3

The Next Generation Internet of Things – Hyperconnectivity and Embedded Intelligence at the Edge

Ovidiu Vermesan[1], Markus Eisenhauer[2], Martin Serrano[5], Patrick Guillemin[4], Harald Sundmaeker[3], Elias Z. Tragos[9], Javier Valiño[6], Bertrand Copigneaux[7], Mirko Presser[8], Annabeth Aagaard[8], Roy Bahr[1] and Emmanuel C. Darmois[10]

[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]IDATE, France
[8]Aarhus University, Denmark
[9]Insight Centre for Data Analytics, University College Dublin, Ireland
[10]CommLedge, France

Abstract

The Internet of Things (IoT) and the Industrial Internet of Things (IIoT) are evolving towards the next generation of Tactile IoT/IIoT, which will bring together hyperconnectivity, edge computing, Distributed Ledger Technologies (DLTs) and Artificial Intelligence (AI). Future IoT applications will apply AI methods, such as machine learning (ML) and neural networks (NNs), to optimize the processing of information, as well as to integrate robotic devices, drones, autonomous vehicles, augmented and virtual reality (AR/VR), and digital assistants. These applications will engender new products, services and experiences that will offer many benefits to businesses, consumers and industries. A more human-centred perspective will allow us

to maximise the effects of the next generation of IoT/IIoT technologies and applications as we move towards the integration of intelligent objects with social capabilities that need to address the interactions between autonomous systems and humans in a seamless way.

3.1 Next Generation Internet of Things

The IoT is enabled by heterogeneous technologies used to sense, collect, store, act, process, infer, transmit, create notifications of/for, manage and analyse data. The combination of emergent technologies for information processing and distributed security, e.g. AI, IoT, DLTs and blockchains, brings new challenges in addressing distributed IoT architectures and distributed security mechanisms that form the foundation of improved and, eventually, entirely new products and services.

New systems in the IoT that use smart solutions with embedded intelligence, connectivity and processing capabilities for edge devices rely on real-time analysis of information at the edge. These new IoT systems are moving away from centralized cloud-computing solutions towards distributed intelligent edge computing systems. Traditional centralized cloud computing solutions are perfect for non-real-time applications that require high data rates, huge amounts of storage and processing power, are not strict to very low latency, cost money and can be used for heavy data analytics and AI processing jobs. On the other hand, distributed edge solutions introduce computations at the edge of the network where information is generated and are perfect for real-time services, since they exhibit very low latency (in the order of milliseconds) and can be used for simple ultra-fast analytics jobs. The collection, storage and processing of data at the edge of the network in a distributed way contributes also to the increased privacy of the user data, since no personal information is stored in backbone centralized servers and each user retains the full control of his data.

IoT developments during recent years have been characterized by attributes that can be “labelled” the 6**A**s: **A**nything (any device), to be transferred from/to **A**nyone (anybody), located **A**ny place (anywhere), at **A**ny time (any context), using the most appropriate physical path from **A**ny path (any network) available between the sender and the recipient based on performance and/or economic considerations, to provide **A**ny service (any business). The IoT paradigm is evolving and entire IoT ecosystems are now built upon innervation elements known as the 6**C**s: **C**ollect (heterogeneity of devices of various complexities and intelligence, that enhance the real-time collection of data generated from the connections of devices and information), **C**onnect (ubiquitous distributed connections of heterogeneous devices and information, where the connections are the foundational component of the IoT), **C**ache (stored information in the distributed IoT computing/processing environment), **C**ompute (advanced processing and computation of data and information), **C**ognize (information analytics, insights, extractions, real-time AI processing and **C**reate (the creation of new interactions, services, experiences, business models and solutions). This is illustrated in Figure 3.1.

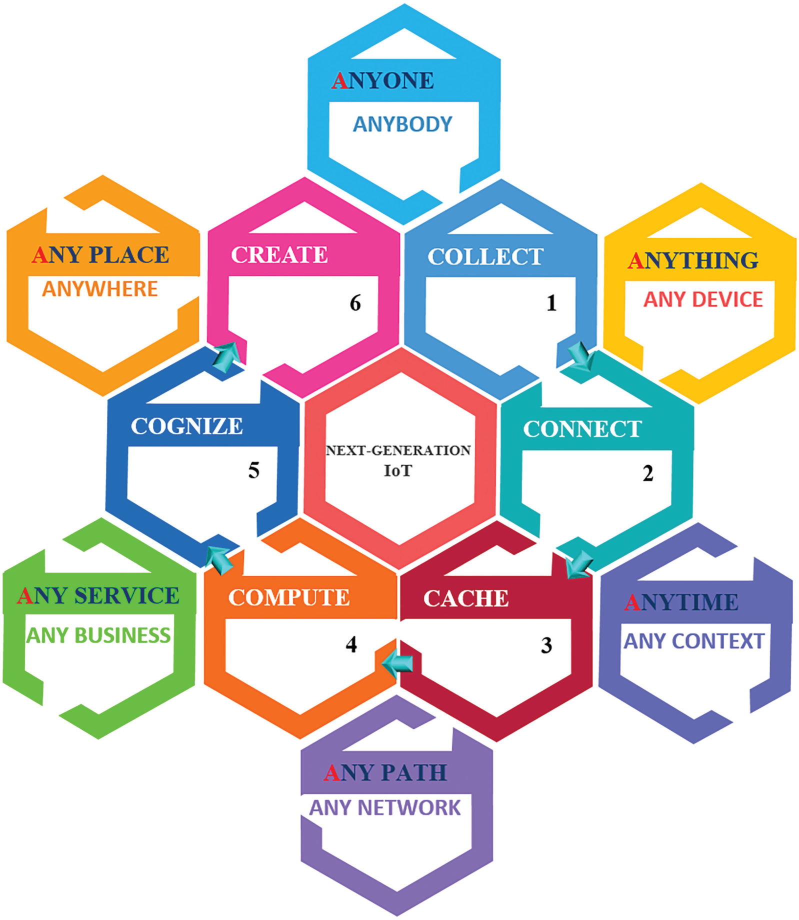
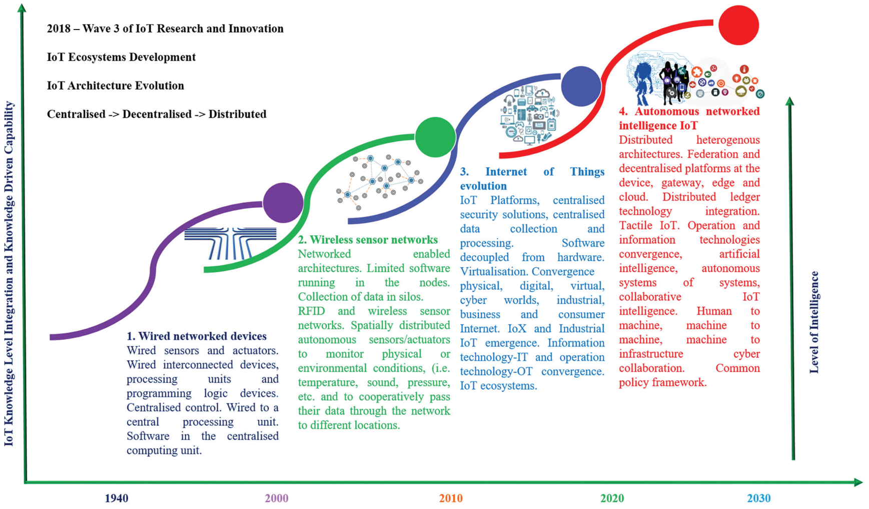


Figure 3.1 Next Generation IoT Hyperconnected: 6As and 6Cs.

The IoT transforms everyday physical objects in the surrounding environment into ecosystems of information that enrich people's lives [97]. The IoT not only influences the future Internet landscape, with implications for security and privacy (personal freedoms), but it could also help to reduce the digital divide. The increased dependence of AI and the IoT on the connectivity network, together with the severity of security challenges, increases their vulnerabilities in parallel. The ongoing and future success of the Internet as a driver for economic and social innovation is linked to how new technologies will respond to these threats. Combining AI with the IoT promises new opportunities, ranging from new services and breakthroughs in science to the augmentation of human intelligence and its convergence with the physical and digital world. The next generation of IoT-combining technologies as presented in Figure 3.3, such as AI, DLTs, hyperconnectivity, distributed edge computing, end-to-end distributed security and autonomous systems - robotics will require increased human-centred safeguards and prioritised ethical considerations in their design and deployment. Next generation IoT evolution is illustrated in Figure 3.2.

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


2018 – Wave 3 of IoT Research and Innovation
IoT Ecosystems Development
IoT Architecture Evolution
Centralised -> Decentralised -> Distributed
IoT Knowledge Level Integration and Knowledge Driven Capability
Level of Intelligence
1940
2000
2010
2020
2030

1. Wired networked devices
Wired sensors and actuators. Wired interconnected devices, processing units and programming logic devices. Centralised control. Wired to a central processing unit. Software in the centralised computing unit.

2. Wireless sensor networks
Networked enabled architectures. Limited software running in the nodes. Collection of data in silos.
RFID and wireless sensor networks. Spatially distributed autonomous sensors/actuators to monitor physical or environmental conditions, (i.e. temperature, sound, pressure, etc. and to cooperatively pass their data through the network to different locations.

3. Internet of Things evolution
IoT Platforms, centralised security solutions, centralised data collection and processing. Software decoupled from hardware. Virtualisation. Convergence physical, digital, virtual, cyber worlds, industrial, business and consumer Internet. IoX and Industrial IoT emergence. Information technology-IT and operation technology-OT convergence. IoT ecosystems.

4. Autonomous networked intelligence IoT
Distributed heterogenous architectures. Federation and decentralised platforms at the device, gateway, edge and cloud. Distributed ledger technology integration. Tactile IoT. Operation and information technologies convergence, artificial intelligence, autonomous systems of systems, collaborative IoT intelligence. Human to machine, machine to machine, machine to infrastructure cyber collaboration. Common policy framework.

Figure 3.2 Next Generation IoT evolution.

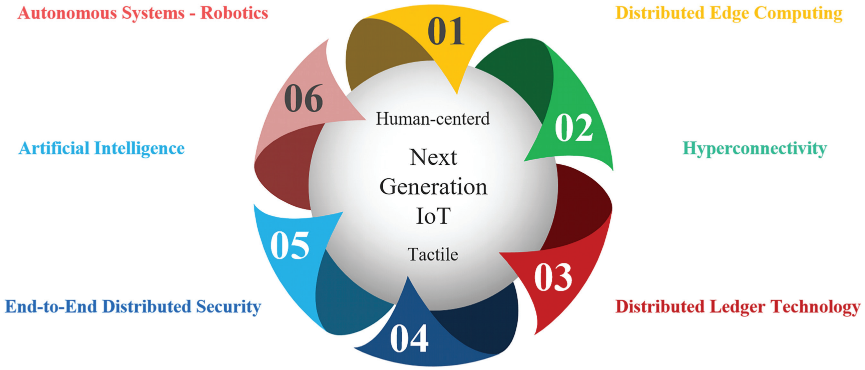

Autonomous Systems - Robotics
Distributed Edge Computing
01
06
02
Human-centerd
Next
Generation
IoT
Tactile
Artificial Intelligence
Hyperconnectivity
05
03
04
End-to-End Distributed Security
Distributed Ledger Technology

Figure 3.3 Next Generation IoT technology convergence.

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 a global concept, the IoT requires a common high-level definition. The IoT is a paradigm involving multidisciplinary activities and has different meanings at different levels of abstraction through the information and knowledge value chain.

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, proposing an unambiguous definition of the "IoT" is non-trivial.

IoT is defined [60] as a dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols where physical and virtual 'things' have identities, physical attributes, and virtual personalities using intelligent interfaces for seamlessly integrating into the information network. In the IoT, 'things' are expected to become active participants in business, information and social processes where they are enabled to interact and communicate among themselves and with the environment by exchanging data and information 'sensed' about the environment, while reacting autonomously to the 'real/physical world' events and influencing it by running processes that trigger actions and create services with or without direct human intervention. Interfaces in the form of services facilitate interactions with these 'smart things' over the Internet, query and change their state and any information associated with them, considering security and privacy issues.

In the context of industry digitisation, IoT/IIoT brings together the primary characteristics of Next Generation Internet (NGI) technology, mobile systems and ubiquitous connectivity with those of industrial control systems, sensing, actuating and control capabilities. Interoperability, platform integration and standardisation are essential for digitising industry applications. IoT/IIoT and industrial control systems have three quality dimensions – integrity, availability and confidentiality – which are essential for implementing applications in industrial vertical domains and across different vertical domains. Whereas the IoT emerged as an add-on to the already existing Internet, it is important to consider the emergence of an NGI where the IoT is deeply embedded and no longer a mere add-on. IoT devices and systems that build on enhanced sensing/actuating, reasoning capabilities and computational power at the edge are already becoming a natural part of an integrated NGI rather than simple extensions of the Internet.

The IoT is promising in a hyperconnected world, where every object has the capability to sense its surrounding environment, transmit information, provide feedback or trigger an action through the application of AI processes in a distributed architecture with processing, intelligence and connectivity at the edge. It is becoming increasingly clear that the main benefit of IoT systems is the network effect, i.e., when different systems are integrated.

As many different systems become integrated, the IoT must face complex interoperability challenges before it can create real cross-domain services with seamless movements of devices and data. However, a lack of stable implementations and the variety of devices available undermine the promised interoperability. A standard solution for IoT interoperability could result in several implementations whose effectiveness would need to be verified and certified; current practices for interoperability testing require different vendors, developers and service providers to participate in physical events. The integration of hyperconnectivity, IoT/IIoT, AI, DLTs and edge computing requires the NGI to address these challenges. This implies the identification of the right business models and the proper governance framework, which support data movement across systems and identify liability in case of any issues, as well as an understanding of the means to overcome the current technical fragmentation in the IoT.

In many applications, the centralised services of cloud computing are being replaced with IoT edge-distributed solutions based on AI methods. With multi-access edge computing (MEC) and ubiquitous hyperconnectivity capabilities (5G and beyond), the IoT is now able to process large amounts of information, resulting from its connections, to be used for intelligent purposes by advanced AI algorithms, which can learn with less data and require fewer processing and memory resources.

The cognitive transformation of IoT applications also allows the use of optimised solutions for individual applications and the integration of immersive technologies, i.e., virtual reality (VR) and augmented reality (AR). Such concepts transform the way individuals and robots interact with one another and with IoT platform systems.

3.2 Next Generation IoT Strategic Research and Innovation

The Internet of Things European Research Cluster (IERC) concentrates the know-how regarding scientific production and research capacity for the Internet of Things in Europe; 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.

Every year, the IERC launches its Strategic Research and Innovation Agenda (SRIA), which is the outcome of discussions involving project representatives/coordinators, a collective group of experts from different stakeholders representing the different domains where IoT is relevant and industry representation that is not necessarily limited to IERC community participation. Such industry participation includes the Alliance for the Internet of Things Innovation (AIOTI), an industry-lead association representing the industrial European and non-European members.

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 of hyperconnectivity, digital transformation, actionable data, information and knowledge.

The IERC works 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.

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. Updated releases of this SRIA build incrementally on previous versions [60, 62, 88] and highlight the main research topics associated with the development of IoT-enabling technologies, infrastructure, and applications [87].

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) [67].

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 form the basis of the IERC SRIA to 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 [87].

The IoT European Large-Scale Pilots Programme [68] 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.).

The IoT European Large-Scale Pilots Programme includes projects promoting the IoT innovation by means of market applications based on services' demand and impact in the European market, technology readiness and socioeconomic interests in European society. The IoT European Large-Scale Pilots Programme is funded by the European Commission (EC) with EUR 100 million over three years (2017–2019) [68].

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 IoT technologies and applications will bring fundamental changes in individuals' and society's views of how technology and business work in the world. A human-centred 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.

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 and development are tightly coupled. 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.

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 next generation IoT/IIoT developments, including human-centred approaches, are interlinked with the evolution of enabling technologies (AI, connectivity, security, etc.) that require strengthening trustworthiness with electronic identities, service and data/knowledge portability across applications and IoT platforms. This ensures an evolution towards distributed IoT architectures with better efficiency, scalability, end-to-end security, privacy and resilience. The virtualization of functions and rule-based policies will allow for free, fair flow of data and sharing of data and knowledge, while protecting the integrity and privacy of data. Vertical industry stakeholders will become more and more integrated in the connectivity-network value chain. Moreover, unified, heterogeneous and distributed applications, combining information and operation technologies (IT and OT), will expose the network to more diverse and specific demands.

Intelligent/cognitive connectivity networks provide multiple functionalities, including physical connectivity that supports transfer of information and adaptive features that adapt to user needs (context and content). These networks can efficiently exploit network-generated data and functionality in real-time and can be dynamically instantiated close to where data are generated and needed. The dynamically instantiated functions are based on intelligent algorithms that enable the network to adapt and evolve to meet changing requirements and scenarios and to provide context- and content-suitable services to users. The intelligence embedded in the network allows the functions of IoT platforms to be embedded within the network infrastructure and data, and the knowledge generated by the intelligent connectivity network and by the users/things can be used by the network itself. This knowledge can be taken advantage of in applications outside of the network.

The connectivity networks for next generation IoT/IIoT are transforming into intelligent platform infrastructures that will provide multiple functionalities and will be ubiquitous, pervasive and more integrated, further embedding telephone/cellular, Internet/data and knowledge networks.

Advanced technologies are required for the NGI to provide the energy-efficient, intelligent, scalable, high-capacity and high-connectivity performance required for the intelligent and dynamically adaptable infrastructure to provide digital services – experiences that can be developed and deployed by humans and things. In this context, the connectivity networks provide energy efficiency and high performance as well as the edge-network intelligence infrastructure using AI, Machine Learning (ML), Deep Learning (DL), Neural Networks (NNs) and other techniques for decentralised and automated network management, data analytics and shared contexts and knowledge.

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 continuously changing IoT landscape and the introduction of new requirements and technologies creates new challenges or raise the need to revisit existing well-acknowledged solutions. Thus, below is a list of 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, trust, safety 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, preventing the exploitation of IoT devices for launching cyber-attacks, i.e., remotely controlling IoT devices for launching Distributed Denial of Service (DDoS) attacks.
- Stronger privacy solutions, considering the requirements of the new General Data Protection Regulation (GDPR) [80] for protecting the users' personal data from unauthorized access, employing protective measures (such as Privacy Enhancing Technologies – 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.

3.2.1 Digitisation

Digitisation is being utilised in many fields, and, as time passes, the influence of digital approaches and techniques is becoming more apparent in several industrial sectors. Buildings and cities are becoming smarter the larger the number of digital services they offer, vehicles are becoming self-driving, design processes are becoming highly efficient and objects and spaces can be visualised before being materialized thanks to the available digital information. Devices with embedded sensors featuring complex logic are scattered everywhere; they measure light, noise, sound, humidity and temperature and are empowered to communicate with each other to form IoT ecosystems.

A common element in all of these developments is that digitisation creates a great amount of information. A considerable part of this information reveals how objects work internally and as elements of more complex setups. Accordingly, many innovative technological installations offer creative solutions concerning how to collect and process this information and how to take necessary action.

The challenge with this information is related to how things interact with each other and with the environment while exhibiting behaviour that is often similar to human behaviour. This behaviour cannot be accurately handled by robots, drones, etc., so this is where technologies, such as swarm logic and AI, come into play.

Security-perceived threats almost always trigger interactive installations equipped to sense and react to surrounding parameters. Changes in these parameters can be visualised, increasing the chances of real threats being detected and asserted.

Thanks to advanced visualisation techniques, the threat landscape is better defined. While security used to be primarily about securing information, the landscape has widened considerably. The timely transfer of information, threat identification, isolation and correct and traceable actions all rely on security protection.

IoT ecosystems evolve, so too must security strategies, which have to account for the layered architecture, where all things, encryptions, communications and actions must be protected against a growing number of diverse attacks, whether via hardware, software or physical tampering.

The IoT system can be seen as a group of agents with non-coordinated individual actions that can collectively use local information to derive new knowledge as a basis for some global actions. The intelligence lies both in agents (AI) and in their interactions (collective intelligence). At the core of swarm logic is the sharing of information and interactions with each other and the surroundings to derive new information. However, this collective intelligence is prone to a number of attacks, especially related to malicious nodes sending false information to influence the decision-making system. Thus, reputation and trust management systems should be in place to be able to identify malicious or misbehaving system agents/nodes and remove them from the system until they behave normally again. These types of attacks can be easily identified and corrected at the edge of the network without having to move all the information to the cloud. Swarm agents can locate and isolate the threat and then converge towards a common point of processing. This is visualised by depicting the real-time state of the agent's movement.

Swarm-designed security is inspired by nature; hence, if IoT can uncover behaviour patterns (of birds, ants, etc.), it may also be capable of meeting security challenges with well-functioning solutions.

3.2.2 Tactile IoT/IIoT

The Tactile IoT/IIoT is a shift in the collaborative paradigm, adding human-centred perspective and sensing/actuating capabilities transported over the network to communications modalities, so that people and machines no longer need to be physically close to the systems they operate or interact with as they can be controlled remotely.

Tactile IoT/IIoT combines ultra-low latency with extremely high availability, reliability and security and enables humans and machines to interact with their environment, in real-time, using haptic interaction with visual feedback, while on the move and within a certain spatial communication range.

Faster Internet connections and increased bandwidth allow to increase the information garnered from onsite sensors within industrial IoT network. This requires new software and hardware for managing storing, analysing and accessing the extra data quickly and seamlessly through a Tactile IoT/IIoT applications. Hyperconnectivity is needed to take VR and AR to the next level for uniform video streaming and remote control/tactile Internet (low latency).

