2

Future Trends in IoT

Joël Bacquet, Rolf Riemenschneider and Peter Wintlev-Jensen

European Commission, Belgium

2.1 Introduction

The Next Generation Internet (NGI) initiative [1] aims at maintaining the European lead in advanced network infrastructures and fully exploit the opportunities offered by the connection to the physical work i.e the Internet of Things (IoT), powered by advanced computing capabilities and data infrastructure. The NGI and its link to IoT has to be at the service of people, industry and society, addressing present and specific societal challenges, combined with artificial intelligence (AI), secure transactions, sovereignty, edge computing, interactive technologies and social media, as depicted in Figure 2.1. Every technological design has to focus on making data and components easy to use and profitable in an open and democratic way to every single user.

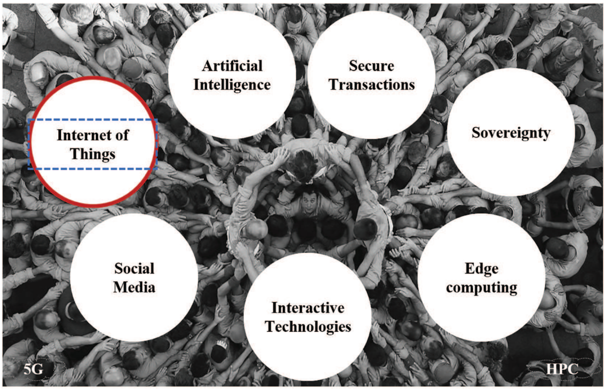

Figure 2.1 NGI Key Pillars.

IoT technologies and applications bring fundamental changes in individuals' and society's view of how technology and business work in the world, and it is therefore an essential element of the Next Generation Internet. IoT is seen today as a disruptive technology for enabling new opportunities and triggering new services and applications. However, collecting massive amounts of data in everyday life poses huge challenges for the user to keep control of his data in terms of managing access, sharing and protection. Additionally, one of Europe's greatest challenges is to keep the sovereignty of the underlying core infrastructure that computes and stores sensitive information, and protect IoT devices from misuse. The societal potential of IoT is extraordinary: better use of natural resources through smart farming, better food quality through devices enabling food traceability and control, better human health through devices linked to remote medicine and independent living, lower carbon emissions from autonomous driving and smart logistics, fewer accidents relying on connected driving, smart cities through smart use of massive data generated from a multitude of new sensors in a city.

The scope of this chapter is to review novel IoT concepts that have been gathered from groups of experts in different fora, including specific workshops organised by the European Commission, inputs the European Research Cluster on the Internet of Things (IERC), the Alliance for Internet of Things Innovation (AIOTI) and the IoT-European Platforms Initiative (IoT-EPI) cluster.

2.2 Key Technological Game Changers for IoT

Novel IoT architecture, platforms and solutions will emerge and will integrate new enabling technologies such as AI, secure Distributed Ledger Technologies (DLTs), or advanced communication networks, in order to meet new user requirements for performance, quality of services, trust and user control data. These IoT architectures, platforms and solutions will rely on the following game changers:

- Next generation IoT devices;
- Edge computing;
- Data-centric architectures;
- Community-driven business models; and
- A resilient and reliable infrastructure.

Towards Next Generation IoT devices. The IoT platform development will move in the next phase with the emergence of tactile interface based on human-centric sensing and actuating, augmented and virtual reality combined with new IoT end-point capabilities capturing contextual environment. Interactive and conversational IoT platforms will emerge with innovative user interfaces interfering with things and humans. These interactive platforms will enable real-time control, physical (haptic) experiences, interactive, context aware, event-driven IoT services with more intelligence at the edge. In supporting trust and security, information flows stay close to the user, decisions are taken at the point of interest, where data is collected and locally processed. For this to happen, the applications need to combine edge computing, IoT and mobile autonomous systems using AI technologies as functionality enablers.

