BOOK REVIEW

Next Generation Internet of Things
Distributed Intelligence at the Edge and Human Machine-to-Machine Cooperation

Ovidiu Vermesan and Joël Bacquet
River Publishers Series in Communications
River Publishers, 2018
326 p.
ISBN 978-87-7022-008-8 (Hardback), ISBN 978-87-7022-007-1 (Ebook)

According to the Editors' opinion, the book provides an overview of the next generation Internet of Things (IoT) topics, including research, innovation, development priorities, and enabling technologies.

The chapters present global views and state-of-the-art results regarding the next generation of IoT research, innovation, development, and deployment, based on the ideas provided by the European Research Cluster, the IoT European Platform Initiative (IoT–EPI), the IoT European Large-Scale Pilots Programme and the IoT European Security and Privacy Projects.

The convergence and combination of IoT, Artificial Intelligence and other related technologies to derive insights, decisions and revenue from sensor data provide new business models and sources of monetization. New IoT distributed architectures, combined with system-level architectures for edge/fog computing, are enhansing IoT platforms, with embedded intelligence into the hyper-connectivity infrastructure.

The next generation of IoT technologies are highly transformational, enabling innovation at scale, and autonomous decision-making in various application domains such as healthcare, smart homes, smart buildings, smart cities, energy, agriculture, transportation and autonomous vehicles, the military, logistics and supply chain, retail and wholesale, manufacturing, mining and oil and gas.

The editors of the book are Ovidiu Vermesan, SINTEF, Norway, and Joël Bacquet, European Union, Belgium.

Dr. Ovidiu Vermesan holds a PhD degree in Microelectronics and a Master of International Business (MIB) degree. He is Chief Scientist at SINTEF Digital, Oslo, Norway. He is currently working on projects addressing Nanoelectronics, integrated sensor/actuator systems, communication, cyber–physical systems and the IoT, with applications in green mobility, energy, autonomous systems and smart cities. He is actively involved in the activities of the Electronic Components and Systems for European Leadership (ECSEL) Joint Technology Initiative (JTI). He is the coordinator of the IoT European Research Cluster (IERC) and a member of the Steering Board of the Alliance for Internet of Things Innovation (AIOTI).

Joël Bacquet is a senior official of DG CONNECT of the European Commission, taking care of the research and innovation policy for the Internet of Things. Before working in this field, he was programme officer in "Future Internet Experimental Platforms", head of the sector "Virtual Physiological Human" in the ICT for health domain. He started working with the European Commission in 1993, in the Software Engineering Unit of the ESPRIT Programme. From 1999 to 2003, he was head of the sector "networked organisations" in the eBusiness unit. Mr. Bacquet is an engineer in computer science having graduated from Institut Supérieur d'Electronique du Nord (ISEN) in France. He also holds an MBA from Webster University, Missouri, USA.

The book is structured in eight chapters. Each chapter starts with a list of the key concepts addressed, its objectives and logical connection with previous chapters' contribution. At the end of each chapter a summary of its main conclusions and references to subsequent chapters that are based on its content as well as the bibliography are provided.

https://doi.org/10.24846/v28i2y201912

Chapter 1 – "*IoT EU Strategy, State of Play and Future Perspectives*", author Mechthild Rohen – EU, describes Digitising European Industry (DEI) strategy, published in 2016, where IoT is a priority of the digitisation process of the economy and society. As part of the DEI strategy, the goal for achieving the IoT leadership is based on several building blocks funded under Horizon 2020: the IoT-European Platforms Initiative (IoT-EPI), the focus areas on IoT under Crosscutting (2016–2017) and on Digitising and transforming European industry and services (2018–2020). With regard to IoT-EPI seven research and innovation projects and two coordination and support actions are mentioned, involving a total funding of EUR 50 million and a partner network of 120 organizations. The IoT Focus Area supports the IoT European Large-Scale Pilots Programme (IoT-LSPs) which started on 1st of January 2017, with a budget of EUR 100 million, in the following domains: smart living environments for ageing well, smart farming and food security, wearables for smart ecosystems, reference zones in EU cities, and autonomous vehicles in a connected environment.

