Wave, ZigBee, etc.) not necessarily using an intermediary application server to establish direct device-to-device communications. The second approach considers that the IoT device connect (i.e. using wired Ethernet or Wi-Fi connections) directly to Internet cloud/fog service of various service providers to exchange data and control message traffic. The third approach, the IoT devices connect to an application layer gateway running an application software operating on the gateway device, providing the "bridge" between the device and the cloud service while providing security, data protocol translation and other functionalities. The gateway has a key role in the communications layer that integrates a collection of communication networks, which enable flow of information across the application domain system. No single technology will cover all aspects and needs of the various domains: the network requirements are largely driven by applications and use cases. The need of connecting anything from anywhere brings new scenarios that depend on latency, mission criticality, time-of-use pricing, peak data rates, security needs, battery life, and distance requirements, which allows various protocols and networks accessible for use. For some applications, the networking will allow connecting to ZigBee, wM-Bus, Power Line Communication (PLC), Wi-Fi, Z-Wave, LonWorks, while for other could be PLC, Ethernet Broadband, Ethernet IP, Wi-Fi/WiMax, 2G/3G/4G cellular or even satellite communication. Figure 3.28 illustrate the trade-off between range and data rates for the gateway and the different communication protocols.

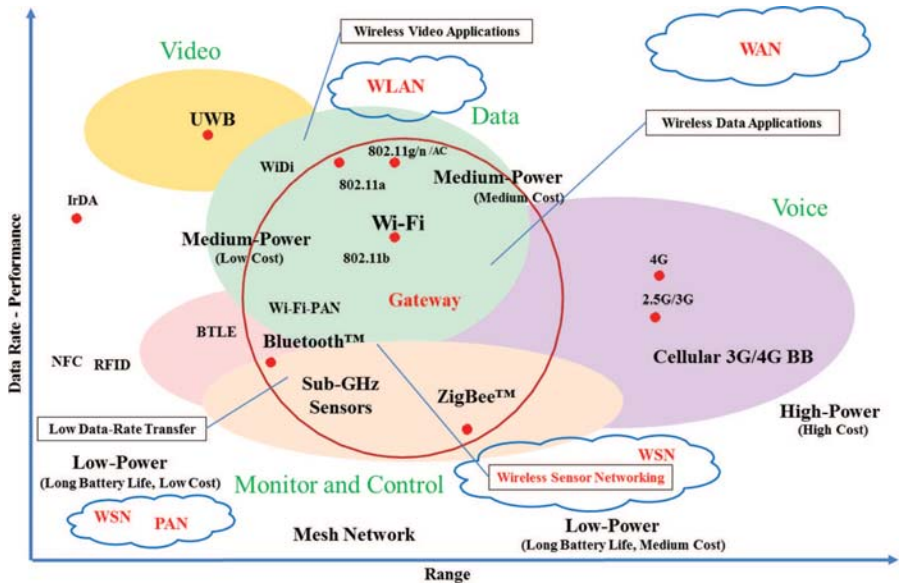

Figure 3.28 Gateway trade-off – data rate vs. range.

Gateway reference architecture allows for using the gateway reference designs in healthcare monitoring, environment parameters monitoring, indoor localization, wearables, by exploiting short-range/medium-range wireless connectivity. The individual rights to access secure information, secure data handling and privacy will be handled by security enabling components.

By delving into finer and more specific technical details, the targeted multi-functionality/multi-protocol reference gateways are complex embedded systems that require complex software running on high-end processor platforms, sometimes using real-time operating systems. The gateway reference designs manage edge heterogeneous devices and translate data across networks and into analytical cloud systems. They provide a customizable middleware development environment that provides security, connectivity, networking options, and device management to simplify the development, integration, and deployment of gateways for the IoT. In the residential environments, the gateways are emerging as integration platforms or an edge computing platform that enables to seamlessly interconnect various devices and other systems into a system of systems. The gateway enables users to securely aggregate, process, share, and filter data for analysis. The new gateways may include the integration of analytics into the gateway functionality

to address specific problems in the embedded applications directly in the localities where analytics results may be promptly detected and trigger rapid reactions in a decentralized way.

The processing solutions to run the determined analytic algorithms in the most efficient and effective way can be adapted to the various gateway reference designs since solutions are extremely size and power constrained and real-time math intensive architectures of DSP. By including analytics into gateway functionality, the device offers edge processing, where analytics are used in the gateway and near the edge devices of the network to reduce the amount of data being transmitted. The analytics allows to discovering meaningful relationships and patterns in data and they can provide the ability to facilitate making an intelligent decision or make a decision based on the data that can provide a way to reduce network bandwidth by only transmitting the relevant information and not the entire data stream.

In addition, in order to increase portability, easy deployability, and easy extensibility in the heterogeneous and ever changing ecosystem of IoT components, virtualization and efficient cloud integration techniques can be used. The gateway design blend communications and computing technologies and integrates software-defined networking (SDN) and network functions virtualization (NFV) to consolidate network, cloud, and data centre functions onto standard, high-volume servers, switches, and storage. Several reference design implementations use general-purpose Java, Java-based OSGi, Eclipse Mihini, and Lua and support open standard IoT protocols, also for the efficient integration with heterogeneous cloud resources, including TR-069, OMA-DM/LWM2M, XMPP, CoAP, MQTT, while using hypervisor and virtualization technologies.

