



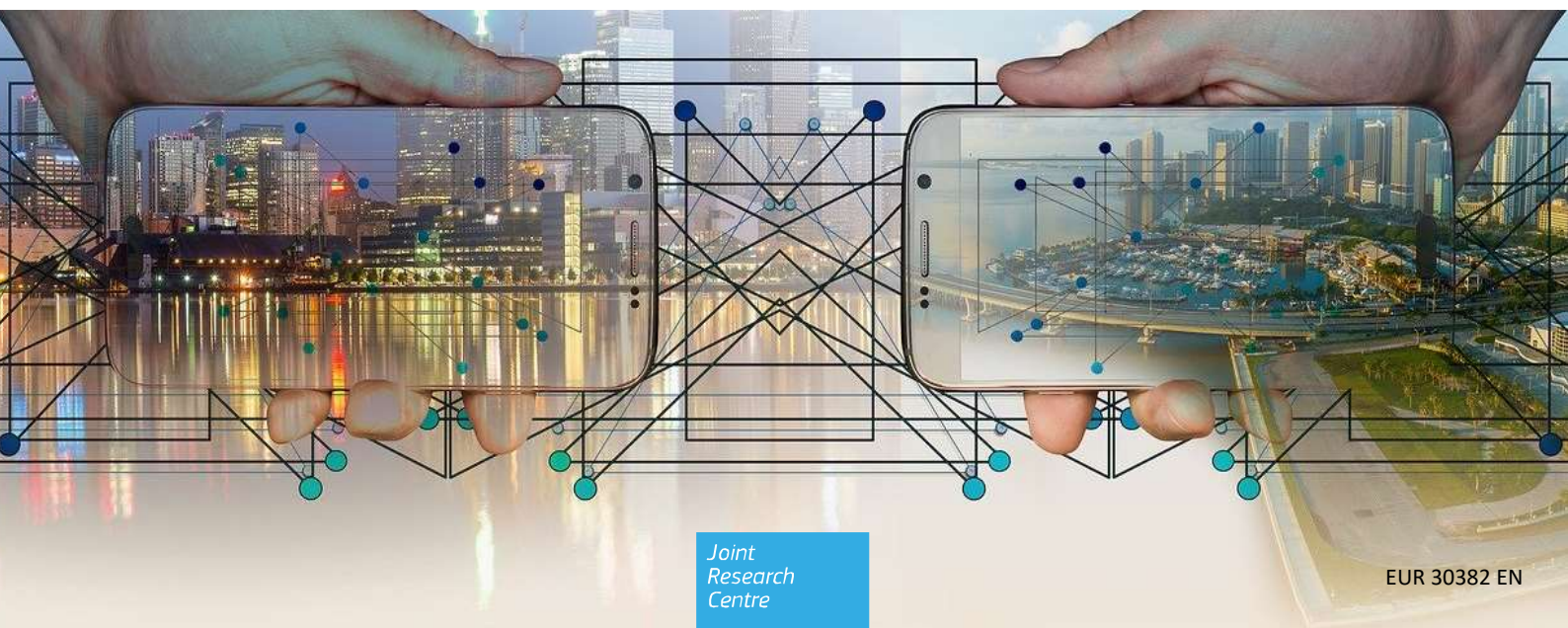
JRC TECHNICAL REPORT

IoT 2.0 and the INTERNET of TRANSFORMATION (Web of Things and Digital Twins)

A multi-facets analysis

Stefano NATIVI, Alexander KOTSEV, Petra SCUDO,
Katarzyna POGORZELSKA, Ioannis VAKALIS,
Alessandro DALLA BENETTA, Andrea PEREGO.

2020



This publication is a Technical report by the Joint Research Centre (JRC), the European Commission's science and knowledge service. It aims to provide evidence-based scientific support to the European policymaking process. The scientific output expressed does not imply a policy position of the European Commission. Neither the European Commission nor any person acting on behalf of the Commission is responsible for the use that might be made of this publication. For information on the methodology and quality underlying the data used in this publication for which the source is neither Eurostat nor other Commission services, users should contact the referenced source. The designations employed and the presentation of material on the maps do not imply the expression of any opinion whatsoever on the part of the European Union concerning the legal status of any country, territory, city or area or of its authorities, or concerning the delimitation of its frontiers or boundaries.

Contact information

Name: Stefano Nativi
Address: Via E. Fermi 2749, 21027 Ispra (VA), Italy
Email: stefano.nativi@ec.europa.eu
Tel.: +39 0332 785075

EU Science Hub

<https://ec.europa.eu/jrc>

JRC120372

EUR 30382 EN

PDF ISBN 978-92-76-22403-7 ISSN 1831-9424 doi:10.2760/553243

Luxembourg: Publications Office of the European Union, 2020

© European Union, 2020



The reuse policy of the European Commission is implemented by the Commission Decision 2011/833/EU of 12 December 2011 on the reuse of Commission documents (OJ L 330, 14.12.2011, p. 39). Except otherwise noted, the reuse of this document is authorised under the Creative Commons Attribution 4.0 International (CC BY 4.0) licence (<https://creativecommons.org/licenses/by/4.0/>). This means that reuse is allowed provided appropriate credit is given and any changes are indicated. For any use or reproduction of photos or other material that is not owned by the EU, permission must be sought directly from the copyright holders.

All content © European Union, 2020, except: page 14 –figure 1: curved arrows (Wikimedia/Amada44/CC0); page 19 –figure 2, Self Driving Car Sensor icon (Berkah Icon from the Noun Project); page 19 –figure 2, sensor icon (Larea from the Noun Project); page 19 –figure 2, switcher icon (Wikimedia); page 19 –figure 2, edge computing icon (TierPoint); page 19 –figure 2, ; page 19 – figure 2, didtributed DB icon (PNGio.com); page 19 –figure 2, AI icon (oNline Web Fonts); page 19 –figure 2, people icon (oNline Web Fonts); page 20 –figure 3, avatar icon (<https://pickaface.net/>); page 20 –figure 3, API icon (https://www.freepik.com/freeicon/api_878052.htm) ; page 20 –figure 4, gear icons (clipart library); page 20 –figure 4, switcher icon (Wikimedia); page 20 – figure 4, cell-phone icon (clipart library); page 20 –figure 4, server-multiple (Wikimedia/RRZEicons); page 20 –figure 4, disk storage icon (nicePNG); page 20 –figure 4, GUI icon (cleanPNG/Waita); page 20 –figure 4, API icon (https://www.freepik.com/free-icon/api_878052.htm); page 30 –figure 5 (Mozilla/ <https://iot.mozilla.org/wot/>); page 32 –figure 6 (AIOTI/ <https://aioti.eu/wp-content/uploads/2019/09/AIOTI-Priorities-2019-2024-Digital.pdf>); page 43 –figure 9 (IDC/https://www.idc.com/downloads/IoT_Taxonomy_Map_V2_Nov2014.pdf); page 67 –figure 20 (OGC); page 81 –figure 21 and 22 (W3C); page 82 –figure 23 (W3C).

How to cite this report: Stefano NATIVI, Alexander KOTSEV, Petra SCUDDO, Katarzyna POGORZELSKA, Ioannis VAKALIS, Alessandro DALLA BENETTA, Andrea PEREGO. "IoT 2.0 and the INTERNET of TRANSFORMATION (Web of Things and Digital Twins)", EUR 30382 EN, Publications Office of the European Union, Luxembourg, 2020, ISBN 978-92-76-22403-7, doi:10.2760/553243, JRC120372.

CONTENTS

- Acknowledgements4
- EXECUTIVE SUMMARY5
- Scope7
- INTRODUCTION.....8
- Terminology and IOT standard definition9
- 1. Methodology 12
 - 1.1 Strategy for the analysis of innovative digital technologies 12
 - 1.2 Evaluation Phase data sources..... 12
- 2. IoT Reference Framework..... 14
- 3. IoT (communications) protocols: Gateways implementations 17
- 4. Security aspects 18
- 5. IoT platforms and ecosystems –implementing the IoT Reference Framework 19
- 6. Convergence time: addressing interoperability challenges 20
 - 6.1 Converging process 20
 - 6.1.1 Amazon, Apple, Google agreed to develop common standards: “Project Connected Home over IP” 20
 - 6.1.2 OCF..... 20
 - 6.1.3 OneM2M..... 21
 - 6.1.4 AIOTI: Contributing to a dynamic European IoT ecosystem..... 21
 - 6.1.5 OMA SpecWorks: for a connected world..... 21
 - 6.2 Mozilla IoT and WebThings 22
- 7. The W3C Web of Things (WoT) initiative 23
 - 7.1 WoT Vision and methodology..... 23
- 8. IoT 2.0, Digital age, local data Ecosystems and the Internet of transformation 24
 - 8.1 Internet of Transformation: IoT 2.0 as the engine of Digital Transformation..... 25
 - 8.1.1 Internet of Everything (IoE), Industrial Internet, Industrial IoT (IIoT), and Consumer IoT (CIoT)26
- 9. IoT Taxonomy 27
 - 9.1 Application Domains View..... 27
 - 9.1.1 Industrial Internet of Things (IIoT) 27
 - 9.1.2 Smart Home/Intelligent Home/Smart Buildings 28
 - 9.1.3 Energy/Smart grids/Renewable Energies/Oil & Gas 28
 - 9.1.4 Smart Cities 28
 - 9.1.5 Health/Wellness/Medical/Biosensing 28
 - 9.1.6 Environment and Climate 29
 - 9.1.7 Security, Safety, Defence and Military 29
 - 9.1.8 Agriculture, Livestock, Food 29

| | | |
|--------|--|----|
| 9.1.9 | Industry 4.0 –Manufacturing, Construction and Distribution | 29 |
| 9.1.10 | Business 4.0 –Private sector services, Retail, Customer experience | 29 |
| 9.1.11 | Multimodal Transport, Logistics, Mobility and Traffic | 29 |
| 9.2 | Things (or connected object) View | 29 |
| 9.3 | Sensor-based View | 31 |
| 9.4 | Projects/initiatives View | 31 |
| 9.5 | Industrial Framework View | 34 |
| 10. | Analysis of IoT Uptake: Emerging Trends..... | 36 |
| 10.1 | Patents data | 36 |
| 10.2 | Scientific Publications and Research projects data | 37 |
| 10.3 | Investment data | 37 |
| 10.4 | Social network data | 37 |
| 11. | Data sources analysis | 38 |
| 11.1 | Patent inventions per sector | 38 |
| 11.2 | Patent inventions generation countries..... | 39 |
| 11.3 | Patent inventions registration countries..... | 40 |
| 11.4 | Patent inventions growth..... | 41 |
| 11.5 | Scientific publications per sector and per country | 42 |
| 11.6 | Scientific publication keywords | 43 |
| 11.7 | Financial Landscape..... | 44 |
| 11.8 | Twitters analysis results | 45 |
| 12. | IoT in Europe – regulatory and legal aspects..... | 47 |
| 13. | Conclusions and Future work | 48 |
| | Bibliography | 49 |
| | ANNEX A. OGC SensorThings API | 54 |
| | ANNEX B. IoT Protocols..... | 56 |
| | Narrowband-IoT | 56 |
| | ZigBee | 56 |
| | LoRa (LoRaWAN)..... | 56 |
| | Thread | 56 |
| | DASH7 Alliance Protocol (D7A)..... | 57 |
| | Sigfox | 57 |
| | NFC (Near-Field Communication) | 57 |
| | ANNEX C. Security of IoT Protocols | 58 |
| | Narrowband-IoT | 58 |
| | ZigBee | 58 |
| | LoRa (LoRaWAN)..... | 58 |
| | Thread | 59 |

| | |
|---|-----|
| Dash7..... | 59 |
| Sigfox | 59 |
| NFC | 59 |
| ANNEX D. IoT Reference Framework Implementation Solutions..... | 61 |
| Amazon Web Services (AWS) IoT | 61 |
| Google IoT | 61 |
| Apple HomeKit..... | 62 |
| Samsung SmartThings | 62 |
| IBM Watson IoT Platform | 63 |
| Bosh IoT Platform | 63 |
| Azure Digital Twins..... | 63 |
| Open sources solutions/platforms..... | 63 |
| ANNEX E. W3C WoT: Web Thing specification | 65 |
| WoT Abstract Architecture | 65 |
| WoT Building Blocks | 66 |
| ANNEX F. Data Mining Queries | 68 |
| ANNEX G. Figures characterizing the different IoT Domains | 69 |
| Industry 4.0 | 69 |
| Agriculture | 74 |
| Food chain..... | 80 |
| Health, Medical and Pharmaceutical..... | 86 |
| Military and Defence | 92 |
| Renewable energy | 97 |
| Smart City..... | 102 |
| Smart Grid/Smart Power | 107 |
| Smart Home | 112 |
| ANNEX H. IoT Legal Regulation | 117 |
| EU IoT Policy..... | 117 |
| Electronic communications and radio spectrum | 117 |
| Standardisation..... | 119 |
| Cybersecurity..... | 120 |
| Protection of personal data and privacy..... | 121 |
| Liability | 122 |
| IoT -the DSM layer | 123 |
| List of figures | 125 |
| List of tables | 126 |

Acknowledgements

The authors of this report would like to express their gratitude to Gianluca Misuraca, Maciej Sobolewski, Daniel Nepelski, Giuditta De Prato, Paul Desruelle, Lorenzino Vaccari, Michael Lutz, and Sven Schade for their contribution in the discussion about the technology evaluation methodology (in the framework of the B6 Technology Task Team) and the useful keywords to be used for the data mining to survey IoT technology maturity.

The authors also thank Geraldine Joanny (JRC I.3), Audrey Dayon (Questel), Dalbir Grewal (PitchBook), and Silvia Sarti (JRC B.6) for their support and help with the instruments and processes utilised for this study.

Finally, the authors thank Sven Schade for the document revision that helped to improve it.

Authors

Stefano NATIVI, Alexander KOTSEV, Petra SCUODO, Katarzyna POGORZELSKA, Ioannis VAKALIS, Alessandro DALLA BENETTA, Andrea PEREGO.

EXECUTIVE SUMMARY

Digitalization has moved humanity in a new industrial and social era. The transformation that it causes has a significant effect also on democracy and on the sovereignty of the European citizens. The Internet of Things (IoT) is one of the key engines of this digital transformation. IoT as a concept can be defined as a digital framework allowing data to be generated, transported, stored, and analysed to create actionable intelligence. IoT platform contributes to and is ingested by the ‘datafication’ process that is at the core of the digital transformation of our society. There exist several possible taxonomies to characterise an IoT ecosystem, reflecting different views representing diverse needs, requirements, and solutions.

The analysis of the IoT technological landscape shows that there is no one single IoT framework, but rather a fragmented scenario of many IoT (proprietary) solutions. This factor has turned out to constrain the development of this important industrial sector. To address that, recently, significant converging trends and industry alliances emerged –e.g. the Amazon, Apple, Google, and Zigbee Alliance to create a common IP-based protocol. Nevertheless, there is still a long way to reaping the full potential of IoT.

Notably, many IoT developments are still considered insecure for a broad range of reasons. Security and privacy aspects are particularly important for IoT communication and transport protocols. With the increasing IoT uptake, the issues associated to security and privacy are becoming more and more demanding. Because of the great number of IoT platforms using a variety of protocols and standards, different security techniques have been implemented. A standardization and convergence process would help to improve the current situation.

In the recent years, IoT has brought important changes and innovations across a broad spectrum of application domains. While the impact of IoT on industry (i.e. IIoT) is still to be fully understood, it becomes clearer and clearer that the emergence of a new generation of IoT, IoT 2.0, has significantly enabled the digital transformation of our society –for this reason, IoT 2.0 is also called the Internet of Transformation. This new paradigm builds on top of existing digital infrastructures and, taking care of connecting as many living (persons) and non-living entities (things) as possible, generates actionable intelligence by leveraging the integration and analytics of the data shared by the connected entities. IoT 2.0 pushes innovative interaction patterns, including Digital Twins, Augmented and Virtual Reality. To fully understand the role of the IoT in the digital transformation, it is necessary to look at it as part of a whole (i.e. a global technological framework), where IoT is inherently interconnected with other disrupting technologies, such as big data and Artificial Intelligence (AI). This essential evolution is at the core of introducing the concept of IoT 2.0. While IoT has connected billions of sensors to Internet, IoT 2.0 promises to make them smart and revolutionize the digital-physical interaction patterns –see Digital Twins. This can significantly help Europe in implementing its strategic plans and noticeably the Green Deal priority. The most frequent topics investigated by the scientific publications deal with challenges and opportunities characterizing: the wireless sensor networks, the cyber-physical interactions, and the security.

IoT first and second generation are a massive market. Financing has escalated since 2015-2016 also due to the significant contributions from sectors such as “smart” home and cities and connected services. Another important support has come from the development of IoT software platforms, which recently mobilized significant investments. In particular, these platforms are likely to be the battlefield of the big IT/Web companies in the next years. They are a technology cornerstone for the digital transformation of society.

The number of patent inventions and companies/investors are not necessarily correlated, for each sector. The maturity of a given sector and the importance/role of its top-10 organizations are other important factors to be considered. Therefore, while “Food Chain” is the largest sector in terms of patent inventions and registrations, “Smart City” is largely dominant in the finance landscape. Finally, “Smart Home” performs very well in both the categories, scoring the richest top investment.

Asia (i.e. China and South Korea) dominates the top-ten list of private and public organizations that originated and registered inventions. USA is well present (through their multi-national ICT companies). European organizations are not present in the top-10 list, with the exception of the “Industry 4.0” sector. For all investigated application domains, by far the highest number of patent requests cover China, while the world coverage is much less. It remains to study whether this is predominantly caused by the need of the other industrial countries to protect their IPR in the fastest and largest growing area of the world, or it is (also) a consequence of the Chinese domestic technological developments. The number of patent inventions and companies/investors are not necessarily correlated with the number of publications, in the diverse domains. From a temporal point of view, the interest in IoT is evident as of 2012-2013, for both patents and scientific publications. While, for investments (in the sectors we got data) the escalation years were 2013-2014.

Global and regional stakeholders are called to work together and address the barriers that are presently limiting the IoT market. EU might provide an open and inclusive approach based on shared values such as openness, trust, and multilateralism. European and international standardization initiative can play an important role, too. As expected, innovation patents are generally registered in Europe, for all the IoT sectors. However, European organizations are part of the top-10 inventors only for the “Industry 4.0” sector.

Scientific publications monitoring clearly shows that EU (also through its Research Framework programmes) is a research and innovation powerhouse. EU is notably one of three major research regions globally, along with China and USA. While, both Chinese and US organizations submit and own more patents, Europe has a leading role in terms of publications. The means for taking advantage of this scientific leadership into innovation and value-added technology remains open.

The rapid social uptake of IoT provides important opportunities and some significant challenges, noticeable security and privacy. For a fully adoption of IoT, there exist some legal barriers, which can be linked both to the existing regulations and to the lack of specific regulations. A comparison of IoT regulations in Europe, China and the USA shows that EU has the highest level of regulations applying to IoT environment. They are more than twice of the regulations existing in USA. If not coordinated and aligned, these regulations may be a barrier to adoption, especially because most of them do not take into account the specificity of IoT environment –e.g. regulations for telecoms.

In the European Union (EU), the General Data Protection Regulation (GDPR) and its associated tools can provide a valuable example of an approach and a legal framework for an ethical and human-centric utilization of personal IoT data. An analogous framework might also be considered for non-personal/industrial/sensor data.

To complete the analysis, we also considered the social viewpoint by processing the data shared by a popular social instrument: Twitter. The analysis results show that IoT 2.0 makes use of AI and Big Data. A key determinant of IoT 2.0 is cybersecurity –in particular, Blockchain. IoT plays an important role in the supply-chain area. Investments and Asia are two important factors that influence IoT success. Finally, the utilization of IoT transforms a domain into a “smart” domain.

SCOPE

This JRC report aims to investigate the maturity level of Internet of Things (IoT) on-going development and reflect upon its contribution to the digital transformation of our society.

Besides, the document tries to identify possible challenges and opportunities by analysing some global data sources. In doing that, we also assessed the advantages and limitations of using multiple different data sources. The analyses results can be used as a starting point for a further and more systematic socio-economic analysis.

This document is a result of a more general work of JRC.B6 that developed a methodological approach for the identification of emerging technological trends to be applied universally in different technological domains.

INTRODUCTION

This JRC report reports the JRC B.6 work on the identification and first evaluation of emerging trends within the Internet of Things (IoT) and Internet of Transformation domains, also considering the broader context of increasingly diverse digital technology ecosystems.

The report is divided into **13 interdependent sections** and **eight annexes** that contains the material necessary document and deepen the sections content. An **introductory section** deals with IoT definition and some significant standardization activities.

Section 1 presents the applied methodology and our analysis strategy. **Sections 2, 3, 4,** and **5** provide a survey of the IoT universe of discourse, including the technological aspect; definitions and architectures, which are relevant for the rest of the document. In particular, **Section 2** defines a technology-neutral reference framework for IoT ecosystems, while **Sections 3** and **4** provide an overview of the most prominent protocols and security standards in the field. **Section 5** recognizes the main existing commercial and open solution to implement the introduced reference framework. The ongoing standardization and convergence effort, among these platforms and with the present analytics infrastructures, are discussed in **Sections 6** and **7**. This convergence process is enabling the second generation of IoT (i.e. IoT 2.0) and thus the Internet of Transformation; they are both introduced in **Section 8**. **Section 9** deals with the possible diverse Taxonomies characterizing IoT domain. **Sections 10** and **11** deal with the analysis of IoT uptake in the scientific and industrial sectors of our society. **Section 12** addresses regulatory and legal aspects and finally **Section 13** presents conclusions and future work.

TERMINOLOGY AND IOT STANDARD DEFINITION

For the scope of this report, before defining the term Internet of Things (IoT), it is useful to introduce a set of terms belonging to the IoT universe of discourse.

Things

IoT involves the connecting of physical entities (“things”) with IT systems through networks [1].

Sensors and Actuators

Foundational to IoT are the electronic devices that interact with the physical world. Sensors get the information from the physical world, while actuators act upon it [1]. Both sensors and actuators can be in many forms: thermometers, accelerometers, video cameras, microphones, relays, heaters or industrial equipment for manufacturing or process controlling [1].

IoT enabling Technologies

Mobile technology, cloud computing, big data and deep analytics (predictive, cognitive, real-time and contextual) play important roles for the IoT, by gathering and processing data to achieve the final result of controlling physical entities and impacting virtual entities [1].

IoT Platform

An IoT platform is a specific component of an IoT ecosystem, such as OCF, oneM2M, or Mozilla Project Things, with its own specifications for application-facing APIs, data modelling, and protocols or protocol configurations [2]. In principle, an IoT platform can be part of more than one ecosystem. IoT platform helps to facilitate device management, handle hardware/software communication protocols, collect and analyse data and enhance the functionality of smart applications.

IoT applications

IoT uses much of the existing technologies – communication network technologies, information technologies, sensing/control technologies, software technologies, hardware/device technologies – and combines them to improve operations, lower costs, create new products and business models, enhance engagement and customer experience. IoT covers a very wide spectrum of applications and represents the integration of systems from different vertical sectors (enterprise, consumer, government, industries etc.) [1]. IoT application domains embrace: smart city, smart grid, smart home/building, digital agriculture, smart manufacturing, intelligent transport system, smart energy, digital Health, etc.

IOT Definitions in International Standards

Originally proposed in 1999, and often discussed within the fields of Human Computer Interaction (HCI), the IoT concept has been recently considered as both an **enabling technology** for other more complex technologies, as well as a (global) **infrastructure for connecting the physical and the virtual worlds**.

Several definitions of IoT exist, reflecting the different aspects, roles and implications that IoT has had in the recent past years and will have in the future ones. For this reason, **IoT must be considered as an innovative technological and interaction paradigm**.

Enabling “Smart Things”

IoT has been commonly introduced as a technology enabling the vision in which "things" are interconnected and are capable of transmitting and receiving data through the Internet –see for example the RFID revolution. ISO/IEC described IoT as [3]:

“an enabling technology that consists of many supporting technologies, for example, different types of communication networking technologies, information technologies, sensing and control technologies, software technologies, device/hardware technologies” [ISO/IEC JTC 1/WG 10]

According to this model, IoT technologies are instrumental to allow “things” (i.e. everyday objects) to perceive and to interact with the world, performing tasks and communicating with each other to share information and coordinate decisions [4].

A (global) Infrastructure linking the physical and the virtual worlds

However, in a Digital Society, IoT technologies and interaction patterns have enabled an infrastructural revolution that is affecting all the sectors of our economy –i.e. a paradigm shift. ISO/IEC 3142 standard defined IoT as [1]:

“an infrastructure of interconnected physical entities, systems and information resources together with the intelligent services which can process and react information of both the physical world and the virtual world and can influence activities in the physical world” [ISO/IEC 3142]

This definition outlines the key aspect of IoT that is changing the traditional HCI (Human Computer Interface) patterns: IoT enables the automatic interaction between the physical world (where we live) and the virtual/digital world –where living and non-living entities leave digital tracks. This important aspect was utilised by two other ISO standards [5] [6]:

“Infrastructure of interconnected objects, people, systems, and information resources together with intelligent services to allow them to process information of the physical and the virtual world and react” [ISO 19731 and ISO/IEC 20924]

The interaction and interoperability of the physical and virtual worlds is important to carry out advanced and “smart” services, helping humans in the everyday life. This has important societal implications, including security. ITU-T recognised that in its recommendation Y.2060 [7], defining IoT as a:

“Global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on, existing and evolving, interoperable information and communication technologies” [Rec. ITU-T Y.2060]

“Note 1 to entry: Through the exploitation of identification, data capture, processing and communication capabilities, the IoT makes full use of things to offer services to all kinds of applications, whilst ensuring that security and privacy requirements are fulfilled.”

“Note 2 to entry: In a broad perspective, the IoT can be perceived as a vision with technological and societal implications.”

The same definition was then reclaimed by ISO/IEC 38505-1 standard, which deals with IT data governance [8].

The Digital Twin interaction pattern

In such a universe of discourse, living and non-living entities (i.e. things) have both a physical and a virtual representation, introducing the Digital Twin interaction pattern. IEC outlined such pattern, providing the following definition, in its online vocabulary, for IoT and services [9]:

“Link between clearly identifiable physical objects (things) and services and a virtual representation in an internet-like structure” [IEC]

“Note 1 to entry: The internet of things and services no longer consists only of human participants but also of things.”

“Note 2 to entry: The objective of the internet of things and services is to minimize the information gap between the real world and the virtual world. An important step towards this objective is the standardization of components and services in the Internet of Things and services.”

Geospatially-enabled IoT

Many IoT use cases require that the actual physical location of devices is available, thus transcending the borders between the physical and virtual worlds. The impact of IoT on concepts such as the Digital Earth is further discussed by [10]. The requirement for inclusion of a geographical dimension further complicates the, anyhow, complex architecture of IoT. This in turn requires the need of a geospatially-enabled standard for the IoT.

The Open Geospatial Consortium (OGC) developed the SensorThings API as an open unified way to interconnect IoT devices, data, and applications over the Web with a geospatial dimension in mind [11]. OGC used the following ITU-T definition of (Internet of) Things:

A thing is an object of the physical world (physical things) or the information world (virtual things) that is capable of being identified and integrated into communication networks. [ITU-T Y.2060]

— More information about the OGC SensorThings APIs are in Annex A.

1. METHODOLOGY

This study implements the evaluation phase of the analytical strategy, developed by the TECH Task Force of JRC.B6 [12], as to IoT ecosystems and platforms. The strategy is briefly described in the next paragraphs.

1.1 Strategy for the analysis of innovative digital technologies

The JRC B.6 Unit analytical strategy (which is consistent with similar approaches recognised by relevant organisations, such as W3C, OECD, and OGC) aims at identifying and assessing innovative technologies that are currently being used and/or tested across the EU. As depicted in Figure 1, this strategy consists of four main phases plus three optional ones:

Phase 1: Emerging technology **Recognition** (i.e. exploration, elicitation, and collection);

- Investigation and Incubation of a specific emerging technology (optional);

Phase 2: Emerging technology **Evaluation**;

- Recognise the lesson learned during the evaluation and possible gaps to be filled (optional).

Phase 3: Analysis **Recommendations**;

- Prioritisation of the recommendations expressed (optional);

Phase 4: Analysis results **Presentation**.

For the emerging technology recognition (the first phase), valuable inputs are (among the others) the JRC Megatrends Hub outcomes [13], as well as the ICT Landscape Conceptual Map of JRC Unit B.6 [14]. In particular, this document reports the activity and outcomes of the Evaluation phase, as far as IoT is concerned. While, for the second phase, the emerging technology evaluation, specific data sources are utilized.

1.2 Evaluation Phase data sources

For the evaluation phase, we used the following group of data sources: (i) publications in scientific journals characterised by an impact factor, (ii) worldwide patents, (iii) a worldwide companies database, and (iv) social network data. The complete list of data sources is further described in Section 10. In the next future, another evidence source (specific to the EU context) to be considered are European projects.

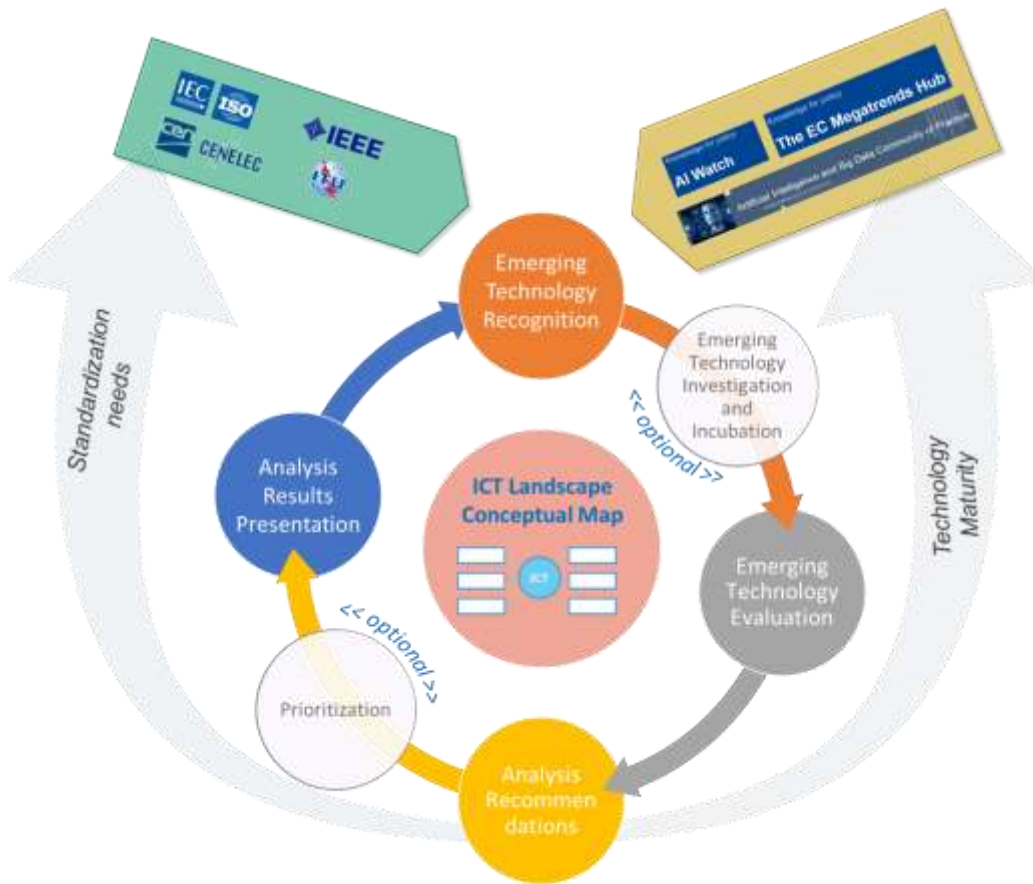


Figure 1. Analytical strategy for emerging technology, developed by B6 Unit

To ensure data mining consistency across the diverse sources taken in consideration for the analysis, we developed a **list of relevant keywords** for IoT (see Annex F for further details). This list originated from a **set of IoT taxonomies** defined according to different viewpoints (see section 8). Finally, we tried to identify **patterns in the spatial and temporal distribution** of technological developments.

This **preliminary analysis** can be further developed in order to focus on specific sub-domains that can make a difference for the European Union society and economy. The preliminary analysis is covered in section 10.

2. IOT REFERENCE FRAMEWORK

In a general setting, considering the definitions and standardisation perspectives outline in the Introduction, the main components contributing to the IoT technology paradigm are:

- things (non-living entities);
- networks;
- computing;
- data;
- analytical models;
- applications;
- humans (living entities).

These components collaborate to implement an intelligence generation process, as depicted in Figure 2. The most general architecture (or reference framework) applied by an IoT platform is showed in Figure 3. This includes [1] [7] [2] [3]:

- (i) **physical layer/device layer/local environments** –including sensor and monitoring services;
- (ii) **communication and transport layer/environments** –including edge and fog connectivity and transport services, e.g. gateways
- (iii) **middleware for data storage & management layer/environment** –including brokering, data aggregation, data pre-processing, and application support services
- (iv) **analytics and application layer/environment** –including data analytics services and intelligence generation and provision services. This supports innovative applications, targeting human users via VR/AG, as well as machines, implementing Machine-to-Machine (M2M) services by exposing APIs.

All the layers/environments are interconnected by a **network environment**. Two other service layers (or service environments) are transversal: the **security and ethics layer/environment** and the **platform/ecosystem governance and business model layer/environment**.

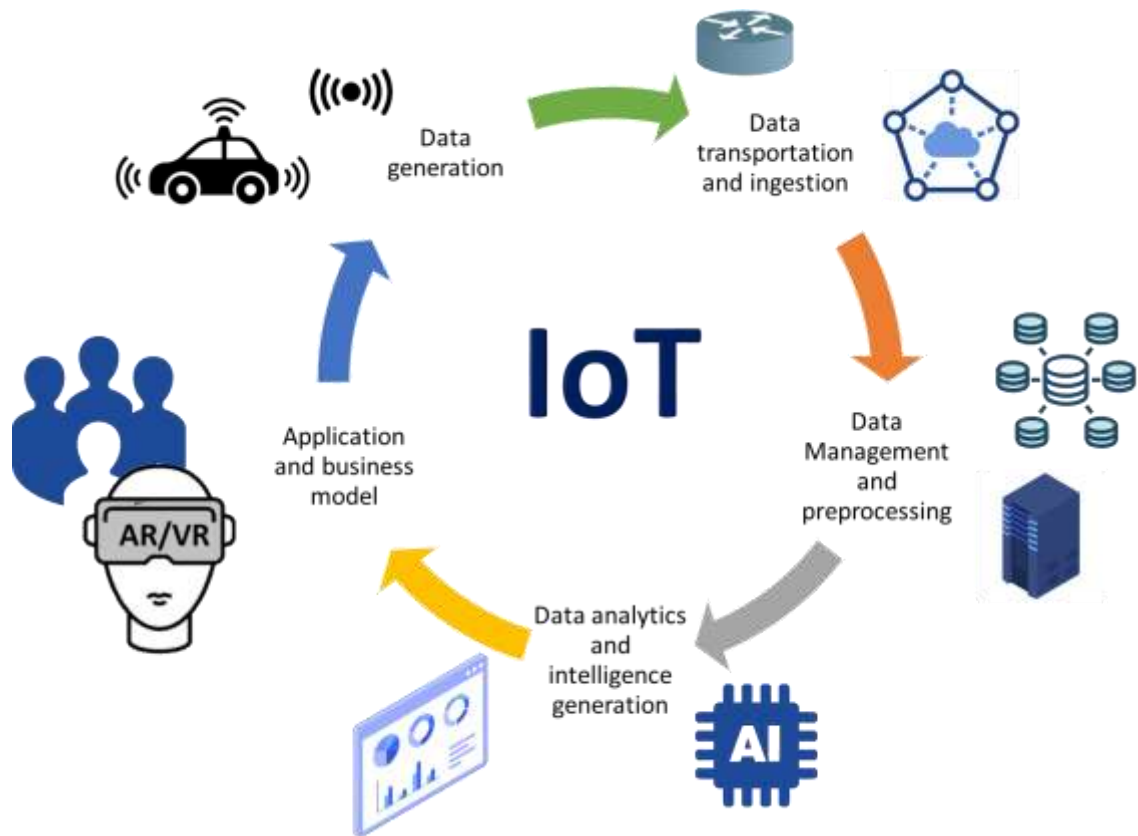


Figure 2. Intelligence generation process by the IoT ecosystem

In keeping with the reference framework of Figure 3, an IoT platform may be defined as:

a digital framework allowing data to be generated, transported, stored, and analysed to create actionable intelligence.

IoT platform enables and is ingested by the Datafication process [15] that is at the core of the present digital transformation of our society.

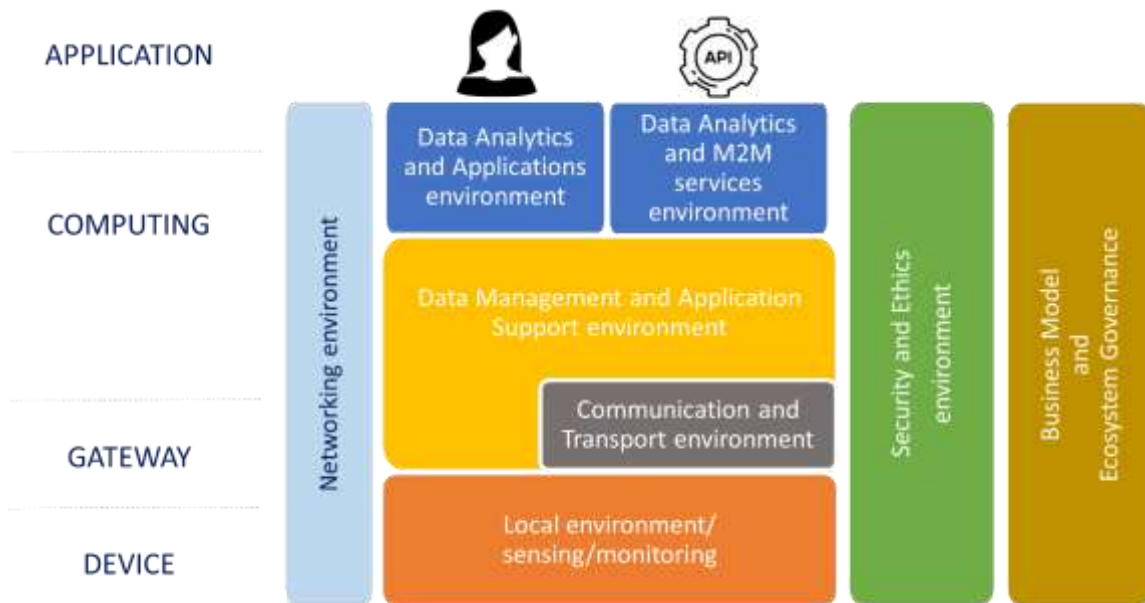


Figure 3. IoT platform reference framework

Figure 4 shows a typical engineering system implementing (fully or in part) the described reference system.

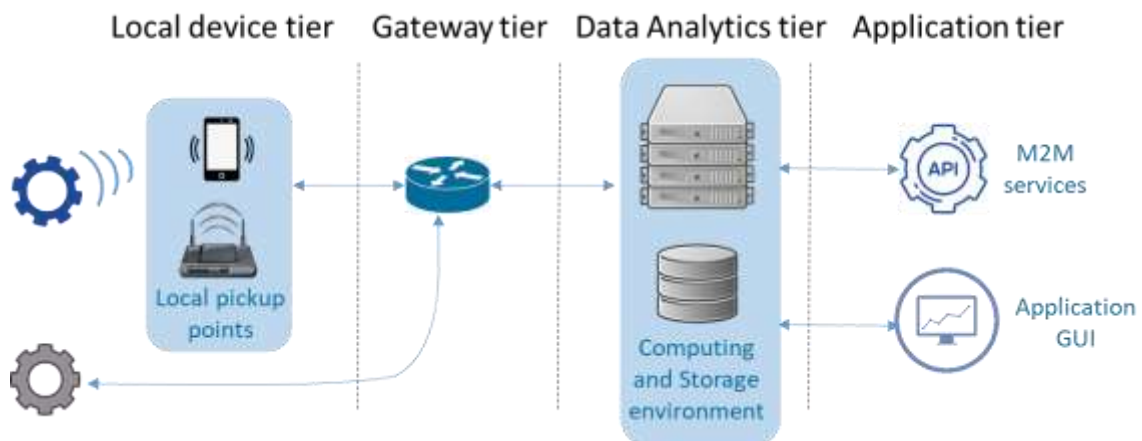


Figure 4. IoT platform engineering implementation

For IoT platforms, the most peculiar tiers are the first two (i.e. Local device and Gateway tiers). Therefore, the next sections will elaborate more on them.

In particular, these two layers play an important role to establish IoT platform ecosystems. An IoT ecosystem enables the connection of different IoT platforms (or some layers of them) to carry out interoperability and synergetic capacities and services.

3. IOT (COMMUNICATIONS) PROTOCOLS: GATEWAYS IMPLEMENTATIONS

As depicted in Figure 3, the local/device environment (i.e. the local device tier) is commonly interconnected to a remote computing and application environments (i.e. the data analytics tier) by specific communication and transport protocols: they are commonly called the IoT protocols. They are a crucial part of the IoT reference framework, because they make hardware useful enabling sensors/devices to exchange data in a structured and meaningful way.

Several IoT-specific protocols have been introduced, in recent years –and new ones are expected, such as the announced CHIP (see section 6.1.1). This is one of the reasons why the IoT needs standardized protocols, avoiding further fragmentation and minimizing the risk of security threats. Presently, some well-used communication protocols include:

- Narrowband-IoT
- ZigBee
- LoRa (LoRaWAN)
- Thread
- DASH7 Alliance Protocol (D7A)
- Sigfox
- NFC (Near-Field Communication)

— These protocols are briefly described in Annex B.

