Ferrera, Enrico; Pastrone, Claudio; Brun, Paul-Emmanuel; De Besombes, Remi; Loupos, Konstantinos; Kouloumpis, Gerasimos; O'Sullivan, Patrick; Papageorgiou, Alexandros; Katsoulakos, Panayiotis; Karakostas, Bill; Mygiakis, Antonis; Stratigaki, Christina; Caglayan, Bora; Starynkevitch, Basile; Skoufis, Christos; Christofi, Stelios; Ferry, Nicolas; Song, Hui; Solberg, Arnor; Matthews, Peter; Skarmeta, Antonio F.; Santa, José; Beliatis, Michail J.; Presser, Mirko A.; Parreira, Josiane X.; Martínez, Juan A.; Barnaghi, Payam; Enshaeifar, Shirin; Iggena, Thorben; Fischer, Marten; Tönjes, Ralf; Strohbach, Martin; Sforzin, Alessandro; Truong, Hien; Soldatos, John; Efremidis, Sofoklis; Koutalieris, Georgios; Gouvas, Panagiotis; Neises, Juergen; Hatzivasilis, George; Askoxylakis, Ioannis; Kulkarni, Vivek; Broering, Arne; Dober, Dariusz; Ramantas, Kostas; Verikoukis, Christos; Posegga, Joachim; Presenza, Domenico; Spanoudakis, George; Pau, Danilo

IoT European Security and Privacy Projects: Integration, Architectures and Interoperability

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

Published: 01/01/2018

Document Version
Publisher's PDF, also known as Version of record

Please cite the original version:
Ferrera, E., Pastrone, C., Brun, P-E., De Besombes, R., Loupos, K., Kouloumpis, G., ... Polyzos, G. C. (2018). IoT European Security and Privacy Projects: Integration, Architectures and Interoperability. In O. Vermesan, & J. Bacquet (Eds.), Next Generation Internet of Things: Distributed Intelligence at the Edge and Human Machine-to-Machine Cooperation (pp. 207-292). (River Publishers Series in Communication).

7

IoT European Security and Privacy Projects: Integration, Architectures and Interoperability

Enrico Ferrera[1], Claudio Pastrone[1], Paul-Emmanuel Brun[2], Remi De Besombes[2], Konstantinos Loupos[3], Gerasimos Kouloumpis[3], Patrick O' Sullivan[3], Alexandros Papageorgiou[3], Panayiotis Katsoulakos[3], Bill Karakostas[4], Antonis Mygiakis[5], Christina Stratigaki[5], Bora Caglayan[6], Basile Starynkevitch[7], Christos Skoufis[8], Stelios Christofi[8], Nicolas Ferry[9], Hui Song[9], Arnor Solberg[10], Peter Matthews[11], Antonio F. Skarmeta[12], José Santa[12], Michail J. Beliatis[13], Mirko A. Presser[13], Josiane X. Parreira[14], Juan A. Martínez[15], Payam Barnaghi[16], Shirin Enshaeifar[16], Thorben Iggena[17], Marten Fischer[17], Ralf Tönjes[17], Martin Strohbach[18], Alessandro Sforzin[19], Hien Truong[19], John Soldatos[20], Sofoklis Efremidis[20], Georgios Koutalieris[21], Panagiotis Gouvas[22], Juergen Neises[23], George Hatzivasilis[24], Ioannis Askoxylakis[24], Vivek Kulkarni[25], Arne Broering[25], Dariusz Dober[26], Kostas Ramantas[27], Christos Verikoukis[28], Joachim Posegga[29], Domenico Presenza[30], George Spanoudakis[31], Danilo Pau[32], Erol Gelenbe[33,34], Sławomir Nowak[34], Mateusz Nowak[34], Tadeusz Czachórski[34], Joanna Domańska[34], Anastasis Drosou[35], Dimitrios Tzovaras[35], Tommi Elo[36], Santeri Paavolainen[36], Dmitrij Lagutin[36], Helen C. Leligou[37], Panagiotis Trakadas[37] and George C. Polyzos[38]

[1]Istituto Superiore Mario Boella, Italy
[2]AIRBUS CyberSecurity, France
[3]INLECOM Systems Ltd, United Kingdom
[4]VLTN BVBA, Belgium
[5]CLMS Hellas, Greece

[6]IBM Ireland Ltd, Ireland
[7]Basile Starynkevitch, CEA, France
[8]EBOS Technologies Ltd, Cyprus
[9]SINTEF, NO
[10]TellU, NO
[11]CA Technologies, SP
[12]Department of Information and Communication Engineering, University of Murcia, Spain
[13]Department of Business Development and Technology, Aarhus University, Denmark
[14]Department of Corporate Technology, SIEMENS, Austria
[15]Odin Solutions S.L, Spain
[16]Department of Electrical and Electronic Engineering, University of Surrey, United Kingdom
[17]University of Applied Sciences Osnabrück, Germany
[18]AGT International, Germany
[19]NEC Laboratories Europe, Germany
[20]Athens Information Technology, Greece
[21]Intrasoft International, Luxembourg
[22]UBITECH LTD, Greece
[23]FUJITSU Europe, Germany
[24]Foundation for Research and Technology – Hellas (FORTH), Greece
[25]Siemens AG, Germany
[26]BlueSoft SP. z o.o., Poland
[27]Iquadrat, Spain
[28]Telecommunications Technological Centre of Catalonia (CTTC), Spain
[29]University of Passau, Germany
[30]Engineering Ingegneria Informatica S.p.A., Italy
[31]Sphynx Technology Solutions AG, Switzerland
[32]ST Microelectronics Srl., Italy
[33]Imperial College London, Great Britain & IITiS PAN, Poland
[34]IITiS PAN, Poland
[35]ITI-CERTH, Thessaloniki, Greece
[36]Aalto University, Finland
[37]Synelixis Solutions S.A., Greece
[38]Athens University of Economics and Business, Greece

Abstract

The chapter presents an overview of the eight that are part of the European IoT Security and Privacy Projects initiative (IoT-ESP) addressing advanced concepts for end-to-end security in highly distributed, heterogeneous and dynamic IoT environments. The approaches presented are holistic and include identification and authentication, data protection and prevention against cyber-attacks at the device and system levels. The projects present architectures, concepts, methods and tools for open IoT platforms integrating evolving sensing, actuating, energy harvesting, networking and interface technologies. Platforms should provide connectivity and intelligence, actuation and control features, linkage to modular and ad-hoc cloud services, The IoT platforms used are compatible with existing international developments addressing object identity management, discovery services, virtualisation of objects, devices and infrastructures and trusted IoT approaches.

7.1 BRAIN-IoT

7.1.1 BRAIN-IoT Project Vision

In line with the optimistic forecasts released in last years, Internet of Things (IoT) products and services are being more and more deployed in mass-market and professional usage scenarios, becoming a reality in our day-by-day life. Commercial and pilot deployments world-wide are progressively demonstrating the value of IoT solutions in real conditions, but also rising some concerns with respect to dependability, security, privacy and safety constraints.

The IoT technology and market landscape will become increasingly complex in the longer term i.e. 10+ years from now, especially after IoT technologies will have proven their full potential in business-critical and privacy-sensitive scenarios. An important shift is expected to happen as technology evolutions will allow to safely employ IoT systems in scenarios involving actuation and characterized by stricter requirements in terms of dependability, security, privacy and safety constraints, resulting in convergence between IoT and Cyber Physical Systems (CPS). Attracted by the trend, several organizations have started studying how to employ IoT systems also to support tasks involving actuation and control in business-critical conditions, resulting in a demand for more dependable and “smart” IoT systems. However, in order to turn such vision in reality, many issues must still be faced, including:

- Heterogeneity and (lack of) interoperability: a wide number of IoT platforms exist on the market, both cloud- based and locally hosted. Standardization and open-source initiatives are facilitating convergence among available platforms, which now employ similar usage patterns and increasingly converging sets of protocols, APIs, device models and data interchange formats. Nevertheless, full interoperability across platform still needs to be tackled on a case by case, platform by platform basis, due the wide amount of possible applications, design choices, customization options, formats and configurations that can be adopted by IoT developers and adopters.
- Difficulty of implementing "Smart Behaviours" in open collaboration context: while Machine Learning (ML) and Artificial Intelligence (AI) techniques are rapidly evolving to provide smart behaviours and solutions to increasingly complex problems, it is intrinsically difficult to generically "bind" such solutions to generic concrete IoT and CPS platforms and to make them collaborate for common tasks, since possible interactions between platforms remain unforeseen a priori.
- Security and safety: the distributed nature of IoT makes enforcement of good security practices intrinsically challenging. The market asks for IoT solutions suitable to safely support business-critical tasks, which can be deployed rapidly and with low costs. The emerging availability of actuation features in IoT systems calls for stricter security requirements. Nevertheless, many of today's IoT-based products are implemented with low awareness of potential security risks. As a result, many IoT products lack even basic, state-of-the-art security mechanisms, resulting in critical effects when such flaws deployed to mass-market scenarios.
- Enforcement of Privacy and Data Ownership policies: as IoT products are increasingly purchased and deployed by corporate and private users in their homes, work places, factories and commercial areas, privacy issues and violations become more frequent. While policies are quickly catching up by enforcing a suitable framework of rules within the EU, a comprehensive solution able to give back control of privacy aspects to users is still missing – creating significant issues when unaware users accept that their data is moved in foreign countries, outside the safe shield provided by EU regulations.
- Business models colliding with long-term resilience and survivability of IoT services: many IoT solutions on the market adopt fully centralized, cloud-oriented approaches. This is often done e.g. to ensure

that customers' devices are forced to use forever a single commercial back-end service. Such lock-in approaches create artificial monopolies, negatively affecting user rights and the overall market competitiveness. This practice introduces singular point of failures in IoT systems, making survivability and resiliency features difficult to be granted in the long term, therefore sometimes resulting in negative experiences for end users.

- Market Fragmentation and incumbency of large players: the current market of IoT platform solution is still affected by fragmentation among the many IoT platforms available each focused in specific application domain or associated technology stacks. Moreover, some market segments (i.e. the cloud-based IoT platforms market) are notably dominated by few dominant players – often based outside the EU, thus hampering the potential business opportunities for EU companies.

While EU-based initiatives and policies are doing significant amount of work to tackle such issues, often with very positive results, solutions suitable to tackle challenges arising for futuristic IoT usage scenarios are still missing. Future critical issues may be hiding under the hood already now and be ready to appear in the close future, putting at stake user acceptance and the credibility of the whole eco-system of IoT solutions vendors, integrators and adopters and hindering wider adoption of IoT solutions in potentially valuable markets.

7.1.2 Objectives

In order to tackle the aforementioned challenges, the BRAIN-IoT (*model-Based fRamework for dependable sensing and Actuation in INtelligent decentralized IoT systems*) project focuses on complex scenarios, where actuation and control are cooperatively supported by populations of heterogeneous IoT systems. In such a complex context, many initiatives fall into the temptation of developing new IoT platforms, protocols, models or tools aiming to deliver the ultimate solution that will solve all the IoT challenges and become "the" reference IoT platform or standard. Instead, usually they result in the creation of "yet-another" IoT solution or standard.

BRAIN-IoT will establish the principle that future IoT applications should *never* be supported by a single, unique, irreplaceable IoT platform. Rather future IoT services should exist within a federated/evolving environment that not only leverages current Industry Standards but is also capable of adapting to embrace future unforeseen industry developments. BRAIN-IoT

aims at demonstrating that the lack of a single IoT standard and platform, which is generally recognized as the most notable weakness of IoT, can be turned into a strength and a guarantee for market competitiveness and user protection – if the proper framework for IoT dynamicity, security and privacy is in place.

The breakthrough targeted by BRAIN-IoT is to establish a practical framework and methodology suitable to enable smart cooperative behaviour in fully de-centralized, composable and dynamic federations of heterogeneous IoT platforms. BRAIN-IoT builds on model-based approaches and open industry standards and aims at supporting rapid development and deployment of applications and services in professional usage scenarios characterized by strict constraints in terms of dependability, safety, security and privacy. The BRAIN-IoT vision is realized through seven Technical Objectives (TOs), as described in Table 7.1.

Table 7.1 BRAIN-IoT technical objectives

Technical Objective (TO)	Description
TO1: to enforce interoperability across heterogeneous IoT devices autonomously cooperating in complex tasks.	BRAIN-IoT approach to interoperability is based on the adoption of shared semantic models, dynamically linked to concrete IoT devices (sensors, actuators, controls, etc.) operating autonomously in complex scenarios. Binding of models to concrete implementations leverages mapping to open industry standards for semantic device description.
TO2: to enable dynamic smart autonomous behaviour involving actuation in IoT scenarios	Building upon shared models (TO1) BRAIN-IoT facilitates the deployment of smart cooperative behaviour, realized by means of modular AI/ML features which can be dynamically deployed to heterogeneous IoT devices in mixed edge/cloud IoT environments. Smart behaviour features are enriched by distributed data processing, federated learning, virtualization/aggregation of data/events/objects, resolution of mixed-criticality situations and conflicts, verification and context-aware self-adaptation of connectivity and real-time event-oriented, reactive approaches.

(*Continued*)

Table 7.1 Continued

Technical Objective (TO)	Description
TO3: to enable the emergence of highly dynamic federations of heterogeneous IoT platforms able to support secure and scalable operations for future IoT use cases	This is achieved by leveraging fully de-centralized peer-to-peer approaches providing linkage between modular, ad-hoc IoT self-hosted and cloud-based services through existing open standards.
TO4: to establish Authentication, Authorization and Accounting (AAA) in dynamic, distributed IoT scenarios	BRAIN-IoT introduces a holistic end-to-end trust framework for IoT platforms suitable to be employed in scenarios characterized by strict security and safety requirements, associated with actuation and semi-autonomous operations, and by special needs for secure identification, authentication of data and devices, encryption, non-deniability, as well as detection of cyber-attacks and protection against them. This is done by adopting established security protocols, joint with distributed security approaches derived by peer-to-peer systems e.g. block-chain.
TO5: to provide solutions to embed privacy-awareness and privacy control features in IoT solutions	BRAIN-IoT develops new patterns for interaction between users and IoT solutions, leveraging semantic mapping of privacy requirements towards data and service models in use in each specific use case, introducing privacy-related APIs and models. This enables the possibility to programmatically inform users about privacy policies in place, as well as enabling them to exercise fine-grained privacy controls.
TO6: to facilitate rapid model-based development and integration of interoperable IoT solutions supporting smart cooperative behaviour	BRAIN-IoT provides tools to ease rapid prototyping (development, integration) of smart cooperative IoT systems. This is achieved by extending available tools for development, integration, commissioning and management of IoT and Cyber-Physical systems.
TO7: to enable commissioning and reconfiguration of decentralized IoT-based applications	BRAIN-IoT enables end-users to dynamically commission and reconfigure their modular IoT instances, choosing among the available platforms, modules implementations and services. This is achieved by extending existing open marketplace of IoT services and data jointly with available catalogues providing open IoT enablers and integrating them with its federation framework.

7.1.3 Technical Approach

The overall BRAIN-IoT concept is depicted in Figure 7.1 following the reference model proposed by Recommendation ITU-T Y.2060. BRAIN-IoT looks at heterogeneous IoT scenarios where instances of IoT architectures can be built dynamically combining and federating a distributed set of IoT services, IoT platforms and other enabling functionalities made available in marketplaces and accessible by means of open and standard IoT APIs and protocols.

At the bottom of the conceptual architecture, the IoT Devices and Gateways layer represents all physical world IoT devices with sensing or actuating capabilities, computing devices and includes complex subsystems such as autonomous robots and critical control devices. It is worth observing that BRAIN-IoT specifically aims to support the integration into an IoT environment of devices and subsystems with actuation features that could possible give rise to mixed-criticality situations and require the implementation of distributed processing approaches. The BRAIN-IoT Management capabilities includes all the features needed to support the envisioned fully decentralized scenario dynamically integrating heterogeneous IoT Devices and Gateways as well as:

- IoT Services – third party services accessible through open interfaces and offering data or various functionalities including data storage, data statistics and analytics, data visualization;

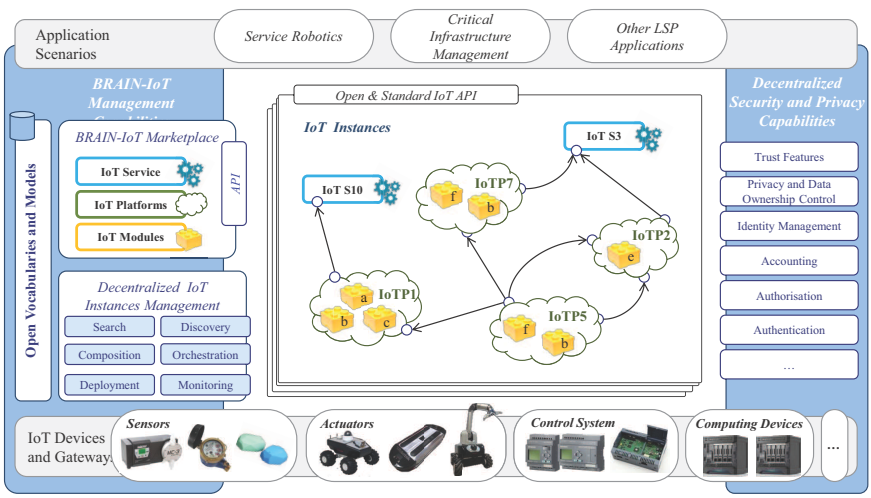

Figure 7.1 The high-level BRAIN-IoT concept.

- IoT Platforms – instances of open IoT platforms whose configuration and functionalities can be dynamically updated;
- IoT Modules – enabling functionalities (e.g., smart control features, data processing, data storage) that can be associated to a specific IoT platform instance and composed in order to meet given functional requirements.

Concerning the IoT Modules, the ones supporting smart control features are particularly relevant for the BRAIN-IoT challenging scenarios encompassing heterogeneous sensors and actuators autonomously cooperating in complex, dynamic tasks, possibly across different IoT Platforms. BRAIN-IoT will then develop a library of IoT modules implementing algorithms promoting collaborative context-based behaviours, control solutions based on Machine Learning Control, real-time data analysis and knowledge extraction techniques. Concerning the IoT Platforms, BRAIN-IoT will support different existing IoT solutions including e.g., FIWARE and SOFIA. All the above IoT building blocks can be described by a set of open and extendable vocabularies as well as semantic and behavioural models. This actually allows moving forward an easier, automated and dynamic integration within the BRAIN-IoT environment of new and existing IoT Services, Platforms and Modules available for traditional IoT applications. In fact, BRAIN-IoT defines a new meta-language, namely the IoT Modelling Language (IoT-ML), which uses the above set of vocabularies and models to formally describe an IoT Instance i.e., how a given set of IoT services and Platforms are interconnected with each other and federated and which IoT Modules are associated to the considered IoT Platforms. IoT-ML will base on existing solutions provided by OMG and W3C. The Decentralized IoT Instances management is instead in charge of offering the capabilities needed to support the dynamic composition of a given set of IoT building blocks into a specific IoT Instance. The vision is to progress from the fog computing paradigm and create distributed IoT Micro-cloud environments hosting IoT Platforms and IoT Modules and advertising their runtime capabilities. The resulting Micro-cloud environments are enhanced with management capabilities that allow search and discovery operations and their dynamic federation to form a specific IoT instance. These capabilities pave the way toward highly dynamic scenarios where IoT Modules and relevant functionalities can be composed and migrated runtime from one IoT Platform to another, complex tasks can be dynamically distributed between the edge and the cloud IoT Platforms depending on variable requirements and where IoT Instances can be fully reconfigured adding/removing runtime new IoT building blocks from the federation. BRAIN-IoT will also provide peculiar management strategies and

techniques permitting the dynamic deployment/transfer of Smart Control IoT Modules across mixed edge and cloud environments. The Decentralized IoT Instances management also handles advanced IoT Instances configurations, properly orchestrating external IoT services with other IoT building blocks active in the resulting BRAIN-IoT fog environment. Finally, monitoring components allow to continuously supervise the overall IoT Instance and relevant composite application. In this way, it is possible to check the status of the federated building blocks, provide alerting, reporting and logging mechanisms and, if needed, trigger an IoT Instance reconfiguration e.g., because of a failure in one of the adopted IoT Modules, Platforms or Services. All the described management capabilities will base on relevant industry standards i.e., W3C Web of Things and OSGi, and will be extended to support agile composition and orchestration. The scalability aspects will be taken into careful consideration to support effective discovery and search of a potential high number of IoT building blocks. The orchestration process is conceived in such a way that it is possible to import/link IoT Modules, Platforms and Services made available from a BRAIN-IoT Marketplace characterized by a relevant set of open APIs. One of the most peculiar aspects being considered in BRAIN-IoT is the management of actuation capabilities in the considered Fog environment. In this context, the possibility to easily develop the previously introduced smart control features is pretty relevant. To this aim, BRAIN-IoT will evolve from already existing solutions, such as Eclipse Papyrus, and develop Model Binding and Synthesis tools extended to support the BRAIN-IoT open vocabularies and models, the IoT-ML and other IoT related standards. The resulting toolset will be used to develop novel Smart Control Features that could be possibly published as IoT Modules in the BRAIN-IoT Marketplace, as depicted in Figure 7.2.