Chapter 2 – "*Future Trends in IoT*", authors Joël Bacquet, Rolf Riemenschneider and Peter Wintlev-Jensen, starts with an overview of the Next Generation Internet (NGI) initiative, which aims at maintaining the European lead in advanced network infrastructures. Then the key technological game changers, providing support for novel IoT architectures, platforms and solutions are detailed: next generation IoT devices, edge computing, data-centric architectures, community-driven business models, and a resilient and reliable infrastructure. The next section is devoted to the interoperability as a key concept for modern IoT platform architecture. The results obtained so far in EU funded projects are overviewed. More research is still needed for the layer-oriented approach 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 objectives of boosting IoT innovation and deployment are presented in the last section of this chapter. The IoT platform centric point of view will evolve to an ecosystem of platforms with IoT platforms, IoT nodes and sets of IoT things. The role of ecosystem governance will increase so that it may control different degrees of interoperation and manage the access to data and services across the whole ecosystem, especially for the use of personal data.

Chapter 3 – "*The Next Generation Internet of Things – Hyperconnectivity and Embedded Intelligence at the Edge*", authors Ovidiu Vermesan, Markus Eisenhauer, Martin Serrano, Patrick Guillemin, Harald Sundmaeker, Elias Z. Tragos, Javier Valinos, Bertrand Copigneaux, Mirko Presser, Annabeth Aagaard, Roy Bahr, and Emmanuel C. Darmois, is based on the idea that IoT and industrial IoT (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). The Next Generation IoT Strategic Research and Innovation is discussed in relation with the activity of the IoT European Research Cluster (IERC). The list of main open research challenges for the future of IoT is provided, with the focus on: digitisation, which creates a great amount of information that reveals how objects work internally and as elements of more complex setups; the tactile IoT/IIoT - a shift in the collaborative paradigm, adding human centred perspective and sensing/actuating capabilities transported over the network; and digital twins for IoT - virtual representations of material assets, using increasingly more advanced technology for their implementation. Further, future IoT enabling technologies (edge computing, AI, networks and communication technologies, and DLT) are detailed. Also, the role of emerging distributed end-to-end security technologies to enhance the ability of an IoT ecosystem to face independently or collectively the current security threats are detailed. The standard security services (e.g. identification, authentication, authorization, availability, confidentiality, integrity, non-repudiation, a root of trust, and secure update) that are valid for the Internet framework and technology should be extended and adapted so that IoT technologies can be applied. The chapter ends with the evaluation of the IoT/IIoT Technology Market Developments, underlining the importance of the digital business model innovation and IoT as a driver and considering the expected grow of the global market for IoT that will reach $1,567 billion by 2025.

Chapter 4 – "*End-to-end Security and Privacy by Design for AHA-IoT Applications and Services*",

authors Macrio Diaz Nava, Armand Castillejo, Sylvie Wuidart, Mathieu Gallissot, Nikolaos Kaklanis, Konstantinos Votis, Dimitrios Tzovaras, Anastasia Theodouli, Konstantinos Moschou, Aqeel Kazmi, Philippe Dallemagne, Corinne Kassapoglou-Faist, Sergio Guillen, Giuseppe Fico, Yorick Brunet, Thomas Loubier, Stephane Bergeon, Martin Serrano, Felipe Roca, Alejandro Medrano and Byron Ortiz Sanchez, describes the cybersecurity and privacy methodologies and solutions that the architecture defined in the ACTIVAGE - "Active and Healthy Ageing" large-scale pilot, and the corresponding implementation in nine deployment sites should follow to secure the IoT systems and protect the personal data from potential malicious cyber-attacks and threats. The EU activities to promote cyber resilience across the EU are presented, including the Large-Scale Pilots to deploy IoT systems in five main areas, with the main goals to solve key practical issues such as interoperability, security and privacy, business models, validation of IoT powered applications and services at large-scale. In this context, the chapter reports the initial outcomes obtained from security and privacy performed in the ACTIVAGE - project. The final section of this chapter is devoted to two use cases illustrating the security and privacy implementation: the countermeasures implemented to secure the data of the Raspberry PI Gateway, and several scenarios where the Blockchain technology can be used to provide efficient solutions on security and privacy.