4. SECURITY ASPECTS

In the IoT reference framework of Figure 3, the security layer is transversal, affecting all the platform services. IoT security is important not only for the coherent functioning of the connected device systems in the various economy sectors, but also for the overall security of the global Internet infrastructure. One of the main differences between IoT and the traditional Internet is the reduced human presence. Recently many serious Internet attacks started by exploiting IoT devices vulnerabilities. The usual practice of attackers is to use bots to target certain devices and then spread the malware to other important entities of Internet.

One of the most serious attacks, took place on the 21st Oct 2016 known as the Dyn cyberattack based on the Mirai malware, resulted to a series of distributed denial-of-service attacks (DDoS attacks) [16]. Even, major Internet stakeholders (like Twitter, Netflix, Spotify, Airbnb, Reddit, etc.) confronted severe problems because of this attack. The analysis of the attacks gave strong indications that they have been executed through a botnet structure that was spread to connected devices like baby monitors, printers, IP cameras, etc. Analogously, breach of user privacy can occur by using similar attack mechanisms that leverage the same vulnerabilities of IoT devices and networks.

Many security stakeholders publish reports, white papers and analysis of vulnerabilities of IoT systems regularly or on a yearly basis. Since the time the term IoT was first introduced, experts underlined how crucial security is for the successful adoption of IoT. One example of this type of security organisations is OWASP (Open Web Application Security Project), which publishes lists of security vulnerabilities in the fields of computers, networking and communication, based on expert analysis and metrics. The most recent list of OWASP on IoT vulnerabilities [17] is the following:

1. Weak, Guessable or Hardcoded Passwords;
2. Insecure Network Services;
3. Insecure Ecosystem Interfaces (web, cloud, mobile, outside the device);
4. Lack of Secure Update Mechanism;
5. Use of Insecure or Outdated Components;
6. Insufficient Privacy Protection;
7. Insecure Data Transfer and Storage;
8. Lack of Device Management;
9. Insecure Default Settings;
10. Lack of Physical Hardening.

As mentioned in previous paragraphs, there is a great number of IoT platforms using a variety of protocols and standards. Consequently, there are many security techniques implemented already and many others proposed or under development. Experts have done efforts to classify and codify the various security aspects to arrive at a uniform way of studying and experimenting in IoT [3].

— Annex C briefly discusses the security of the IoT protocols introduced, previously.

5. IOT PLATFORMS AND ECOSYSTEMS –IMPLEMENTING THE IOT REFERENCE FRAMEWORK

Several implementations of the described IoT reference framework exist. Several of them implements only part of the framework – e.g. one or few layers. The most popular and complete implementations are briefly introduced in Annex D. – they commonly realize the technology ecosystem approach. They include:

- Amazon Web Services (AWS) IoT;
- Google IoT;
- Apple HomeKit;
- Samsung SmartThings;
- IBM Watson IoT Platform;
- Bosh IoT Platform;
- Microsoft Azure Digital Twin;
- Open sources solutions/platforms:
- Eclipse;
- Thinger.io;
- OpenIoT;
- ThingSpeak.
- Mozilla WebThings

— See Annex D.

6. CONVERGENCE TIME: ADDRESSING INTEROPERABILITY CHALLENGES

Presently, it does not exist a universal language for IoT and there exists a lack of interoperability across platforms and ecosystems. Device makers and app programmers must choose between disparate IoT frameworks (e.g. Apple, Amazon, Google, IBM, Samsung). As a result, developers are faced with data silos, high costs and limited market potential. This lack of interoperability also affects end users, who must determine whether the products they want to buy are compatible with the platform they belong to; otherwise, they must find a way to integrate the new devices in their platform (ecosystem) by solving the interoperability issues on their own. This can be likened to the situation before the Internet when there were competing non-interoperable networking technologies. The Internet makes it easy to develop networked applications independently of those technologies [2].

Several standardization organisations, consortia, and foundations have been developed to address the interoperability issues. The most relevant and/or promising are briefly described in this section. In particular, W3C launched an initiative called Web-of-Things (WoT) that aims to confront fragmentation by forming a web-based abstraction layer (i.e. Web of Things) capable of interconnecting IoT platforms, devices, cloud services and standards. Section 7 will introduce W3C WoT and its open implementation Mozilla WebThings.

6.1 Converging process

IoT platforms and applications development has reached a good maturity level to enable the process of convergence among the diverse solutions and specifications. Relevant convergence and alliance initiatives are briefly described in the following paragraphs.

6.1.1 Amazon, Apple, Google agreed to develop common standards: "Project Connected Home over IP"

In December 2019, after years of trying and failing to dominate the smart home market with their own standards, tech giants Amazon, Apple and Google agreed to create an open-source standard for internet-connected home products – such as smart speakers, thermostats, cameras, plugs, digital assistants, etc. [18]. They will work with the Zigbee Alliance, Samsung, Ikea, and other major players in the sector. The companies have set up a working group, called "Project Connected Home over IP" (or CHIP), which will meet, discuss, and (they hope) agree on a set of standards over the coming months [19].

The new standard should emerge in draft form in late 2020, meaning that 2021 will be the start of a new era in smart home tech, where you can have a single app on your phone to talk to everything else. The initial push appears to be to work with digital voice assistants [20].

6.1.2 OCF¹

The Open Connectivity Foundation (OCF) is dedicated to ensuring secure interoperability for consumers, businesses and industries by delivering a standard communications platform, a bridging specification, an open source implementation and a certification program allowing devices to communicate regardless of form factor, operating system, service provider, transport technology or ecosystem. The OCF 1.0 specifications were ratified and accepted for publication by ISO and IEC as International Standards –i.e. ISO/IEC 30118.x.

According to OCF, their specifications leverage existing industry standards and technologies, provides connection mechanisms between devices and between devices and the cloud, and manages the flow

¹ <https://openconnectivity.org/>

of information among devices, regardless of their form factors, operating systems, service providers or transports [21].

OCF merged its effort to another supplier-sponsored initiative, the AllSeen Alliance, into a single body representing a wider range of supplier interests. This unification combined the best of both organisations under OCF name and bylaws.

6.1.3 OneM2M²

OneM2M brings together several major ICT SDOs around the world, such as ARIB (Japan), ATIS (North America), CCSA (China), **ETSI (Europe)**, TTA (North America), TSDSI (India), TTA (S. Korea) and TTC (Japan). These SDOs share the objective of developing common standards for a common service layer that applies across different industry segments.

The purpose and goal of oneM2M is to develop technical specifications that address the need for a common M2M Service Layer that can be readily embedded within various hardware and software, and relied upon to connect the myriad of devices in the field with M2M application servers worldwide. A critical objective of oneM2M is to attract and actively involve organisations from M2M-related business domains such as: telematics and intelligent transportation, healthcare, utilities, industrial automation, smart homes, etc. [22].

Recently, it was established a liaison between oneM2M and IIC (Industrial Internet Consortium), to identify under-addressed technical areas and standardization gaps that, once resolved, would speed up the pace of commercial adoption for IoT solutions (i.e. platforms and applications) among providers and users alike. In particular, the two organisations mapped their respective architecture frameworks and architecting methodology: IIC's Industrial Internet Reference Architecture (IIRA) and oneM2M's architecture and its three-stage standardization procedure [23].

6.1.4 AIOTI: Contributing to a dynamic European IoT ecosystem³

The Alliance for Internet of Things Innovation (AIOTI) was initiated by the European Commission in 2015 to strengthen the dialogue and interaction among IoT players in Europe, to contribute to the creation of a dynamic European IoT ecosystem and speed up the take up of IoT. AIOTI members include key European IoT players (i.e. large companies, successful SMEs and dynamic start-ups) as well as research centres, universities, and associations.

In August 2018, AIOTI published its recommendations for the future IoT research priorities under Horizon Europe and Digital Europe programs in the period 2021-2027 [24]. This work continues by publishing the vision on Future Networks, Services and Applications under Horizon Europe and our priorities for the new political cycle in the EU (2019-2024).

6.1.5 OMA SpecWorks⁴: for a connected world

In 2018, IPSO Alliance –an organization promoting the Internet Protocol (IP) for what it calls "smart object" communications– merged with the Open Mobile Alliance (OMA) to form OMA SpecWorks [25]. It is *"an innovative kind of Standards Development Organization (SDO) where the needs for wireless industry consensus versus the quick and accurate creation of specifications and other technical documentation are balanced via a working group-driven, efficient and agile process. As a non-profit organization with a long history in mobile and Internet of Things (IoT) technology development, OMA SpecWorks is a specifications factory where industry-leading companies bring their ideas and talent to build market-accelerating standards that allow products and services to interoperate seamlessly across fixed and mobile wireless data networks"* [26].

² <http://www.onem2m.org/>

³ <https://aioti.eu/>

⁴ <https://www.omaspecworks.org/>

OMA releases different types of specifications that are publicly available from its portal. OMA releases are published in two phases:

- Candidate Release (-C) – as soon as the documents making up the release have been approved by OMA, they are published as a Candidate Release.
- Approved Release (-A) – when a Candidate Release has undergone a period of public comment and completed any applicable interoperability testing, then, it is published as an Approved Release.

6.2 Mozilla IoT⁵ and WebThings

Mozilla WebThings is a software distribution for smart home gateways focused on privacy, security and interoperability. According to Mozilla, *“this project contributes to implement the Web of Things as a unifying application layer for IoT, linking together multiple underlying IoT protocols using existing web technologies”* [27].

Mozilla WebThings has introduced a common data model and API for the Web of Things. The Mozilla *Web Thing Description* model provides a vocabulary for describing physical devices connected to the Web in a machine-readable format with a default JSON encoding [28]. Common device capabilities can be specified using optional semantic annotations. The Mozilla *Web Thing REST API* and *Web Thing WebSocket API* allow a Web client to access the properties of devices, request the execution of actions and subscribe to events representing a change in state [28]. The current supported binding protocols and templates are shown in Figure 5.

| Web of Things | | | | |
|-------------------------|-------------|-------------------------|----------|----------------------------|
| Weave | AMQP | MQTT | HomeKit | MQTT |
| WiFi/Thread | WiFi | WiFi | WiFi/BLE | WiFi/ZigBee/ BLE/Thread |
| Linux/Android Things | Windows IoT | Linux/AWS Greengrass | iOS | Linux/ARTIK |

Figure 5. Mozilla IoT unifying application layer. Source: [28]

⁵ <https://iot.mozilla.org/>

7. THE W3C WEB OF THINGS (WOT) INITIATIVE

W3C WoT aims at addressing the present IoT fragmentation by forming a web-based abstraction layer (i.e. Web of Things) capable of interconnecting IoT platforms, devices, cloud services and standards. To achieve this goal, application developers need platform independent APIs and means that allow interoperability between platforms. W3C approach is based upon rich metadata that describe the data and interaction models exposed to applications and the communications and security requirements for platforms to communicate effectively [2].

7.1 WoT Vision and methodology

WoT wants to connect real-world objects to the WWW (World Wide Web); as a result, WoT is intended as a unifying application layer for the IoT, linking together multiple underlying IoT protocols using existing web technologies. A further aspect of WoT is to enable platforms to share the same meaning when they exchange data. WoT is seeking to create a decentralized IoT by [2]:

- giving things URLs on the WWW to make them linkable and discoverable;
- defining a standard data model and APIs to make them interoperable;
- enabling expression of the semantics of things and the domain constraints associated with them, building upon W3C extensive work on RDF and Linked Data.

Mozilla IoT and WebThings provides a technological implementation of the WoT vision.

— The W3C specification for a Web-Thing is provided in Annex E.

8. IOT 2.0, DIGITAL AGE, LOCAL DATA ECOSYSTEMS AND THE INTERNET OF TRANSFORMATION

In the digitalization age, the IoT growth is going to impact all the sector of the digital society, in a significant way. There exist many different analyses and predictions regarding the size of such impact, including the followings [29]:

- The global IoT market was worth over \$150 billion in 2018 and is expected to exceed \$1.5 trillion by 2025 (Source: IoT Analytics).
- The global IoT market is expected to grow in the years to come reaching a global market of \$520 billion by 2021 (Source: Bain & Company).
- By 2020, there will be four internet-connected devices for every human on the planet (Source: Gartner).
- By 2021 there will be over 30 billion connected devices (more than 75 billion in 2025) (Source: Statista).
- There will be over 14 billion connected devices by the end of 2019, and over 25 billion by the end of 2021 (Source: Gartner).
- By 2020, the lack of data science specialists will prevent 75 % of all businesses from maximizing their IoT goals (Source: Gartner).
- The number of smart home devices purchased is expected to exceed 1.94 billion by 2023, with device sales exceeding \$78 billion by that time as well. (Source: Strategy Analytics).
- Smart cities are a major and emerging market for IoT. Over one-fifth of all publicly announced IoT projects involve IoT-driven smart cities of some kind, with most of these smart cities (45 percent) located in Europe (Source: IoT Analytics)
- Over 25 % of all cyber-attacks against businesses will be IoT-based by 2025 (Source: Gartner).

IoT is a key enabling technology for building local **data ecosystems**. AIOTI called them the “IoT-enabled Data Marketplaces”, introducing four stages to link the different technologies and challenges [29] – see Figure 6.

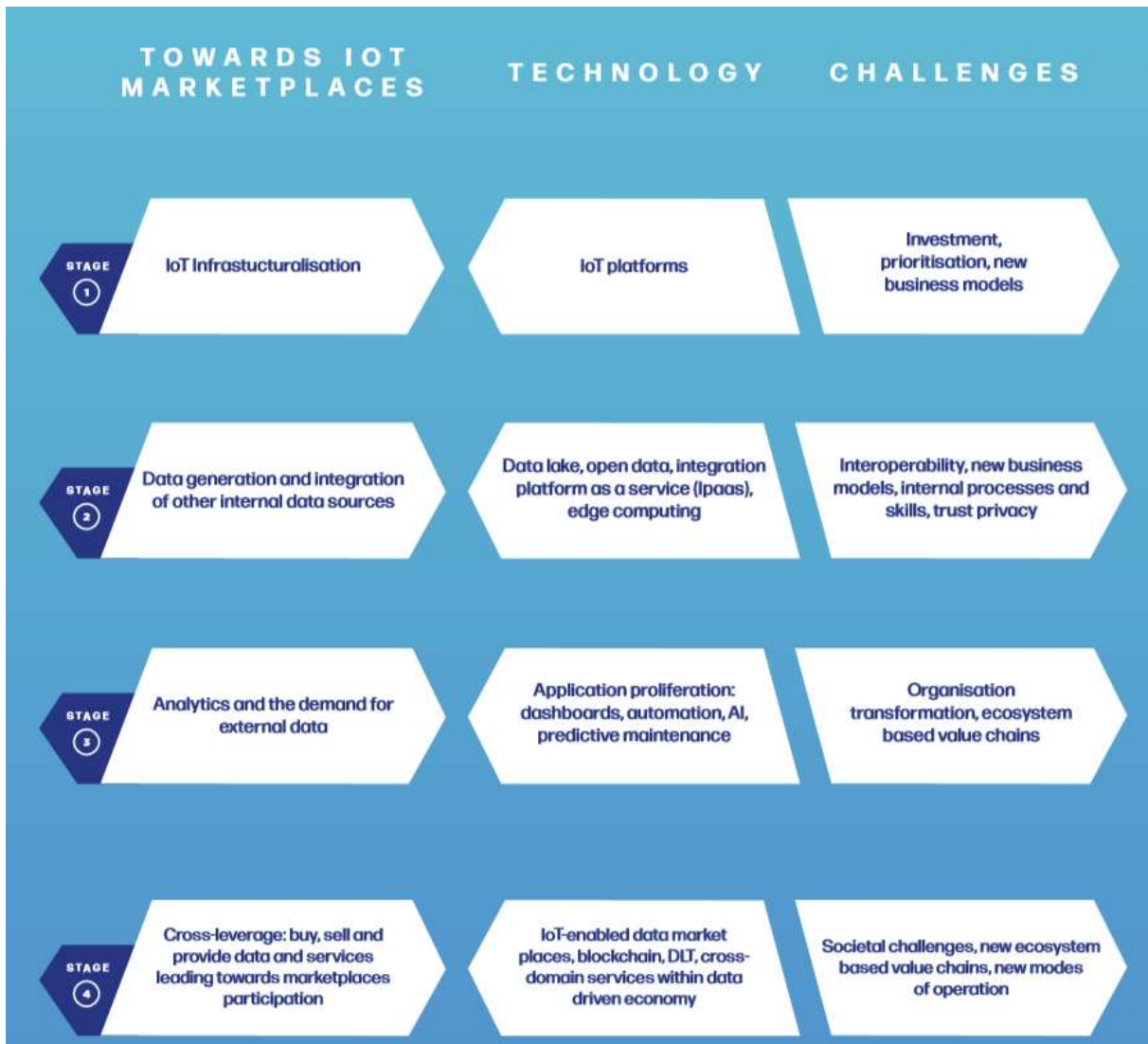


Figure 6. AIOTI process towards IoT marketplaces. Source [29]

8.1 Internet of Transformation: IoT 2.0 as the engine of Digital Transformation

Mapping the evolution stages, depicted in Figure 6, to the general IoT platform reference framework in Figure 3, it is possible to recognise the technology challenges. In addition, by applying an evolutionary approach, it is possible to distinguish between an old IoT generation, taking care of connecting as many “things” as possible and a new generation, called IoT 2.0, which deals with generating actionable intelligence from devices and their data. Empowered by billions of connected devices, sensors and actuators, IoT 2.0 will be bigger, more powerful and much more settled than IoT. IoT 2.0 will be the key technology (as sort of *Internet*) for the digital transformation of a hyper-connected society, for this reason it is also called “Internet of Transformation” [30]. As in the past Internet generated intelligence with documents sharing, presently, IoT 2.0 aims to generate actionable intelligence from devices and data sharing. To achieve that, IoT 2.0 will deal with related IT technologies, processes, people, benefits, outcomes and massive real-life opportunities, rather than just device technology and gateways aspects. Considering the need to manage an immense number of different objects deployed on different platforms, several experts think that three key characteristics of IoT 2.0 will be: (a) the establishment of common standards; (b) the evolution of platform architecture from the current hub-and-spoke model towards a more distributed peer-to-peer model;

and (c) a greater autonomy of the devices, which will lead to greater cognitive, adaptive, and predictive capabilities both at the individual device level and at the platform level [31].

8.1.1 Internet of Everything (IoE), Industrial Internet, Industrial IoT (IIoT), and Consumer IoT (CIoT)

Since IoT 2.0 can be recognized as the most impactful technology for the digital transformation of our society, it has become an umbrella term for many use cases, technologies and transformation processes. To distinguish between the diverse application contexts and the related challenges and opportunities, IoT 2.0 is often referred by using more specific terms: Industrial IoT (IIoT) or Industrial Internet [32] [33] when it is applied to the industrial processes, and Consumer IoT (CIoT) when it makes use of the billions of physical personal devices (e.g. smartphones, wearables, fashion items and the growing number of smart home appliances) [34] [35]. Due to this pervasive and multi-device nature of IoT 2.0, some prefers the term Internet of Everything (IoE). Regardless the terminology, IoT 2.0 is about an Internet of Transformation, which deals with technologies, processes, people, benefits, outcomes and massive real-life opportunities. It is an ecosystem where everything is interconnected –see IoE, including not only machine-to-machine communication but also people to machine and people to people communication through technology [36].

9. IOT TAXONOMY

Several possible taxonomies to characterise an IoT platform are possible, according to different views representing diverse needs and requirements – see Figure 7. In this JRC report, we will consider taxonomies based on the following views:

- Application Domains;
- Things (or connected objects);
 - Sensors –a sub-category of connected objects that is particularly relevant for stakeholders;
- Initiatives and projects;
- Industrial solutions and technologies contributing to IoT ecosystem.

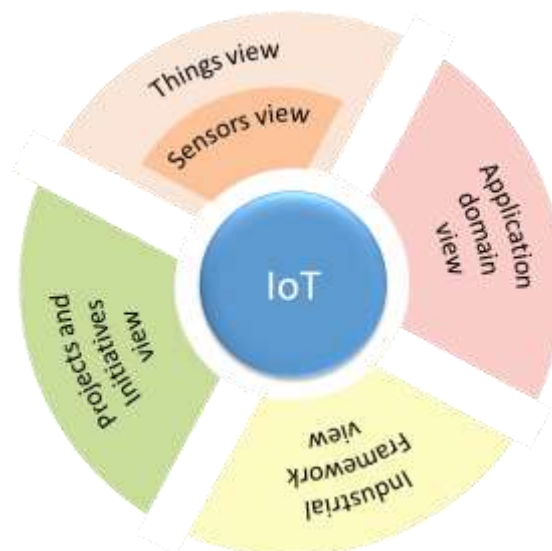


Figure 7. IoT Taxonomies viewpoints

Naturally, other viewpoints are also interesting, even if not fully explored in this document, such as the connectivity view: cellular (5G/4G, LTE, etc.), Wi-Fi, (Wi-Fi), LPWAN (NB-IoT, LoRa, Sigfox, etc.), WSNs (ZigBee, 6LoWPAN, etc.), and satellite technologies.

9.1 Application Domains View

The range of projects and applications covered by the IoT term is vast. For the scope of this document, the following application domains and related taxonomies were recognised.

9.1.1 Industrial Internet of Things (IIoT)

IIoT refers to the use of smart sensors, actuators and other devices to enhance manufacturing and industrial processes with the support of network infrastructure. Other terms used extensively in publications are **Industrial Internet** or **Industry 4.0**. IIoT combines the potential of smart machines and real-time processes exploiting the data that simple devices are producing in industrial and manufacturing environments. In the industrial sector, networked sensors and actuators are present long time before the introduction of IoT, and it is useful to distinguish among IT (Information

Technology), OT (Operational Technology), and ICS (Industrial Control Systems). With the IoT expansion and diversification, the industrial sector will be subject to changes to adapt to this new technology paradigm.

9.1.2 Smart Home/Intelligent Home/Smart Buildings

Smart sensors, actuators, monitors, cameras, doorbells, lighting, water heaters, thermostats, heating/cooling/ventilation control systems (HVACs), robots/mobile home devices, gateways, home management systems, Building Energy Management Systems (BEMS).

9.1.3 Energy/Smart grids/Renewable Energies/Oil & Gas

Generators, Renewable Energy generators, Smart meters, power plants, renewable energy sources management systems, transmission/storage systems, smart appliances, smart transport, smart home interfaces, smart distribution systems, smart grid management systems, offshore platform monitoring, leakage detection/prediction of pipelines, tanks' level monitoring. Automated calculation of a distributed stock through various storage tanks and delivery pipes/trucks for improved planning and resource optimisation.

9.1.4 Smart Cities

The Smart City domain comprises IoT-based services applied to different areas of urban settings. Smart City applications envisage the best use of public resources, improvement of the quality of services provided to people, and reduction of operating costs of public administration. Services include:

- (i) mobility and intelligent tourism, providing, for example, information about the state of roads, occupation of parking lots and the history of tourist attractions;
- (ii) smart grids, allowing better management of the network through new information on energy consumption;
- (iii) intelligent buildings, allowing new forms of residential automation, and infrastructures for monitoring and controlling;
- (iv) public safety and environmental monitoring, facilitating the management of environmental disasters and strengthening the security of buildings open to the public;
- (v) Monitoring of Bridges, dams, levees, canals for material condition, deterioration, vibrations discovers maintenance repair work and prevents significant damage. Monitoring of highways and providing appropriate signage ensures optimised traffic flow;
- (vi) Smart Parking is optimizing and tracking the usage and availability of parking spaces and automates billing/reservations;
- (vii) Smart control of street lights based on presence detection, weather predictions, etc. reduced cost;
- (viii) Garbage containers can be monitored to optimise the waste management and the trash collection route.

9.1.5 Health/Wellness/Medical/Biosensing

Home-based (or hospital, clinic-based) monitoring devices (fixed), portable augmented reality inspection devices, portable monitoring devices (ingestible sensors, wearable sensors), smart pharmaceuticals, monitoring and diagnosing of patients, managing of people and medical resources, remotely and continuously monitoring the vital signs of patients in order to improve medical care, ease the diagnosis by providing health indicators for patients, and enable the identification and tracking of equipment in a medical institution.

9.1.6 Environment and Climate

Climate/environment monitoring systems (sensors, gateway, monitoring system management), weather stations, sensors networks, particle-based monitoring systems all play an increasingly important role in understanding our planet. Environment monitoring typically relies on numerous distributed sensors that send their measurement data to common gateways, edge and cloud services. In addition, monitoring of air pollution, water pollution and other environmental risk factors such as fine dust, ozone, volatile organic compound, radioactivity, temperature, humidity to detect critical environment conditions can prevent unrecoverable health or environment damages.

9.1.7 Security, Safety, Defence and Military

Smart security cameras, smart police surveillance, proximity sensing, magnetometers, gyroscopes, accelerometers, digital compasses, weapon systems, ground vehicles, military wearables, smart equipment for military bases, automated security screening, smart resource management systems, connected aircraft devices.

9.1.8 Agriculture, Livestock, Food

Combined environmental smart farming sensors, greenhouse automation, lighting systems, irrigation systems, crop monitoring and crop management systems, livestock management, collar tags, health, activity and nutrition monitoring, end-to-end farm management systems, intra-farm mobility, food safety monitoring, food traceability, sensors monitoring production time, shipping, temperature, storage conditions, monitoring of soil moisture and the conditions of the plants, control microclimate conditions, monitor weather conditions that can damage the crops.

9.1.9 Industry 4.0 –Manufacturing, Construction and Distribution

Manufacturing tools, machines/robots, monitoring for industrial processes, industrial safety and security systems, smart sensing for industrial environment, monitoring and management of stocks in warehouses and yards, monitoring devices for product distribution, smart logistics, smart chips and sensors for storage, monitoring of construction sites, shipping and transportation, smart supply chain systems, warehouse operations, space optimisation automation, tracking inventory devices (sensors, RFID/NFC technology labels), monitoring of pollutant gases, locating employees, improving the manufacturing process, improvement of the processes involved in supply chains.

9.1.10 Business 4.0 –Private sector services, Retail, Customer experience

Smart solutions for retail sector, smart retail labels (SRLs) for pricing accuracy, inventory, consumer-marketing, consumer apps (B2C), cameras and RFID readers for smart buyers apps, asset monitoring of high value assets, usage based insurance and financing based on tracking and customized insurance policies, automated reading of residential and C&I (Commercial and Industrial) meters, smart billing offers.

9.1.11 Multimodal Transport, Logistics, Mobility and Traffic

Smart traffic monitoring systems, monitoring for fuel costs, en-route tracking for shipment, systems for autonomous driving, systems for autonomous transport – road, rail, air, water, radars, satellites, smart traffic monitoring, smart parking.

9.2 Things (or connected object) View

There is no common way to describe or classify the ‘things’ or “connected objects” that make up the IoT or the projects or systems and services based on them. IoT applications could be made up of a simple sensor that reports whether a door is open or not (in the case of a simple security system), or

whether a button has been pressed (in the case of a remote doorbell) to very sophisticated solutions that monitor dozens of phenomena, make complex calculations based on those phenomena, and then prompt a response (in the case of autonomous drones, for example). For the scope of this report, from a “thing” (or connected object) viewpoint, the following “things” categories were recognised:

- Smart Devices;
- Persistent Nodes;
- Collectables;
- Actor/Sentient Agent;
- Semi Autonomous Agent;
- Loose Perishables;
- Gateways.

In addition to the previous “thing” categories, a taxonomy based on the “connected objects” would also consider a set of key characteristics of things –since IoT is an evolving field, this features must be considered extensible [37] [38] [39]:

- Energy;
- Connectivity;
- Security;
- Safety;
- Functional attributes and sensing;
- Interaction modality/expressing;
- Hardware and software environments;
- Cost.

Figure 8 shows the concepts and keywords characterizing the connected object categories and key traits, which can be used for a general taxonomy.

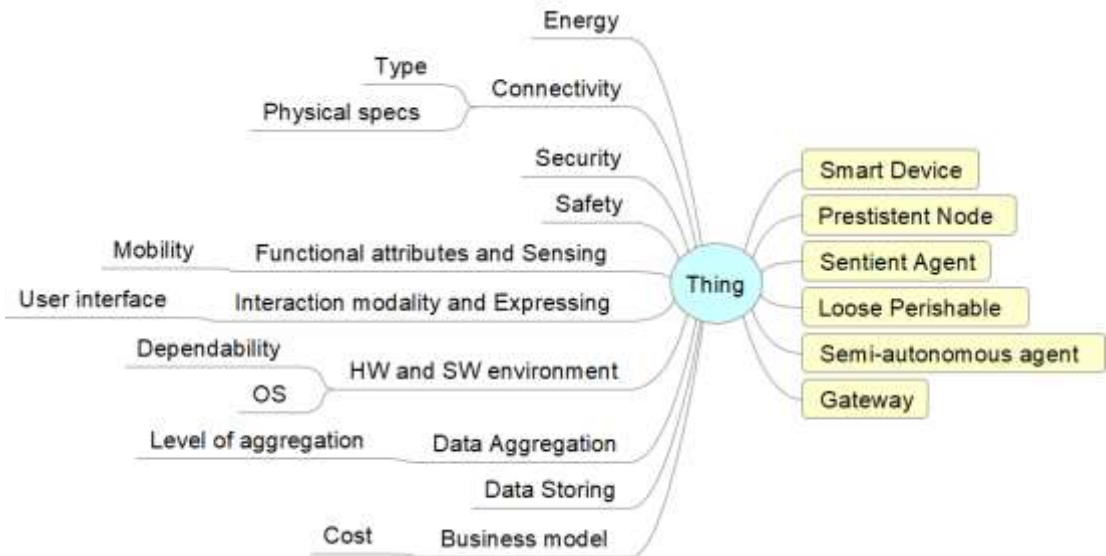


Figure 8. Connected objects taxonomy

9.3 Sensor-based View

A major element that produces inputs used by IoT applications are sensors, which provide measures of people, objects and the environment, in real-time or within certain time intervals, according to the application.

According to Cisco, 500 billion devices are expected to be connected to the Internet by 2030. Each device includes sensors that collect data, interact with the environment, and communicate over a network [40]. Sensors have different purposes since they provide different types of measures of:

- (i) physical quantities, such as speed, fuel level and tire pressure of vehicles;
- (ii) environment, as the temperature of a room and the amount of CO₂ on a busy street;
- (iii) people, as the amount of oxygen and glucose present in a blood sample.

The combination of sensors serving different purposes allows the creation of complex services, for example, a system for agriculture, which combines position and humidity sensors to control the level of water in the fields. Table 1 [41] reports IoT sensor types and sub-types, while Table 2 categorises them per application domain [41].

Table 1. IoT sensor types and sub-types. Source [41]

| Type | Motion | Position | Environment | Mass Measurement | Biosensor |
|---------|--------------|-------------|------------------|-------------------------|-----------|
| | Movement | Orientation | Temperature | Volume | Blood |
| | Velocity | Inclination | Humidity | Pressure | Organ |
| | Inertia | Proximity | Luminance | Density | Mental |
| | Vibration | Presence | Acoustic | Deformation | Tissue |
| | Acceleration | Location | Radiation | Viscosity | |
| | Rotation | | Gas | Flow | |
| Subtype | | | Magnetic Field | Load | |
| | | | Weather | Moisture | |
| | | | Chemical | Shock | |
| | | | Electrical | Contact | |
| | | | Color | Strain | |
| | | | EMF ² | Corrosion | |
| | | | | Electrical Conductivity | |
| | | | | Oxygen | |
| | | | | | |
| | | | | | |

9.4 Projects/initiatives View

Many projects and initiatives deal (or claiming to be dealing) with IoT. For the scope of this document, from a project/initiative viewpoint, the following taxonomy was recognised. It currently looks at IoT projects in terms of three key dimensions:

- Technical complexity: A measure of the technical sophistication of the solution;
- Safety, security, privacy: A measure of the sensitivity of data collected by the IoT system;
- Data sharing: A measure of the extent to which data is shared within the system, and beyond it.

For example, IoT-UK [42] provided some dimensionality levels (on the base of which projects can be classified), as reported in Table 3, Table 4, and Table 5.

Table 2. Taxonomy of IoT Sensors and domains. Source [41]

| Domain | Industrial | Smart Cities | Healthcare |
|--------|------------|--------------|------------|
| | | | |

| Area | Agriculture | Logistic | Plant Floor | Transport | Buildings | Environment | Monitoring | Management | |
|--------------------------|--------------|-------------|-------------|----------------|--------------|----------------|--------------|--------------|--|
| Sensor (subtypes) | Chemical | Gas | Acoustic | Acceleration | Acceleration | Acoustic | Acceleration | Acceleration | |
| | Conductivity | Humidity | Chemical | Acoustic | Acoustic | Chemical | Blood | Location | |
| | Gas | Inclination | Contact | Contact | Colour | Conductivity | Emotion | Luminance | |
| | Humidity | Location | Gas | Gas | Deformation | Corrosion | Gas | Pressure | |
| | Location | Luminance | Humidity | Inclination | Flow | Density | Humidity | Temperature | |
| | Luminance | Pressure | Inclination | Load | Gas | EMF | Inclination | | |
| | Moisture | Shock | Inertial | Luminance | Humidity | Flow | Movement | | |
| | Pressure | Temperature | Location | Magnetic Field | Inclination | Gas | Organ | | |
| | Temperature | Vibration | Luminance | Moisture | Luminance | Humidity | Orientation | | |
| | | | | Moisture | Movement | Magnetic Field | Load | Presence | |
| | | | | Movement | Oxygen | Movement | Location | Pressure | |
| | | | | Temperature | Presence | Orientation | Luminance | Radiation | |
| | | | | Orientation | Pressure | Presence | Moisture | Temperature | |
| | | | | Presence | Proximity | Pressure | Movement | Tissue | |
| | | | | Vibration | Shock | Proximity | Pressure | Vibration | |
| | | | | Volume | Temperature | Temperature | Proximity | | |
| | | | | Weather | Velocity | Vibration | Strain | | |
| | | | | | Volume | | Temperature | | |
| | | | | | | | Volume | | |
| | | | | | | | Weather | | |

Table 3. Technical complexity levels. Source [42]

| TCom Level | Description | Examples |
|------------|---|---|
| 0 | Dumb/passive objects. Not connected, identified or monitored | Any unconnected, unidentified object |
| 1 | Identifiable dumb/passive objects with a virtual existence that can meaningfully be counted/ tracked by online systems | RFID Tags, barcoded or QR-coded objects |
| 2 | Connected objects. Objects linked to an IP network, with some means of reading, programming or controlling them. These should be counted as elements within the IoT universe, but they are often underused assets. | Printers, doorbells, IP connected fire alarms or security systems |
| 3 | Connected broadly homogeneous objects in a simple integrated system, whether the benefit of that system accrues to the end user or the system provider | Networks of multiple temperature sensors within a single building or campus. Environmental monitoring networks, wearable devices (such as Fitbit or other wellness technologies) |
| 4 | Connected heterogeneous objects in a single, integrated system. This involves taking data from a variety of sensors of different types, all deployed for the same end user or organisation to help improve processes, make better decisions or change outcomes. | The deployment of a range of sensors in a care home or hospital or the combination of parking, traffic volume and traffic control data in an urban road management system |
| 5 | Different objects deployed across multiple interconnected systems for multiple organisations, in multiple locations, all within a similar domain. System supports analysis of aggregated data derived from all deployment locations. | Partnering university campuses' security cameras, fire alarms, temperature sensors, access control systems and energy monitoring systems integrated into a single unified control and monitoring solution |
| 6 | As for TCom 5, but where multiple domains are connected. This involves gathering data from a variety of sensor types, across a variety of systems and ecosystems, and creating combined views of the data that offer new sources of value (economic or social) or where there is a high degree of automation across homogeneous systems | Smart cities where multiple organisations, or different city departments and their partners, have built applications that draw on diverse sets of data from multiple sources to develop or improve services. Such applications might include the adjustment of street lighting in response to incoming data on night-time police activity levels, or the adjustment of traffic lights in response to real-time data sources about local environment data, or current people movement data based on mobile phone location data. Or, in the second case, the automated adjustment of environmental controls across a service provider's care estate based on real-time data feeds from sensors deployed in those settings. |
| 7 | As for TCom 6, but involving both multiple ecosystems and a high degree of automation | A smart city solution drawing data from multiple providers and sources, which is then used for automated traffic control and routing of emergency services, or the automated adjustment of traffic lights based on real-time mobile phone location data |

Table 4. System Security Level (SSL). Source [42]

| SSL | Description | Examples |
|-----|--|--|
| 0 | No data involved, no control of the system | |
| 1 | No sensitive data involved, no control of the objects in the system | Wireless doorbell |
| 2 | System provides anonymous, aggregated statistics, no control of the system | Remote temperature sensors |
| 3 | System generates sensitive data or supports some degree of remote control of the system objects | Biometric data, door actuation mechanisms |
| 4 | System generates sensitive data, supports some degree of remote control of the system objects and connects with external systems | Integrated facilities management systems, tele-health monitoring, security and safety systems. |

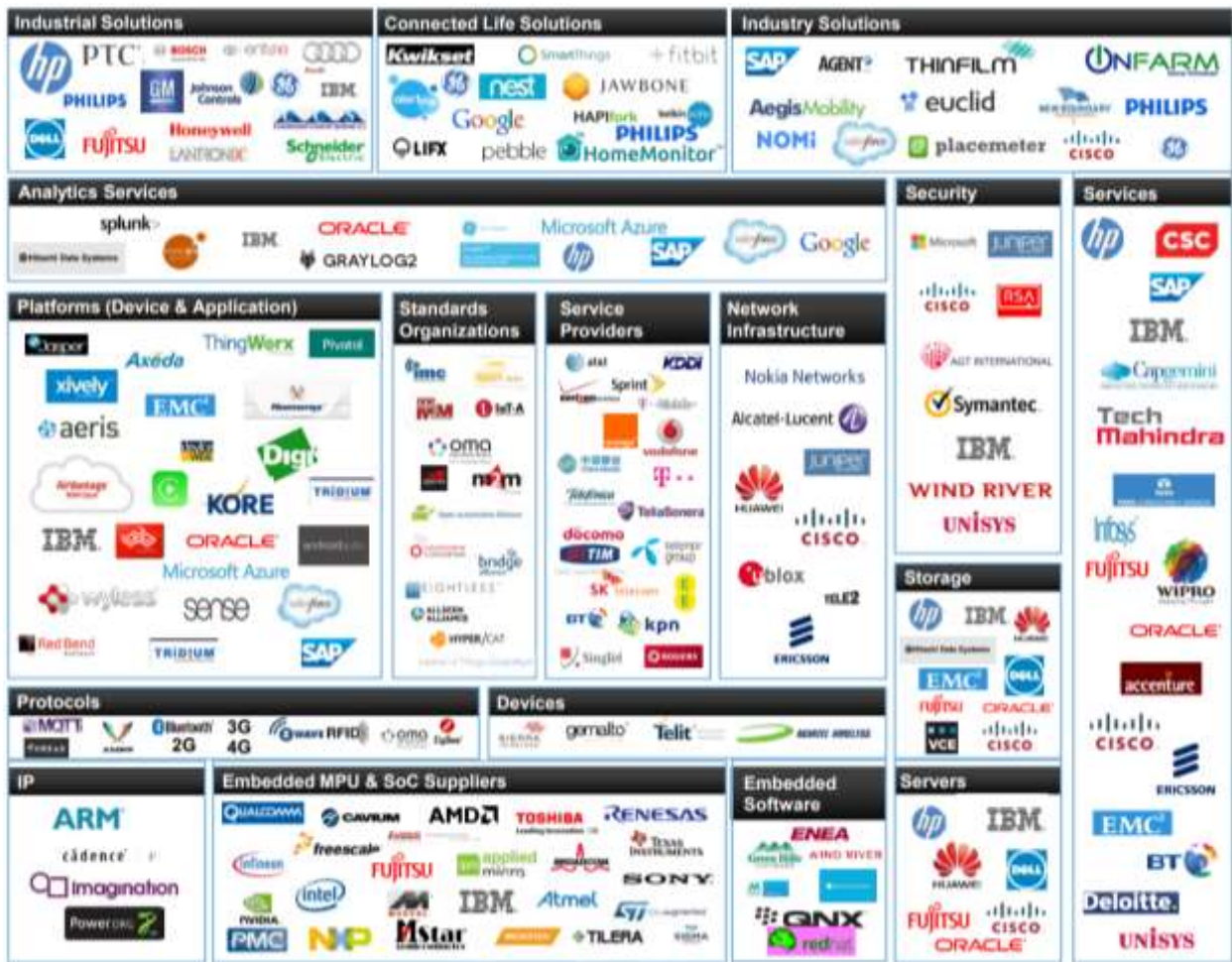
Table 5. Data Sharing Level (DTL). Source [42]

| DSL | Description | Examples |
|-----|---|---|
| 0 | No data is shared | Simple point-to-point monitoring systems such as consumer weather stations and wireless doorbells |
| 1 | Basic sharing between two parties: agreed sharing of sensitive data between the customer/buyer/user and the seller or provider (whether that seller or provider operates in the commercial or public sector) | Cloud-based security systems, remote cameras, home monitoring systems |
| 2 | Third person sharing: sharing of sensitive data between the seller or provider and unrelated third parties in a commercial context. | Person tracking information to support targeted marketing offers |
| 3 | Multi-domain and third-party sharing: sharing of sensitive data between the customer/buyer/user and multiple sellers or providers involved in delivering services; where those providers come from different ecosystems (including the commercial and public sectors) | The aggregation of parking, traffic and environmental data in an urban traffic management application |
| 4 | Open access to sensitive data, including data generated through use of public finance or infrastructure | Integration of multiple security systems in a public safety context |

9.5 Industrial Framework View

As already introduced, IoT is a technological paradigm and industries provides solutions to implement a complex framework composed by several services, tools, and technologies. Therefore, it is possible to introduce a taxonomy distinguishing the different categories of industrial sectors/products that compose an IoT framework. A good example of such a taxonomy is introduced by IDC [43] –as depicted in Figure 9. This covers:

- **Solutions:** Industrial solutions, Connected Life Solutions, Industry Solutions
- **Services:** Analytics services, Security, general Services
- **Enabling technologies/components:** Platforms (Devices & Applications), Standards Organisations, Service Providers, Network Infrastructures, Protocols, Devices, Storage, IP, Embedded MPU & SOC Suppliers, Embedded Software, Servers.