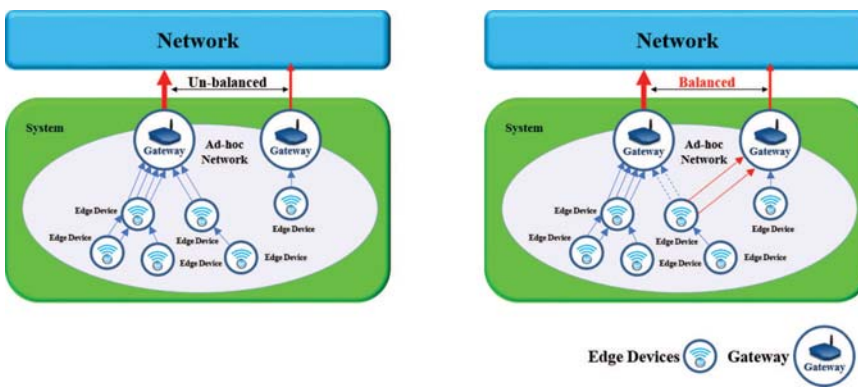

Figure 3.29 Network requirements – un-balance and balanced case.

The modular integrated connectivity creates a scalable mobile platform (modems for 2G/3G/4GLTE), enabling high-speed data and voice. and various onboard selected LoRa, Sigfox, On Ramp Wireless, NWave/ Weightless SIG, 802.11 Wi-Fi/Wi-Fi Aware, Bluetooth, ZigBee, 6LowPAN, Z-Wave, EnOcean, Thread, wMBus protocols using multiple ISM radio bands simultaneously (i.e. 169/433/868/902 MHz, 2.4 GHz, and 5 GHz), The connectivity modules are based on integrated ICs, reference designs, and feature-rich software stacks based on a flexible, modular concept that properly addresses various application domains.

The load of the network will be different with models using unbalanced load of the ad-hoc network from the core network point of view, while other using network-based solutions by balancing the topology from the core network point of view. In this case the identified network requirement to be supported are the calculation of the optimal ad-hoc network topology by using monitoring information, and notification of appropriate actions based on calculation results as presented in

The deployment of billions of devices requires network agnostic solutions that integrate mobile, narrow band IoT (NB-IoT), LPWA networks, (LoRA, Sigfox, Weightless, etc) as presented in Figure 3.30, and high speed wireless networks (Wi-Fi), particularly for applications spanning multiple jurisdictions.

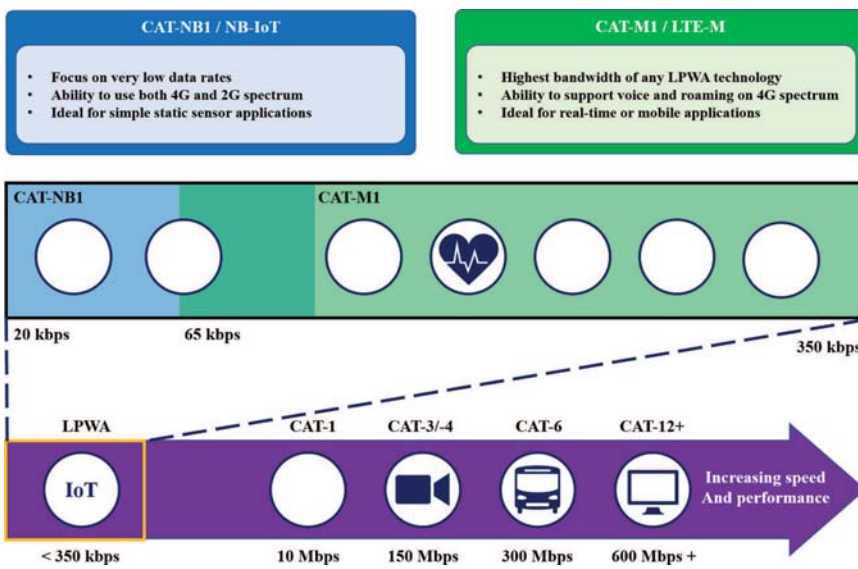

Figure 3.30 LPWA, NB-IoT and LTE-M for low data rates IoT applications.

LPWA networks have several features that make them particularly attractive for IoT devices and applications that require low mobility and low levels of data transfer:

- Low power consumption that enable devices to last up to 10 years on a single charge
- Optimised data transfer that supports small, intermittent blocks of data
- Low device unit cost
- Few base stations required to provide coverage
- Easy installation of the network
- Dedicated network authentication
- Optimised for low throughput, long or short distance
- Sufficient indoor penetration and coverage

These different types of networks are needed to address IoT product, services and techniques to improve the Grade of Service (GoS), Quality of Service and Quality of Experience (QoE) for the end users. Customization-based solutions, are addressing industrial IoT while moving to a managed wide-area communications system and, ecosystem collaboration.

Intelligent gateways will be needed at lower cost to simplify the infrastructure complexity for end consumers, enterprises, and industrial environments. Multi-functional, multi-protocol, processing gateways are likely to be deployed for IoT devices and combined with Internet protocols and different communication protocols.

These different approaches show that device interoperability and open standards are key considerations in the design and development of internetworked IoT systems.

Ensuring the security, reliability, resilience, and stability of Internet applications and services is critical to promoting the concept of trusted IoT based on the features and security provided of the devices at various levels of the digital value chain.

3.5 IoT Distributed Security – Blockchain Technology

IoT-based businesses, applications and services are scaling up and going through various digital transformations in order to deliver value for money and remain competitive, they are becoming increasingly vulnerable to disruption from denial-of-service attacks, identity theft, data tampering and other threats. A quality-of-service (QoS) security framework for IoT architecture is presented in [2], comprising of authentication, authorization, network and trust management components.

The IoT must embrace distributed technologies in order to both scale and provide end-to-end security, trust and accountability. In [1], swarm intelligence (SI), a subfield of artificial intelligence (AI), is presented as a source of inspiration for the design of new IoT security solutions. The use of SI makes it possible to add both cognitive and collective intelligence to IoT objects. Thus, IoT objects will strive to improve to a higher level of local intelligence in order to fulfil their function in a distributed manner, while the collective intelligence is centralised in order to solve problems that are more complex.

IoT objects are becoming more intelligent and more capable of making decisions both individually and collectively; they are also driven by collaboration, collective efforts and competition. Thus, the consensus problem, which is fundamental to decision-making in multi-agent systems, has received attention recently – and not least due to the newly emerging blockchain technology.