Finally, Figure 7.3. summarizes the above description of the BRAIN-IoT environment offering a view of possible configurations of an IoT Instance with different distribution of the IoT building blocks between edge and cloud.

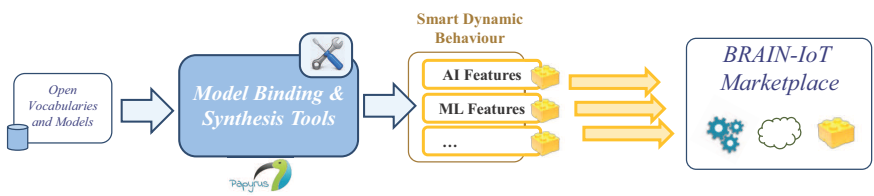

Figure 7.2 BRAIN-IoT development concept.

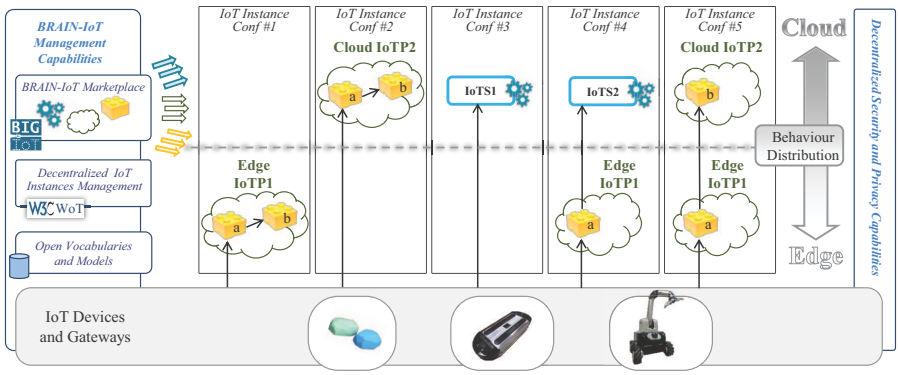

Figure 7.3 BRAIN-IoT deployment concept.

7.1.4 Security Architecture Concept

From the security and privacy perspective, IoT currently presents two main inherent weaknesses:

- Security is not considered at the design phase,
- As of today, no solution is offering a complete end-to-end security approach for any kind of devices (from the temperature sensor, the smoke detector, to the robot).

Existing systems don't apply the "secure-by-design" concept where security is seen as one of the major constraint of the system. To provide secure IoT solutions, modelling and analysis need to be integrated in the design and validation of application scenarios and IoT architectures. If the focus moves to a scenario where different heterogeneous building blocks are dynamically composed, additional security and privacy concerns arise. As a consequence, BRAIN-IoT provides a methodology to address security in the considered fog environment, based on an iterative process, allowing to take into account new scenarios. More specifically, BRAIN-IoT extend the successful methods of attack tree modelling and quantitative analysis to support secure composable IoT systems. This extension enables transparent risk assessment of IoT security architectures, i.e., it will address the needs and potential risks involved in an IoT environment specifying when and where to apply security controls in an understandable way thus raising user-awareness and trustworthiness. The results of the analysis are specific technical requirement to implement for each use case/scenario in order to reach the targeted security level.

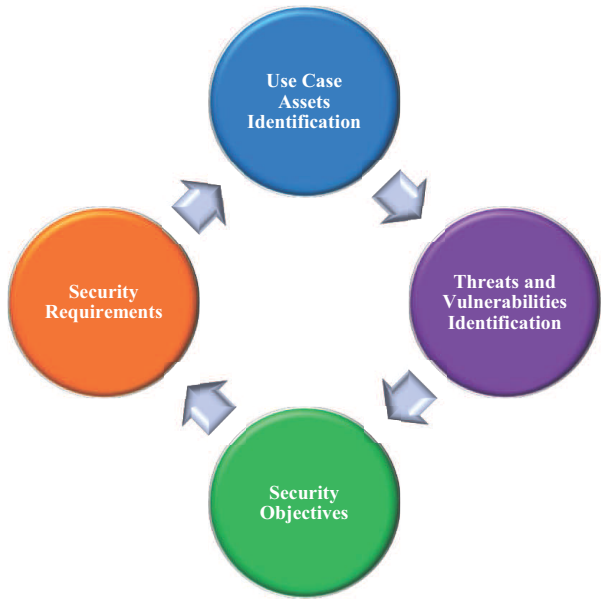

Figure 7.4 Iterative risk analysis methodology.

Second, existing security solution for IoT have many weaknesses, such as:

- Lot of flow disruption (with network component accessing data in clear text)
- Some protocol chooses to downgrade security algorithm to fit performance constraints,
- State-of-the-art solution are complex to set up in decentralized environment.

In order to provide a new approach, BRAIN-IoT integrates innovative Decentralized Security and Privacy Capabilities including Authentication, Authorization and Accounting for the overall distributed fog environment and end-to-end security for IoT data-flows. This security layer is based on a combination of well-established standards, such as PKI, with more innovative solution, stateless oriented, to fit the constraints of any kind of IoT (low power, low bandwidth, etc.)

A cross-platforms framework facilitating the adoption of privacy control policies is also hosted in the BRAIN-IoT environment. The objective is to provide end users with the means to easily monitor and control which data to – collect and to who make it available.

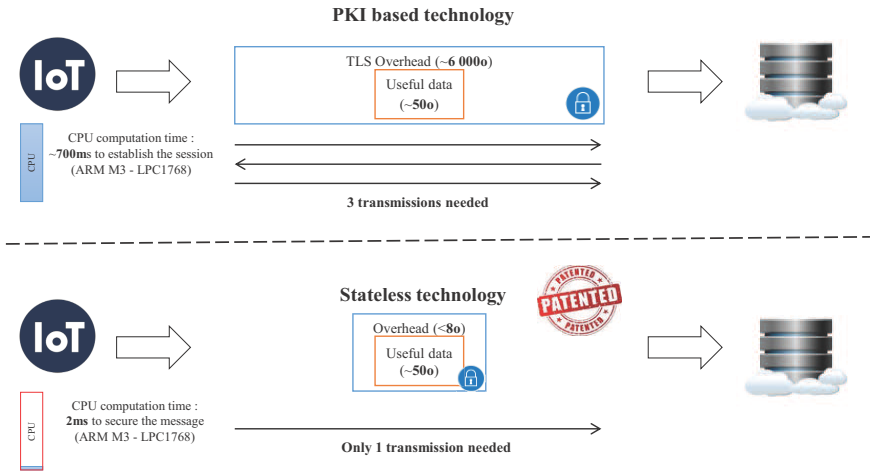

Figure 7.5 Decentralised security and privacy capabilities.

7.1.5 Use Cases and Domain Specific Issues

The overall depicted concept draws requirements and challenging use cases from IoT applications in two usage scenarios, namely Service Robotics and Critical Infrastructure Management, which provide the suitable setting to reflect future challenges in terms of dependability, need for smart behaviour, security and privacy/data ownership management which are expected to become more significant and impacting in the long-term (10+years).

7.1.5.1 Service robotics

The Service Robotics use case will involve several robotic platforms, like the open-source Robotics Operating System (ROS), which need to collaborate to scan a given warehouse and to assist humans in a logistics domain. The term Service Robotics is generally related to the use of robots to support operations done by humans and the logistics domain is one of the more interesting, for the presence of several tasks, where the robots can help the workers, making their tasks easier and safer. As example, they can cooperate to move a heavy object from one place to another. At the same time, robots involved in the scenario should scan the whole warehouse and update in real-time informative interfaces for the managers and the workers (e.g. warehouse's map), sharing the collected information. In addition, to the information related to the maps of the whole monitored area, the connected robots will also be equipped with a set of sensors, which will allow collecting interesting info, like room

temperature, presence of humans or presence of obstacles in the robot path. Since several robots collaborate to collect the information, they can keep the status of the area updated in real-time and balance the effort required among them. At the beginning, the robots are configured with some default information, like the map of the warehouse. Then, this information is updated in real-time, while the robots perform their main tasks. The demonstration use-case proposed will include both real-time collection of data and control of the included robots. Particularly, the actuation of these robots will be an interesting test-bed for the platform, to demonstrate how the solutions developed by BRAIN-IoT allow to control remotely, in a standard way, the complex devices involved in this scenario.

The BRAIN-IoT solution enables the service robotics scenario, demonstrating how the tool-chain and marketplace developed by the project can be used to enable the cooperation of the different robots. In the envisioned scenario, the BRAIN-IoT toolkit will be leveraged to design and test all the aspects of the use case: the behaviours of the robots, the interactions with humans and the cooperation of involved robots, to do specific tasks. The use of the BRAIN-IoT toolkit will enable to limit the development of new ad-hoc software components, indeed, where possible, the solution will be based on open-source components and services already developed in other IoT platforms, provided to the developers through the BRAIN-IoT's marketplace and interconnected using the services and tools developed in the project. This scenario described will involve also several security aspects. Mechanisms of encryption and authentication will be adopted in the whole final solution, to guarantee the protection of the data exchanged and of the users' privacy. To avoid inappropriate use of the robots by malicious users and to avoid possible incidents due to remote control (i.e. authorized workers that try to control the robots remotely, without a correct visual of what is happening in the warehouse), techniques of indoor localization are considered to guarantee that only workers located in specific zones near the robots can control them. Furthermore, the solution will protect the privacy of users, anonymizing the data collected, to avoid sharing users' info, also if the data are stolen by malicious users.

7.1.5.2 Critical infrastructure management

The Critical Water Infrastructure Monitoring and Control use case focuses on the management of the water urban cycle in metropolitan environment of Coruña. The base of this system will be made of a complex portfolio of probes, meters, sensors, devices and open-data sources deployed on the

field, including: water, flow and pressure meters on the water mains; smart devices, which measure the main chemical-physical characteristics of water; pluviometers, which can monitor the level of rainwater in a specific zone, water circular pumps, which can be used to control the flow of liquids in heating systems. These devices will be geographically distributed, heterogeneous and will be provided by different owners: directly by the water utility, by end-users themselves or by third-party service providers, like, SMEs providing ancillary water services. For this reason, there will be many different data involved in these scenarios: meteorological open data, reservoir water level data, purification data, distribution data in the various subsystems, customer data in urban water supply processes, sewage collection and sewage treatment data in different subsystems. The collection of all these data will allow to provide value-added services, like showing to the client, commercial or not, the quality of the water provided to them or the possibility to react quickly to critical situation and to do predictive maintenance, through the ability to detect anomalous behaviours and to fix them, before they become an issue difficult to be fixed.

The BRAIN-IoT solution will enable this scenario, allowing to collect data from all the different domains and to actuate the devices where needed. The WoT-based approach used for the design of the platform, will be leveraged to collect the data, provided by different public and private IoT platforms, using heterogeneous protocols and data formats. Furthermore, BRAIN-IoT focuses particularly to design and develop ways to control devices abstracted by these solutions. For example, the system needs to allow the managers to control the circulator pumps, regulating the fluid flow in heating system, to avoid problems or to react to some critical situation detected through the monitoring sensors. The collection of the data about water consumption from different sources generates risks about privacy protection. Indeed, the data can be shared with public entities or third-party services providers for several purposes, like statistical measures. To do this, the data need to be associated with all the potentially interesting contextual information (i.e. Position of the data, timeslot when the data have been measured and so on) but removing the association with all the personal info of the entity, related with that data. Finally, security mechanisms will be used for the actuation of devices that is potentially a dangerous task, which must be executed only by expert personal that need to know well what they are doing and the context in which the device is operating. For this reason, mechanisms of accounting, authentication and authorization will be used to guarantee that only authorized expert users are able to do these tricky operations.

7.2 Cognitive Heterogeneous Architecture for Industrial IoT – CHARIOT

7.2.1 Introduction

Recently, cloud Computing as well as Internet of Things (IoT) technologies are rapidly advancing under the concept of future internet. Numerous IoT systems and devices are designed and implemented following industrial domain requirements but most of the times not considering recent risk relating to openness, scalability, interoperability as well as application independence, leading to a series of new risks relating to information security and privacy, data protection and safety. As a result, securing data, objects, networks, infrastructure, systems and people under IoT is expected to have a prominent role in the research and standardization activities over the next several years. CHARIOT EC co-funded, research project, clearly recognises and replies to this challenge, identifying needs and risks and implementing a next generation cognitive IoT platform that can enable the creation of intelligent IoT applications with intelligent shielding and supervision of privacy, cybersecurity and safety threats, as well as complement existing IoT systems in non-intrusive ways and yet help guarantee robust security by placing devices and hardware as the root of trust. The scope of this article is to provide a detailed overview of the CHARIOT vision, technical objectives and overall solution, a high-level presentation of the system architecture as the project approaches in the design of the CHARIOT solution and platform.

7.2.2 Business Challenge and Industrial Baselines

The CHARIOT project activities are aligned with actual business and industrial requirements on the recent needs on data safety, security and privacy over modern IoT systems following demands of highly increasing numbers of IoT devices. It is expected that by 2025, there will be 75 Billion IoT-connected devices World Wide while spending on IoT devices and services reached $2 trillion in 2017, with China, North America, and Western Europe accounting for 67% of all devices [8]. This growth in connected devices is anticipated accelerate due to a rise in adoption of cross-industry devices (LED lighting, HVAC systems, physical security systems and lots more). On top of this CHARIOT also recognizes various IoT security breaches that have been dominating headlines, while 96% of security professionals expect an increase in IoT breaches this year [13]. In the direction of a more secure IoT infrastructure, there have been some requests for government regulation of the

IoT, asserting that IoT manufacturers and customers are not paying attention to the security of IoT devices [14]. CHARIOT has clearly recognized the above requirements and has an aligned set of objectives towards increase of security, privacy and safety of industrial IoT networks and components.

7.2.3 The CHARIOT EC, Research Project – Vision and Scope

CHARIOT (Cognitive Heterogeneous Architecture for Industrial IoT) is an EC, co-funded, research project granted under the IoT-03-2017 – R&I on IoT integration and platforms as a Research and Innovation (RIA) EC topic. The CHARIOT consortium consists of research and innovation organisations from major research streams all merged into the CHARIOT solution providing the competence to deliver a 'holistic approach addressing Privacy, Security and Safety of IoT operation in industrial settings with safety critical elements'. The consortium includes competences in the fields of Project management and IoT governance (INLECOM, UK), Cognitive Architectures & Platforms for IoT (IBM, Ireland), Static source code analysis tools (CEA, France), Analytics Prediction models and Dashboard development (EBOS, Cyprus) as well as IoT deployment architectures, cloud/fog technologies (VTLN, Belgium, TELCOSERV, Greece), security including cybersecurity (ISC, ASPISEC, Italy) and integration aspects (CLMS, Greece).

CHARIOT provides a design method and cognitive computing platform supporting a unified approach towards Privacy, Security and Safety (PSS) of IoT Systems including the following innovations summarised below:

- A **Privacy and security protection method** building on state of the art Public Key Infrastructure (PKI) technologies to enable the coupling of a pre-programmed private key deployed to IoT devices with a corresponding private key on a Blockchain system. This includes the implementation of security services utilising a cryptography-based approach and IoT security profiles all integrated to the CHARIOT platform.
- A **Blockchain ledger** in which categories of IoT physical, operational and functional changes are both recorded and affirmed/approved by the various run-time engines of the CHARIOT ecosystem while leveraging existing blockchain solutions in innovative ways.
- **Fog-based decentralised infrastructures** for Firmware Security integrity checking leveraging Blockchain ledgers to enhance physical, operational and functional security of IoT systems, including actuation and deactivation.

- An **accompanying IoT Safety Supervision Engine** providing a novel solution to the challenges of securing IoT data, devices and functionality in new and existing industry-specific safety critical systems.
- A **Cognitive System and Method** with accompanying supervision, analytics and prediction models enabling high security and integrity of Industrials IoT.
- **New methods and tools for static code analysis** of IoT devices, resulting in more efficient secure and safer IoT software development and V&V.

CHARIOT is closely following a business and industrially driven approach to align the developed technologies and outcomes to actual industrial needs in the fields of transport, logistics etc and in general domains of IoT applications. With this vision, CHARIOT, will apply its outputs and recent developments to three living labs in order to demonstrate its realistic and compelling heterogeneous solutions through industry reference implementations at representative scale, with the underlying goal of demonstrating that Secure, Privacy Mediated and Safety IoT imperatives are collectively met, in turn delivering a key stepping stone to the EU's roadmap for the next generation IoT platforms and services. The actual living labs will be implemented in the industrial framework of TRENITALIA (rail), Athens International Airport (transport) and IBM Ireland (smart buildings) [9, 10].

7.2.4 CHARIOT Scientific and Technical Objectives

We present below a summary of the CHARIOT scientific and technical objectives as the main scope and outcomes of the CHARIOT unified design method and cognitive computing platform supporting a unified approach towards Privacy, Security and Safety (PSS) of IoT Systems, that places devices and hardware at the root of trust, in turn contributing to high security and integrity of industrial IoT.

- **Objective 1:** Specify a Methodological Framework for the Design and Operation of Secure and Safe IoT Applications addressing System Safety as a cross cutting concern. The CHARIOT design method will bridge the systems engineering gaps that currently exists between a) the formal safety engineering techniques applied in the development and testing of safety critical systems and b) the rapidly evolving and ad-hoc manner in IoT devices are developed and deployed. This includes classification and usage guidelines of relevant standards and platforms,

introduction of new concepts and methods for coupling pre-programmed private security keys on the IoT device with a Blockchain system and ledger to enhance its security and privacy protection and guarantee that only authorised entities who have a matching key can influence operation, function and change, thereby invalidating the potential for a substantial spectrum of cyber-attacks and significantly before they become actual exploits. Developments will also include a specialized static source code analysis tool and cross-compiler to help avoid safety defects and add some meta-data into the binary permitting that binary executable to be suitably "filtered" or "authenticated" by gateways and, in turn, shielding against cyber-attacks while consolidate all the above into the CHARIOT IoT Design Method.

- **Objective 2:** Develop an Open Cognitive IoT Architecture and Platform (the CHARIOT Platform), that exhibits intelligent safety behaviour in the diverse and complex ways in which the safety critical system and the IoT system will interact in a secure manner. This includes the creation of an open IoT Cognitive Architecture for a "Web-of-Things" like environment, supporting a range of solutions and applications interacting with highly distributed, heterogeneous and dynamic IoT and critical safety system environments. Under this objective, CHARIOT will also provide interfacing to a topological representation and functional behaviour models of IoT system components and safety profiles as well as a integrated IoT Platform by enhancing the existing state of the art in cognitive computing platforms and build the additional CHARIOT safety and privacy features through open APIs and including security services utilising the Blockchain technology, the IoT security profiles and fog computing services.
- **Objective 3:** Develop a runtime IoT Privacy, Security and Safety Supervision Engine (IPSE) which will act continuously to understand and monitor the cyber-physical ecosystem made up of the IoT devices, safety critical systems and a PSS policy knowledge-base in real-time. This cognitive engine will ensure that potentially endangering behaviours of the IoT system are predicted and avoided and, where that is not possible, handled in an agreed manner in conjunction with safety critical systems runtime environments to avoid a breach of the safety constraints. IPSE will include four innovative cognitive applications: A Privacy Engine based on PKI and Blockchain technologies, a Firmware Security integrity checking, an IoT Safety Supervision Engine (ISSE) and an Analytics Prediction models and Dashboard.

- **Objective 4:** Test and validate against Industrial IoT safety in three Living Labs (LLs) addressing different industrial areas in IoT safety: in transport (rail and airports) and in buildings. The LLs will be used to demonstrate the capabilities of the proposed approach and provide compelling and representative industry use cases with associated test data that will effectively demonstrate an integrated end-to-end application for how the broader CHARIOT approach to security, privacy and safety will be applied in different industry-representative contexts at enterprise scale.
- **Objective 5:** Ensure large outcomes scale up through wide dissemination, exploitation actions and a Capacity Building Programme aiming at infrastructure sustainability, organisational development, and human capital development through training on the practical use of the CHARIOT Concepts, Capabilities, Services and Platform Offering.

7.2.5 Technical Implementation

The technical implementations in CHARIOT will be performed in a series of phases, perfectly aligned to the project scientific objectives presented above. These include the design, development, integration and testing of several key-components as will be presented in the chapters that follow.

7.2.5.1 The CHARIOT Open IoT cognitive cloud platform

The CHARIOT cognitive platform comprises of a set of functions, logical resources and services hosted in a cloud data centre supporting a range of cognitive solutions and application interacting with an ecosystem of highly distributed, heterogeneous and dynamic IoT and critical safety system environments. This module provides connectivity and intelligence, supporting actuation and control features as required by the final applications. It takes advantage of an existing IoT platform (IBM's Watson IoT [15]) to demonstrate concept and capability and will also support integration with other safety, privacy and machine-learning cloud services via relevant open APIs, thus supporting third party integration and innovation. Through such interfaces, the CHARIOT platform will subsequently be compatible with existing international developments, addressing object identity management, fog, discovery services, virtualisation of objects, devices and infrastructures and trusted IoT approaches. The CHARIOT platform is being designed respecting open principles.