All IDC research is ©2014 by IDC. All rights reserved.

Figure 9. IDC IoT Taxonomy map. Source [43]

10. ANALYSIS OF IOT UPTAKE: EMERGING TRENDS

To understand the present uptake of IoT technologies and applications and recognize emerging trends, a set of global data were accessed and analysed. These data considered the industrial, scientific, financial, and social dimensions. The following sections describe the diverse data types and sources analysed.

From the multi-view taxonomies, previously introduced, a set of keywords were identified in order to mine the data sources (see Section 10) accessed to evaluate IoT uptake and future trends. This was a recursive process where the data mining results provided useful feedbacks to refine (e.g. aggregate or disambiguate) the standing keywords list –as depicted in Figure 10.

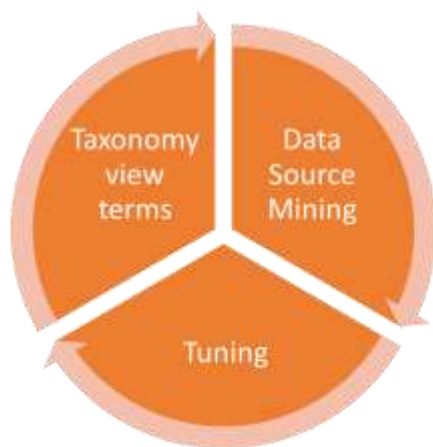


Figure 10. Keywords list generation and consolidation process

— The queries defined for mining the utilized data sources are reported in Annex F.

10.1 Patents data

The analysis of patents has been conducted by means of a license of the Orbit Intelligence software by Questel. Orbit Intelligence covers over 100 international and regional patent authorities worldwide, of which 45 allowing for full text search with translation into English. The organisations and countries covered are: the World Intellectual Property Organization, the European Patent Office and the national authorities in UK, Canada, France, Germany, China, Japan, South Korea and India.

The research has been performed using the 'FamPat family number'. FamPat provides a comprehensive family coverage of worldwide patent publications. In FamPat, a single family record combines together all publication stages of the family; family definitions incorporate different patenting authorities' definitions of an invention. Questel makes use of an in house-developed family definition combining the strict family from EPO with additional rules. Searches for Assignee, Inventor or Classes are conducted on all family equivalents. Patent searches include full legal information and timely updates.

The keywords and Boolean operators used for each single patent query are listed in Annex F. In some cases, the possibility to combine, exclude or apply similarity search has been exploited. Searches were

performed on the basis of title, abstract, claims and concepts in the Advanced Search modality and graphs and tables were derived using Orbit Intelligence statistical tools.

10.2 Scientific Publications and Research projects data

For the analysis of scientific publications that investigate the broader context of the IoT we used the EC JRC I.3 Tools for Innovation Monitoring (TIM) [44]. The TIM Technology tools aim at providing specific and relevant knowledge on innovation and technological development. TIM Technology offers the possibility to policy-makers to answer concrete policy needs related to innovation networks, impact evaluation of EU programmes, emerging trends and technologies, funding orientations, regional strategies, and other needs related to research and innovation policy.

TIM technology utilises several data repositories:

- Scientific publications – Elsevier;
- Patents – European Patent Office;
- European projects – CORDIS and EUREKA.

10.3 Investment data

For investment data we used a temporary licence of the PitchBook database [45] that covers more than 900 000 private companies and allows to track global venture capital, private equity and public markets. The keywords and Boolean operators used for each single investment query are listed in Annex F.

10.4 Social network data

For social data we used the started monitoring Twitter in order to compute statistics regarding discussions on the topic of IoT. The period covered is from September 2019 to February 2020. We collected around 1,600,000 tweets in English language only. For our analysis we have filtered the tweets by excluding those without valid hashtags and by reducing the number of tweets to 450,000. We used the same taxonomy as defined in Section 11. **Error! Reference source not found.** (below) for querying tweets corresponding to one of the 9 application domains defined in this document.

The scope of this analysis is to develop a hashtags network by applying modern analytic techniques of network analysis, exploring the relations between hashtags in a specific domain and extracting the most relevant hashtags or concepts and ideas. In order to detect sub-domains, we used the Louvain⁶ method to calculate communities where the hashtags are closely related. The colours of the community are computed randomly by using standard colour pallets and the network layout is developed using the circle packing algorithm.

For each application domain, we developed a hashtags network. Usually, there are five or six communities for the hashtags network developed. The communities, in this study, can represent technologies, specific domain, geographical area or brands. For each community, there exists a master node, characterized by a high co-occurrence frequency with the others hashtags –i.e. degree value, in network terminology. On the study visualizations, the degree value is represented by the node size.

⁶ <https://python-louvain.readthedocs.io/en/latest/>

11. DATA SOURCES ANALYSIS

In order to get insights into the emerging trends in the IoT domain, we utilized a set of data sources, described in Section 10, dealing with patent inventions, scientific publications, and financial data. Those sources were analysed by adopting an application-domain view, as introduced in Section 9.1. To ensure consistency, in mining the selected data sources, we used the same consolidated list of keywords and Boolean operators described in Annex F.

The next paragraph provides a first analysis of the achieved results, across the different domains. While, data characterizing each application domain are contained in Annex G.

— Annex G presents the outcomes resulting from the mining of the diverse data sources.

11.1 Patent inventions per sector

For each recognized application domain of IoT, the number of patent inventions (simple patent families) was worked out outlining the weight of the top-10 organizations. As depicted in Figure 11, some preliminary insights are:

- “Food chain” domain is largely the most covered area for IoT inventions registration –it has almost the double of patents of the second one.
- Only for “Smart City” and “Smart Grid/Smart Power” domains, the weight of the top-10 organization is significant –i.e. about half and more than half of the patents, respectively.
- Patents ownership shows a high variability across the sectors. The relative patents share values, owned by the top 10 players, range from 8% (of “Agriculture” and “Health, Medical and Pharmaceutical” sectors) to 62 % of the “Smart Grid/Smart Power” application domain.
- Agriculture and IoT is a sector not yet mature enough.

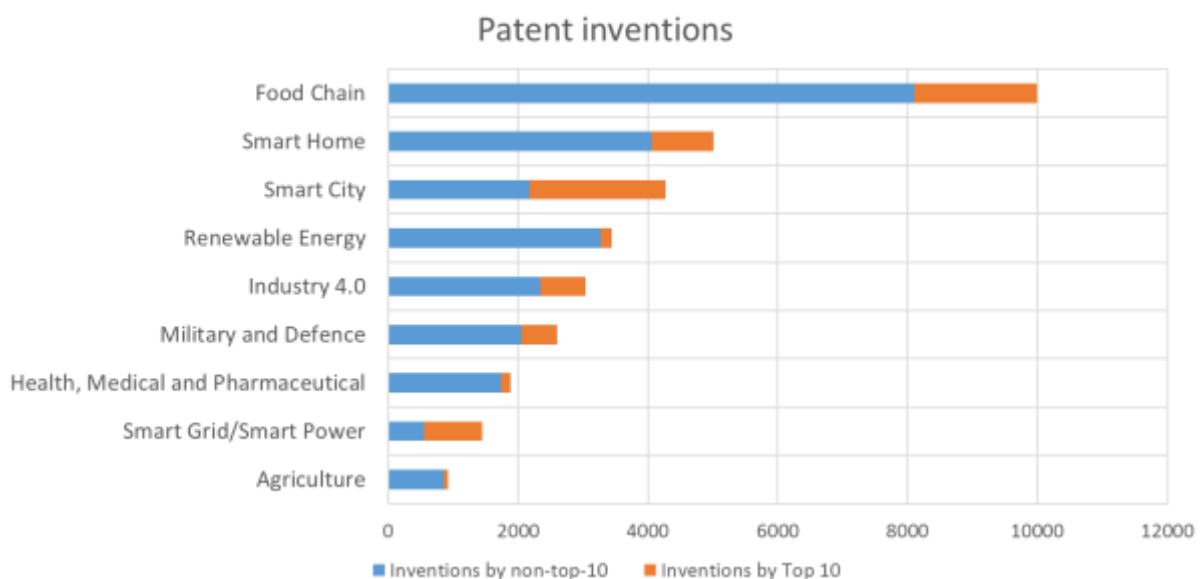


Figure 11. Patent inventions across the analyzed IoT application domains

11.2 Patent inventions generation countries

The number of patents registered by the top-10 organizations, per sector, was clustered per country in order to recognize the most innovative regions –i.e. inventions ownership. Some first insights are shown in

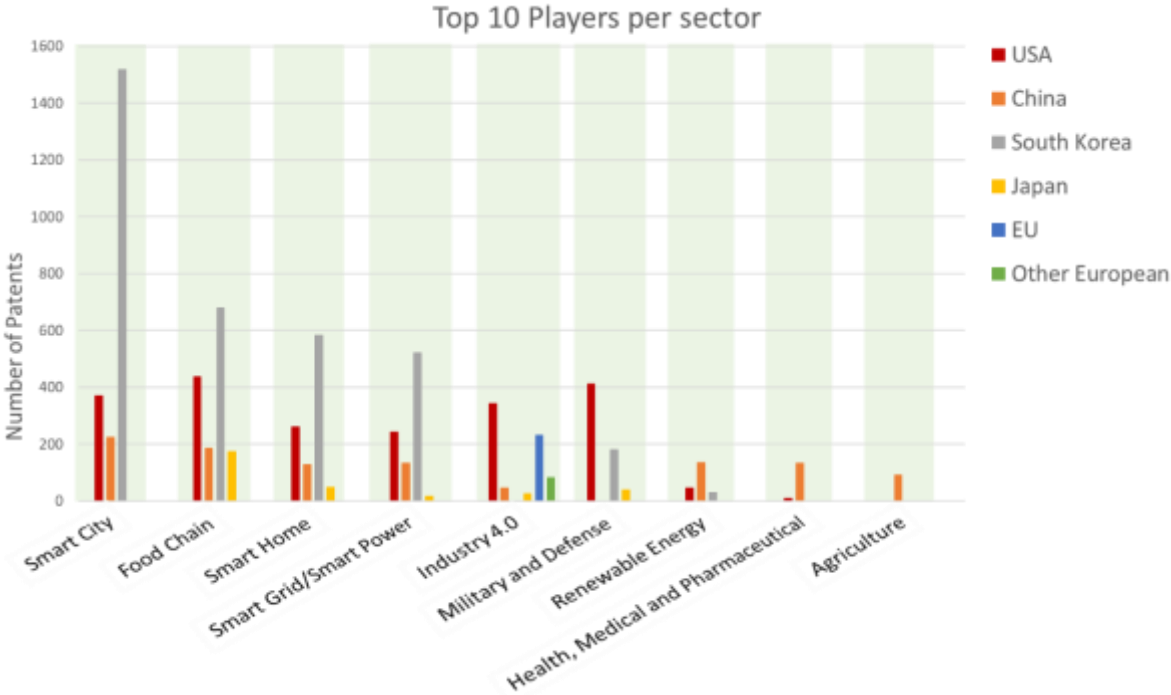


Figure 12:

- (a) European organizations are present in the top-10 list of one domain only, “Industry 4.0”.
- (b) Chinese organizations are well positioned in all the market sectors, but “Military and Defence” –it remains to study whether this is because they do not register their military inventions in other countries.
- (c) USA organizations are well-positioned in all the IoT market sectors, but “Agriculture”.
- (d) South Korea organizations (noticeably Samsung Electronics and LG electronics) lead the largest market sectors (in particular “Smart City”), but they are not present in the top-10 list for “Industry 4.0”.
- (e) All the top-10 organizations of the “Agriculture” sector are Chinese.
- (f) Almost all the top-10 organizations of the “Health, Medical and Pharmaceutical” sector are Chinese.
- (g) Samsung Electronics is by far the owner of the highest number of patented inventions. The company appears in the top 10 players for 6 of the 9 application domains, recognized by the study –i.e. all but ‘Agriculture’, ‘Health, Medical and Pharmaceutical’, and ‘Industry 4.0’.

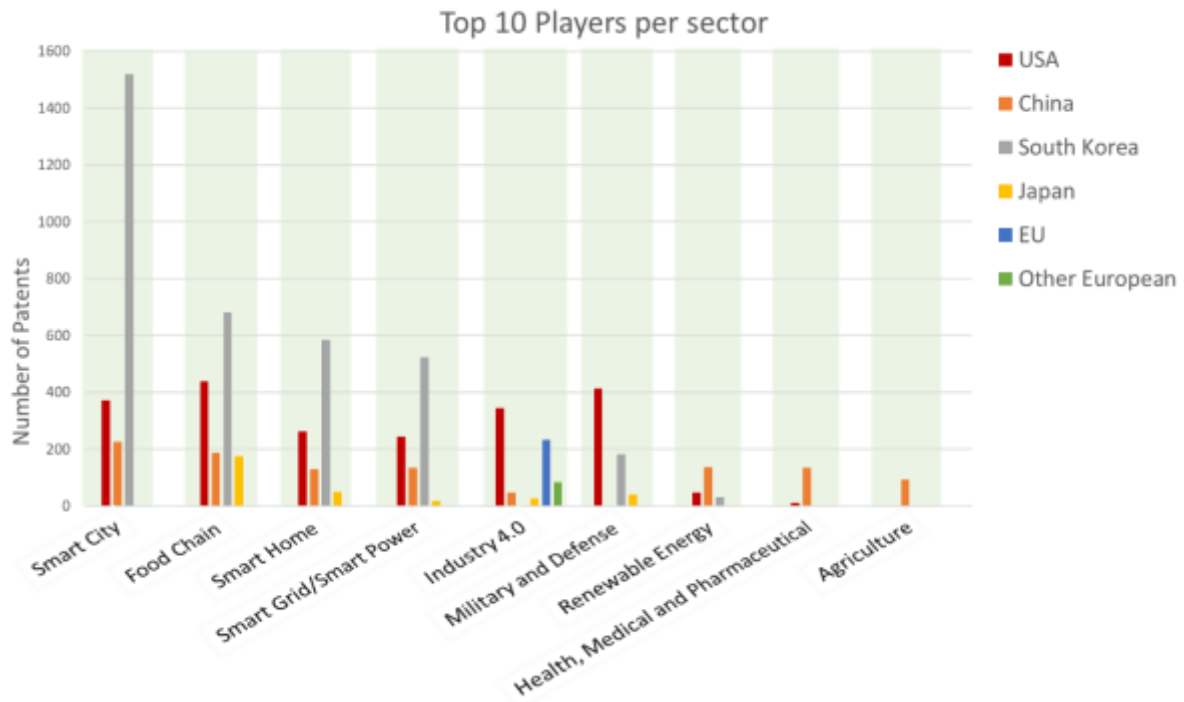


Figure 12. Geographic distribution of the Top-10 organizations, per sector.

11.3 Patent inventions registration countries

As to the IoT marketplaces, it is useful to analyse the countries where a given invention has been registered, in order to protect and leverage it. Figure 13 shows where patents have been registered, for each sector, distinguishing among three different areas: EU market, most interesting national market, and worldwide market. It is noteworthy that:

- (a) EU market is always an attractive IoT marketplace, with the exception of the “Agriculture” sector.
- (b) For EU, the three largest market sectors are, in order: “Smart City”, “Food Chain” and “Smart Home”
- (c) China is the most interesting market for all the sectors, with the exceptions of “Military and Defence” and “Smart Grid/Smart Power” –see also the correlation with the previous analysis on the top-10 industrial players.
- (d) Also considering the previous analysis on top-10 industries, in terms of future IoT marketing, China has great potentialities in the sectors of “Renewable Energy”, “Health, Medical, and Pharmaceutical” and “Agriculture”.

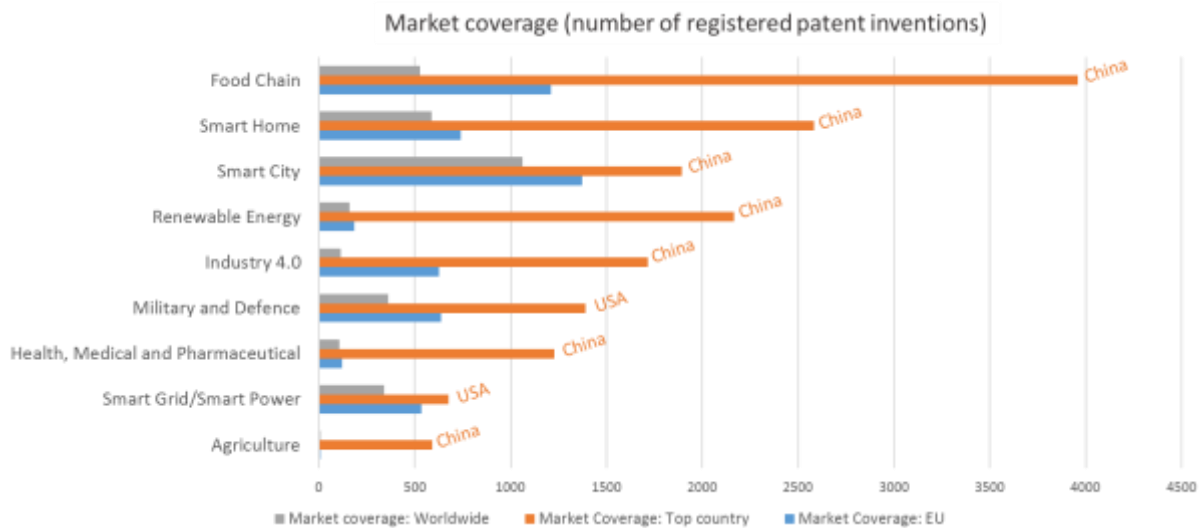


Figure 13. Patent invention registration countries and consequent market coverage.

11.4 Patent inventions growth

To understand the maturity and disrupting nature of IoT technology in the different sectors, it is useful to analyze the patents growth, in the last 10 years. Naturally, for all the considered application sectors, IoT-related patents have had a constant growth in the last decade. However, this growth is different being characterised by a year when the growth decisively escalated moving from a linear to a geometrical/exponential one. This acceleration can be caused by different factors, including political, societal, and technological reasons –including the introduction of correlated or enabling technologies. Figure 14 shows the different “acceleration” years, per each analysed sector. It is noteworthy:

- (a) “Industry 4.0” and “Food Chain” are the *veteran* IoT sectors. While for the first the exponential growth started around 2010, the latter (the largest IoT patent sector) exploded about 2014, only.
- (b) “Smart Home”, the second largest IoT patent sector, started relatively late (around 2010) but was a steep growth.
- (c) The third largest IoT patent sector, “Smart City“, is characterized by a timeline similar to “Smart Home”.
- (d) “Renewable Energy” and “Health, Medical and Pharmaceutical” patent sectors have seen a recent growth.

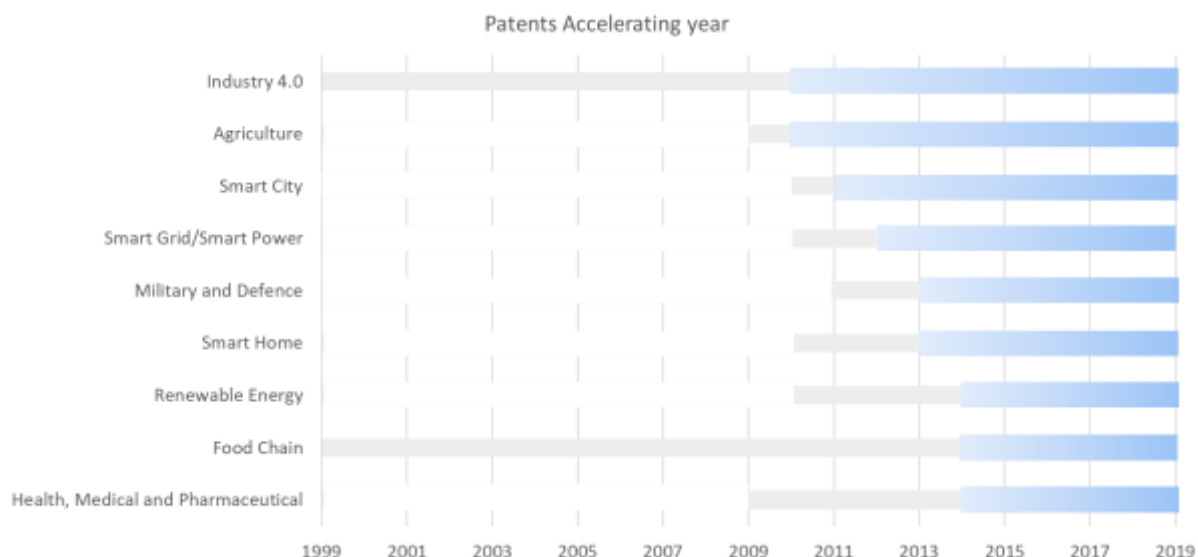


Figure 14. Patents growth escalation years, per domain sector (grey = regular growth; blue = exponential growth).

11.5 Scientific publications per sector and per country

Another important source to understand the maturity and importance of technology, in a given application domain, is the number of scientific publications. For all the considered application domains, the publications dealing with IoT have seen an escalation growth as of 2014-2015.

Figure 15 shows the number of publications per sector in the last 20 years, distinguishing the contributions from Europe and the rest of the world. While, Figure 16 depicts the percentage of European contribution in the respect of the country that has published most on a specific domain (i.e. the leading country) and the rest of the world. It is worthy to note that:

- (a) Despite the relatively low number of registered patents, the “Health, Medical and Pharmaceutical” domain has the largest number of publications.
- (b) While “Food Chain” is the most popular sector for patent inventions, it has the lowest number of publications.
- (c) European contribution is always significant, with the exception of “Military and Defence”. Europe provides more than 50% of the publications on “Industry 4.0”, and almost half the publications dealing with “Smart City”. In those sectors, Europe resulted the leading country.
- (d) Europe and China are the leading publication countries on all the considered domains. In addition to “Industry 4.0” and “Smart City”, Europe publishes most on “Smart Grids/Smart Power”, too. For all the others domains, most of the publications come from China.

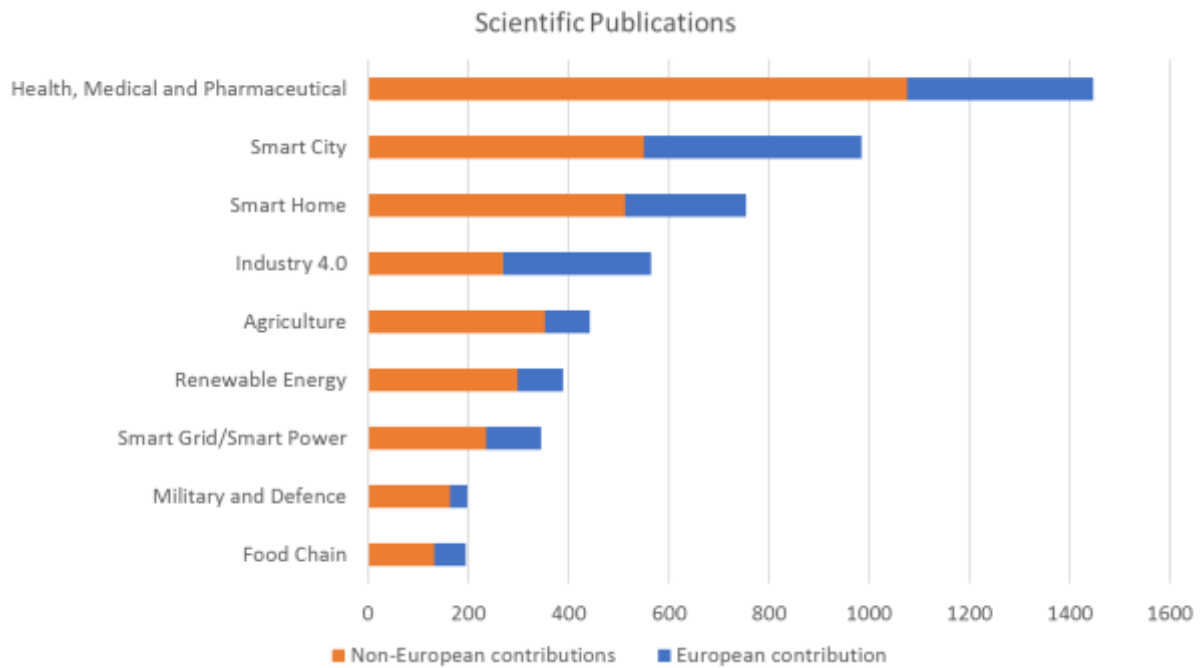


Figure 15. Number of scientific publications on the diverse application domains.

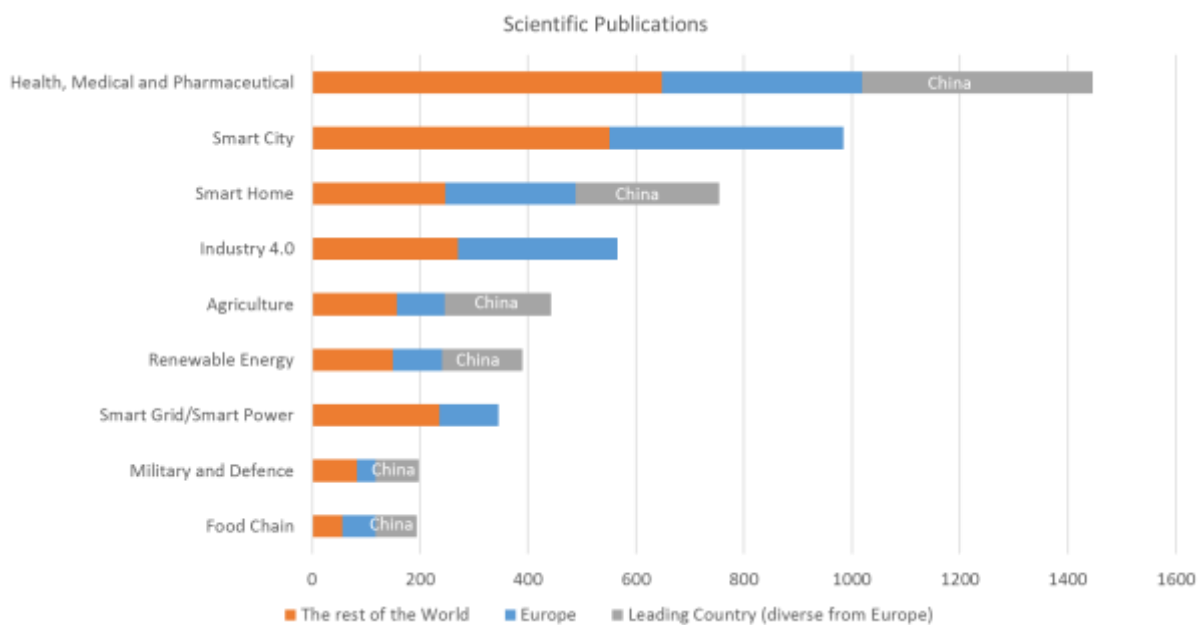


Figure 16. Number of scientific publications from Europe, the country that publishes most, and the rest of the world.

11.6 Scientific publication keywords

Analyzing the ten most popular keywords from scientific publications, it is possible to distinguish two categories of recurrent terms:

(a) Application-related keywords

- Smart manufacturing/factoring; IIoT (Industrial IoT)

- Smart Farms/Agriculture; Precision agriculture; Soil moisture.
- Food safety; Traceability, Supply chain.
- E health; Health monitoring.
- Intrusion detection; Cyber-attacks; Vulnerability.
- Energy efficiency.
- Gas sensors; Smart meters; Demand response; Privacy.
- Smart building; Home automation.

(b) Technology-related keywords

- Wireless sensor network;
- Cyber-physical;
- Security; Block chaining
- Low power
- Cloud computing; Edge computing; Fog computing
- Big Data;
- AI/ML
- RFID

11.7 Financial Landscape

The financial landscape is captured by analysing the number of public and private companies and investors, as well as the number of exits –acquisitions are extremely important to understand the value and maturity of a market sector. Finally, top investments are considered. Unfortunately, financial analyses do not cover all the recognized sectors but only six of them.

Figure 17 shows the number of public and private companies and investors that are active on the diverse domain sectors; on the same axis, it also reports the number of exits. Finally, on the right ordinal axis, it shows the top investment for each sector –in MEur. It is noteworthy that:

- “Food Chain”, the largest sector in producing patent inventions, has the lowest number of companies, investors, and exits –this suggests a certain maturity of the sector.
- “Smart City” has by far the largest number of companies, investors, and exits as well as the second largest top investment –this suggests a sector interested by a fast evolution.
- In comparison to “Smart City”, “Smart Home” has a far less number of companies (as for “Food Chain”) but its top investment values almost the double –this suggests a consolidated sector that lives a new spring.
- “Agriculture” IoT sector values the third top investment.
- As expected, the number of companies and investors are directly correlated.

For all the analyzed market sectors, the investments present a continue growing over the time –the analysis period is 2010-2018. Such growth escalated around 2015-2016 for all the considered sectors, with the exception of the “Renewable Energy” domain.

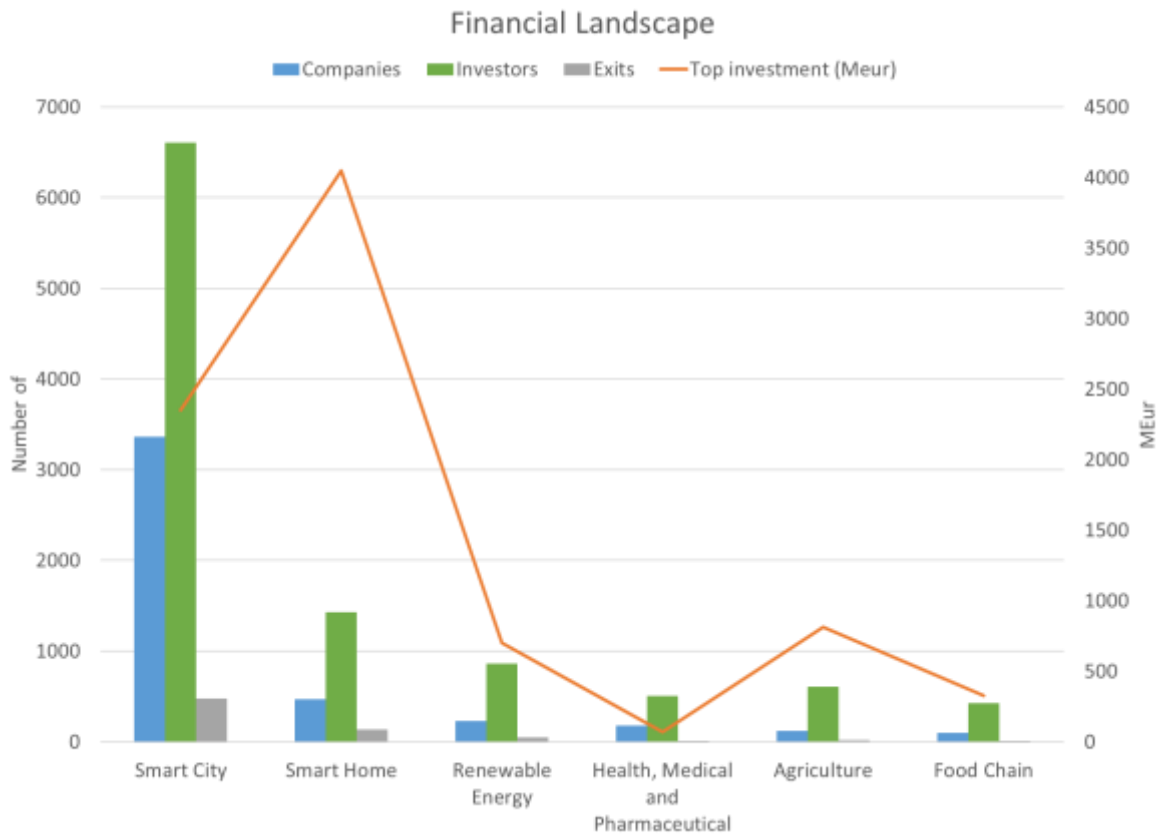


Figure 17. Financial landscape characterizing the IoT sectors (i.e. number of public and private companies and investors, number of exits, top investment).

11.8 Twitters analysis results

Exploring the relations and the degree value that characterize the mined hashtags, in all the specific domain, it is possible to extract the recurring concepts and ideas, along with their connections, which are present regardless the domain specificity. These concepts and ideas characterize IoT in the Twitter universe of discourse. The obtained conceptual schema is depicted in Figure 18. These concepts, in the Twitter world, are perceived as both the enabling technologies and the main determinants for the IoT success.

Noticeably, IoT makes use of AI and BD. A key determinant of IoT is cybersecurity –in particular Blockchain. IoT plays an important role in the Supply-chain area. Investments and Asia are two important factors that influence IoT success. Finally, the utilization of IoT transforms a domain into a “smart” domain.

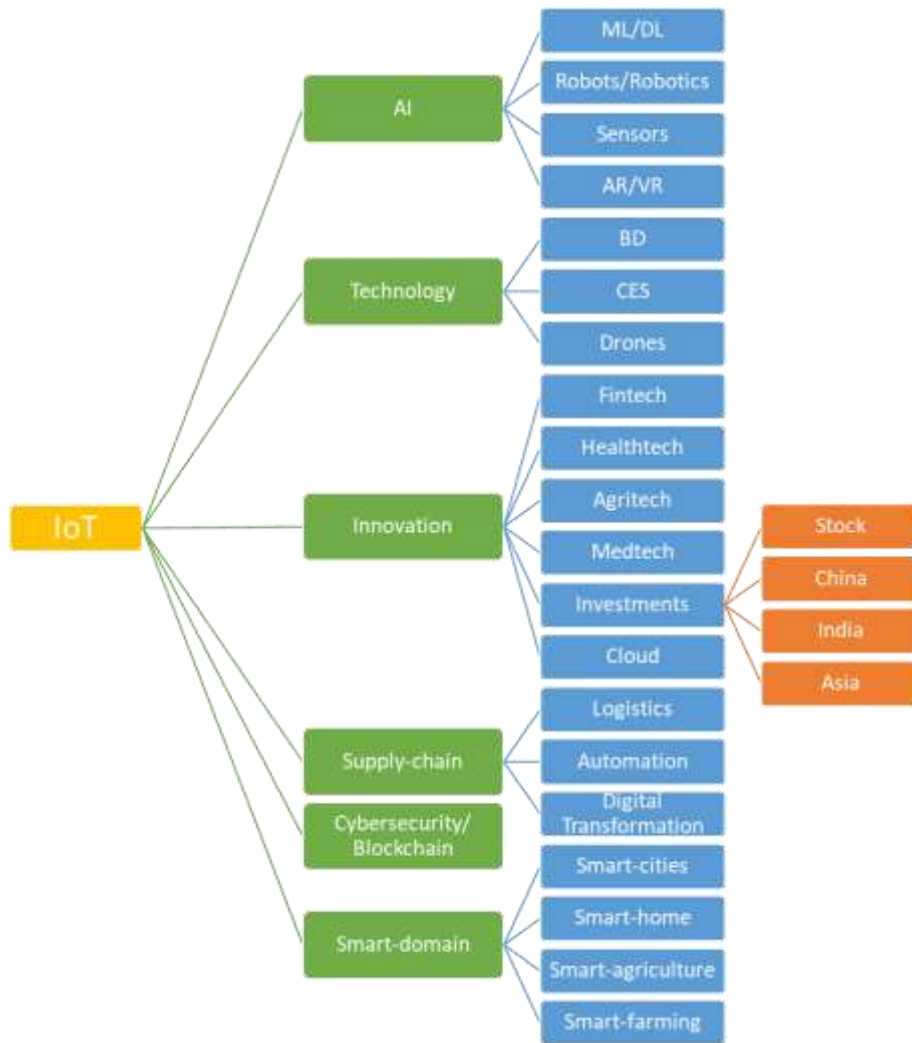


Figure 18. Conceptual model inferred from the Twitters analysis

12. IOT IN EUROPE – REGULATORY AND LEGAL ASPECTS

Presently, there is no legal framework specifically tailored for IoT. The **existing laws applicable to IoT are scattered across different domains**. Their feasibility to handle the interconnected world of IoT is to be further reassessed, potential legal barriers identified and new legal solution proposed if needed.

Currently the regulatory concerns in the context of IoT revolve around setting up technological infrastructure and building trust in users and business.

At the same time there are more **regulations coming from the area of robotics, AI, and Big Data**, which are important part of IoT. Seamless integration of these domains, and potentially many more in the future will be one of the constant challenges pertaining to the IoT legal fabric and stemming from the mere nature of the IoT. One highlights that IoT, now mostly seen as a network of connected devices and sensors, is bound to develop towards the Internet of Everything (IoE): a network of devices, people, networks, data, processes, etc. This will need development of the **agile legal framework capable of dealing with issues of the interconnected future**.

IoT has a horizontal and cross-cutting character connecting areas that have been developed as regulatory vertical silos (e.g. agriculture, manufacturing, construction, energy and resources, environmental protection, transport, healthcare, aviation, education, banking, etc.). The present overview uncovers the **horizontal legal frameworks applicable to IoT** at four key levels: 1) at level concerned with setting up the technological infrastructure; 2) level concerned with network interoperability; 3) level linked to creating trustworthy environment for a user; and 4) and level concerned with bringing value to the society.

As far as the first level is concerned, the key legal frameworks relating to IoT are those on electronic communications and radio spectrum. Interoperability is primarily secured by the laws on standardisation. On the level of the creation of the trustworthy environment for a user, the existing EU policy documents and industry organisations point to privacy, data protection and (cyber)security as the most relevant to IoT. **Liability and laws relating to the Digital Single Market (DSM)** are key regulatory challenges linked to bringing value to the economy and society.

The legal barriers in adoption of IoT can be linked either to the existing regulations or to the lack of the relevant IoT regulation. A comparison of IoT regulations in Europe, China and the U.S. by international law firm Hogan Lovells [46] shows that comparatively the EU has the highest level of regulations applying to the IoT environment. There are more than twice as many regulations as there are in the U.S. These may serve as a barrier to adoption, especially because most of those regulations (e.g. for telecoms) do not take into account the specificity of the IoT environment. On the other hand, the lack of IoT specific law that provides for general rules can be a barrier mostly for the business, because business needs some level of security to invest.

— The above-mentioned IoT-relevant regulatory and legislation area are discussed in more detail in Annex G.

13. CONCLUSIONS AND FUTURE WORK

The second generation of IoT platforms (IoT 2.0) is leveraging the digital transformation paradigm and technologies (e.g. AI and ML) to generate intelligence and serve actionable knowledge to clients. The network (Internet) has further become the true engine of our society and economy transformation, introducing new and more reliable communication patterns between the physical (e.g. things and daily transactions) and the digital worlds –digital replicas of real things and transactions to understand their behaviour and run simulations.

In this landscape, IoT is rapidly moving from being used in specialist domains to become a mainstream technology. This process, in turn, pushes the development of edge solutions, such as edge clouds, moving the intelligence generation from the center to the edge of the network. However, there are still some interoperability challenges to fully integrate IoT platforms and consolidate the maturity process characterizing IoT technology. Since these interoperability barriers have significantly limited IoT diffusion, important IT players are developing an essential process of standardization and convergence in IoT field.

The European Green Deal strategy will provide an important boost to IoT development and integration in mainstream applications because of the need to improve efficiency in all the economic sectors, at both the industrial and social level. A green economy is mainly a “smart” economy, where the physical and the digital worlds are closely connected to optimize resources management and consumption. Therefore, IoT 2.0 is crucial for collecting the necessary information generated by real entities/phenomena and for providing back the required intelligence (for example carried out by running simulations) to act on the physical world.

Future work will investigate the role of digital twins and other physical-digital interaction patterns, such as augmented and virtual reality, in the process of making our society smarter and hence greener. B6 unit of JRC is deeply involved in this area, also through a couple of actions promoted to develop the Green Deal Data Space [47]: GreenData4All and Destination Earth.

BIBLIOGRAPHY

- [1] ISO/IEC 30141:2018, "Internet of Things (IoT) — Reference Architecture," ISO/IEC, Geneva, 2018.
- [2] W3C, "Web of Things (WoT) Architecture," W3C, Cambridge, MA, USA, 2019.
- [3] ISO/IEC JTC 1/WG 10, "Information technology – Internet of Things Reference," ISO/IEC, Geneva, 2016.
- [4] A. Al-Fuqaha and e. alteri, "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications," *IEEE Commun. Surveys Tuts*, vol. 17, no. 4, p. 2347–2376, 2015.
- [5] ISO 19731, "Digital analytics and web analyses for purposes of market, opinion and social research — Vocabulary and service requirements," ISO, Geneva, 2017.
- [6] ISO/IEC 20924, "Information technology — Internet of Things (IoT) — Vocabulary," ISO/IEC, Geneva, 2018.
- [7] ITU-T Y.2060, "Recommendation Y.2060: Overview of the Internet of things," ITU, Geneva, 2012.
- [8] ISO/IEC 38505-1, "Information technology — Governance of IT — Governance of data — Part 1: Application of ISO/IEC 38500 to the governance of data," ISO/IEC, Geneva, 2017.
- [9] IEC, "Terms and definitions relating to information technology: internet of things and services," 09 05 2018. [Online]. Available: <http://www.electropedia.org/iev/iev.nsf/display?openform&ievref=871-05-05>. [Accessed 27 12 2019].
- [10] C. K. A. K. A. O. F. a. T. S. Granell, "Internet of Things," in *Manual of Digital Earth*, Singapore, Springer, 2020, pp. 387-423.
- [11] OGC, "SensorThings API International Standard," OGC, 2016.
- [12] S. Nativi, P. Desruelle, G. Misuraca, S. Schade, A. Kotsev and M. Lutz, "Strategy for the Analysis of Innovative Digital Technology ver.6.0. J," JRC (B6 Unit), Ispra, 2019.
- [13] European Commission DG JRC , "The EC Megatrends Hub," JRC, 2019. [Online]. Available: https://ec.europa.eu/knowledge4policy/foresight/about_en. [Accessed 02 01 2020].
- [14] S. Nativi, "ICT Landcape Conceptual Document ver. 3.0," JRC (B6 Unit), Ispra, 2019.
- [15] K. Cukier and V. Mayer-Schoenberger, "The Rise of Big Data," May/June 2013. [Online]. Available: <https://www.foreignaffairs.com/articles/2013-04-03/rise-big-data>. [Accessed 15 September 2020].
- [16] L. Hay Newman, "What We Know About Friday's Massive East Coast Internet Outage," 2016. [Online]. Available: <https://www.wired.com/2016/10/internet-outage-ddos-dns-dyn/>. [Accessed 03 01 2020].
- [17] The OWASP IoT Security Team, "OWASO Top 10 IoT," 2018. [Online]. Available: <https://www.owasp.org/images/1/1c/OWASP-IoT-Top-10-2018-final.pdf>. [Accessed 03 01 2020].
- [18] Zigbee Alliance, "Amazon, Apple, Google, and the Zigbee Alliance and Its Board Members Form Industry Working Group to Develop a New, Open Standard for Smart Home Device Connectivity," December 2019. [Online]. Available: https://zigbeealliance.org/news_and_articles/connectedhomeip/. [Accessed 31 12 2019].
- [19] MIT Technology Review, "Amazon, Apple and Google joining forces could be what makes smart homes happen," 12 2019. [Online]. Available: <https://www.technologyreview.com/f/614978/amazon-apple-and-google-joining-forces-could-be-what-makes-smart-homes-happen/>. [Accessed 31 12 2019].
- [20] K. McCarthy, "The IoT wars are over, maybe? Amazon, Apple, Google give up on smart-home domination dreams, agree to develop common standards," 18 Dec 2019. [Online]. Available: https://www.theregister.co.uk/2019/12/18/iot_standards_war/. [Accessed 31 12 2019].