Chapter 5 – "*Use Cases, Applications and Implementation Aspects for IoT Interoperability*", authors Regel Gonzalez-Usach, Carlos E. Palau, Matilde Julian, Andrea Belsa, Miguel A. Llorente, Miguel Montesinos, Maria Ganzha, Katarzyna Wasielewska and Pilar Sala, emphases the role of interoperability as a very complex and difficult challenge in IoT. The INTER-IoT solution for platform-to-platform interoperability, across any IoT layer and any application domains is presented and relevant use cases of its implementation in the domains of e-Health, AHA, AAL, Transport and Logistics are discussed. With this aim, the chapter is structured as following:

- current interoperability State of the Art;
- Inter-IoT approaches for implementation: multilayer approach, virtualization of each INTER-IoT layer interoperability solution, universal semantic translation, methodology and tools for guiding the implementation, middleware for the interconnection of platforms, and the virtual gateway;
- Inter-Iot use cases and applications: INTER-Health (lifestyle monitor from the medical perspective, INTER-IoT integration of health platforms, INTER-Health technical functionalities, INTER-Health pilot); INTER-LogP in smart transport & logistics (pilot for access control at the port area, pilot for health accident at the port area); ACTIVAGE for active and healthy ageing (active and healthy ageing initiative, use cases for enabling an assisted living environment in elder homes, to allow the elderly to live at home in a safe and autonomous way); other potential use cases (e.g. Smart Cities).

The INTER-IoT interoperability framework provides innovative elements, such as an universal semantic platform-to-platforms translator, a middleware that enables the interconnection and interoperation of any platform at middleware level, despite of the standards and formats employed, and a partially virtualized gateway. Furthermore, INTER-IoT implementation is guided and eased through a novel methodology (INTER-METH) specifically designed for this aim. Also, INTER-IoT facilitates the creation of natural human interfaces in IoT systems and the integration of IoT with Artificial Intelligence.

Chapter 6 – "*Smart Data and the Industrial Internet of Things*", authors Christian Beecks, Hassan Rasheed, Alexander Grass, Shreekantha Devasya, Marc Jentsch, Jose´ A´ ngel Carvajal Soto, Farshid Tavakolizadeh, Anja Linnemann and Markus Eisenhauer, is dedicated to the current priorities in digitizing the industrial sector with cyber-physical systems, IoT technologies, cloud computing services, and Smart Data analytics, which leads to the fourth industrial revolution. The aims of the EU Framework Programme for Research and Innovation the two Public-Private Partnership (PPP) initiatives - Factories of the Future (FoF) and Sustainable Process Industry (SPIRE) are underlined. The main focus is put on two EU projects conducted by the Fraunhofer Institute for Applied Information Technology (FIT):

- the MONSOON (MOdel based coNtrol framework for Site-wide OptimizatiON of data-intensive processes) project, which aims to

establish a data-driven methodology to support the identification and exploitation potentials by applying multi-scale model based predictive controls in production processes;

- the COMPOSITION (Ecosystem for COllaborative Manufacturing PrOceSses – Intra- and Interfactory Integration and AutomaTION) project that has two main goals: (a) to integrate data along the value chain inside a factory, and (b) to create a semi-automatic ecosystem, incorporating and inter-linking both the Supply and the Value Chains.

The main conclusion is that data-driven investigations in industrial environment require a solid platform for handling data analytics at scale.

Chapter 7 – "*IoT European Security and Privacy Projects: Integration,* authored by a large team of specialists representing 38 research and industrial organizations across EU, presents an overview of the eight projects that are part of the European IoT Security and Privacy Projects initiative (IoT-ESP) addressing advanced concepts for end-to-end security in highly distributed, heterogeneous and dynamic IoT environments.

The BRAIN-IoT (model-Based fRamework for dependable sensing and Actuation in INtelligent decentralized IoT systems) project focuses on complex scenarios, where actuation and control are cooperatively supported by populations of heterogeneous IoT systems. BRAIN-IoT is developed according to the principle that future IoT services should exist within a federated/evolving environment. Two use cases are presented: in service robotics (to assist humans in a logistics domain) and the critical water infrastructure monitoring and control (management of the water urban cycle in metropolitan environment).

The CHARIOT (Cognitive Heterogeneous Architecture for Industrial IoT) project provides a design method and cognitive computing platform supporting a unified approach towards Privacy, Security and Safety (PSS) of IoT systems. The technical objectives of the project are detailed. The phases of technical implementation are described, and the system demonstration, validation and benchmarking prospects are overviewed.

The ENACT (Development, Operation, and Quality Assurance of Trustworthy Smart IoT Systems) project introduces a new enabler to support the risk driven and context-aware planning of IoT systems development, including mechanisms to facilitate the selection of the most relevant and trustworthy devices and services to be used in future stages. Three use cases from the Intelligent Transport Systems (Rail), eHealth and Smart Building application domains will guide, validate and demonstrate the project results.