Towards edge computing, shifting computing and data processing close to the source of data. The usual approach in most current IoT solutions is to execute data crunching in the cloud. In many scenarios this is the most suitable approach due to distributed nature of data collection. However, the value generated by many IoT devices decreases over time (e.g. for a thermostat control). With billions of IoT devices, it does not make sense to store all data in the cloud, but to limit data transfer to the cloud and store only information that is necessary to avoid data deluge. There are scenarios in which significant amount of data is collected at one location and the output of that local data processing is used to control a local process. In such cases, edge processing approach is desirable over processing in the cloud. For instance, this approach will require more computational capacity at device and gateway level to meet real-time requirements, preserve privacy and reduce the attack surface towards IoT devices by keeping most sensitive data local. This approach will imply a disruption from the vertical silo approach promoted by current commercial solutions, where all data are captured in cloud repositories and then fed back to the user. One of the most pertinent research tracks for edge computing will be to set the confidence level from information gathered from a cloud server, aggregated data from federated clouds and/or information retrieved from the internet. In the times of fake news, whilst experiencing novel possibilities of aggregating and manipulating data using AI, it poses unprecedented challenges for users and connected systems to set the appropriate confidence or criticality level of any external information. It remains a challenge for any future AI systems to make transparent how knowledge has been elicited that relies on trusted sources and algorithms. In contrast, edge computing novel architecture should support more decentralized decision and action support system available directly at the device level. In addition, edge computing solutions can create partial views on an environment to facilitate the decision-making process, perform data pruning, processing, anonymization, etc.

Towards data-centric architectures, dealing with the exploding volume of data generated across the different application fields and relying on AI techniques for pre-processing of data. Data storage and data flow will stress capabilities of the IoT platforms, mainly due to the large number of devices and objects, with the need of storing, processing and exchanging large amount of data in due time. Data storage is directly linked with security and privacy components, and data markets, including the availability for the regular citizen and not only corporations and stakeholders, other than with Data Sovereignty (subject to the laws of the country in which data is retrieved and located). The application of AI (mainly machine learning) across the whole IoT pipeline will have its roots in the cloud but will have to be deployed at the edge level, embedded in the things or the gateways to meet time constraints. An IoT data centre like the IBM Watson will be capable of re/defining experience and learning, detecting recurring patterns and systematic failures, in particular it will be able to adapt a holistic risk assessment of a system state in a complex environment. As said, critical functions have to be replicated and delegated to a local agent that ensures the functioning of a system even if it is offline. On the application/services side, AI-powered digital agents can act on behalf of the end users, interact with the most appropriate sensors and access the data related to the users' current activities. Up to an extent, these agents can act autonomously and proactively, for a seamless bridging of the real and digital world. Real-time intelligence provided by such lightweight agents would enable smart devices to have better understanding of their surroundings, the user's conditions and allow them to behave accordingly.

Towards community-driven business models ensuring security and privacy, building on DLTs. Novel business models and services increasingly built on social networks that are associated with daily life needs like mobility, shopping or home care, might be linked to a building, a quartier or city. We have seen success stories in the economy, like Uber, Airbnb or eBay, that have grown exponentially and that build on the fundamentals of a sharing economy. These peer-to-peer (P2P) marketplaces are driven by common interest and shared values.

In order to secure and enable growth of those P2P platforms, scale and secure technologies for authentication, authorization and accounting must evolve from isolated platforms to an ecosystem of connected platforms. DLT enables autonomy and ultimately, secures machine-to-machine (M2M) transactions without a central platform provider. Also, DLT can be a solution to manage the certificates for access to information from objects, including personal data, as well as smart contracts enabling new business models for P2P platform services. Things like money, loyalty points, intellectual property, certificates or even identity, can be sent across the globe, safely, (almost) instantly and without the need for a middle man/intermediary. Security and privacy mechanisms, based on blockchains or any other DLT, may provide new benefits and possibilities to the individual users to effectively and securely manage their personal data space, like authenticating the origin of the data and allowing the use of the data for specific stakeholders and applications, allowing the control of the re-selling of the data. The creation of micro-contracts and using cryptocurrencies may support the final benefit or revenues to the users. Traditional industrial sectors like energy, transport, or food chains may be transformed through P2P platform services, with an impact detrimental to today's business models. It remains a challenge and obligation not to ignore but to embrace P2P platforms that contribute to the growth of a community and demonstrate the opportunities of emerging technologies like DLT or blockchains for IoT platforms. DLT holds promise to mediate interactions in future decentralized IoT environments, but next-generation DLT solutions are needed to make this a reality. Current distributed ledgers seem not to be scalable and had difficulties to handle a high transaction load.