- [21] OCF, "About Open Connectivity Foundation," 2019. [Online]. Available: <https://openconnectivity.org/foundation/>. [Accessed 31 12 2019].
- [22] OneM2M, "oneM2M - Standards for M2M and the Internet of Things," 2017. [Online]. Available: <http://www.onem2m.org/about-onem2m/why-onem2m#>. [Accessed 31 12 2019].
- [23] A. Deol, K. Figueredo, S.-W. Lin, B. S. D. Murphy and J. Yin, "Advancing the Industrial Internet of Things: An Industrial Internet Consortium and oneM2M™ Joint Whitepaper," 12 12 2019. [Online]. Available: http://www.onem2m.org/images/files/IIC_oneM2M_Whitepaper_final_2019_12_12.pdf. [Accessed 12 12 2019].
- [24] AIOTI, "Advancing EU IoT Research and Innovation," August 2018. [Online]. Available: https://aioti.eu/wp-content/uploads/2018/09/AIOTI_Position_Paper_HEU_2018_for_publishing.pdf. [Accessed 31 12 2019].
- [25] OMASpecWorks, "IPSO Alliance Merges with Open Mobile Alliance to Form OMA SpecWorks," 27 03 2018. [Online]. Available: <https://www.omaspecworks.org/ipso-alliance-merges-with-open-mobile-alliance-to-form-oma-specworks/>. [Accessed 31 12 2019].
- [26] OMA SpecWorks, "About OMA SpecWorks," 2019. [Online]. Available: <https://www.omaspecworks.org/about/>. [Accessed 31 12 2019].
- [27] Mozilla, "WebThings," [Online]. Available: <https://iot.mozilla.org/about/>. [Accessed 02 01 2020].
- [28] Mozilla, "Web Thing API: unofficial draft," 02 01 2020. [Online]. Available: <https://iot.mozilla.org/wot/>. [Accessed 02 01 2020].
- [29] AIOTI, "European IoT challenges and opportunities: 2019–2024," [Online]. Available: <https://aioti.eu/wp-content/uploads/2019/09/AIOTI-Priorities-2019-2024-Digital.pdf>. [Accessed 31 12 2019].
- [30] i-SCOOP, "Digital transformation technologies: IoT as the Internet of Transformation," [Online]. Available: <https://www.i-scoop.eu/digital-transformation/digital-transformation-technologies-iot/>. [Accessed 02 01 2020].
- [31] J. Carter, "A closer look at the Internet of Things 2.0 – and why it's inevitable," 29 04 2017. [Online]. Available: <https://www.techradar.com/news/a-closer-look-at-the-internet-of-things-20-and-why-its-inevitable>. [Accessed 02 01 2020].
- [32] S. Ranger, "What is the IIoT? Everything you need to know about the Industrial Internet of Things," 01 March 2019. [Online]. Available: <https://www.zdnet.com/article/what-is-the-iiot-everything-you-need-to-know-about-the-industrial-internet-of-things/>. [Accessed 22 September 2020].
- [33] Industrial Internet Consortium, "THE INDUSTRIAL INTERNET CONSORTIUM: A GLOBAL NOT-FOR-PROFIT PARTNERSHIP OF INDUSTRY, GOVERNMENT AND ACADEMIA," IIconsortium, September 2020. [Online]. Available: <https://www.iiconsortium.org/>. [Accessed September 2020].
- [34] Reply, "The Evolution of Consumer IoT," September 2020. [Online]. Available: <https://www.reply.com/en/topics/internet-of-things/the-evolution-of-the-consumer-internet-of-things#:~:text=The%20Consumer%20IoT%20refers%20to,internet%2C%20collecting%20and%20sharing%20data..> [Accessed September 2020].
- [35] i-SCOOP, "Consumer Internet of Things (CIoT) – what is it and how does it evolve?," September 2020. [Online]. Available: <https://www.i-scoop.eu/internet-of-things-guide/what-is-consumer-internet-of-things-ciot/>. [Accessed September 2020].
- [36] S. Khvoynitskaya, "Internet of everything vs internet of things: what is the difference?," 24 January 2020. [Online]. Available: <https://www.itransition.com/blog/internet-of-everything-vs-internet-of-things>. [Accessed 22 September 2020].
- [37] B. Dorsemayne, J. Gaulier, J. Wary, P. Urien and N. Kheir, "Internet of Things: a definition & taxonomy," in *2015 9th International Conference on Next Generation Mobile Applications, Services and Technologies*, Cambridge (UK), 2015.
- [38] C. Elena-Lenz, "Internet of Things: Six Key Characteristics," 23 08 2014. [Online]. Available: <https://designmind.frogdesign.com/2014/08/internet-things-six-key-characteristics/>. [Accessed 18 03 2020].
- [39] O. Vermesan and P. Friess, "Internet of Things - From Research and Innovation to Market Deployment," River Publishers Series in Communications, 2014.
- [40] Cisco, "Internet of Things at-a-glance," 2016. [Online]. Available: <https://www.cisco.com/c/dam/en/us/products/collateral/se/internet-of-things/at-a-glance-c45-731471.pdf>. [Accessed 12 01 2020].

- [41] V. Rozsa, M. Deniszczwicz, M. Dutra, P. Ghodous, C. Ferreira da Silva and e. al., "An Application Domain-Based Taxonomy for IoT Sensors," in *23rd ISPE International Conference on Trans-disciplinary Engineering: Crossing Boundaries*, Curitiba, Brazil, 2016.
- [42] IoT UK, "Internet of Things Taxonomy," 12 2016. [Online]. Available: file:///C:/Users/Stefano/Downloads/slidelegend.com_internet-of-things-taxonomy-iotuk_5ae96e767f8b9adb6a8b4575.pdf. [Accessed 19 03 2020].
- [43] IDC, "IDC's Internet of Things (IoT) Taxonomy Map," 2014. [Online]. Available: https://www.idc.com/downloads/IoT_Taxonomy_Map_V2_Nov2014.pdf. [Accessed 19 03 2020].
- [44] E. JRC, "Tim Analytics tools," European Commission, [Online]. Available: <https://www.timanalytics.eu/website/>.
- [45] P. platform. [Online]. Available: <https://pitchbook.com/>.
- [46] L. Hogan, "Comparisson of regulatory requirements in the European Union, United States, and China," [Online]. Available: <https://www.hoganlovells.com/en/blogs/internet-of-things/study-shows-complexity-and-uncertainty-of-iot-regulation-in-europe>.
- [47] European Commission, "A European strategy for data -COM(2020) 66 final:," European Commission, Brussels, 2020.
- [48] GSMA, "NB-IoT Deployment Guide to Basic Feature set Requirements," 2019. [Online]. Available: <https://www.gsma.com/iot/wp-content/uploads/2019/07/201906-GSMA-NB-IoT-Deployment-Guide-v3.pdf>. [Accessed 01 01 2020].
- [49] B. Garcia, "What is ZigBee?," 06 11 2018. [Online]. Available: <https://www.teldat.com/blog/en/zigbee-smart-energy-smart-metering-home-automation/>. [Accessed 01 01 2020].
- [50] Zigbee Alliance, "The Zigbee Alliance is the standard-bearer of the open IoT," [Online]. Available: <https://zigbeealliance.org/>. [Accessed 01 01 2020].
- [51] A. Lavric and V. Popa, "Internet of Things and LoRa™ Low-Power Wide-Area Networks: A survey," in *2017 International Symposium on Signals, Circuits and Systems (ISSCS)*, Iasi (Romania), 2017.
- [52] U. Raza, P. Kulkarni and M. Sooriyabandara, "Low Power Wide Area Networks: An Overview," 11 01 2017. [Online]. Available: <https://arxiv.org/pdf/1606.07360.pdf>. [Accessed 01 01 2020].
- [53] : LoRa Alliance & WBA IoT WG, "Wi-Fi & LoRaWAN® Deployment Synergies: Expanding addressable use cases for the Internet of Things," September 2019. [Online]. Available: <https://lora-alliance.org/sites/default/files/2019-09/wi-fi-and-lorawanr-deployment-synergies.pdf>. [Accessed 01 01 2020].
- [54] Thread Group Alliance , "THREAD Certified Products," [Online]. Available: <https://www.threadgroup.org/what-is-thread>. [Accessed 01 01 2020].
- [55] DASH 7 Alliance, "DASH7 ALLIANCE PROTOCOL," [Online]. Available: <https://dash7-alliance.org/#technology>. [Accessed 01 01 2020].
- [56] Sigfox, "SIGFOX TECHNOLOGY," [Online]. Available: <https://www.sigfox.com/en/what-sigfox/technology>. [Accessed 01 01 2020].
- [57] D. Bergquist, "NFC and IoT: What You Need to Know," 05 02 2019. [Online]. Available: <https://www.verypossible.com/blog/nfc-and-iot-what-you-need-to-know>. [Accessed 01 01 2020].
- [58] Worldpay Editorial Team, "How secure are NFC terminals?," 30 07 2019. [Online]. Available: <https://www.worldpay.com/en-us/insights-hub/article/how-secure-are-nfc-terminals>. [Accessed 01 01 2020].
- [59] AWS, "AWS IoT: IoT services for industrial, consumer, and commercial solutions," [Online]. Available: <https://aws.amazon.com/iot/>. [Accessed 01 01 2020].
- [60] C. Baby, "IoTZone: A Look at the AWS IoT Ecosystem," 16 08 2018. [Online]. Available: <https://dzone.com/articles/aws-iot-ecosystem>. [Accessed 01 01 2020].
- [61] Google Cloud, "Overview of Internet of Things," 23 07 2019. [Online]. Available: <https://cloud.google.com/solutions/iot-overview>. [Accessed 01 01 2020].

- [62] S. Boral, "IoT Tech Trends: What Happened to Google's Brillo and Weave?," 27 05 2019. [Online]. Available: <https://www.iottectrends.com/what-happened-google-brillo-weave/>. [Accessed 03 01 2020].
- [63] Apple, "HomeKit," [Online]. Available: <https://developer.apple.com/homekit/>. [Accessed 01 01 2020].
- [64] Apple, "HomeKitADK," December 2019. [Online]. Available: <https://github.com/apple/HomeKitADK>. [Accessed 01 01 2020].
- [65] Samsung Electronics Co. Ltd., "Samsung ARTIK™ Smart IoT Platform and ThingWorx Unite to Simplify Industrial IoT Asset Monitoring," 26 02 2018. [Online]. Available: <https://news.samsung.com/us/samsung-artik-smart-iot-platform-thingworx-industrial-iot-asset-monitoring/>. [Accessed 01 01 2020].
- [66] Samsung, "How to Do More by Doing Less with Samsung's Ecosystem," 22 07 2019. [Online]. Available: <https://news.samsung.com/us/samsungs-ecosystem-how-to-do-more-by-doing-less/>. [Accessed 01 01 2020].
- [67] Samsung, "SmartThings Classic Developer Documentation," 2020. [Online]. Available: <https://smarthings.developer.samsung.com/docs/index.html>. [Accessed 01 01 2020].
- [68] IBM, "IBM Watson IoT Platform," [Online]. Available: <https://www.ibm.com/us-en/marketplace/internet-of-things-cloud>. [Accessed 01 01 2020].
- [69] Bosh Software Innovation, "Capabilities of the Bosch IoT Suite," [Online]. Available: <https://www.bosch-iot-suite.com/capabilities-bosch-iot-suite/>. [Accessed 03 01 2020].
- [70] Harvard Business Review, "Data-driven Work Spaces: IoT and AI expand the Promise of Smart Buildings," 27 09 2018. [Online]. Available: https://azure.microsoft.com/mediahandler/files/resourcefiles/create-smart-spaces-with-azure-digital-twins/Harvard_Business_Review_Data_Driven_Work_Spaces_EN_US.pdf. [Accessed 17 03 2020].
- [71] S. Boral, "IoT Tech Trtends: 9 of the Best IoT Platforms to Watch in 2019," 01 09 2019. [Online]. Available: <https://www.iottectrends.com/best-iot-platforms/>. [Accessed 03 01 2020].
- [72] E. Commission, "COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS: INTERNET OF THINGS — An action plan for Europe," European Commission, Brussels, 2009.
- [73] E. Commission, "COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS: A Digital Single Market Strategy for Europe,," European Commission, Brussels, 2015.
- [74] E. Commission, "COMMISSION STAFF WORKING DOCUMENT: Advancing the Internet of Things in Europe Accompanying the document: Digitising European Industry Reaping the full benefits of a Digital Single Market," European Commission, Brussels, 2016.
- [75] ITU Academy, "Policies and Regulations," [Online]. Available: https://www.itu.int/en/ITU-D/Regional-Presence/AsiaPacific/Documents/Events/2018/IoT-BDG/IoT_Policy_Sept26%20Ismail%20Shah.pdf. [Accessed 03 01 2020].
- [76] I. Brock, C. Coslin, C. Derycke, C. Di Mauro and M. Felwick, "European Union: European Product Liability Directive: Stay Tuned, Guidance Is Around The Corner," 19 06 2019. [Online]. Available: <https://www.mondaq.com/Technology/816332/European-Product-Liability-Directive-Stay-Tuned-Guidance-Is-Around-The-Corner>. [Accessed 18 03 2020].
- [77] European Council, "Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products," 7 8 1985. [Online]. Available: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31985L0374&from=EN>. [Accessed 18 03 2020].
- [78] European Commission, "Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce')," 17 7 2000. [Online]. Available: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32000L0031>. [Accessed 18 03 2020].
- [79] European Parliament and Council, "On-line services in understanding of Directive (EU) 2015/1535 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (codification)," 17 09 2015. [Online]. Available: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L1535>. [Accessed 18 03 2020].

- [80] EUROPEAN PARLIAMENT AND OF THE COUNCIL, "Regulation (EU) 2019/1150 on promoting fairness and transparency for business users of online intermediation services," 20 6 2019. [Online]. Available: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R1150>. [Accessed 18 03 2020].
- [81] European Parliament and of the Council, "Regulation (EU) 2018/1807 on a framework for the free flow of non-personal data in the European Union," 14 11 2018. [Online]. Available: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R1807&from=EN>. [Accessed 18 03 2020].
- [82] European Parliament and of the Council, "Directive 96/9/EC on the legal protection of databases," 11 03 1996. [Online]. Available: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31996L0009&from=EN>. [Accessed 18 03 2020].
- [83] European Parliament and of the Council, "Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society," 22 05 2001. [Online]. Available: <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2001:167:0010:0019:EN:PDF>.
- [84] E. P. a. o. t. Council, "Directive (EU) 2019/790 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC," 17 04 2019. [Online]. Available: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019L0790&from=EN>. [Accessed 18 03 2020].
- [85] E. P. a. o. t. Council, "Directive 2003/98/EC on the re-use of public sector information," 17 11 2003. [Online]. Available: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32003L0098&from=EN>.
- [86] European Parliament and Council, "DIRECTIVE 2013/37/EU on amending Directive 2003/98/EC on the re-use of public sector information," 26 06 2013. [Online]. Available: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32013L0037&from=EN>. [Accessed 18 03 2020].
- [87] E. P. a. o. t. Council, "Directive (EU) 2019/1024 on open data and the re-use of public sector information," 26 06 2019. [Online]. Available: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019L1024&from=EN>. [Accessed 18 03 2020].
- [88] Bain & Company, "Unlocking Opportunities in the Internet of Things," *Online document*, 2018.
- [89] Statista, "Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025," *Online document*, 2019.

ANNEX A. OGC SensorThings API

At a high level the OGC SensorThings API provides two main functionalities and each function is handled by a part. The two parts are (i) the Sensing part, and (ii) the Tasking part [11]. In addition to that, the standard supports asynchronous data transactions through Message Queue Telemetry Transport (MQTT).

The Sensing part provides a standard way to manage and retrieve observations and metadata from heterogeneous IoT sensor systems. The sensing part of the standard relies on a simple data model (see Figure 19) organised around the concept of Datastreams that interconnect ‘Things’, ‘Sensors’ along with their current or historic geographic locations.

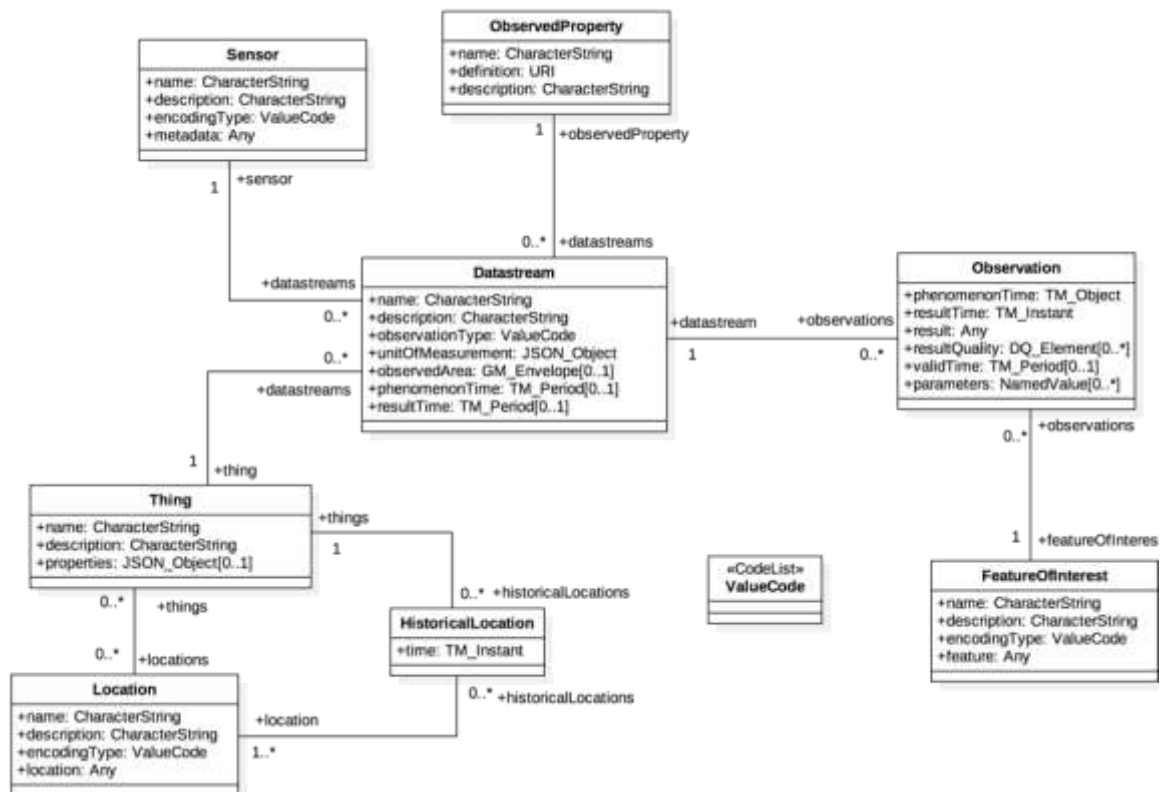


Figure 19. The SensorThings API Sensing data model. Source: OGC

The Tasking part provides a standard way for parameterizing - also called tasking - of taskable IoT devices, such as individual sensors and actuators, composite consumer / commercial / industrial / smart cities in-situ platforms, mobile and wearable devices, or even unmanned systems platforms such as drones, satellites, connected and autonomous vehicles, etc. The tasking data model (see Figure 20) provides a simple way for enabling tasking capabilities for IoT devices in an interoperable manner.

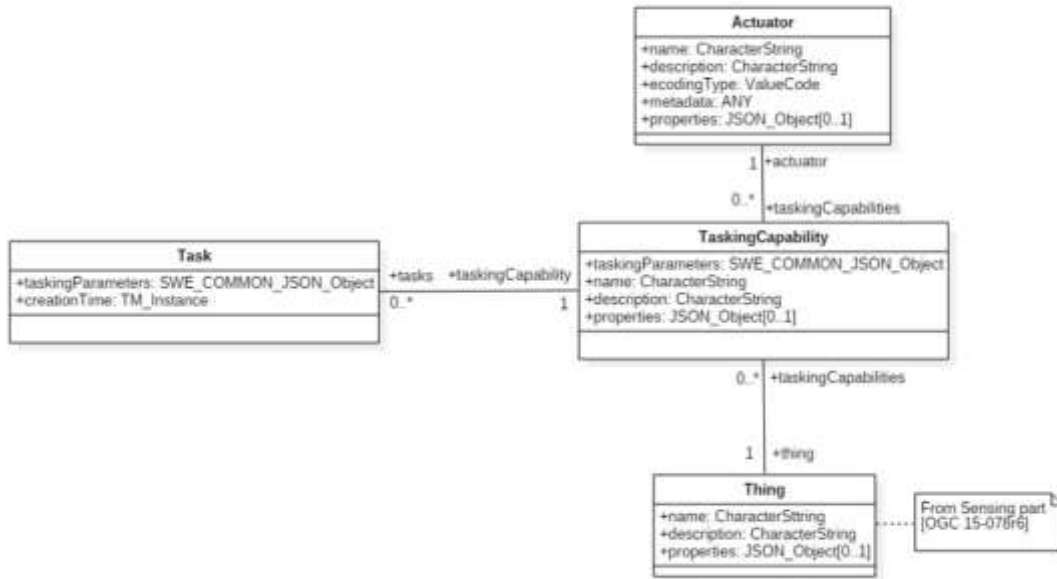


Figure 20. The SensorThings API Tasking data model. Source: OGC

ANNEX B. IoT Protocols

Narrowband-IoT

Narrowband IoT (NB-IoT) is a Low Power Wide Area Network Technology, developed by the 3rd Generation Partnership Project, released as a standard in 2016 with a maximum data rate of 85 kb/s. Narrowband IoT is a subset of the Long-Term Evolution (LTE) standard for wireless broadband communication of mobile devices, but limiting its operability to a single narrowband around 200kHz [48]. It relies on the cellular network, and hence trusted as mostly secure, however it doesn't have good coverage within tall buildings and is not deployed yet in all EU countries.

ZigBee

ZigBee is the most widely used and documented protocol for the creation of wireless personal area networks (WPANs) with small, low power digital radio frequency devices, such as those employed for home automation and medical data collection [49]. Zigbee builds on the physical layer, media access control and security protocol defined in the IEEE 802.15.4 standard for low-rate WPANs. ZigBee operates on industrial, scientific and medical (ISM) radio bands with frequencies varying according to local jurisdiction. Most commercial devices run over 2.4 GHz for home use, while data range between 20 Kbit/s for 868 MHz band and 250 Kbit/s for 2.4 GHz band. ZigBee is a well documented, standardized technology: drawbacks are its inadequacy in tall, multi-storey buildings, interference effects on Wi-Fi and Bluetooth standards running on the same frequencies and security delegated to a single device [50].

LoRa (LoRaWAN)

LoRa™ (Long Range) is a modulation technique that enables the long-range transfer of information with a low transfer rate [51]. It is a proprietary protocol for Low-Power Wide Area Networks (LPWAN) characterized by low power consumption and adaptive transmission rates. In realizing the vision of the Internet of Things (IoT), LPWA technologies complement and sometimes supersede the conventional cellular and short-range wireless technologies in performance for various emerging smart city and machine-to-machine (M2M) applications [52].

LoRa™ runs on ISM (Industrial, Scientific and Medical) radio bands with frequency depending on the region (868 MHz in Europe, 915 MHz in North America and 433 MHz in Asia), with a maximum data rate of 50 Kbps. LoRaWAN uses a proprietary spectrum modulation technique derived from the Chirp Spread Spectrum modulation (CSS) which allows to trade off data rate for sensitivity selecting the spread used. The technology allows for a high penetration in buildings, shared gateways to limit coverage problems, easy deployment. It does not present interference in the presence of WiFi and Bluetooth [53].

Thread

Thread is a low-power wireless mesh networking protocol, based on the universally-supported Internet Protocol (IP) version 6 (IPv6), and built using open and proven standards. Thread enables device-to-device and device-to-cloud communications and reliably connects hundreds (or thousands) of products and includes mandatory security features. According to the Thread Group Alliance, Thread networks have no single point of failure, can self-heal and reconfigure when a device is added or removed, and are simple to setup and use [54].

Thread is based on the broadly supported IEEE 802.15.4 radio standard (like ZigBee), which is designed from the ground up for extremely low power consumption and low latency.

Thread is developed by the Thread Group Alliance with a membership fee. The protocol is IP-addressable, with cloud access, and AES- encryption. Like ZigBee, the signal has a poor wall penetration and interference with Wi-Fi and Bluetooth frequencies.

DASH7 Alliance Protocol (D7A)

The DASH7 Alliance Protocol (D7A) is an Open Standard for bi-directional, sub-GHz (868 MHz in Europe) medium range wireless communication tailored for ultra lower sensor-actuator applications using private networks. D7A stems from ISO 18000-7 for Active RFID and operates in the sub-GHz ISM radio bands –ISO/IEC 18000-7 standard is used by the United States Army for logistic purposes. The protocol specification is free to use without any patent or licence requirements [55]. D7A fills the gap between the Short and the Large Area Networks, particularly in urban and industrial network installations, connecting actuators and messaging applications (sensors, alarms, states) with ranges up to 500 m.

D7A runs on a GFSK modulation scheme with data rate depending on the FSK modulation and frequency in the range 10-167 kb/s. It has a good penetration into buildings, low power consumption and no interference at WiFi and Bluetooth frequencies. D7A is applied on a tree (rather than mesh) network and hardware must be manually implemented. It has a poor market diffusion.

Sigfox

Sigfox is a proprietary lightweight IoT protocol for LPWAN, connecting low-power consumption devices over wide areas, therefore competing with LoRa. According to the company, Sigfox provides “*a software based communications solution, where all the network and computing complexity is managed in the Cloud, rather than on the devices. All that together, it drastically reduces energy consumption and costs of connected devices*” [56].

Sigfox uses unlicensed ISM radio bands with frequency depending on the region (868 MHz in Europe, 915 MHz in North America and 433 MHz in Asia –the same as LoRa). It operates on very narrow bandwidths, 100 Hz, with a maximum data rate of 100 bps. Sigfox deploys proprietary base stations connected to back end servers using an IP-based network. End devices connected to these base stations employ differential binary phase-shift keying (BPSK) modulation and Gaussian frequency shift keying (GFSK). Communication to and from base stations is bidirectional, but with a strong asymmetry in that data from base stations to end devices can only occur following uplink communication.

NFC (Near-Field Communication)

NFC has its origins in radio frequency identification (RFID) technology; any NFC-enabled device has a small chip that is activated when it comes in close proximity to another NFC chip (10 centimetres or less). NFC enables simple and safe two-way interactions between electronic devices [57]. There are two types of NFC devices: active and passive. Active NFC devices (e.g. smartphones) are capable of both sending and receiving information. Passive NFC devices can transmit information when read by active devices, but cannot read information themselves.

The benefits of NFC include easy connections, rapid transactions, and simple exchange of data. NFC serves as a complement to other popular wireless technologies such as Bluetooth, which has a wider range than NFC but which also consumes more power. Mobile wallets such as Apple Pay and Android Pay are the most visible use case of NFC technology. According to a 2017 survey, 17 % of U.S. consumers regularly use their smartphone to pay for transactions, with adoption over 50 percent in some emerging economies such as India and Thailand. In June 2017, Apple unlocked the iPhone’s NFC chip capabilities for uses other than Apple Pay, and Android devices have long had NFC access as well. With more than 2 billion NFC-enabled devices (and counting), use of the technology is expected to grow rapidly in the near future [57]. Due to its security level and connection behaviour (i.e. proximity, user initiation and security validation), NFC can address many of the challenges associated with IoT.

ANNEX C. Security of IoT Protocols

Security and privacy aspects are particularly important for the communication and transport protocols. The following paragraphs outlines some important featured implemented by the protocols and few shortcomings. Figure 2

Narrowband-IoT

Narrowband-IoT shares the security strengths of the LTE protocol; networking and security issues are delegated to the cellular network. Deployed devices may be vulnerable to signal jamming; other security considerations are up to the cellular network owners, which users are asked to trust. LTE security sets cryptographic algorithms for both confidentiality and integrity termed EPS Encryption Algorithms (EEA) and EPS Integrity Algorithms (EIA). Many keys in LTE are 256-bits long, even though in some current implementations only the 128 least significant bits are used. The UICC is the next-generation Subscriber Identity Module (SIM) card used in modern mobile devices and it represents the foundation of the LTE security architecture. The UICC hosts the Universal Subscriber Identity Module (USIM) application that performs the full range of security critical operations required by LTE cellular networks, such as authentication and other cryptographic functions. The UICC is a tamper resistant removable storage device that users can leverage to move their cellular service from one cellular device to another, while also providing the capability of storing contacts and other user data. From a security perspective, one of the most important functions of the UICC is cryptographic key and credential storage.

ZigBee

The ZigBee protocol manages security at different levels. At network level, the Coordinator initializes a ZigBee network and sets up either a distributed or a centralized security scenario. In the first case, routers may issue security keys to other routers and end devices; in the second case, the Coordinator acts as Trusted Centre, being the only device that can authenticate other devices and generate the network key. In both cases, the distribution of the network key requires devices to hold a preconfigured key used to encrypt the network key. In the distributed security case, the preconfigured link key is known by all devices; in the centralized one only by the Trusted Centre and joining devices. The network key is a 128 bit key used for all inter device communications which is shared among devices by the Coordinator; the link key is another 128-bit key used to encrypt the network key. At application level, ZigBee operates similarly to network level, once through the AES 128-bit scheme: it deploys a global link key and a unique link key at the application level, equivalent to the network-layer ones. The ZigBee security mechanism relies heavily on symmetric cryptography and on secure storage of keys at device level.

LoRa (LoRaWAN)

LoRAWAN frames are encrypted with AES-CCM, with a MIC (Market Identifier Code) code for integrity check (in conformity with the IEEE standard 802.15.4). Activation of end devices may proceed either via Over-The-Air-Activation (OTTA) or via Activation By Personalization (ABP). Each device has an associated IEEE-EUI64 identification code (DevEUI) at MAC layer and two pre-installed keys: the NwkKey and the AppKey. The AppKey is used only to sign (encrypt) the Join Message, composed of the DevEUI, NtwKey and the JoinEUI which identifies the remote server. The remote server receives the Join Message and replays to the device if the MIC is correct with a Join Accept message. The message contains a JoinNonce – a specific device unique counter value – and is incremented for each Join Accept sent to the device. The JoinNonce unique value is used by the device to derive the (four) session keys. The Join Accept message is accepted only if the MIC value is correct. Derivation of the session keys is obtained encrypting (128-bit encryption) the JoinNonce, the JoinEUI, the DevNonce and specific padding values for each derived key. In general, LoRaWAN requires secrecy at a tamper proof level in

all the devices. Any mismanagement on storage and production of the secret keys generates a weakness related to a bad protocol implementation and makes the network unsecure.

Thread

A Thread network typically originates from a selected Leader (usually a Border Router) that acts as a Commissioner for the first connected Router. All other devices are consequentially connected to the network. The basic network protection is provided by a 128-bit network wide key used in the MAC layer to protect the 802.15.4 MAC data frames. The key is encrypted via a Key-Exchange-Key and shared through DTLS in authentication phase. It is then used to encrypt messages with standard AES-CCM as in ZigBee. Network information and security data are required to be maintained into a non-volatile memory. The Thread authentication mechanism requires the presence of a Commissioner elected as authentication server and authorized for providing network credentials to the devices that want to join the network. Assuming a good implementation of the standard and cryptographic protocol, Thread implements security features that have been for years part of scientific research – such as elliptic curve cryptography and secure key exchange algorithm for IoT devices. Thread is a young protocol, released in 2015, when IoT security was already considered a major scientific topic.

Dash7

Dash7 relies as a unique security measure on a single 128-bit network wide key used in AES-CCM for both encryption and integrity of messages. Therefore, physically tampering the devices, i.e. the gateway, is possible with potential outcome of compromising the entire network. It is thus a good measure to add to the protocol extra physical protection measures. Although the original security assessment of Dash7 is weak, spoofing or other attempts to remotely intercept messages are made difficult by the specific PHY layer employed as it requires a quite cumbersome receiving antenna and by the asynchronous nature of the protocol itself. The relative low security assessment of this protocol is due to the intent to maintain a low power consumption of the devices and the fact that the protocol was adapted from a standard developed for RFID communications.

Sigfox

The Sigfox network connects end devices to one or several proprietary base stations operating on a LPWAN. Sigfox Ready devices operate on a limited number of messages per day (at most 140), with a short payload size (12 bits maximum) and at limited bitrate (100 bits/s). Upon reception by a base station, messages go through a preliminary check and are and are transmitted to the SigFox Core Network that proceeds to verification before delivering them to the application provider via a call back. In case of bidirectional communication, the Core Network builds the response authenticates it and evaluates the best base station to convey the answer. Message authentication proceeds via ensuring that the message has been generated by the device with the ID claimed in the message; checking that the ID is actually one authorized by the SigFox network. Devices are identified by a unique identifier ID code, while the matching of a message with the corresponding ID device is ensured by a Message Authentication Code (MAC). The MAC generation algorithm relies on a Network Authentication Key (NAK) which involves AES 128-bit cryptographic algorithm. Anti-reply security is achieved introducing a sequence number, SEQ, in the message which is stored by the SigFox core network. Major risks affecting a SigFox network concern: leak of device sensitive assets leading to a large number of devices compromised, the use of compromised devices to conduct denial of service attacks.

NFC

NFC security relies on three main features [58]. **Proximity:** NFC has a very small transmission zone, merely centimetres. This poses a challenge to thieves who would need to stand very close to the terminal in order to intercept the transaction. **User Initiation:** the user must initiate the transaction between their device and the NFC-enabled terminal, and usually provide secondary verification like a PIN code, fingerprint, or facial recognition in order to complete the transaction. **Secure element validation:** this is similar to the validation process for EMV (Europay, Mastercard, and Visa) chip cards.

After a connection is established between the NFC terminal and the customer's device or contactless card, the secure element chip within the device or card must validate the purchase. The transaction can only be complete after validation. Instead of transferring card data between the card/device and the reader, a unique digital signature is assigned to every payment.

ANNEX D. IoT Reference Framework Implementation Solutions

Amazon Web Services (AWS) IoT

“AWS has broad and deep IoT services, from the edge to the cloud” [59]. AWS IoT provides a platform where the sensor grids, connected vehicles, factory floors, and the similar things can be connected easily and securely to the cloud and other devices [60]. AWS IoT services target industry, consumers, and commerce; they include:

- Device services: to connect devices and operate them at the edge
 - Amazon FreeRTOS –an operating system for microcontrollers that makes small, low-power edge devices easy to program, deploy, secure, connect, and manage.
 - AWS IoT Greengrass –a software that lets you run local compute, messaging, data caching, sync, and machine learning inference capabilities on connected devices in a secure way.
- Connectivity & Control Services: to secure, control, and manage devices from the cloud
 - AWS IoT Core –to connect devices and securely interact with cloud applications and other devices.
 - AWS IoT Device Defender –to continuously monitor and audit IoT configurations.
 - AWS IoT Device Management –to securely register, organize, monitor, and remotely manage IoT devices at scale.
- Analytics Services: to work with IoT data and extract value from your IoT data
 - AWS IoT Analytics –to run sophisticated analytics on massive volumes of IoT data.
 - AWS IoT SiteWise –to collect, organize and analyse industrial data at scale.
 - AWS IoT Events –to detect and respond to events from large numbers of IoT sensors and applications.
 - AWS IoT Things Graph –to connect different devices and cloud services to build IoT applications.

Google IoT

Google IoT ecosystem takes as its technology cornerstone the Google Cloud Platform to combine a set of elements and build a robust, maintainable, end-to-end IoT solution on Cloud Platform. According to Google, these are the main elements [61]:

- Device management
 - Google Cloud IoT Core –to provide a fully managed service for managing devices. This includes registration, authentication, and authorization inside the Cloud Platform resource hierarchy as well as device metadata stored in the cloud, and the ability to send device configuration from the service to devices. Google Cloud IoT Core also provides a secure MQTT (Message Queue Telemetry Transport) broker, for devices managed by IoT Core, allowing devices to send real-time telemetry as well as immediately receive messages sent from cloud to device. The IoT Core MQTT broker directly connects with Cloud Pub/Sub.
 - Google Wave is a communication platform, as well as a command language, to work as a single protocol and manage all Google IoT devices from phones and Google Cloud. From its inception, Weave was conceived to transport ZigBee, Thread, Wi-Fi, Bluetooth, BLE,

Ethernet, LoRaWAN and numerous other protocols. An essential principle of Weave is that all Google cloud devices and users can integrate in one common ecosystem [62].

- Pipeline processing tasks
 - Google Cloud Dataflow –to provide the open Apache Beam programming model as a managed service for processing data in multiple ways, including batch operations, extract-transform-load (ETL) patterns, and continuous, streaming computation. Cloud Dataflow can be particularly useful for managing the high-volume data processing pipelines required for IoT scenarios.
- Data Storage
 - Cloud Datastore and Firebase Realtime Database –to store processed or raw data in structured but schemaless databases and make state or telemetry data available to mobile or web apps.
- Rule processing and streaming analytics
 - Google Cloud Functions –to write custom logic that can be applied to each event as it arrives. This can be used to trigger alerts, filter invalid data, or invoke other APIs.
 - Cloud Dataflow –to process data and events with more sophisticated analytics, including time windowing techniques or converging data from multiple streams.
- Analytics
 - Google BigQuery –to provide a fully managed data warehouse with a familiar SQL interface.
 - Cloud Datalab –to explore, analyse, and visualise large-scale data.
 - Tensorflow and Cloud Machine Learning Engine –to extract insights from IoT data that is inherently multi-dimensional and noisy by nature.

Apple HomeKit

iOS and iCloud are the technology cornerstone of Apple IoT ecosystem. The **Apple HomeKit** allows users to communicate with and control connected accessories in their home using the **Apple Home app**. HomeKit framework can provide a way to configure accessories (**iOS devices**) and create actions to control them. Users can even group actions together and trigger them using Siri [63]. **Apple HomePod** automatically sets itself up as a home hub able to control HomeKit accessories remotely with the Home app and create home automations. Apple TV and iPad can be setup to become a home hub, too.

HomeKit ADK is used by silicon vendors and accessory manufacturers to build HomeKit compatible devices. HomeKit ADK implements key components of the HomeKit Accessory Protocol (**HAP**), which embodies the core principles Apple brings to smart home technology: security, privacy, and reliability. HomeKit Open Source ADK is an open-source version of the HomeKit Accessory Development Kit. It can be used by any developer to prototype non-commercial smart home accessories. For commercial accessories, accessory developers must continue to use the commercial version of the HomeKit ADK available through the MFi Program [64].

Samsung SmartThings

Samsung SmartThings ecosystem has as technology cornerstones **Samsung ARTIK™ IoT Platform**, **SmartThings Cloud**, and Tizen 4.0. “Samsung ARTIK™ IoT Platform with SmartThings Cloud provides production-ready hardware, software and tools, together with integrated cloud services to enable companies to quickly develop secure IoT products and services” [65]. Tizen 4.0 is a Linux-based mobile operating system backed by the Linux Foundation. Tizen is not fully open source software and portions

of the OS are licensed under the Flora License, a derivative of the Apache License 2.0 that only grants a patent license to "Tizen certified platforms".

The **Samsung SmartThings app** allows to access SmartThings features across a family of Samsung products, including smart phones, TVs, and fridges [66].

The **SmartThings IDE** (Integrated Development Environment) provides SmartThings developers with a set of tools to manage their SmartThings account, and build and publish custom SmartApps and Device Handlers [67].

IBM Watson IoT Platform

"IBM Watson IoT Platform ingests device data and transforms that data into meaningful insights – which can optimize processes and guide new product design" [68].

The IBM ecosystem is based on the following keystone technologies: **IBM Cloud**, the **IBM Watson IoT platform**, and **IBM Watson Studio** (formerly IBM Data Science Experience).

The platform allows to implement the following process: (a) connect, manage and secure devices; (b) capture, process, and store IoT data to transform it into valuable assets; (c) explore, visualize, and gain insight with AI driven analytics; (d) share and track with Blockchain Ledger.