Blockchain technology addresses trust and security issues in an open and transparent manner, allowing the democratisation of trust. This is achieved by maintaining a record of every transaction made by every participant and having many participants verify each transaction, thus providing highly redundant verification and eliminating the need for centralised trust authorities. Consensus is thus achieved in a more effective way [3].

The concept of distributed consensus is at the core of blockchain technology [7]. Distributed consensus in the digital world means various nodes in a network coming to an agreement in a way that is very similar to a group of people, i.e., each member contributes their own opinion, and the group as a whole comes to a collective decision (except of course that the implementation in the digital process is a rather complex computer science problem). Nevertheless, the success of the concept lies precisely in the fact that both the collective decision and the process are recorded. Any time a transaction is challenged, for example, if an abnormal behaviour can be traced back to it, the recording is able to provide proof of the context in which the transaction had been performed.

Thus, the rationale behind blockchain technology keeping records of both the decision and the process is to ensure verifiability, so that all past and current transactions can be verified at any time in the future. This allows a high degree of accountability, without compromising the privacy of either the digital assets or the parties involved. Anonymity is therefore another important feature of blockchain technology.

Anonymity is difficult to achieve, even with a group of people seeking consensus, due to the very basic principles that consensus is built upon: members engage in dialogue and share information for the purpose of increasing the group's understanding of the issues, thus providing a rationale for each member's particular opinion, position and, ultimately, the group's collective decision. The same level of interaction is not required in the case of majority rule, and so people can more easily remain anonymous.

Although the concept of the blockchain is linked to Bitcoin, it is applicable to any digital asset exchanged online, where the asset is not money, but information. An example is the healthcare sector, where information is highly confidential. With the advance of technology, patients are located more and more often outside of hospitals and medical centres, and so their secure communication network involves more agents. Thus, the security of all transactions in the wider distributed network is essential.

Blockchain, the underlying technology of Bitcoin, is a 'chain of digital signatures', as described by Satoshi Nakamoto [4]. It enables parties connected to the same network to exchange information and other assets without the need for a third party to mediate the exchange. Blockchain technology entails a digital platform of distributed database technologies and protocols, which ensure that the transactions are irrefutable and that the information stored and shared is unalterable. The blockchain is copied to all parties in the network. Each transaction is verified and validated by a consensus of the parties. The transactions are arranged chronologically in blocks and are linked together so that each block embeds the history of all assets and decision processes since the first transaction. Therefore, it is almost impossible to generate a fraudulent transaction or the race against the other parties and the consensus that ultimately leads to the transaction being verified and validated. This provides a guaranteed protection against malicious interventions.

There is no universally agreed-upon definition of blockchains. They consist of various types, such as public or private. Blockchains also use different consensus mechanisms so that they can be adapted for use in a specific application field. Despite these differences, each implementation of blockchain technology invariably has a number of common features that distinguish it from other technologies. Blockchain technology is:

- Decentralized, meaning that there is no need for a central or other trusted authority to keep the data or supervise since each node has a copy of the entire database.

- Consensus-driven, meaning that new blocks are only added upon agreement that they are verified and validated.
- Anonymous, meaning that the identities of the nodes that participated in a current or past transaction are withheld but can be traced in case the transaction is challenged in the future.
- Unalterable, meaning that it is difficult, if not impossible, to change historical data simply because all nodes possess copies of the records.
- Time-stamped, meaning that the date and time a block is added to the blockchain is recorded.
- Programmable, meaning that transactions and other actions are executed only when certain conditions are met.

Although it is a promising alternative to established practices based on centralised control, blockchain technology still faces challenges in several areas, such as privacy, scalability, security, costs and integration.

Variations of the Bitcoin 'proof-of-work' consensus mechanism as well as novel designs have been proposed to deal with environments that depart from the idealistic assumption that the nodes in a network will always act in an honest and predictable way. 'Proof-of-stake', 'smart contracts', 'Byzantine consensus' and 'deposit-based consensus' are examples of such solutions [5]. Nevertheless, reaching a consensus in the context of dishonest and distrusting nodes, which is a challenge in the field of distributed computing, also remains difficult with blockchain technology.

Despite the challenges, it is relatively easy to achieve one goal: making people trust the blockchain technology. It is a matter of common sense to question the integrity of a service that works without any trusted central authority. One way to earn people's confidence is through transparency, and exposing the technology's internal workings. Another way to achieve this is to prove the legitimacy of the technology for applications other than Bitcoin. To demonstrate the former approach, this chapter briefly addresses two aspects of the internal workings of blockchain-namely, 'smart contracts' and block verification and validation. Regarding the latter means of promoting trust, insights into the use of blockchain in healthcare are provided.

3.5.1 Verification and Validation in Blockchain

One thing not easily understood about blockchain technology is how a newly created transaction is verified and validated using distributed technologies. In the same way that people need a favourable environment to reach a consensus in the real world, a specific set of conditions is also required in the digital,

online world. Although it is not easy, blocks can be generated fraudulently; therefore, it is necessary to decide which blocks to trust. The debate process that leads to a decision needs better exposure. What are the algorithms used to reach a consensus so that a transaction can be verified and validated?

A transaction created to initiate a service is represented as a 'block' and contains, at a minimum, a unique identifier and the source, destination, type and amount of the asset being exchanged. The block thus generated is broadcast to the rest of the network. The nodes perform verification and validation activities, based on which the transaction is accepted or rejected. If accepted the 'block' is added to the blockchain. What verification and validation mean and how much information is necessary to accept a transaction vary from node to node and from service to service. Depending on the results from the nodes, a consensus algorithm is needed to produce a decision.

Verification activities mainly consist of checking digital signatures and the relationship between each virtual node and the actor behind it. Biometrics are a reliable form of verification, and embedding biometrics into the blockchain or linking the blockchain to a biometrics database has already been proposed.