While the open nature of the architecture does not preclude the adoption of specific vendor technologies in the initial platform Proof-of-Concept (PoC) implementation for the living labs, the architecture will be intentionally designed with open interfaces such that individual middleware and components can be easily substituted with alternatives in future implementations. The platform will also explore the development and deployments of probes to provide methods of collecting information on the IoT devices and on the safety-critical-systems in real-time, in turn facilitating the creation of a topological representation and functional behaviours of the IoT systems by the Safety Supervision Engine.

The cognitive engine will be used to test the concept of adapting autonomously, instructing the "system" to behave in intended ways and perform required updates and changes through authorised actors. Based on a pattern of events evidenced in ledgers, the cognitive system will adapt/instruct the IoT system(s) to adapt in appropriate ways based on leveraging innovative machine learning and data mining approaches.

PKI and Blockchain Technologies

Leveraging existing blockchain technologies along with traditional PKI schematics enables CHARIOT to revolutionize the field of identity management and access control. Blockchain acts as the backbone of the system by enabling trust between the various CHARIOT services as well as between the gateways and the IoT sensors within the network. The implementation will be based on a permissioned blockchain that will become the mediator of any communications occurring within the network.

7.2.5.2 Static code analysis and firmware security tool

A significant component of the CHARIOT overall solution is the development and enhancement of a free software cross-compilation toolset – leveraging on existing open source technologies – for IoT engineers designing IoT systems and developing source code running on them. Strong highly safety-critical IoT software requires a costly, but extensive, formal methods approach [11], in which developers agree to put a lot of efforts in formally specifying then analysing their source code and using proof assistants to ensure lack of bugs (w.r.t. some explicitly, detailed and formalized specification). But the CHARIOT project aims to help less life-critical IoT software developers by providing them with a tool to help them in developing IoT software and better use of existing free software IoT frameworks. This will be an open software toolset that assists IoT software developers, particularly as

not experts in computer science but a competent engineer in a specific industrial domain (railroad, automotive, smart building, maritime, etc.), so even heuristic source code analysis techniques (leveraging above some formal methods approaches) can improve his/her coding productivity. This tool will be developed as part of the CHARIOT solution and a plugin/extension module for GCC based compilers that the software industry is currently using and will be executed at compilation/linking stage and will use meta-programming techniques to foster "declarative" high-level programming styles. This will enable the developers (as the IoT device firmware developers) to identify most safety critical functions executed at the IoT device or gateway level. Also, firmware compiled with that toolset will carry some cryptographic signature to enable filtering of firmware updates in the gateway.

7.2.5.3 Integrated IoT privacy, security and safety supervision engine

This engine is a set of novel runtime components which act in concert to understand and monitor the cyber-physical ecosystem made up of the IoT gateway and devices, the safety critical systems and safety/security policy knowledge-base. The Privacy Engine utilises existing security protocols and technologies such as Blockchain to provide a strong foundation for the trusted interchange of information about and between the participants in the system-of-systems. The Safety Engine also analyses the IoT topology and signal metadata relative to the relevant safety profiles and applies closed-loop machine-learning techniques to detect safety violations and alert conditions. The objective of this engines is to develop a cognitive engine that will leverage the Cyber-Physical topological representation of the system-of-systems combined with the security/safety-polices to provide a real-time risk map will allow for both static analysis and continuous monitoring to assess safety impact and appropriate response actions.

The supervision engine will be responsible for interacting with the CHARIOT IoT platform, providing the centralised intelligence and control functionality for applying the necessary privacy, security, and safety policies to all components in the IoT system of systems, monitor IoT devices and systems to detect abnormalities in their behaviour and analyse their causes, maintain an internal topological representation of the constantly evolving IoT system of systems and collect and represent PSS policies and the threat intelligence in the topology to provide a real-time risk map, impact assessment and triggering of appropriate response actions. The engine will also maintain safety, security and privacy even when unknown devices and

sensors are connected to the network, ensuring that they do not interfere to the normal operation of existing IoT components, assess the topology to detect whether the IoT ecosystem has entered or is predicted to be advancing towards an abnormal (unsafe/insecure) state, and automatically activate a safety remediation in response to this unsafe state, to reduce the impacts on users and other IoT components and restrict abnormal operations and allow operations of safe functions to maintain at reduced level the operation of the controlled system.

7.2.5.4 Analytics prediction models user interface

This system component is an innovative cognitive web application, which constitutes together with other relevant components – such as the Privacy and the IoT Safety Supervision Engine – the IPSE. The application collects the data received by the various IoT gateways and sensors in the fog network and using appropriate algorithms, Analytics Prediction models will be created and presented through a user friendly configurable dashboard.

This module will be the advanced-intelligence dashboard for both understanding of the IoT ecosystem topology and for post data analytical purposes to assist in the refinement and improvements of PSS policies while at the same time act as the interface between the CHARIOT platform and the system operator/user.

7.2.6 System Demonstration, Validation and Benchmarking

The overall system operation will be demonstrated and validated via full integration to the actual operating environments and infrastructures of three industrial sites over precise key-performance-indicators that contribute to the separate business environment and value. The three key selected sites (living labs, LLs) will be: a) Trenitalia (transport – rail) b) IBM Ireland business campus (smart buildings) and c) Athens international airport (transport – airport). Details on the three separate cases have been included below:

7.2.6.1 Living lab 1: Trenitalia

The primary objective in this LL is to enhance the safe operation of the Italian railways service. This includes, reduction of risk to passengers and personnel, compliance with appropriate regulations, and creation of a safe and efficient operating environment in the railways. At the same time this use case will focus on utilizing the feed from IoT used to monitor electrical and mechanical components dedicated on assessing energy consumption and

dispatch them to the on-board control servers and the land-based central control system. The application of the CHARIOT tool will facilitate the timely recognition of sensors malfunction, along with prediction of maintenance requirements.

7.2.6.2 Living lab 2: IBM business campus

In this LL, the objective will be to enable the continued IoT evolution of the IBM technology campus from a set of individuals "automated/smart" buildings into to a truly cognitive IoT environment that provides a safer and more efficiently managed working environment for all IBM staff, customers and visitors and also to use the knowledge gained to help drive advancements in Cognitive IoT to a global scale by reflecting it in IBM products and services.

7.2.6.3 Living lab 3: Athens international airport

The application of CHARIOT in this Living Lab will address safety of airport Infrastructures, enhance protection of Athens airport's facilities from physical and cyber threats. To achieve this, CHARIOT will enhance airports capability on early detection/prediction of hazardous situations, in parallel with reduction in false positive alarms that disrupt airport operations.

7.2.7 Summary and Discussion

This chapter provides the overall concept of the CHARIOT project and business orientation. It summarizes the project scope and business value as derived from actual industrial needs in the framework of safety, security and privacy of industrial IoT. CHARIOT started in January 2018 and it currently in the stage of requirements extraction and definition of the system overall architecture as this is aligned with the project end-users (living labs) that drive and validate the technological developments. Currently, CHARIOT is also defining the technical and methodological framework of the overall solution adapted for the cases of the three living labs that is going to evolve into the concise implementations for the next project phases, in a systematic approach to Privacy, Security, and Safety in Industrial IoT environments, using a strategic/objectives driven systematic way, in a process of continuous improvement. CHARIOT intends to have a first implementation of the system within the first months of 2019 and will integrate this to all infrastructures involved and as planned. This project has received funding from the

European Union's Horizon 2020 research and innovation programme under grant agreement No 780075". The authors acknowledge the research outcomes of this publication belonging to the CHARIOT consortium.

7.3 ENACT: Development, Operation, and Quality Assurance of Trustworthy Smart IoT Systems

Until now, IoT system innovations have been mainly concerned with sensors, device management and connectivity, with the mission to gather data for processing and analysis in the cloud in order to aggregate information and knowledge [16]. This approach has conveyed significant added value in many application domains, however, it does not unleash the full potential of the IoT [82]. The next generation IoT systems need to perform distributed processing and coordinated behaviour across IoT, edge and cloud infrastructures [17], manage the closed loop from sensing to actuation, and cope with vast heterogeneity, scalability and dynamicity of IoT systems and their environments. Moreover, the function and correctness of such systems has a range of criticality from business critical to safety critical. Thus, aspects related to trustworthiness such as security, privacy, resilience and robustness, are challenging aspects of paramount importance [16]. Therefore, the next generation of IoT systems must be trustworthy above all else. In ENACT, we will call them trustworthy smart IoT systems, or for short; trustworthy SIS.

Developing and managing the next generation trustworthy SIS to operate in the midst of the unpredictable physical world represents daunting challenges. Challenges, for example, that include that such systems always work within safe operational boundaries [18] by controlling the impact that actuators have on the physical world and managing conflicting actuation requests. Moreover, the ability of these systems to continuously evolve and adapt to their changing environments are essential to ensure and increase their trustworthiness, quality and user experience. DevOps is a philosophy and practices that covers all the steps from concept to delivery of a software product. In ENACT we see DevOps advocating a set of software engineering best practices and tools, to ensure Quality of Service while continuously evolving complex systems, foster agility, rapid innovation cycles, and ease of use [19]. DevOps has been widely adopted in the software industry. However, there is no systematic DevOps support for trustworthy smart IoT systems today [18–20]. The aim of ENACT is to enable DevOps in the domain of trustworthy smart IoT systems.

7.3.1 Challenges

The key research question of ENACT is thus the following: "*how we can tame the complexity of developing and operating smart IoT systems, which (i) involve sensors and* ***actuators*** *and (ii) need to be* ***trustworthy****?"*. Our fundamental approach is to evolve DevOps methods and techniques as baseline to address this issue. We thus refine the research question as follows: "*how we can apply and evolve the DevOps tools and methods to facilitate the development and operation of trustworthy smart IoT applications?"*.

Challenge 1: Support continuous delivery of trustworthy SIS. Currently there is little effort spent on providing solutions for the delivery and deployment of application across the whole IoT, edge and cloud space. In particular, there is a lack of languages and abstractions that can be used to support the orchestration of software services and their continuous deployment on heterogeneous devices [21] together with the relevant security mechanisms and policies.

Challenge 2: Support the agile operation of trustworthy SIS. The operation of large-scale and highly distributed IoT systems can easily overwhelm traditional operation teams. Other management models such as NoOps and Serverless Computing are evolving to solve this problem. Whatever the operations management model the major challenges will be to improve efficiency and the collaboration with development teams for rapid and agile evolution of the systems. Currently, there is a lack of mechanisms dedicated to smart IoT systems able to *(i)* monitor their status, *(ii)* indicate when their behaviour is not as expected, *(iii)* identify the origin of the problem, and *(iv)* automate typical operation activities. Furthermore, the impossibility of anticipating all the adaptations a system may face when operating in an open context, creates an urgent need for mechanisms that will automatically maintain the adaptation rules of a SIS.

Challenge 3: Support continuous quality assurance strengthening trustworthiness of SIS. Maintaining quality of service is a complex task that needs to be considered throughout the whole life-cycle of a system. This complexity is increased in the smart IoT system context where it is not feasible for developers and operators to exhaustively explore, anticipate or resolve all possible context situations that a system may encounter during its operation. This is due to the open context in which these systems operate and as a result can hinder their trustworthiness. Quality of Service is particularly important when the system can have an impact on the physical world through

actuators. In addition, testing, security assurance as well as the robustness of such systems is challenging [20].

7.3.2 The ENACT Approach

DevOps seeks to decrease the gap between a product design and its operation by introducing software design and development practices and approaches to the operation domain and vice versa. In the core of DevOps there are continuous processes and automation supported by different tools at various stages of the product life-cycle. In particular, the ENACT DevOps Framework will meet the challenges below and support the DevOps practices during the development and operation of trustworthy smart IoT systems. ENACT will provide innovations and enablers that will feature trustworthy IoT systems built by implementing the seven stages of the process as depicted in Figure 7.6.

Plan: The ENACT approach is to introduce a new enabler to support the risk-driven and context-aware planning of IoT systems development, including mechanisms to facilitate the selection of the most relevant and trustworthy devices and services to be used in future stages.

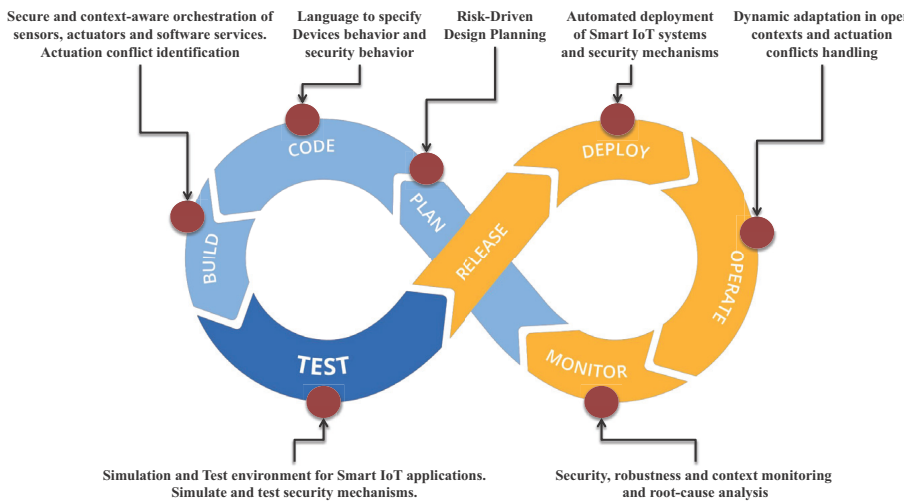

Figure 7.6 ENACT support of DevOps for trustworthy smart IoT systems.

Code: The ENACT approach is to leverage the model-driven engineering approach and in particular to evolve recent advances of the ThingML [21] language and generators to support modelling of system behaviours and automatic derivation across vastly heterogeneous and distributed devices both at the IoT and edge layers.

Build and Deploy: The ENACT approach is to provide a new deployment modelling language to specify trustworthy and secure orchestrations of sensors, actuators and software components, along with the mechanisms to identify and handle potential actuation conflicts at the model level. The deployment engine will automatically collect the required software components and integrate the evolution of the system into the run-time environment across the whole IoT, Edge and Cloud space.

Test: ENACT enablers will allow continuous testing of smart IoT systems in an environment capable of emulating and simulating IoT and edge infrastructure by targeting the constraints related to the distribution and infrastructure of IoT systems. This system is intended to be able to simulate some basic attacks or security threats.

Operate: The ENACT approach will provide enablers for the automatic adaptation of IoT systems based on their run-time context, reinforced by online learning. Such automatic adaptation will address the issue of the management complexity. The complexity of open-context IoT systems can easily exceed the capacity of human operation teams. Automatic adaptation will improve the trustworthiness of the smart IoT system execution.

Monitor: The ENACT approach is to deliver innovative mechanisms to observe the: status, behaviour, and security level of the running IoT systems. Robust root cause analysis mechanisms will also be provided.

In addition to the DevOps related contributions identified above, the ENACT DevOps Framework will provide specific cross-cutting innovations related to trustworthiness, which can be seamlessly applied, in particular based on the following ENACT concepts:

Resilience and robustness: The ENACT approach is to provide novel solutions to make the smart IoT systems resilient by providing enablers for diversifying IoT service implementations, and deployment topologies (e.g., implying that instances of a service can have a different implementation and operate differently, still ensuring consistent and predictable global behaviour). This will lower the risk of privacy and security breaches and significantly reduced impact in case of cyber-attack infringements.

Security, privacy and identity management: The ENACT approach is to provide support to ensure the security of trustworthy SIS. This not only includes smart preventive security mechanisms but also the continuous monitoring of security metrics and the context with the objective to trigger reactive security measures.

7.3.3 ENACT Case Studies

Three use cases from the Intelligent Transport Systems (Rail), eHealth and Smart Building application domains will guide, validate and demonstrate the ENACT research.

7.3.3.1 Intelligent transport systems

This use case will assess the feasibility of IoT services in the domain of train integrity control, in particular for the logistics and maintenance of the rolling stock and on-track equipment. In this domain, the infrastructure and the resources that should be used are usually expensive and require a long-time in planning and execution. Therefore, the usage of the rail systems must be optimised at maximum, following security and safety directives due to the critical and strategic characteristics of the domain. This use case will involve logistic and maintenance activities. Within the ENACT scope, it will be focused on the logistics activities.

A logistic and maintenance scenario will be defined with the aim to provide information about the wagons that form the rolling stock. This scenario will cover not only optimizing cargo storing and classification, but also providing the appropriate resources to assure the correct functioning of the system. These will be only possible if the train integrity is confirmed when the different wagons are locked and moving together. This situation will assure the proper transportation of cargo or passengers, avoiding possible accidents. This use case will involve an infrastructure consisting of large sets of on-board sensors (e.g., Integrity Detector, Asset data info, Humidity and temperature sensors) and multiple gateways interacting with cloud resources.

7.3.3.2 eHealth

The eHealth use case will develop a digital health system for supporting and helping various patients staying at home to the maximum extent possible either during treatment or care. Elderly people are one type of subject in this case study. The Digital health system will feature elderly care to allow the

subjects to live at home as long as possible. Another type of patients that we consider is Diabetes patients that need to follow their glucose level and regularly be followed up by health personnel.

The digital health system will both control equipment normally present in smart homes to make life comfortable (automatic light control, door locks, heater control, etc.), and control various types of medical devices and sensors. These devices and sensors support the care and wellness for the specific patient and consist of a wide variety of types, including: blood pressure meter, scales, fall detection sensors, glucose meter, video surveillance, medicine reminder, indoor and out-door location etc). In addition, the system needs to integrate with other systems to provide information or alarms for example to response centres, care-givers, physicians, next of kin etc., and to feed information to medical systems such as electronic patient journals (EPJ). The pivotal role of the system's Edge Computing will be what we denote "the medical gateway" which integrates sensors and devices, controls the edge and ensures the right data are provided to the various stakeholders and to integrated systems such as EPJ.

7.3.3.3 Smart building

This use case will make use of smart building sensors, actuators and services. To this aim two sets of applications covering Smart Energy Efficiency and Smart Elderly Care will be developed within a Care Centre environment. Energy efficiency of new and existing buildings is crucial to achieve carbon emission reduction, and as we increasingly spend more time indoors, adequate levels of user comfort need to be guaranteed by the smart buildings. This implies a trade-off between energy use and the different aspects of users' comfort. They will be tested in the KUBIK, a smart building especially designed for testing new solutions for sustainable buildings. The use case will simulate a care centre consisting of small apartments where a group of elderly people live together. This care centre use case includes sensors and actuators that monitor and control the environment in order to ensure the safety of the facilities, to perform energy efficiency measures and also to support the care-takers in monitoring the wellbeing of users.

The trend for smart buildings is to provide an increasing range of services supported by an increasing number of IoT sensors and actuators. Example of such services or applications include thermal comfort, visual comfort, energy efficiency, security, etc. Applications in this space need to share building infrastructure and may have conflicting objectives. The solution requires a clear hierarchy between the different actuation scenarios.

7.4 Search Engines for Browsing the Internet of Things – IoTCrawler

Efficient and secure access to Big IoT Data will be a pivotal factor for the prosperity of European industry and society. However, today data and service discovery, search, and access methods and solutions for the IoT are in their infancy, like Web search in its early days. IoT search is different from Web search because of dynamicity and pervasiveness of the resources in the network. Current methods are more suited for fewer (hundreds to millions), static or stored data and services resources. There is yet no adaptable and dynamic solution for effective integration of distributed and heterogeneous IoT contents and support of data reuse in compliance with security and privacy needs, thereby enabling a true digital single market. Previous reports show that a large part of the developers' time is spent on integration. In general, the following issues limit the adoption of dynamic IoT-based applications:

- The heterogeneity of various data sources hinders the uptake of innovative cross-domain applications.
- The large amount of raw data without intrinsic explanation remains meaningless in the context of other application domains.
- Missing security and neglected privacy present the major concern in most domains and are a challenge for constrained IoT resources.
- The large-scale, distributed and dynamic nature of IoT resources requires new methods for crawling, discovery, indexing, physical location identification and ranking.
- IoT applications require new search engines, such as bots that automatically initiate search based on user's context. This requires machine intelligence.
- The complexity involved in discovery, search, and access methods makes the development of new IoT enabled applications a complex task.

Some ongoing efforts, such as Shodan and Thingful provide search solutions for IoT. However, they rely mainly on a centralised indexing and manually provided metadata. Moreover, they are rather static and neglect privacy and security issues. To enable the use of IoT data and to exploit the business potential of IoT applications, an effective approach needs to provide:

- An adaptive distributed framework enabling abstraction from heterogeneous data sources and dynamic integration of volatile IoT resources.
- Security, privacy and trust by design as integral part of all the processes from publication, indexing, discovery, and subscription to higher-level application access.