Bosh IoT Platform

The Bosch IoT Suite (already been integrated in millions of devices and counting) is the basis on which Bosch, its customers, and its partners can build a broad range of IoT solutions, services, and projects [69]. It incorporates the Bosch Group's industry know-how and is available across all industries, such as agriculture, energy, homes & buildings, retail, mobility, and manufacturing. Bosh IoT Platform provides a set of (cloud) services for:

- Device connectivity;
- Digital twins;
- Device management;
- Software provisioning;
- Data management and analytics;
- User and permissions management.

Azure Digital Twins

Azure Digital Twins is an IoT service that helps users to create comprehensive models of physical environments. This platform creates spatial intelligence graphs to model the relationships and interactions between people, places, and devices. It supports data queries addressing a physical space, rather than disparate sensors. The platform promises to build reusable, highly scalable, spatially aware experiences that link streaming data across the physical and digital world [70].

Open sources solutions/platforms

Open source solutions IoT platforms include [71]:

- **Eclipse:** it has over 40 open-source projects that are designed for the various IoT stacks);
- **Thingier.io:** a platform supporting multiple protocols, sensors and actuators. It is hardware agnostic and offers a highly interactive, rich interface for coding. It is possible to download the Thingier.io infrastructure in AWS, Ubuntu and Raspberry Pi;
- **OpenIoT:** a free IoT middleware system. It allows developers to connect different sensors and cloud networks useful for the development;
- **ThingSpeak:** an open IoT platform supporting a variety of connected applications.

- **Mozilla WebThings** (see section 6.2).

ANNEX E. W3C WoT: Web Thing specification

According to W3C, a Thing (or Web Thing) is “an abstraction of a physical or a virtual entity whose metadata and interfaces are described by a WoT Thing Description, whereas a virtual entity is the composition of one or more Things” [2]. A Web Thing is characterized by four architectural aspects – as depicted in Figure 21.

- behaviour;
- Interaction Affordances;
- security configuration;
- Protocol Bindings

A central aspect in W3C WoT vision is the provision of machine-understandable metadata: WoT Thing Description (TD). Ideally, such metadata is self-descriptive, so that Consumers are able to identify what capabilities a Thing provides and how to use the provided capabilities. A TD describes Thing instances with general metadata such as name, ID, descriptions, and also can provide relation metadata through links to related Things or other documents. TDs also contain Interaction Affordance metadata; Public Security Metadata; and communications metadata defining Protocol Bindings. The TD can be seen as the index.html for Things, as it provides the entry point to learn about the provided services and related resources, both of which are described using hypermedia controls [2].

The Interaction Affordances provide a model of how Consumers can interact with the Thing through abstract operations, but without reference to a specific network protocol or data encoding. An example for this is “a door with a handle. The door handle is an affordance, which suggests that the door can be opened. For humans, a door handle usually also suggests how the door can be opened; an American knob suggests twisting, a European lever handle suggests pressing down” [2].

The protocol binding adds the additional detail needed to map each Interaction Affordance to concrete messages of a certain protocol. In general, different concrete protocols may be used to support different subsets of Interaction Affordances, even within a single Thing.

The security configuration aspect of a Thing represents the mechanisms used to control access to the Interaction Affordances and the management of related *Public Security Metadata* and *Private Security Data*.

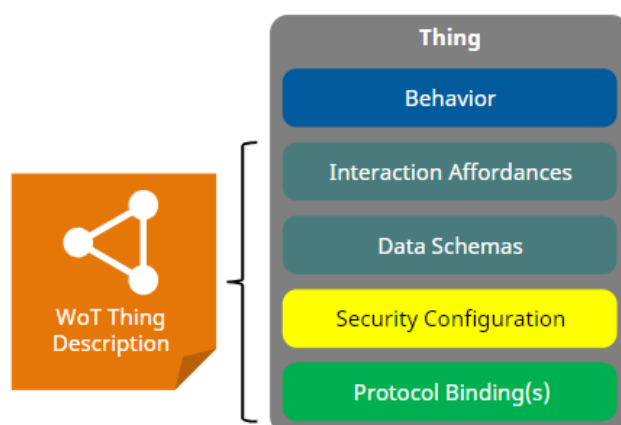


Figure 21. Web Thing architectural aspects. Source [2].

WoT Abstract Architecture

The WoT abstract architecture is depicted in Figure 22. Referring to the IoT ecosystem reference framework (see Figure 3), three different layers are recognised:

- The local network (local layer)
- The edge (gateway layer)
- The cloud (data and computing layer)

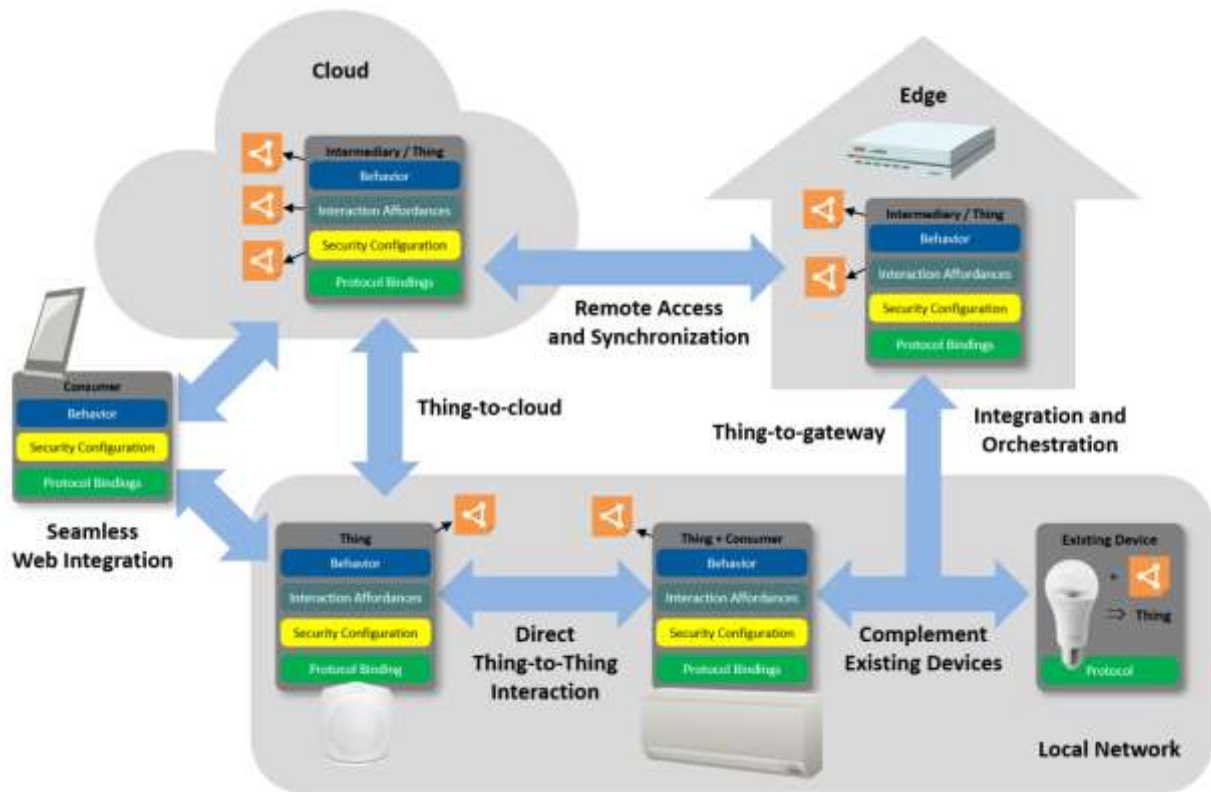


Figure 22. Abstract architecture of W3C WoT. Source [2].

WoT Building Blocks

WoT building blocks allow the implementation of systems that conform with the abstract WoT Architecture. A WoT building block is depicted in Figure 23. In this figure the WoT building blocks are highlighted with black outlines. This is an abstract view and does not represent any particular implementation; instead it illustrates the relationship between the building blocks and the main architectural aspects of a Thing.

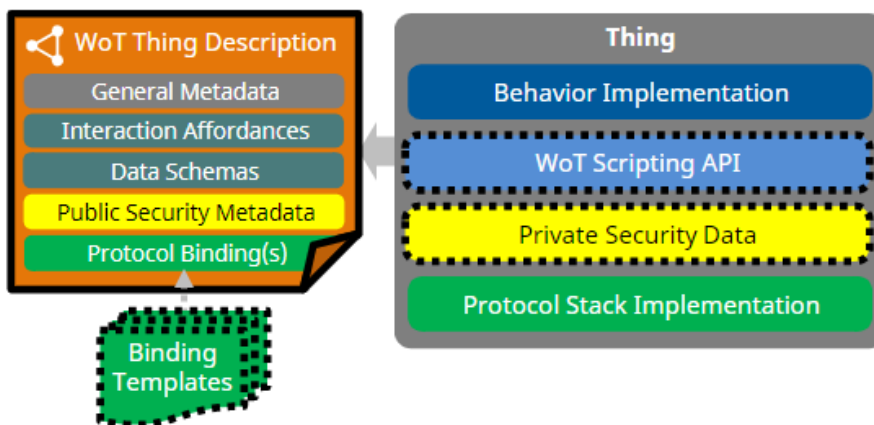


Figure 23. WoT Building Blocks and their relationship with WoT Thing aspects. Source [2]

ANNEX F. Data Mining Queries

The keywords and Boolean operators used for mining the utilized data sources are listed below. It is noteworthy that, in some case, the possibility to combine, exclude or apply similarity search has been exploited.

- (i) Industry 4.0: (IoT OR Internet of Things) AND (industry 4.0 OR industrial process OR smart manufacturing)
- (ii) Smart home: (IoT OR Internet of Things) AND (smart home OR smart building OR building automation)
- (iii) Smart city: (IoT OR Internet of Things) AND (smart city)

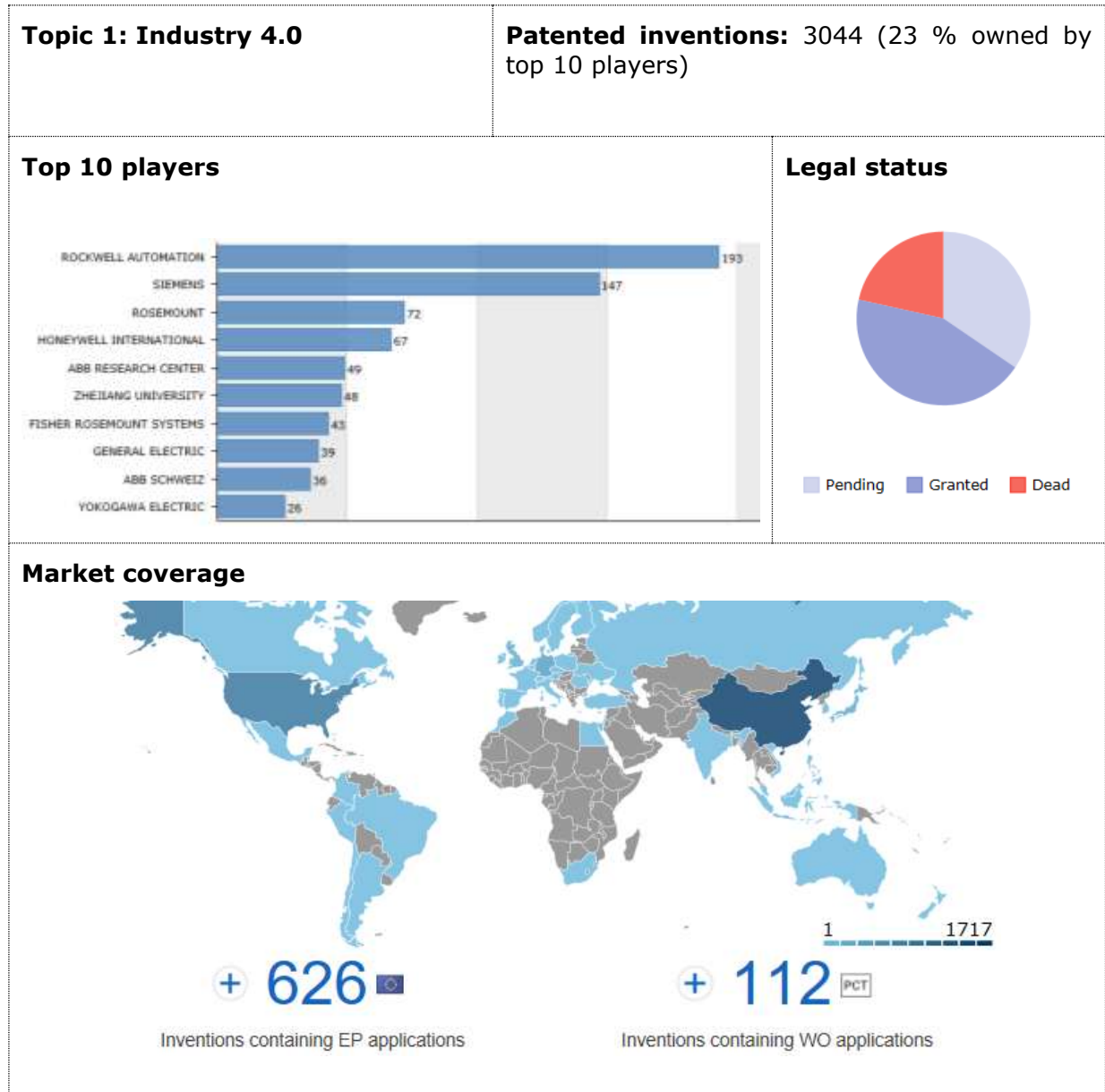
The searches on Smart home and Smart city have been executed so to exclude from smart home all records connected to smart city services.

- (iv) Smart grid – large scale: (IoT OR Internet of Things) AND (power plant OR power distribution OR power monitoring OR electric power)
- (v) Smart grid – small scale: (IoT OR Internet of Things) AND (smart grid OR intelligent grid)
- (vi) Renewable energy: (IoT OR Internet of Things) AND (renewable energy OR PV OR wind OR solar energy)
- (vii) Food chain: (IoT OR Internet of Things) AND (food OR food production OR food management OR food safety)
- (viii) Health: (IoT OR Internet of Things) AND (health OR healthcare OR medical)
- (ix) Military: (IoT OR Internet of Things) AND (defence OR military)

ANNEX G. Figures characterizing the different IoT Domains

Industry 4.0

Patents



Key actors



Spatial distribution



Author keywords

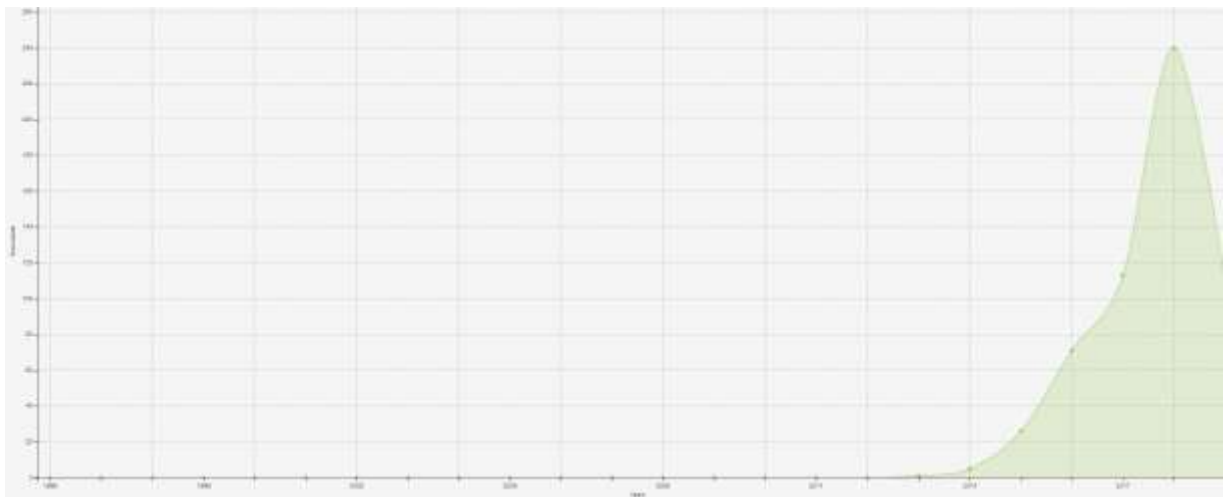
Cyber physical

Occurrence

98

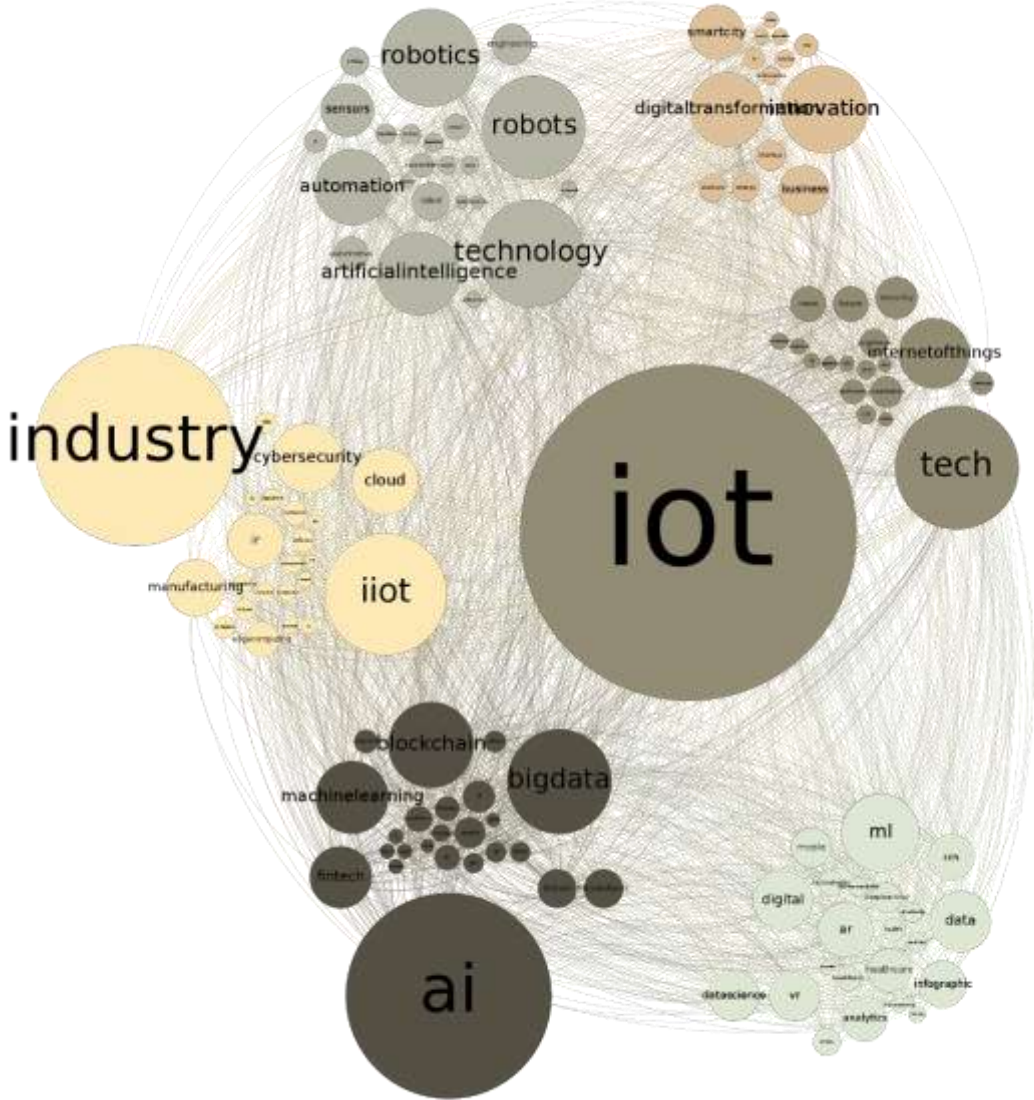
| | |
|-------------------------------|----|
| Smart manufacturing | 64 |
| Industrial Internet of Things | 56 |
| Big data | 43 |
| Smart factory | 43 |
| Manufacturing | 24 |
| Cloud computing | 24 |
| Digitization | 13 |
| Security | 13 |
| Artificial intelligence | 13 |

Temporal distribution



Investments

Data were not available at the time of the investigation.



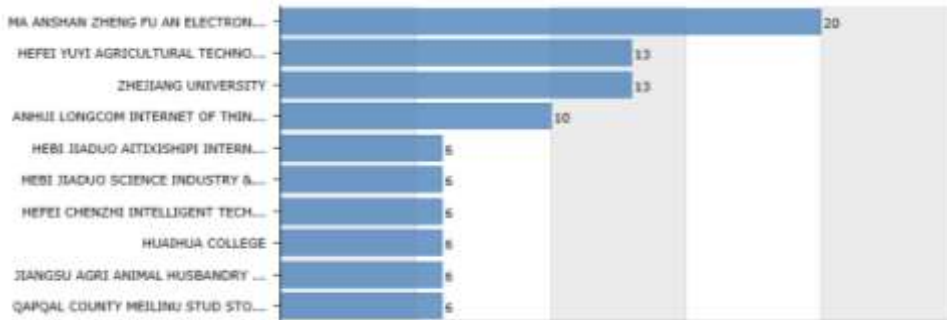
Agriculture

Patents

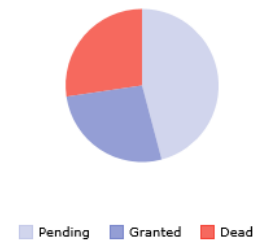
Topic 2: Agriculture and IoT

Patented inventions: 922 (8 % owned by top 10 players)

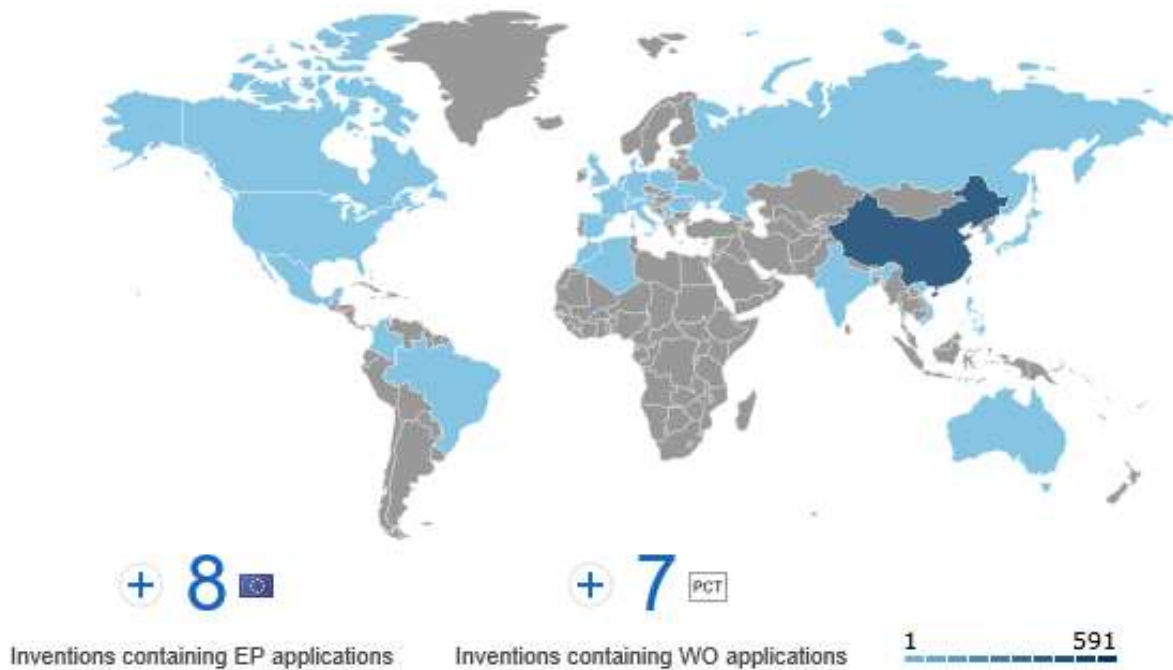
Top 10 players



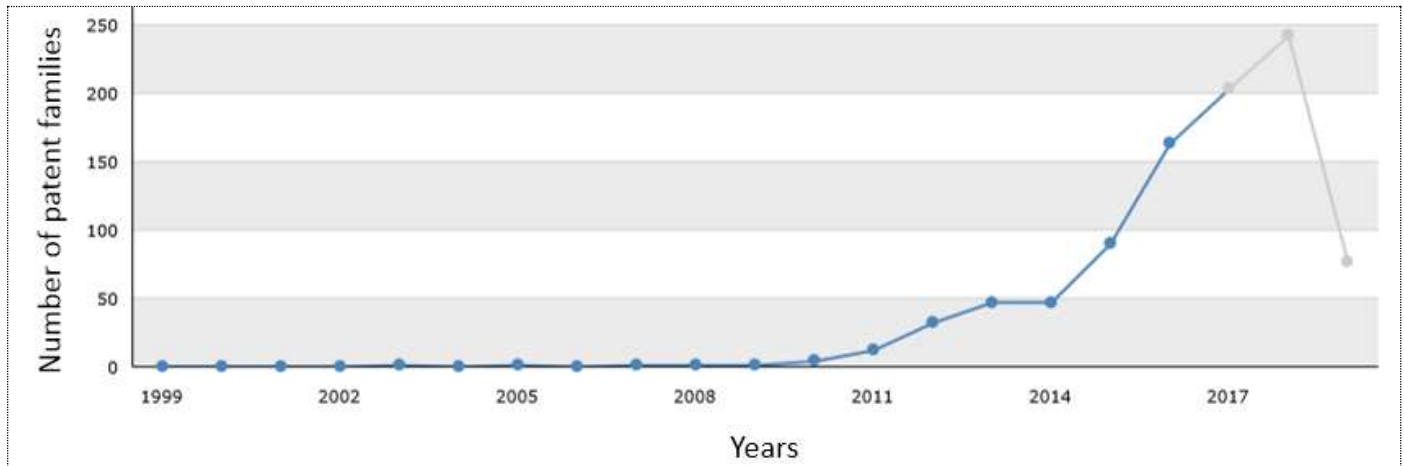
Legal status



Market coverage



Temporal distribution



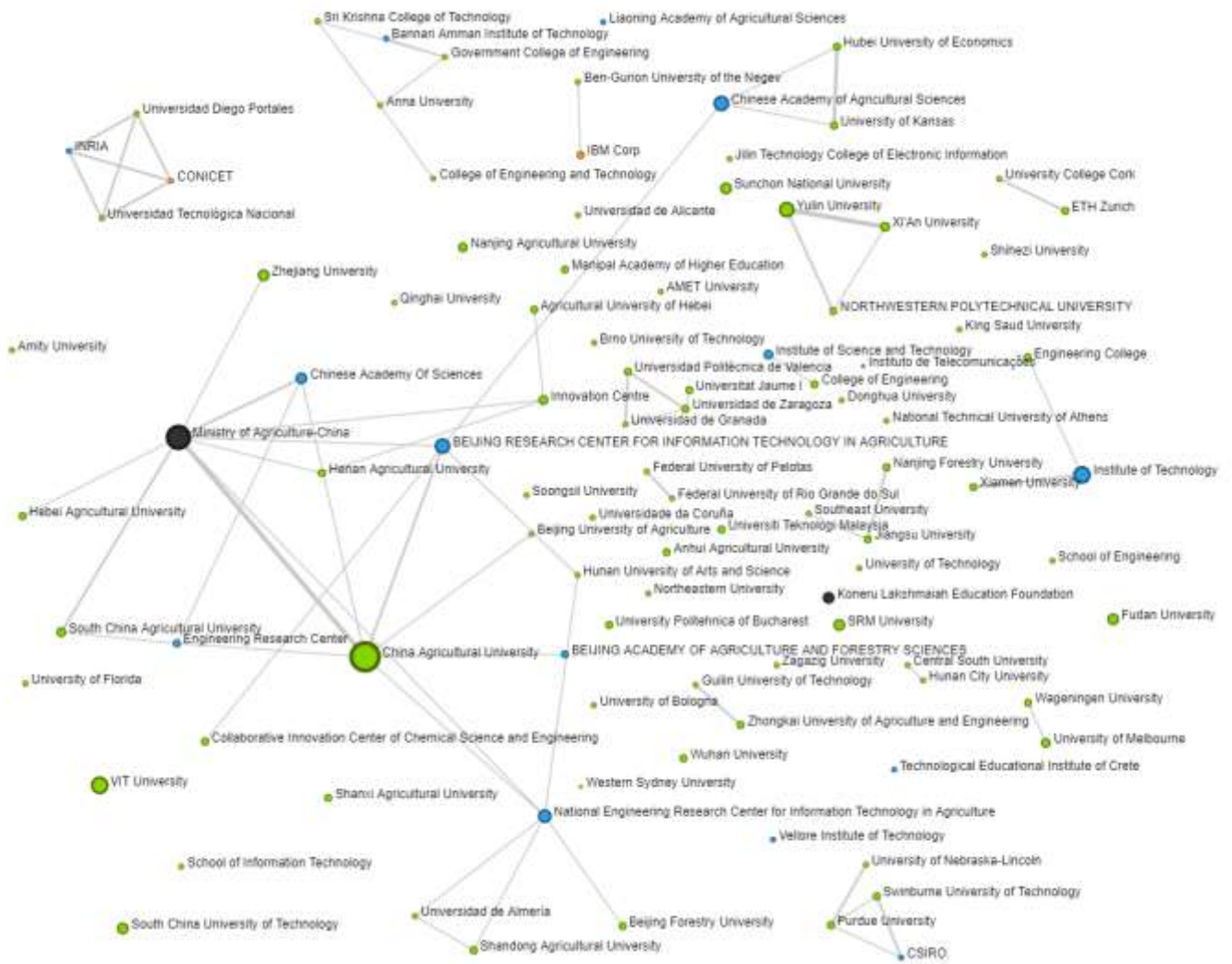
Technologies and applications



Scientific publications

| | |
|-------------------------------------|-----------------------------------|
| Topic 2: Agriculture and IoT | Number of articles: 442 |
|-------------------------------------|-----------------------------------|

Key actors

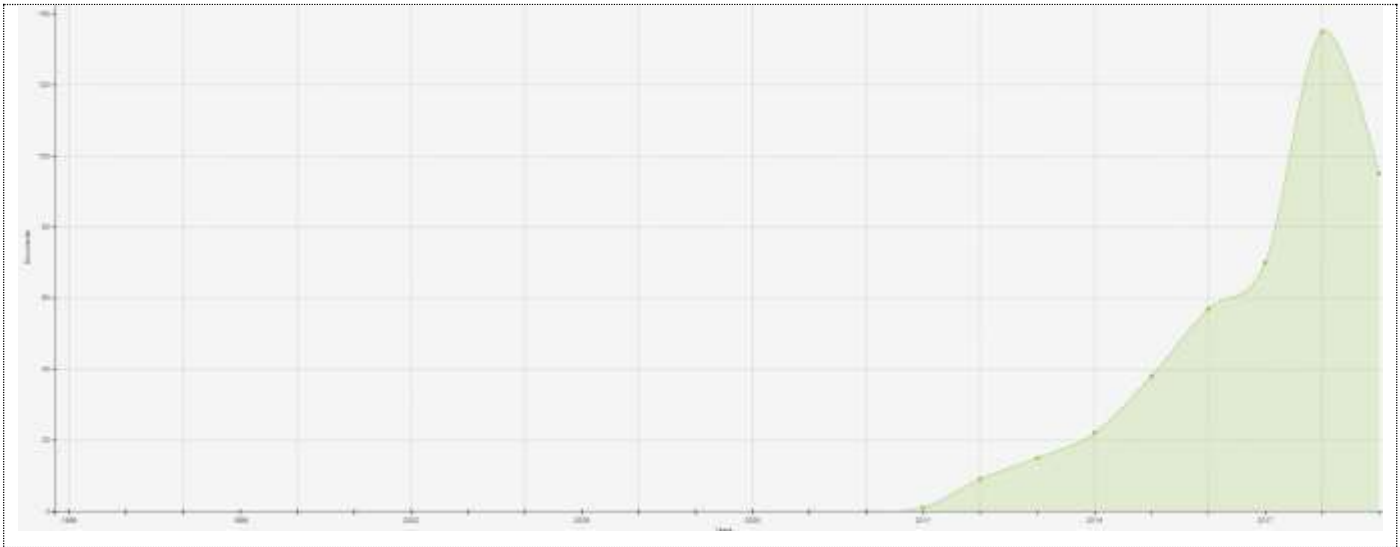


Spatial distribution



| Author keywords | Occurrence |
|--------------------------------|-------------------|
| Precision agriculture | 51 |
| Wireless sensor network | 46 |
| Cloud computing | 27 |
| Smart agriculture | 24 |
| Agricultural production | 23 |
| Smart farms | 21 |
| Big data | 19 |
| Supply chain | 13 |
| Soil moisture | 12 |
| RFID | 11 |

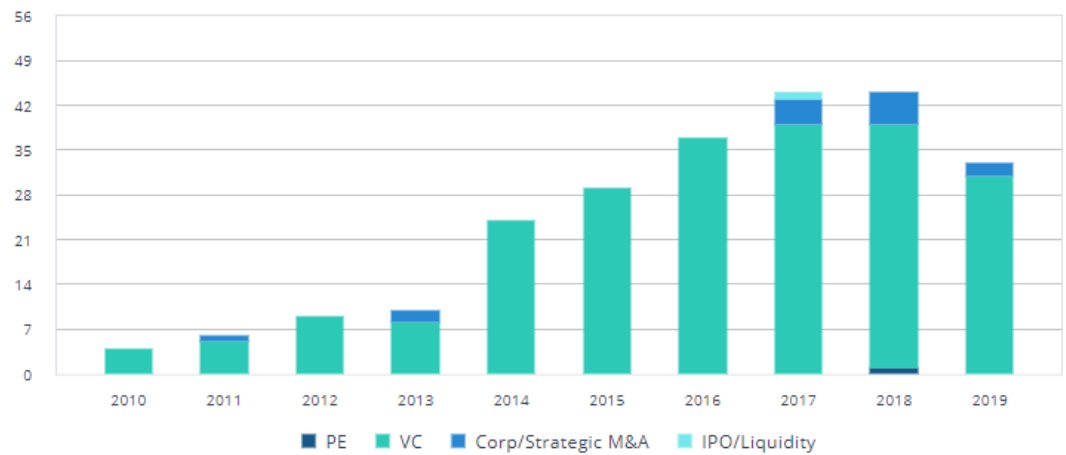
Temporal distribution



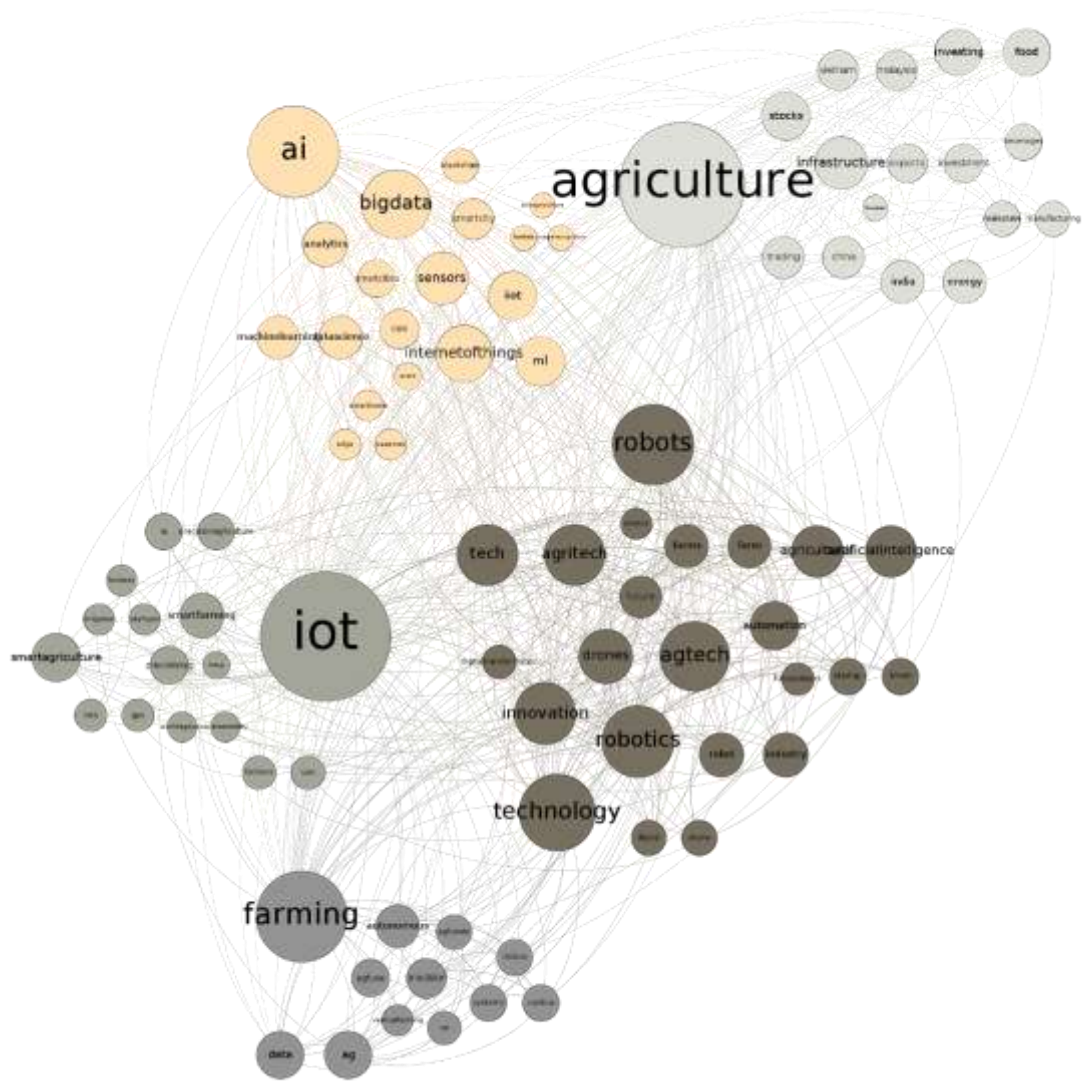
Investment

| | | | | |
|----------------|------------|----------------|-----------|-------------------------|
| Companies: 122 | Deals: 482 | Investors: 608 | Exits: 19 | Largest deal: 815,62M € |
|----------------|------------|----------------|-----------|-------------------------|