Towards resilient and reliable infrastructure. Future IoT services and applications will require infrastructures to support IoT device connectivity, data streaming and security with new requirements for service quality and reliability. Decentralized data governance and data security will be possible thanks to distributed architectures using DLT, where the control of personal data is significantly improved. But a trusted DLT platform will require beyond a protocol scalable, performant infrastructure and shared governance to establish trust and security. Another challenge for the infrastructure will be the treatment of IoT traffic which will be a major research and deployment issue, to increase availability, resilience and use of data coming from IoT. The emerging trends are related to distributed architectures, software defined technologies and new networking capabilities.

2.3 Interoperability

IoT environments are rather complex with heterogeneous physical devices supporting various communication protocols, while they are possibly connected to an intermediary gateway and then to their virtual representations (i.e. services) running on different platforms. Thus, it is possible to interact with a single IoT device in many ways using its varied interfaces and representations.

IoT platforms require interoperability on multiple levels, which means finding the characteristic functionalities of each layer and defining meta-protocols that can be mapped on the ones used in the platforms (i.e. on the level of syntactic interoperability, the characteristic functionality is resource access). A lot of work has been done in this field in particular in the IoT-EPI, which focuses mainly on architectures and semantic interoperability [2]. As an example, the INTER-IoT project [3] has defined an IoT multi-layer approach to provide semantic interoperability, as illustrated in Figure 2.2.

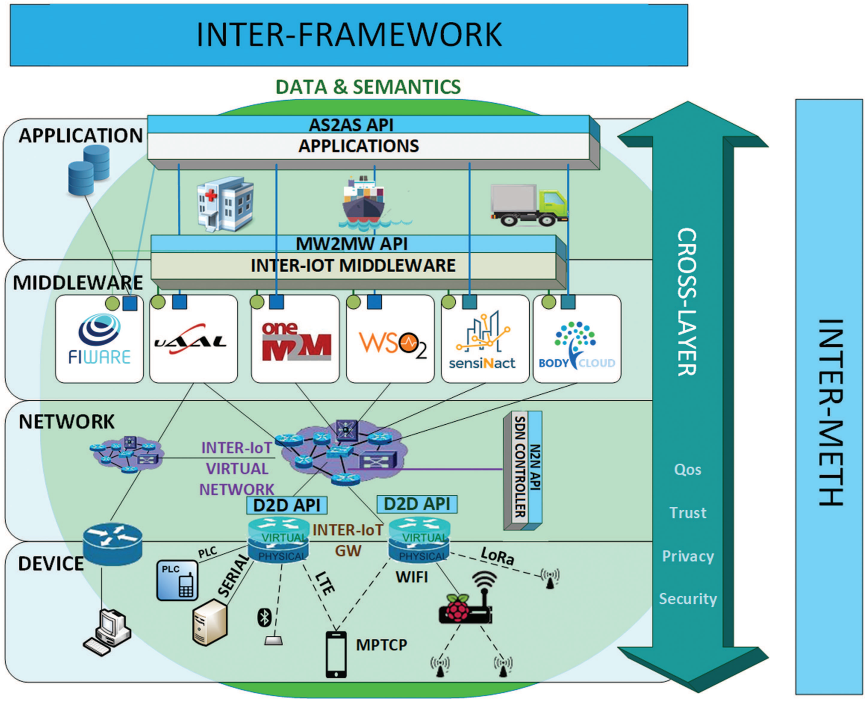

Figure 2.2 Inter-IoT Multi-layer architecture.

Nevertheless, research on a layer-oriented approach is still needed to address tighter interoperability at all layers of IoT systems (device, network, middleware, application, data and semantics) with a strong focus on guaranteeing trust, privacy and security aspects within this interoperability.