- Scalable methods for crawling, discovery, indexing and ranking of IoT resources in large-scale cross-platform and cross-disciplinary systems and scenarios.
- Machine initiated semantic search to enable automated context dependent access to IoT resources.
- Monitoring and analysing the Quality of Service (QoS) and Quality of Information (QoI) to support fault recovery and service continuity in IoT environments.

IoTCrawler is an EU H2020 project that addresses the above challenges by proposing efficient and scalable methods for crawling, discovery, indexing and ranking of IoT resources in large-scale cross-platform and cross-disciplinary systems and scenarios. It develops enablers for secure and privacy-aware discovery and access to the resources, and monitors and analyses QoS and QoI to rank suitable resources and to support fault recovery and service continuity. The project evaluates the developed methods and tools in various use-cases, such as Smart City, Social IoT, Smart Energy and Industry 4.0. The key elements of IoTCrawler are shown in Figure 7.7.

The project aims to create scalable and flexible IoT resource discovery by using meta-data and resource descriptions in a dynamic data model. This means, for example, that if a user is interested in measuring temperature in a certain location, the result (e.g. list of sensors) should only contain sensors

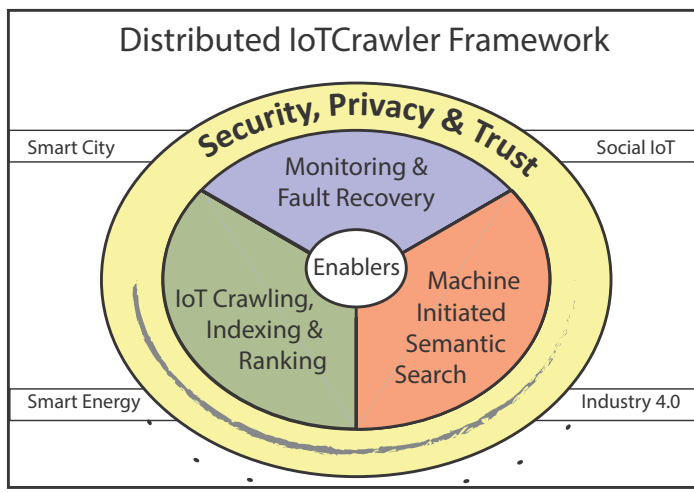

Figure 7.7 Key concepts of the IoTCrawler proposal. [40] ©2018 IEEE.

that can measure temperature, but the user may accept sensors that closely fulfil her/his application requirements even though all other characteristics may not be favourable (e.g. cost of acquisition may be high and sensor response time may be slow). For this reason, the system should understand the user priorities, which are often machine-initiated queries and search requests, and provide the results accordingly by using adaptive and dynamic techniques.

7.4.1 Architecture of IoTCrawler

IoTCrawler provides novel approaches to support an IoT framework of interoperable systems including security and privacy-aware mechanisms, and offers new methods for discovery, crawling, indexing and search of dynamic IoT resources. It supports and enable machine-initiated knowledge-based search in the IoT world. Figure 7.8 depicts the IoTCrawler framework and highlights its key components, which are detailed next.

7.4.1.1 IoT framework of interoperable (distributed) systems

The diversity of the market has resulted in a variety of sophisticated IoT platforms that will continue to exist. However, to evolve and enable the full benefits of IoT, these platforms need access to data, information and services across various IoT networks and systems within an integrated ecosystem of IoT resources. IoTCrawler envisions a cooperation of platforms and systems to provide smart integrated IoT based services. Nevertheless, instead of defining an overarching hyper-platform on top, the integration proposed by IoTCrawler is carried out by the definition of a common interface, enabling this way cooperation and interconnection of various platforms by making their data and services discoverable and accessible to other applications and services. An IoTCrawler-enabled platform can internally be implemented in different ways, since it only has to support the common and open interfaces to join the ecosystem. The open IoT interfaces are split in two planes that are called control and data planes. The control plane will coordinate and control the data and information processing in the platforms (monitoring and quality analysis). The data plane will allow for IoT data flow exchange between platforms (crawling, indexing and search).

7.4.1.2 Holistic security, privacy and trust

An ecosystem of IoT platforms brings immense benefits but also potential risks for users and stakeholders. The very principle that makes the IoT so

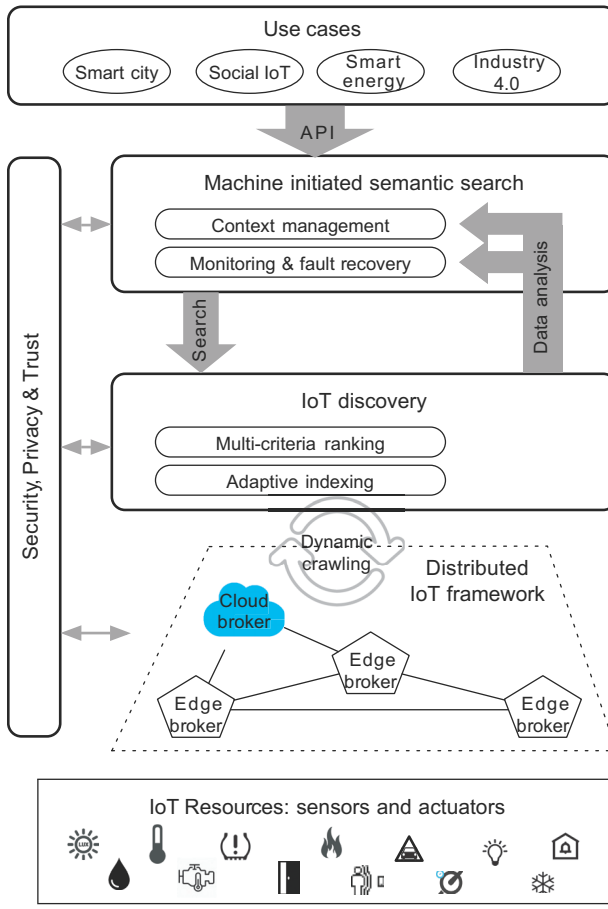

Figure 7.8 Overall architecture of the IoTCrawler framework. [40] ©2018 IEEE.

powerful – the potential to share data instantly with everyone and everything – creates huge security and privacy risks. Since IoT systems are, by their nature, distributed and operate often in unprotected environments, the maintenance of security, privacy, and trust is a challenging task. IoTCrawler addresses quality, privacy, trust and security issues by employing a holistic and end-to-end approach to the data and service publication to search and access workflow. Device and connectivity management will ensure that the end devices only connect to trusted access networks. IoTCrawler develops solutions for mitigating privacy intrusion and data correlation based on data collected from multiple sources. Both technical and information governance

procedures and guidelines are defined and implemented. This makes sure that the technical solutions are in place for avoiding the security and privacy risks, and also appropriate information governance procedures and best practices and measures are followed in development, deployment and utilisation of the use-cases and third-party applications.

7.4.1.3 Crawling, discovery and indexing of dynamic IoT resources

Information access and retrieval on the early days of the Internet and the Web mainly relied on simple functions and methods. For example, Yahoo's first search engine was simply based on the "grep" function in Unix or the AltaVista search engine initially did not have a ranking mechanism. The Internet and the Web have gone a long way in the past two decades to improve the way we access the information on the Web. While the current information and search retrieval on the Web is far from ideal, there are several sophisticated methods and solutions that provide crawling, indexing, ranking and search and retrieval of extremely large volumes of information on the Internet. The new generations of Web search engines have now focused on information extraction, personalised and customised knowledge and extraction techniques and solutions. Some early works are demonstrated by Google's knowledge graph, Wolfram Alpha and Microsoft Bing. The current information access and retrieval methods on the IoT are still at the same stage that the Web and the Internet were in their early days. Information retrieval on the large-scale IoT systems is currently based on the assumption that the sources are known to the devices and consumers or it is assumed that opportunistic methods will send discovery and negotiation messages to find and interact with other relevant resources in their outreach (e.g. Google's recent Physical Web project is designed based on this assumption). Overall, IoT systems have more ad-hoc resources that do not comply with document and URL processing and indexing norms; the resources, such as mobile phones and sensing devices, can publish data and then move to another location or disappear. Service and data crawling and discovery for smart connected devices and services will also involve automated associations and integration to provide an extensible framework for information access and retrieval in IoT. IoTCrawler focuses on providing reliable, quality and resource-aware and scalable mechanisms for data and services publishing, crawling, indexing in very large-scale distributed dynamic IoT environments.

7.4.1.4 Machine-Initiated semantic search

In the past, search engines were mainly used by human users to search for content and information. In the newly emerging search model, information is provided depending on the users' (human user or a machine) context and requirements (for example, location, time, activity, previous records, and profile). The information access can be initiated without the user's explicit query or instruction but used on its necessity and relevance (context-aware search). This will require machine interpretable search results in semantic forms. Moreover, social media, physical sensors (numerical streaming values), and Web documents must be better integrated, and the search results should become more machine interpretable information rather than remaining as pure links (e.g. the Web search engines mainly return a list of links to the pages as their results; with some exceptions on popular questions and topics).

IoTCrawler enables context-aware search and automated processing of data by semantic annotation of the data streams, thus making their characteristics and capabilities available in a machine processable way. There are several existing works that provide methods and techniques for semantic annotations and description of the IoT devices, services and their messages and data. However, most of these methods rely on centralised solutions and complex query mechanisms that hinder their scalability and wide scale deployment and use for the IoT. IoTCrawler supports an ecosystem of multiple platforms and develops dynamic semantic annotation and reasoning methods that will allow continuous and seamless integration of new devices and services by exploiting and adapting existing annotations based on similarity measures.

The automatic discovery has to consider the current context. Context-awareness requires the integration and analysis of social, physical and cyber data. IoTCrawler develops enablers for context-aware IoT search. Hence the requirements of the different applications are mapped to the solutions by selecting resources considering parameters such as security and privacy level, quality, latency, availability, reliability and continuity. IoTCrawler improves reliability and robustness by fault recovery mechanisms and mitigation of malfunctioning devices using device activation/deactivation in the associated area. The fault recovery also requires mechanisms to support communication among networked IoT resources located in diverse locations and across different platforms, and to provide secure and efficient re-distribution of information in case of failure.

7.4.2 Use Cases

IoTCrawler is currently evaluating its technologies in four real world use-cases: Smart Cities, Social IoT, Smart Energy, and Industry 4.0 (see Figure 7.9). Further use-cases will be identified and ranked in co-creation workshops with the relevant stakeholders within the project.

7.4.2.1 Smart city

The city of Aarhus has been considered as a target for smart city deployment in the project. IoTCrawler helps to overcome the negative perceptions of Internet of Things and Smart Cities by developing smart city experimentation

Figure 7.9 IoTCrawler use cases at a glance.

tools for Aarhus' City Lab that can make citizens and companies engaged and be curious about smart city solutions. IoTCrawler also provides the enabling technologies to discover new data sources in Aarhus for Open Data platforms and has the potential to become a reference platform supporting IoT data and service sharing as part of the sharing economy. To track the performance of a smart city, IoTCrawler develops enablers for monitoring activity and quality of the sensors. This can be used to set up KPI's for City Labs and to track its performance. The smart city deployment of Murcia is also considered in IoTCrawler, exploiting the large sensor platform installed.

7.4.2.2 Social IoT

Social IoT relates to using sensors deployed at sports and entertainment events in order to quantify the performance of professionals or experience of participants. This enables participants to engage in events beyond simply watching, thus creating a unique personal record of their experience, and in combination with social and digital media allows event manager to create new insights and content for their audience. IoTCrawler has access to over 800 events, including fashion events (e.g. New York Fashion week), culinary events, sports events (e.g. Basketball Final Four), or events such as Miss Universe. For each event, sensors are deployed at local venues and participants and spectators are equipped with wearable devices. This results in a range of diverse data sets that are collected, analysed, stored, and used, e.g. for content creation. Discovering and semi-automatically describing existing sensors, data sets and streams using IoTCrawler technologies has the potential to significantly increase the overall value of the dataset access and their integration, making it accessible to a larger group of people and enabling new applications. As described above, the data sets include raw sensor data and processed analytic results. However, data processing often involves data from other third-party sources. For this reason, play-by-play data is used to correlate analytical results to match events, and social media sources can be used to link to user generated content. IoTCrawler's discovery, indexing and search enablers have the potential to significantly reduce the effort associated with the integration of sensor technologies, and other external data sources.

7.4.2.3 Smart energy

Smart Buildings play an important role in distributed energy systems as they turn from energy consumers to the so-called "energy prosumers". In future energy systems, Smart Buildings actively interact with the Smart

Grids in order to stabilise them or participate in energy trading as well as for structural condition monitoring and proactive maintenance. For this purpose, buildings offer semantically annotated properties of the technical equipment within especial energy flexibilities (i.e. for shifting electrical and thermal loads). In this frame, this use-case employs the technologies developed in IoTCrawler to dynamically discover the flexibilities of Smart Buildings and analyse their potential as well as their demand for applications that are necessary to manage and offer energy to the Smart Grid or the energy market. This information can be used by energy retailers or grid operators to deploy best fitting applications to individual buildings. The project uses semantic enrichment of grid data and data analytics to enhance smart grid applications and reduce the need for manual engineering and setup of systems.

7.4.2.4 Industry 4.0

Industry 4.0 includes advances such as predictive maintenance, energy prediction, or human-robot collaboration. The results of IoTCrawler will be used to improve predictive maintenance planning for horizontal machining centres in aerospace and Die&Mould industries. Currently, data integration consumes more than 80% of the time in the industry. IoTCrawler has the potential to significantly accelerate the development and deployment of Industry 4.0 analytics solutions, by discovering and semi-automatically integrating machine metadata, sensor data provided by the machines and information stored in related enterprise databases. Extending the discovery to actuator services (e.g. air conditioning, heating, and machine operation) allows to link actions for avoiding load peaks to energy analytics pipeline. IoTCrawler also increases workers' safety by identifying critical conditions (e.g. gas exposition) in the permanent sensor data stream of drones, and forward such condition markers to monitoring teams and production management subsystems.

7.4.3 Main Innovations in the Areas of Research

The literature within key areas of the IoTCrawler proposal is reviewed next, indicating the main innovations of the work within the general framework described above.

7.4.3.1 Search and discovery

Being essential for any network architecture, one of the key components of the proposed architecture is the search and discovery operation. Distributed

Hash Table (DHT) is used to provide a high scalability in storage and a flexible support for query and update operations. DHT is a totally decentralised system that stores data objects for easy and quick access (query) and update (store). DHTs are built on top of overlay networks into which network objects are spread and identified with unique keys, e.g. the well-studied overlay network and DHT Chord mechanism [22], which is the direct ancestor of Kademlina [23] (BitTorrent's DHT). Overlay networks and DHTs are well suited to form the basement of a proper discovery mechanism, such as the Overlay Management Backbone (OMB) approach [24]. To add suitable schema evolution to the information/content discovery, description mechanisms such as the Resource Description Framework (RDF) and JSON-LD [25] are needed. Combining a DHT mechanism with RDF, the work in [26] proposes to use an adapted version of RDQL [27] to perform the queries. The main problems of this approach are that it consumes a lot of storage space and that it is not efficient for simple searches. SPARQL [28] is the de facto query language for RDF, by providing a coherent and simple search mechanism.

The IoTCrawler approach exploits the remarkable qualities of the overlay network and DHT described above to build a distributed discovery infrastructure. However, the nodes are deployed in separate domains to distribute both the storage/finding load and the management of information access.

7.4.3.2 Security for IoT

In spite of the emergence of different cross-world initiatives in recent years (IERC, ITU-T SG20, IEEE IoT Initiative4 or IPSO Alliance are just some of them), there is a lack of a unified vision on security and privacy considerations in the IoT paradigm, which embraces the whole lifecycle of smart objects that are making up the digital landscape of the future. In the IoT, data confidentiality and authentication, access control within the networks, privacy and trust among users and things are among some of the key issues [29].

IoTCrawler explores the use of advanced cryptographic techniques based on Attribute-Based Encryption (ABE). Specifically, it analyses the application and extension of the Ciphertext-Policy Attribute-Based Encryption (CP-ABE) as a flexible and promising cryptographic scheme in order to enable information to be shared while confidentiality is still preserved. In CP-ABE, the cipher-text embeds the access structure to describe which private-keys can decrypt it, and the same private-key is labelled with descriptive attributes. IoTCrawler addresses the integration of CP-ABE with different

signatures schemes to provide end-to-end integrity to the information that is shared for anticipatory purposes. Users are given means to define how their personal information is shared and under which circumstances using a policy-based approach. Additionally, IoTCrawler investigates the integration of this solution within the search and discovery process for IoT.

The Blockchain paradigm [30] is also included in IoTCrawler. A Blockchain is a distributed database that maintains a continuously growing set of transactions in a way that is designed to be secure, transparent, highly resistant to outages, auditable, and efficient, at the same time it is distributed. However, despite the benefits that Blockchain technologies offer, we still need to overcome two major challenges in IoTCrawler. First, privacy, since transactions tend to be public, and encryption to protect transactions' contents is not enough because it still allows the remaining nodes in the system to learn about the occurrence of a particular exchange in the system; and, second, scalability, because existing permission-less blockchains (e.g. Bitcoin) are only able to scale to a considerable number of nodes at the expense of attained throughput, e.g. Bitcoin's throughput is about seven transactions per second.

Moreover, IoTCrawler will leverage Trusted Execution Environments (TEEs) to enhance the security primitives deployed in the proposed framework, given that existing TEEs suffer from a number of shortcomings, especially with respect to their security and privacy provisions.

In the area of Authentication, Authorisation and Accounting (AAA), IoTCrawler proposes a lightweight access control scheme based on Capability Tokens for IoT as presented in [31, 32], where these tokens act as a proof of possession providing a straightforward validation mechanism without requesting a third party. We propose a mechanism for interoperability of different authentication and authorisation solutions based on a bridge to third party elements, such as the standard stacks as LDAP and FIWARE Service Enablers to support a lightweight federation-like approach.

7.4.3.3 Data validation and quality analysis

The assessment of Quality of Data can basically be evaluated in five common dimensions: Completeness, Correctness, Concordance, Plausibility and Currency. In [33] the authors provide a table of different terms used to describe one of the dimensions of data quality. Furthermore, they provide a mapping between data quality dimensions and data quality assessment methods. In [34] Sieve is introduced, a framework to flexibly express quality assessment methods and fusion methods. The STAR-CITY project [35] describes a system for semantic traffic analytics. Based on various heterogeneous data

sources (e.g., Dublin bus activity, events in Dublin city), their system is able to predict future traffic conditions with the goal to make traffic management easier and to support urban planning.

One of the major challenges in the assessment of quality metrics to sensory IoT data is the lack of ground truth. The authors of [36] and [37] developed and evaluated a concept for the assessment of node trustworthiness in a network based on data plausibility checks. They propose that every node performs a plausibility check to identify malicious nodes sending faulty data. Similar to this work, they use data sources in order to find "witnesses" for a given sensor reading. The authors in [38] propose three different approaches to deal with a missing ground truth in social media: spatiotemporal, causality, and outcome evaluation. Their concept to use spatiotemporal evaluation to predict future behaviour of humans is like the proposed IoTCrawler approach, disregarding that we evaluate past events. Prior work of the authors emphasised the importance of an appropriate distance model reflecting infrastructure, e.g., roads, and physics, i.e. traffic or air movements [39]. The approach in IoTCrawler refines the state of the art by utilising sensor and domain independent correlation and interpolation models whilst incorporating knowledge of the city infrastructure to evaluate data stream plausibility.

7.4.4 Conclusion

This part presents the key ideas and the architecture of a crawling and discovery engine for the Internet of Things resources and their data. We describe our work in the context of the H2020 IoTCrawler project, which proposes a framework to make possible the effective search over IoT resources. The system goes beyond the state of the art through adaptive, privacy-aware and secure algorithms and mechanisms for crawling, indexing and search in distributed IoT systems. Innovative technological developments are proposed as enablers to support any IoT scenario. We discuss four use cases of the platform, which are presented in the areas of Smart Cities, Social IoT, Smart Energy and Industry 4.0. The project is currently implementing the envisaged framework, at the same time the main interoperability issues are considered to support the real-life uses cases identified. This work has been sponsored by the European Commission, through the IoTCrawler project (contract 779852), and the Spanish Ministry of Economy and Competitiveness through the Torres Quevedo program (reference PTQ-15-08073).