Investment over time

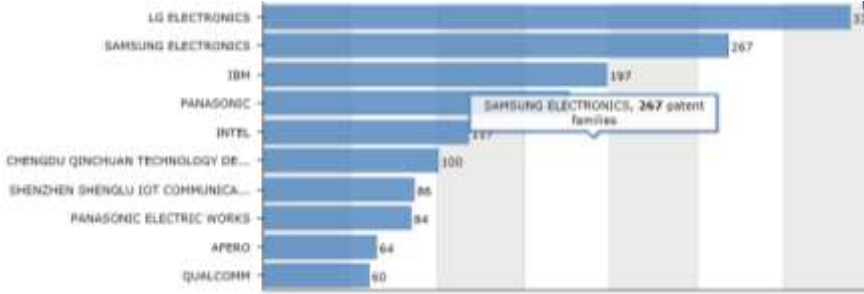






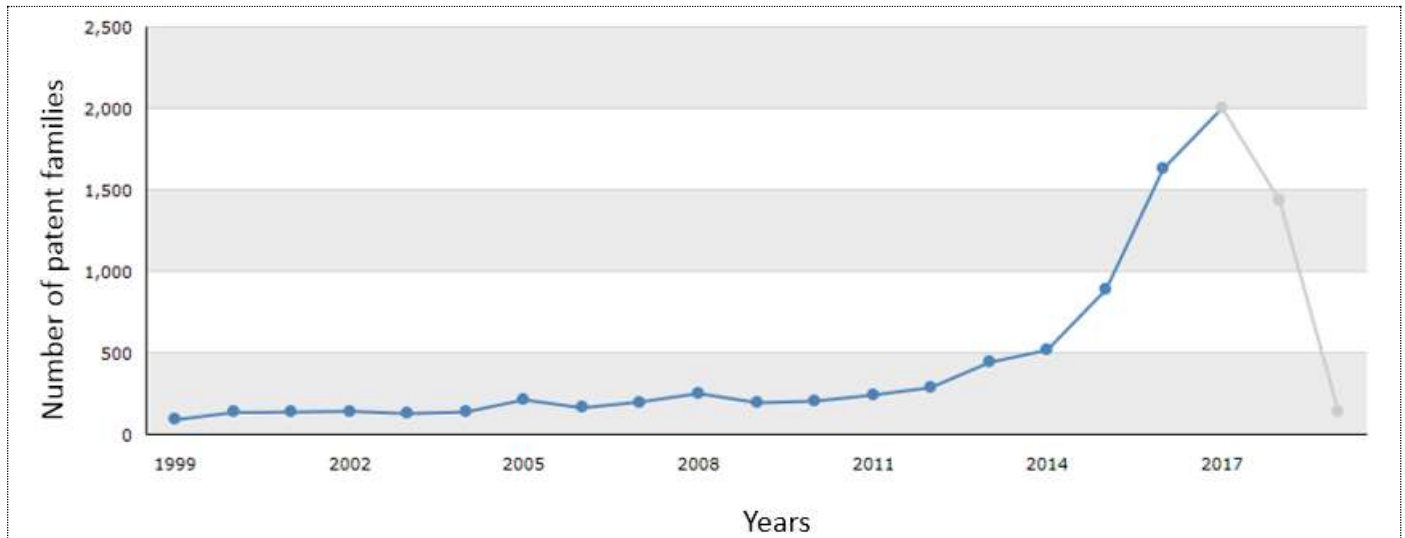
Twitter Analysis



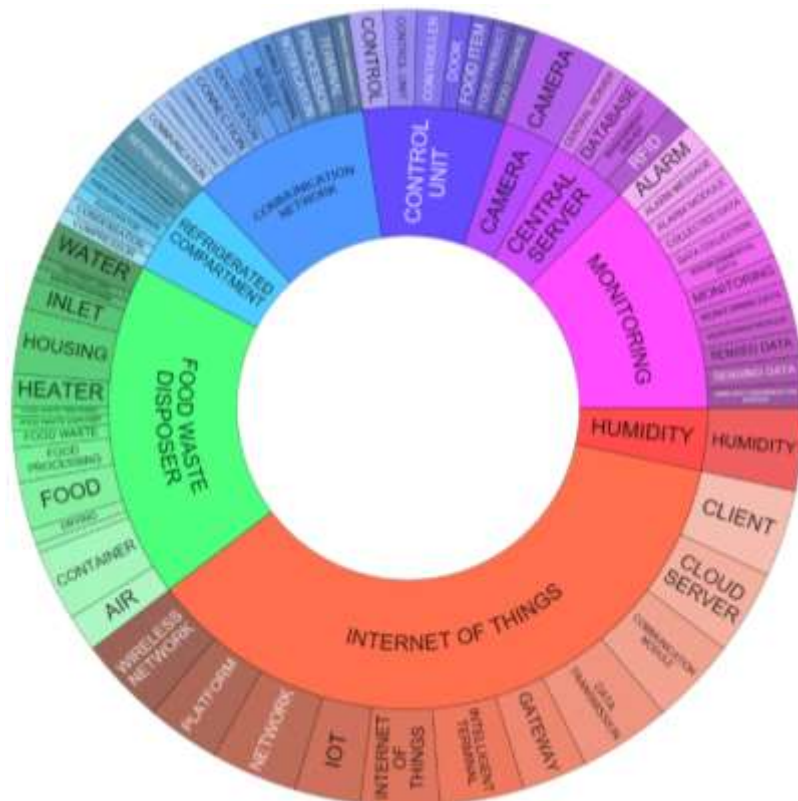
Food chain

Patents

| Topic 3: Food chain | Patented inventions: 10000 (19 % owned by top 10 players) | | | | | | | | | | | | | | | | | | | | | | |
|---|---|-----------------|----------------|-----|---------------------|-----|-----|-----|-----------|-----|-------|-----|-----------------------------------|----|-----------------------------------|----|--------------------------|----|-------|----|----------|----|---|
| Top 10 players  <table border="1"><thead><tr><th>Company</th><th>Patent Families</th></tr></thead><tbody><tr><td>LG ELECTRONICS</td><td>333</td></tr><tr><td>SAMSUNG ELECTRONICS</td><td>267</td></tr><tr><td>IBH</td><td>197</td></tr><tr><td>PANASONIC</td><td>177</td></tr><tr><td>INTEL</td><td>100</td></tr><tr><td>CHENGDU QINCHUAN TECHNOLOGY DE...</td><td>86</td></tr><tr><td>SHENZHEN SHENGLU IOT COMMUNICA...</td><td>84</td></tr><tr><td>PANASONIC ELECTRIC WORKS</td><td>64</td></tr><tr><td>AFERO</td><td>64</td></tr><tr><td>QUALCOMM</td><td>60</td></tr></tbody></table> | Company | Patent Families | LG ELECTRONICS | 333 | SAMSUNG ELECTRONICS | 267 | IBH | 197 | PANASONIC | 177 | INTEL | 100 | CHENGDU QINCHUAN TECHNOLOGY DE... | 86 | SHENZHEN SHENGLU IOT COMMUNICA... | 84 | PANASONIC ELECTRIC WORKS | 64 | AFERO | 64 | QUALCOMM | 60 | Legal status  <p>■ Pending ■ Granted ■ Dead</p> |
| Company | Patent Families | | | | | | | | | | | | | | | | | | | | | | |
| LG ELECTRONICS | 333 | | | | | | | | | | | | | | | | | | | | | | |
| SAMSUNG ELECTRONICS | 267 | | | | | | | | | | | | | | | | | | | | | | |
| IBH | 197 | | | | | | | | | | | | | | | | | | | | | | |
| PANASONIC | 177 | | | | | | | | | | | | | | | | | | | | | | |
| INTEL | 100 | | | | | | | | | | | | | | | | | | | | | | |
| CHENGDU QINCHUAN TECHNOLOGY DE... | 86 | | | | | | | | | | | | | | | | | | | | | | |
| SHENZHEN SHENGLU IOT COMMUNICA... | 84 | | | | | | | | | | | | | | | | | | | | | | |
| PANASONIC ELECTRIC WORKS | 64 | | | | | | | | | | | | | | | | | | | | | | |
| AFERO | 64 | | | | | | | | | | | | | | | | | | | | | | |
| QUALCOMM | 60 | | | | | | | | | | | | | | | | | | | | | | |
| Market coverage  <p>+ 1210  Inventions containing EP applications</p> <p>+ 527  Inventions containing WO applications</p> <p>1 ————— 3958</p> | | | | | | | | | | | | | | | | | | | | | | | |
| Temporal distribution | | | | | | | | | | | | | | | | | | | | | | | |



Technologies and applications



Scientific publications

| | |
|----------------------------|-----------------------------------|
| Topic 3: Food chain | Number of articles: 194 |
| Key actors | |



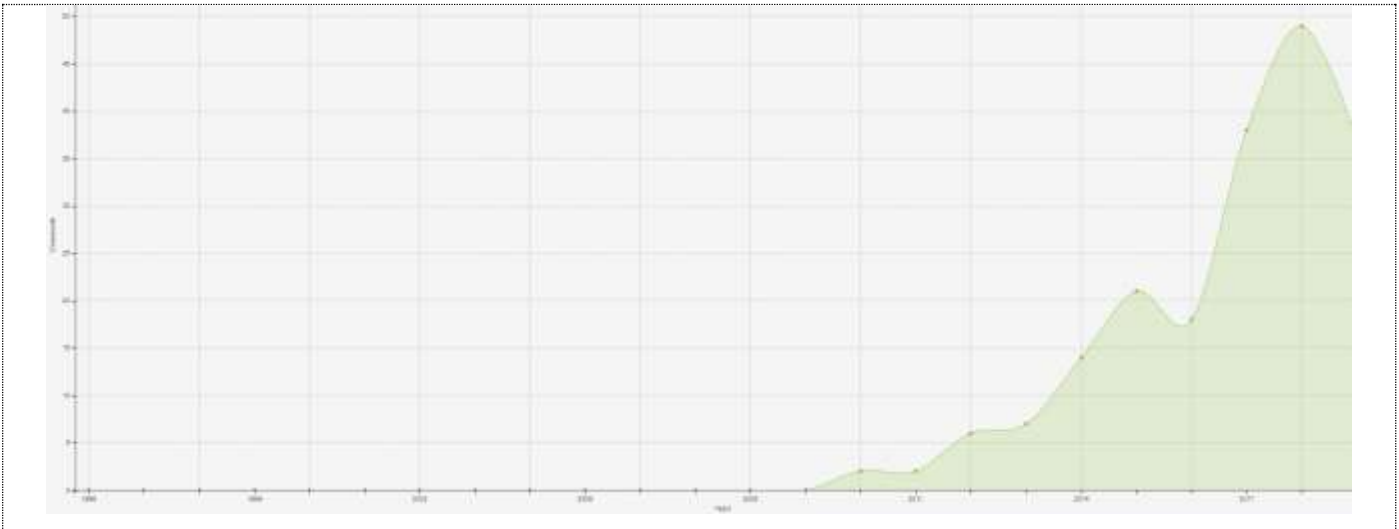
Spatial distribution



Frequently occurring terms

| Author keywords | Occurrence |
|-------------------------------|------------|
| Supply chain | 15 |
| Foods | 12 |
| Food supply chain | 11 |
| Food safety | 10 |
| Traceability | 10 |
| Wireless sensor network (WSN) | 9 |
| Agriculture | 9 |
| RFID | 8 |
| Radio frequency | 8 |
| Agricultural production | 7 |

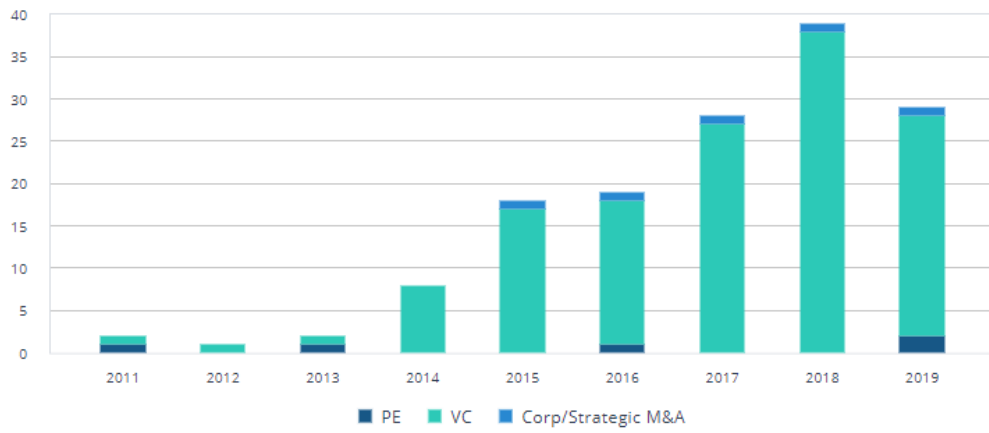
Temporal distribution



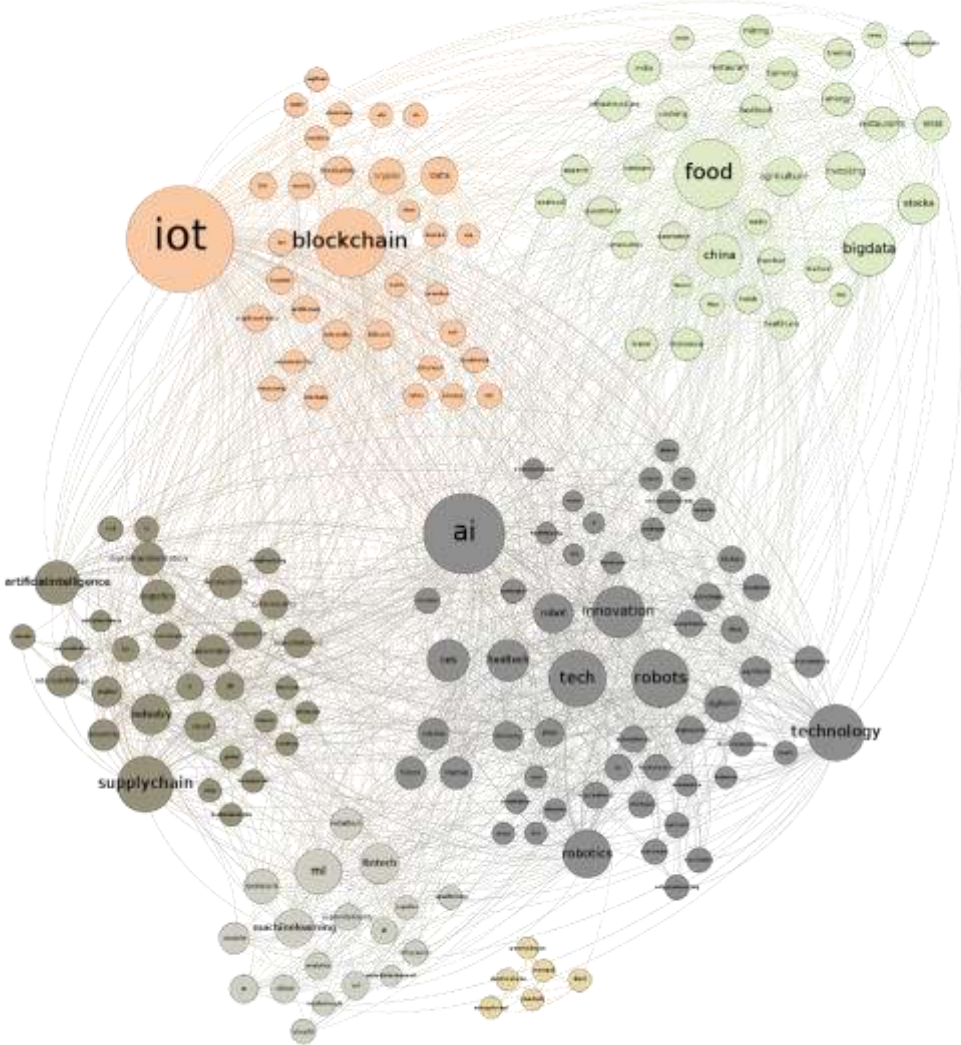
Investments

| | | | | |
|---------------|------------|----------------|-----------|-------------------------|
| Companies: 95 | Deals: 293 | Investors: 427 | Exits: 12 | Largest deal: 326,78M € |
|---------------|------------|----------------|-----------|-------------------------|

Investment over time

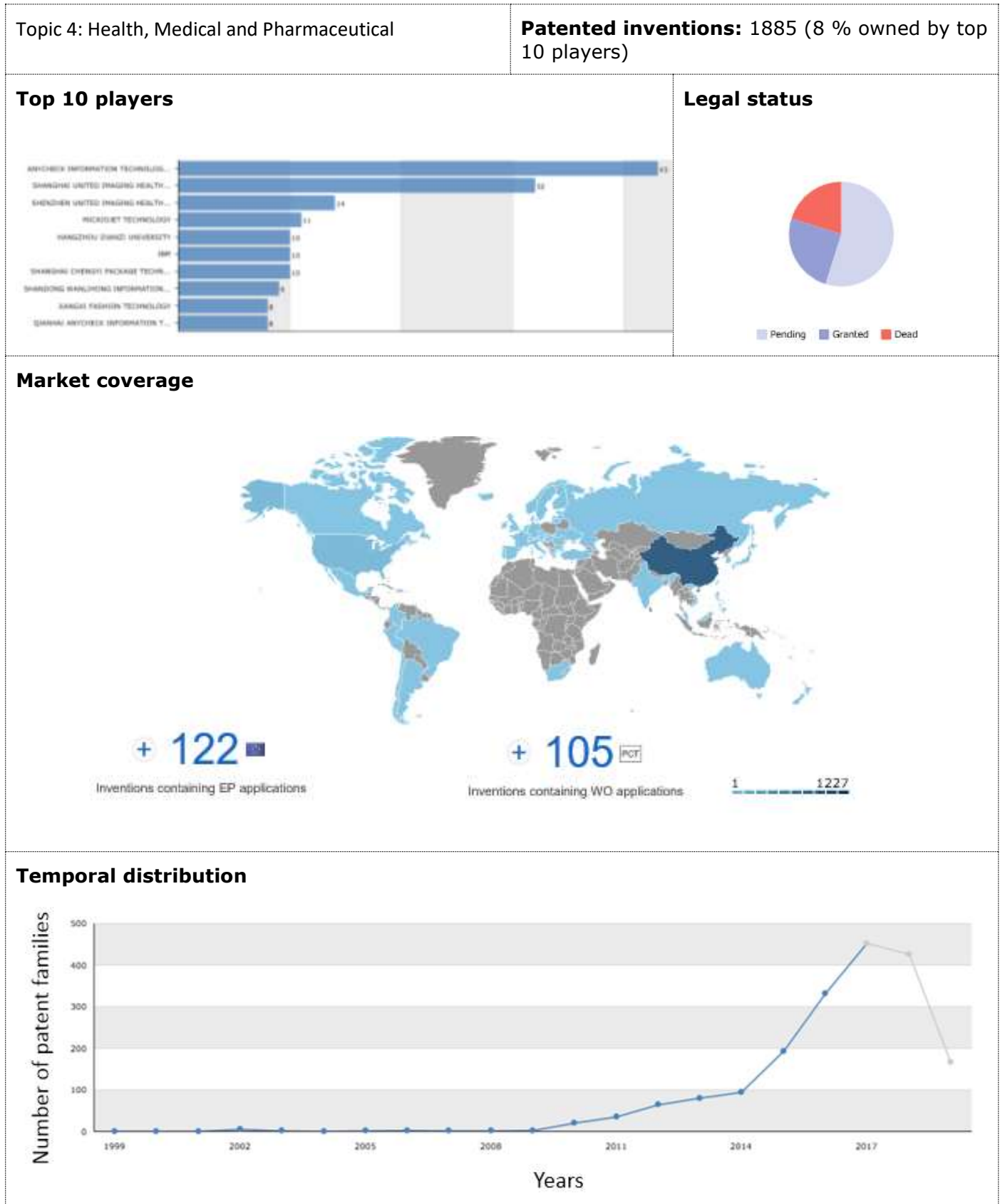


Twitter analysis



Health, Medical and Pharmaceutical

Patents

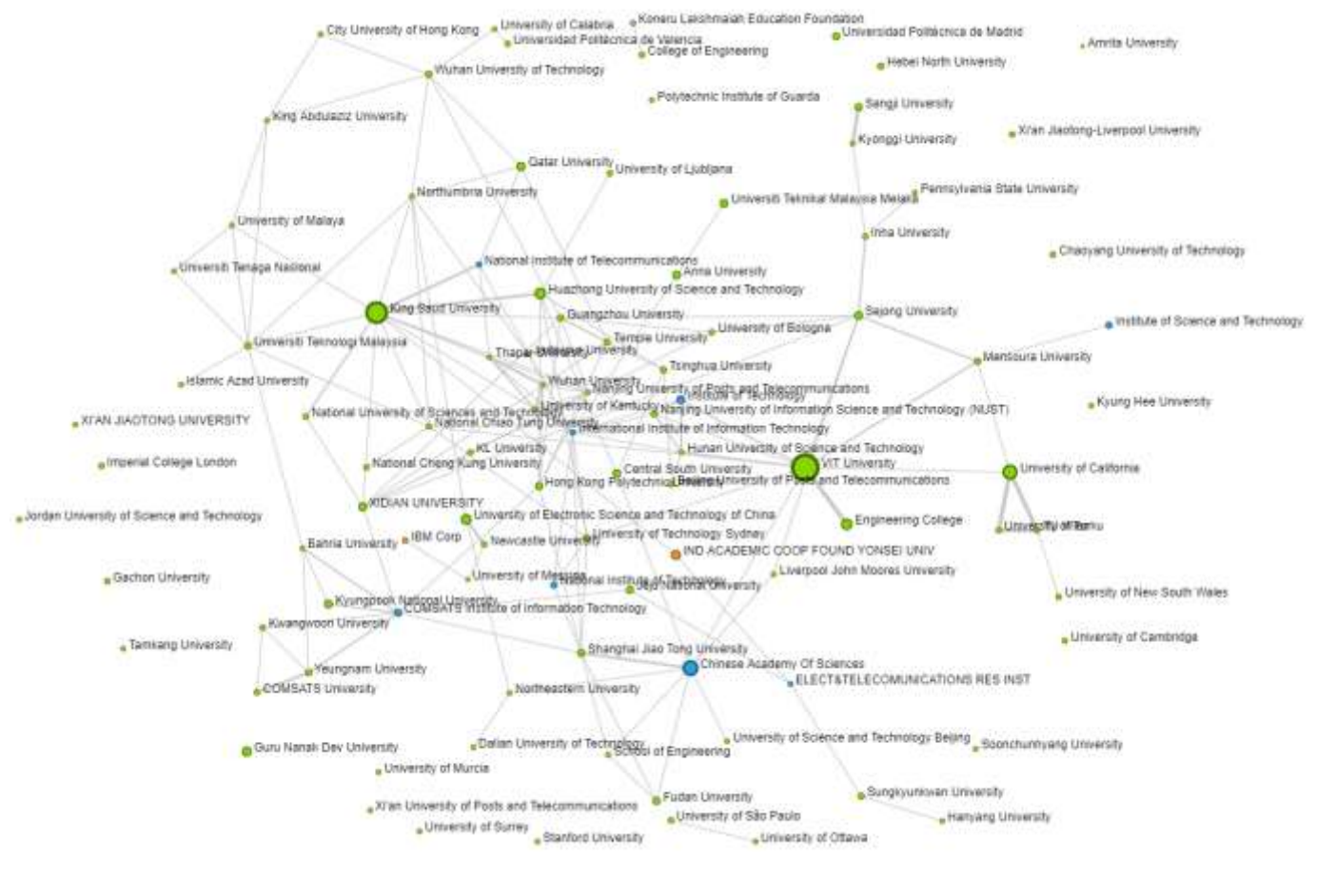


Scientific publications

Topic 4: Health, Medical and Pharmaceutical

Number of articles: 1446

Key actors

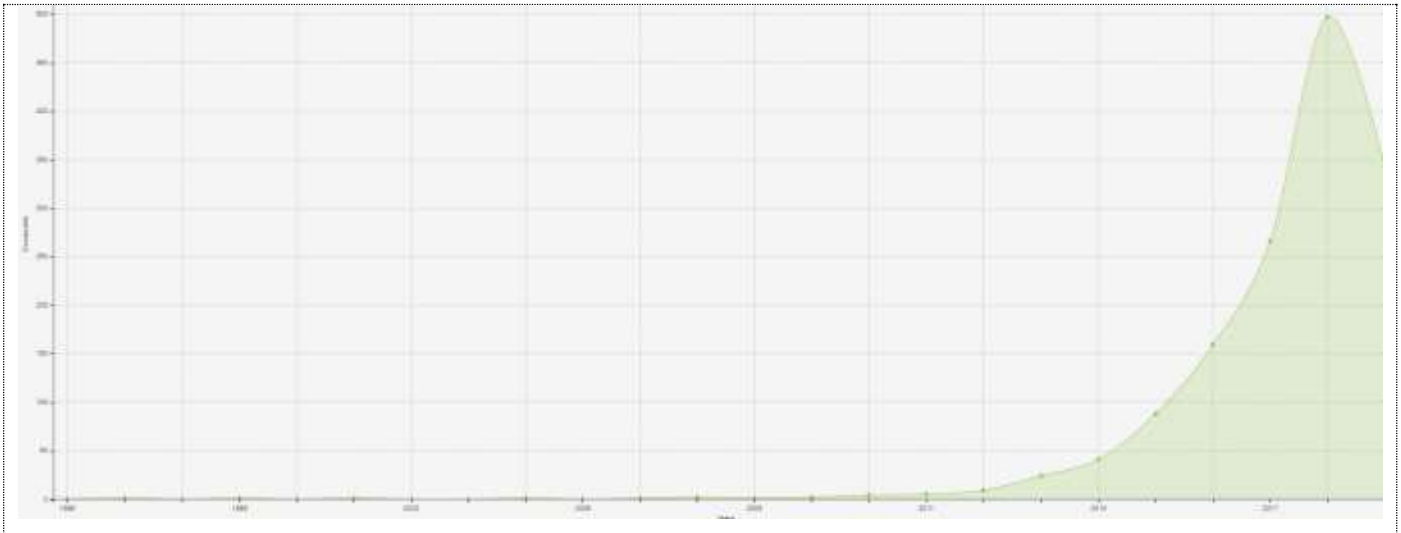


Spatial distribution



| Author keywords | Occurrence |
|--------------------------------------|-------------------|
| Big data | 83 |
| Cloud computing | 78 |
| Security | 73 |
| E health | 63 |
| Wireless sensor network (WSN) | 60 |
| Health care | 43 |
| Privacy | 37 |
| Machine learning | 36 |
| Health monitoring | 34 |
| Smart city | 29 |

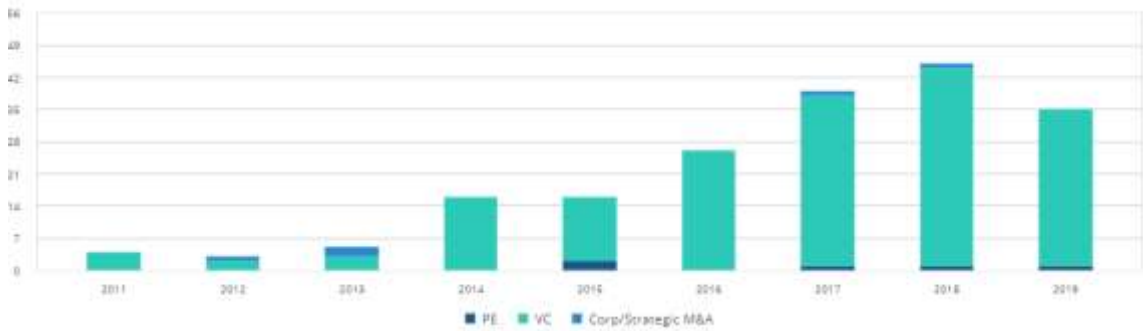
Temporal distribution



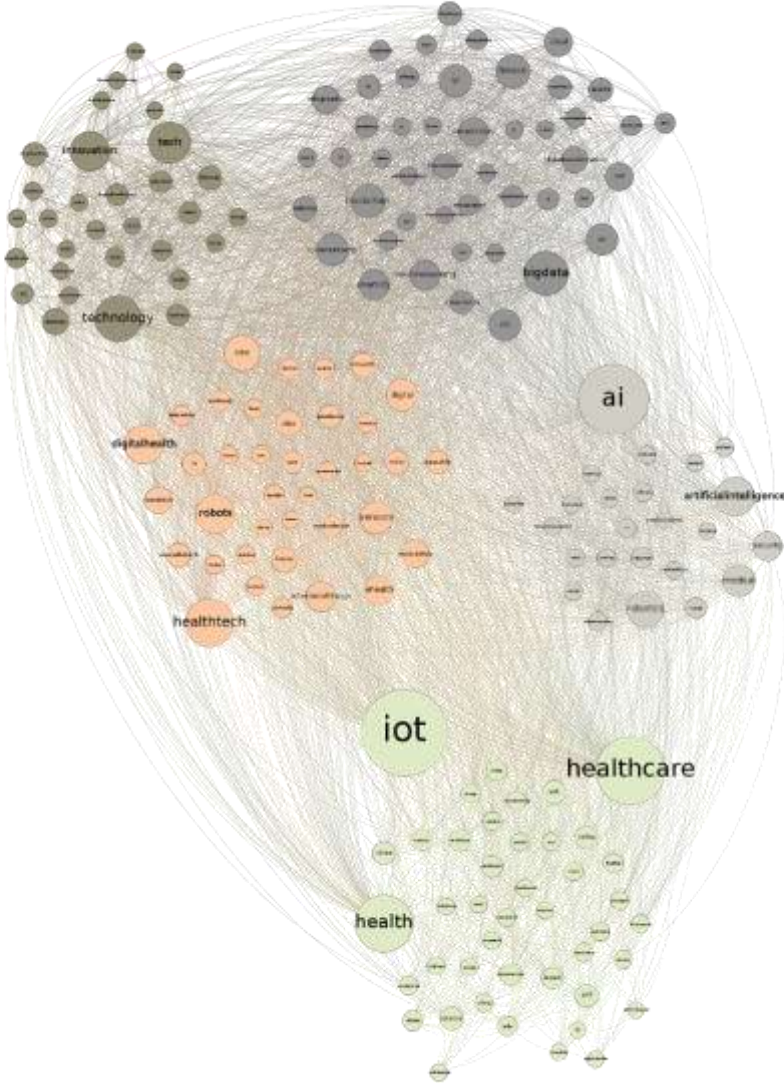
Investments

| | | | | |
|----------------|------------|----------------|-----------|------------------------|
| Companies: 181 | Deals: 486 | Investors: 503 | Exits: 11 | Largest deal: 68.31M € |
|----------------|------------|----------------|-----------|------------------------|

Investment over time



Twitter Analysis



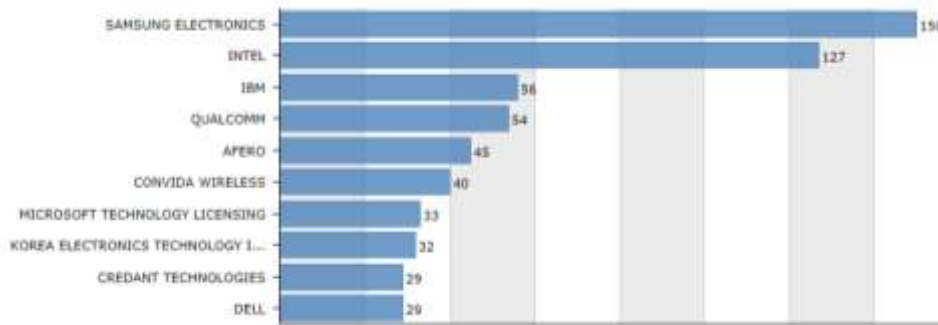
Military and Defence

Patents

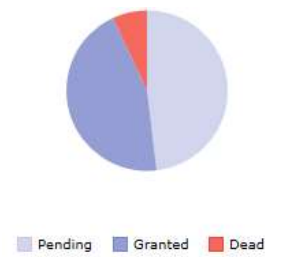
Topic 5: Military and Defence

Patented inventions: 2604 (21 % owned by top 10 players)

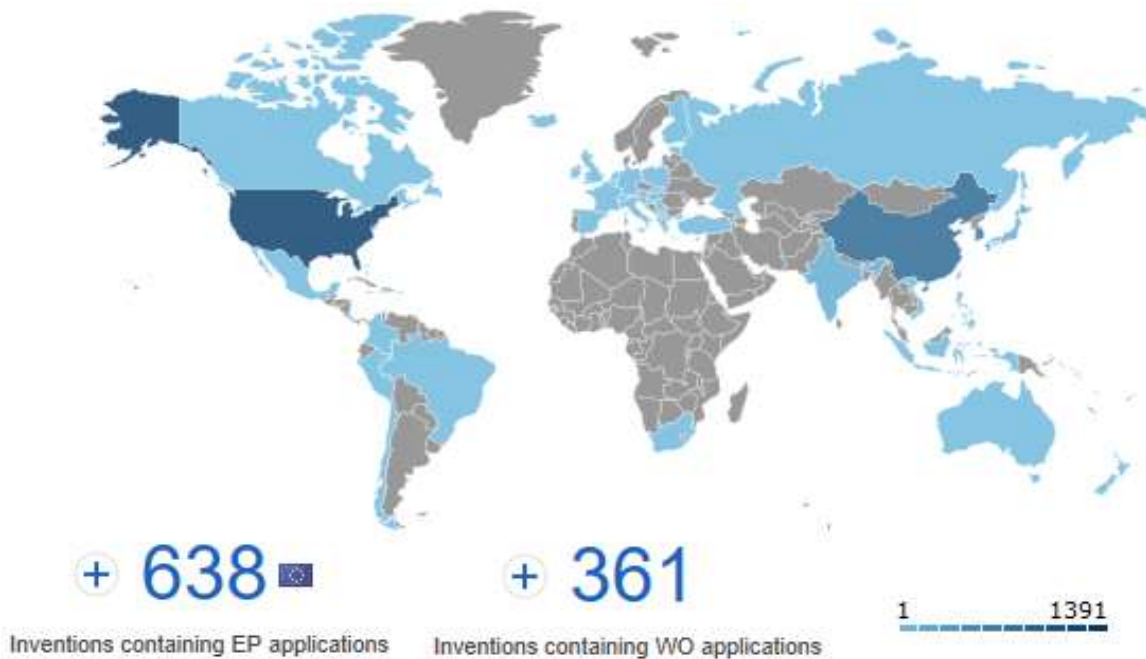
Top 10 players



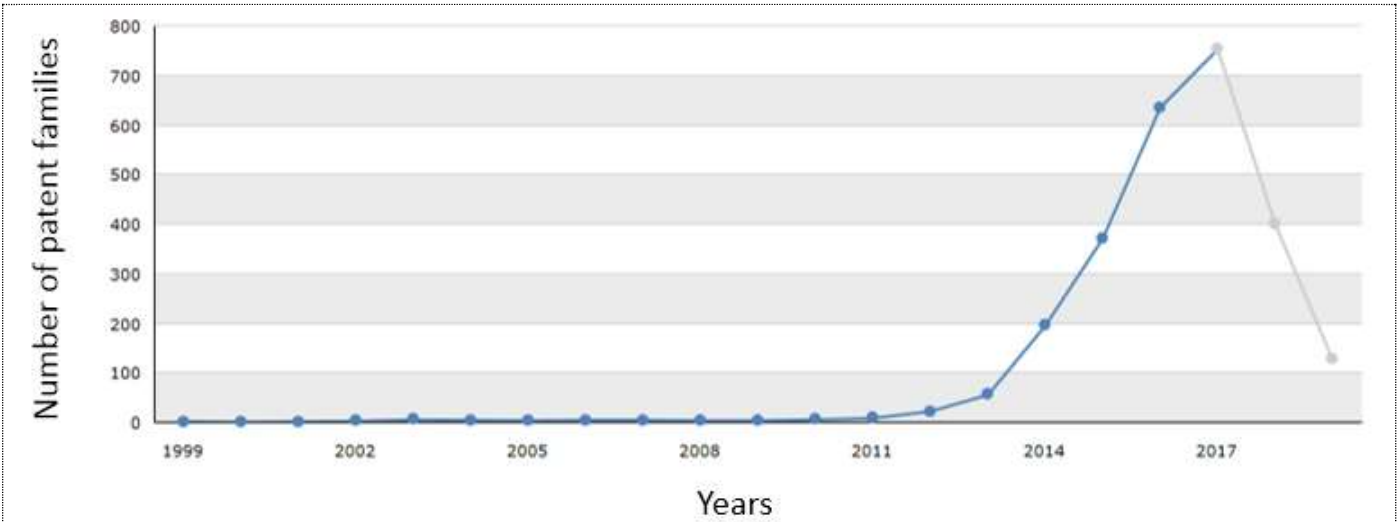
Legal status



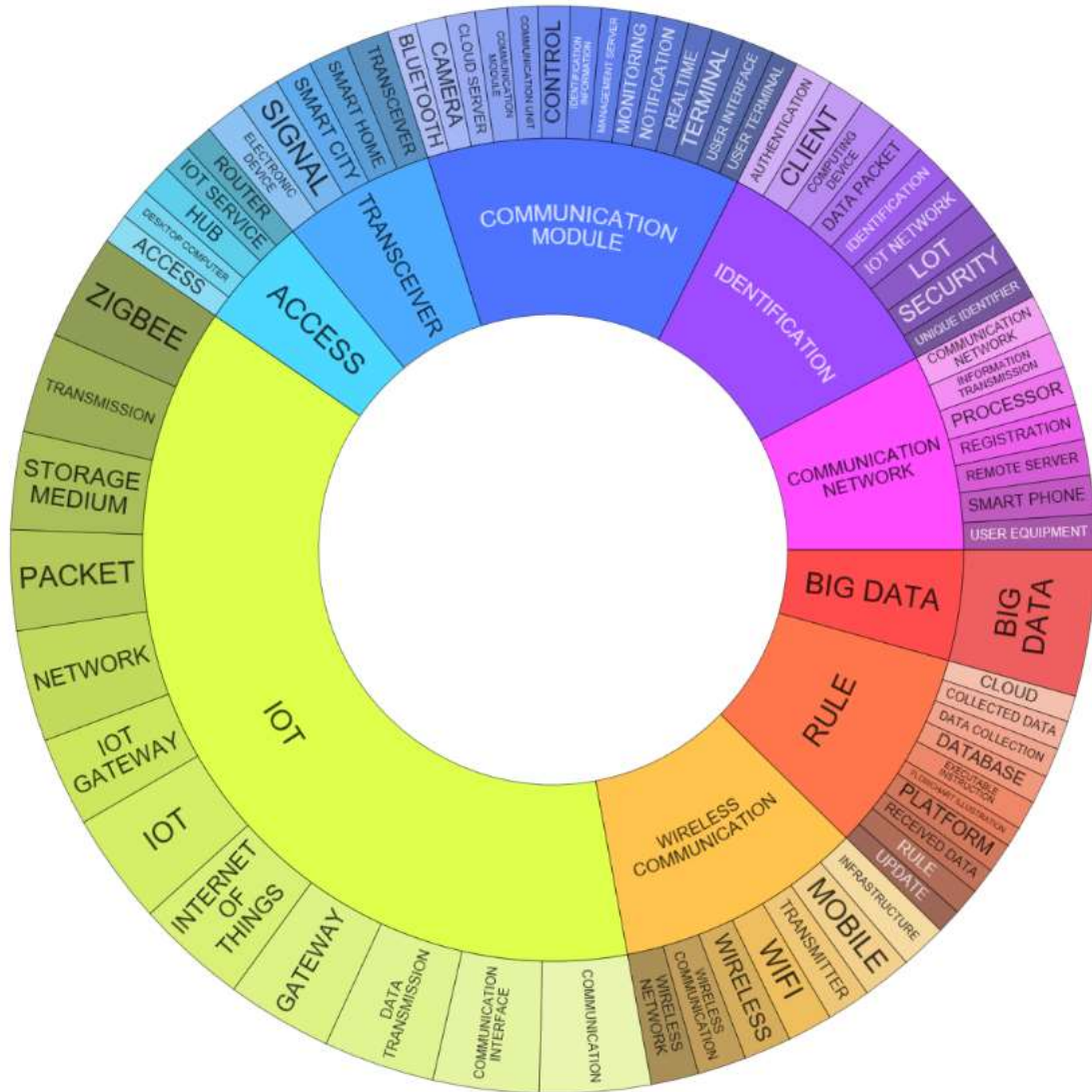
Market coverage



Temporal distribution



Technologies and applications



Scientific publications

Topic 5: Military and Defense

Number of articles: 197

Key actors

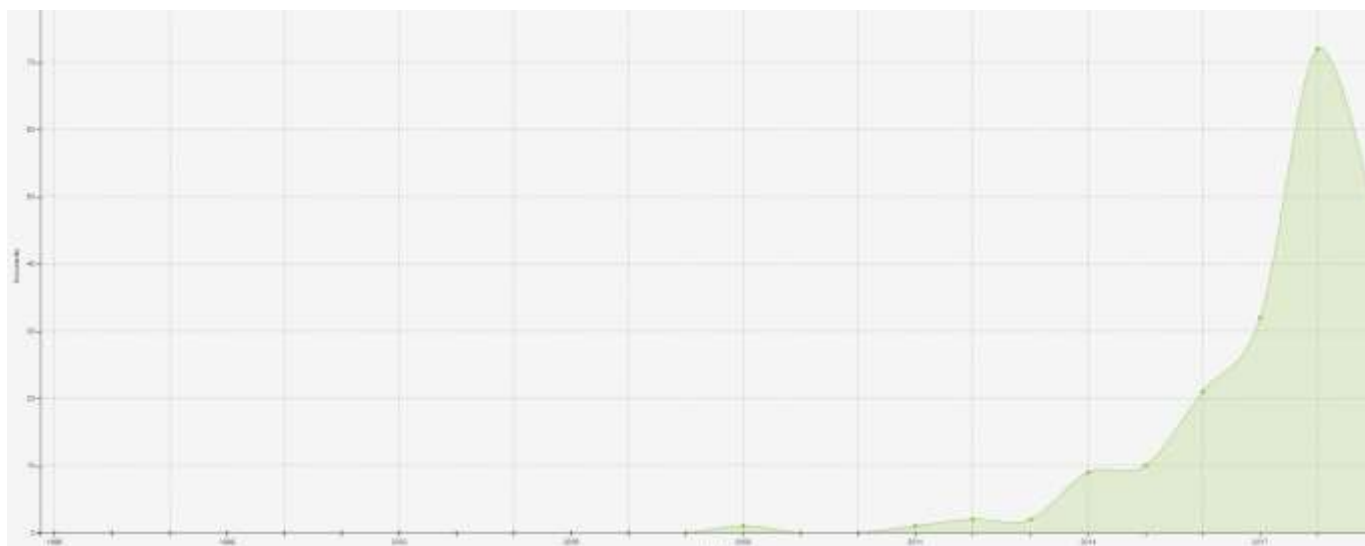


Spatial distribution



| Author keywords | Occurrence |
|--------------------------------------|-------------------|
| Security | 29 |
| Wireless sensor network (WSN) | 21 |
| Network security | 10 |
| Intrusion detection | 7 |
| Cyber attacks | 6 |
| Big data | 6 |
| Defensive | 6 |
| Machine learning | 6 |
| Attacks | 6 |
| Vulnerability | 5 |