The Tactile IoT/IIoT provides the capabilities to enable the delivery of real-time control and physical (haptic) experiences remotely. The capabilities of the Tactile IoT/IIoT support the creation of a personal spatial safety zone, which is able to interact with nearby objects also connected to the Tactile IoT/IIoT. If applied to traffic, in the long term, this safety zone will be able to protect drivers, passengers and pedestrians. Autonomous vehicles could detect safety-critical situations and react instantly to avoid traffic accidents and warn other objects of impending danger. In production environments, occupational safety levels will improve as production machines or robots detect and avoid the risk of harm to people in their vicinity [45]. A representation of the Tactile Internet of Things Model is shown in Figure 3.4.

The Tactile IoT/IIoT is the next evolution that enables the control of the IoT/IIoT in real-time, with all human senses interacting with machines, by using various technologies both at the network and application level to enable and enhance the interaction in the cyberspace. At the edges, the Tactile IoT/IIoT will be enabled by the sensor/actuators and robotic “things”. Content and data are transmitted over a 5G network, while intelligence is enabled close to the user experience through mobile edge computing. At the application level, automation, robotics, telepresence, AR, VR and AI will be integrated in various IoT/IIoT use cases.

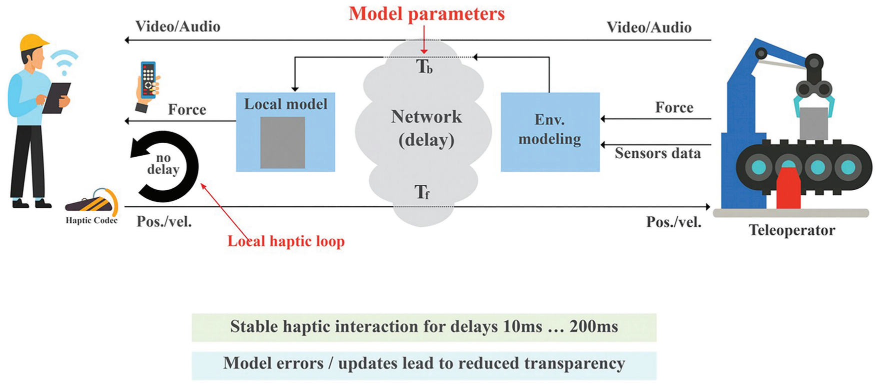


Figure 3.4 Tactile Internet of Things model.

Source: Adapted from Prof Eckehard Steinbach, TU Munich.

The Tactile IoT/IIoT provides a medium for remote physical interaction in real-time, which requires the exchange of closed-loop information between virtual and/or real objects (i.e., humans, machines and processes). The IEEE P1918.1 working group defines the Tactile Internet as a "network or network of networks for remotely accessing, perceiving, manipulating or controlling real or virtual objects or processes in perceived real-time by humans or machines" [44]. The domains of Tactile IoT are illustrated in Figure 3.5.

The Tactile Internet will benefit VR by providing the low-latency communication required to enable "Shared Haptic Virtual Environments", where several users are physically coupled via a VR simulation to perform tasks that require fine-motor skills. Haptic feedback is a prerequisite for high-fidelity interaction, allowing the user to perceive the objects in the VR not only audio-visually but also via the sense of touch. This allows for sensitive object manipulations as required in tele-surgery, micro-assembly or related applications demanding high levels of sensitivity and precision. When two users interact with the same object, a direct force coupling brought into existence by the VR and the users can feel one another's actions. High-fidelity interaction is only possible if the communication latency between the users and the VR is in the order of a few milliseconds. During these few milliseconds, the movements of the users need to be transmitted to the VR server, where the physical simulation is computed, and the result is returned to the users in the form of object status updates and haptic feedback. Typical update rates for the physical simulation and the display of haptic information are in the

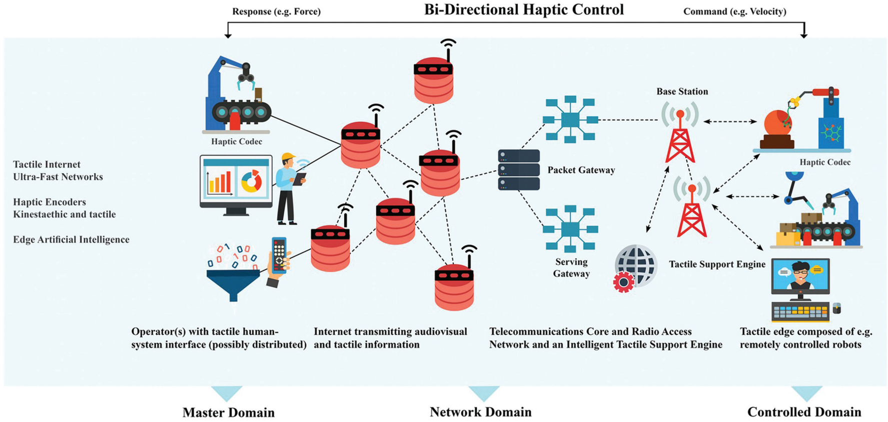

Response (e.g. Force)
Bi-Directional Haptic Control
Command (e.g. Velocity)
Haptic Codec
Tactile Internet
Ultra-Fast Networks
Haptic Encoders
Kinestaethic and tactile
Edge Artificial Intelligence
Packet Gateway
Serving
Gateway
Base Station
Tactile Support Engine
Haptic Codec
Operator(s) with tactile human-system interface (possibly distributed)
Internet transmitting audiovisual and tactile information
Telecommunications Core and Radio Access Network and an Intelligent Tactile Support Engine
Tactile edge composed of e.g. remotely controlled robots
Master Domain
Network Domain
Controlled Domain

Figure 3.5 Tactile Internet of Things representation.

order of 1000 Hertz, which corresponds to an ideal round-trip communication latency of 1 millisecond (ms) [45].

The use of 5G wireless communications for Tactile IoT/IIoT requires latencies of 1 ms or less. The speed of light in fibre is about 200 km/s. Tactile IoT/IIoT which are distributed over distances larger than about 200 km will require a low-latency IoT core network [50].

Tactile Internet has to meet a number of design requirements such as very low end-to-end latency of 1 ms, high reliability for real-time response, data security, availability and dependability of systems without violating the very low latency requirement due to additional encryption delays. These key design objectives of the Tactile Internet can only be accomplished by keeping tactile applications local, close to the users, which calls for a distributed (i.e., decentralized) service platform architecture based on cloudlets and mobile edge computing. Furthermore, scalable procedures at all protocol layers are needed to reduce the end-to-end latency from sensors to actuators. Importantly, the Tactile Internet will set demanding requirements for future access networks in terms of latency, reliability, and also capacity (e.g., high data rates for video sensors) [51]. Tactile Internet of Things interactions are illustrated in Figure 3.6.

In the future, coworking with robots in IoT applications will favour geographical clusters of local production ("inshoring") and will require human expertise in the coordination of the human-robot symbiosis with the purpose of inventing new jobs humans can hardly imagine or did not even know they

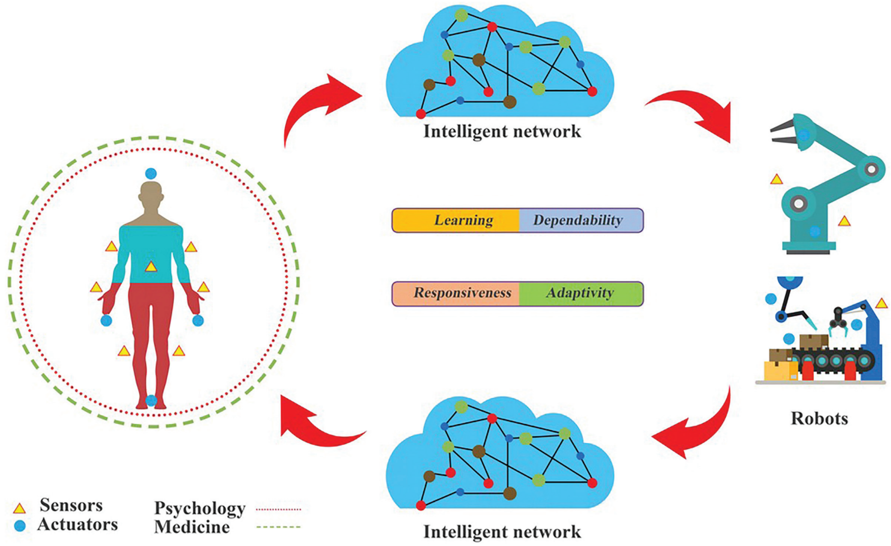


Figure 3.6 Tactile Internet of Things interactions.

Source: Adapted from 5G LAB.

wanted done. Fibre-wireless (FiWi) enabled Human-to-Robot (H2R) communications may be a stepping stone to merging mobile IoT/IIoT, and advanced robotics with automation of knowledge work and cloud technologies, which together represent the five technologies with the highest estimated potential economic impact in 2025 [51, 52].

As presented in Figure 3.7 current Internet cannot guarantee new application delivery constraints. In this context the future technological developments of 5G as the neutral next generation World Wide Wireless Internet by integrating new technologies with a holistic integrated approach combining IPv6-based, machine-to-machine, mobile IoT, mobile edge computing, software defined networks (SDN), network functions virtualisation (NFV), Fringe Internet, Tactile IoT/IIoT, based on seamless worldwide networking interoperability and spectrum harmonisation need to address and solve these constrains for the new applications.

3.2.3 Digital Twins for IoT

Digital twins are virtual representations of material assets. For the IoT, digital twins have never been trendier, as IoT vendors are using increasingly more advanced technology for their implementation, not least with an add-on marketing effect.

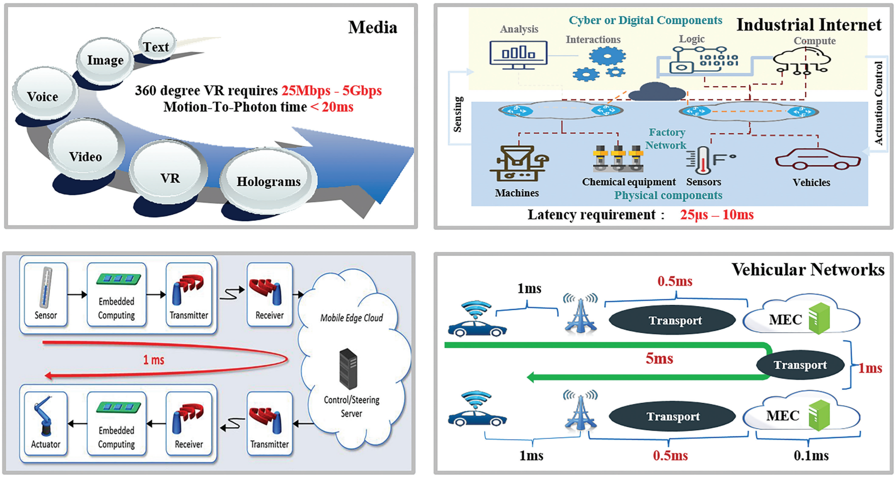


Figure 3.7 New applications for NGI and IoT/IIoT [99].

The current solutions provided by some of the key IoT platforms have mainly been for the representation of physical objects, while such features as simulation, manipulation and optimisation are still missing.

Thanks to technologies, such as blockchain, swarm logic and AI, digital twins now have these capabilities. In the pursuit of better security, digital twins can trigger and simulate threat scenarios in the digital world, as well as optimise the security strategy to handle such scenarios should they occur in the real world.

The digital twin, as a virtual representation of the IoT's physical object or system across its lifecycle, using real-time data to enable understanding, learning and reasoning, is a one element connecting the IoT and AI. The digital twin represents the virtual replica of the IoT physical device by acting like the real thing, which helps in detecting possible issues, testing new settings, simulating all kinds of scenarios, analysing different operational and behavioural scenarios and simulating various situations in a virtual or digital environment, while knowing that what is performed with that digital twin could also happen when it is done by the 'real' physical "thing". Digital twins as part of IoT technologies and applications are being expanded to more applications, use cases and industries, as well as combined with more technologies, such as speech capabilities, AR for an immersive experience and AI capabilities, enabling us to look inside the digital twin by removing the need to go and check the 'real' thing. A digital twin representation is shown in Figure 3.8.

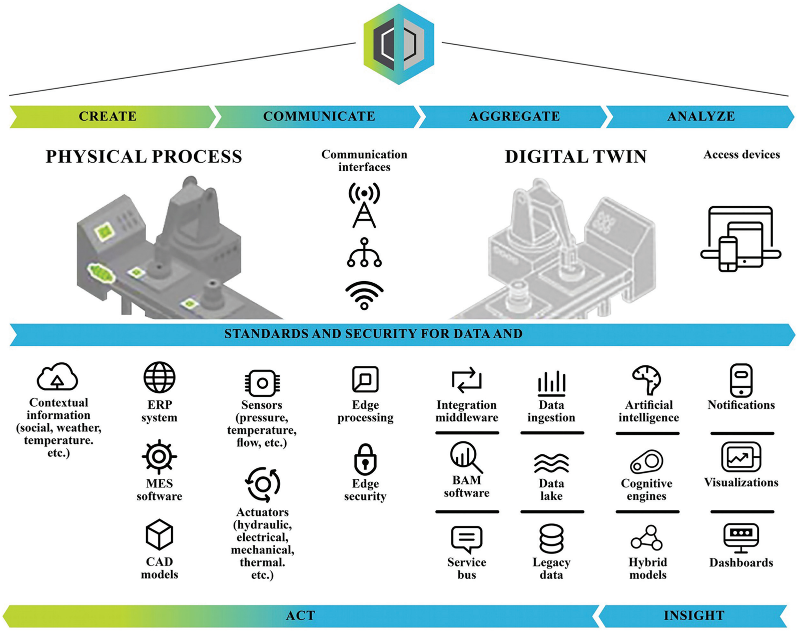


Figure 3.8 Digital Twin representation.

Source: Adapted Deloitte University Press.

Digital twins for IoT must possess at minimum the following attributes:

- Correctness – give a correct replication of the IoT ecosystem and its devices
- Completeness – updated vis a vis the functionality in the real-world system
- Soundness – exhibit only the functionality available in the real-world system
- Abstractness – free from details specific to particular implementations
- Expandability – adapt easily to emerging technologies and applications
- Scalability – must be able to operate at any scale
- Parameterised – accessible for analysis, design and implementation
- Reproducible – be able to replicate the same result for the same input as the real system.

The IoT's digital twins can expand the interface between man and machine through their virtual representation and advanced technologies on levels, such as AI and speech, which enable people and devices/machines to take actions based on operational data at the edge (provided by IoT devices and edge computing processing).

3.3 Future Internet of Things Enabling Technologies

3.3.1 Edge Computing

By 2023, the number of cellular IoT connections is forecast to reach 3.5 billion worldwide. The digitisation of assets, equipment, vehicles and processes in a factory means that the number of connected devices will increase exponentially. The estimated number of connected devices needed in a typical smart factory is 0.5 per square metre[1]. This calculation is based on potential use cases and assets that would benefit from a connection. This illustrates the distribution of cellular connectivity requirements (supporting the previously mentioned use cases) in a fully deployed smart factory. The share of each type of connected device[2] depends on whether the site has a low or high level of automation[3]. Evolving to a higher level of automation will increasingly lead to a higher share of 5G connected devices. Both high bandwidth and consistently low latency are necessary to support large data volumes and real-time critical data, as well as to ensure consistent and secure communication [20].

This requires change in IoT digital infrastructures. According to Gartner, for example, 80 percent of enterprises will have shut down their traditional data centre by 2025, versus 10 percent in 2018. Workload placement, which is driven by a variety of business needs, is the key driver of this infrastructure evolution. In this context, edge computing sits at the peak of Gartner's 2018 Hype Cycle for Cloud Computing and there is plenty of scope for false starts and disillusionment before standards and best practices are settled upon, and mainstream adoption can proceed. Edge computing delivers the decentralized complement to today's hyperscale cloud and legacy data centres. To maximize application potential and user experience, technology innovation leaders plan distributed computing solutions along a continuum from the core to the edge.

[1] Average number based on data from different manufacturing sites. In dense areas, the connection density could be up to one connected device per square metre.

[2] The exact distribution figures for a specific manufacturing site depend on the communication needs.

[3] The level of automation is a continuum from manual to fully automatic operations.

According to business-to-business (B2B) analysts MarketsandMarkets, the edge computing market will be worth $6.72 billion by 2022, up from an estimated $1.47 bn in 2017 – a Compound Annual Growth Rate (CAGR) of 35.4 per cent. Key driving factors are the advent of IoT and 5G networks, an increase in the number of “intelligent” applications and the growing load on cloud infrastructure. Among the vertical segments considered by MarketsandMarkets, Telecom and IT are expected to have the biggest market share during the 2017–2022 forecast period. That’s because enterprises faced with high network load and increasing demand for bandwidth will need to optimize and extend their Radio Access Network (RAN) to deliver an efficient Mobile (or Multi-access) Edge Computing (MEC) environment for their apps and services. The fastest-growing segment of the edge computing market during the forecast period, says MarketsandMarkets, is likely to be retail: high volumes of data generated by IoT sensors, cameras and beacons that feed into smart applications will be more efficiently collected, stored and processed at the network edge, rather than in the cloud or an on-premises data centre [19].

The use of intelligent edge devices requires reducing the amount of data sent to the cloud through quality filtering and aggregation, while the integration of more functions into intelligent devices and gateways closer to the edge reduces latency. By moving intelligence to the edge, local devices can generate value and optimise the processing of information and communication. This allows for protocol consolidation by controlling the various ways devices can communicate with each other. There are different edge computing paradigms, such as transparent computing, fog computing and mobile edge computing (MEC). MEC emerged in the context of 5G architectures and enables an open RAN as well as being able to host third party applications and content at the edge of the network. Fog computing, fog networking or fogging is a decentralized computing infrastructure in which data, processing, storage and applications are distributed in the most logical, efficient place between the data source and the cloud. Fog computing extends cloud computing and services to the edge of the network, bringing the advantages and power of the cloud closer to where information is created and acted upon. In a fog environment, intelligence is in the local area network. Information is transmitted from endpoints to a gateway, where it is then transmitted to sources for processing and return transmission. In edge computing, intelligence and power of the edge gateway or appliance are in devices such as programmable automation controllers. Edge computing allows the reduction of points of failure, as each edge device operates independently and determines which information to store locally and which to send to the cloud for further analysis. Fog computing is scalable and offers a view of the network as multiple data points feed information into it. Fog computing enables high-performance, interoperability and security in a multi-vendor computing-based ecosystem and is focusing on resource allocation at 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. One more difference compared to MEC is the need to support exotic I/O and accelerator aware provisioning, real-time, embedded targets as well as real-time networks such as Time Sensitive Networks (TSN), e.g., IEEE 802.1. Another edge computing technology is represented by CMU's Cloudlet, which enables new classes of mobile applications that are both compute-intensive and latency-sensitive in an open ecosystem based on cloudlets. The Cloudlets have lately been transformed to Open Edge Computing[4] based on OpenStack[5]. Open Edge Computing has the vision that any edge node will offer computational and storage resources to any user in close proximity using a standardized mechanism. Edge computing technologies are characterized by openness, as operators open the networks to third parties to deploy applications and services, while their differences enable edge computing technologies to support broader IoT applications with various requirements.

The connectivity requirements of the manufacturing industry are matched by the capabilities of cellular networks. To enable smart manufacturing, there are different network deployment options depending on the case-by-case needs and the digitisation ambitions of the factory. One option is using virtualization and Dedicated Core Networks (DECOR) to map local private networks and virtual networks running within a mobile operator's public network. A 4G and 5G network with dedicated radio base stations and Evolved Packet Core in-a-box can be deployed on the premises to ensure that traffic stays local to the site. In this case, on-premises cellular network deployment with local data breakout ensures that critical production data do not leave the premises, using Quality of Service (QoS) mechanisms to fulfil use case requirements and optimize reliability and latency. Critical applications can be executed locally, independent of the macro network, using cellular network deployment with edge computing [20].

[4] http://openedgecomputing.org/

[5] https://www.openstack.org/

The Multi-access Edge Computing (MEC) standard is developed in the ETSI Industry Specification Group/ISG Multi-access Edge Computing (ETSI ISG MEC) [96]. The ETSI ISG MEC is the leading voice in standardization and industry alignment concerning MEC. It is a key building block in the evolution of mobile-broadband networks, complementing Network Function Virtualisation (NFV) and Software Defined Network (SDN), and is:

- A key enabler for IoT and mission-critical, vertical solutions
- Widely recognized as one of the key architectural concepts and technologies for 5G
- Able to enable many 5G use cases without a full 5G roll-out (i.e. with 4G networks)
- Enabling a myriad of new use cases across multiple sectors as well as innovative business opportunities.

The ETSI ISG MEC work on Phase 2 is extending the applicability of MEC technology and rendering MEC even more attractive to operators, vendors and application developers.

One example of deployment is the Cloud IoT Edge that extends Google Cloud's data processing and machine learning to edge devices (e.g., robotic arms, wind turbines, oil rigs, etc.) so they can act on the data from their sensors in real-time and predict outcomes locally. Cloud IoT Edge can run on Android Things or Linux-based operating systems. It is composed of two runtime components, Edge IoT Core and Edge ML, and takes advantage of Google's purpose-built hardware accelerator ASIC chip, Edge TPU$^{\text{TM}}$. The Edge TPU is a purpose-built small-footprint ASIC chip designed to run TensorFlow Lite machine-learning models on edge devices. Cloud IoT Edge is the software stack that extends Google's cloud services to IoT gateways and edge devices. Cloud IoT Edge a runtime component for gateway-class devices (with at least one CPU) to store, translate, process and extract intelligence from edge data, while interoperating with the rest of Google's Cloud IoT platform (see Figure 3.9) [21].