Validation activities focus on the business logic and distinguish between public and private blockchains. While Bitcoin uses miners, private networks use individual validators, or trusted actors whose identity is known to the rest of the network. The incentive for transaction validators is not in the form of bitcoins but rather in being part of the network and benefiting from its information and services [8]. The more validators are in a network, the more decentralised and credible its decisions will be.

3.5.2 IoT Blockchain Application in Healthcare

Another way to earn people's confidence in the blockchain technology is to prove the legitimacy of the technology for applications other than Bitcoin. There are multiple applications of blockchain in the healthcare industry, with the potential to offer innovative solutions to challenges caused by the increasing volume of patient data managed by various stakeholders. This in turn increases the vulnerability to hacking and ransomware attacks, as those which recently targeted hospitals in several European countries and the US. As the purpose of such attacks is to deprive the medical institution of its own data by locking this data, this would be more difficult to achieve if the data is distributed and replicated across many nodes in a blockchain-based network.

Another application is remote healthcare, which is a new way of managing the care of patients with long-term conditions outside hospitals, either because there are no hospitals in the geographic area or in order to reduce costs. Innovative solutions are required in order to place the individual at the centre of healthcare. The individual owns his/her own health and can access a life-time supply of records, anytime, anywhere. When necessary, the records are shared, accessed and interpreted by various stakeholders in a transparent, efficient and accountable manner. The blockchain represents the individual's healthcare path through life.

Another aspect of blockchain technology that is not easily understood is the new trend of smart contracts, which seems to mean different things to different people. Smart contracts are a self-executing code on a blockchain that automatically implements the terms of an agreement between parties.

In the healthcare industry, with the growth of connected health devices performing various functions, an Internet of Medical Things (IoMT) has started to evolve. The interoperability of the exchanged data, together with data security, privacy and reliability, must be a top priority, and blockchain and smart contracts have the potential to offer good solutions.

A proof-of-concept, which demonstrated how the principles of decentralisation and blockchain technology can be applied in the healthcare industry, has recently been reported in the literature [6]. The concept gives patients a comprehensive, immutable log as well as easy access to their medical information across providers and treatment sites. Medical stakeholders (researchers, public health authorities, etc.) are incentivised to participate in the network as blockchain 'miners'. The concept of contracts is depicted in Figure 3.31, where three type of contracts are shown on the left-hand side: Registrar Contracts (RC), which deal with identity registration and authentication; Patient-Provider Relationship Contracts (PPR), which deal with authorisation and the relationship between the patient and provider and fine-grained access control to medical data and, finally, Summary Contracts (SC), which deal with aggregate data for patients and providers. The blockchain implements references and pointers, allowing navigation in the relationship graphs between contracts and network nodes, examples of which are shown on the right-hand side.

On top of blockchain technology, smart contracts can be the solution to the integration of IoT and Artificial Intelligence (AI). Smart contracts are in fact codes that can trigger, for instance, a rule-based reasoning when certain conditions are met. Rules and conditions are pre-defined, and the AI techniques and methods used are limited mostly to the creation of intelligent

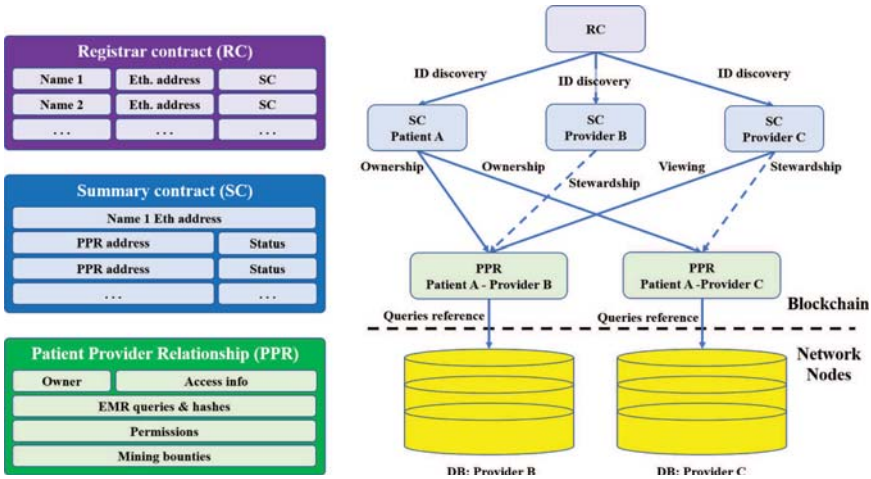

Figure 3.31 Smart contracts on the left-hand side and relationship graph between contracts and network nodes on the right-hand side [6].

representations of the nodes and existing medical records. However, it is envisaged that in the near future, more advanced AI techniques will be adopted so that nodes could learn to reason and act both independently and in groups in a more intelligent manner. In other words, these techniques will develop both local and collective intelligence. The traditional blockchain will become a cognitive blockchain, able to learn from past cases and adapt over time.

Blockchain technology augmented with both local and collective intelligence will make it possible for IoT objects to reason about household energy consumption, monitor and remotely collect patients' health status data, take actions through IoT devices and much more. Relevant use cases for the integration of these cutting-edge technologies are being reported in the literature, contributing to increasing levels of trust in them. The ultimate goal is to improve quality of life, whether by optimising household energy consumption, the use of self-driving cars, access to healthcare and so on.

3.6 IoT Platforms

IoT refers to an ecosystem in which applications and services are driven by data collected from devices that sense and interface with the physical world. Important IoT application domains span almost all major economic sectors: health, education, agriculture, transportation, manufacturing, electric grids, and many more.

IoT platforms enable companies to bring IoT solutions rapidly to the market by cutting development time and expenses for IoT systems.