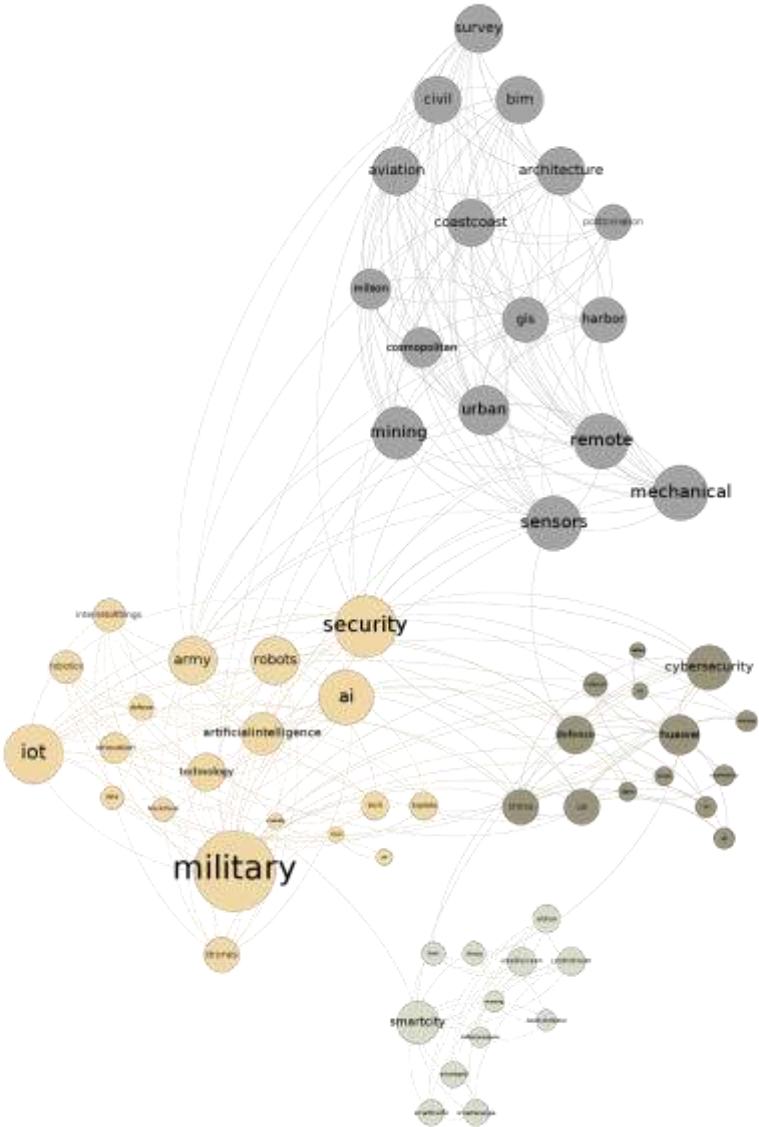
Temporal distribution



Investments




Data were not available at the time of the investigation

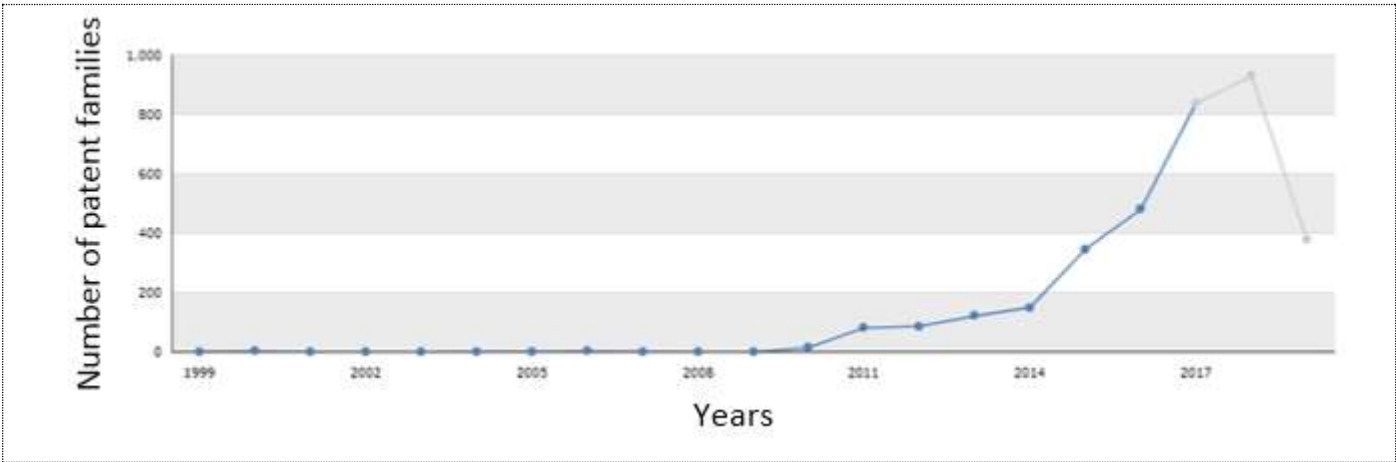
Twitter Analysis



Renewable energy

Patents

| <p>Topic 6: Renewable energy</p> | <p>Patented inventions: 3447 (5% owned by top 10 players)</p> | | | | | | | | | | | | | | | | | | | | | | |
|---|--|-------|---------------------------------|----|---------------------|----|---|----|---|----|-------------------|----|--------------------------------------|----|------------------------------------|----|-------|----|----------------------------------|----|------------------|----|--|
| <p>Top 10 players</p>  <table border="1"> <thead> <tr> <th>Entity</th> <th>Count</th> </tr> </thead> <tbody> <tr> <td>STATE GRID CORPORATION OF CHINA</td> <td>24</td> </tr> <tr> <td>SHANGHAI ELECTRONIC</td> <td>22</td> </tr> <tr> <td>WUJI TONGCHUN NEW ENERGY SCIENCE AND TECHNOLOGY CO., LTD.</td> <td>20</td> </tr> <tr> <td>SHANGHONG YONGYI INFORMATION TECHNOLOGY CO., LTD.</td> <td>19</td> </tr> <tr> <td>HONGKONG ELECTRIC</td> <td>18</td> </tr> <tr> <td>STATE GRID ENERGY RESEARCH INSTITUTE</td> <td>18</td> </tr> <tr> <td>CHANGCHUN UNIVERSITY OF TECHNOLOGY</td> <td>18</td> </tr> <tr> <td>INTEL</td> <td>18</td> </tr> <tr> <td>SHANGHAI AGRICULTURAL UNIVERSITY</td> <td>14</td> </tr> <tr> <td>GENERAL ELECTRIC</td> <td>12</td> </tr> </tbody> </table> | Entity | Count | STATE GRID CORPORATION OF CHINA | 24 | SHANGHAI ELECTRONIC | 22 | WUJI TONGCHUN NEW ENERGY SCIENCE AND TECHNOLOGY CO., LTD. | 20 | SHANGHONG YONGYI INFORMATION TECHNOLOGY CO., LTD. | 19 | HONGKONG ELECTRIC | 18 | STATE GRID ENERGY RESEARCH INSTITUTE | 18 | CHANGCHUN UNIVERSITY OF TECHNOLOGY | 18 | INTEL | 18 | SHANGHAI AGRICULTURAL UNIVERSITY | 14 | GENERAL ELECTRIC | 12 | <p>Legal status</p>  <p> ■ Pending ■ Granted ■ Dead </p> |
| Entity | Count | | | | | | | | | | | | | | | | | | | | | | |
| STATE GRID CORPORATION OF CHINA | 24 | | | | | | | | | | | | | | | | | | | | | | |
| SHANGHAI ELECTRONIC | 22 | | | | | | | | | | | | | | | | | | | | | | |
| WUJI TONGCHUN NEW ENERGY SCIENCE AND TECHNOLOGY CO., LTD. | 20 | | | | | | | | | | | | | | | | | | | | | | |
| SHANGHONG YONGYI INFORMATION TECHNOLOGY CO., LTD. | 19 | | | | | | | | | | | | | | | | | | | | | | |
| HONGKONG ELECTRIC | 18 | | | | | | | | | | | | | | | | | | | | | | |
| STATE GRID ENERGY RESEARCH INSTITUTE | 18 | | | | | | | | | | | | | | | | | | | | | | |
| CHANGCHUN UNIVERSITY OF TECHNOLOGY | 18 | | | | | | | | | | | | | | | | | | | | | | |
| INTEL | 18 | | | | | | | | | | | | | | | | | | | | | | |
| SHANGHAI AGRICULTURAL UNIVERSITY | 14 | | | | | | | | | | | | | | | | | | | | | | |
| GENERAL ELECTRIC | 12 | | | | | | | | | | | | | | | | | | | | | | |
| <p>Market coverage</p>  <p> + 184 EP Inventions containing EP applications </p> <p> + 161 Inventions containing WO applications </p> <p style="text-align: right;"> 1 2166 </p> | | | | | | | | | | | | | | | | | | | | | | | |
| <p>Temporal distribution</p> | | | | | | | | | | | | | | | | | | | | | | | |

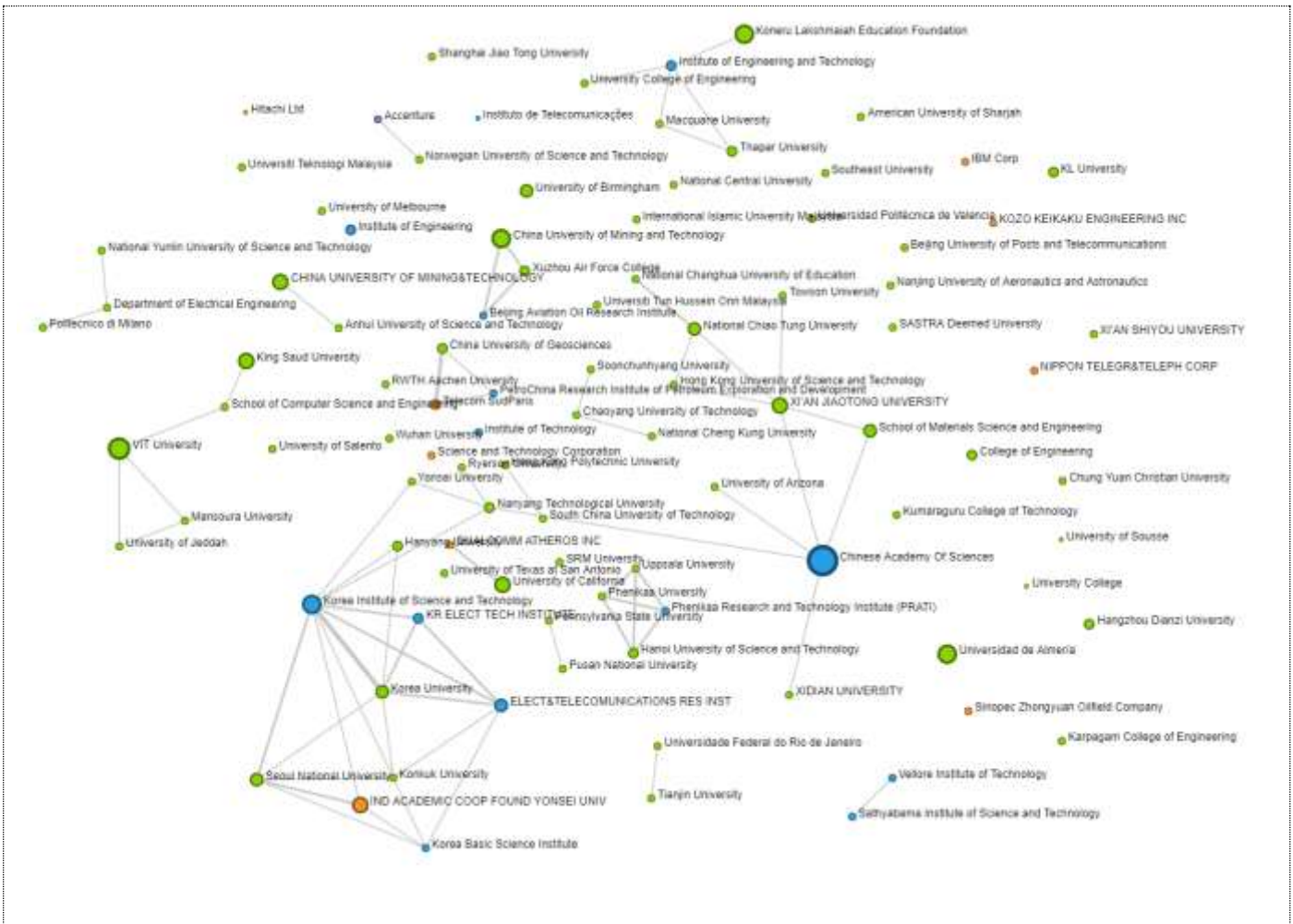


Technologies and applications



Scientific publications

| | |
|---------------------------|-----------------------------------|
| Topic 6: Renewable energy | Number of articles: 389 |
| Key actors | |

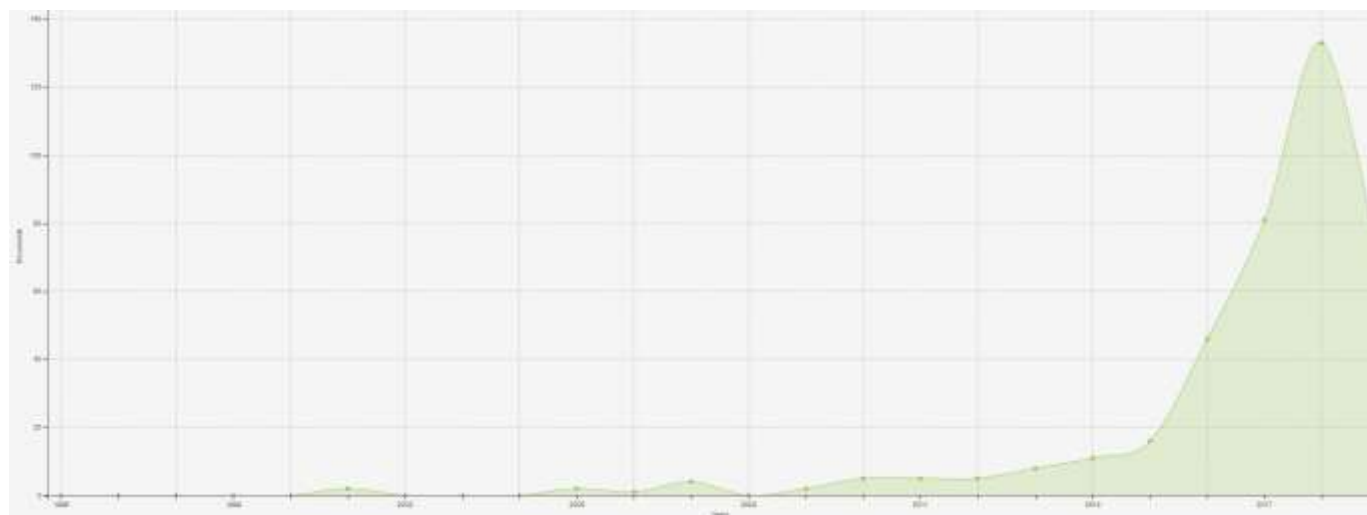


Spatial distribution



| Author keywords | Occurrence |
|--------------------------------------|-------------------|
| Gas sensor | 24 |
| Smart grid | 19 |
| Genetic algorithm | 17 |
| Smart home | 16 |
| Wireless sensor network (WSN) | 13 |
| Energy efficiency | 13 |
| Cloud computing | 13 |
| Smart city | 12 |
| Low power | 8 |
| Big data | 8 |

Temporal distribution



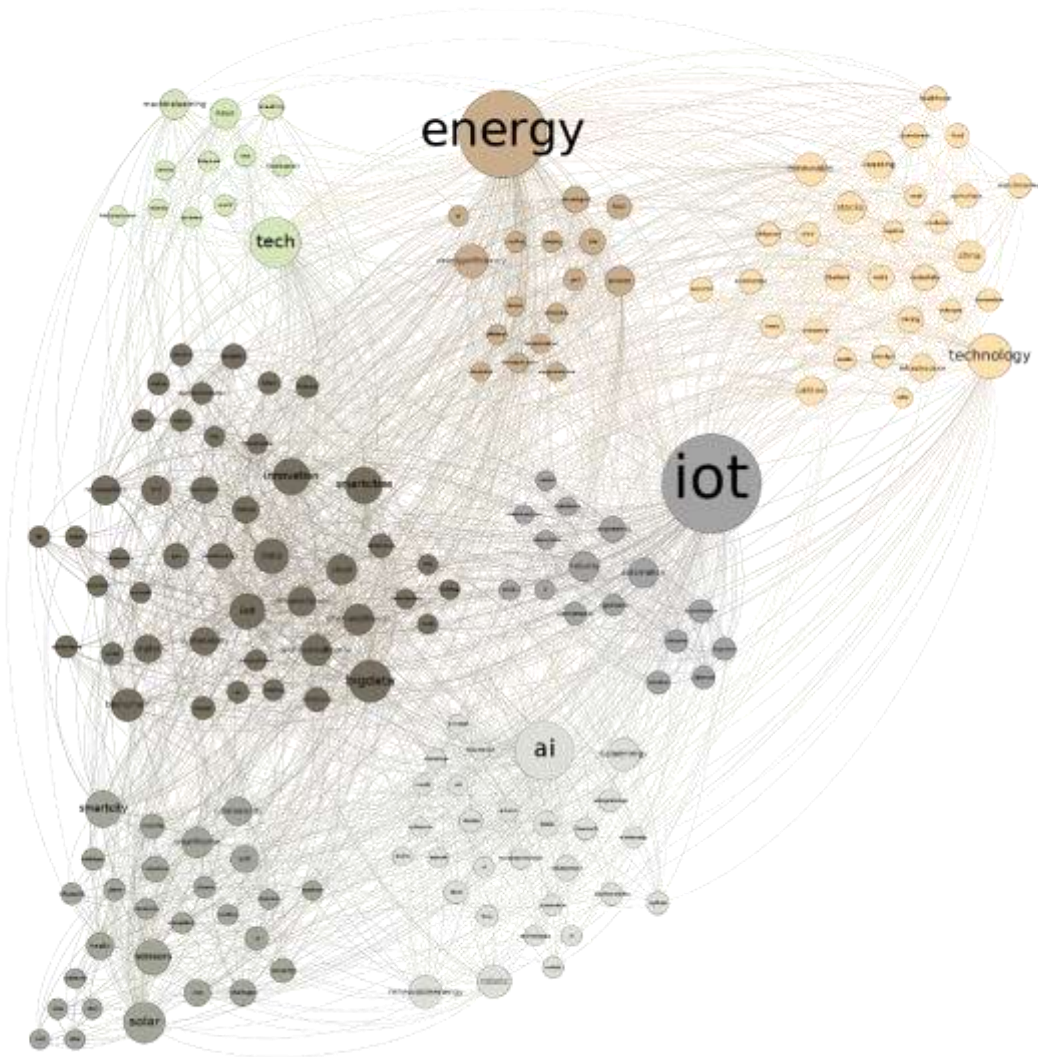
Investments

| | | | | |
|----------------|------------|----------------|-----------|------------------------|
| Companies: 226 | Deals: 826 | Investors: 861 | Exits: 47 | Largest deal: 699,3M € |
|----------------|------------|----------------|-----------|------------------------|

Investment over time



Twitter Analysis



Smart City

Patents

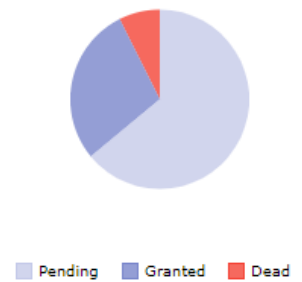
Topic 7: Smart City

Patented inventions: 4275 (49 % owned by top 10 players)

Top 10 players



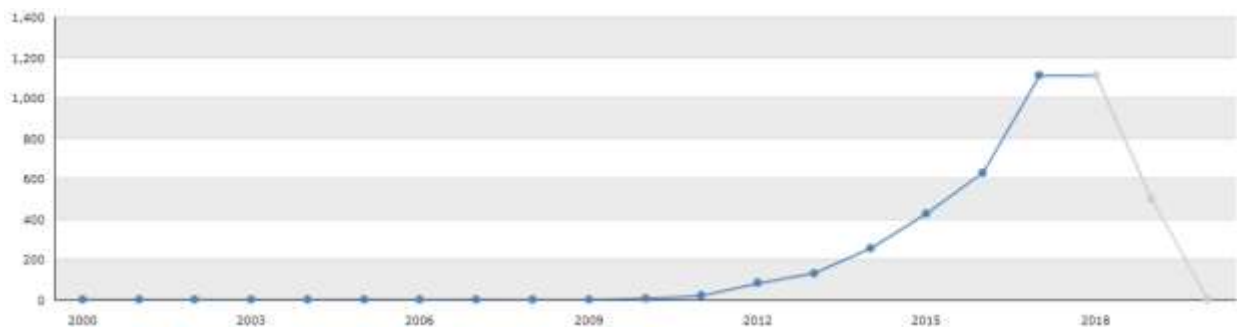
Legal status



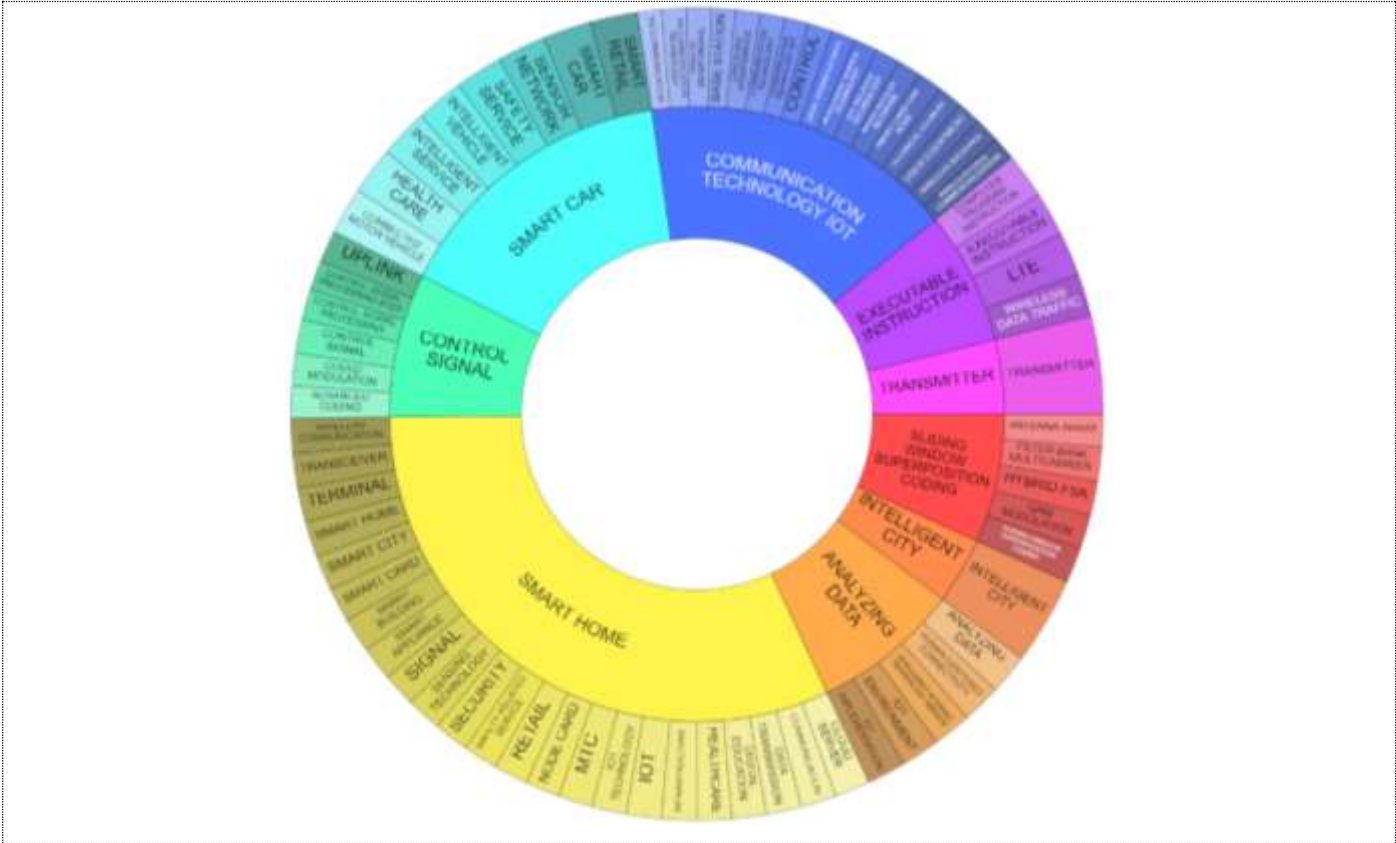
Market coverage



Temporal distribution

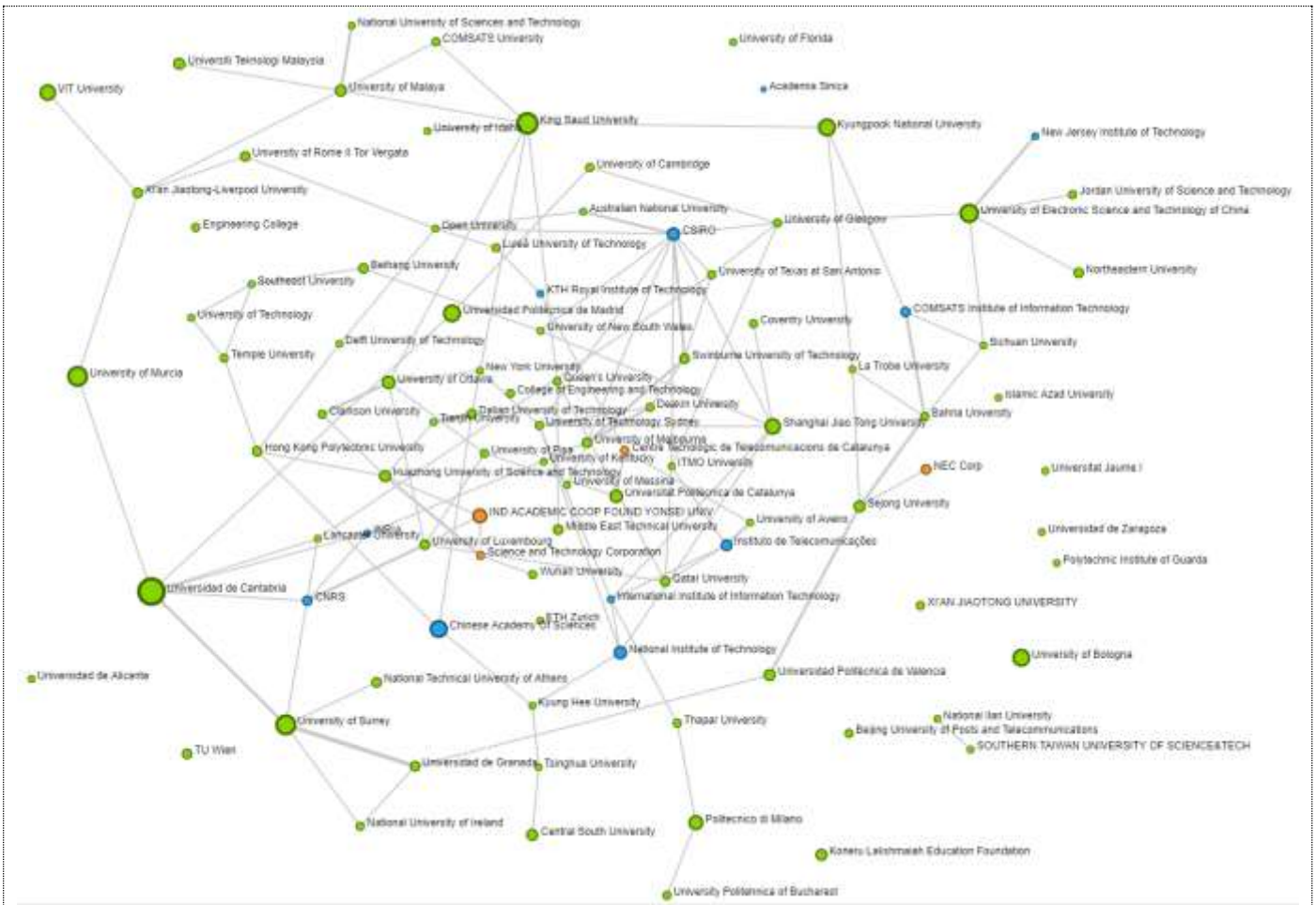


Technologies and applications



Scientific publications

| | |
|----------------------------|--------------------------------|
| Topic 7: Smart City | Number of articles: 984 |
| Key actors | |

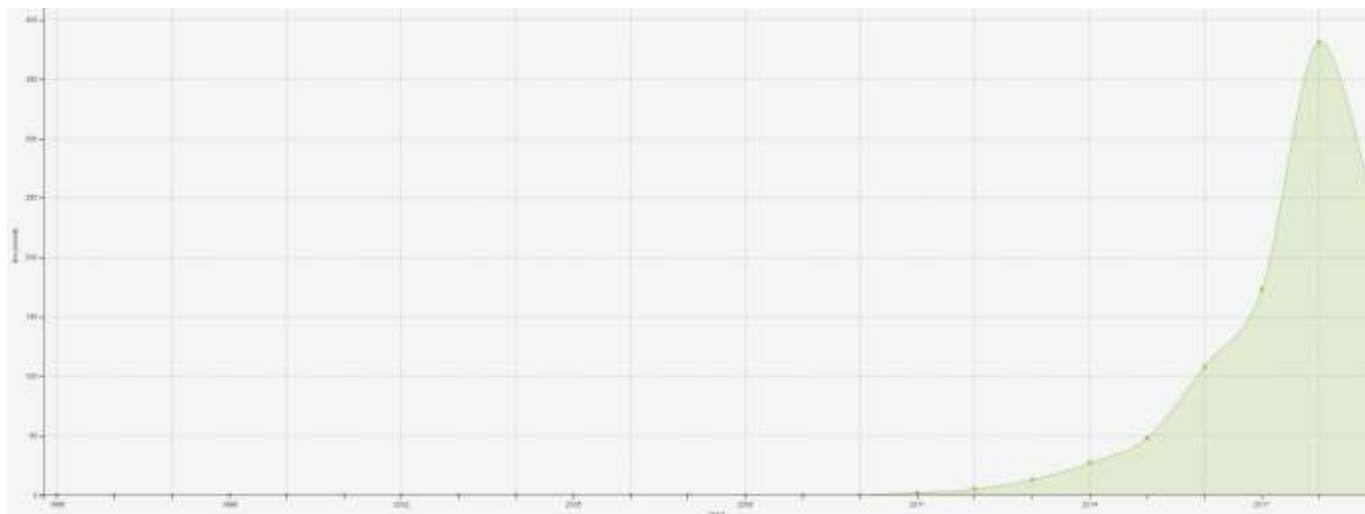


Spatial distribution



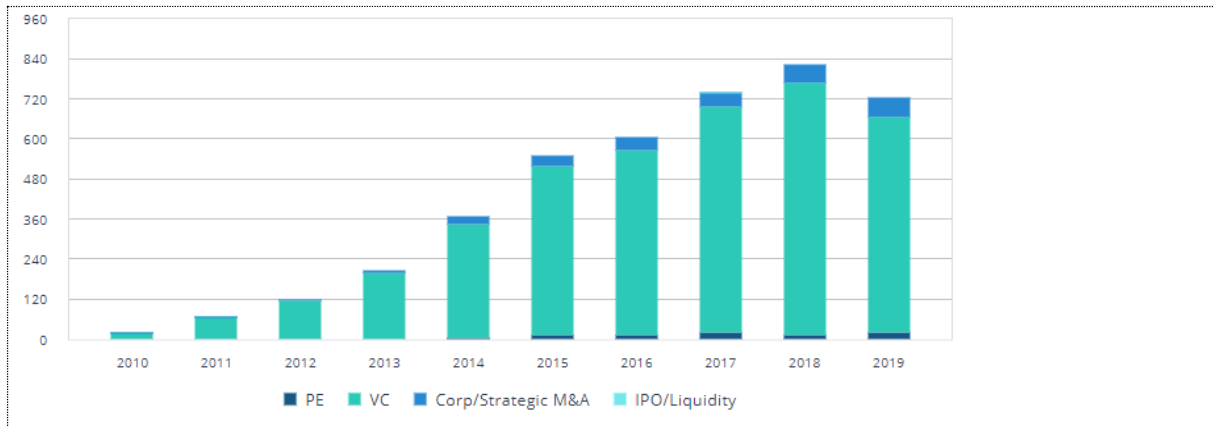
| Author keywords | Occurrence |
|-------------------------------|------------|
| Big data | 84 |
| Cloud computing | 69 |
| Wireless sensor network (WSN) | 57 |
| Security | 43 |
| Fog computing | 30 |
| Energy efficiency | 24 |
| Machine learning | 22 |
| Edge computing | 21 |
| Smart home | 19 |
| Block chaining | 19 |

Temporal distribution

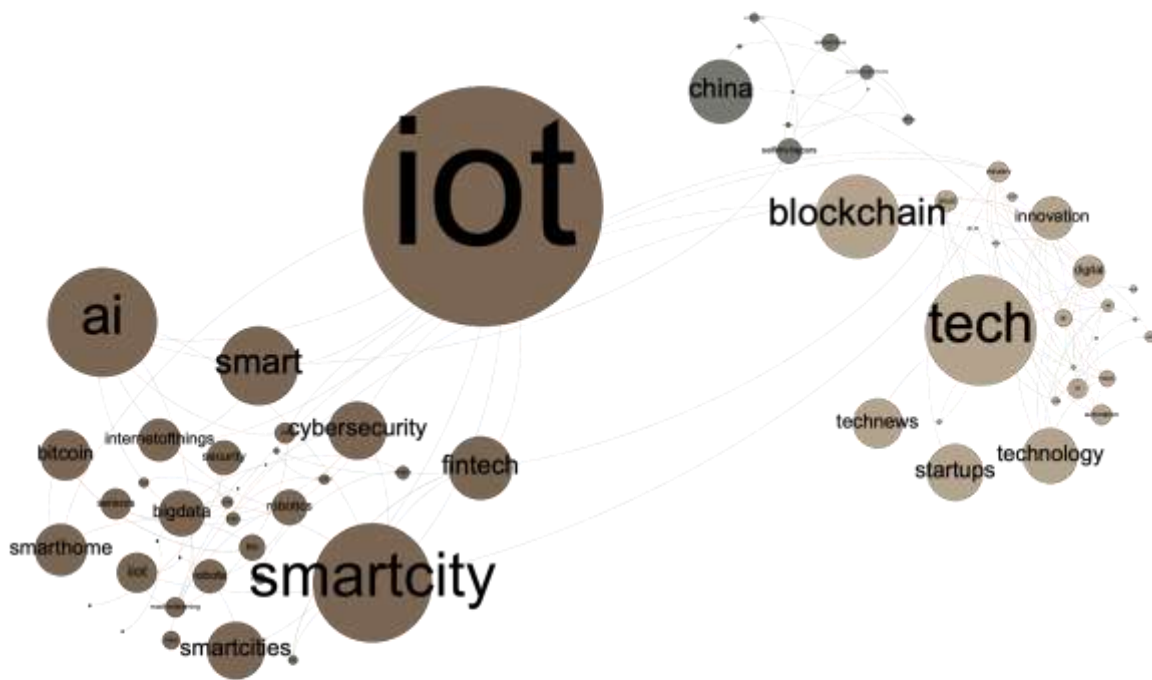


Investments

| | | | | |
|----------------------|-------------|-----------------|------------|-----------------------|
| Companies: 3360 | Deals: 8702 | Investors: 6608 | Exits: 478 | Largest deal: 2,35B € |
| Investment over time | | | | |

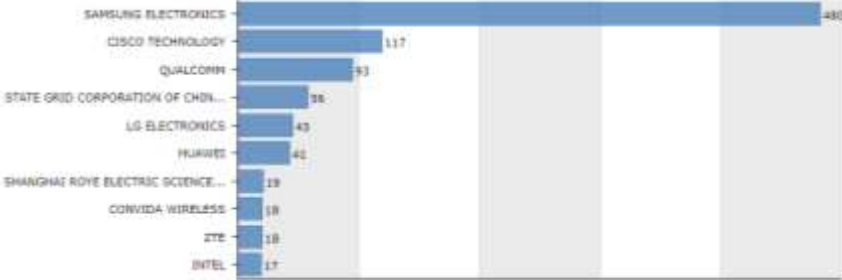
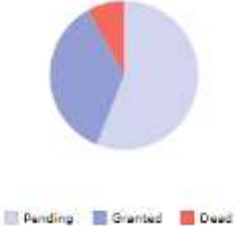






Twitter Analysis

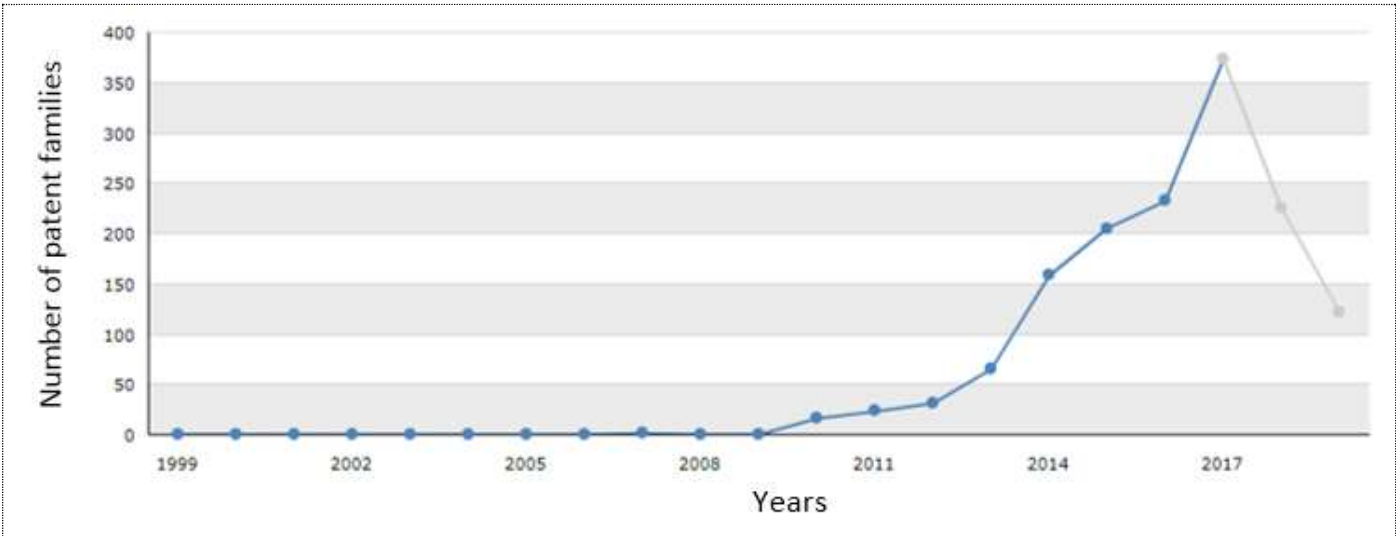


Smart Grid/Smart Power⁷

Patents

| <p>Topic 8: Smart Grid/Smart Power</p> | <p>Patented inventions: 1451 (62 % owned by top 10 players)</p> | | | | | | | | | | | | | | | | | | | | | | |
|--|--|---------|---------------------|-----|------------------|-----|----------|----|---------------------------------|----|----------------|----|--------|----|-----------------------------------|----|------------------|----|-----|----|-------|----|---|
| <p>Top 10 players</p>  <table border="1"> <thead> <tr> <th>Company</th> <th>Patents</th> </tr> </thead> <tbody> <tr> <td>SAMSUNG ELECTRONICS</td> <td>480</td> </tr> <tr> <td>CISCO TECHNOLOGY</td> <td>117</td> </tr> <tr> <td>QUALCOMM</td> <td>93</td> </tr> <tr> <td>STATE GRID CORPORATION OF CHINA</td> <td>36</td> </tr> <tr> <td>LG ELECTRONICS</td> <td>43</td> </tr> <tr> <td>HUAWEI</td> <td>40</td> </tr> <tr> <td>SHANGHAI ROYE ELECTRIC SCIENCE...</td> <td>19</td> </tr> <tr> <td>CONVIDA WIRELESS</td> <td>18</td> </tr> <tr> <td>ZTE</td> <td>18</td> </tr> <tr> <td>INTEL</td> <td>17</td> </tr> </tbody> </table> | Company | Patents | SAMSUNG ELECTRONICS | 480 | CISCO TECHNOLOGY | 117 | QUALCOMM | 93 | STATE GRID CORPORATION OF CHINA | 36 | LG ELECTRONICS | 43 | HUAWEI | 40 | SHANGHAI ROYE ELECTRIC SCIENCE... | 19 | CONVIDA WIRELESS | 18 | ZTE | 18 | INTEL | 17 | <p>Legal status</p>  <p>Legend: Pending (light blue), Granted (dark blue), Dead (red)</p> |
| Company | Patents | | | | | | | | | | | | | | | | | | | | | | |
| SAMSUNG ELECTRONICS | 480 | | | | | | | | | | | | | | | | | | | | | | |
| CISCO TECHNOLOGY | 117 | | | | | | | | | | | | | | | | | | | | | | |
| QUALCOMM | 93 | | | | | | | | | | | | | | | | | | | | | | |
| STATE GRID CORPORATION OF CHINA | 36 | | | | | | | | | | | | | | | | | | | | | | |
| LG ELECTRONICS | 43 | | | | | | | | | | | | | | | | | | | | | | |
| HUAWEI | 40 | | | | | | | | | | | | | | | | | | | | | | |
| SHANGHAI ROYE ELECTRIC SCIENCE... | 19 | | | | | | | | | | | | | | | | | | | | | | |
| CONVIDA WIRELESS | 18 | | | | | | | | | | | | | | | | | | | | | | |
| ZTE | 18 | | | | | | | | | | | | | | | | | | | | | | |
| INTEL | 17 | | | | | | | | | | | | | | | | | | | | | | |
| <p>Market coverage</p>  <p>+ 533  Inventions containing EP applications</p> <p>+ 339  Inventions containing WO applications</p> <p>1  675</p> | | | | | | | | | | | | | | | | | | | | | | | |
| <p>Temporal distribution</p> | | | | | | | | | | | | | | | | | | | | | | | |

⁷ The SmartGrid/Smart Power search results focus on the local context and exclude patents specific to large utility companies.