7.5 SecureIoT: Multi-Layer Architecture for Predictive End-to-End Internet-of-Things Security

The proliferation and rising sophistication of Internet of Things (IoT) infrastructures and applications comes with a wave of new cybersecurity challenges. This is evident in several notorious security incidents on IoT devices and applications, which have occurred during the last couple of years. These include the "Lizard Stressor" attacks on home routers (January 2015), the 1.4 million cars that were recalled by Chrysler due to potential hacking of their control software (July 2015), Tesla's autopilot crash (July 2016), as well as the first large scale distributed denial of service (DDoS) attack based on IoT devices (October 2016). Most of these incidents are directly associated with the complexity, heterogeneity and dynamic behaviour of emerging IoT deployments, which poses security challenges, which can be hardly addressed by state of the art platforms. Some of the most prominent of these challenges, include:

- The fact that they provided limited support for end-to-end security, since they lack mechanisms that address IoT security at all levels, i.e. from the field and devices level to the edge and cloud levels. Moreover, existing security solutions tend to be framed within a single platform and ecosystem and cannot effectively operate in scenarios involving multiple platforms and ecosystems [41].
- Their inability to deal with very volatile and dynamic environments comprising networks of smart objects. State-of-the-art IoT platforms and their security mechanisms provide within cloud-based environments that ensure cybersecurity for large numbers of IoT devices. Nevertheless, they make only limited provisions for dynamic applications involving networks of smart objects (i.e. objects with (semi)autonomous behaviour). In the latter, IoT devices and smart objects are likely to join or leave, while security and privacy policies can also change dynamically and without prior notice. Hence, to support large scale interactions across multiple IoT platforms and networks of smart objects, there should be some means of predicting and anticipating the security behaviour and trustworthiness of an IoT entity (e.g., device, platform, groups of objects) prior to interacting with it.

SecureIoT is motived by the need to support cyber-security in scenarios involving cross-platform interactions and interactions across networks of smart objects (i.e. objects with semi-autonomous behaviour and embedded

intelligence), which require more dynamic, scalable, decentralized and intelligent IoT security mechanisms. To this end, it introduces a multi-layer, data-driven security architecture, which collects and processes information from the field, edge and cloud layers of an IoT system, in order to identify security threats at all these layers and accordingly to drive notifications and early preparedness to confront them. Furthermore, SecureIoT foresees cross-layer coordination mechanisms and will employees advanced analytics towards a holistic and intelligent approach that will predict and anticipate secure incident in order to timely confront them. Also, SecureIoT introduces a range of security interoperability mechanisms in order to support cross-vertical and cross-platform cyber-security scenarios. The SecureIoT architecture serves as basis for the provision of security services to IoT developers, deployers and platform providers, including a risk assessment, a compliance auditing and a secure programming support service. In this context, the rest of this chapter is structured as follows: Section 2 introduces the SecureIoT architecture and its main principles. Section 3 discusses the security services to be offered by the project, while Section 4 presents some use cases that will be used to validate the project's results.

7.5.1 SecureIoT Architecture

7.5.1.1 SecureIoT architecture overview

Figure 7.10. provides a high-level overview of the security architecture of the project. The architecture provides placeholders for predictive IoT security mechanisms, which can be contributed by different security experts in order to protect IoT infrastructures and services. In the scope of SecureIoT the partners will specify and implement such mechanisms in the areas of security monitoring and predictive analysis, which will serve as a basis for supporting the project's use cases. Nevertheless, the project's architecture is more general and therefore able to accommodate additional algorithms and building blocks. The architecture complies with the reference architectures specified by the Industrial Internet Consortium (IIC) and the OpenFog consortium [42], as it specifies: (i) **The field level**, where IoT devices (including smart objects) reside; (ii) **The fog/edge level**, which controls multiple devices close to the edge of the network. Note that the fog/edge level might be the first security layer in an IoT application, especially when resource constrained devices are deployed; (iii) **The enterprise and platform levels**, which reside at the core and where application and platform level security measures are applicable. Moreover, the SecureIoT architecture will also specify:

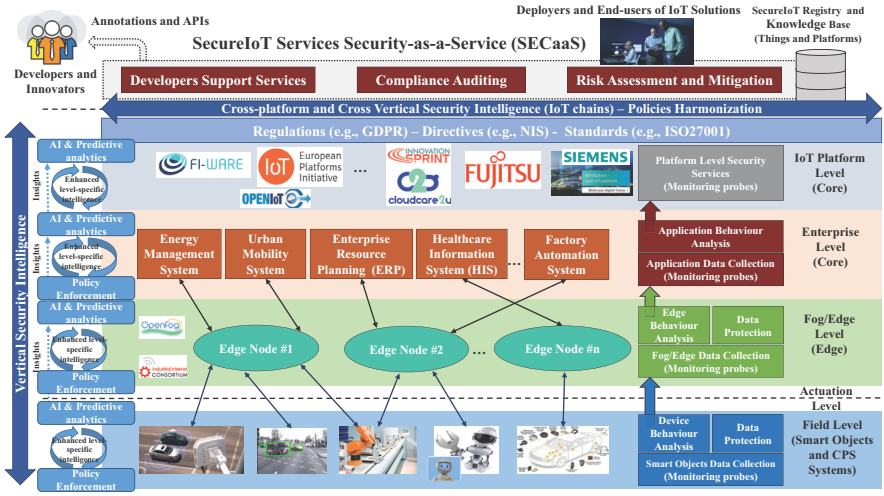

Figure 7.10 Overview of SecureIoT Architecture.

- Interfaces for (security) data collection at all levels of the security architecture, including monitoring probes that are deployed at all levels.
- Data analytics modules (including AI and predictive analysis) at all levels, which extract insights about the future security state of the IoT infrastructure and applications.
- Semi-automated Policy Enforcement Points (PEPs), which are driven by predictive insights and enforce policies at different levels. PEPs will provide the means for enforcing security and cryptographic functionalities, configuring IoT platforms and devices for enhanced security, as well as for distributing security sensitive datasets.
- Multi-level security mechanisms and measures, which combine security monitoring, analytics and insights from multiple levels.

Applicable policies and security measures are driven by regulations (e.g., GDPR), directives (e.g., NIS, ePrivacy) and standards (such as ISO27001 [43]). The ultimate goal of the architecture is to provide concrete services such as the SECaaS. The delivery of these services is facilitated by the development and maintenance of a security knowledge base, where metadata about IoT entities (i.e. objects platforms etc.) are registered along with knowledge collected and summarized based on multiple publicly available threat intelligence sources. Note that the security

services of the architecture are offered as a service based on a Security-as-a-Service (SECaaS) paradigm. This however does not imply that the security services are solely deployed in the cloud. Rather, they can be offered based on a combination of cloud-based SaaS (Software-as-a-Service) security services and FaaS (Fog-as-a-Service) functions provided at the fog level.

7.5.1.2 Intelligent data collection and monitoring probes

Assessing and optimizing the security posture of IoT components require the collection and the processing of their respective monitoring and configuration data. The produced monitoring data will allow IoT stakeholders to assess the security posture of their IoT platforms, to predict security issues, to enforce policies for hardening systems, to prevent network misuse, to quantify business risk, and to collaborate with partners to identify and mitigate threats. The collection of these data requires the development of dedicated probes and monitoring layers at different levels of the deployed IoT platform (device, network, edge and core) to capture a comprehensive and a complete view of its operations and interactions. In SecureIoT, monitoring probes will be provided to support the collection of log data, including network flows and software configurations, at the component, services and network levels.

A key characteristic of SecureIoT's security monitoring infrastructure (and related probes) will be its built-in intelligence in the data collection and pre-processing mechanisms, which will be implemented over the SecureIoT monitoring probes that will interfaces to different IoT platforms. As part of this intelligence, the data collection mechanisms will ensure data quality, data filtering, as well as adaptive selection of the needed data sources based on dynamic changes to the configuration of the IoT platforms, applications and smart objects. In order to implement this intelligence, the monitoring probes will be enhanced with data streaming analytics mechanisms, which will be able to process security-related information sources on the fly (i.e. almost at real-time) in order to adapt the filtering and data collection accordingly. This data collection intelligence will facilitate fast processing, as well as the implementation of predictive analytics schemes.

7.5.1.3 SecureIoT systems layers and information flows

Figure 7.11. presents the layers of a SecureIoT compliant system, with emphasis on the flow of information from an IoT platform to the SecureIoT SECaaS services. The following layers are presented:

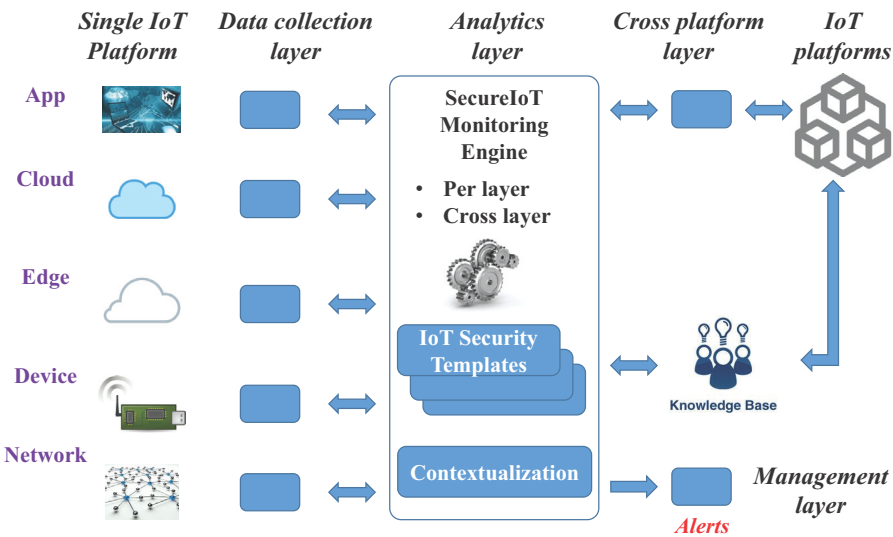

Figure 7.11 Layers of SecureIoT systems.

- **A layer of an individual IoT platform or system**, which typically comprises network, devices/field, edge/fog, cloud and application-level components. These components are usually part of the target IoT platform or systems that needs to be secured based on SecureIoT.
- **A data collection layer**, which comprises the above-mentioned security monitoring probes. Note that probes will be specified and developed for all parts and components of the IoT system i.e. from the network and devices components all the way up to the IoT applications' components.
- **A data analytics layer**, which is destined to process the data derived from the various probes. This layer is empowered by data analytics algorithms, but also by a range of cybersecurity templates, which specify rules and patterns of the security incidents that are to be identified. Taking network-level attacks as example, templates for specific types of network attacks will be specified such as TCP SYN attacks, UDP flood attacks, HTTP POST DoS (Denial of Service) attacks [43]. Each of the templates will comprise the rules and conditions under which the attacks will be identified. Likewise, templates for other types of attacks, including application specific ones will be specified and used. Along with these templates, the data analytics layer will comprise a contextualization

component, which will be used to judge whether the attacks indicators are abnormal for the given IoT platform and application context.
- **A cross-platform layer**, which is destined to aggregate and correlate information derived from multiple-IoT platforms. It will serve as a basis for identifying attack indicators in cross-platform scenarios.

All of the above layers and components will leverage the services of a knowledge base that will comprise information and knowledge about IoT-related cybersecurity attacks. It will be also used to drive the operation of the IoT security templates and the contextualization component.

7.5.1.4 Mapping to RAMI 4.0 layers

SecureIoT is destined to support cybersecurity scenarios in both consumer and industrial settings. In order to strengthen the industrial relevance of the project's architecture, the project will provide a mapping of the main building blocks of the SecureIoT architecture to the Reference Architecture Model Industry4.0 (RAMI 4.0) [45]. While this mapping is work in progress, the following associations and mappings are envisaged:

- **The SecureIoT field layer**, maps to the Field and Control Device hierarchy levels of RAMI4.0, as well as to its Asset Integration layer.
- **The SecureIoT edge layer**, maps tot eh Station and Workcenter hierarchy levels of RAMI4.0, as well as to its Asset, Integration and Communication layers.
- **The SecureIoT cloud layer**, maps to the Workcenter, Enterprise and Connected World hierarchy levels of RAMI4.0, as well as to its Information, Functional and Business layers.
- **The SecureIoT application layer**, maps to the Enterprise and Connected World hierarchy levels of RAMI4.0, as well as to its Business layer.
- **The SecureIoT data collection layer**, maps to the Field Device, Control Device, Station and Work Centers hierarchy levels of RAMI4.0, as well as to its Communication and Information layers.
- **The SecureIoT analytics layer**, maps to the Enterprise and Connected World hierarchy levels of RAMI4.0, as well as to its Information layer.
- **The SecureIoT management layer**, maps to the Enterprise and Connected World hierarchy levels of RAMI4.0, as well as to its Information, Functional and Business layers.

7.5.2 SecureIoT Services

Based on its architecture, the project will offer risk assessment, compliance auditing and programmers' support services as outlined in the following paragraphs.

7.5.2.1 Risk assessment (RA) services

The SecureIoT RA services will aim at an efficient balance between realizing opportunities for gains, while minimizing vulnerabilities and losses. They will strive to ensure that an acceptable level of security is provided at an affordable cost. The SecureIoT framework will quantify risks in terms of a "likelihood factor", which will be calculated based on combination of the probability and impact of any identified vulnerabilities. This "likelihood factor" will be appropriately weighted and ultimately normalized based on a risk calculation model in-line with NIST's Common Vulnerability Scoring System (CVSS). Special emphasis will be paid in evaluating the criticality of risks associated with the behaviour and the operation of smart objects, as well as of services spanning multiple platforms. SecureIoT will therefore formulate a formal methodology and an accompanying model that will produce risk quantifications based on the identified vulnerabilities, potential threats and the impact estimation per potentially successful exploitation. SecureIoT will develop a risk quantification engine based on an expert system, which will provide flexibility in implementing different rules and assign different rates to the various risks.

7.5.2.2 Compliance auditing services

This service will be delivered as a tool available to solution deployers, operators and end-users. Based on information collected through the security analytics, including the information of the IoT knowledge base. It will provide support for a set of security and privacy controls on the IoT infrastructures at multiple levels. The tool will be configured to support auditing of IoT infrastructures and services, against existing sets of security and privacy controls. The auditing will identify non-compliant behaviours and will provide recommendations about areas that require attention. Several prominent sets of security and privacy rules that will be supported concerning controls and measures specified in the scope of the GDRP regulation, NIS and ePrivacy directives.

7.5.2.3 Programming support services

This service will enable developers to secure applications as part of their programming efforts. In particular, it will enable them to: (a) Enforce Distributed Access Control; (b) Ensure the cryptographic protection of data; and (c) Physical distribute sensitive data for enhanced security. These activities will be supported based on programming annotations, which will specify distributed access control, cryptographic protection and physical data distribution activities. A series of source generation, bytecode transformation and runtime reflection actions will be undertaken at specified Policy Enforcement Points (PEPs), which will be implemented at various levels i.e. the device, edge, core and application layers of the SecureIoT architecture. To this end, along with the security monitoring probes, the SecureIoT architecture will provide the means for configuring elements at the PEPs.

7.5.3 Validating Use Cases

The project's architecture and services will be validated in three use cases, which are briefly discussed in the following paragraphs.

7.5.3.1 Industrial plants' security

The use case will focus on plant networks for operations and support – e.g. SCADA, MES, PLCs, etc. – and enterprise networks connected to IoT-platforms providing support for automation and supply chain collaboration. The technical approach of the industrial IoT use case is twofold as reliability and availability of real world production must not be brought at risk. The following security challenges will be addressed, based on the SecureIoT services:

- **Secure operations of connected factories with thread prediction**: The SecureIoT risk assessment service will be therefore used to predict security issues arising from deployed automation technologies in a multi-vendor environment. Furthermore, SecureIoT's prediction and mitigation services will enable the plant control to draw the right conclusions and prepare for attacks before they emerge.
- **Compliance and Protection of product/user data in a multi-vendor environment**: Factories need to protect product and user data sets. SecureIoT will be used in order to enforce privacy and data protection policies. Likewise, the compliance auditing SecureIoT service will be also used to identify and remedy gaps in the industrial IoT environment.
- **Predictive Maintenance and Avoiding Machine Break-Downs in "Human in the Loop" Scenarios**: Predictive maintenance requires

trustworthy exchange, storage and processing of sensor and asset management datasets. Security analytics of IoT application level entities will be exploited as part of the SecureIoT risk assessment service in order to proactively identify issues with transmission and protection of datasets involved in the predictive maintenance process, in order to ensure the reliability of the process and avoid damages/losses in scenarios where machines foretell their lifetime and initiative actions in the supply chain (e.g., ordering of spare parts, scheduling of maintenance).

7.5.3.2 Socially assistive robots

This use case will focus on security challenges associated with the integration of a socially assistive robot (i.e. QT robot from SecureIoT partner LuxAI) with a cloud-based IoT platform. This integration will target the delivery of personalized ambient assisted living functionalities, such as personalized rehabilitation and coaching exercises. In order to support these applications a dense IoT network, enable continuous interaction between IoT devices, robots, human users and the environment will be established. The integration challenge will however lie on keeping track of the state of the robot and the environment, as well as on implementing distributed task assignment strategies (such as the Consensus-Based Bundle Algorithm (CBBA)), which enable the distribution of application logic across different smart objects. The following security challenges will be addressed:

- **Network and message security**: The SecureIoT risk assessment and mitigation services will be used to identify threats associated with communications and network performance in order to appropriately adapt the operation of the application (e.g., stop the training if needed and deliver proper alerts to users).
- **Prediction and avoidance of dangerous/risky situations**: SecureIoT will monitor the robots' operation both at the software level (i.e. through information flow tracking) in order to identify possible hacking of the robot, but also at the application level in order to detect abnormal operation/behaviour that can lead at risk.
- **Secure programming environment for robotics missions**: The programming interfaces of the robot will be enhanced with SecureIoT programming model and annotations in order to enable the developer of a rehabilitation mission to enforce policies specified in some policy language such as XACML (eXtensible Access Control Markup Language).

- **Compliance to GDPR**: An analysis of the application for GDPR compliance will take place, including automated identification of non-compliance risks (based on the SecureIoT risk assessment) and subsequent implementation of GDRP compliant policies based on the secure programming XACML-based mechanisms.

7.5.3.3 Connected car use cases

This use case concerns security in connected cars scenarios, including: (i) **Usage Based Insurance** scenarios where vehicle data are analysed to assess driver behaviour and hence determine risks in order to better tailor insurance premiums for the customers; and (ii) **Warnings on traffic and road conditions**, that involve analysing data coming from multiple vehicles to understand the traffic conditions in different locations. From the point of view of cybersecurity for the usage-based insurance, it is important to ensure that the data transmitted is only accessible by the responsible organisation (privacy) and that the system cannot be corrupted such that a risky driver appears to be low risk. Moreover, the integrity of the data is a key requirement to ensure that insurance premiums are calculated fairly based on objectively assessed risk using accurate and trusted data. Likewise, for the traffic and road condition warnings it is vital that the data sent to the car is an accurate interpretation of the data provided from each vehicle. It This is because the system could be used maliciously to create congestion if the data is corrupted. Moreover, integrity of software running in the connected car is crucial. Recent attacks or security alarms raised has been focused on taking control over IoT devices and gateways. Over the air firmware update could be used as a countermeasure mechanism after an anomalous (or malware) detection.

To address these challenges, the SecureIoT risk assessment framework will be employed, including predictive risk assessment functionalities. In case of identified issues, preventive measures will be activated (i.e. enforcement of data protection policies, provision of alerts to end-users, instigation and scheduling of over the air updates).

7.5.4 Conclusion

SecureIoT is a first of a kind attempt to introduce a standards-based architecture for end-to-end IoT security. The project's architecture is aligned to recent standards for industrial IoT security, including standards of the Industrial Internet Consortium and the OpenFog consortium. It makes provisions for

collecting and analysing data from all layers of an IoT platform, while at the same time catering from cross platform and cross layer security analysis. Moreover, the SecureIoT architecture provides the means for defining and executing security actions at specific PEPs, as a means of enforcing policies and instigating mitigation actions. Based on this architecture, the project will implement risk assessment, compliance and the programming support services.

SecureIoT is currently in its requirements engineering and specification phase, while it has also commenced its architecture specification activities. As part of the latter, the project will provide a mapping of its architectural concepts to the RAMI4.0 reference model. Moreover, the project will start the implementation of the data collection and data analytics mechanisms that will underpin the realization of the architecture and of its services. The project holds the promise to enhance the functionalities and lower the costs for securing IoT applications spanning multiple IoT platforms and smart objects. We will aspire to disseminate more detailed results through publications, presentations and other activities of the IERC cluster in the coming ten months. This work has been carried out in the scope of the H2020 SecureIoT project, which is funded by the European Commission in the scope of its H2020 programme (contract number 779899). The authors acknowledge valuable help and contributions from all partners of the project.