The demands of the future internet, including future IoT applications and services, will require a much larger object space, resource efficient implementation in devices, object interaction across so far siloed application spaces, as well as support for intelligent and trusted mechanisms for service provision. Standards have to support interoperability for any object to be seamlessly connected. New connected objects allow users to optimize functions in their daily life (to be safe, for entertainment and comfort, or daily activity support). This requires that objects seamlessly and securely connect, but that they are also identified due to their functionality. On semantic interoperability, despite several efforts to find common ontologies to be reused and different standardization efforts (e.g. SAREF, W3C or ETSI), in a real interoperability environment, new ontologies have to be defined, to address specific deployment. Efforts have to be devoted to semantic translation or alignment in order to provide an easy support for ontology matching between IoT platforms. Work needs to continue on common vocabularies, data models and semantic mapping techniques that could become the key technologies for semantic interoperability via common efforts on the abstract core model for IoT domains.

Under the new Focus Area on Digitisation in the Horizon 2020 Work Programme 2018–2020, the European Commission calls for a pilot on Interoperable Smart Homes and Grids under call DT-ICT-10-2018-19. IoT is expected to enable a seamless integration of home appliances with related home comfort and building automation services allowing to match user needs with the management of distributed energy across the grid. Through Digitisation of Energy, there will be much more assets connected to the grid, which are intelligently communicating with the grid. This comes with all kinds of complexities in terms of interoperability, but mainly due to a lot of different IoT platforms coming from different manufacturers and sectors, like building automation, heating, electrical vehicle charging, appliances, etc. The energy sectoral ecosystem finds itself in a transition period that entails the grid operator, the energy business and services, and the changing role of a consumer or prosumer. The interconnectivity of different systems and assets will become very powerful through IoT platforms if interoperability can be achieved across federated systems that enable the integration of data and novel services.

2.4 Boosting IoT Innovation and Deployment

In future IoT solutions, the importance of data will prevail and further grow. Measuring the economic value of data is a key challenge, focusing on the understanding of the economic value of the data instances and streams in different IoT infrastructure deployment use-cases. The openness of localized sensor data will provide new means to boost the IoT market. Providers of such data will experience new revenue streams. Moreover, new form of marketplaces will be created; that of local data marketplaces, which will also boost innovation. Especially when considering use cases like smart cities, smart transportation or smart grids, where sensing information is characterized by lot of heterogeneous and sensitive data sources, the real benefit from such kind of data markets is seized when data is shared across private, public and industrial value chains. Apart from technology enablers for data marketplaces like DLT, the European Commission favours communities and ecosystems that provide incentives for sharing data on any kind of assets or resources to create an added value through new services and applications (e.g. shared parking, car-sharing, P2P energy, etc.). It remains a challenge for public decision makers to adapt the regulatory framework for new data economy towards a Free Flow of Data, harmonization of data access across borders, data protection and portability in support of a Digital Single Market.

The IoT platform centric point of view will evolve to an ecosystem of platforms with IoT platforms, IoT nodes and sets of IoT things. Instead of IoT platform companies trying to lock-in their customers through closed system approaches, thus creating complex integration links, new common and open interoperation among all these structures will be needed. Ecosystem governance is necessary for controlling different degrees of interoperation and for managing the access to data and services across the whole ecosystem, especially for the use of personal data.

2.5 Conclusion

IoT is a key technology transversal to all sectors of activity and will be fundamental for the NGI initiative. The next generation of IoT will build on a new generation set of devices and systems that will make use of new infrastructure enhancements, better sensing and actuating capabilities, end-to-end semantic knowledge, more powerful computation capabilities on the edge, intrinsic adoption of AI from the edge to the backbone, and the ability to set-up new relationships (like smart contracts, context awareness or intelligent behaviour) among things, services and people, while respecting the human-centric concerns in terms of privacy, security, openness, sustainability and control of personal data.

The inputs collected from the relevant workshops and IoT stakeholder communities are key inspiring sources on the strategic directions needed to support future research, development and innovation of IoT in the context of the NGI initiative. These sources are major inputs to the elaboration of future research and innovation work programmes within Horizon 2020 and beyond.

References

[1] The Next Generation Internet initiative, online at: https://www.ngi.eu/

[2] IoT European Platforms Initiative – white paper on "Advancing IoT Platforms interoperability"

[3] INTER-IoT project, online at: http://www.inter-iot-project.eu/