An IoT Platform can be defined as an intelligent layer that connects the things to the network and abstract applications from the things with the goal to enable the development of services. The IoT platforms achieve a number of main objectives such as flexibility (being able to deploy things in different contexts), usability (being able to make the user experience easy) and productivity (enabling service creation in order to improve efficiency, but also enabling new service development). An IoT platform facilitates communication, data flow, device management, and the functionality of applications. The goal is to build IoT applications within an IoT platform framework. The IoT platform allows applications to connect machines, devices, applications, and people to data and control centres. The functionally of IoT platforms covers the digital value chain of an end-to-end IoT system, from sensors/actuators, hardware to connectivity, cloud and applications as illustrated in Figure 3.32. Different types of platforms have emerged [14].

IoT platforms' functionalities covers the digital value chain from sensors/actuators, hardware to connectivity, cloud and applications. Hardware connectivity platforms are used for connecting the edge devices and processing the data outside the datacentre (edge computing/fog computing), and program the devices to make decisions on the fly. The key benefits are security, interoperability, scalability and manageability by using advanced data management and analytics from sensor to datacentre. IoT software platforms

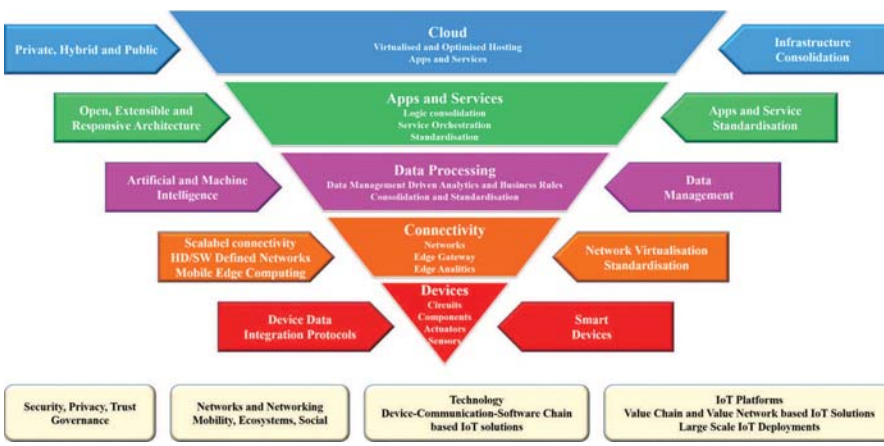

Figure 3.32 IoT Platforms covering the data value chain [14].

include the integration of heterogeneous sensors/actuators, various communication protocols abstract all those complexities and present developers with simple APIs to communicate with any sensor over any network. The IoT platforms also assist with data ingestion, storage, and analytics, so developers can focus on building applications and services, which is where the real value lies in IoT. Cloud based IoT platforms are offered by cloud providers to support developers to build IoT solutions on their clouds. Infrastructure as a Service (IaaS) providers and Platform as a Service (PaaS) providers have solutions for IoT developers covering different application areas. PaaS solutions, abstract the underlying network, compute, and storage infrastructure, have focus on mobile and big data functionality, while moving to abstract edge devices (sensors/actuators) and adding features for data ingestion/processing and analytics services [14]. The functions offered for the IoT consumer/business/industrial platforms are presented in Figure 3.33.

The IoT Platforms provide a framework for categorizing the technology capabilities that are necessary to deliver connected things, operations, assets, and the enterprises [14].

The four main blocks of capabilities presented in Figure 3.33 are:

- Connectivity that includes the hardware and software to network within the factory and the enterprise, standards for integrating machines, clouds, applications and the technology for managing devices, transferring data, and triggering events;
- Data analytics: including the use of a set of statistical and optimization tools to refine, monitor, and analyse structured and unstructured data for enabling different services;
- Cloud that integrate various types of cloud technologies across the enterprise to implement computing and storage capabilities (i.e. at the edge, within the factory, at the enterprise, or outside the firewall);
- Application area that integrates the tools for creating new mashup software applications that leverage the areas of the IoT platform.

Various types of IoT platforms have emerged in the last past years as they developed from the platforms that specific stakeholders or industrial sectors have promoted. A summary of the findings in [14] is presented below.

The IoT platforms on the market can be grouped into four categories: device centric communication/connectivity centric IoT platforms, industry centric IoT platforms and cloud centric IoT platforms. Non-commercial open source platforms are emerging and gaining in importance in several domains.

Figure 3.33 Implementation elements in the main areas covered by IoT platforms [14].

The device centric IoT platforms are developed as hardware-specific software platforms supported by companies that commercialize IoT device components and have built a software backend that is referred to as an IoT platform. These backends are often reference implementations to ease the development of end-to-end IoT solutions, which are made available as starting points to other ecosystem partners.

The connectivity IoT platforms address the connectivity of connected IoT devices via communication networks. The starting points are often traditional M2M platforms for connectivity and device management, and then these are evolving into platforms that provide support for the management of the full IoT service life cycle. Connectivity based platforms primarily focus on providing out of the sandbox solutions for device/product manufacturers, which they can drop into their existing products to make them connected. New platforms provide analytics tailored for extracting the business insights about the performance of connected devices.

The cloud centric IoT platforms are offerings from larger cloud providers, which aim to extend their cloud business into the IoT. They offer different solutions with for example Infrastructure-as-a-service IaaS back ends that provide hosting space and processing power for applications and services. The back ends used to be optimized for other applications have been updated and integrated into IoT platforms offerings from large companies.

The industrial centric IoT platforms are the platforms designed to address the challenges of industrial IoT and integrates extensive features compared with the IoT consumer and business solutions (i.e. strong integrated IT and OT end-to-end security framework).

As the IoT platforms landscape is developing very fast with companies applying different strategies and business models such as sectorial approach that starts with the connectivity layer and is extending to expend to a platform features from the bottom-up.