7.6 SEMIoTICS

7.6.1 Brief Overview

SEMIoTICS aims to develop a pattern-driven framework, built upon existing IoT platforms, to enable and guarantee secure and dependable actuation and semi-autonomic behaviour in IoT/IIoT applications. Patterns will encode proven dependencies between security, privacy, dependability, and interoperability (SPDI) properties of individual smart objects and corresponding properties of orchestrations involving them. The SEMIoTICS framework will support cross-layer intelligent dynamic adaptation, including heterogeneous smart objects, networks and clouds, addressing effective adaptation and autonomic behaviour at field (edge) and infrastructure (backend) layers based on intelligent analysis and learning. To address the complexity and scalability needs within horizontal and vertical domains, SEMIoTICS will develop and integrate smart programmable networking and semantic interoperability mechanisms. The practicality of the above approach will be validated using

three diverse usage scenarios in the areas of renewable energy (addressing IIoT), healthcare (focusing on human-centric IoT), and smart sensing (covering both IIoT and IoT); and will be offered through an open Application Programming Interface (API). SEMIoTICS consortium consists of strong European industry (Siemens, Engineering, STMicroelectronics), innovative SMEs (Sphynx, Iquadrat, BlueSoft) and academic partners (FORTH, Uni Passau, CTTC) covering the whole value chain of IoT, local embedded analytics and their programmable connectivity to the cloud IoT platforms with associated security and privacy. The consortium is striving for a common vision of creating EU's technological capability of innovative IoT landscape both at European and international level.

7.6.2 Introduction

Global networks like IoT create an enormous potential for new generations of IoT applications, by leveraging synergies arising through the convergence of consumer, business and industrial Internet, and creating open, global networks connecting people, data, and "things". A series of innovations across the IoT landscape have converged to make IoT products, platforms, and devices, technically and economically feasible. However, despite these advancements the realization of the IoT potential requires overcoming significant business and technical hurdles. This includes several system aspects, including dynamicity, scalability, heterogeneity, and E2E security and privacy [46–48], as they are described below.

IoT are dynamic, ever-evolving and often unpredictable environments. This relates to both IoT infrastructures as a whole (e.g. rapid development of new smart objects and IoT applications introducing new requirements to existing infrastructures and networks) and individual IoT applications (e.g. new users and types of objects connecting to said applications). This necessitates dynamically adaptive behaviour at runtime, at the IoT infrastructure, the IoT applications, and locally at the smart objects integrated by them. Intrinsic requirements (e.g. scale, latency) dictate the need for, at least, semi-autonomic adaptation at all layers.

The fast-growing number of interconnected users, smart objects and applications requires high scalability of the IoT infrastructure and network layers. At the network, the vastly increased demands require highly efficient programmable connectivity, service provisioning and chaining in ways that guarantee the much-needed end-to-end (E2E) optimizations, addressing dynamic IoT application requirements. Scalability at the IoT infrastructure

level requires seamless discovery and bootstrapping of smart objects, as well as highly efficient orchestration, event processing and analytics and IoT platform integration.

Despite advancements in standardization, there is still limited semantic interoperability within IoT applications and platforms. Semantic interoperability requires three key abilities: (a) to recognize and balance the heterogeneous capabilities and constraints of smart objects, (b) to interpret data generated by such objects correctly, and (c) to establish meaningful connections between heterogeneous IoT platforms.

Smart objects, IoT applications, and their enabling platforms are often vulnerable to security attacks and changing operating and context conditions that can compromise their security [49]. They also generate, make use of, and interrelate massive personal data in ways that can potentially breach legal and privacy requirements [49]. Preserving security and privacy properties remains a particularly challenging problem, due to the difficulty of: (a) analysing vulnerabilities in the complex E2E compositions of heterogeneous smart objects, (b) selecting appropriate controls (e.g., different schemes for ID and key management, different encryption mechanisms, etc.), for smart objects with heterogeneous resources/constraints, and (c) preserving E2E security and privacy under dynamic changes in IoT applications and security incidents, in the context of the ever-evolving IoT threat landscape [50].

The above challenges give rise to significant complexities and relate to the implementation and deployment stack of IoT applications to address them. The overall aim is: demands without considering the data volume. Taking into consideration this ratio, green IT technologies have important environmental and economic benefits. Circular Economy (CE) advocates a continuous development cycle that reforms the currently prominent 'take-make-dispose' linear economic mode by preserving and enhancing the natural capital. SEMIoTICS will also provide the intelligence analytics capabilities and Information Communication Technologies (ICT) that are required for turning IoT data into a worthy asset for CE-centric businesses (e.g. [51]).

7.6.3 Vision

The main goal of the SEMIoTICS project is to develop a pattern-driven framework, built upon existing IoT platforms. The proposed framework will enable and guarantee the secure and dependable actuation and semi-automatic behaviour in IoT/IIoT applications. Specifically, the SEMIoTICS vision in delivering smart, secure, scalable, heterogeneous network and data-driven IoT is based on two key features:

- **Pattern-driven approach:** Patterns are re-usable solutions to common problems and building blocks to architectures. In SEMIoTICS, patterns encode proven dependencies between security, privacy, dependability and interoperability (SPDI) properties of individual smart objects and corresponding properties of orchestrations (composition) involving them. The encoding of such dependencies enables: (i) the verification that a smart object orchestration satisfies certain SPDI properties, and (ii) the generation (and adaptation) of orchestrations in ways that are guaranteed to satisfy required SPDI properties. The SEMIoTICS approach to patterns is inspired from similar pattern-based approaches used in service-oriented systems [52, 53], cyber physical systems [54] and networks [55, 56].
- **Multi-layered Embedded Intelligence:** Effective adaptation and autonomic behaviour at field (edge) and infrastructure (backend) layers depends critically on intelligent analysis and learning the circumstances where adaptation actions did not work as expected. Intelligent analysis is needed locally for semi-autonomous, prompt reaction, but taking into account IoT smart objects limited resources (thus requiring specialized lightweight algorithms) [55, 57]. It should also be possible to fuse local intelligence to enable and enhance analysis and intelligent behaviour at higher levels (e.g. using results of local analysis of "thing events" to globally predict and anticipate failure rates) [58].

7.6.4 Objectives

The SEMIoTICS project will target IoT applications with heterogeneous smart objects, various IoT platforms and different SPDI requirements. Seven main objectives are identified by the SEMIoTICS project including:

- The development of patterns for orchestration of smart objects and IoT platform enablers with guaranteed SPDI properties
- The development of semantic interoperability mechanisms for smart objects, networks, and IoT platforms, like semantic information broker that resolve the semantics of correlated ontologies and common APIs that enable cross-platform programming and interaction
- The development of dynamically and self-adaptable monitoring mechanisms, supporting integrated and predictive monitoring of smart objects in a scalable manner

- The development of core mechanisms for multi-layered embedded intelligence, IoT application adaptation, learning and evolution, and E2E security, privacy, accountability and user control
- The development of IoT-aware programmable networking capabilities based on adaptation and Software-Defined Networking (SDN)/Network Function Virtualization (NFV) orchestration
- The development of a reference prototype open architecture demonstrated and evaluated in both IIoT (renewable energy) and IoT (healthcare), as well as in a horizontal use case bridging the two landscapes (smart sensing), and delivery of the respective open API
- The adaptation of EU technology offerings internationally

These objectives are accomplished, considering the intrinsic requirements of three main use case scenarios for an industrial wind park, an e-health system, and a smart sensing setting.

7.6.5 Technical Approach

Figure 7.12 shows our initial vision of the logical architecture of SEMIoTICS framework and how it relates to smart objects, IoT applications, and existing IoT platforms, and how does it map onto a generic deployment infrastructure consisting of private and public clouds, networks, and field devices. Within the figure, blue boxes show components of the framework that are to be developed by SEMIoTICS; white boxes indicate components of IoT applications managed by the framework. The key role of the SEMIoTICS framework in the IIoT/IoT implementation stack is to support the secure, dependable and privacy-preserving connectivity and interoperability of IoT applications and smart objects used by them, and the management, monitoring and adaptation of these applications, objects and their connectivity.

7.6.5.1 Enhanced IoT aware software defined networks

The sheer number of smart objects that are expected to connect to the Internet by 2020 (more than 50bn smart objects) will increase network traffic dramatically and introduce more diversity of network traffic (from elephant flows to mice flows). This makes the development of networking techniques that are significantly more scalable and agile than today's networks an absolute necessity. Networks will need to dynamically reconfigure their resources and maintain network connectivity. Also, applications running on top of smart connected devices will need to be resource and network-aware, in order to

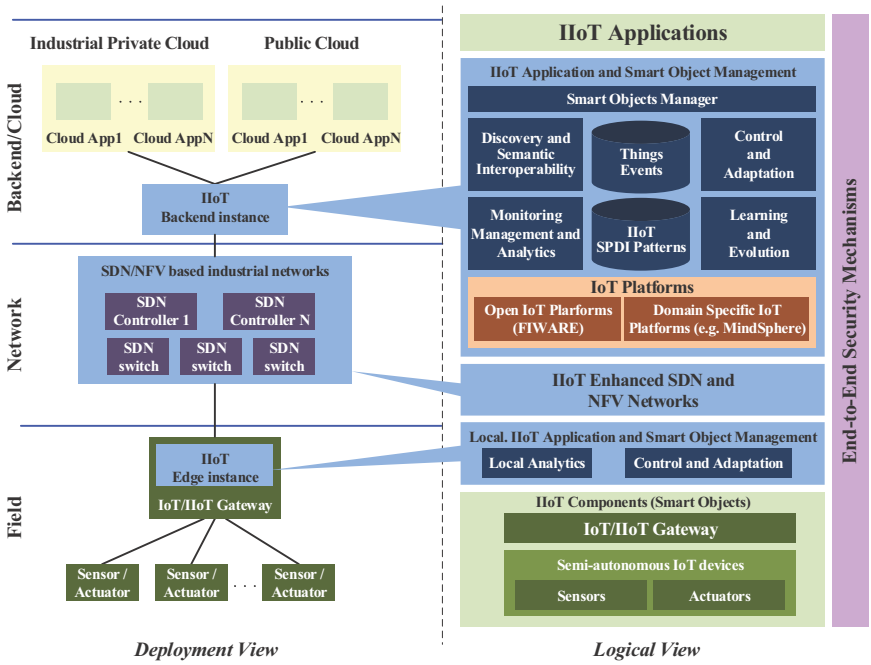

Figure 7.12 SEMIoTICS architecture (deployment and logic views).

take full advantage of underlying network programmability. In summary, **IoT requires more agile networks**.

SDN can provide a solution to this problem. It allows **network programmability**, which can be used to decouple network control from the forwarding network (aka data) plane and to make the latter directly programmable by the former. Integrating IoT and SDN will **increase network efficiency** as it will make it possible for a network to respond to changes or events detected at the IoT application layer through network reconfiguration. If a spontaneous concentration of people in a specific place is detected by an IoT application, for example, the application can send a request to the SDN controller to reconfigure the network and provide more bandwidth to the area before network congestion occurs. As another example, consider an IoT application where sensor readings are transmitted periodically. In such cases, network resources on the path connecting the sensors to the backend IoT application can be reserved during the reporting cycles to enable efficient flows and released outside them. SEMIoTICS aims to develop a middleware layer between the IoT applications and the SDN-controlled field

network, abstracting the underlying protocol implementations and SDN APIs. This will allow **IoT applications** to **trigger** the **network reconfiguration** through **pattern-driven adaptations**. In this view, SDN becomes another component in the IoT implementation stack which, like other components, can be dynamically configured through SPDI patterns [56].

7.6.5.2 Localized analytics for Semi-Autonomous IIoT operation

An IDC FutureScape report [59] for IoT reported that by 2018, 40 percent of IoT data will be stored, processed, analysed and acted where they are created before they are transferred to the network. There are two main reasons for this: *big data volume* and *fast reaction*.

First of all, IoTs/IIoTs are generating an unprecedented volume and variety of data depending on the vertical use case. Not all these data need to be sent always to the cloud for storage and processing. Indeed, the volume of the data makes it in many cases extremely difficult to process them globally in an efficient manner and hinders learning the relations that are hidden in the data. For this reason, we need to enrich the generated and collected data with semantic information at the source and intermediate stations, process them locally with machine learning algorithms to extract the most important features of the data and only then transfer the learned local features to the cloud for further, global, processing and feature analysis. Hence, new approaches, techniques, and corresponding designs need to be developed to store, analyse, and derive insight from these data sets. This has already been identified as a challenge by the industry, e.g. Forrester [60] highlighting the need of IoT applications for distributed analytics since centralized analytics cannot cope for many IoT usage scenarios, and Gartner [61] emphasizing the importance of IoT edge architecture and IT/OT integration for achieving such distributed and layered data analysis.

The second reason driving the need for localized analytics is fast reaction. By the time the data makes its way to the cloud for analysis and some analysis results have been obtained and transferred back to the field layer, so much time has passed that the opportunity to act effectively on the obtained analysis results at the field layer (e.g. smart actuation) is usually long gone. Again, this is a crucial requirement for the industry – Forbes and Moor Insights & Strategy (MI&S) [62] expects that machine learning-enabled reaction to changes in the current environmental/system context to be essential for IoT solutions. By 2020 MI&S believes that the machine learning at edge combined with central machine learning in cloud arrangements will exist in a large number of solutions and will account for a great deal of the innovation

in IoT world – giving a substantial market advantage to the providers of such solutions. By doing a fast analysis on the local data (whose volume is much reduced compared to the entire data produced by the IIoT/IoT system and thus should be analysable with substantially fewer resources), an IIoT/IoT system can react quickly to context changes and adapt to them, in ways that optimise the use of both its own resources and the environment's, and eventually improving the overall user experience. SEMIoTICS will develop localized analytics at the edge for semi-autonomous operation with smart actuation and use the results of the localized analytics to help improve the subsequent, global analysis that will be performed on the cloud for learning across the whole system and extraction of global patterns – itself a task whose results can be used by local analytics mechanisms to improve their performance and be able to proactively react to situations that had not been observed at that local point in the past but had occurred at other parts of the system.

7.6.6 Security Architecture Concept

As aforementioned, the SEMIoTICS vision is articulated around the development of a framework for smart object and IIoT/IoT application management based on trusted patterns, monitoring and adaptation mechanisms, enhanced IoT centric networks and multi-layered embedded intelligence. These core elements of our approach are described below.

7.6.6.1 Pattern-based trustworthy IIoT/IoT

The key element enabling the SEMIoTICS approach is the use of architectural SPDI patterns. These **patterns define generic ways of composing** (i.e., establishing the connectivity between) and **configuring** the heterogeneous **smart objects and software components** that may exist at all layers of the IoT applications implementation stack, including: sensors and actuators; smart devices; software components at the network, cloud, IoT enabling platforms and/or other middleware layer; as well as software components at the IoT application layer. To do so, **patterns specify** abstract and **generic smart object interaction and orchestration protocols**, enhanced (if necessary) by transformations to ensure the semantic compatibility of data. Furthermore (and more importantly), the smart object interaction and orchestration protocols encoded by the patterns must have proven ability (i.e., an ability proven through formal verification or demonstrated through testing and/or operational evidence) to achieve not only a semantically viable interoperability between the smart objects that they compose but also specific

SPDI properties, which may be required of compositions. The **compositions** defined by patterns are both **vertical** and **horizontal**, i.e., they can involve smart objects at the same (horizontal) or different layers (vertical) layer of the IoT implementation stack. As an example of a pattern that guarantees "data integrity" – i.e., absence of unauthorized modifications of data – consider the **integrity preserving cascade composition pattern** discussed in [63, 64]. According to this pattern in a sequential composition of processes $P_1, \ldots, P_n$ where the input data of P_i are meant to be the output data of P_{i-1}, and the communication between P_{i-1} to P_i (i=2,..., n) is based on an orchestrator O which facilitates data transfers from P_{i-1} to P_i, **overall data integrity is preserved** if data integrity is preserved within each P_i, within O and across all communications from P_{iS} to O and vice versa. The integrity cascade composition pattern applies both to horizontal compositions (e.g., in software services workflows as in [63, 64]) and vertical composition (e.g., in transfer of data in invocation of operations of IoT enabling middleware).

Another (more complex) example of a pattern fitting the SEMIoTICS vision is the **synchronously controlled distribution line (SCDL) pattern** discussed in [54]. SCDL guarantees that a distributed asynchronous sensor system installed upon a physical pipeline (e.g., a pipeline of an electricity distribution network) will operate in virtual synchrony and provide **a guaranteed density of readings** (i.e., a bounded minimum number of readings per distant and per time unit). The pattern suggests a composition consisting of: (i) sensors connected to a controller through a middleware component that realizes a bounded reliable message delivery protocol; (ii) a controller with the capability to authenticate sensors, store readings received from them in fixed length intervals, and **substitute missing or corrupted sensor readings** with synthetic readings computed through the linear interpolation of readings from their closest adjacent sensors and the end of reading intervals. The application of the **SCDL pattern** is proven to **guarantee** the **consumption of readings** at the end of the reading interval where they fit, make them available in a synchronous manner, filter out illegitimate readings and produce **readings of the required density** for the pipeline. In SCDL pattern, these properties are **guaranteed** even **in the presence of missing or corrupted raw data**, as long as there is a minimal number of legitimate sensor readings. Examples of additional patterns have been given in [52] and [56]. These include patterns for confidentiality in service orchestrations and patterns for availability in Software Defined Networks, respectively.

Inspired by these earlier works, SEMIoTICS patterns will develop patterns specifying:

- **Composition structures** for integrating smart objects and components of IoT enabling platforms (e.g., platform enablers) in a manner that guarantees SPDI properties.
- The **E2E SPDI properties** that the compositions expressed by the pattern preserve.
- The **component level SPDI properties** that the types of smart objects and/or components orchestrated by the pattern, must satisfy in order to preserve the end-to-end SPD properties.
- **Additional conditions** that need to be satisfied for guaranteeing end-to-end SPDI properties. These may, for example, include configuration conditions that need to be satisfied by the IoT platforms and the networks providing the connectivity between them, for guarantying the end-to-end availability properties of IoT application (composition).
- **Monitoring checks** that must be monitored at runtime in order to verify that any assumptions about the individual smart objects and components that are orchestrated by a pattern or other operational conditions, which are critical for the preservation of the end-to-end SPDI properties of the pattern, hold at runtime.
- **Adaptation actions** that may be undertaken to adapt IoT applications, which realise the composition structure of the pattern, at runtime. Such actions may, for example, include the replacement of individual smart objects within a composition; the adaptation of the process realizing the composition; the modification of the configuration of the network services used to connect the smart objects of the composition and/or the deployment platforms upon which these objects run. Adaptation actions are specified along with guard conditions determining when they can be executed (guards are monitored, and adaptation is triggered when they are satisfied).

SEMIoTICS will also develop a generic engine supporting the execution of patterns at runtime to realize the overall process of monitoring, forming, adapting and managing smart object orchestrations in IoT applications.

7.6.6.2 Monitoring and adaptation

The SEMIoTICS framework will support **evolving runtime** management and **adaptation** of IoT applications and smart objects [55–58]. Adaptation will be triggered by monitoring the guard conditions of the patterns used by the IoT application of interest, and applying the actions defined in the patterns when such conditions are satisfied. The SEMIoTICS framework will also **monitor** and analyse the **effectiveness of patterns** and the **adaptation**

actions undertaken in reference to the contextual and operational conditions in which they were undertaken. This will be to **identify** deficiencies or **failures** in applying the patterns, to **diagnose** the reasons which may have caused **deficiencies** or **failures** and avoid the application of the same pattern(s) under the same conditions in subsequent phases. The use of a specific type of network connectivity or a specific type of sensor object amongst alternative options may, for example, prove to be a non-optimal option for network performance or sensor signal reliability under particular conditions. Similarly, certain data transformations may prove excessively time consuming for achieving the required scalability in an IoT application. Monitoring will also be necessary to ensure that any component level SPDI properties assumed by the pattern are upheld whilst the pattern is active (i.e., in use) in an IoT application.

Beyond the basic monitoring of the contextual circumstances surrounding the operation of different smart objects and IoT applications, the SEMIoTICS framework will incorporate **learning** and **evolution mechanisms** supporting the analysis of any adaptation and configuration actions undertaken for an IoT application. This will be necessary in order to identify whether the application of patterns is effective over time (e.g., it does indeed prevent the occurrence of breaches of SPDI properties) and what might be the reasons for not being effective when this is the case.

7.6.7 Use Cases

SEMIoTICS will target three IoT application scenarios: two verticals in the areas of energy and health care and one horizontal in the areas of intelligent sensing. These scenarios have been selected since they involve: (a) different and heterogeneous types of smart objects (i.e., sensors, smart devices, actuators) and software components; (b) different vertical and horizontal IoT platforms; and (c) different types of SPDI requirements. Due to these dimensions of variability, our scenarios provide comprehensive coverage of technical issues, which should be accounted for in developing the SEMIoTICS approach and infrastructure, and to this end provide an effective way for driving the R&D work programme of SEMIoTICS and evaluating and demonstrating its outcomes.

7.6.7.1 Renewable energy – Wind energy

Current state of the art of Wind Turbine Controller in a Wind Park control network is typically an embedded or highly integrated operating system, which follows rigorously development and pre-qualification prior

to deployment in the real world. As a result of this slow process, new features, adding new sensors, actuators and related advancements require several months or even years to be fully matured and operational in the field.