Computing at the edge of the mobile network defines IoT-enabled customer experiences and requires a resilient and robust underlying network infrastructure 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 uses the power of local computing and different types of 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.). Edge computing advantages, such as improved scalability, local

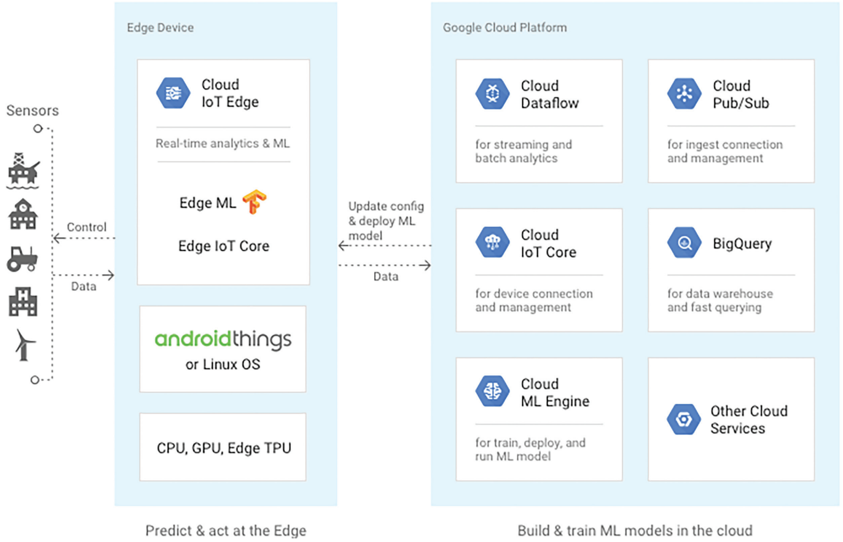

Edge Device
Google Cloud Platform
Sensors
Cloud IoT Edge
Real-time analytics & ML
Edge ML
Edge IoT Core
androidthings or Linux OS
CPU, GPU, Edge TPU
Control
Data
Update config & deploy ML model
Data
Cloud Dataflow
for streaming and batch analytics
Cloud Pub/Sub
for ingest connection and management
Cloud IoT Core
for device connection and management
BigQuery
for data warehouse and fast querying
Cloud ML Engine
for train, deploy, and run ML model
Other Cloud Services
Predict & act at the Edge
Build & train ML models in the cloud

Figure 3.9 How Cloud IoT Edge works [21].

processing, contextual computing and analytics, make it well suited to IoT application requirements. Edge computing technologies like MEC – offering low latency, proximity, high bandwidth, real-time insight into radio network information and location awareness – enable the development of many new types of IoT applications and services for industrial sectors. Augmented Reality (AR) mobile applications have inherent collaborative properties in terms of data collection in the uplink, computing at the edge and data delivery in the downlink [17].

AR information requires low latency and a high rate of data processing in order to provide correct information depending on the location of the device. The processing of information can be performed on a local MEC server instead of a centralized server to provide the user experience required. IoT devices generate additional messaging on telecommunication networks and require gateways to aggregate messages and ensure low latency and security. An architecture used for leveraging MEC to collect, classify and analyse the IoT data streams is presented in [18]. The MEC server manages different protocols and distribution of messages and processes the analytics. The MEC environment supports the creation of new value chains and new type of ecosystems, which provide new opportunities for mobile operators and application and content providers.

Information transmission costs and latency limitations of mobile connectivity pose challenges to many IoT applications that rely on cloud computing. Mobile edge computing enables IoT applications to deliver real-time and context-based mobile moments to users of IoT solutions, while managing the cost base for mobile infrastructure. The benefits are improved performance, deployment of intelligence and analytics at the edge, reduced overload of the communication networks, low latency, compliance, satisfaction of concerns related to data privacy and data security and reduced operational costs. Several challenges listed below, however, have to be addressed when considering edge-computing implementations [91]:

- 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 is closer to their actual users.
- Mobile edge computing implementation and integration pose the challenge of providing a distributed architecture with improved robustness, reliability and local intelligence, as well as processing that enables the autonomous execution of processes, rules and algorithms.
- 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.
- The need to optimize and reduce connectivity, data migration and bandwidths costs associated with sending data to the cloud, while implementing local intelligence, processing and distributed storage.
- Edge computing solutions for avoiding intermittent connectivity, low bandwidth and/or high latency at the network edge considering the increased numbers of smart edge devices running software for machine learning or AI software
- Optimization of the communication with nodes in the intervening edge computing infrastructure.

Regarding future IoT applications, it is expected that more of the network intelligence will reside closer to the source. This will push for the rise of edge cloud/fog and MEC-distributed architectures, as most data will be too noisy, latency-sensitive or expensive to be transferred to the cloud. Edge computing technologies for IoT require developers 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 IoT applications. The edge computing model requires a distributed architecture and needs to support various interactions and communication approaches to be used broader in consumer/business/industrial domains. To do this, it needs to provide peer-to-peer networking, edge-device collaboration (self-organizing, self-aware, self-healing, etc.), distributed queries across data stored in edge devices as well as in the cloud and temporary storage locations, distributed data management, (e.g., for defining where, what, when and how long, in relation to data storage) and information governance (e.g., information quality, discovery, usability, privacy, security, etc.). In this context, the research challenges in this area are:

- Open distributed edge computing architectures and implementations for IoT and IIoT (IT/OT convergence for IoT applications as traditionally the operational technologies (OT) used to manage and automate industrial equipment are placed at the edge of the network, while information technologies (IT) are more centralized).
- Integrated IoT distributed architecture for IT/OT integration to be used with new business models needed for interpreting or contextualizing IoT data for decision-making, while leveraging integrated data and standard processes to drive outcomes.
- Modelling and performance analysis for edge computing in IoT.
- Built-in end-to-end distributed security at every level of the architecture, in addition to mechanisms for monitoring and managing computing and networking endpoints for IoT systems.
- Heterogeneous wireless communication and networking in edge computing for IoT to handle multiple connectivity solutions using different protocols. Providing different orchestration solutions (e.g., operating both vertically and horizontally with vertical orchestrators to handle services in a specific domain, while horizontal orchestrators manage services across different domains providing integration among them) for edge computing to implement a platform to support both IT and OT activities in IIoT.
- Orchestration techniques for providing compute resources in separate islands, where it is possible to process information and provide services at the local level for a period of time without a coordinate computation and communication.
- Resource allocation and energy efficiency in edge computing for IoT.

- QoS and quality of experience (QoE) provisioning in edge computing for IoT.
- Trustworthiness distributed end-to-end security and privacy issues in edge computing for IoT.
- Federation and cross-platform service supply in transparent computing for IoT.

3.3.2 Artificial Intelligence

Artificial intelligence concerns activity devoted to making machines intelligent, with intelligence understood as a quality that enables an entity to function appropriately and with foresight in its environment [43].

Intelligent IoT devices are considered intelligent machines, while the collective attributes of a machine (i.e., computer, robot or other device) capable of performing functions, such as learning, decision-making or other intelligent human behaviours, are defined as AI. IoT-based sensor data generated in healthcare, bioinformatics, information sciences and policy- and decision- making in governments and enterprises can be processed using methods that rely on AI to provide new data insights and generate new types of knowledge. The benefits of both AI and the IoT can be expanded when the technologies are combined, both on the edge devices' end and core servers' end. AI machine-learning methods can obtain insights from the data to analyse and predict the future connections of IoT devices in advance.

AI is playing a starring role in the IoT because of its ability to quickly bring insights from data. ML offers the ability to automatically identify patterns and detect anomalies in the data that smart sensors and devices generate: information such as temperature, pressure, humidity, air quality, vibration and sound.

Companies are finding that machine learning can provide significant advantages over traditional business intelligence tools for analysing IoT data, including being able to make operational predictions up to 20 times sooner and with greater accuracy than threshold-based monitoring systems [25].

AI techniques extend machine learning strategies that can be applied to intelligent IoT devices for complex decisions based on detecting patterns, self-learning, self-healing, context-awareness and autonomous decision-making. These will involve and affect the future implementations of digital twin models and continuous learning with roles in autonomous vehicles applications, the IoRT and predictive maintenance.

Democratized AI, defined as the possibility to put the AI techniques under the reach of everyone, is one of five trends, along with digitalized

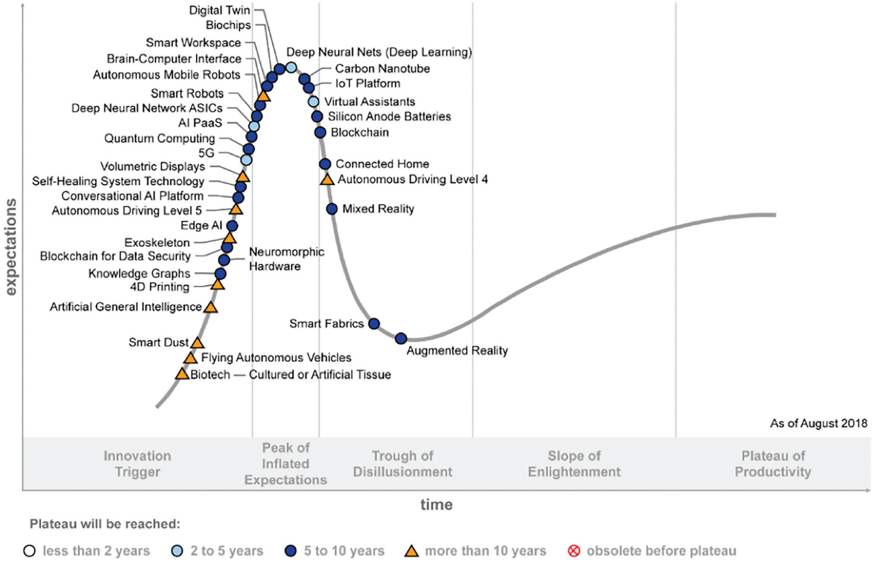


Figure 3.10 Gartner's Hype Cycle for emerging technologies 2018.

ecosystems, do-it-yourself biohacking, transparently immersive experiences and ubiquitous infrastructure, that is driving Gartner's latest Hype Cycle for emerging technologies (see Figure 3.10) [42], derived from 35 individual technologies.

The five trends blur the lines between human and machine with the AI group containing technologies such as AI platform as a service (PaaS), artificial general intelligence, autonomous driving (Levels 4 and 5), autonomous mobile robots, conversational AI platform, deep neural nets, flying autonomous vehicles, smart robots and virtual assistants.

The technologies enabling the next generation IoT are included under all five areas and comprise AI, edge AI, autonomous systems, blockchain, digital twins, augmented reality (AR), 5G, neuromorphic hardware and IoT platforms. The ubiquitous infrastructures of edge computing and the always-on, always-available, limitless infrastructure environment are enabling technologies that form the basis for the next generation IoT landscape.

When combined, AI and IoT transform both the Internet, the global economy and societal interactions. Within the next decade, it is expected that AI and machine learning to be embedded in various forms of technology that incorporate information exchange, analysis and knowledge.

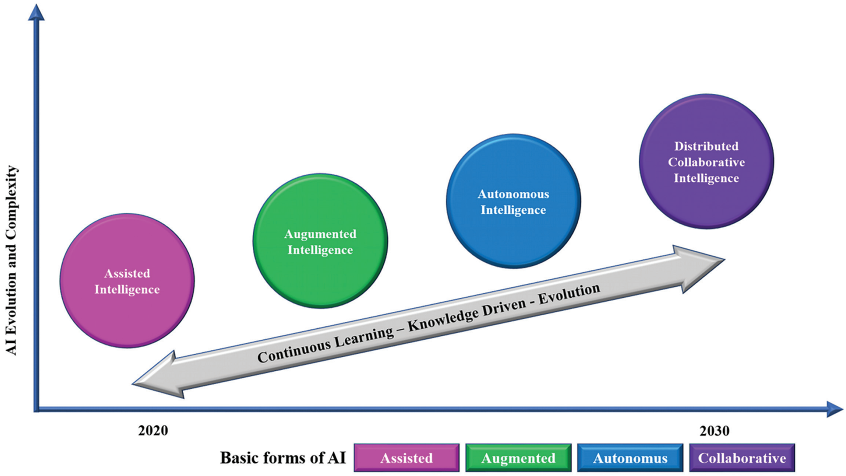


Figure 3.11 Artificial Intelligence Roadmap.

The opportunities created range from new services and breakthroughs in science, to the augmentation of human and machine intelligence and their convergence with the digital, virtual and cyber worlds. The future challenges related to the delegation of decision-making to machines and IoT autonomous systems, lack of transparency and whether technological change will outpace the development of governance and policy norms need to be addressed and solutions must be provided.

The evolution of basic forms of AI from assisted, augmented, autonomous to collaborative is illustrated in Figure 3.11.

In this context, the development of software and IoT devices capable of making ethical judgements as part of autonomous collaborative systems is emerging. As IoT autonomous systems are developing and combined with the ubiquity of AI in applications, such as the Internet of Vehicles for driverless vehicles, artificial ethical agents could become a legal necessity.

The combined developments in AI and the IoT enable new ways of interacting with connected objects through voice or gesture, while AR and virtual reality (VR) are powered by data generated by the IoT. Sensor/actuator technologies, the IoT, AI and increased connectivity bandwidth (ubiquitous, reliable and secure connectivity) are pushing the development of the Tactile IoT based on the convergence of these technologies where the lines between the digital and the physical blur.

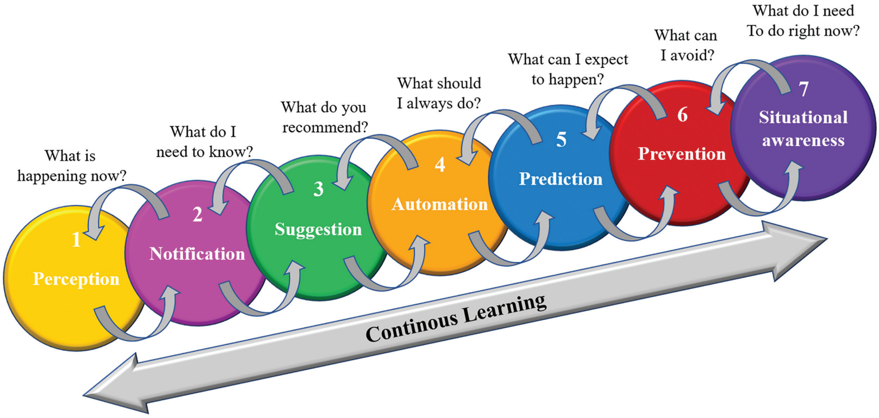


Figure 3.12 Outcomes of Artificial Intelligence.

Source: Constellation Research.

The disruptive nature of AI comes from the speed, precision, and capacity of augmenting humanity. When AI is defined through seven outcomes as presented in Figure 3.12, the business value of AI projects gain meaning and can easily show business value through a spectrum of outcomes [54, 55]:

- Perception describes what is happening now.
- Notification is a way of providing answers to questions through alerts, workflows, reminders and other signals that help deliver additional information through combined manual input and machine learning.
- Suggestion recommends action. This is built on past behaviours and modifications over time that are based on weighted attributes, decision management and machine learning.
- Automation repeats recurrent actions. It is leveraged as machine learning matures over time and tuning takes place.
- Prediction informs what to expect. It builds on deep learning and neural networks to anticipate and test for behaviours.
- Prevention helps avoid negative outcomes. It applies cognitive reckoning to identify potential threats.
- Situational awareness explains what must be known immediately. It resembles mimicking human capabilities in decision making.

AI methods to search for information in data and for learning from past and predict the future is illustrated in Figure 3.13.

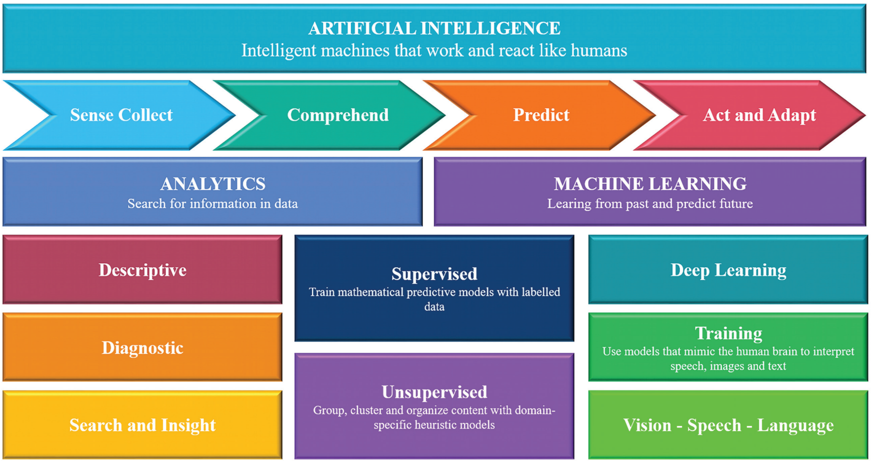
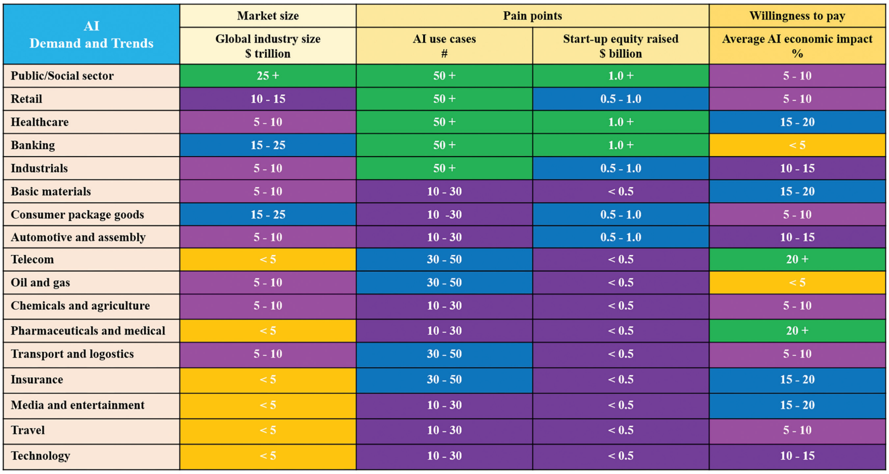

ARTIFICIAL INTELLIGENCE
Intelligent machines that work and react like humans
Sense Collect
Comprehend
Predict
Act and Adapt
ANALYTICS
Search for information in data
MACHINE LEARNING
Learing from past and predict future
Descriptive
Diagnostic
Search and Insight
Supervised
Train mathematical predictive models with labelled data
Unsupervised
Group, cluster and organize content with domain-specific heuristic models
Deep Learning
Training
Use models that mimic the human brain to interpret speech, images and text
Vision - Speech - Language

Figure 3.13 Artificial Intelligence methods.

Companies face a difficult task when deciding which opportunities to pursue, among the hundreds available, but they can narrow their options through a structured approach. The first step involves picking an industry and identifying the potential for disruption within the industry, which is estimated by looking at the number of AI use cases, start-up equity funding, and the total economic impact of AI, defined as the extent to which solutions reduced costs, increased productivity, or otherwise benefited the bottom line in a retrospective analysis of various applications. The greater the economic benefit, the more likely that customers will pay for an AI solution. Figure 3.14 shows the data compiled for 17 industries for AI-related metrics [46].

AI is a promising technological innovation, raising already high expectations for 2025. The IoT is the source of data for AI and machine learning applications, as fleets of connected IoT devices, autonomous vehicles and robots need to be automated to allow them to react to environmental conditions in real-time. By 2021, AI will support more than 80% of emerging technologies, while, in the following year, it will support more than 80% of enterprise IoT projects, according to Gartner. By 2020, it will create 2.3 million jobs, although 50% of organizations will lack the relevant AI and data talent.

While software has been a predominant factor in most corporate and investor interest for many years, hardware has become important again with the growth of AI. The cloud continues to be an option for various applications, not least due to its scale advantage, and the choice between cloud or edge



AI Demand and Trends	Market size	Pain points		Willingness to pay
	Global industry size $ trillion	AI use cases #	Start-up equity raised $ billion	Average AI economic impact %
Public/Social sector	25 +	50 +	1.0 +	5 - 10
Retail	10 - 15	50 +	0.5 - 1.0	5 - 10
Healthcare	5 - 10	50 +	1.0 +	15 - 20
Banking	15 - 25	50 +	1.0 +	< 5
Industrials	5 - 10	50 +	0.5 - 1.0	10 - 15
Basic materials	5 - 10	10 - 30	< 0.5	15 - 20
Consumer package goods	15 - 25	10 -30	0.5 - 1.0	5 - 10
Automotive and assembly	5 - 10	10 - 30	0.5 - 1.0	10 - 15
Telecom	< 5	30 - 50	< 0.5	20 +
Oil and gas	5 - 10	30 - 50	< 0.5	< 5
Chemicals and agriculture	5 - 10	10 - 30	< 0.5	5 - 10
Pharmaceuticals and medical	< 5	10 - 30	< 0.5	20 +
Transport and logostics	5 - 10	30 - 50	< 0.5	5 - 10
Insurance	< 5	30 - 50	< 0.5	15 - 20
Media and entertainment	< 5	10 - 30	< 0.5	15 - 20
Travel	< 5	10 - 30	< 0.5	5 - 10
Technology	< 5	10 - 30	< 0.5	10 - 15

Figure 3.14 AI dependency on market size, pain points, and willingness to pay across different industries.

Source: Adapted from McKinsey & Company, [46].