Large companies use the top-down approach that they have a portfolio of software platform or cloud services and build extension to address the specific requirements for IoT applications. The development is starting from the analytics and cloud part and developing out the IoT platform features from the top-down. In the industrial sector, there are different strategies with companies developing their own industrial IoT platform or using and partnership approach y building alliances to offer the full industrial IoT platform suite. A different approach is developing or extending the IoT platforms offers through targeted acquisitions and/or strategic mergers. Another strategy used by several companies is to use the tactical/strategic investments throughout the IoT ecosystem developed around their IoT platforms and technologies.

Open source platforms are predominately emerging in consumer IoT space, such as the home automation sector or are outcomes of collaborative IoT research initiatives. The main driver is the cumbersome integration of an increasingly diverse set of end devices and protocols – making it costly for proprietary platform providers.

The IoT developments in the last few years have generated multiple architectures, standards and IoT platforms and created a highly fragmented IoT landscape creating technological silos and solutions that are not interoperable with other IoT platforms and applications. In order to overcome the fragmentation of vertically-oriented closed systems, architectures and application areas and move towards open systems and platforms that support multiple applications, for enhancing the architecture of IoT open platforms by adding a distributed topology and integrating new components for integrating evolving sensing, actuating, energy harvesting, networking and interface technologies.

The key technological shift is to provide tools and methods for implementing components and mechanisms in different architectural layers that operates across multiple IoT architectures, platforms and applications contexts and add functionalities for actuation and smart behaviour.

The developments of IoT platforms need to evolve the distributed architecture concept, the methods and tools for IoT open platforms, including software/hardware components, which provide connectivity and intelligence, actuation and control features while linking to modular and ad-hoc cloud and edge services. The IoT open platforms architecture need to allow data analytics and open APIs as well as semantic interoperability across use cases and the federation of heterogeneous IoT systems across the full technology stack. Cloud- and edge based storage and data analytics, and smart applications running on the cloud and at the edge on intelligent sensing/actuating devices (i.e. autonomous vehicles, autonomous devices, robotic things, etc.).

The new concepts need to integrate hardware- and software- level security capabilities to create redundancies to prevent intrusions and enable robust, secure, trusted IoT end-to-end solutions using blockchain technology to facilitate the implementation of decentralized open IoT platforms that assure secured and trusted data exchange as well as record keeping.

The blockchain can serve as the general ledger, keeping a trusted record of all the messages exchanged between smart devices in a decentralized IoT topology.

The IoT platforms need to advance the existing IoT open platforms to enable both integration and federation of existing IoT mechanisms, solutions, and platforms, thus leveraging the exploitation of existing IoT systems while ensuring compatibility with existing developments addressing object identity management, discovery services, virtualisation of objects, devices and infrastructures and trusted IoT approaches.

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, 2014, 2015 and 2016 Strategic Research and Innovation Agendas.

The IoT European Research Cluster SRIA is part of a continuous IoT community dialogue supported by the EC DG Connect – Communications Networks, Content and Technology, E4 – Internet of Things 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 IoT Strategic Research and Innovation agenda document. Their contributions are gratefully acknowledged.

List of Contributors

Abdur Rahim Biswas, IT, CREATE-NET, WAZIUP
Alessandro Bassi, FR, Bassi Consulting, IoT-A, INTER-IoT
Alexander Gluhak, UK, Digital Catapult, UNIFY-IoT
Amados Daffe, SN/KE/US, Coders4Africa, WAZIUP
Antonio Skarmeta, ES, University of Murcia, IoT6
Arkady Zaslavsky, AU, CSIRO, bIoTope
Arne Broering, DE, Siemens, BIG-IoT
Bruno Almeida, PT, UNPARALLEL Innovation, FIESTA-IoT, ARMOUR, WAZIUP
Carlos E. Palau, ES, Universitat Politcnica de Valencia, INTER-IoT
Charalampos Doukas, IT, CREATE-NET, AGILE
Christoph Grimm, DE, University of Kaiserslautern, VICINITY
Claudio Pastrone, IT, ISMB, ebbits, ALMANAC
Congduc Pham, FR, Universite de Pau et des Pays de l'Adour, WAZIUP
Elias Tragos, IE, Insight Centre for Data Analytics, NUIG and FORTH-ICS, RERUM, FIESTA-IoT
Eneko Olivares, ES, Universitat Politcnica de Valencia, INTER-IoT
Fabrice Clari, FR, inno TSD, UNIFY-IoT
Franck Le Gall, FR, Easy Global Market, WISE IoT, FIESTA-IoT, FESTIVAL

Frank Boesenberg, DE, Silicon Saxony Management, UNIFY-IoT
François Carrez, UK, University of Surrey, FIESTA-IoT
Friedbert Berens, LU, FB Consulting S.à r.l, BUTLER
Gabriel Marão, BR, Perception, Brazilian IoT Forum
Gert Guri, IT, HIT, UNIFY-IoT
Gianmarco Baldini, IT, EC, JRC
Giovanni Di Orio, PT, UNINOVA, ProaSense, MANTIS
Harald Sundmaeker, DE, ATB GmbH, SmartAgriFood, CuteLoop
Henri Barthel, BE, GS1 Global
Ivana Podnar, HR, University of Zagreb, symbIoTe
JaeSeung Song, KR, Sejong University, WISE IoT
Jan Höller, SE, EAB
Jelena Mitic DE, Siemens, BIG-IoT
Jens-Matthias Bohli, DE, NEC
John Soldatos, GR, Athens Information Technology, FIESTA-IoT
José Amazonas, BR, Universidade de São Paulo, Brazilian IoT Forum
Jose-Antonio, Jimenez Holgado, ES, TID
Jun Li, CN, China Academy of Information and Communications Technology, EU-China Expert Group
Kary Främling, FI, Aalto University, bIoTope
Klaus Moessner, UK, UNIS, IoT.est, iKaaS
Kostas Kalaboukas, GR, SingularLogic, EURIDICE
Latif Ladid, LU, UL, IPv6 Forum
Levent Gürgen, FR, CEA-Leti, FESTIVAL, ClouT
Luis Muñoz, ES, Universidad De Cantabria
Manfred Hauswirth, IE, Insight Centre for Data Analytics, NUIG, OpenIoT, VITAL
Marco Carugi, IT, ITU-T, ZTE
Marilyn Arndt, FR, Orange
Markus Eisenhauer, DE, Fraunhofer-FIT, HYDRA, ebbits
Martin Bauer, DE, NEC, IoT-A
Martin Serrano, IE, Insight Centre for Data Analytics, NUIG, OpenIoT, VITAL, FIESTA-IoT, BIG-IoT
Martino Maggio, IT, Engineering – Ingegneria Informatica Spa, FESTIVAL, ClouT
Maurizio Spirito, IT, Istituto Superiore Mario Boella, ebbits, ALMANAC, UNIFY-IoT
Maarten Botterman, NL, GNKS, SMART-ACTION
Ousmane Thiare, SN, Université Gaston Berger, WAZIUP