The IoTCrawler (Search Engines for Browsing the Internet of Things) project proposes efficient and scalable methods for crawling, discovery, indexing and ranking of IoT resources in large-scale cross-platform and cross-disciplinary systems and scenarios. It provides novel approaches to support an IoT framework of interoperable systems including security and privacy-aware mechanisms, and offers new methods for discovery, crawling, indexing and search of dynamic IoT resources. The architecture of the IoT Crawler is detailed and four use cases are introduced: Smart City, Social IoT, Smart energy and Industry 4.0.

The SecureIoT (Multi-Layer Architecture for Predictive End-to-End Internet-of-Things Security) project is motivated by the need to support cyber-security in scenarios involving cross-platform interactions and interactions across networks of smart objects (i.e. objects with semi-autonomous behaviour and embedded intelligence), which require more dynamic, scalable, decentralized and intelligent IoT security mechanisms. The SecureIoT architecture and its main principles are introduced, the security services to be offered by the project are discussed, and some use cases (industrial plants' security, socially assistive robots, connected cars) used to validate the project's results are presented.

The SEMIoTICS project has the goal to develop a pattern-driven framework, built upon existing IoT platforms. Specifically, the SEMIoTICS vision in delivering smart, secure, scalable, heterogeneous network and data-driven IoT is based on two key features: pattern-driven approach and multi-layered embedded intelligence. Three use cases are presented: renewable energy – wind energy (localized edge analytics for wind turbine control), healthcare (advanced fall prevention aimed at both senior citizens and adults with mild cognitive impairment) and generic IoT & smart sensing (IoT things with capabilities to learn from and act upon the data they are sensing).

The SerIoT project aims to deliver a secure, open, scalable and trusted IoT architecture that will be implemented and tested as a complete, generic solution to create and manage large scale IoT environment operating across IoT platforms and paying attention to security problems. The SerIoT architecture is divided into the following layers: IoT data acquisition, ad-hoc anomaly detection, visual analytics and decision support tools, mitigation and counteraction module. The project use cases are devoted to: smart cities (surveillance and intelligent transportation IoT networks), flexible manufacturing (detection of physical attacks on wireless sensor networks), and a novel food chain scenario.

The SOFIE (Secure Open Federation for Internet Everywhere) will design, implement and pilot a systematic, open and secure way to establish new business platforms that utilise existing IoT platforms and distributed ledgers. Its technical approach combines several IoT platforms and distributed ledgers into a federated IoT platform supporting the reuse of existing IoT infrastructure and data by various applications and businesses. Through the usage of distributed ledgers, SOFIE will promote open business platforms, allowing the creation of new kinds of decentralised open marketplaces. The project use cases are a food chain pilot, the mixed reality mobile gaming pilot, and the energy pilot supporting electricity marketplaces and micropayments.

Chapter 8 – "*CREATE Your IoT*", authors Luis Miguel Girao, So Kanno, Maria Castellanos and Patricia Villanueva, describes the background and origin of the artistic series *CREATE Your IoT*, being created and hosted at the heart of the EU Large-Scale Pilots Programme (LSPs). A methodology for integrating ICT and arts or to include artistic practices in the ICT development cycle was designed to be fully adaptable. The methodology is intended to be applied in the specific areas of innovation of the IoT LSPs initiative: food and farming, healthy aging, public mass events, self-driven vehicles and smart cities. The current result of the work undertaken consists of a series of works aiming at pointing out ways of how other innovative actions can be implemented on top of the developments made available by LSPs.

Overall, the book "*Next Generation Internet of Things - Distributed Intelligence at the Edge and Human Machine-to-Machine Cooperation*", edited by O. Vermesan and J. Bacquet, provides a wealthy of up-to-date information about the current trends in IoT development, basic technologies supporting the next generation IoT/industrial IoT (5G, artificial intelligence, Distributed Ledger Technologies, edge/fog computing, virtual/ augmented reality), new IoT distributed architectures and platforms, and a large variety of application domains. The content of the book is based on research, development and innovation activities at the European level, under the coordination of prominent initiatives and programmes supporting the IoT domain. An important contribution of the book consists in the presentation of main research results and use cases provided by relevant RDI European projects in progress. For all these reasons, the book should be of interest for a large category of professionals in this field, including technical policy building decision makers, researchers and developers, PhD students.

Reviewed by:

Gabriel NEAGU, PhD
Senior Research Scientist
National Institute for R&D in Informatics - ICI Bucharest