- **Taking local action on sensing and analysing structured data to find the inclination of a steel tower** – When the nacelle is turned during a cable untwisting event (Sensing), the gravity acceleration (Ag) component measured by an accelerometer in longitude direction (Ay) will vary as a function of the inclination (Inc) of the steel tower. O&M personnel in remote control center wants to know the inclination of all the steel towers on a number of specific wind farms, as these details will have to be shared with the customer to monitor the deformation and fatigue of the steel. To find the inclination of a steel tower, a full cable-untwist procedure has to be activated. This happens, depending on wind conditions, 3–4 times a month. It is also possible to manually instruct the wind turbine to perform the unwind procedure. At the time of the unwindingprocedure a hi-frequency set of data is recorded. A relatively large amount of data is required to calculate the inclination. This datasheet needs to be sent back to the remote control center to model and calculate the inclination. In SEMIoTICS, localized edge analytics will be applied which will result in semi-autonomous IIoT behavior as only the container containing the algorithm and result of the inclination calculation is transferred to between the wind turbine and the remote control centre. The unnecessary data traffic between each turbine and remote control centre is greatly reduced. Without the localized analytics functionality, all the hi-frequency acceleration and nacelle position data should have transferred to remote control centre resulting in suboptimal operation.
- **Smart Actuation by sensing unstructured video/audio data** – Within the turbine, there are many events which can be captured by IIoT sensors such as Grease leakage detection during normal operation or unintended noise detection when the turbine rotor is changing the direction in the line of wind to maximize energy production. The sensing of this unstructured data and acting locally to prevent any damage to the parts of the turbine in the long run will be of key importance. Localized analytics, as proposed in SEMIoTICS, which will lead in smart actuation to protect the critical infrastructure of renewable energy resources.

SEMIoTICS implements:

- Industrial Things semantic discovery, Bootstrapping of IIoT devices and Gateway
- Inventory of the things at the SDN controller
- REST-based Intent interface for network-agnostic cloud applications
- Security at every layer
- Local data analytics at the Sensors, Actuators and Gateway

7.6.7.2 Healthcare

This healthcare use case is an attempt to come up with usable, acceptable and sustainable IoT solution for assisted mobility through falls prevention leading to active and healthy ageing. Falls in older adults are a significant cause of morbidity and mortality and are an important class of preventable injuries. This use case specifically focuses on advanced fall prevention and management solution aimed at both senior citizens and adults with Mild Cognitive Impairment or mild Alzheimer's disease and their (informal) caregivers. The objective of this scenario is to extend the existing IoT platform like AREAS with Assisted Mobility Module (AMM) which is a dedicated module for the management of, and integration of information from, a network of IT services and hardware devices constituting an advanced fall prevention and management solution aimed at both senior citizens and adults with Mild Cognitive Impairment or mild Alzheimer's disease and their (informal) caregivers. Given the figures introduced at the beginning, the social dimension of the solution is reflected in the improved quality of life for people that are susceptible to falls, given that AMM will prolong the time they can work and live independently. The envisaged evolution of the AMM will see the inclusion of additional robotic elements, in particular, the system will include a:

- Robotic Assistant (RA) connected to a network of embedded **IoT devices and services for monitoring** (and maintaining a diary of) a **patient's activities, health status and treatment**, as well as for supporting cognitive skills training, notifying/reminding the patient of upcoming treatments (e.g. medication schedules) and visits.
- Personal assistant robots may help the patients with their **daily activities like walking trail and other routine**.

SEMIoTICS will contribute in the:

- Integration of distributed IoT devices with higher degree of autonomy (i.e. robotic devices)
- Exploitation of computational resources both in the cloud and at the edge
- Security and privacy of patient data, safety of a patient

7.6.7.3 Generic IoT & smart sensing

Today's IoT embedded devices are often described as smart devices. "Smart" usually shall be associated to some Things that show some form of intelligence, bright behaviour during their operations. Unfortunately, current meaning and their reality is that they are locally programmable and always connected to some cloud infrastructure (e.g. typically through a wireless connection such as Wi-Fi or Bluetooth Low Energy) to send raw data. Therefore, these devices transmit sensed data to the cloud without any analytic being performed locally and without showing remarkable forms of computational intelligence. An IoT thing is intelligent is it has capabilities **to learn from and act upon the data (at least without supervision)** it is sensing. Sometimes, they also receive back from the cloud some form of actuation (control) instructions, which are determined by a centralized server-based analysis of sensed and other data. A typical example, on domotic applications, is the one where several sensing nodes stream some relevant raw data at given interval (e.g. temperature, humidity, pressure) to a cloud service. An example is the Microsoft Azure or IBM Bluemix cloud platforms and related ecosystem. In this scenario, the intelligent data processing always resides remotely, and the communication channel is (implicitly) assumed to be always present and open.

The use case provides:

- Evolution of platform technologies enabling local analytics computing (i.e. edge computing)
- Enhanced IoT system scalability and increased robustness
- Open market enhanced middleware portfolio for intelligent embedded devices and innovative businesses opportunities

SEMIoTICS's research efforts focus in the:

- Support for tight integration at device level of sensing and computational elements in close tight cooperation on dedicated embedded HW (i.e. edge computing)

- Increased system scalability and computational partitioning to enhance system responsiveness and stability by exploiting self-adapting online learning mechanisms
- Enhanced architectural models redefining system from bottom to top for handling the continuous and discrete sensing.

7.6.8 Summary

SEMIoTICS aims to develop an open IIoT/IoT framework, interoperating with existing IIoT/IoT platforms (e.g. FIWARE, MindSphere) and programmable networking, through their exposed APIs. The SEMIoTICS framework will also integrate IIoT and IoT sensing and actuating technologies. A core element of the SEMIoTICS approach is the development and use of patterns for orchestration of smart objects and IoT platform enablers in IoT applications with guaranteed SPDI properties. Patterns constitute an architectural concept well founded in software systems engineering. SEMIoTICS advocates the patterns approach to systems engineering, but uses a novel pattern type (i.e., SPDI patterns) to guarantee semantic interoperability, security, privacy and dependability in large scale IIoT/IoT applications integrating smart objects. Said patterns will be supported by mechanisms featuring integrated and predictive monitoring of smart objects of all layers of the IoT implementation stack in a scalable manner, as well as core mechanisms for multi-layered embedded intelligence, IoT application adaptation, learning and evolution, and end-to-end security, privacy, accountability, and user control. This approach will enable and guarantee secure and dependable actuation and semi-autonomic behaviour in IoT/IIoT applications, supporting cross-layer intelligent dynamic adaptation, including heterogeneous smart objects, networks and clouds.

7.7 SerIoT

The Internet of Things or Internet of Everything envisages billions of physical things or objects (sensors and actuators) connected to the Internet via heterogeneous access networks. IoT is emerging as the breakthrough technology introducing the next wave of innovations, including revolutionary applications, significantly improving and optimizing our daily life.

The IoT is capable to create a complex Network of Networks system through IP protocol and Mobile Network connectivity, allowing “things” to be read, controlled and managed at any time and at any place. This brings

such technical issues as the lack of a shared infrastructure, lack of common standards, problems with the flexibility, scalability, adaptability, maintenance, and updating the IoT devices, etc.

Especially important are security concerns, resulting from all of the listed technological aspects [77, 78]. In case of lack of the IoT related security standards and commonly accepted technological solutions, every vendor creates their own solutions. Moreover, the solutions currently used in IT systems are mostly unsuitable for direct application in IoT, e.g. authentication based on central server that works well for small scale systems but does not provide sufficient mechanisms for future large scale IoT ecosystems. On the other hand, attacks on the IoT platforms will have significant economic, energetic and physical security consequences, beyond the traditional Internet lack of security.

7.7.1 SerIoT Vision and Objectives

SerIoT aims to conduct research for the delivery of a secure, open, scalable and trusted IoT architecture. The solution will be implemented and tested as a complete, generic solution to create and manage large scale IoT environment operating across IoT platforms and paying attention on security problems.

A decentralized approach, based on peer to peer, overlay communication is proposed [69]. SerIoT will optimize the security of IoT platforms in a cross-layered manner. The concept of Software Defined Networks (SDN) is used and SDN controllers are organized in hierarchical structure [74, 75]. The objectives of SerIoT include to provide the prototype implementation of a self-cognitive [66–68], SDN based core network, easily configurable to adapt to any IoT platform, including advanced analytics modules, self-cognitive honeypots and secure routers. The solution will be supported by appropriate technologies such as Decision Support System (DSS) supplementing controller's functionality. The DSS will be able to detect the potential threats and abnormalities. The system will be supplemented with comprehensive and intuitive visual analytics and mitigation strategies that will be used according to the detected threats. It will be validated in the final phase of the project through representative use cases scenarios, involving heterogeneous EU wide SerIoT network system.

7.7.2 SerIoT Architecture Concept

The SerIoT architecture [65] is based on a software-managed network implementing SDN technology and is divided into the following layers and modules (See Figure 7.13.).

The **IoT Data Acquisition layer** is comprised of the low-level IoT-enabled components that create the infrastructure backbone, including honeypots, dedicated engines and storage capabilities and the SDN secure routers. The SDN routers will use OpenFlow communication and will be based on Open Switch implementation being significantly extended to cooperate with related SerIoT modules and security mechanism.

The backbone network will be divided into domains (subnets). Every subnet constitutes an autonomic SDN network, controlled by the SDN controller and extended according to SerIoT needs. Controllers will be organized into hierarchical structure [76]. The first level controller is responsible for the routing within the subnet using gathered data. It will be also able to route packets to neighbouring subnets (via the appropriate border node). In the case of destinations outside their own subnet and neighbouring subnets, routing requests will be sent to a second (or third, fourth, etc.) level controllers. The controllers will continuously gather information to feed the analytics module.

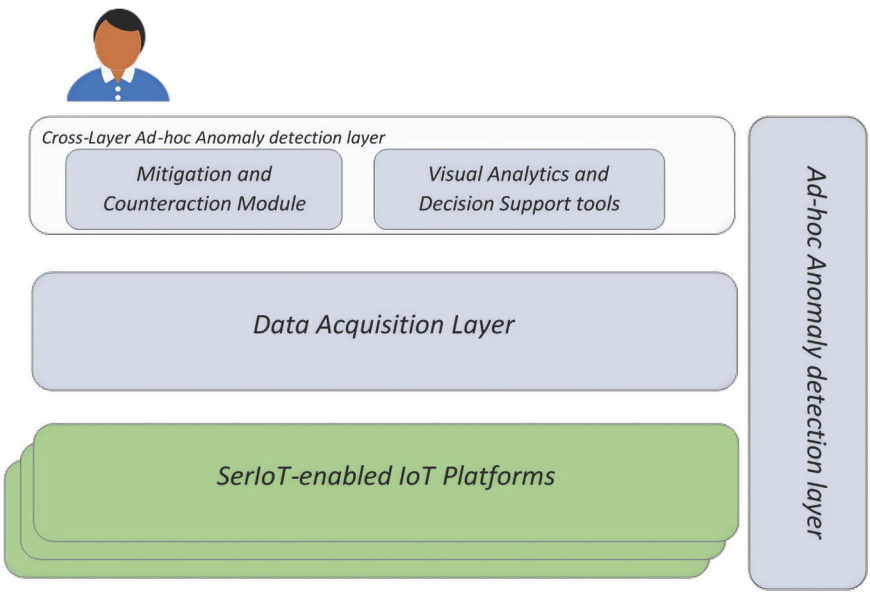

Figure 7.13 The structure of layered SerIoT architecture.

These components will be connected to visual analytics module and support decision making system.

The **Ad-hoc Anomaly detection layer** will provide a number of security mechanisms, executed across IoT devices, honeypots and SDN routers. Anomaly detection techniques based on local traffic characteristics (as dynamic changes in queue lengths) will be regularly probed by smart "cognitive packets" sent by the SDN controller and feeding the controller routing decisions. The controller will have the ability to detect suspicious and risky paths, and re-schedule the routing paths over secure, preferable connections according to secure aware routing, but also energy and Qality of Service (QoS) aware routing [71–73].

The **Visual Analytics and Decision Support tools** will deal with the interactive decision support applications that will be delivered to the end-users, able to effectively detect potential abnormalities at different levels of the network. The end-user tool will be developed together with a novel visual analytics framework, dealing with the effective management and visualization of data.

The **Mitigation and Counteraction Module** will be responsible for implementing decisions taken by the Decision Support tools. The module will use dedicated software and network components as SDN routers, honeypots and IoT devices.

The SerIoT platform will ensure the separation of enterprise and private data. The system will provide monitoring mechanisms and anomaly detection techniques, using a cross-layer data collection infrastructure that will allow effective information transmission and data aggregation for analysis. A prototype honeypot with the ability to analyse network traffic and detecting anomalies will be developed. This new architecture for ensuring security, based on SDN technology, should bring a significant progress in comparison to current solutions.

The innovatory approach used in SerIoT network will be using Cognitive Packets [70] for gathering network data on QoS, security state and energy usage, and Cognitive Packet Network routing engine, based on Random Neural Networks (RNN) [79, 80]. The concept is a combination of neural-networks-based routing and source routing. It was successfully applied in SDN network [71], and in the SerIoT project will be extended both in terms of data used as input for routing engine and of scale of the networks. Security data will be used as input for learning of RNN, along with QoS and energy usage data, to allow finding secure and efficient routes for every SDN flow.

7.7.3 Use Cases

The solutions of the SerIoT project will be evaluated in individual laboratory test-beds and also in an integrated EU wide test-bed which will interconnect significant use cases developed by SerIoT industry partners.

SerIoT aims to design and to deploy four innovative use cases arising from three significant for the global economy domains where the use of IoT is rapidly increasing: (i) Smart Cities domain will be covered by two ambitious use cases where Surveillance and Intelligent Transportation IoT networks will be evaluated, (ii) Flexible Manufacturing domain with the detection of physical attacks on wireless sensor networks, and finally (iii) a novel Food Chain Scenario will be exploited demonstrating mobility security issues.

Each of the use cases considers one or several scenarios. A scenario is intended to describe and specify the system behaviour according to a specific situation, or in other words to describe the situation in which a specific system should work and how the system works and interacts with the different users:

- Use Case 1 (Surveillance) scenarios:
- Facilities monitoring
- Embedded intelligence in buses
- Use Case 2 (Intelligent Transport Systems ITS in Smart Cities) scenarios:
- Automated driving
- Public transport maintenance
- Public transport security
- Road side ITS stations
- Use Case 3 (Flexible Manufacturing Systems) scenarios:
- Wireless robots in warehouse
- Critical infrastructure protection
- Use Case 4 (Food Chain) scenario:
- Fresh food deadline control

7.7.4 Industrial and Commercial Involvement

SerIoT has strong support regarding industrial know-how and implementation. Among the Consortium partners there are eight industrial or small/medium size enterprises (SME) with diverse and complementary technological and research expertise, covering the full spectrum of research and innovation activities anticipated in the project [65]. Six of these partners are large industrial societies able to support the multi-disciplinary topics

introduced in SerIoT, i.e. IoT telecom/network infrastructure & Industry 4.0 Use Cases by DT/T-Sys, IoT anomaly detection by ATOS, IoT applications & platform by DT/T-Sys., design-driven & cross-layer analytics by ATOS. Moreover, SMEs involved in the consortium are among the leading and innovative companies in their sectors. Hence, a large amount of innovation foreseen in the project will be also carried by SMEs. What all SerIoT SME partners share in common is their proven ability to apply research results into successful and well established commercial products (e.g. HOP Core, Wear & Extended innovative solution by HOPU). Having in mind their strong commitment in delivering new services in their customers, industrial & SME partners have identified complementary private investments to support the SerIoT business perspectives.

Moreover, specific dissemination actions will be carried out, through already established communication channels, networks and working groups in order to ensure that the new & open solutions of the project will be conveyed to major stakeholders in Europe and Worldwide.

7.7.5 Summary

In this paper we outline the EU H2020 SerIoT project that addresses IoT security challenges. As a scientific project, SerIoT will provide a new approach to understand the threats to IoT based infrastructures and deliver methods to solve the security problems in the IoT. Pioneering research and development based on holistic approaches will be conducted. A generic IoT framework based on an adaptation of the concept of Software Defined Networks with Cognitive Packets will be developed as well as the new methods for intrusion detection with the use of a cross-layer approach. Visual analytics tools for analysing threats in IoT ecosystem will be used.

7.8 SOFIE – Secure Open Federation for Internet Everywhere

The **main goal** of the SOFIE [83] project is to *enable diversified applications from various application areas to utilise heterogeneous IoT platforms and autonomous things across technological, organisational and administrative borders in an open and secure manner, making reuse of existing infrastructure and data easy*. SOFIE is guided by the needs of three pilot use cases with diverse business requirements: food supply-chain, mixed reality mobile gaming, and energy markets. Furthermore, we will explore the synergies among

these areas, building a foundation for cross-application-area use of existing IoT platforms and data.

SOFIE will design, implement and pilot a systematic, open and secure way to establish new business platforms that utilise existing IoT platforms and distributed ledgers. With *"openness"*, we mean flexible and administratively open business platforms, as well as technically decentralised federation to enable the interoperability of different IoT platforms, ledgers, and autonomous devices. To realise this vision, SOFIE brings together large system vendors and integrators (ENGINEERING and Ericsson), high tech SMEs delivering highly innovative products and solutions (GuardTime, Synelixis) and prestigious universities (Aalto University and the Athens University of Economics and Business). The results of the project will be guided by these three use cases and will be tested in an equal number of real-life trials. For this purpose, the consortium includes ASM TERNI S.p.A., a public multi-utility company and Emotion who will trial SOFIE developments in the energy sector, OPTIMUM, a leading SME in the area of supply chain IT systems, which (together with SYNELIXIS) will trial SOFIE in the realisation of a farm-to-fork scenario and Rovio Entertainment Corporation, which will lead the SOFIE trial in a mixed reality mobile gaming context.

7.8.1 Objectives

- The SOFIE consortium has broken down the high-level goal into the following specific and tangible objectives:
- Define a secure, open, decentralised and scalable IoT federation architecture for sensing, actuation, and smart behaviour. In order to stay open and interoperable, emerging standard interfaces should be used between the components and towards the outside world.
- Make IoT data and actuation accessible across applications and platforms in a secure and controlled way. SOFIE must provide the means to reuse data, within the limits set by its owner, across applications.
- Develop a solution to provide integrity, confidentiality and auditability of IoT data, events and actions. SOFIE shall define and implement ledger-independent transactions that can be simultaneously entered into various closed and open blockchains and other persistent ledgers.
- Develop an IoT federation framework to facilitate creation of IoT business platforms. The framework can be used to create business platforms, including those for the three pilot use cases.

- Deploy and evaluate the SOFIE federation framework in three field trials.
- Evaluate the commercial viability of the SOFIE federation approach based on the three field trials and research on business models.
- Establish the SOFIE IoT federation approach as a major enabler for the IoT industry through dissemination, standardization, education, workshops and pilots.

7.8.2 Technical Approach

SOFIE combines several IoT platforms and distributed ledgers into a federated IoT platform supporting the reuse of existing IoT infrastructure and data by various applications and businesses. Figure 7.14 illustrates the overall architectural approach.

SOFIE achieves decentralization of business platforms through the use of DLTs. Since the properties of various DLTs, such as scalability, throughput, resilience, and openness, are significantly different, SOFIE relies on using multiple different DLTs in parallel. To allow transactions to be recorded into multiple blockchains or other ledgers, SOFIE will design and implement the inter-ledger transaction layer. We will build upon existing leading-edge work, including the W3C-associated Inter-ledger Protocol (ILP), applying the results to the IoT domain, and developing them further. The transactions will be implemented as multi-stage smart contracts whose resolution depends on

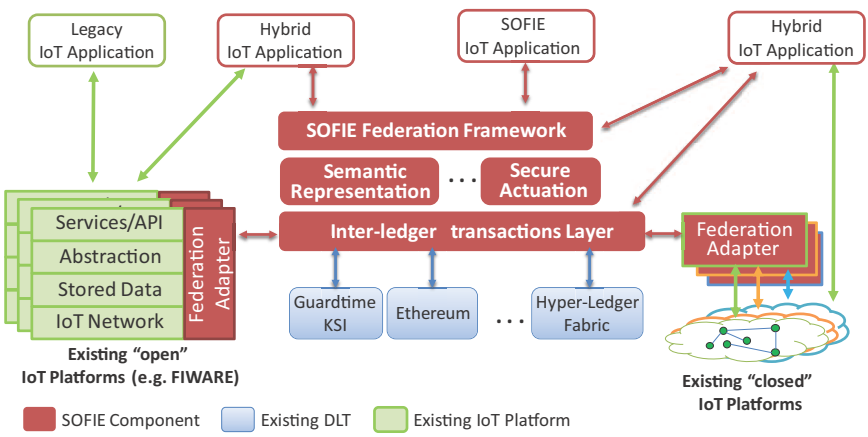

Figure 7.14 SOFIE Secure and Open Federation Architecture.

the transactions being correctly recorded in all the participating ledgers, but without requiring that all the ledgers support smart contracts.