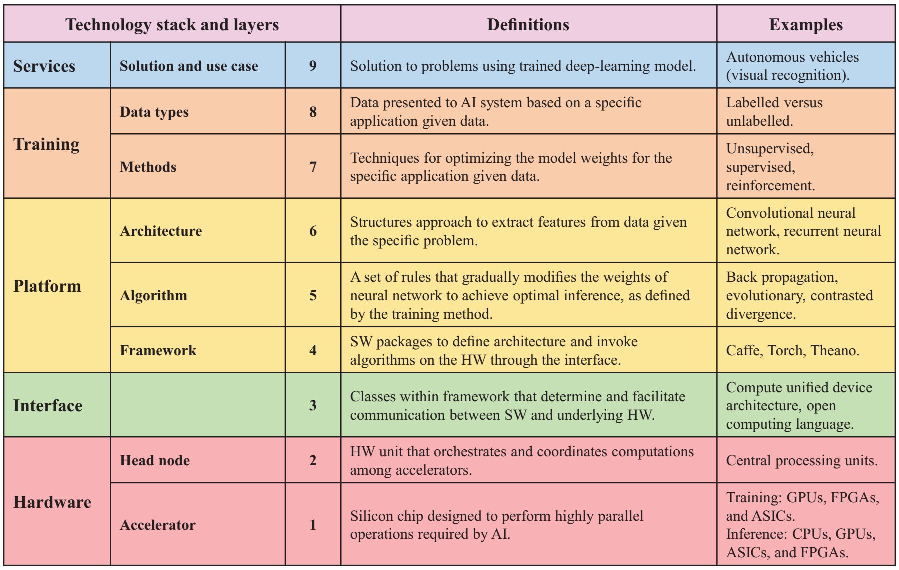
solutions will depend on the IoT use cases and applications. Regarding cloud hardware, the market remains fragmented. The hardware preference of customers and suppliers vary for application-specific integrated circuit (ASIC) technology and graphics processing units (GPUs).

The low latency connectivity at the edge is critical, driving the current development and growing role for inference at the edge. ASICs — with their superior performance per watt — provide a more optimized user experience, including lower power consumption and higher processing, for many applications. Enterprise edge is covered by several technologies, such as field programmable gate arrays, GPUs and ASIC technology.

The ML and DL technology stack is divided into nine layers [46], across services, training, platform, interface, and hardware as presented in Figure 3.15.

Despite rather old technological foundations, in recent years, machine learning has brought about important progress for applications such as computer vision or natural language processing.

It has also recently attracted sizeable investments with an explosion in VC money and a growing focus (through buy outs and investments) amongst Internet companies. The key AI innovations are presented Figure 3.16.



Technology stack and layers			Definitions	Examples
Services	**Solution and use case**	**9**	Solution to problems using trained deep-learning model.	Autonomous vehicles (visual recognition).
Training	**Data types**	**8**	Data presented to AI system based on a specific application given data.	Labelled versus unlabelled.
	Methods	**7**	Techniques for optimizing the model weights for the specific application given data.	Unsupervised, supervised, reinforcement.
Platform	**Architecture**	**6**	Structures approach to extract features from data given the specific problem.	Convolutional neural network, recurrent neural network.
	Algorithm	**5**	A set of rules that gradually modifies the weights of neural network to achieve optimal inference, as defined by the training method.	Back propagation, evolutionary, contrasted divergence.
	Framework	**4**	SW packages to define architecture and invoke algorithms on the HW through the interface.	Caffe, Torch, Theano.
Interface		**3**	Classes within framework that determine and facilitate communication between SW and underlying HW.	Compute unified device architecture, open computing language.
Hardware	**Head node**	**2**	HW unit that orchestrates and coordinates computations among accelerators.	Central processing units.
	Accelerator	**1**	Silicon chip designed to perform highly parallel operations required by AI.	Training: GPUs, FPGAs, and ASICs. Inference: CPUs, GPUs, ASICs, and FPGAs.

CPU - Central processing unit; GPU - Graphic processing unit; FPGA - Field-programmable gate arrays; ASIC - Application-specific integrated circuit

Figure 3.15 Machine Learning (ML) and Deep Learning (DL) technology multi-layered stack.

Source: Adapted from McKinsey & Company, [46].

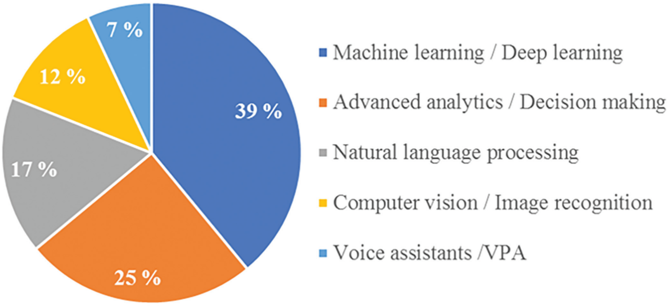


Figure 3.16 Key AI innovations according to the IDATE Technology 2025 survey.

Source: IDATE DigiWorld.

The most anticipated AI applications for 2025 move beyond the current focus on language and vision by targeting advanced data analytics capacities and enabling decision-making applications.

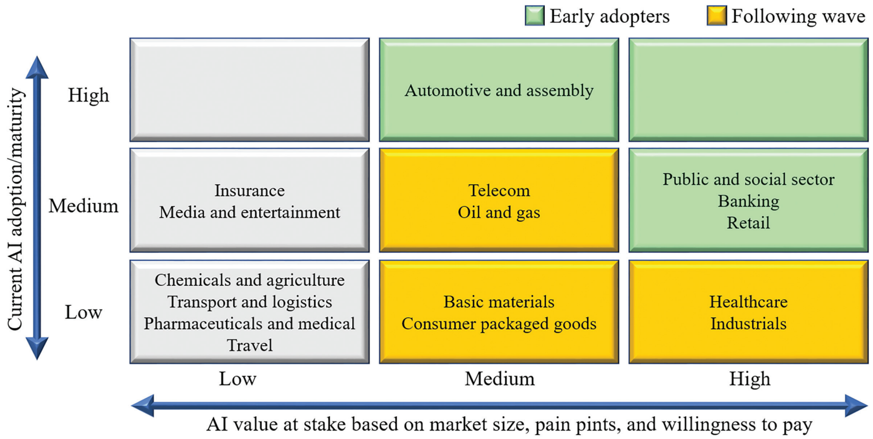
Unprecedented abilities in Data Analytics

If computers are starting to catch up with humans in their ability to detect objects in images, applying deep learning to a field where algorithms are already ahead of most humans, such as data analytics, promises potentially momentous breakthroughs.

Applying deep learning to data analytics enables complex pattern recognition and prediction. This is especially noteworthy in the case of "unsupervised training" machine learning, that is, when the algorithm is fed with unstructured data and tries to spot interesting patterns on its own.

Several industries offer the strongest opportunities for AI: public sector, banking, retail, and automotive as presented in Figure 3.17. While the public sector's prominence may seem surprising in an age where governments are cutting budgets, many officials see the value of AI in improving efficiency and efficacy, and they are willing to provide funding. As they plan their AI strategies, suppliers may focus their investments on potential consumers of AI solutions who are willing to be the first domino [46].

An important domain concerning the application of deep learning data analytics is the health sector. Using deep learning approaches can help in health record data analysis to improve diagnostics, risk analysis and preventive medication.


🟩 Early adopters
🟨 Following wave
Current AI adoption/maturity
AI value at stake based on market size, pain pints, and willingness to pay

	Low	Medium	High
High		Automotive and assembly	
Medium	Insurance Media and entertainment	Telecom Oil and gas	Public and social sector Banking Retail
Low	Chemicals and agriculture Transport and logistics Pharmaceuticals and medical Travel	Basic materials Consumer packaged goods	Healthcare Industrials

Prioritisation made based on industry attractiveness, AI adoption/maturity and value at stake

Figure 3.17 AI adoption/maturity vs. value at stake.

Source: Adapted from McKinsey & Company, [46].

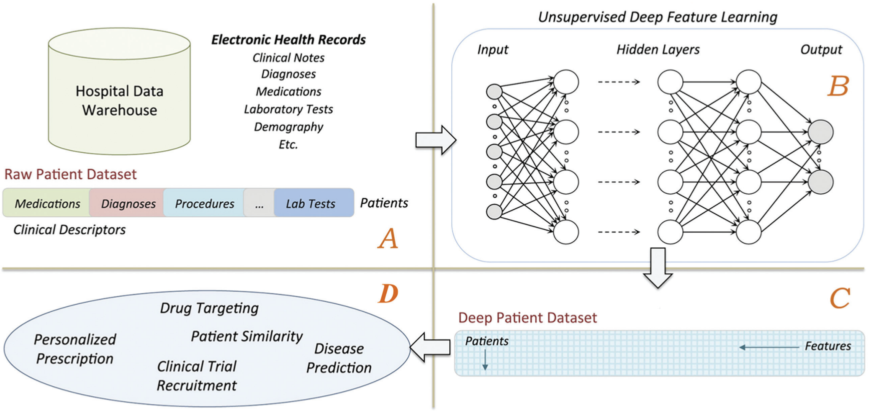


Figure 3.18 Use of unstructured deep learning in the analysis of hospital patient data.
Source: Nature/Mount Sinai Hospital.

Examples of health applications include reconstructing brain circuits, predicting the activity of potential drug molecules or predicting the effects of mutations in non-coding DNA on gene expressions.

The Mount Sinai Hospital (see Figure 3.18) recently highlighted the potential for using unstructured deep learning in the secondary use of electronic health records in order to predict health status, as well as to help prevent disease or disability.

The interest in deep learning approaches is especially strong in the case of traditional data analysis methodologies, which have been applied with limited success, as it can improve prediction results.

The IoT as Key Data provider for AI

Access to relevant data sets (often derived from vertical industries) in order to train the deep learning algorithms will be critical. The development of the IoT can play a critical role in providing access to the relevant data sets for training future AI including the digital twin models.

Shrinking computer chips and improved manufacturing techniques have led to cheaper and more powerful sensors. As the number of sensors employed in IoT ecosystems increases rapidly, so do the amounts of raw data produced, in turn calling for new computational models to handle this by employing intelligence at the edge for information processing. The new computational models need to cope not only with larger quantities but also with increased complexity of the raw data in terms of their syntax and semantics. Machine learning and deep learning are able to collect and process data from billions of sensors.

Algorithmic developments in AI are coupled with increased data resources and computational demands that are served mainly today by cloud infrastructures. New developments to address AI algorithms for processing data at the edge are underway. Despite the rapid advances of AI in vision, speech recognition, natural language processing and dialog, there is still room for improvement when developing end-to-end intelligent systems that must encapsulate multiple competencies and deliver services in real-time using limited resources. In this direction, the developments are focusing on designing and delivering embedded and hierarchical AI solutions in the combined IoT/IIoT, edge and cloud computing environments that provide real-time decisions, using less data and computational resources, while orchestrating the access to each type of resource in a way that enhances the accuracy and performance of the models. The distributed AI concept builds on top of a hierarchy where low-level, context-agnostic models, which run on the IoT and on IoT devices, can dynamically feed higher-order models running on higher-capacity resources, so as to better capture the context knowledge. Due to the adoption of AI methods and techniques making use of a wide range of available resources (IoT/IIoT/edge/cloud), IoT applications are now able to offer a trade-off between accuracy and performance, depending on the overall requirements.

Complex IoT applications allow distributed intelligence embedded in limited resource sensors at the edge of the network, providing an effective demonstrator of the potential of AI as a service model. There is a need to identify AI and machine learning (ML) methodologies for temporal data to build distributed learning systems that can scale from the IoT/IIoT to edge and cloud resources.

The development of connected vehicles, smart cities and connected health are especially likely to provide access to the massive amounts of data required by deep learning approaches. However, other domains of IoT deployments, such as the industrial Internet are increasingly generating data sets that could fit the deep learning approach. The number of data points that manufacturing facilities generate and the ability to find correlations and pattern and recommend decisions among these IoT data could be addressed by deep learning or other AI methods approaches.

AI and IoT/IIoT requirements for complex integrated systems

In complex IoT applications, the same conditions will seldom apply twice to the same situation, even when they involve the same process; the context and the operation conditions in a specific environment, such as the stress and fatigue of the equipment, always contribute to the creation of an entirely new set of input values for the model. To cope with this expected richness of the model, feedback and training data need to be requested continuously and by a multitude of manufacturing equipment, resulting in a default global (and hence, cross-border) AI model. Deep learning approaches can aggregate the underlying model inputs and gradually build the necessary user and context profiles, but the models (low and higher order) need to continuously adapt to the influx of new data.

A multi-parametric model of manufacturing equipment profiles requires the federation of a multitude of underlying models and data (functional, behavioural, environment, operational, informational, etc.), orchestrated in a distributed and decentralized fashion so as to ensure that the evaluation is happening close to the data sources (ensuring real-time reactions) in an efficient and collaborative fashion.

Thus, the applications across industrial sectors integrating AI and IoT need to address a multitude of requirements in order to fulfil the integration of functional and non-functional attributes for such complex systems. The requirements for complex IoT/IIoT systems that have embedded artificial intelligence (AI) techniques and methods can be summarized as presented in Figure 3.19 and the following list:

Explainability: Enables human users to understand the decisions made by AI systems and the rationale behind them. This ability will make it easier to track down eventual failures and assess decisions' strengths and weaknesses. Ultimately, this will increase the trust in the systems' decisions. This ability will have to integrate with human-computer interface techniques which are able to track complex reasoning processes.

Availability: Enables IoT applications to provide data and resources in a timely manner for a set percentage of time (i.e., the uptime) as well as retain their core functionality, even if the system has undergone a security attack. Industrial IoT applications may target mission-critical tasks along the production line; system outages will therefore have direct economic impact. In the near future, it is also envisaged that IoT systems, due to embedded AI, will be able to perform autonomously via online learning over their lifetime and remove even the downtime needed for maintenance. AI systems should be available in terms of integration into new applications and process steps.

Trustworthiness: Enables IoT systems to be trusted, only allowing authenticated devices or services that can be uniquely identified to participate in the decision-making processes of the system. This makes it possible to report

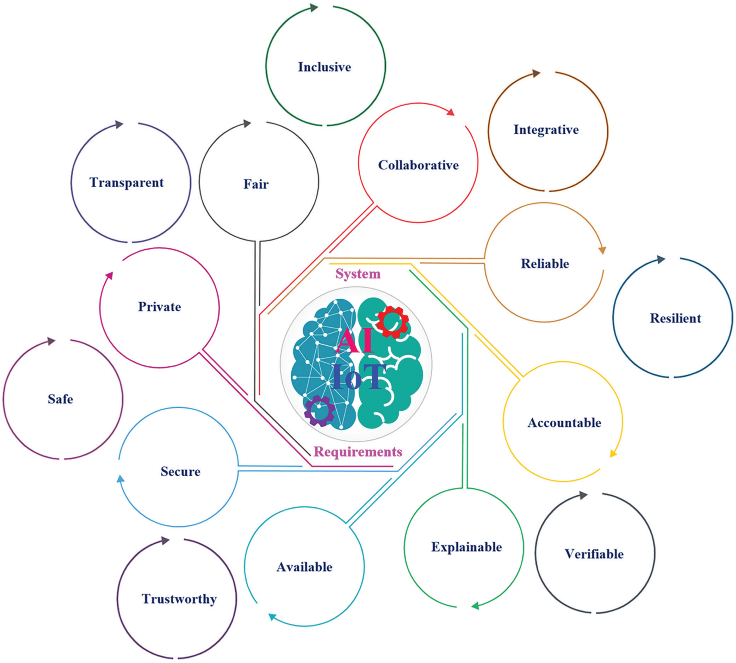


Figure 3.19 AI and IoT/IIoT requirements for complex system integrated systems.

the source of vulnerabilities and inconsistencies. As more and more AI-enabled systems become connected through the IoT, trustworthiness becomes an indispensable requirement. Precisely due to the AI, trustworthiness will become multi-dimensional, far beyond verifying identity. Consequently, trust will no longer be 'true' or 'false', but rather about degrees of trustworthiness that will control the access levels of devices/users to critical services.

Security: Enables systems to guarantee distributed end-to-end security, which is essential to ensure robustness against all types of attack vectors in the IoT. This includes securing the AI system itself as well as securing communication between edge computing IoT devices with encryption and authentication mechanisms against attacks with manipulated input data.

Safety: Enables systems to protect persons and objects during operation. AI systems that operate physically next to and collaboratively with humans through robots or other machines must not exhibit random or unpredictable behaviour. Safety by design is essential, entailing compliance with relevant safety standards. Importantly, the employed AI and IoT systems must be robust against implausible data and operate with extremely low latency to quickly and appropriately react to unforeseen events (i.e., to prevent accidents).

Privacy: Enables IoT and AI-based systems that operate on mission- and business-critical data to keep this data private. This entails both limiting access to and placing restrictions on certain types of information with the goal of preventing unauthorized access (confidentiality) as well as protecting data from being modified or corrupted without detection. Such data must therefore be processed locally at the edge and only leverage data available within privacy limits (smart data).

Transparency: Enables IoT and AI-based systems to provide insight into devices and processes in situations such as auditing, inspections to assess vulnerabilities, or when security breaches arise. This may be supported by digital twins that represent the complete system state at any point in time.

AI methods for data visualization can further enhance transparency and contribute to making the systems state easier to understand.

Fairness: Enables IoT systems which embed AI technologies to support or automate decision processes while adhering to the same fairness and compliance standards as humans.

Inclusiveness: Enables AI-based IoT systems to allow human intervention even in the most automated decision and communication processes. This is essential to avoid the formation of isolated non-AI capable sub-systems within a process, production system or supply chain.

Collaboration: Enables AI-based IoT systems to self-organize around a common goal; for example, in the presence of a threat, as well as to collaborate with humans, both physically (e.g., human-robot collaboration) and by exchanging information (human-machine interfaces). Collaboration is an emergent property of complex interactions and dynamics, increasingly present in industry. Industry-grade AI will not be concentrated on a single device or system. Instead, many different AI-enabled subsystems will be distributed (distributed AI) across IoT nodes, embedded devices and other edge devices (embedded AI).

Integration: Enables IoT-embedding AI systems to exhibit an open and flexible perspective by consolidating insights from all existing systems and processes. Bridging possible gaps is a key prerequisite of the establishing AI methods in the industry according to a sustainable roadmap.

Reliability: Enables IoT systems to operate without systems outages and regular human intervention. Reliability is essential for productivity and is a key prerequisite for AI systems that are put into continuous operation with short maintenance time in mission-critical production environments.

Resiliency: Enables IoT with embedded AI to always operate in stable states, including to return to such states after failures. Resilience is essential for their safe support for our digital economy. In the future, they should even be able to detect failure and initiate measures for compensating it.

Accountability: Enables IoT systems with embedded AI systems that support or even replace human decisions to be accountable to their customers, partners and regulators. Normally, accountability features will be integrated "by design" and will be available via the supplier of these systems.

Verifiability: Enables IoT and AI-based systems to demonstrate the functionality and properties they are supposed to have. AI systems for industrial applications must fulfil the same standards as legacy systems and will be applied to safety-, mission- and business-critical tasks. This requires that AI embedded systems can be validated (to reach correct results), verified (verifiable AI) and certified (certifiable AI) for the targeted applications.

The research challenges for implementing AI at the edge of networks for IoT applications are as follows:

- Mechanisms for collecting and aggregating data and information and developing edge models that generate insights from the data available in real-time by providing methods and techniques to train models in the edge environment with appropriately distributed storage capabilities
- 'AI-friendly' processors to address the AI workloads for IoT applications requiring AI computationally intensive capabilities; research and development concerning architectural concepts to shift central control to the edge and the use of modified graphics processor units, hybrid processors and AI-based processors, embedding accelerators and neural networks for processing specific AI algorithms
- New energy- and resource-efficient methods for image recognition and geospatial processing using AI at the edge, based on machine learning and other AI techniques
- Edge computing implementation based on neuromorphic computing and in-memory computing to process unstructured data, such as images or video, used in IoT applications

- Edge computing implementations based on distributed approaches for IoT computing systems at the edge
- Distributed IoT end-to-end security for AI-based solutions that process data at the edge using a group of edge nodes to work together on a particular task, thereby ensuring that no security holes or attacks are possible
- AI for smart data storage in edge-based IoT
- AI for software-defined networking in edge-based IoT
- Swarm intelligence algorithms for edge-based IoT/IIoT
- Machine learning, deep learning and multi-agent systems for edge-based IoT/IIoT
- Cognitive aspects of AI in edge-based IoT/IIoT
- Neural networks for AI in edge-based IoT/IIoT
- Distributed heterogeneous memory systems design for AI in edge-based IoT/IIoT

3.3.3 Networks and Communication

It is predicted that the adoption of low-power short-range networks for wireless IoT connectivity will increase through 2025 and will coexist with wide-area IoT networks [82], while 5G networks will deliver 1,000 to 5,000 times more capacity than 3G and 4G networks today. IoT technologies are extending known business models, leading to the proliferation of different ones as companies push beyond the data, analytics and intelligence boundaries. 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.

5G and the IoT promise new capabilities and use cases, which are set to impact not only consumer services but also many industries embarking on their digital transformations. New massive IoT cellular technologies, such as NB-IoT and Cat-M1, are taking off and driving growth in the number of cellular IoT connections, with a CAGR of 30 percent expected between 2017 and 2023. These complementary technologies support diverse LPWAN use cases over the same underlying LTE network [20].

3.3.3.1 Network technology – hyperconnectivity beyond 5G

The development of critical communication capabilities will be an essential enabler for the development of the IoT. It will enable IoT use cases to go beyond data collection and respond to complex scenarios requiring precise actuation, automation and mission critical communications.

The next generation technological enhancements to telecommunication networks, brought about by 5G, will allow new connectivity to become the catalyst for next generation IoT services by creating innovations such as advanced modulation schemes for wireless access, network slicing capabilities, automated network application lifecycle management, software- defined networking and network function virtualization, as well as providing support for edge- and cloud-optimized distributed network applications.

The requirements of critical IoT communications are numerous and diverse, ranging from the increased reliability and resilience of the communication network, to ultra-low latencies and high capacity, while also integrating the context of the mission with the ability to respond to strict energy efficiency constraints or to cover large outdoor areas, deep indoor environments or vehicles moving at high speeds. Bandwidth and delay for services enabled by legacy networks and 5G are presented in Figure 3.20.