Technologies and applications



Scientific publications

| | |
|---------------------------------|--------------------------------|
| Topic 8: Smart Grid/Smart Power | Number of articles: 345 |
| Key actors | |

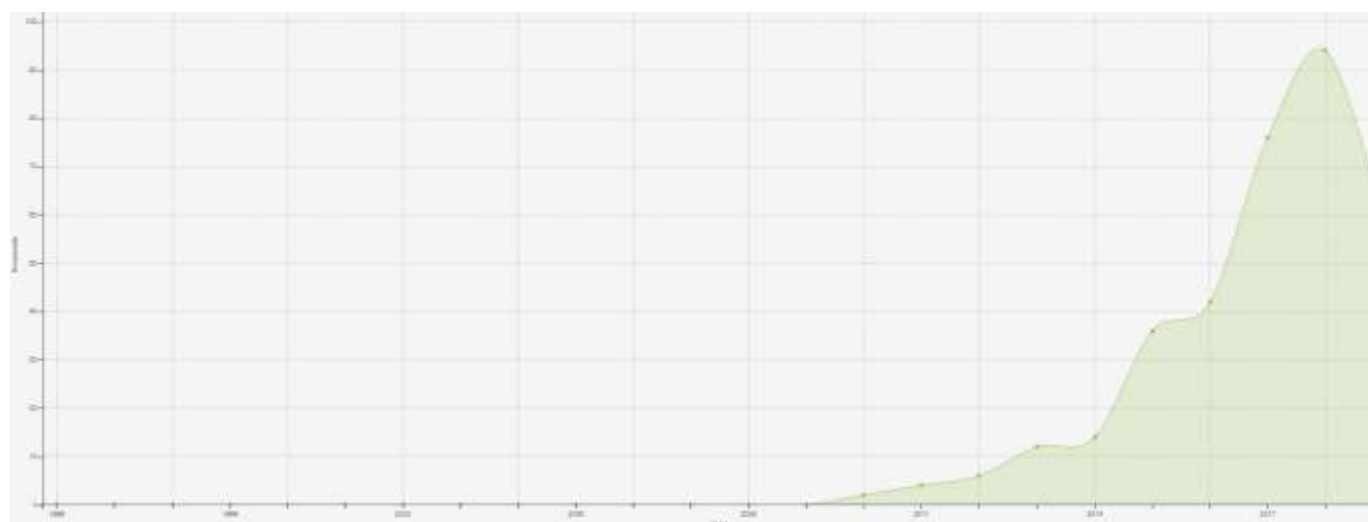


Spatial distribution



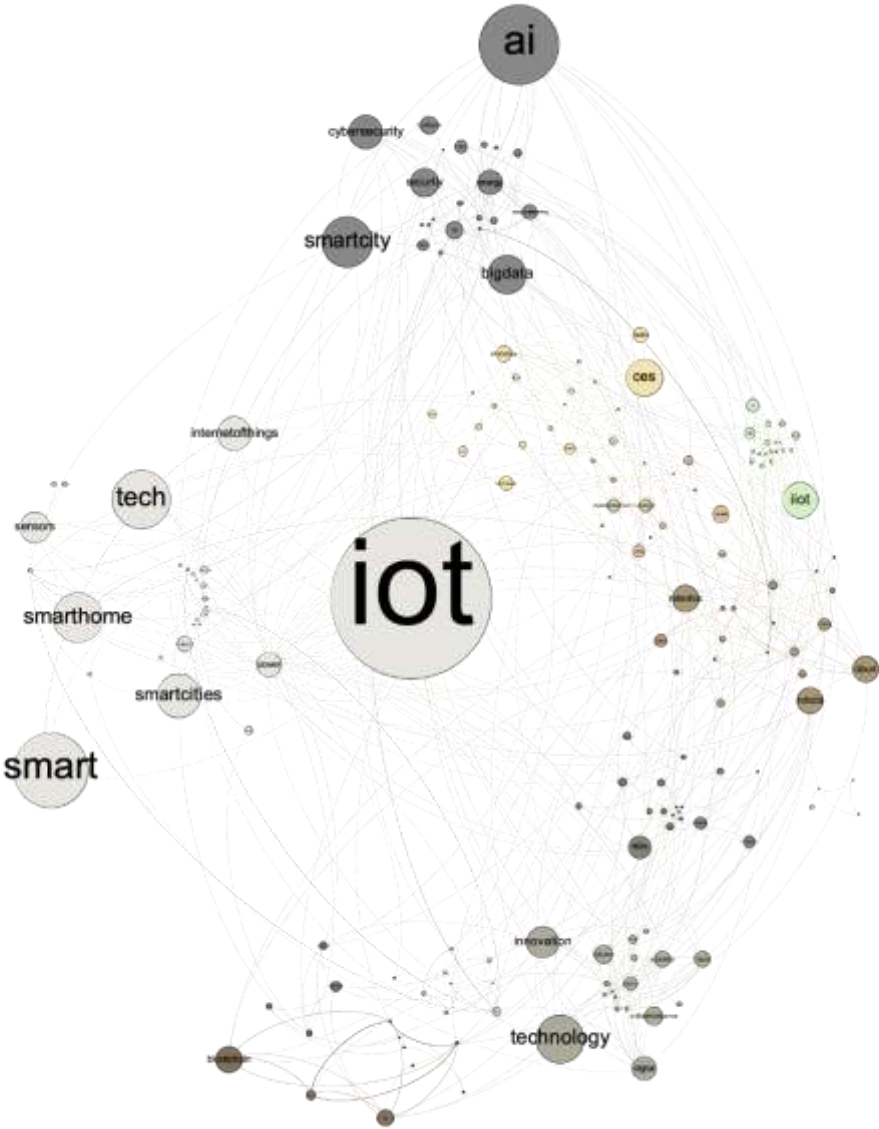
| Author keywords | Occurrence |
|--------------------------------------|-------------------|
| Security | 34 |
| Smart meters | 24 |
| Smart city | 22 |
| Wireless Sensor Network (WSN) | 20 |
| Big data | 20 |
| Privacy | 14 |
| Cloud computing | 13 |
| Smart home | 13 |
| Cyber physical | 12 |
| Demand response | 11 |

Temporal distribution



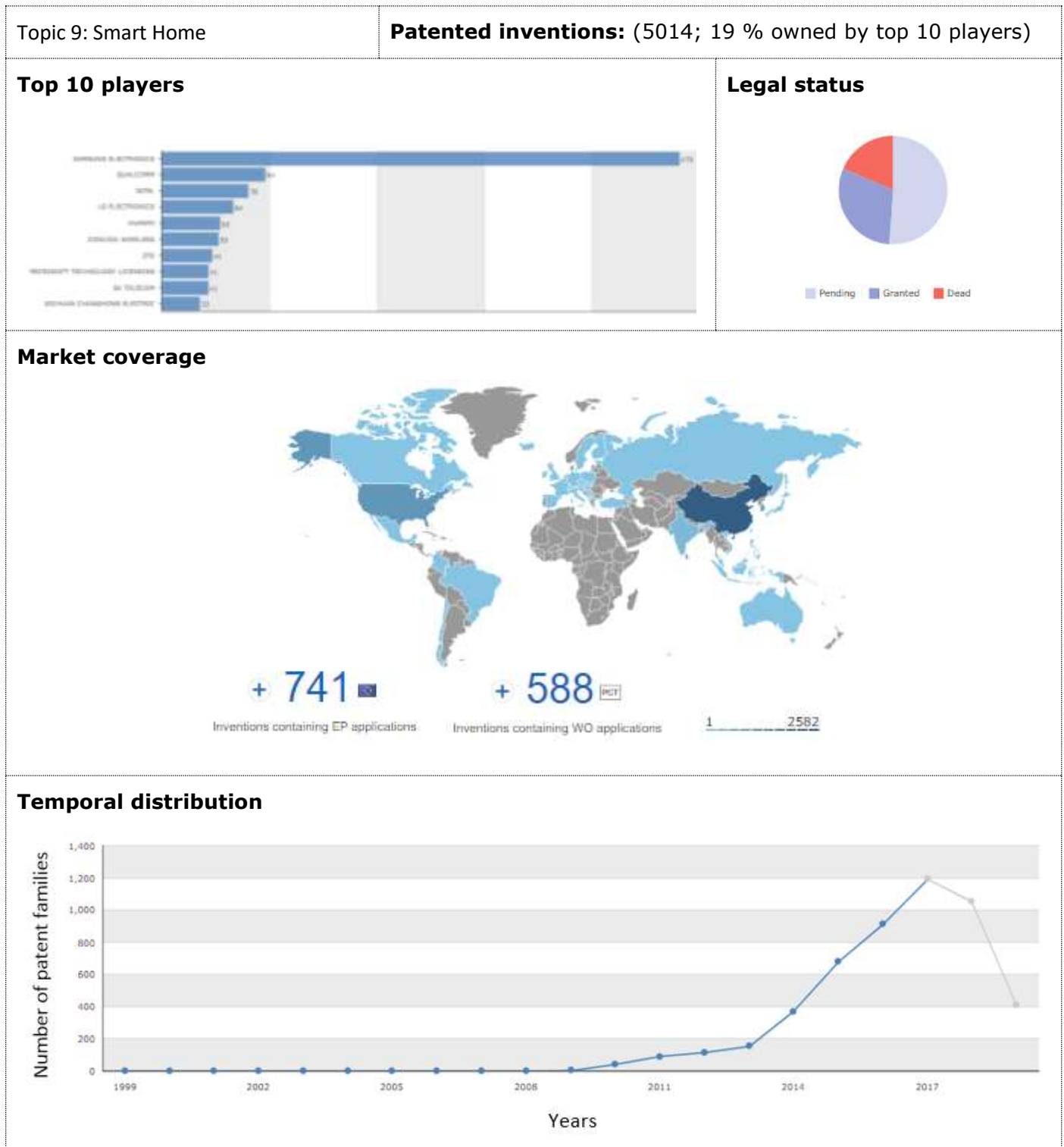
Investments

Data were not available at the time of the investigation



Smart Home

Patents

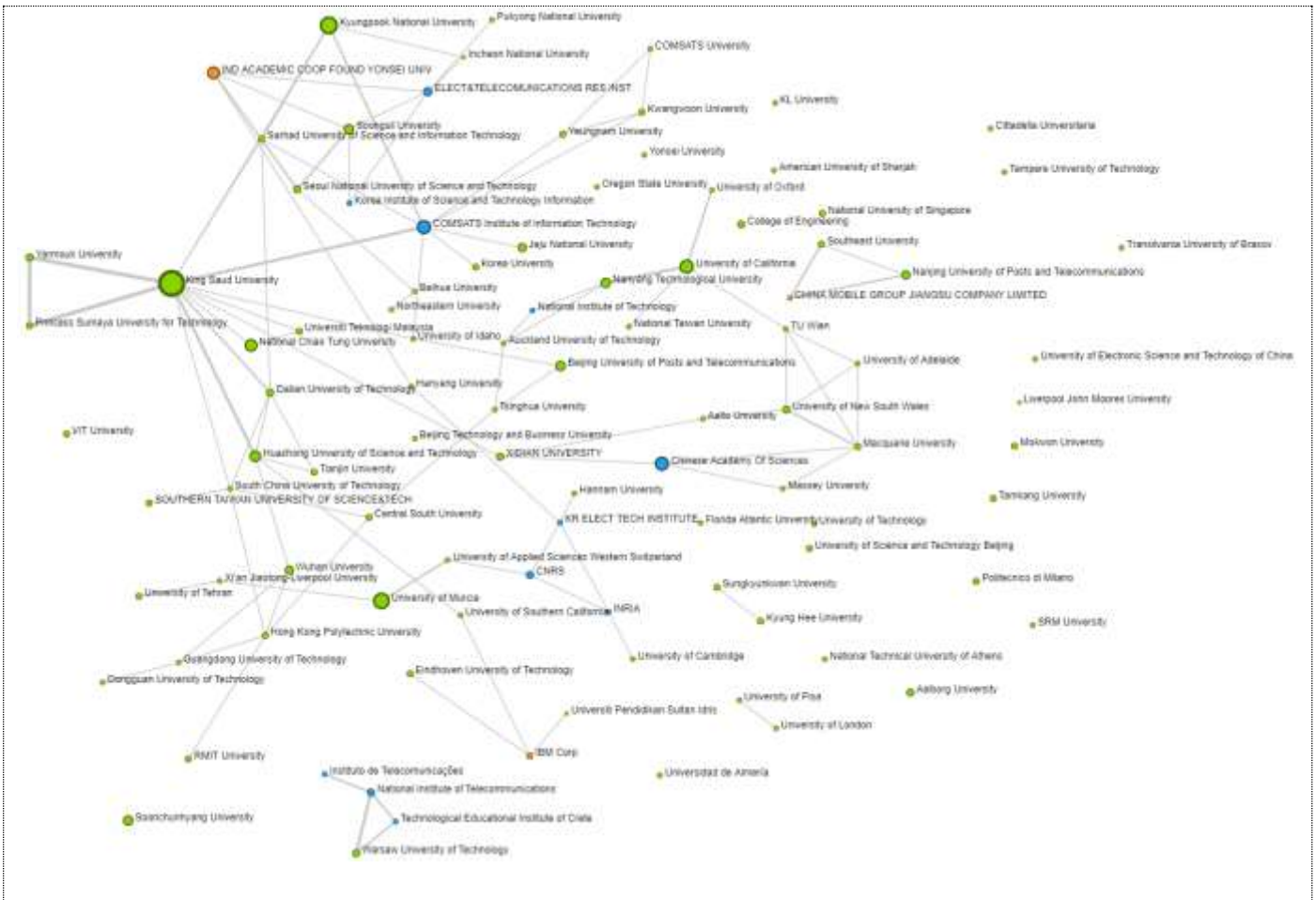


Technologies and applications



Scientific publications

| | |
|---------------------|--------------------------------|
| Topic 9: Smart Home | Number of articles: 754 |
| Key actors | |

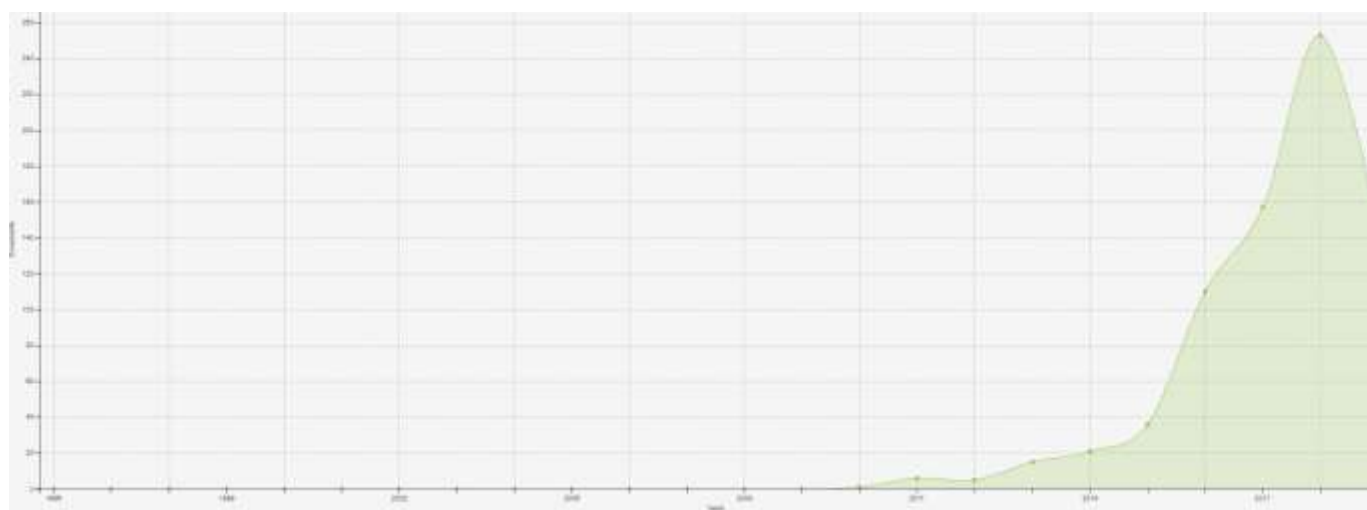


Spatial distribution



| Author keywords | Occurrence |
|--------------------------------------|-------------------|
| Smart building | 57 |
| Wireless sensor network (WSN) | 47 |
| Security | 40 |
| Smart city | 33 |
| Energy efficiency | 26 |
| Cloud computing | 26 |
| Home automation | 24 |
| Big data | 23 |
| Smart grid | 21 |
| Cyber physical | 19 |

Temporal distribution



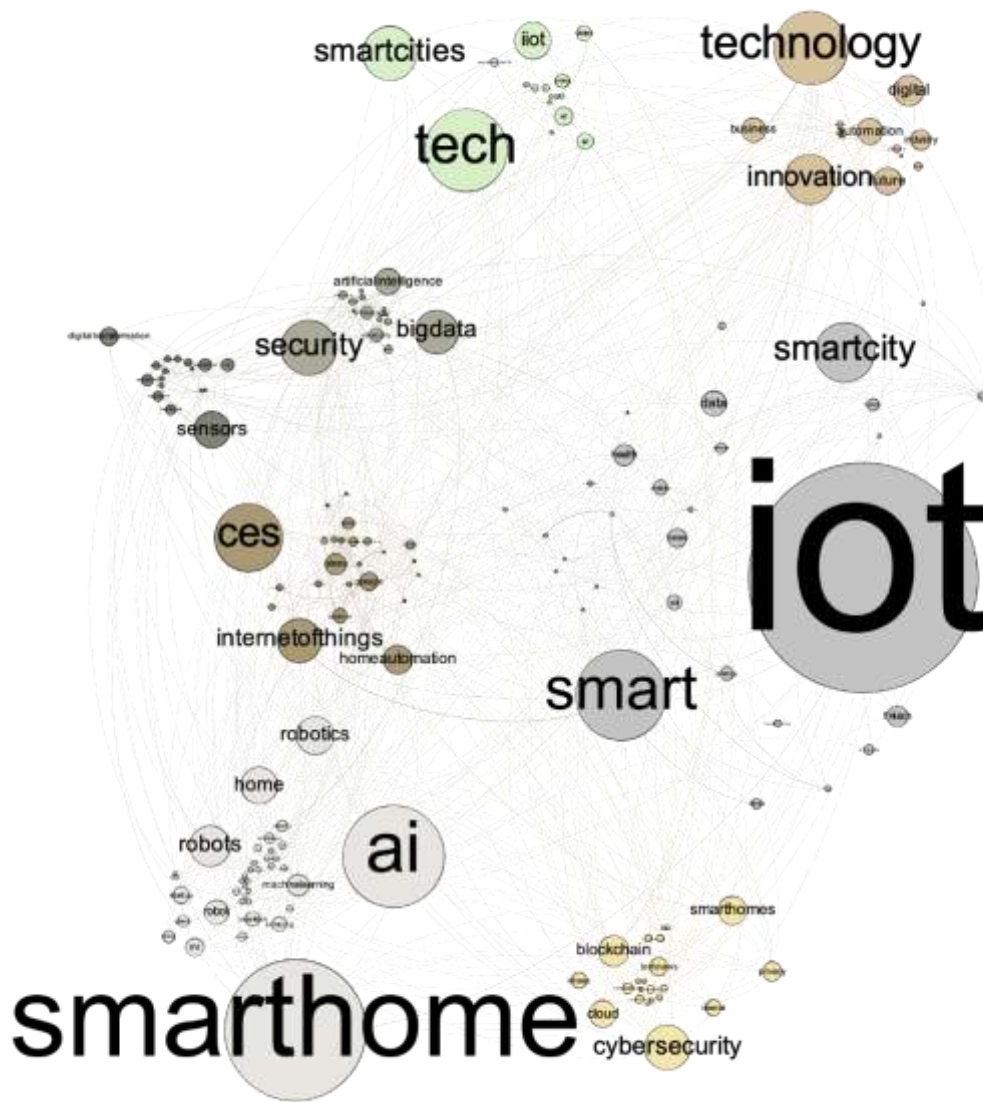
Investments

| | | | | |
|----------------|-------------|-----------------|------------|------------------------|
| Companies: 466 | Deals: 1350 | Investors: 1426 | Exits: 138 | Largest deal: 4.05 B € |
|----------------|-------------|-----------------|------------|------------------------|

Investment over time



Twitter Analysis



ANNEX H. IoT Legal Regulation

EU IoT Policy

First Communication relating to the European IoT Policy was published in 2009. "IoT—An Action Plan for Europe" [72] was a formal recognition of the IoT phenomena and general regulatory gaps relating to it. During the last few years the European Commission has adopted a set of policy actions that accelerate the take-up of IoT with aim to unleash its potential in Europe for the benefit of European citizens and businesses. In March 2015 the Alliance for Internet of Things Innovation (AIOTI) was launched by the European Commission to support the creation of an innovative and industry driven European IoT ecosystem. This flags the intention of the European Commission to work closely with all Internet of Things stakeholders and actors towards the establishment of a competitive European IoT market and the creation of new business models. On the question of whether the emergence of IoT necessitates new regulation, the AIOTI WG04 concluded in the negative, arguing that "[a]ny regulatory proposal targeting the IoT should address only well-defined market failures that cannot be addressed through existing law and self-regulatory measures". The AIOTI also pointed to the elevated risk of regulatory error in a complex and fast-moving environment, such as the IoT.

In May 2015 the Digital Single Market Strategy was adopted [73]. The Digital Single Market strategy includes elements which lead Europe a step further in accelerating developments on IoT. In particular, the strategy underlines the need to avoid fragmentation and to foster interoperability for IoT to reach its potential. To meet the Digital Single Market strategy needs and inform about its upcoming policy, the European Commission published in April 2016 the European Commission Staff Working Document "Advancing the Internet of Things in Europe" [74]. This document is part of the "Digitising European Industry" initiative and specifies the EU's vision on the IoT. The vision is based on three pillars:

- a thriving IoT ecosystem;
- a human-centred IoT approach;
- a single market for IoT.

From the international law perspective, the EU needs to observe works of the International Telecommunication Union (ITU). The ITU is a specialised UN agency that is a relevant international body in the context of regulating IoT enabling infrastructure in Europe. The ITU has a legitimacy to harmonise IoT-related standards on the global scale. The two most IoT-relevant areas of the ITU activities are: a) coordination of radio spectrum and assignment of orbital slots for satellites (including telecommunication satellites), b) standardisation.

Electronic communications and radio spectrum

IoT is quite different from the general connectivity that the ICT regulators strive to enable. In connecting people, "the connectivity is the main service, whereas in IoT it is rather the application and related device and sensors. Business models are different, so is the footprint" [75]. As IoT connections are mostly wireless, the accommodation of the resulting traffic between connected devices needs more radio spectrum and harmonised use of the spectrum.

The use of the spectrum is a foundation of the IoT infrastructure, hence the legislature dealing with the electronic communication and radio spectrum in particular is a part of a legal framework for the IoT-related activities.

Regulatory aspects

The electronic communication law was significantly amended⁸ in order to take into account the needs of the DSM. In 2018 the European Electronic Communications Code was adopted in December 2018. As far as the IoT is considered, the Code creates a regulatory and institutional framework for implementation of internal market in electronic communications networks and services that results in the deployment and take-up of very high capacity networks, sustainable competition, interoperability of electronic communications services, accessibility, security of networks and services and end-user benefits. It takes into account the requirements of networks based on machine-to-machine communication.

Regulatory aspects and institutional competencies for radio spectrum in the EU are set out in the Decision [676/2002/EC](#)⁹ of the European Parliament and of the Council of 7 March 2002 on a regulatory framework for radio spectrum policy in the European Community (Radio Spectrum Decision).

The allocation and management of radio spectrum in the European Union is administered by national administrations as radio spectrum remains principally the responsibility of Member States. While the European Commission does not manage radio spectrum directly, its task is to ensure that the use and management of radio spectrum in the EU takes into account all relevant EU policies. Therefore the Commission addresses a number of specific goals that can only be achieved at EU level taking into account the work of international organisations, such as the ITU. The goals are: a) harmonising the use of radio spectrum; b) working towards more efficient use of spectrum; c) improving the availability of information about the current use, future plans for use and availability of spectrum.

The current EU-level radio spectrum policy programme was set up in 2012¹⁰ in order to better embrace the policy needs and to support goals and key actions outlined in the "Europe 2020: a strategy for smart, sustainable and inclusive growth" ("Europe 2020 Strategy")¹¹ and the "Digital Agenda for Europe"¹², and was included among the 50 priority actions of the "Towards a Single Market Act"¹³.

The decision that sets up the radio spectrum policy programme is a first binding legal act that specifically mentions radio spectrum in the context of IoT. It requires Member States in cooperation with the Commission to foster, where appropriate, the collective use of spectrum as well as shared use of spectrum in order to improve efficiency and flexibility, and to seek to ensure spectrum availability for the IoT including for radio-frequency identification (RFID).

Current legal framework on electronic communication and radio spectrum relevant to IoT

The legal framework on Electronic Communication:

- Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (Recast);

⁸ Directives 2002/19/EC, 2002/20/EC, 2002/21/EC and 2002/22/EC have been significantly amended and the European Electronic Communications Code has been adopted in December 2018.

⁹ DECISION 676/2002/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 7 March 2002 on a Regulatory Framework for Radio Spectrum Policy in the European Community (Radio Spectrum Decision), OJ L 108, 24.4.2002, p. 1–6.

¹⁰ DECISION No 243/2012/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 March 2012 establishing a multiannual radio spectrum policy programme, OJ L 81, 21.3.2012, p. 7–17.

¹¹ EUROPE 2020 A strategy for smart, sustainable and inclusive growth, COM/2010/2020 final.

¹² Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A Digital Agenda for Europe, COM/2010/0245 final.

¹³ COMMISSION COMMUNICATION Towards a Single Market Act for a highly competitive social market economy: 50 proposals for improving our work, business and exchanges with one another, COM(2010)608 final/2. In Article 8 (Specific Union policies) Point 6 it provides: "Member States and the Commission shall seek to ensure spectrum availability for radio-frequency identification (RFID) and other 'Internet of Things' (IoT) wireless communication technologies and shall cooperate to foster the development of standards and the harmonisation of spectrum allocation for IoT communication across Member States."

- Directives 2002/19/EC, 2002/20/EC, 2002/21/EC and 2002/22/EC, and Directive 2002/58/EC of the European Parliament and of the Council (with Implementing and amending legislation).

The legal framework applicable to the use of the radio spectrum specifically in the context of IoT constitutes of:

- Commission Decision 2006/771/EC¹⁴ (with amending decisions) – provides a general legal framework relating to the use of the radio spectrum
- Implementing decisions specifically taking into account IoT:
 - Commission Implementing Decision (EU) 2018/1538¹⁵– it harmonises spectrum by creating a sharing environment in order to "enable the introduction of technically advanced RFID solutions as well as new short-range devices enabling new types of machine-to-machine and IoT applications." (Preamble, Point 4)
 - Commission Implementing Decision (EU) 2018/637¹⁶ - harmonises use of the 900 MHz and 1800 MHz frequency bands for terrestrial systems capable of providing pan-European electronic communications services taking into account technical conditions for the IoT;
 - Commission Implementing Decision (EU) 2016/687¹⁷- harmonises the technical conditions for the availability and efficient use of specific spectrum bands in the Union for terrestrial systems capable of providing wireless broadband electronic communications services.

Standardisation

In the digital society, including IoT, standardisation becomes indispensable to ensure the interoperability¹⁸ between devices, applications, data repositories, services and networks.

Regulatory aspects

An Action Plan for Europe (2009)¹⁹ highlighted that "standardisation will play an important role in the uptake of IoT, by lowering entry barriers to newcomers and operational costs for users, by being a prerequisite for interoperability and economies of scale and by allowing industry to better compete at international level."

A Digital Single Market (DSM) Strategy for Europe²⁰ underlines the need to avoid fragmentation and to foster interoperability for the IoT to reach its potential. Standardisation is a fundamental pillar in the construction of a DSM and Data Economy, and IoT in particular.

¹⁴ Commission Decision 2006/771/EC of 9 November 2006 on harmonisation of the radio spectrum for use by short-range devices, latest consolidated version: [18/08/2017](https://eur-lex.europa.eu/eli/dec/2006/771/consolidated).

¹⁵ Commission Implementing Decision (EU) 2018/1538 of 11 October 2018 on the harmonisation of radio spectrum for use by short-range devices within the 874-876 and 915-921 MHz frequency bands (notified under document C(2018) 6535), OJ L 257, 15.10.2018, p. 57-63.

¹⁶ Commission Implementing Decision (EU) 2018/637 of 20 April 2018 amending Decision 2009/766/EC on the harmonisation of the 900 MHz and 1800 MHz frequency bands for terrestrial systems capable of providing pan-European electronic communications services in the Community as regards relevant technical conditions for the Internet of Things, OJ L 105, 25.4.2018, p. 27-30.

¹⁷ Commission Implementing Decision (EU) 2016/687 of 28 April 2016 on the harmonisation of the 694-790 MHz frequency band for terrestrial systems capable of providing wireless broadband electronic communications services and for flexible national use in the Union, OJ L 118, 4.5.2016, p. 4-15.

¹⁸ For different layers of interoperability see H. van der Veer and A. Wiles, Achieving Technical Interoperability – the ETSI Approach, ETSI White Paper No.3, 3rd edition, April 2008 and Initial report on IoT standardisation activities" – EC, 2018, available at: [see https://european-iot-pilots.eu/wp-content/uploads/2018/11/D06_05_WP06_H2020_CREATE-IoT_Final.pdf](https://european-iot-pilots.eu/wp-content/uploads/2018/11/D06_05_WP06_H2020_CREATE-IoT_Final.pdf).

¹⁹ COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS: Internet of Things – An action plan for Europe, COM(2009)278 final.

²⁰ COMMUNICATION FROM THE COMMISSION A Digital Single Market Strategy for Europe, COM/2015/0192 final.

The EC seeks a way to regulate this area without inhibiting innovation. The Standardisation Communication²¹ outlines future EU strategy in the area of standardisation.

The description of the current in the IoT standardisation was addressed by the "Initial report on IoT standardisation activities" (2018).²² The Report identifies many standards that fall either under category of a) standards for communications or b) standards for data models. The Report highlights that no standards related to security have been identified, not even from a methodology standpoint.

The Commission through Horizon 2020 IoT Focus Area is funding research into IoT integration and platforms that will address notably issues of authentication, identification and discovery in the context of IoT.

The AIOTI Working Group on IoT Standardisation works towards a structured discussion among the IoT stakeholders in order to provide consolidated technical elements for standardisation as well as guidance and recommendations.

Current Legal framework

- Regulation 1025/2012²³ - the central legal act applicable to standardisation in general. It aims at modernising and improving the European standardisation and creates a framework for a more transparent, efficient and effective European standardisation system for all industry sectors. This Regulation takes into account the fast evolution of ICT and the way in which new products and services, such as 'smart' or connected devices or the Cloud, transform markets.

The Regulation is a legal base for future Commission's actions in the field. It establishes a system whereby the Commission may decide to identify the most relevant and most widely accepted ICT technical specifications issued by organisations that are not European, international or national standardisation organisations. The possibility to use the full range of ICT technical specifications when procuring hardware, software and information technology services is expected to enable interoperability and help avoid lock-in for public administrations and encourage competition in the supply of interoperable ICT solutions.

- INSPIRE Directive - while an IoT-specific framework is to be created, there are regulations that cover standardisation and interoperability that apply to more specifically defined areas of the IoT. Example of such legislation is INSPIRE Directive²⁴ (with implementing legislation) that establishes an infrastructure for spatial information in Europe with aim to make spatial or geographical information more accessible and interoperable for a wide range of purposes.

Cybersecurity

Cybersecurity is a key issue for digitalisation in general. In the context of IoT the issue of cybersecurity is multiplied even further. Cybersecurity is a key concern for a successful take up of the IoT. Whilst IoT deployment is in its infancy, the number of cyber-attacks is bound to grow exponentially if known vulnerabilities persist as connected objects are increasingly used.

Current legal framework

The body of law directly applicable to IoT Cybersecurity includes:

²¹ COMMUNICATION FROM THE COMMISSION ICT Standardisation Priorities for the Digital Single Market, COM/2016/0176 final.

²² Initial report on IoT standardisation activities" – EC, 2018, available at: see https://european-iot-pilots.eu/wp-content/uploads/2018/11/D06_05_WP06_H2020_CREATE-IoT_Final.pdf

²³ (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council, OJ L 316, 14.11.2012, p. 12.

²⁴ Directive 2007/2/EC of the European Parliament and of the Council of 14 March 2007 establishing an Infrastructure for Spatial Information in the European Community (INSPIRE)

- Cybersecurity Act (2019)²⁵ - lays down the regulatory and institutional environment, for the establishment of European cybersecurity certification schemes for the purpose of ensuring an adequate level of cybersecurity for ICT products, ICT services and ICT processes in the Union, as well as for the purpose of avoiding fragmentation of the internal market with regard to cybersecurity certification schemes in the Union.

To this end the Cybersecurity Act promotes "**cyber-hygiene**" (simple, routine measures that, where implemented and carried out regularly by citizens, organisations and businesses, minimise their exposure to risks from cyber threats) and "**security-by-design**"(implementation of measures at the earliest stages of design and development to protect security of products, services and processes to the highest possible degree)

The future certification framework would provide a minimum level of secure authentication, from the hardware level to network integrity. This would entail some analysis of the functions with which each device is equipped, secure data processing and secure connectivity for the devices to which data are transmitted.

- Network Information Security (NIS) directive - calls for cybersecurity solutions in critical sectors, such as energy, transport, health and finance.²⁶

Protection of personal data and privacy

Privacy and protection of personal data are two fundamental rights of the EU.²⁷ DSM Strategy safeguards those fundamental rights while also encouraging innovation.

Current legal framework:

- General Data Protection Regulation (GDPR)

Many of the data processing activities involved in the operation of IoT will fall within the material scope of the General Data Protection Regulation (GDPR)²⁸ that entered into force in May 2018. The aim of the GDPR is to protect all EU citizens from private data breaches. This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.

Given that IoT devices tend to process personal data, data protection should be built into any IoT solution from the very outset and throughout the development life-cycle, as part of the principle of 'privacy by design'. Moreover, concepts of transparency, fairness, purpose limitation, data minimisation, data accuracy and the ability to deliver on data subject rights should be built into the design of the IoT product. All of this should be documented, and evidenced as part of the GDPR Principle of Accountability.

The GDPR has very specific rules with regards to when Data Protection Impact Assessment (DPIA) should be performed. DPIA is especially required in case of processing personal data using new technologies. The AOTI Guidelines on the requirements of a DPIA under the GDPR mentions IoT. It suggests that if personal data are processed using IoT it's best to check whether you need a DPIA as

²⁵ Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), OJ L 151, 7.6.2019, p. 15–69.

²⁶ Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, OJ L 194, 19.7.2016, p. 1–30.

²⁷ See Articles 7 and 8 of the Charter of Fundamental Rights of the European Union.

²⁸ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, p. 1–88, in force since May 2018.

“the innovative use or applying new technological or organizational solutions” is already one of nine criteria which are “recommended” to use in order to see whether the need for a DPIA will be likely.

If personal data is used with other types of connected devices one needs to make sure that the full IoT ecosystem - including those devices, connectivity, platforms, cloud and so on – is a secure environment with security controls and policies on the levels of these various IoT components and an ability to report as the GDPR requires. These levels also include data and information streams further along the road.

- ePrivacy Regulation (ePR)

ePR is a legislative proposal to regulate privacy in electronic communications.²⁹ It would repeal the Privacy and Electronic Communications Directive 2002 (ePrivacy Directive) and is *lex specialis* to the General Data Protection Regulation. It would particularise and complement the latter on the electronic communications data that qualify as personal data like the requirements for consent to the use of cookies and opt-outs.

The scope of the ePrivacy Regulation would apply to any business that provides any form of online communication service, uses online tracking technologies, or engages in electronic direct marketing

Liability

Liability is a key legal concept for development of the economic activity, including IoT. Due to the ecosystem complexity, IoT potentially poses a great challenge for the attribution of liability. While shared liability is not new, the interconnectedness involved in IoT is new and unique.

Regulatory approach

The main question relating to liability in the context of IoT is if the current liability system provides adequate mechanisms to handle complexity of the IoT ecosystem.

The question of liability in the context of digital technologies and solutions has been explored by The Expert Group on Liability and New Technologies created by the EC. The Expert Group consist of two formations: a) the New Technologies formation, and b) the Product Liability Directive formation.

The New Technologies formation will assess if the existing European and national liability regimes are adapted to the development of the new technologies such as Artificial Intelligence, advanced robotics, the Internet of Things and cybersecurity issues [76]. The New Technologies formation can give recommendations on how the current liability regimes should be designed if it finds them inadequate for the new technologies. The experts are expected to holistically analyse questions related to liability. In this task, the experts will not be bound by the existing legal instruments and concepts at EU and national level; they could propose new concepts.³⁰ The recommendations should address issues such as: the assignment of liability (e.g. liable person, exclusive/joint liability, the role of mandatory or voluntary insurance to cover the liability risk), the nature of liability (fault/non-fault based), whether it is necessary for the victim to establish a defect, who should bear the burden of proof and which redress possibilities insurance providers would have to recover compensated damage.³¹

The Product Liability Formation is tasked to provide expertise and assistance to the Commission in drawing up guidance on the Directive, but also to contribute to the report on the broader implications for, potential gaps in and orientations for the liability and safety frameworks for artificial intelligence (AI), the Internet of Things (IoT) and robotics.

²⁹ Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications); not adopted, under discussions in the Council of the EU.

³⁰ Call for Applications for The Selection of Members of The Expert Group on Liability and New Technologies: available at: <https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3592>

³¹ Ibidem.

Current legal regime

Currently, liability related to IoT mainly arises from the following legislation:

- GDPR – liability arises for a controller and processor in the context of personal data;
- Product Liability Directive [77]- Products liability establishes the liability of manufacturers, processors, distributors, and sellers when their products cause personal harm or property damage to others. It introduces the concept of strict liability, regardless of whether the defect is their fault. Hardware and software are subject to the rules. Since the directive provides that "product is defective when it does not provide the safety [...]" (Article 6), the liability regime is tied with the product safety legislation which aims to prevent accidents by setting common safety rules;
- E-commerce directive [78]- the e-Commerce Directive is the legal framework for "information society services" [79] in the Internal Market with the purpose to remove obstacles to cross-border online services in the EU. It establishes the "intermediary liability regime" in the area of online services, which would be relevant, for example, in the context of selling an IoT service.
 - The Directive establishes a general rule of lack of responsibility of intermediary service providers based on the specific list of conditions.

IoT -the DSM layer

The commercial innovative activities based on the IoT network are subject to the sectoral laws as well as more horizontal laws dealing with the DSM, in particular with information society services and electronic data processing. Recently, the law on the DSM has been undergoing substantial changes due to the underpinning technology advances. There are still many outdated legal solutions that call for amendment (for example the e-Commerce Directive). While they are potential candidates for serving as a legal obstacle rather than an enabler, they do form a binding legal framework.

Current legal regime

The legal regime concerned with information society services and electronic data processing will include in particular:

- E-commerce directive [78]- the e-Commerce Directive is the legal framework for "information society services" [79] in the Internal Market with the purpose to remove obstacles to cross-border online services in the EU. It establishes the "intermediary liability regime" in the area of online services, which would be relevant, for example, in the context of selling an IoT service;
- Regulation (EU) 2019/1150 [80] – it aims at ensuring that business users of online intermediation services and corporate website users in relation to online search engines are granted appropriate transparency, fairness and effective redress possibilities;
- Regulation (EU) 2018/1807 [81]- deals with the free flow of non-personal data in the EU. It is directly relevant as IoT is one of the major sources of non-personal data;
- Directive 96/9/EC [82], 2001/29/EC [83] and 2019/790 [84] - lay down rules which aim to harmonise EU law applicable to copyright and database protection as well as other related rights in the framework of the internal market, taking into account, in particular, digital and cross-border uses of protected content. It also lays down rules on exceptions and limitations to copyright and related rights, on the facilitation of licences, as well as rules, which aim to ensure a well-functioning market. It would apply to IoT in case of the processing the protected content;

- Directive 2003/98/EC (PSI) [85] with 2013 amendment [86] –set out rules on the re-use of public sector information;
- Directive (EU) 2019/1024 (recast) [87] – obliges Member States to ensure that public sector documents are re-usable for commercial or non-commercial purposes (given that the conditions set out in the directive are met). The documents can be made accessible for re-use under license, sale, dissemination, exchange or provision of information.

List of figures

| | |
|--|----|
| Figure 1. Analytical strategy for emerging technology, developed by B6 Unit | 13 |
| Figure 2. Intelligence generation process by the IoT ecosystem | 15 |
| Figure 3. IoT platform reference framework | 16 |
| Figure 4. IoT platform engineering implementation | 16 |
| Figure 5. Mozilla IoT unifying application layer. Source: [28] | 22 |
| Figure 6. AIOTI process towards IoT marketplaces. Source [29] | 25 |
| Figure 7. IoT Taxonomies viewpoints | 27 |
| Figure 8. Connected objects taxonomy..... | 30 |
| Figure 9. IDC IoT Taxonomy map. Source [43] | 35 |
| Figure 10. Keywords list generation and consolidation process | 36 |
| Figure 11. Patent inventions across the analyzed IoT application domains | 38 |
| Figure 12. Geographic distribution of the Top-10 organizations, per sector. | 40 |
| Figure 13. Patent invention registration countries and consequent market coverage. | 41 |
| Figure 14. Patents growth escalation years, per domain sector (grey = regular growth; blue = exponential growth). | 42 |
| Figure 15. Number of scientific publications on the diverse application domains. | 43 |
| Figure 16. Number of scientific publications from Europe, the country that publishes most, and the rest of the world..... | 43 |
| Figure 17. Financial landscape characterizing the IoT sectors (i.e. number of public and private companies and investors, number of exits, top investment). | 45 |
| Figure 18. Conceptual model inferred from the Twitters analysis | 46 |
| Figure 19. The SensorThings API Sensing data model. Source: OGC | 54 |
| Figure 20. The SensorThings API Tasking data model. Source: OGC | 55 |
| Figure 21. Web Thing architectural aspects. Source [2]. | 65 |
| Figure 22. Abstract architecture of W3C WoT. Source [2]. | 66 |
| Figure 23. WoT Building Blocks and their relationship with WoT Thing aspects. Source [2] | 66 |

List of tables

Table 1. IoT sensor types and sub-types. Source [41]31

Table 2. Taxonomy of IoT Sensors and domains. Source [41]31

Table 3. Technical complexity levels. Source [42]32

Table 4. System Security Level (SSL). Source [42]33

Table 5. Data Sharing Level (DTL). Source [42]33

GETTING IN TOUCH WITH THE EU

In person

All over the European Union there are hundreds of Europe Direct information centres. You can find the address of the centre nearest you at: https://europa.eu/european-union/contact_en

On the phone or by email

Europe Direct is a service that answers your questions about the European Union. You can contact this service:

- by freephone: 00 800 6 7 8 9 10 11 (certain operators may charge for these calls),
- at the following standard number: +32 22999696, or
- by electronic mail via: https://europa.eu/european-union/contact_en

FINDING INFORMATION ABOUT THE EU

Online

Information about the European Union in all the official languages of the EU is available on the Europa website at: https://europa.eu/european-union/index_en

EU publications

You can download or order free and priced EU publications from EU Bookshop at: <https://publications.europa.eu/en/publications>. Multiple copies of free publications may be obtained by contacting Europe Direct or your local information centre (see https://europa.eu/european-union/contact_en).

The European Commission's science and knowledge service

Joint Research Centre

JRC Mission

As the science and knowledge service of the European Commission, the Joint Research Centre's mission is to support EU policies with independent evidence throughout the whole policy cycle.



EU Science Hub
ec.europa.eu/jrc



@EU_ScienceHub



EU Science Hub - Joint Research Centre



EU Science, Research and Innovation



EU Science Hub