Payam Barnaghi, UK, UNIS, IoT.est
Philippe Cousin, FR, FR, Easy Global Market, WISE IoT, FIESTA-IoT, EU-China Expert Group
Philippe Moretto, FR, ENCADRE, UNIFY-IoT, ESPRESSO, Sat4m2m
Raffaele Giaffreda, IT, CNET, iCore
Roy Bahr, NO, SINTEF, UNIFY-IoT
Sébastien Ziegler, CH, Mandat International, IoT6
Sergio Gusmeroli, IT, Engineering, POLIMI, OSMOSE, BeInCPPS
Sergio Kofuji, BR, Universidade de São Paulo, Brazilian IoT Forum
Sergios Soursos, GR, Intracom SA Telecom Solutions, symbIoTe
Sophie Vallet Chevillard, FR, inno TSD, UNIFY-IoT
Srdjan Krco, RS, DunavNET, IoT-I, SOCIOTAL, TagItSmart
Steffen Lohmann, DE, Fraunhofer IAIS, Be-IoT
Sylvain Kubler, LU, University of Luxembourg, bIoTope
Takuro Yonezawa, JP, Keio University, ClouT
Toyokazu Akiyama, JP, Kyoto Sangyo University, FESTIVAL
Veronica Barchetti, IT, HIT, UNIFY-IoT
Veronica Gutierrez Polidura, ES, Universidad De Cantabria
Xiaohui Yu, CN, China Academy of Information and Communications Technology, EU-China Expert Group

Contributing Projects and Initiatives

SmartAgriFood, EAR-IT, ALMANAC, CITYPULSE, COSMOS, CLOUT, RERUM, SMARTIE, SMART-ACTION, SOCIOTAL, VITAL, BIG IoT, VICINITY, INTER-IoT, symbIoTe, TAGITSMART, bIoTope, AGILE, Be-IoT, UNIFY-IoT, ARMOUR, FIESTA, ACTIVAGE, AUTOPILOT, CREATE-IoT, IoF2020, MONICA, SYNCHRONICITY, U4IoT.

List of Abbreviations and Acronyms

Acronym	Meaning
3GPP	3rd Generation Partnership Project
API	Application Programming Interface
ARM	Architecture Reference Model
Bluetooth	Proprietary short range open wireless technology standard
BUTLER	EU FP7 research project uBiquitous, secUre inTernet of things with Location and contExt-awaReness

CAGR	Compound annual growth rate
DoS/DDOS	Denial of service attack Distributed denial of service attack
EC	European Commission
ESOs	European Standards Organisations
ESP	Energy Service Provider
ETSI	European Telecommunications Standards Institute
EU	European Union
FP7	Framework Programme 7
GS1	Global Standards Organization
IBM	International Business Machines Corporation
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
IoB	Internet of Buildings
IoE	Internet of Energy
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-I	Internet of Things Initiative
IoV	Internet of Vehicles
IP	Internet Protocol
IPv6	Internet Protocol version 6
LTE	Long Term Evolution
M2M	Machine to Machine
MIT	Massachusetts Institute of Technology
OASIS	Organisation for the Advancement of Structured Information Standards
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
PAN	Personal Area Network
PET	Privacy Enhancing Technologies
PPP	Public-private partnership
PV	Photo Voltaic
SENSEI	EU FP7 research project Integrating the physical with the digital world of the network of the future
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
SRIA	Strategic Research and Innovation Agenda
TC	Technical Committee
W3C	World Wide Web Consortium
ZigBee	Low-cost, low-power wireless mesh network standard based on IEEE 802.15.4
Z-Wave	Wireless, RF-based communications technology protocol

References

[1] O. Vermesan and P. Friess (Eds.). Digitising the Industry Internet of Things Connecting the Physical, Digital and Virtual Worlds, ISBN: 978-87-93379-81-7, River Publishers, Gistrup, 2016.

[2] O. Vermesan and P. Friess (Eds.). Building the Hyperconnected Society – IoT Research and Innovation Value Chains, Ecosystems and Markets, ISBN: 978-87-93237-99-5, River Publishers, Gistrup, 2015.