Starting with LTE Advanced, cellular communication standards have begun responding to these requirements by developing new technologies.

These first developments are opening new possibilities, especially for public safety operations, but they are still limited in scope. They notably lack the ability to provide the ultra-low latencies required by many critical use cases.

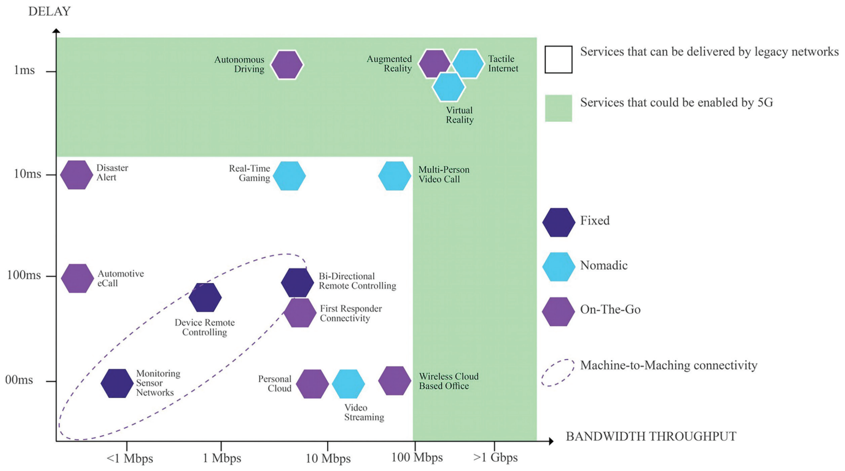


Figure 3.20 Bandwidth and delay for services enabled by legacy networks and 5G.

Source: Adapted from [95].

Table 3.1 Key critical IoT communications requirements

Requirements	Details
Reliability	High availability of the network Low packet losses
Resilience	Ability to function in degraded conditions Low convergence time
Energy efficiency	Projected lifespan of equipment batteries
Low latencies	End-to-end latencies of communication systems under 10 ms and sometimes inferior (under 5 ms or even under 1 ms).
Coverage	Coverage of very a large area (rural) Deep indoor coverage Coverage of moving vehicles Ability to deploy and use private networks
Security	Authentication of communications Encryption of communications Attack detections
Capacity	Ability of the network to operate with a very large number of users

Source: IDATE.

The development of 5G is seen as central to enabling critical IoT communications; indeed, many of the planned 5G features (from network slicing and massive multi-user multiple-input, multiple-output (MIMO) to new messaging services, cellular vehicles- to-everything or improved relay capabilities) represent highly important advances for critical scenarios, including reliable, low latencies. The critical IoT communications requirements are presented in Table 3.1.

End-to-end (E2E) network slicing is a foundation to support diversified 5G services and is key to 5G network architecture evolution. Based on Network Functions Virtualisation (NFV) and Software Defined Network (SDN), physical infrastructure of the future network architecture consists of sites and three-layer data centres (DCs). Sites support multiple modes (such as 5G, LTE, and Wi-Fi) in the form of macro, micro, and pico base stations to implement the RAN real-time function. These functions have high requirements for computing capability and real-time performance and require the inclusion of specific dedicated hardware. Three-layer cloud DC consists of computing and storage resources. The bottom layer is the central office DC, which is closest in relative proximity to the base station side. The second layer is the local DC, and the upper layer is the regional DC, with each layer of arranged DCs connected through transport networks. According to diversified service requirements, networks generate corresponding network topologies and a series of network function sets (network slices) for each corresponding service type using NFV on a unified physical infrastructure. Each network slice is derived from a unified physical network infrastructure, which greatly reduces subsequent operators' network construction costs. Network slices feature a logical arrangement and are separated as individual structures, which allows for heavily customizable service functions and independent operation and management [47].

Advanced ML and AI techniques can also be used for optimizing the connectivity of future mobile heterogeneous IoT devices to allow them to support efficiently a number of diverse services. ML techniques can be used to identify the optimal radio technology in mobile IoT devices considering the load and the services they support. Additionally, in future cognitive radio-based IoT devices, ML techniques can be used to optimize the spectrum channel and width, the devices will use and create a self-organizing network of cooperating devices to improve spectrum utilization [92–94].

As illustrated in Figure 3.21, Enhanced Mobile Broad Band (eMBB), Ultra Reliable Low Latency Communications (uRLLC), and Machine Type Communications (mMTC) are independently supported on a single physical infrastructure. eMBB slicing has high requirements for bandwidth to deploy cache in the mobile cloud engine of a local DC, which provides high-speed services located in close proximity to users, reducing bandwidth requirements of backbone networks. uRLLC slicing has strict latency requirements in application scenarios of self-driving, assistant driving, and

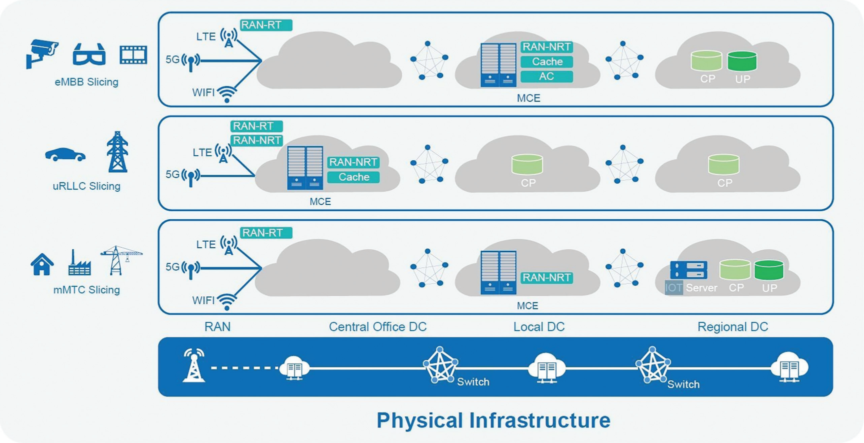


Figure 3.21 End-to-End Network Slicing for Multiple Industries Based on One Physical Infrastructure [47].

remote management. RAN Real-Time and non-Real-Time processing function units must be deployed on the site side providing a beneficial location preferably based in close proximity to users. Vehicle-to-Everything (V2X) server and service gateways must be deployed in the mobile cloud engine of the central office DC, with only control-plane functions deployed in the local and regional DCs. mMTC slicing involves a small amount of network data interaction and a low frequency of signalling interaction in most MTC scenarios. This consequently allows the mobile cloud engine to be deployed in the local DC, and other additional functions and application servers can be deployed in the regional DC, which releases central office resources and reduces operating expenses [47].

Highly dependent upon both the creation of new technologies and the deployment of new communication networks (requiring both important investments all along the value chain), critical IoT capabilities are unlikely to be largely available before 2025.

The 5G spectrum high bands are expected to be deployed include the 28 GHz band, as well as the 26 GHz, 37 GHz and 39 GHz bands. The 28 GHz band may be used in certain countries by the end of 2018 or early 2019, while the other high bands are estimated to be available in late 2019. Low bands below 1 GHz are of interest due to their favourable radio wave propagation characteristics, as they provide coverage in remote areas and into buildings. A new band in the 600 MHz range is expected to be made available by the end of 2018 for 5G services. Part of the mid-bands between 1 GHz and 7 GHz are expected to be allocated in several countries. Mid-bands within the 3.3 GHz to 5 GHz range will likely be made available around 2020 and are seen as important spectrum resources for terrestrial 5G access networks. The midbands are particularly beneficial as they offer a favourable "middle ground" between propagation characteristics (coverage) and bandwidth (capacity). There are several spectrum bands already in use by service providers. In general, all the current 3GPP bands including low bands (600 MHz, 700 MHz, 800 MHz, 850 MHz and 900 MHz) and mid-bands (1.5 GHz, 1.7 GHz, 1.8 GHz, 1.9 GHz, 2.1 GHz, 2.3 GHz and 2.6 GHz) are being considered for 5G services in the future. These bands, and composite arrangements of these bands, will be central to delivering 5G coverage and capacity for enhanced mobile broadband, IoT, industrial automation and mission-critical business cases, as well as for Public Protection and Disaster Relief (PPDR) services. In addition, 3 GPP has recently started a separate Study Item to investigate the feasibility of using the 6.5 GHz band (5,925 MHz to 7,125 MHz) for 5G services [20]. Frequency ranges being studied

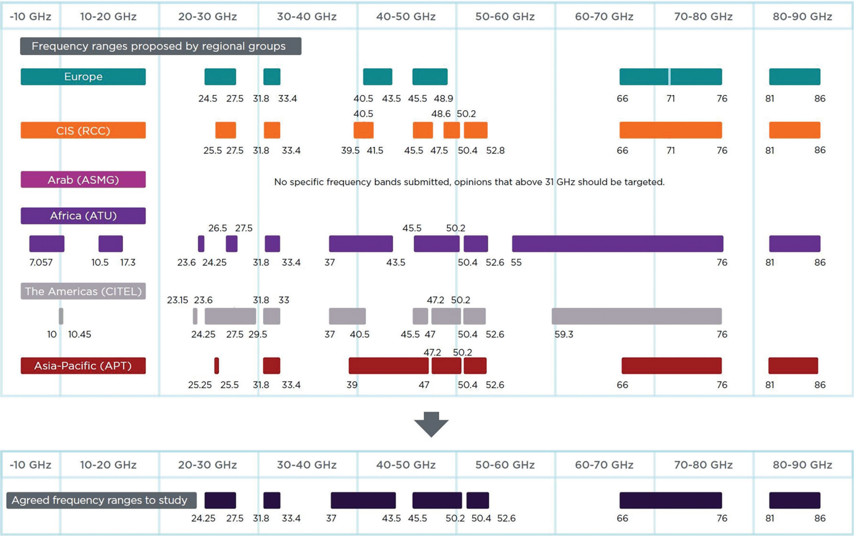


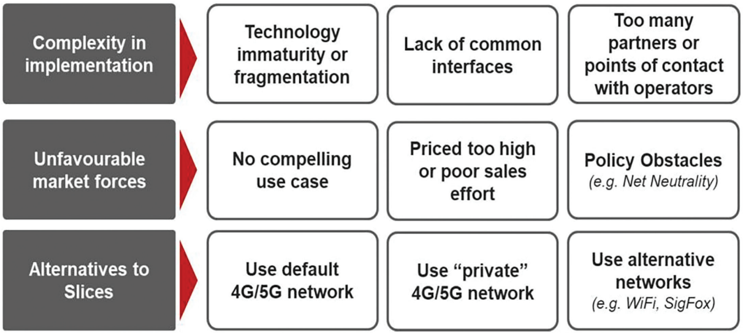
Figure 3.22 Frequency ranges being studied for identification at World Radio Communication Conference 2019 [95].

for identification at World Radio Communication Conference 2019 [95] are presented in Figure 3.22.

IoT applications, based on AR and VR, will revolutionize customer experience in gaming, retail shopping and other customer-centric applications. Consumer experience will be enhanced by high data rates, while extremely low latencies will be achieved.

However, these developments are of interest to many industries, including the automotive, manufacturing, health, energy and public service sectors. There are several factors that could impact commercial adoption of Network Slicing as presented in Figure 3.23. The adoption of Network Slicing influences the IoT applications and the selection of connectivity solutions. In this context, industry activities to standardise Network Slicing should focus on minimising the complexity of the technical solution so that adoption can be made relatively easy, the IoT use cases need to be defined to drive economies of scale and reduce unitary cost of deployment and the operators need to make the cost of deploying Network Slicing marginal to the broader investment case for 5G [49].

The development of a critical IoT is mainly a business-to-business (B2B) and business-to-business-to-consumer (B2B2C) demand, and strongly driven



Complexity in implementation	Technology immaturity or fragmentation	Lack of common interfaces	Too many partners or points of contact with operators
Unfavourable market forces	No compelling use case	Priced too high or poor sales effort	Policy Obstacles *(e.g. Net Neutrality)*
Alternatives to Slices	Use default 4G/5G network	Use "private" 4G/5G network	Use alternative networks *(e.g. WiFi, SigFox)*

Figure 3.23 Factors that could impact commercial adoption of Network Slicing [49].

by the digital transformation of vertical industries and expanding the traditional cellular technology development (which relies heavily on consumer brands).

The global market is thus limited in volume, with market estimates according to IDATE of about 60 million units by 2030; but this will be compensated by high average revenue per units (ARPUs) as the technology will respond to a critical demand in many industries in terms of generating important cost reductions and new revenue opportunities.

The leading market in volume will be the automotive sector, in which the development of the most advanced autonomous cars will use critical IoT capabilities to perform tasks, such as complex intersection control, dynamic area management, and cooperative cruise control and platooning. The automotive industry is already strongly involved in the standardization process of 5G with the set-up of the 5G Automotive Association (5GAA).

Other verticals of importance include connected health, in which critical IoT capabilities promise the generalization of teleoperations and robotics surgery. Manufacturing will also be strongly impacted, as critical IoT capabilities are among the building blocks of the smart factory (enabling advanced automation and remote control). The key requirements for critical IoT communications in different industrial sectors are presented in Table 3.2.

The 5G use cases can be realized to provide solutions in the B2C, B2B, B2B2X and IoT market segments. In B2C market, operators offer the services such as high definition video (TV, movies, streaming live sports) or home security solutions directly to the end consumers. In B2B market, operators offer the services such as mobility solutions and Cloud services to the businesses (SMEs, large corporations) where the services are typically consumed

Table 3.2 Vertical industrial sectors – key requirements for critical IoT communications

Verticals	Critical IoT Scenarios	Demand Strength	Key Requirements
Automotive	Automated cars	+++	Latency, reliability, coverage (large scale and mobility), point-to-point communication (V2V, V2I)
Health	Robotics	++	Latency, reliability, energy efficiency.
Industrial IoT	Automation, time-critical automation, remote control	++	Latency, reliability, coverage (deep indoor) point-to-point communication, Energy efficiency and local (private) deployments
Energy	Fault prevention and alert, grid backhaul network	++	Latency, reliability, point-to-point communication, large-scale coverage
Public safety	Mission-critical communications	++	Reliability, coverage, resilience, energy efficiency.
Agriculture, forestry, environment	Automation	+	Latency, reliability, energy efficiency, coverage of rural areas

Source: IDATE.

by the employees of the business. In B2B2X market, the services such as ‘In stadium’ high definition video service are offered to businesses like stadium operators and they in turn offer the service to their premium customers. In IoT market, operators can leverage the low latency, high reliability, high bandwidth and massive connections capabilities to offer several vertical industry use cases like connected vehicles, smart utilities and remote surgery types of applications by participating in the industry specific ecosystems and innovating new business models. Figure 3.24 illustrates the 5G applications market potential and readiness matrix presenting the connectivity and value-added services opportunities in different sectors [98].

International Mobile Telecommunications system requirements for the year 2020 mapped to 5G use cases [95] are presented in Figure 3.27. These promising prospects are attracting many actors to define their future role in the critical IoT market. The capabilities of 5G will indeed lead to more complex value chains with more actors providing connectivity and bundling

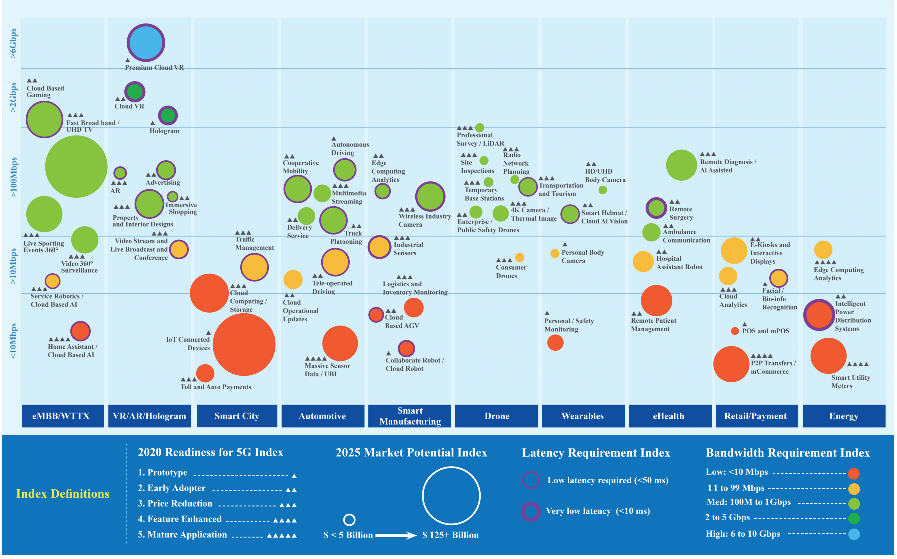


Figure 3.24 5G Applications Market Potential and Readiness Matrix [100].

connectivity with vertical specific services. It is seen by telecommunication companies as an opportunity to diversify and offer vertical specific services, but the rest of the value chain is also eager to benefit from new revenue streams: from equipment providers betting on small cell networks, to over-the-top (OTT) players looking over unlicensed networks or pure vertical players integrating connectivity in their new services. Figure 3.25 illustrates the use of 5G connectivity in different industrial application areas.

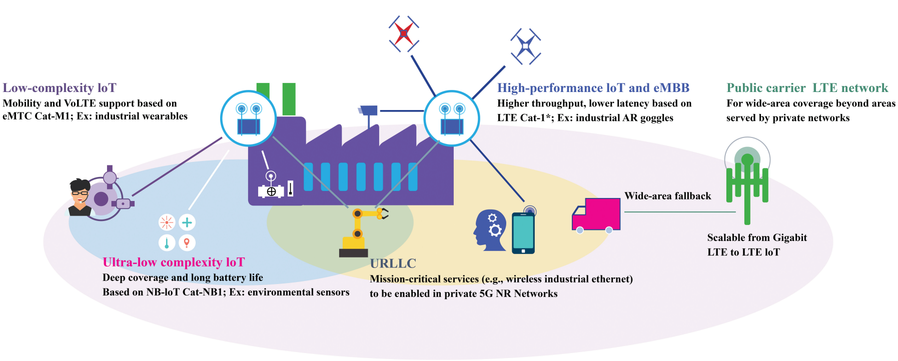
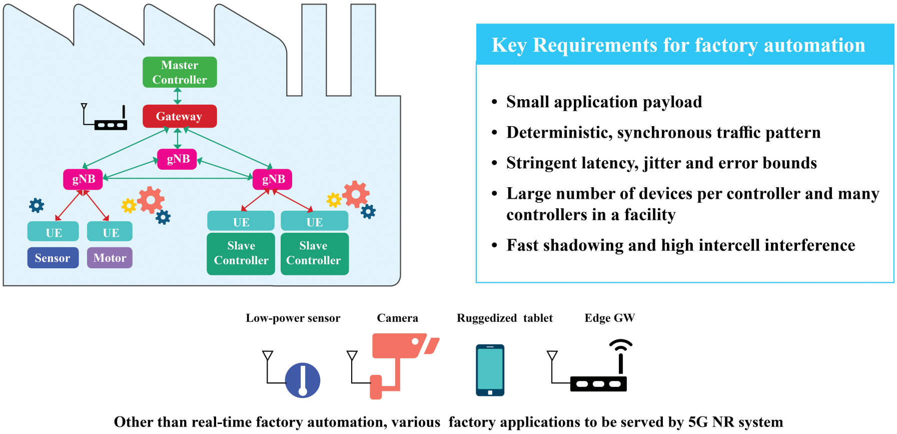

Low-complexity IoT
Mobility and VoLTE support based on eMTC Cat-M1; Ex: industrial wearables
High-performance IoT and eMBB
Higher throughput, lower latency based on LTE Cat-1*; Ex: industrial AR goggles
Public carrier LTE network
For wide-area coverage beyond areas served by private networks
Wide-area fallback
Scalable from Gigabit LTE to LTE IoT
Ultra-low complexity IoT
Deep coverage and long battery life Based on NB-IoT Cat-NB1; Ex: environmental sensors
URLLC
Mission-critical services (e.g., wireless industrial ethernet) to be enabled in private 5G NR Networks

Figure 3.25 5G use in different industrial application areas.

Industrial sectors will depend on smart wireless technologies like 5G and LTE advanced for efficient automation of equipment, predictive maintenance, safety, process tracking, smart packing, shipping, logistics and energy management.

Smart sensor technology offers unlimited solutions for industrial IoT for smarter, safe, cost effective and energy efficient industrial operation. A number of key requirements for factory of the future automation scenarios for connectivity are presented in Figure 3.26.

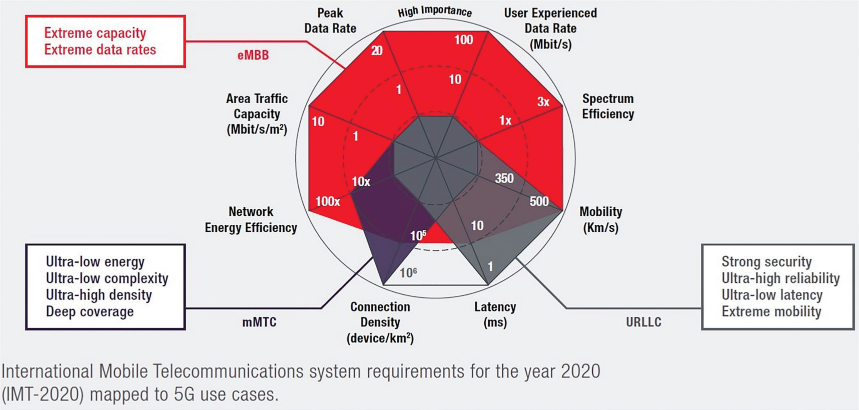


Key Requirements for factory automation

- Small application payload
- Deterministic, synchronous traffic pattern
- Stringent latency, jitter and error bounds
- Large number of devices per controller and many controllers in a facility
- Fast shadowing and high intercell interference

Other than real-time factory automation, various factory applications to be served by 5G NR system

Figure 3.26 Key requirements for connectivity for factory of the future automation.