[3] Outlier Ventures Research, Blockchain-Enabled Convergence – Understanding The Web 3.0 Economy, online at https://gallery.mailchimp.com/65ae955d98e06dbd6fc737bf7/files/Blockchain_Enabled_Convergence.01.pdf

[4] What is a blockchain? https://www2.deloitte.com/content/dam/Deloitte/ch/Documents/innovation/ch-en-innovation-deloitte-what-is-blockchain-2016.pdf

[5] R. Chan. Consensus Mechanisms used in Blockchain. https://www.linkedin.com/pulse/consensus-mechanisms-used-blockchain-ronald-chan
[6] A. Ekblaw et al. A Case Study for Blockchain in Healthcare: "MedRec" prototype for electronic health records and medical research data, 2016 https://www.healthit.gov/sites/default/files/5-56-onc_blockchainchallenge_mitwhitepaper.pdf
[7] M. Crosby et al. BlockChain Technology. Beyond Bitcoin. Berkeley, University of California, 2015 http://scet.berkeley.edu/wp-content/uploads/BlockchainPaper.pdf
[8] G. S. Samman. How Transactions Are Validated On A Distributed Ledger, 2016. https://www.linkedin.com/pulse/how-transactions-validated-distributed-ledger-george-samuel-samman
[9] ITU-T, Internet of Things Global Standards Initiative, http://www.itu.int/en/ITU-T/gsi/iot/Pages/default.aspx
[10] International Telecommunication Union – ITU-T Y.2060 – (06/2012) – Next Generation Networks – Frameworks and functional architecture models – Overview of the Internet of things
[11] 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
[12] Yole Développement, Technologies & Sensors for the Internet of Things, Businesses & Market Trends 2014–2024, 2014, online at http://www.yole.fr/iso_upload/Samples/Yole_IoT_June_2014_Sample.pdf
[13] Parks Associates, Monthly Wi-Fi usage increased by 40% in U.S. smartphone households, online at https://www.parksassociates.com/blog/article/pr-06192017
[14] A. Gluhak, O. Vermesan, R. Bahr, F. Clari, T. Macchia, M. T. Delgado, A. Hoeer, F. Boesenberg, M. Senigalliesi and V. Barchetti, "Report on IoT platform activities", 2016, online at http://www.internet-of-things-research.eu/pdf/D03_01_WP03_H2020_UNIFY-IoT_Final.pdf.
[15] McKinsey & Company, Automotive revolution - perspective towards 2030. How the convergence of disruptive technology-driven trends could transform the auto industry, 2016
[16] IoT Platforms Initiative, online at https:// www.iot-epi.eu/
[17] IoT European Large-Scale Pilots Programme, online at https://european-iot-pilots.eu/

[18] Où porterons-nous les objets connectés demain?, online at http://lamontreconnectee.net/les-montres-connectees/porterons-objets-connectes-demain/

[19] S. Moore, (2016, December 7) Gartner Survey Shows Wearable Devices Need to Be More Useful, online at http://www.gartner.com/newsroom/id/3537117

[20] Digital Economy Collaboration Group (ODEC), online at http://archive.oii.ox.ac.uk/odec/

[21] D. Maidment, Advanced Architectures and Technologies for the Development of Wearable Devices, White paper, 2014, online at https://www.arm.com/files/pdf/Advanced-Architectures-and-Technologies-for-the-Development-of-Wearable.pdf Accenture. Are you ready to be an Insurer of Things?, online at https://www.accenture.com/_acnmedia/Accenture/Conversion-Assets/DotCom/Documents/Global/PDF/Strategy_7/Accenture-Strategy-Connected-Insurer-of-Things.pdf#zoom=50

[22] Connect building systems to the IoT, online at http://www.electronics-know-how.com/article/1985/connect-building-systems-to-the-iot

[23] S. Kejriwal and S. Mahajan, Smart buildings: How IoT technology aims to add value for real estate companies The Internet of Things in the CRE industry, Deloitte University Press, 2016, online at https://www2.deloitte.com/content/dam/Deloitte/nl/Documents/real-estate/deloitte-nl-fsi-real-estate-smart-buildings-how-iot-technology-aims-to-add-value-for-real-estate-companies.pdf

[24] ORGALIME Position Paper, 2016, online at http://www.orgalime.org/sites/default/files/position-papers/Orgalime%20Comments_EED_EPBD_Review%20Policy%20Options_4%20May%202016.pdf

[25] J. Hagerman, U.S. Department of Energy, Buildings-to-grid technical opportunities, 2014, https://energy.gov/sites/prod/files/2014/03/f14/B2G_Tech_Opps–Intro_and_Vision.pdf

[26] S. Ravens and M. Lawrence, Defining the Digital Future of Utilities – Grid Intelligence for the Energy Cloud in 2030, Navigant Research White Paper, 2017, online at https://www.navigantresearch.com/research/defining-the-digital-future-of-utilities

[27] Roland Berger Strategy Consultants, Autonomous Driving, 2014, online at https://www.rolandberger.com/publications/publication_pdf/roland_berger_tab_autonomous_driving.pdf

[28] Roland Berger Strategy Consultants, Automotive Disruption Radar – Tracking disruption signals in the automotive industry, 2017, online at

https://www.rolandberger.com/publications/publication_pdf/roland_berger_disruption_radar.pdf
[29] The EU General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679).
[30] RERUM, EU FP7 project, www.ict-rerum.eu
[31] Gartner Identifies the Top 10 Internet of Things Technologies for 2017 and 2018, online at http://www.gartner.com/newsroom/id/3221818
[32] A Look at Smart Clothing for 2015, online at http://www.wearable-technologies.com/2015/03/a-look-at-smartclothing-for-2015/
[33] Best Smart Clothing – A Look at Smart Fabrics 2016, online at http://www.appcessories.co.uk/best-smart-clothing-a-look-at-smart-fabrics/
[34] C. Brunkhorst, "Connected cars, autonomous driving, next generation manufacturing - Challenges for Trade Unions", Presentation at IndustriAll auto meeting Toronto Oct. 14th 2015, online at http://www.industriall-union.org/worlds-auto-unions-meet-in-toronto
[35] Market research group Canalys, online at http://www.canalys.com/
[36] 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
[37] 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
[38] 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
[39] M. Yuriyama and T. Kushida, "Sensor-Cloud Infrastructure – Physical Sensor Management with Virtualized Sensors on Cloud Computing", NBiS 2010: 1–8
[40] Mobile Edge Computing Will Be Critical For Internet-Of-Things And Distributed Computing, online at http://blogs.forrester.com/dan_bieler/16-06-07-mobile_edge_computing_will_be_critical_for_internet_of_things_and_distributed_computing