International Mobile Telecommunications system requirements for the year 2020 (IMT-2020) mapped to 5G use cases.

Figure 3.27 International Mobile Telecommunications system requirements for the year 2020 (IMT-2020) mapped to 5G use cases [95].

5G communications could be considered a disruptive element enabling the vision of a truly global IoT, given that one of the key features of 5G is the focus on the integration of heterogeneous access technologies, including satellite communication systems. Satellites could play an important role in providing ubiquitous coverage and reliability in remote areas and enabling new IoT services. IoT devices are not equipped with satellite connectivity, while IoT protocols are not designed with satellite requirements in mind. Thus, cross-layer optimization is required to allow the collection of IoT data from satellites, load balance and the offloading of terrestrial networks, in turn enabling smooth integration of IoT and satellite networks.

5G offers a more reliable network and will deliver a secure network for the IIoT by integrating security into the core network architecture. Industrial facilities will be among the major users of private 5G networks.

Future networks have to address the interference between different cells and radiation and develop new management models to control roaming, while exploiting the coexistence of different cells and radio access technologies.

New management protocols controlling the user assignment with regard to cells and technology will have to be deployed in the mobile core network for 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 emergence of safety applications, minimizing latency and the various protocol translations will benefit 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 in order to maximize efficiency in terms of latency, security, energy efficiency and accessibility.

In this context, there is a need for higher network flexibility, which combines cloud technologies with software-defined networks and network function virtualization, which will enable network flexibility to integrate new applications and configure network resources to an adequate degree (sharing computing resources, splitting data traffic, security rules, QoS parameters, mobility etc.).

The evolution and pervasiveness of present communication technologies have the potential to grow to unprecedented levels in the near future by including the Web of Things (WoT) into the developing IoT. Network users will be humans, machines and things, and groups of them.

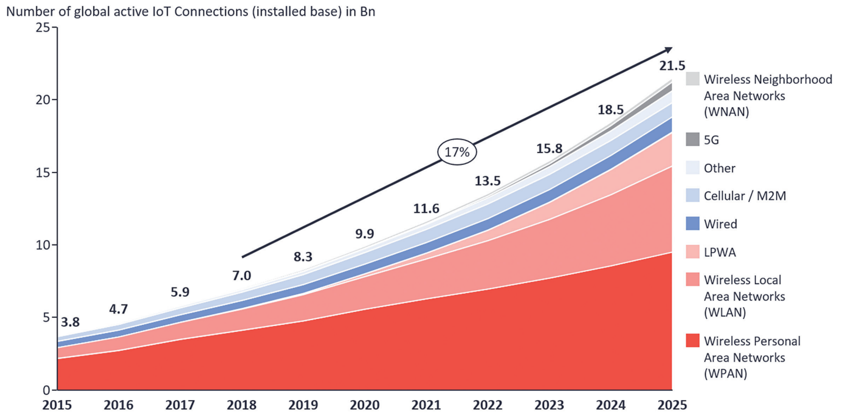
3.3.3.2 Communication technology

Global connection growth is mainly driven by IoT devices, both on the consumer side (e.g., smart home) and on the enterprise/B2B side (e.g., connected machinery). The number of IoT devices that are active is expected to grow to 10 billion by 2020 and 22 billion by 2025. Figure 3.28 presents the global number of connected IoT devices categorised by the communication/protocol technology [27].

These trends require the extension of the spectrum in the 10–100 GHz range and unlicensed band and technologies, such as WiGig or 802.11ad, which are mature enough for massive deployment and can be used for cell backhaul, point-to-point or point-to-multipoint communication.

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 with the simultaneous use of multiple ISM radio bands (i.e., 169/433/868/902 MHz, 2.4 GHz and 5 GHz). Connectivity modules are based on integrated circuits (ICs), reference designs and feature-rich software stacks created according to a flexible modular concept, which properly addresses various application domains.

The load of the network will differ, with some models using the unbalanced load of the ad hoc network from the core network point of view, and



Note: IoT Connections do not include any computers, laptops, fixed phones, cellphones or tablets. Counted are active nodes/devices or gateways that concentrate the end-sensors, not every sensor/actuator. Simple one-directional communications technology not considered (e.g., RFID, NFC). Wired includes Ethernet and Fieldbuses (e.g., connected industrial PLCs or I/O modules); Cellular includes 2G, 3G, 4G; LPWAN includes unlicensed and licensed low-power networks; WPAN includes Bluetooth, Zigbee, Z-Wave or similar; WLAN includes Wi-fi and related protocols; WNAN includes non-short range mesh; Other includes satellite and unclassified proprietary networks with any range.
Source: IoT Analytics Research 2018

Figure 3.28 Global number of connected IoT devices [27].

others using network-based solutions by balancing the topology from the core network point of view. In this case, the identified network requirements to be supported are the calculation of the optimal ad hoc network topology, by using monitoring information, and the notification of appropriate actions.

Wireless Personal Area Networks (WPANs)

The highest number of IoT devices is connected through short-range technology (WPAN), which typically does not exceed 100 m in the maximum range. These include Bluetooth-connected devices, such as headsets, as well as ZigBee- and Z-Wave-connected devices, which can mostly be found in smart homes, e.g., for connecting smoke alarms or thermostats [27]. Zigbee 3.0 is a networking solution used on top of IEEE 802.15.4 radio technology, which includes Wi-Fi and IP Internet capability. Zigbee 3.0 has meshing capability and is used as an IoT connectivity solution for a range of smart home and industrial applications, including lighting, security, thermostats and remote controls. It is secure and supports battery-free devices, meshing, low latency and energy harvesting (e.g., motion, light, piezo, Peltier). Zigbee 3.0 also includes Zigbee Green Power, which was developed as an ultra-low-power wireless standard to support energy-harvesting IoT devices and is effective for IoT devices that are only sometimes on the network (i.e., when they have power), enabling them to go on and off the network securely, so they can be off most of the time.

6LowPAN is a network protocol that defines encapsulation and header compression mechanisms. The standard has the freedom of a frequency band and a physical layer and can also be used across multiple communications platforms, including Ethernet, Wi-Fi, 802.15.4 and sub-1 GHz ISM. The protocol is implementing open IP standards including TCP, UDP, HTTP, COAP, MQTT and web sockets, and offers end-to-end addressable nodes, allowing a router to connect the network to IPs. 6LowPAN is a mesh network that is robust, scalable and self-healing. Mesh router devices can route data destined for other IoT devices, while hosts are able to sleep for long periods of time.

Wireless Local Area Networks (WLANs)

Another large category comprises WLANs, which offer a range of connectivity up to 1 km. Wi-Fi is the most common standard in this category and experiencing significant growth, mostly through the use of home assistants, smart TVs and smart speakers, but also increasingly through use in industrial settings such as factories (although it continues to play a minor role in those settings compared to other technologies) [27]. With the introduction of Wi-Fi 6 (802.11ax standard), the connectivity performance is enhanced for the use of IoT devices and businesses and operators running large-scale deployments.

Wi-Fi 6 brings more capabilities to support next generation connectivity uses. Wi-Fi 6 offers faster speeds for all devices on the 2.4 GHz and 5 GHz spectra, with a raw throughput speed boost of as much as 37%. Wi-Fi 6 IoT devices can shut down Wi-Fi connections most of the time using the Target Wake Time feature and connect only briefly as scheduled in order to transmit data they have gathered since the last time this was performed, thus extending battery life. Wi-Fi 6 uses orthogonal frequency-division multiple access (OFDMA) to improve the efficiency of multi-user multiple-input, multiple-output (MIMO) streams. MIMO works both on the uplink and on the downlink and can simultaneously receive data from different devices on different channels (maximum of eight in Wi-Fi 6) at once. The Target Wake Time feature improves sleep and wake efficiency, reduces power consumption and decreases congestion on crowded networks. In Wi-Fi 6, the theoretical maximum bandwidth of a single stream is 3.5 Gbit/s, and up to four streams can be delivered to a single device, which means a maximum of up to 14 Gbit/s.

Low-Power Wide Area Networks (LPWANs)

A large chunk of the future growth in the number of IoT devices is expected to come from LPWANs. By 2025, it is expected that more than two billion devices will be connected through LPWANs. The technology, which promises extremely high battery life and a maximum communication range of over 20 kilometres, is used by the three main competing standards, LoRa, Sigfox and NB-IoT, which are currently being rolled out worldwide with more than 25 million devices already connected to date, the majority of which are smart meters [27]. Another research report predicts that there will be 2.7 billion LPWAN IoT connections by 2029 [28]. LPWANs operate in the unlicensed industrial, scientific and medical (ISM) spectrum at 900 MHZ, 2.4 GHz and 5 GHz.

LoRa is the standard protocol of the LoRa Alliance (open, non-profit association established in 2015 with more than 500 members). LoRa has a bandwidth of 250 kHz and 125 kHz and a maximum data rate of 50 Kbps, enabling bidirectional communication albeit not simultaneously, and has a maximum payload of 243 bytes. The range is up to 5 km in urban areas and 20 km in rural areas depending on the application. There are around 50 million LoRa-based end nodes and 70,000 LoRa gateways that have already been deployed worldwide [29]. LoRa networks use gateway devices to work and manage the network for connecting IoT devices.

Sigfox operates and commercializes its own proprietary communications technology, which is an ultra-narrowband (100 Hz) with a maximum data rate of 100 bps. It also operates in the unlicensed ISM spectrum and its small payload (maximum 12 bytes) means it can offer greater coverage geographically, reaching up to 10 km in urban areas and 40 km in rural areas. Sigfox offers bidirectional connections, with the downlink from base stations to end IoT devices occurring following uplink communication. The daily uplink messages are limited to 140.

Weightless (Weightless-N, Weightless-W and Weightless-P) operates in the unlicensed spectrum and is an open standard (Weightless SIG) designed to operate in a variety of bands, with all the unlicensed sub-GHz ISM bands, while featuring a 100 kbps maximum data rate on uplink and downlink. Weightless can handle 2,769 end points per base station on standard smart meter set-ups (200 bytes uploaded every 15 min).

NB-IoT coexists with GSM and LTE and is a 3GPP LTE standard, based on licensed cellular networks providing a 200 kHz bandwidth and a 200 kbps maximum data rate, which offers bidirectional communication, albeit not simultaneously, and has unlimited messages with a maximum payload 1,600 bytes. The global shipments of NB-IoT devices will have a compound annual growth rate of 41.8% from 106.9 million units in 2018 to 613.2 million in 2023 [30].

LTE-M is another 3GPP providing extended coverage by using an installed LTE base with the same spectrum, radios and base stations. It is implemented as a 4G technology with an important role in 5G. The uplink/downlink transfers 1 Mbps and, due to low latency and full duplex operation, can carry voice traffic. LTE-M supports more demanding IoT mobile devices, which require real-time data transfer (e.g., transport, wearable), while NB-IoT supports more IoT static sensors and devices.

Cellular and non-cellular LPWA network connections will grow globally at a 53% CAGR until 2023, driven by market growth in smart meters and asset trackers. In 2017, smart meters and asset trackers contributed to almost three quarters of all LPWA network connections, dominated by non-cellular LPWA network technologies. By 2023, non-cellular LPWA will cede its market-share dominance to NB-IoT and LTE-M, as cellular LPWA moves to capture over 55% of LPWA connections.

Private LPWA networks, built to address a single vertical application or an individual enterprise, have been popular choices for over a decade and accounted for 93% of LPWA connections in 2017. LoRa and other non-cellular LPWA technologies have benefited from the decreasing cost of ICs, low implementation costs and flexibility of private networks, which can be tailored to meet specific enterprise IoT applications. As the geographic footprint of public networks rapidly expands, cellular and non-cellular public networks will capture over 70% of LPWA connections by 2023 [31].

Future IoT devices will require network agnostic solutions that integrate mobile, NB-IoT, LoRa, Sigfox, Weightless etc. and high-speed wireless networks (Wi-Fi), particularly for applications spanning multiple jurisdictions.

LPWA networks have several features that make them particularly attractive for IoT devices and applications, which 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
- Optimized data transfer that supports small, intermittent blocks of data
- Low device unit costs
- Few base stations required to provide coverage
- Easy installation of the network
- Dedicated network authentication
- Optimized for low throughput, long or short distance
- Sufficient indoor penetration and coverage

Wired

Few people think of wired connections when they think of the IoT. In many settings, a wired device connection is still the most reliable option that provides very high data rates at very low cost, albeit without much mobility. Particularly in industrial settings, fieldbus and Ethernet technologies use wired connections to a large extent, and it is expected that they will continue to do so in the future [27]. Sensor/actuator units that are installed within a building automation system can use wired networking technologies like Ethernet. Power Line Communication (PLC) is a hard-wired solution that uses existing electrical wiring instead of dedicated network cables and for industrial applications has significant advances. According to the frequency bands allocated for operation PLC systems can be divided into narrowband PLC (NBPLC), and broadband PLC (BPLC). NBPLC refers to low bandwidth communication, utilising the frequency band below 500 kHz and providing data rates of tens of kpbs, while BPLC utilises a wider frequency band, typically between 2 MHz and 30 MHz, and allows for data rates of hundreds of Mbps. BPLC is recommended for smart home applications requiring high-speed data transfer applications like Internet, HDTV, and audio, while the use of NBPLC systems is more appropriate for remote data acquisition, automatic measuring systems, renewable energy generation, advanced metering, street lighting, plug-in electric vehicles, etc. BPLC has higher speed, that reduce the data collection period and ensures a real-time remote-control command, but its stability and reliability are still determined by the quality of power lines. Another way to classify PLC is as PLC over AC lines and PLC over DC lines. Most companies are currently providing AC-PLC solutions, PLC in DC lines also has applications for distributed energy generation, and transportation (electronic controls in airplanes, automobiles and trains).

Cellular / M2M

2G, 3G and 4G technology, for a long time, were the only option for remote device connectivity. As LPWA and also 5G gain momentum, it is expected that these legacy cellular standards will cede their share to new technologies as they present a more lucrative opportunity to many end users [27].

5G

5G is under development and the technology, which promises a new era of connectivity through its massive bandwidth and extremely low latency, is now heavily promoted by governments, particularly China. The Chinese government views 5G adoption as a competitive asset in the quest to move the equilibrium of technological innovation from the US and Europe towards China. In the US, the first pre-standard 5G networks will provide fixed wireless access (FWA) services to residential and small business users by the end of this year. While many more use cases will be targeted once the final standard is ratified in 2020, we should already see first adopters next year and expect quick growth from there [27].

5G includes two of the tree scenarios, massive machine type communications (mMTC) and ultra-reliable and low latency communications (URLLC), which support IoT applications for industries with available, ultra-low latency links for next generation IoT services.

The Internet as network technology is focusing on the internet working among underlay technologies in order to provide end-to-end services. Telecoms/communication and Internet/computer communication are converging via telephone/cellular and Internet/data networks. The TCP/IP paradigm started as an overlay of network technologies, while TCP/IP is nowadays integrated in pre-existent network infrastructures and starting to include transport and application functionality in the network as well.

5G is including the wired/core section of the network, as well as LANs, to architecturally integrate cloud/fog/edge systems, based on software network functions, providing differentiated service support. The next generation Internet and 5G are converging into a fully integrated interoperable network, where people and IoT physical, digital and virtual devices interact in real-time. 5G connectivity is one important element in building real-time interactive systems and implementing a tactile IoT/IIoT in order to provide the communication infrastructure with low latency, very short transit time, high availability, reliability and security. LTE evolution will continue, while LTE and 5G will co-exist in upcoming years. The availability of device hardware and attractive service pricing will influence the adoption of 5G for various IoT applications across different industrial sectors.

5G monetization is a critical success factor for the deployment of 5G and monetization models must be supported by different pricing models. Some of the monetization models to be considered are [98]:

- Monetize network, infrastructure and business services by leveraging the network and infrastructure capabilities:
    - ○ Operators provide services such as Network as a Service, Information broadcasting, Cloud services with high QoS that attract premium in B2B segments.
    - ○ Operators become platform providers for a variety of micro-services, assuring low latency where needed by providing them on the edge. With this model, application developers and vendors could simply define how they want their applications to perform and let the connectivity provider make it happen.
    - ○ Operators enable the developers to monetize their applications that connect to many millions of devices and in turn will be able to secure revenues from developers and the end users of these devices.
    - ○ Leveraging the infrastructure, vertical industrial solutions can be offered by establishing ecosystems with complex partnerships and revenue sharing models. Key for success is to make the economics work for both the operators and other participants in the ecosystem to bring useful solutions to the market quickly.
- Monetize value: 5G creates opportunity for operators to monetize the 'value' created by services with revenue sharing type of models rather

than being simply the connectivity provider. Applications such as translation services, home automation can be monetized by putting compute functionality on the ultra-low latency edge networks and thus putting it on the Cloud without compromising on latency.

- Advertisements in the new digital services like high definition content offers new monetization opportunities for operators.
- Data monetization: Operators have access to customer data – customer priorities and interactions, network data – usage, pattern, massive number of device related data. This massive amount of data along with data analytics creates new opportunities for operators to monetize insights.

Wireless Neighbourhood Area Networks (WNANs)

WNANs sit between WLAN and long-range technologies, such as cellular, in terms of communication range. Typical proponents of this technology include mesh networks such as Wi-SUN or JupiterMesh. In some cases, the technology is used as an alternative to LPWA/cellular (e.g., in utilities' field area networks) and in other cases such as a complementary element (e.g., for deep indoor metering where nothing else reaches) [27].

Wi-SUN is an open standards-based field area network (FAN) used for the IoT and can support applications such as advanced metering infrastructure, distribution automation, intelligent transport and traffic systems, street lighting, and smart home automation. The suite of IoT technologies is based on IEEE 802.15.4, TCP/IP and related standard protocols with a bandwidth of up to 300 kbps, a low latency of 20 ms, power efficiency (less than 2 mA when resting; 8 mA when listening), resilience, scalability (networks to 5,000 devices; 10 million end points worldwide) and using security mechanisms based on public key certificates, AES, HMAC, dynamic key refresh and hardened crypto. The PHY layer is based on IEEE 802.15.4g, which provides bidirectional communication. The network layer is IPv6 with 6LoWPAN adaptation supporting star and mesh topologies, as well as hybrid star/mesh deployments.

These different types of networks are needed to address IoT products, services and techniques so as to improve the grade of service (GoS), quality of service and quality of experience (QoE) for end users. Customization-based solutions are addressing the IIoT 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. Multifunctional, multiprotocol 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 a trusted IoT, based on the features and security provided by devices at various levels of the digital value chain.

3.3.4 Distributed Ledger Technology/Blockchain Technology

A distributed ledger is a record of transactions or data that is maintained in a decentralized form across different systems, locations, organizations or devices. It allows data or funds to be effectively sent between parties in the form of peer-to-peer transfers without relying on any centralized authority to broker the transfer. A distributed consensus mechanism allows members of the network (nodes) to establish a common "truth". There are different mechanisms for this: in the case of Bitcoin and other "cryptocurrencies", a computationally complex "proof-of-work" algorithm is used to protect the integrity of the network against change to the public "blockchain" by making it impractical for malevolent players to alter the chain. Whilst Bitcoin operates on a public blockchain, there is also the possibility to operate distributed ledgers privately where network participants are provided with relevant permissions to either read or write to (i.e., append) the ledger [33, 34].

Blockchain is a technological disruption in secured infrastructures. It is based on a combination of encrypted algorithms and duplicated data storage on a network of computers. Used as a secured infrastructure, it can meet the demand for security from various industries.

From a technological perspective, blockchain is a data storage infrastructure technology. It makes it possible to store data securely (each entry is authenticated, irreversible and duplicated), with decentralized control: there is no central authority that controls the information on the chain. This is achieved using encryption technologies (hash function and asymmetric cryptography) and a computer network of independent nodes.

Blockchain technologies were initially designed to be used with the Bitcoin cryptocurrency, where they were employed to create a reliable ledger of all financial transactions. But blockchain technology is also developing in ways that are opening new prospects:

- The use of blockchains as a ledger of transactions (the initial use case)
- The use of blockchains to accurately archive and date important pieces of information
- The introduction of smart contracts: automated conditional transactions that are executed without human intervention or the involvement of a trusted third party
- The advent of decentralized applications: applications that use the blockchain as their execution infrastructure, without a centralized IT platform

The information architecture used by Bitcoin technology provides a source for the development, contextualization, exchange and distributed security of data needed for the IoT.

Blockchains for the IoT transform the way business transactions are conducted globally within a trustworthy environment to automate and encode business transactions while preserving enterprise-level privacy and security for all parties in the transaction. Blockchain solutions are, for instance, being developed to identify IoT objects and to sign automatic and decentralized contracts between connected devices.

The benefits of blockchains for the IoT are providing mechanisms for building trust between stakeholders in an IoT application and IoT devices with blockchain cryptography, to reduce the risk of collusion and tampering, to facilitate cost reductions by removing the overheads associated with middlemen and intermediaries, and to accelerate transactions by reducing the settlement time from days to almost real-time. Considerations in the application of distributed ledgers for the IoT include addressing the storage space, the computing power of the devices, security, communication power, transaction confirmation time, consensus mechanisms, congestions, costs/fees and price volatility.

IoT applications using distributed ledger technologies (DLTs) must evaluate several attributes regarding the implementation of use cases, which must take into account the retention in the distributed ledger, multiparty sharing needs, the trade-off between retrieval and flexibility performance for the ledger database features and the trade-off in real-time, as there is a time lapse between the moment when data or transactions are generated and when the consensus mechanism confirms that the information is part of the ledger. The evolution of the blockchain is illustrated in Figure 3.29.

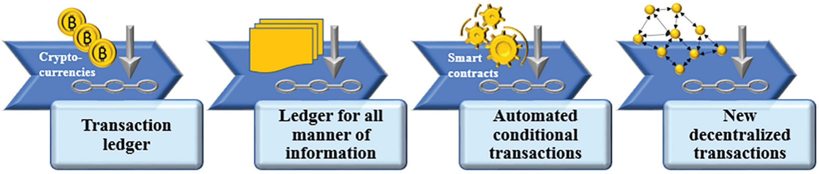

Crypto-currencies
Transaction ledger
Ledger for all manner of information
Smart contracts
Automated conditional transactions
New decentralized transactions

Figure 3.29 Evolution of the blockchain.

Source: Adapted from IDATE DigiWorld, Blockchain, October 2016.

IoT devices will be used in building blockchain-based solutions to support applications aimed at improving operational efficiency, transforming the user experience and adopting new business models in a secure, private and decentralised manner, so that all stakeholders benefit. This is especially the case for blockchain applications that can track and control property: from asset management applications (IoT devices being used to track assets along the logistics chain) to a radical transformation of business relationships, transitioning to a world where any property or object can easily be rented out to another user securely and without the need to interact directly with the user (the user signs a smart rental contract, which, once the payment has been made, gives him/her access to the lock for a set period of time).

The IoT can make use of blockchain-based computing platforms (e.g., iExec, Golem, Sonm, Hypernet, Ripple) or Hyperledger, which is an open source Linux Foundation platform. Recently, the Enterprise Ethereum Alliance, a blockchain standards organization, and Hyperledger announced that they have joined each other's groups [22, 23]. Other solutions offered by Ripple, BigchainDB and Sovrin exist [37–39].

The Hyperledger platform [22, 24] connects data from the IoT via specific adapters in order to integrate a variety of existing sensors and protocols, as well as integrate and connect transactions that are related to these sensors with blockchain systems that might belong to different stakeholders. The platform allows for the use of cognitive artificial intelligence (AI) components to infer new insights from these combined data. Further research is needed to define how to optimally combine blockchains, cognitive AI and the IoT for various industry domains.

Combinations of blockchain technology and the IoT into an IoT-driven blockchain, as used in the aviation industry, are presented in [40, 41] (see Figures 3.30 and 3.31).

The combination of blockchains and the IoT provides several benefits in supply chains such as: tracking objects as they travel along the export/import

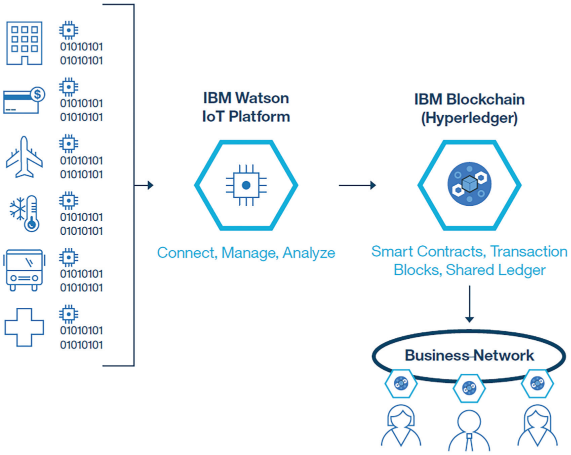


Figure 3.30 Combining blockchain technology and the IoT with the use of IBM Watson and blockchain platforms [41].

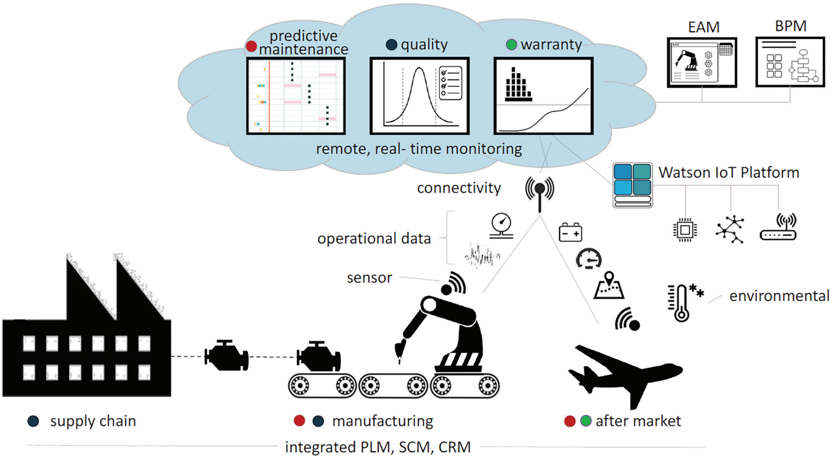


Figure 3.31 Using blockchain and the IoT to improve operations in the aviation industry [40].

supply chain, while enforcing shipping and lines of credit contracts and expediting incremental payments; maintaining an indelible history of parts and end assembly through supply chains, potentially including critical events that affect life or scheduled maintenance; providing decentralized edge computing to securely run computing workloads, such as analytics, on edge devices owned by third parties; interconnecting IoT devices by allowing distributed devices to request and pay for services through distributed role management and micropayments, as well as regulatory compliance, in order to track equipment or process history in an indelible record, and enabling easy sharing of this information with regulatory agencies or insurers [41].

IOTA is a next generation blockchain focused on use in the IoT as a "ledger of things". IOTA uses a revised distributed ledger design known as a "tangle", which aims to be massively scalable as well as avoid the cost of replicating all data to all nodes [35, 36].

Hypernet is proposing new architecture and has implemented a new programming model beneath the blockchain layer to handle distributed computation problems, which require inter process communication. Hypernet is based on the principle of distributed average consensus (DAC), and the combination with blockchains allows for the efficient distribution of compute jobs, while effectively managing processing units in dropping on and off the network. The platform creates a secure backbone, where buyers and providers of computational power can engage, based on trust. The on-chain (scheduled) and off-chain (DAC) technology layers of Hypernet fit together, with both driven by consensus.

Golem, iExec and Sonm have built their concept on traditional computing architectures developed specifically to be used in data centres. These data centre architectures pose challenges to a distributed network used in the IoT as the amount of network communication and data transfer overhead is very high and the architectures do not tolerate computers randomly dropping in and out of the network. As data centre architectures are optimised for one particular topology, they cannot be used on a distributed network, as the network topology is unknown.

Blockchain-based systems require devices in the blockchain to have the resources run the blockchain software and process blockchain data. However, distributed ledgers are open, with devices connected to a distributed ledger known as "nodes". Each "block" within the ledger has a maximum size of 1 MB and IoT devices used to hold a full copy of the ledger need to have processing and storage capabilities necessary to hold at least a few "full nodes" containing the complete ledger.

IoT security issues are relevant when using blockchain technology, as there is a need for proper security credentials to view a transaction and IoT device commissioning and secure key management are challenging issues in the case of IoT devices.

Addressing and solving the limitations of blockchain technology in the future could allow for the integration of blockchain-based platforms for the

IoT. Furthermore, considering that a blockchain contains the transaction and can also contain the contract, the IoT device can process financial information, buying/selling data from/to another IoT device or system, which could produce a transactional system less prone to the problems of resilience.

The blockchain model has several limitations for the use with IoT devices as blockchain processing tasks are computationally intensive and timeconsuming, while IoT devices have limited processing and storage resources to directly participate in a blockchain.

Lower-end IoT edge devices with limited storage space, communications bandwidth and processing power are not especially suitable to support resource-intensive distributed ledgers but can utilize the services of a distributed ledger network (e.g., by using an API). IoT gateway devices, such as an IoT home gateway, could potentially support blockchains (e.g., Raspberry Pi as a "full node"). The requirement for large amounts of disk storage adds cost and complexity, making it more likely that this would be reserved for higher-end gateway products. Lower-end IoT gateways and connections with limited bandwidth are more likely to access the distributed ledger network using an API. High-end IoT edge nodes, such as industrial controllers, smart building controllers and enterprise systems should be able to run capable distributed ledger solutions. Maintaining a local copy of the distributed ledger provides for local high-performance access to the data held on the ledger, as well as continuity in the case that connectivity to the Internet may be disrupted. IoT mobile edge computing nodes (i.e., deployed in the carrier network) can be used to build new distributed ledger solutions typically offered by telecoms operators to enterprise customers as a permissioned distributed ledger [33].

The research challenges for implementing DLTs and blockchains at the edge of networks for IoT applications are as follows:

- Techniques for increased scalability, as DLTs and blockchains do no scale as required by IoT applications for use in a distributed system.
- Solutions for dealing with the required processing power, as IoT devices do not have the processing and storage capabilities required to perform encryption for all the objects involved in a blockchain-based ecosystem. Connecting large numbers of IoT devices requires large volumes and very low cost, while the majority of these IoT devices are not capable of running the required encryption algorithms at the desired speed.
- Techniques to speed up the process of validating the transactions for IoT devices.

- Storage capabilities (e.g., internal flash memory or external NOR or NAND flash) to be used to store transactions and device IDs, as well as the ledger on the nodes as the ledger increases in size as time passes.
- Addressing the complexities of the convergence of DLTs, blockchains and IoT technologies and providing simpler implementations at the system level.
- Interoperability issues when combining data sources from different applications, while considering the lack of data model standards for industrial vertical markets.
- Legal and compliance issues for hybrid transactions management across different industrial sectors.
- Security, privacy and trust of blockchain and decentralized schemes.
- Performance optimization of blockchain and decentralized schemes.
- Lightweight protocols and algorithms based on blockchains.
- Blockchain-based lightweight data structures for IoT data.
- Blockchain-based IoT security solutions.
- Blockchains in 5G.
- Blockchains in edge and cloud computing.

3.4 Emerging IoT Security Technologies

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. In this context, they are becoming increasingly vulnerable to disruption from denial-of-service attacks, identity theft, data tampering and other threats.

Emerging distributed end-to-end security technologies enhance the ability of an IoT ecosystem and its devices to exhibit complex behaviour independently or collectively in the presence of threats, in a pursuit to achieving end-to-end security. By using such technologies as blockchain, swarm logic and AI, IoT can offer security by design and end-to-end security solutions never implemented before. Techniques such as simulation and optimisation allow for the integration of security early in the design, where a diversity of security breach scenarios can be tested and guarded before they occur in real life.

Interoperability, scalability and security are three of the most essential attributes of IoT environments and ecosystems, which are absent or not fully addressed in today's architectures. Several technologies have succeeded in offering sound and complete solutions to these matters, although not without challenges still remaining. A new 3D IoT layered architecture capturing the

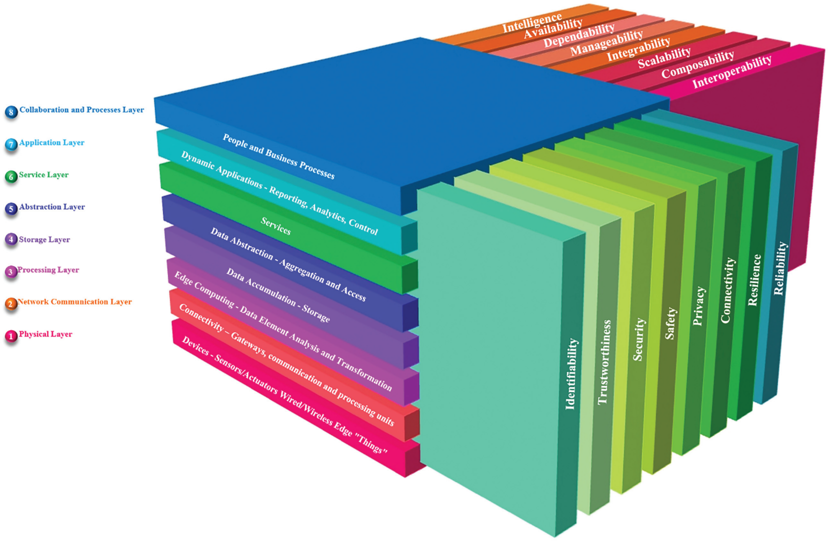

Intelligence
Availability
Dependability
Manageability
Integrability
Scalability
Composability
Interoperability
8 Collaboration and Processes Layer
7 Application Layer
6 Service Layer
5 Abstraction Layer
4 Storage Layer
3 Processing Layer
2 Network Communication Layer
1 Physical Layer
People and Business Processes
Dynamic Applications - Reporting, Analytics, Control
Services
Data Abstraction - Aggregation and Access
Data Accumulation - Storage
Edge Computing - Data Element Analysis and Transformation
Connectivity – Gateways, communication and processing units
Devices - Sensors/Actuators Wired/Wireless Edge "Things"
Identifiability
Trustworthiness
Security
Safety
Privacy
Connectivity
Resilience
Reliability

Figure 3.32 3D IoT Layered Architecture.

IoT systems functions and cross-cutting functions is presented in Figure 3.32. Among them, blockchain technology has been developed for scale and with interoperability in mind; hence, it is often generalized as DLT. Its security mechanism, based on public ledger and consensus, is applied across the stack and the network, whether this is centralized, decentralized or distributed. Nevertheless, in spite of all security advancements, guarding against single scenarios of fraud, hacking and other breaches still remains a challenge.

Different IoT topologies require different security configurations and strategies, and this is especially true at the edges, where devices can be diverse, less traditional, small and possibly out of reach for security updates. The edges are therefore vulnerable, providing entry points for malicious attacks, which are difficult to track and therefore easily propagate throughout the whole IoT ecosystem.

As edge devices are often unsophisticated devices, it may be difficult to build security into the design. However, it is here that swarm technology may come to the rescue. Edge devices may form clusters, where they collaborate and share resources and functions in the presence of perceived danger. Each edge device, now belonging to a cluster, will exhibit collective intelligence and be able to evolve and adapt to new requirements and threat situations. Swarm technology helps to identify the threat and define its landscape.

In the evolving IoT market, security goes beyond securing the information exchanged among the IoT nodes. The entire operation of an IoT ecosystem depends on protection at all levels, from single devices to communications. Moreover, devices must exhibit a high level of resilience against a growing range of attacks, including hardware, software and physical tampering.

Security is therefore critical to IoT technologies and applications, and end-to-end security is essential to enabling the implementation of trustworthy IoT solutions for all stakeholders in IoT ecosystems and IoT value networks to enable the development, deployment and maintenance of systems in IoT applications and provide a common framework to enable the growth of IoT value network solutions.

The standard security services that are valid for the Internet framework and technology, such as authentication, confidentiality, integrity, non- repudiation, access control and availability, should be extended to also apply to IoT technologies but adapted with their particularities and constraints in mind.

Identification: is the act of allowing a device or service to be specifically and uniquely identified without ambiguity. This may take the form of RFID tag identifiers, IP addresses, global unique identifiers, functional or capability identifiers, or data source identifiers.

Authentication: is the act of confirming the truth of an attribute of an entity or a single piece of data by using passwords, PINs, smart cards, digital certificates, or biometrics to sign in. In contrast with Identification, Authentication is the process of actually confirming the Identity of a device or confirming that data arriving or leaving are genuine and have not been tampered with or forged.

Authorization: is the function of specifying access rights to resources and ensuring that any request for data or control of a system is managed within these policies. Authorization mechanisms tend to be centralized, which may be a challenge in IoT systems that tend to be increasingly decentralized, without an authority involved. Whatever the degree of democratized authorization, where more entities can grant permissions, the authorization system must be consistent, persistent and attack resistant.

Availability: has two definitions within the IoT domain. Firstly, as with mainstream Information Assurance, the system must provide data and resources in a timely manner for a set percentage of the time (e.g. 99.99% uptime availability). Secondly, in the IoT it is critical that many devices are available or retain their critical functionality, even if the system has undergone an attack.

Confidentiality: is a set functionality that limits access or places restrictions on certain types of information, with the goal of preventing unauthorized access. Confidentiality is usually achieved through encryption and cryptographic mechanisms and is essential within an IoT ecosystem where a large amount of information is exchanged among the nodes.

Integrity: is a critical measure in information assurance and is defined as providing consistency or a lack of corruption within the IoT system. It requires the final information received to correspond with the original information sent and that data cannot be modified without detection. Malicious modification of the information exchanged may disrupt the correct functioning of an entire IoT ecosystem.

Non-repudiation: is an aspect of authentication that enables systems to have a high level of mathematical confidence that data, including identifiers, are genuine. This ensures that either a transmitting or receiving party cannot later deny that the request occurred (cannot later "repudiate") and provides data integrity around the system. This is of particular importance in terms of tracking illegal activities within an IoT system, as it allows for accountability to be enforced. Whether Non-repudiation needs to be enforced under certain circumstances will depend on the particular applications.

A Root of Trust: is an immutable boot process within an IoT system based on unique identifiers, cryptographic keys and on-chip memory, to protect the device from being compromised at the most fundamental level. The Chain of Trust extends the Root of Trust into subsequent applications and use cases. Given that IoT systems rely on a large number of devices that collect and process information, it is paramount to ensure their credibility so that they are honest and leverage correct outputs.

Secure Update: enables IoT systems and devices to install new firmware from authorized sources without the firmware being compromised. Software updates are critical processes and are susceptible to a number of threats and attacks. During an update, the device receives the firmware wirelessly and installs it, removing the previous version. However, to reassure that the process is being done properly and securely, the sender of the firmware should be verified as trusted, the firmware should be validated as not compromised, the initial security keys should be protected, etc. Additionally, depending on the services that the device offers, the downtime during a firmware update may need to be kept at a minimum. If not properly protected, devices may be open to manipulation, typically through the installation of malicious code on a device.

3.5 IoT/IIoT Technology Market Developments

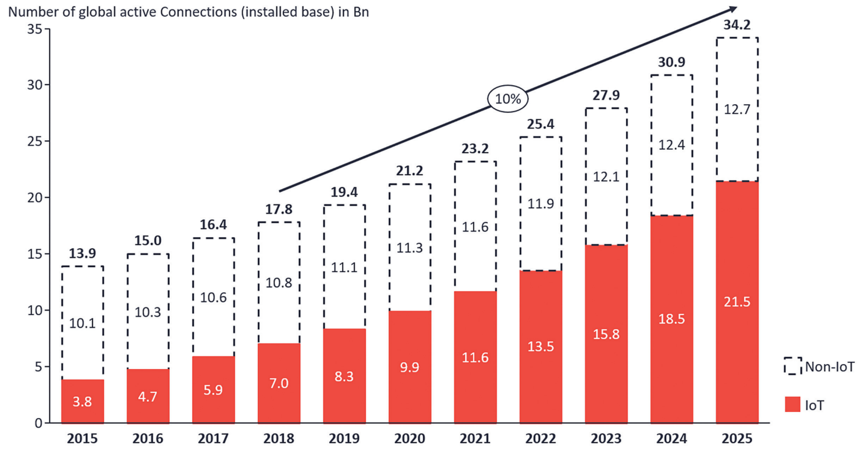
IoT/IIoT components, communication, systems, platforms, solutions applications and services markets are developing steadily, posing new challenges for research and innovation concerning IoT technologies addressing next generation developments.

The IoT chip market is expected to register a CAGR of over 13.68% during the forecast period of 2018–2023. The report profiles end user segments (such as healthcare, building automation and automotive segments) in the IoT chip market in various regions. Chipsets designed for IoT systems have unique factors including the need for optimal energy efficiency. The network effect is clearly evident as the impact of increasingly interconnected IoT systems will cause an acceleration in overall demand for chipsets due to the interdependency of platforms, gateways and devices [26].

The number of connected devices that are in use worldwide now exceeds 17 billion, with the number of IoT devices at seven billion (not including smartphones, tablets, laptops or fixed-line phones). Global connection growth is mainly driven by IoT devices – both on the consumer side (e.g., smart home) and on the enterprise/B2B side (e.g., connected machinery). The number of IoT devices that are active is expected to grow to 10 billion by 2020 and 22 billion by 2025 (see Figure 3.33). The global market for IoT (end user spending on IoT solutions) is expected to grow by 37% from 2017 to $151 billion. Due to the market acceleration regarding the IoT, those estimates have been revised upwards and it is now expected that the total market will reach $1,567 billion by 2025. Software and platforms are expected to continue to drive the market as more data are moved to the cloud, new IoT applications are brought to market, and analytics continue to gain in importance [27].

3.5.1 Digital Business Model Innovation and IoT as a Driver

The growing digitisation of businesses as well as societies has facilitated an increase in the amount of data made available and to be adopted and explored in the development of businesses. Digitisation is creating a second economy that is vast, automatic and invisible – thereby bringing the biggest change since the Industrial Revolution [1]. Data has become massive and has



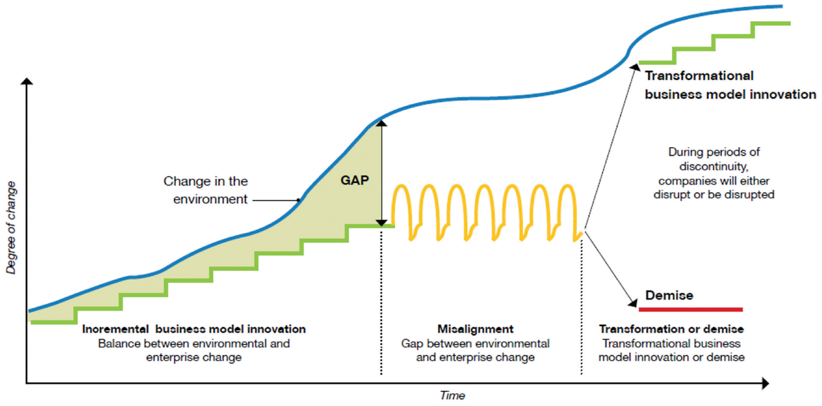
Note: Non-IoT includes all mobile phones, tablets, PCs, laptops, and fixed line phones. IoT includes all consumer and B2B devices connected – see IoT break-down for further details

Figure 3.33 Total number of active device connections worldwide [27].

moved from static data to real-time data streams created by the IoT based on a large number of transactions of millions of sensors and devices across the ecosystems of many organizations, even now moving from the central paradigm of the cloud more and more towards the edge in a distributed manner [2]. Some studies estimate an increase in annually created, replicated and consumed data from around 1,200 exabytes in 2010 to 40,000 in 2020 [3], with a growing proportion of data generated and consumed by machines [3]. In businesses, IoT data can be applied, for instance, to target customers more effectively; make better pricing decisions; predict failures; and optimise the use of assets, production or logistics. To fully exploit IoT in business we need to understand how businesses integrate technology [2].

3.5.1.1 Business models and business model innovation

Business models are intended to make sense of how businesses work. Business models are abstracted in different ways in the literature. Business models are discussed in [6] as a narrative that describes the customer, customer value, revenue collection of the model and the delivery of this value. Another level of abstraction is presented in [11]. In this reference the business model is described as an archetype of 55 different business model building blocks that can be combined in various ways to accommodate the business model in which the business operates. The most popular and most adopted breakthrough on another level of abstraction is the graphical framework. The most


Degree of change
Change in the environment
GAP
Transformational business model innovation
During periods of discontinuity, companies will either disrupt or be disrupted
Demise
Inoremental business model innovation
Balance between environmental and enterprise change
Misalignment
Gap between environmental and enterprise change
Transformation or demise
Transformational business model innovation or demise
Time

Source: Adapted from Gerry Johnson, Kevan Scholes, Richard Whittington, *Exploring Corporate Strategy*, 7th Edition © 2005 Prentice Hall, Pearson Education Limited.

Figure 3.34 The importance of Business Model Innovation with respect to external changes in the environment.

widely adopted graphical framework is the Business Model Canvas presented in [10]. The business model literature points to the fact that the technological development of the Internet and recent developments of ICT has boosted the usage of the business model concept and innovation in general. According to [9] in the context of innovation, the term Business Models is used to either commercialize new technology or ideas and as a source of innovation to the business model itself, that can lead to a competitive advantage.

The use and importance of business model innovation is stated in [12] and illustrated in Figure 3.34:

- Business Model Innovation will continue to become increasingly important for ensuring sustained competitiveness of both large and small businesses.
- Business Model Innovation is expected to serve as a facilitator of new market exploration and an important source of competitive advantage.
- Continuous adaptation of business models is imperative to ensure organizational fit with the environment.

However, there are significant research gaps combining technology trends with business model innovation:

- Empirical evidence remains patchy and often builds on observations of businesses that have successfully implemented new business models without knowing how the innovation has been created in the first place.

- Business Model Innovation frameworks are technology agnostic and often abstract the complexity of ecosystems, technology development/operations and organisations challenges.

3.5.1.2 The use of IoT for digital business development

IoT and digital technologies are central for digital business development and the disruptive business innovation tendencies of this decade and probably also decades to come. Consequently, Nambisan et al. [4] conceptualise digital innovation as "the creation of (and consequent change in) market offerings, business processes, or models that result from the use of digital technologies" and therefore, digital innovation management refers to the "practices, processes, and principles that underlie the effective orchestration of digital innovation". Thus, we need to examine how different company types, industries and sectors apply digital technologies to design digital businesses and digital business models.

3.5.1.3 The design and implementation processes of digital business development

Through digitisation of the business functions through IoT, data can be provided to enhance and develop each of these functions and thus the entire value chain. In practice this is demonstrated in the dramatic change of the marketing functions focus on online, social media and mobile marketing and less of a focus on traditional advertising, thus creating stronger interactions and continuous data collections with customers through social networks. Through the online environment, assortment and pricing decisions is made easier and much more flexible. Logistics and logistics streams are key to competitive delivery and services, and the marketing and logistic functions therefore need to cooperate more effectively in order to deliver superior customer value, and at a lower and more competitive cost [2]. With standards to represent different forms of data (text, numbers, pictures and video) facilitating communication via Bluetooth and the internet has led to the evolution of new products and services, and thus data has become a commodity. Thus, we need to explore the specific processes that go into the adoption and implementation of digital business development viewed from both a business and technology angle.

The effect and business opportunities of digitisation across ecosystems.

Digitisation affects entire ecosystems, their business models and the underlying business functions of a company's value chain. With intelligent devices becoming interconnected in IoT, new developments have created associated infrastructure and an expanding knowledge base, and these innovative combinations are being reflected in enterprises' "digital" business models [5]. Thus, we need to examine which metric and measurement systems are applied and require development to better assess the tangible as well as intangible value creation and capture of digital business development.

How technology, organisation and business interact is still poorly understood. Most studies have focussed on successful businesses and have been conducted within a discipline like business, innovation, technology or organisation. The literature provides some patchy evidence which shows Business Model Innovation (BMI) as a cross-disciplinary activity, connected with technology. It is also clear that IoT is a strong driver for business development and digitisation in industry, with many new applications and services emerging and driving new business models. We call for more concerted efforts to link business and technology at the applied research level and to devise new methods of studying IoT.

Acknowledgments

The IoT European Research Cluster - European Research Cluster on the Internet of Things (IERC) maintains its Strategic Research and Innovation Agenda (SRIA), considering 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, 2016 and 2017 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 over the Years of IERC Activities:

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 Kung, FR, Trialog, CREATE-IoT
Antonio Skarmeta, ES, University of Murcia, IoT6
Arkady Zaslavsky, AU, CSIRO, bIoTope
Arne Bröring, DE, Siemens, BIG-IoT
Arthur van der Wees, Arthurs Legal, CREATE-IoT
Bruno Almeida, PT, UNPARALLEL Innovation, FIESTA-IoT, ARMOUR, WAZIUP
Carlos E. Palau, ES, Universitat Politècnica 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, Université de Pau et des Pays de l'Adour, WAZIUP
Dimitra Stefanatou, Arthurs Legal, CREATE-IoT
Elias Tragos, IE, Insight Centre for Data Analytics, UCD and FORTH-ICS, RERUM, FIESTA-IoT
Emmanuel C. Darmois, FR, COMMLEDGE, CREATE-IoT
Eneko Olivares, ES, Universitat Politècnica 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
Giorgio Micheletti, IT, IDC, CREATE-IoT
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 Frãmling, 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, DERI, 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, DERI, OpenIoT, VITAL, FIESTA-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
Pasquale Annicchino, CH, Archimedes Solutions, CREATE-IoT
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
Ross Little, ES, Atos, CREATE-IoT
Roy Bahr, NO, SINTEF, UNIFY-IoT, CREATE-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
Sonia Compans, FR, ETSI, CREATE-IoT
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, BRAIN-IoT, ENACT, IoTCrawler, SecureIoT, SOFIE, CHARIOT, SEMIoTICS, SerIoT.

References

[1] Arthur, W. B. (2011). “The second economy”. McKinsey Quarterly, Vol. 4, No. 1, pp. 90–99.

[2] Aagaard, A. (2018). “Digital business models – driving transformation and innovation”. Palgrave MacMillan.

[3] Gantz, J., and Reinsel, D. (2012). “The digital universe in 2020: big data, bigger digital shadows, and biggest growth in the Far East”, International Data Corporation, Framingham.

[4] Nambisan, S., Lyytinen, K., Majchrzak, A., and Song, M. (2017). “Digital innovation management: reinventing innovation management research in a digital world”. MIS Quarterly, Vol. 41, No. 1, pp. 223–238.

[5] Kiel, D., Arnold, C., Collisi, M., and Voigt, K. I. (2016). “The impact of the industrial Internet of Things on established business models”. In Proceedings of the 25th International Association for Management of Technology (IAMOT) Conference, Orlando, Florida, USA, May 15–19.

[6] Magretta, J. (2002). “Why business models matter”. *Harvard Business Review*, Vol. 80, No. 5, pp. 86–92.

[7] Amit, R., and Zott, C. (2012). Creating value through business model innovation. *MIT Sloan Management Review*, Vol. 53, No. 3, p. 41.

[8] Afuah, A., and Tucci, C. L. (2001). *Internet business models and strategies*. New York: McGraw-Hill, p. 358.

[9] Dodgson, M., Gann, D. M., and Phillips, N. (Eds.). (2013). *The Oxford handbook of innovation management.* OUP Oxford.

[10] Osterwalder, A., and Pigneur, Y. (2010). *Business model generation: a handbook for visionaries, game changers, and challengers*. Wiley.

[11] Gassmann, H., Frankenberger, K., and Csik, M. (2014). "The St. Gallen business model navigator". Working paper: University of St. Gallen: ITEM-HSG.

[12] Knab, S., and Rohrbeck, R. (2014). "Why intended business model innovation fails to deliver: insights from a longitudinal study in the German smart energy market." Proceedings of the R&D Management Conference, Stuttgart, Germany, June 3–6, 2014.

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

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

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

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

[17] Lin, S., Cheng, H. F., Li, W., Huang, Z., Hui, P., and Peylo, C. (2017). Ubii: physical world interaction through augmented reality, IEEE Trans. Mob. Comput. Vol. 16. pp. 872–885.

[18] Sun, X., and Ansari, N. (2016). EdgeIoT: mobile edge computing for the Internet of Things, IEEE Commun. Vol. 54, pp. 22–29.

[19] Edge Computing Market, MarketsandMarkets Report, 2017, Online: https://www.marketsandmarkets.com/Market-Reports/edge-computing-market-133384090.html

[20] Ericsson Mobility Report, June 2018, Online: https://www.ericsson.com/assets/local/mobility-report/documents/2018/ericsson-mobility-report-june-2018.pdf

[21] Cloud IoT Edge, Online: https://cloud.google.com/iot-edge/

[22] Hyperledger, Online: https://www.hyperledger.org/

[23] Enterprise Ethereum Alliance (EEA), Online: https://entethalliance.org/

[24] Hyperledger Fabric, Online: https://www.ibm.com/blockchain/hyperledger/fabric-support

[25] Herr, G., Lyon, J., and Gillen, S. (2016). “Industrial intelligence: cognitive analytics in action,” presentation at EMEA Users Conference, Berlin.

[26] Research and Markets, Online: https://www.researchandmarkets.com/

[27] State of the IoT 2018: number of IoT devices now at 7B – Market accelerating, IoT analytics, Online: https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/

[28] IDTechEx, Comparison of Low Power Wide Area Networks (LPWAN) for IoT 2018–2019, Online: https://www.idtechex.com/research/articles/comparison-of-low-power-wide-area-networks-lpwan-for-iot-2018-2019-00014777.asp

[29] SEMTECH, Online: https://www.semtech.com/

[30] Ryberg, T., BERG INSIGHT, NB-IoT networks are here, now it’s time to make business, Online: https://www.iot-now.com/2018/07/04/85156-nb-iot-networks-now-time-make-business/

[31] NB-IoT, CAT-M, SIGFOX and LoRa Battle for Dominance Drives Global LPWA Network Connections to Pass 1 Billion By 2023, ABIresearch, 2018, Online: https://www.abiresearch.com/press/nb-iot-cat-m-sigfox-and-lora-battle-dominance-drives-global-lpwa-network-connections-pass-1-billion-2023/

[32] Wi-SUN FAN Overview, Online: https://tools.ietf.org/id/draft-heile-lpwan-wisun-overview-00.html

[33] Opportunities and Use Cases for Distributed Ledgers in IoT, GSMA 2018, Online: https://www.gsma.com/iot/wp-content/uploads/2018/09/Opportunities-and-Use-Cases-for-Distributed-Ledgers-in-IoT-f.pdf

[34] Nakamoto, S., Bitcoin: A Peer-to-Peer Electronic Cash System, Online: https://bitcoin.org/bitcoin.pdf

[35] Popov, S., (2018). The Tangle, Online: https://assets.ctfassets.net/r1dr6vzfxhev/2t4uxvsIqk0EUau6g2sw0g/45eae33637ca92f85dd9f4a3a218e1ec/iota1_4_3.pdf

[36] IOTA, Online: https://iota.org

[37] Ripple, Online: https://ripple.com

[38] Sovrin, Online: https://sovrin.org

[39] BigchainDB, Online: https://www.bigchaindb.com

[40] Gutierrez, C. (2017). Boeing Improves Operations with Blockchain and the Internet of Things, Online: https://www.altoros.com/blog/boeing-improves-operations-with-blockchain-and-the-internet-of-things/

[41] Gutierrez, C., and Khizhniak, A. (2017). Improving Supply Chain and Manufacturing with IoT-Driven Blockchains, Online: https://www.altoros.com/blog/ibm-aims-to-improve-manufacturing-and-supply-chain-by-coupling-iot-and-blockchain/

[42] Panetta, K. (2018). 5 Trends Emerge in the Gartner Hype Cycle for Emerging Technologies, Online: https://www.gartner.com/smarterwithgartner/5-trends-emerge-in-gartner-hype-cycle-for-emerging-technologies-2018/

[43] Nilsson, N. J. (2010). The Quest for Artificial Intelligence: A History of Ideas and Achievements, Cambridge, UK Cambridge University Press.

[44] IEEE, Tactile Internet Emerging Technologies Subcommittee, Online: http://ti.committees.comsoc.org/

[45] The Tactile Internet ITU-T Technology Watch Report ITU-T, 2014, Online: https://www.itu.int/dms_pub/itu-t/oth/23/01/T23010000230001PDFE.pdf

[46] Batra, G., Queirolo, A., and Santhanam, N. (2018). McKinsey & Company, Artificial intelligence: The time to act is now, Online: https://www.mckinsey.com/industries/advanced-electronics/our-insights/artificial-intelligence-the-time-to-act-is-now

[47] 5G Network Architecture A High-Level Perspective, (2016). White Paper, HUAWEI Technologies Co., Ltd., Online: https://www-file.huawei.com/-/media/CORPORATE/PDF/mbb/5g_nework_architecture_whitepaper_en.pdf?la=en&source=corp_comm

[48] 5G Security Architecture White Paper, (2017). HUAWEI Technologies Co., Ltd., 2017, Online: https://www-file.huawei.com/-/media/CORPORATE/PDF/white%20paper/5g_security_architecture_white_paper_en-v2.pdf?la=en&source=corp_comm

[49] Network Slicing Use Case Requirements, GSMA, April 2018, Online: https://www.gsma.com/futurenetworks/wp-content/uploads/2018/07/Network-Slicing-Use-Case-Requirements-fixed.pdf

[50] Szymanski, T. H. (2016), Securing the Industrial-Tactile Internet of Things with Deterministic Silicon Photonics Switches, IEEE Access, Vol. 4, pp. 8236–8249.

[51] Maier, M., Chowdhury, M., Prasad Rimal, B., and Pham Van, D. (2016). The Tactile Internet: Vision, Recent Progress, and Open Challenges, IEEE Communications Magazine, Vol. 54, No. 5, pp. 138–145.

[52] Maier, M. (2014). "FiWi Access Networks: Future Research Challenges and Moonshot Perspectives," Proc. IEEE Int'l. Conf. Commun.

(ICC), Workshop on Fiber-Wireless Integrated Technologies, Systems and Networks, Sydney, Australia, pp. 371–375.

[53] Chowdhury, M., and Maier, M. (2017). Collaborative Computing for Advanced Tactile Internet Human-to-Robot (H2R) Communications in Integrated FiWi Multirobot Infrastructures, IEEE Internet of Things Journal, Vol. 4, No. 6, pp. 2142–2158.

[54] Spectrum of Seven Outcomes for AI, Online: https://www.constellationr.com/

[55] Wang, R. (2016). Monday's Musings: Understand The Spectrum Of Seven Artificial Intelligence Outcomes, Online: http://blog.softwareinsider.org/2016/09/18/mondays-musings-understand-spectrum-seven-artificial-intelligence-outcomes/

[56] Chan, R., Consensus Mechanisms used in Blockchain. https://www.linkedin.com/pulse/consensus-mechanisms-used-blockchain-ronald-chan

[57] Ekblaw, A. et al. (2016). A Case Study for Blockchain in Healthcare: "MedRec" prototype for electronic health records and medical research data, https://www.healthit.gov/sites/default/files/5-56-onc_blockchainchallenge_mitwhitepaper.pdf

[58] Crosby, M. et al. (2015). BlockChain Technology. Beyond Bitcoin. Berkeley, University of California, http://scet.berkeley.edu/wp-content/uploads/BlockchainPaper.pdf

[59] Samman, G. S. (2016). How Transactions Are Validated On A Distributed Ledger, https://www.linkedin.com/pulse/how-transactions-validated-distributed-ledger-george-samuel-samman

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

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

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

[63] Yole Développement, Technologies & Sensors for the Internet of Things, Businesses & Market Trends 2014–2024, 2014, Online: http://www.yole.fr/iso_upload/Samples/Yole_IoT_June_2014_Sample.pdf

[64] Parks Associates, Monthly Wi-Fi usage increased by 40% in U.S. smartphone households, Online: https://www.parksassociates.com/blog/article/pr-06192017

[65] Gluhak, A., Vermesan, O., Bahr, R., Clari, F., Macchia, T., Delgado, M. T., Hoeer, A. Boesenberg, F., Senigalliesi, M., and Barchetti, V. (2016). "Report on IoT platform activities", 2016, Online: http://www.internet-of-things-research.eu/pdf/D03_01_WP03_H2020_UNIFY-IoT_Final.pdf

[66] McKinsey & Company, Automotive revolution – perspective towards 2030. How the convergence of disruptive technology-driven trends could transform the auto industry, 2016.

[67] IoT Platforms Initiative, Online: https:// www.iot-epi.eu/

[68] IoT European Large-Scale Pilots Programme, Online: https://european-iot-pilots.eu/

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

[70] Moore, S. (2016). Gartner survey shows wearable devices need to be more useful, Online: http://www.gartner.com/newsroom/id/3537117

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

[72] Maidment, D. (2014). Advanced Architectures and Technologies for the Development of Wearable Devices, White paper, Online: 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: https://www.accenture.com/_acnmedia/Accenture/Conversion-Assets/DotCom/ Documents/Global/PDF/Strategy_7/Accenture-Strategy-Connected-Insurer-of-Things.pdf#zoom=50

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

[74] Kejriwal, S., and Mahajan, S. (2016). Smart buildings: How IoT technology aims to add value for real estate companies The Internet of Things in the CRE industry, Deloitte University Press, Online: 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

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

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

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

[78] Roland Berger Strategy Consultants, Autonomous Driving, (2014). Online: https://www.rolandberger.com/publications/publication_pdf/roland_berger_tab_autonomous_driving.pdf

[79] Roland Berger Strategy Consultants, (2017). Automotive Disruption Radar – Tracking disruption signals in the automotive industry, Online: https://www.rolandberger.com/publications/publication_pdf/roland_berger_disruption_radar.pdf

[80] The EU General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679).

[81] RERUM, EU FP7 project, www.ict-rerum.eu

[82] Gartner Identifies the Top 10 Internet of Things Technologies for 2017 and 2018, Online: http://www.gartner.com/newsroom/id/3221818

[83] A Look at Smart Clothing for 2015, Online: http://www.wearable-technologies.com/2015/03/a-look-at-smartclothing-for-2015/

[84] Best Smart Clothing – A Look at Smart Fabrics, (2016), Online: http://www.appcessories.co.uk/best-smart-clothing-a-look-at-smart-fabrics/

[85] Brunkhorst, C. (2015). "Connected cars, autonomous driving, next generation manufacturing – Challenges for Trade Unions", Presentation at IndustriAll auto meeting Toronto 14th Oct. 2015, Online: http://www.industriall-union.org/worlds-auto-unions-meet-in-toronto

[86] Market research group Canalys, Online: http://www.canalys.com/

[87] Digital Agenda for Europe, European Commission, Digital Agenda 2010–2020 for Europe, Online: http://ec.europa.eu/information_society/digital-agenda/index_en.htm

[88] Vermesan, O., Friess, P., Woysch, G., Guillemin, P., Gusmeroli, S. 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

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

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

[91] Mobile Edge Computing Will Be Critical For Internet-of-Things and Distributed Computing, Online: http://blogs.forrester.com/dan_bieler/16-06-07-mobile_edge_computing_will_be_critical_for_internet_of_things_and_distributed_computing

[92] Stamatakis, G., Elias, T., and Apostolos, T. (2018). "Energy Efficient Policies for Data Transmission in Disruption Tolerant Heterogeneous IoT Networks." *Sensors* 18.9: 2891.

[93] Stamatakis, G., Elias, Z. T., and Apostolos, T. (2015). "Periodic collection of spectrum occupancy data by energy constrained cognitive IoT devices." *Wireless Communications and Mobile Computing Conference (IWCMC), 2015 International*. IEEE.

[94] Stamatakis, G., Elias, Z. T., and Apostolos, T. (2015). "A Two-Stage Spectrum Assignment Scheme for Power and QoS Constrained Cognitive CSMA/CA Networks." *Globecom Workshops (GC Wkshps), 2015 IEEE*. IEEE.

[95] Test Considerations for 5G New Radio, White Paper, Keysight Technologies, April 2018, online at: http://literature.cdn.keysight.com/lit web/pdf/5992-2921EN.pdf

[96] ETSI ISG Multi-access Edge Computing, online at: https://portal.etsi.org/MEC

[97] Serrano, M., and Soldatos, J. (2015). "IoT is More Than Just Connecting Devices: The OpenIoT Stack Explained" IEEE Internet of Things Newsletter, September, 8th 2015.

[98] Nagavalli, Y. (2018). Huawei Software, September 2018, Prepare Now for the 5G Monetization Opportunity, online at: http://telecoms.com/intelligence/prepare-now-for-the-5g-monetization-opportunity/

[99] Li, R. (2018). "Towards a New Internet for the Year 2030 and Beyond," Third Annual ITU IMT-2020/5G Workshop and Demo Day, Geneva, Switzerland, July 18, 2018, online at: https://www.itu.int/en/ITU-T/Workshops-and-Seminars/201807/Documents/3_Richard%20Li.pdf

[100] 5G Applications Market Potential & Readiness Matrix, Huawei Wireless X Labs and ABI Research, 2018, online at: https://www-file.huawei.com/-/media/CORPORATE/PDF/x-lab/5G-Applications-Market-Potential_Readiness-Matrix.pdf?la=en&source=corp_comm