The inter-ledger transaction layer will be used for three main purposes:

- **Describe the ("things") data in the existing IoT platforms,** enabling financially tied IoT actuation between organisations and storing security-related data.
- **Enable secure and traceable IoT actuation.** The idea is to negotiate and use smart contracts that may span multiple ledgers to record intention or desire to actuate, to trigger actuation, to permanently record both actuation instances and the related sensor values, and to trigger any financial transactions, thereby supporting smart behaviour.
- **Enable interoperability between diverse existing IoT platforms.** This is achieved by augmenting the existing IoT platforms with a federation adapter.

These together allow applications to: discover what data and things are available in the IoT platforms; acquire the necessary permissions for access (e.g. by promising to pay or placing a pledge); access the data and/or request actuation in a secure, recorded, and compensated manner; and verify whether the requested actuation took place or not. Beneath the inter-ledger transaction layer are distributed ledgers. These include commonly used blockchains such as Ethereum, and private commercial blockchains such as KSI Blockchain developed by SOFIE partner Guardtime [81].

The SOFIE federation approach is designed to be technology-agnostic, allowing systems with different APIs and data formats to interoperate to the extent allowed by the applicable security policies. Some of the existing IoT platforms already support interoperability across different protocols and standards. Examples of this include FIWARE through its IoT adapters [84], such as the already existing LWM2M and oneM2M adapters, and W3C WoT, where the IoT servient concept supports both proprietary APIs and various protocol adapters. While most of the data will reside within existing IoT systems, a key aspect of SOFIE is the so-called **smart contract**, available in some blockchains, such as Ethereum. From the SOFIE point of view, a smart contract is simply a computer program and its associated computational state that "lives" in a blockchain.

7.8.3 Security Architecture

The SOFIE security architecture provides end-to-end security (confidentiality and integrity), identification, authentication and authorization, and supports users' privacy and control over their data. Most existing solutions already provide decent end-to-end security within the system and system-specific authentication. Therefore, SOFIE concentrates on innovating in the areas of data sovereignty, privacy and federated key management, authentication, and authorization.

IoT data can often be personal and therefore governed by a new EU's GDPR legislation. Ensuring compliance with the GDPR is a major design requirement for the SOFIE security architecture. SOFIE plans to use MyData [85] together with Sovrin Foundation identity blockchain [86] to allow individuals to better control how their personal data is used.

In order to support data sovereignty and privacy, SOFIE adopts a three-level approach to the storage of data. First, there is a private data store managed entirely by the stakeholder. A private blockchain (such as Guardtime's KSI Blockchain) forms the second level data that is shared between collaborating stakeholders (for examples producer, reseller, and supermarket in the food chain use case). Finally, some data (such as hashes of transaction trees from the lower level) will be stored in a public blockchain, such as Ethereum or Bitcoin. Such an approach allows fine grained control of the data, from total openness (e.g. to bring transparency to certain public services) to very tight access control (e.g. to protect trade secrets or the privacy of people). In either case, integrity and non-repudiation of the data is guaranteed.

7.8.4 Use Cases

The SOFIE approach will be tested in three different use cases described below. The **food chain pilot** aspires to demonstrate the field-to-fork scenario towards security in food production and consumption. SOFIE applications and realization of a community-supported heterogeneous end-to-end agricultural food chain will be demonstrated and evaluated. The use case will combine multiple types of ground, micro-climate, soil, leaf and other information stations, existing IoT platforms, mobility, location-based services (LBS), food tracking information, smart micro-contracts, and decentralized autonomous organizations implemented with smart contracts. The consumer may trace the entire history of the product based on the QR or RFID tag on the package, even in the shop before buying the product. Consumers can

reliably verify not only the farmer from whom the product originates, but also the entire production and supply chain history associated with each food item, starting from the source of the seeds, the quality of the soil and the air in the producer's premises, the amount of water that has been consumed, the fertilization process, the method and time of growing, the weather conditions, the transportation mode and distance, the storage conditions etc. This gives consumers the ability to make decisions about their food based on health and ethical concerns, including environmental sustainability, fair labour practices, the use of fertilizers and pesticides, and other similar issues.

In the **Mixed Reality Mobile Gaming Pilot, virtual and real worlds will be combined.** Mobile gaming is a rapidly growing market, popular games, such as *Pokémon Go*, are already taking advantage of augmented reality and SOFIE aims to take such interaction further. SOFIE will integrate a mobile game with the real world using a federated IoT platform aiming to: a) enable the gamers to interact with the real world via sensors and actuators, b) take advantage of existing and emerging IoT infrastructure (e.g. building automation), c) enable payments in virtual and real currencies between the gamers, games, and other parties, and d) create new business opportunities for various parties, including gaming companies, as well as the owners of buildings and public spaces (e.g. malls) and various businesses (e.g. shops and cafés). The gamers will be both moving in the physical world and interacting with it through the games. Existing IoT infrastructure, for instance movement sensors and control of lighting and passage, will be included in the game world through the federated SOFIE platform. Owners of spaces and businesses will be able to bring their existing or new IoT infrastructure into the gaming world, while the blockchain-based marketplace will allow for all kinds of business models, including In-Game Assets (IGA) trading.

The **energy pilot** aims at optimized Demand Response and at supporting electricity marketplaces and micropayments. The energy pilot consists of two parts: first, a **real-field** pilot will demonstrate the capability of creating smart micro-contracts and micro-payments in a fully distributed energy marketplace, located in Terni, Italy. The pilot will cover the end-to-end scenario form electricity production, distribution, storage and consumption. During the scenario electricity produced by renewable sources (PVs) will be fed into the low voltage (LV) electricity network. Most of this electricity will be normally consumed by energy customers (i.e. houses, offices, etc). However, the surplus of the generated power would generate reverse power flows through the LV distribution network substation. The electricity distribution network is designed to handle only unidirectional electricity flows, thus

reverse flows may generate significant problems. To avoid this abnormal operation, electrical vehicles (EVs) will be offered significant promotional benefits to match their EV charging needs with the network time and space balancing requirements. The EV chargers will be communicating with the EV drivers, with the car battery management system, the local energy generation and consumption, and the smart meters to predict if the requested charging service/network grid stabilization will be available in due time. Second, a **laboratory and interoperability pilot** based on real-data from smart energy meters deployed in the greater area of Tallinn, Estonia. The trial will be based on the Estfeed open software platform [87] for energy consumption monitoring and management from the customer (consumers/prosumers) side, which is capable of interacting with the power network and to provide data feeds for efficient use of energy.

To assess **cross-SOFIE interoperability**, SOFIE pilots will be federated as shown in Figure 7.15. In the cross-pilot, the emphasis will be on the demonstration of the exploitation of data stored/cached in different locations to be accessed across different platforms, as well as the development of

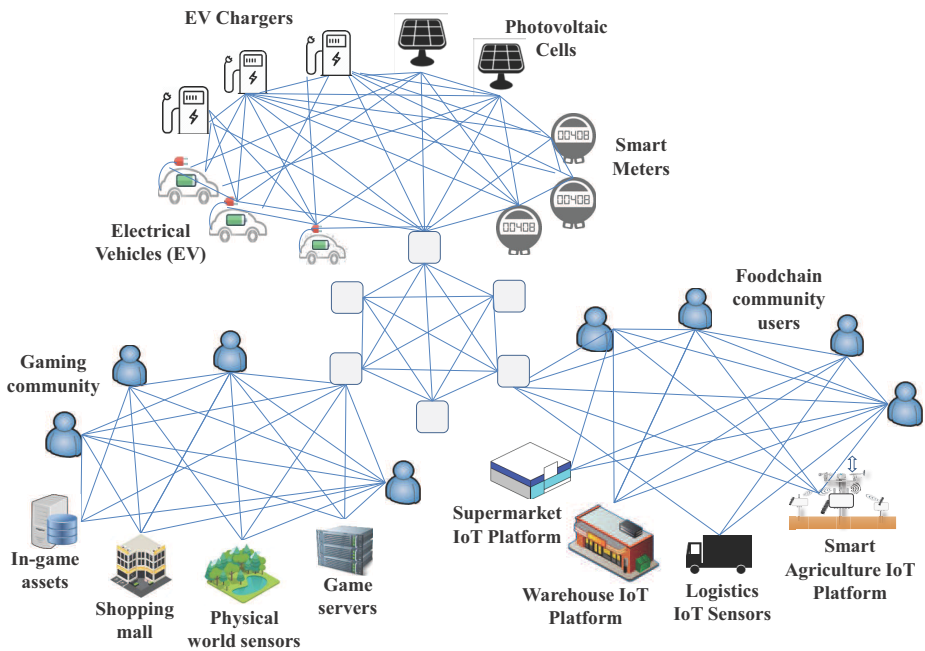

Figure 7.15 Three SOFIE pilots.

applications exploiting different underlying infrastructures. The SOFIE interfaces abstraction will allow virtual entities in one platform to be exploited by applications from a different platform, while data semantics and analytics will facilitate the data exploitation. Initial consideration of scenarios to be tested include: Energy and gaming pilots exploiting data protection/privacy (e.g., for building access), energy pilots (EV) exploiting smart agriculture data with respect to environmental conditions and payments and contracts across pilots (e.g., getting food discounts from gaming achievements).

7.8.5 Conclusions

The SOFIE federation approach will help make the existing siloed IoT platforms interoperable, enabling cross-platform applications and reuse of data in a secure and scalable manner. SOFIE will offer data sovereignty in GDPR-compliant way, giving users more control of their data. Through the usage of distributed ledgers, SOFIE will promote open business platforms, allowing creation of new kinds of decentralised open marketplaces, which no single entity – public or private – can technically control and thus exercise sole pricing power over them. This in turn will lower the barrier of entry for small businesses and individuals. The SOFIE federation framework will be released as open-source and SOFIE partners have the capacity to deliver and boost the penetration of SOFIE offerings in the market and relevant standardization bodies.

List of Notations and Abbreviations

Notations	Abbreviations
AAA	Authentication, Authorisation and Accounting
ABE	Attribute-Based Encryption
CP-ABE	Ciphertext-Policy Attribute-Based Encryption
DHT	Distributed Hash Table
IoT	Internet of Things
JSON-LD	JavaScript Object Notation for Linked Data
KPI	Key Performance Indicator
QoS	Quality of Service
QoI	Quality of Information
OMB	Overlay Management Backbone
RDF	Resource Description Framework
RDQL	RDF Data Query Language

Notations	Abbreviations
TEEs	Trusted Execution Environments
API	Application Programming Interface
bD	by-Design
CE	Circular Economy
E2E	End-to-End
GDPR	General Data Protection Regulation
EU	European Union
ICT	Information Communication Technologies
IoT	Internet of Things
IIoT	Industrial IoT
ML	Machine Learning
NFV	Network Function Virtualization
SDN	Software-Defined Networking
SPDI	Security, Privacy, Dependability and Interoperability

References

[1] International Telecommunication Union (ITU), report on Climate Change, Oct. 2008.
[2] G. Koutitas, P. Demestichas, 'A review of energy efficiency in telecommunication networks', Proc. In Telecomm. Forum (TELFOR), pp. 1–4, Serbia, Nov. 2009.
[3] Gartner Report, Financial Times, 2007.
[4] I. Cerutti, L. Valcarenghi, P. Castoldi, 'Designing power-efficient WDM ring networks', ICST Int. Conf. on Networks for Grid Applic., Athens, 2009.
[5] W. Vereecken, et. al., 'Energy Efficiency in thin client solutions', ICST Int. Conf. on Networks for Grid Applic., Athens, 2009
[6] J. Haas, T. Pierce, E. Schutter, 'Datacenter design guide', White Paper, The Green grid, 2009.
[7] Intel, 'Turning challenges into opportunities in the data center', White Paper, online at: www.intel.com/Intel.pdf
[8] Adel S. Elmaghraby, Michael M. Losavio, "Cyber security challenges in Smart Cities: Safety, security and privacy", Journal of Advanced Research Volume 5, Issue 4, Pages 491–497, July 2014.
[9] CHARIOT Grant Agreement number 780075, Annex 1, Part A.
[10] CHARIOT Grant Agreement number 780075, Annex 1, Part B.
[11] VESSEDIA Project website, https://vessedia.eu/ (last access May 2018).

[12] CHARIOT Project website, http://www.chariotproject.eu/ (last access May 2018).
[13] How To Make 2017 The Year Of IoT Security, William H. Saito, Forbes, 2017.
[14] With the Internet of Things, we're building a world-size robot. How are we going to control it?, Bruce Schneier, New York Magazine, January 2017.
[15] The Internet of Things becomes the Internet that thinks with Watson IoT, https://www.ibm.com/internet-of-things, (last access May 2018).
[16] IEC: IoT 2020: Smart and secure IoT platform. IEC white paper (2016)
[17] NESSI: Cyber physical systems: Opportunities and challenges for software, services, cloud and data. NESSI white paper (2015).
[18] NESSI: SOFTWARE CONTINUUM: Recommendations for ICT Work Programme 2018+. NESSI report (2016).
[19] Humble, J., Farley, D.: Continuous Delivery: Reliable Software Releases through Build, Test, and Deployment Automation. Addison-Wesley Professional (2010).
[20] Taivalsaari, A., Mikkonen, T.: A roadmap to the programmable world: software challenges in the iot era. IEEE Software 34(1) (2017) 72–80.
[21] Morin, B., Fleurey, F., Husa, K.E., Barais, O.: A generative middleware for heterogeneous and distributed services. In: 19th International ACM SIGSOFT Symposium on Component- Based Software Engineering (CBSE), IEEE (2016) 107–116.
[22] I. Stoica, R. Morris, D. Karger, M. F. Kaashoek, and H. Balakrishnan, "Chord: A scalable peer-to-peer lookup service for internet applications," in Proceedings of the 2001 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications, (New York, NY, USA), pp. 149–160, ACM, 2001.
[23] P. Maymounkov and D. Mazieres, "Kademlia: A peer-to-peer information system based on the xor metric," in Proceedings of the First International Workshop on Peer-to-Peer Systems, (London, UK), pp. 53–65, Springer-Verlag, 2002.
[24] L. Cheng, et al., "Self-organising management overlays for future internet services," in Proceedings of the 3rd IEEE International Workshop on Modelling Autonomic Communications Environments, (Berlin, Germany), pp. 74–89, Springer-Verlag, 2008.
[25] G. Klyne and J. J. Carroll, "Resource Description Framework (RDF): Concepts and Abstract Syntax," 2004. http://www.w3.org/TR/rdf-concepts/

[26] M. Cai, M. Frank, B. Yan, and R. MacGregor, "A subscribable peer-to-peer RDF repository for distributed metadata management," Web Semantics: Science, Services and Agents on the World Wide Web, vol. 2, no. 2, pp. 109–130, 2004.

[27] A. Seaborne, "RDQL – A Query Language for RDF," 2004. http://www.w3.org/Submission/RDQL/

[28] E. Prud'hommeaux and A. Seaborne, "SPARQL Query Language for RDF," 2008. http://www.w3.org/TR/rdf-sparql-query/

[29] Jan Henrik Ziegeldorf, Oscar García Morchon, Klaus Wehrle. "Privacy in the Internet of Things: threats and challenges," Security and Communication Networks 7(12): 2728–2742, 2014.

[30] S. Nakamoto, "Bitcoin: A P2P Electronic Cash System," 2009.

[31] Hernandez-Ramos, J.L.; Pawlowski, M.P.; Jara, A.J.; Skarmeta, A.F.; Ladid, "L. Toward a Lightweight Authentication and Authorization Framework for Smart Objects," IEEE J. Select.Areas Commun., 33, 690–702, 2015.

[32] José L. Hernández-Ramos, Antonio J. Jara, Leandro Marín, and Antonio F. Skarmeta Gómez, "DCapBAC: embedding authorization logic into smart things through ECC optimizations," International Journal of Computer Mathematics, 93(2): 345–366, 2014.

[33] N. G. Weiskopf and C. Weng, "Methods and dimensions of electronic health record data quality assessment: enabling reuse for clinical research," Journal of the American Medical Informatics Association, vol. 20, no. 1, pp. 144–151, 2013.

[34] P. N. Mendes, H. Muhleisen, and C. Bizer, "Sieve: Linked data quality assessment and fusion," in Proceedings of the 2012 Joint EDBT/ICDT Workshops, ser. EDBT-ICDT '12. New York, NY, USA: ACM, 2012, pp. 116–123.

[35] F. Lecue, S. Tallevi-Diotallevi, J. Hayes, R. Tucker, V. Bicer, M. Sbodio, and P. Tommasi, "Smart traffic analytics in the semantic web with star-city: Scenarios, system and lessons learned in dublin city," Web Semantics: Science, Services and Agents on the World Wide Web, vol. 27, pp. 26–33, 2014.

[36] N. Bissmeyer, S. Mauthofer, K. M. Bayarou, and F. Kargl, "Assessment of node trustworthiness in VANETs using data plausibility checks with particle filters," in Vehicular Networking Conference (VNC), 2012 IEEE, Nov 2012, pp. 78–85.

[37] N. Bissmeyer, J. Njeukam, J. Petit, and K. M. Bayarou, "Central misbehavior evaluation for VANETs based on mobility data plausibility," in

Proceedings of the Ninth ACM International Workshop on Vehicular Inter-networking, Systems, and Applications, ser. VANET '12. New York, NY, USA: ACM, 2012, pp. 73–82.

[38] R. Zafarani and H. Liu, "Evaluation without ground truth in social media research," Communications of the ACM, vol. 58, no. 6, pp. 54–60, 2015.

[39] R. Toenjes, D. Kuemper, and M. Fischer, "Knowledge-based spatial reasoning for IoT-enabled smart city applications," in 2015 IEEE International Conference on Data Science and Data Intensive Systems. IEEE, 2015, pp. 736–737.

[40] Antonio F. Skarmeta, et al. "IoTCrawler: Browsing the Internet of Things" in IEEE 2018 Global Internet of Things Summit (GIoTS).

[41] Bröring, A., S. Schmid, C.-K. Schindhelm, A. Khelil, S. Kaebisch, D. Kra-mer, D. Le Phuoc, J. Mitic, D. Anicic, E. Teniente (2017): Enabling IoT Ecosystems through Platform Interoperability. IEEE Software, 34(1), pp. 54–61.

[42] OpenFog Consortium "OpenFog Reference Architecture for Fog Computing", February 2017.

[43] International Standardization Organization, "ISO 27001: Information Se-curity Management System Requirements", Geneva, Switzerland, 2013.

[44] B. Nagpal, N. Singh, N. Chauhan and R. Murari, "A survey and taxonomy of various packet classification algorithms," 2015 International Conference on Advances in Computer Engineering and Applications, Ghaziabad, 2015, pp. 8–13. doi: 10.1109/ICACEA.2015.7164675.

[45] Z. Ma, A. Hudic, A. Shaaban and S. Plosz, "Security Viewpoint in a Reference Architecture Model for Cyber-Physical Production Systems," 2017 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), Paris, 2017, pp. 153–159. doi: 10.1109/EuroSPW.2017.65

[46] A. Botta, W. De Donato, V. Persico, A. Pescapé, "Integration of Cloud computing and Internet of Things: A survey," Futur. Gener. Comput. Syst., vol. 56, pp. 684–700, 2016.

[47] M. A. Razzaque, M. Milojevic-Jevric, A. Palade, S. Cla, "Middleware for internet of things: A survey," IEEE Internet Things J., vol. 3, no. 1, pp. 70–95, 2016.

[48] I. Lee, K. Lee, "The Internet of Things (IoT): Applications, investments, and challenges for enterprises," Bus. Horiz., vol. 58, no. 4, pp. 431–440, 2015.

[49] Kert M. et al., "State of the Art of Secure ICT Landscape," NIS Platform WG 3, V2, April 2015

[50] ENISA, "Threat Landscape Report." 2016, online at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016

[51] G. Hatzivasilis, et al., "The industrial Internet of Thins as an enabler for a Circular Economy Hy-LP: a novel IIoT protocol, evaluated on a wind park's SDN/NFV-enabled 5G industrial network." Computer Communications, Elsevier, vol. 119, pp. 127–137, April 2018.

[52] L., Pino, "Pattern Based Design and Verification of Secure Service Compositions." IEEE Transactions on Services Computing (2017).

[53] L. Pino, G, Spanoudakis, A. Fuchs, S. Gurgens, "Discovering Secure Service Compositions," 4th International Conference on Cloud Computing and Services Sciences (CLOSER 2014), Barcelona, Spain, April 2014.

[54] A. Maña, E. Damiani, S. Gürguens, G. Spanoudakis, "Extensions to Pattern Formats for Cyber Physical Systems," Proceedings of the 31st Conference on Pattern Languages of Programs (PLoP'14. Monticello, IL, USA. Sept. 2014.

[55] K. Fysarakis, et al. "RtVMF: A Secure Real-Time Vehicle Management Framework," in IEEE Pervasive Computing, vol. 15, no. 1, pp. 22–30, Jan.-Mar. 2016. doi: 10.1109/MPRV.2016.15.

[56] N. Petroulakis, G. Spanoudakis, I. Askoxylakis, "Patterns for the design of secure and dependable software defined networks," Computer Networks 109 (2016): 39–49.

[57] G. Hatzivasilis, I. Papaefstathiou, C. Manifavas, "Real-time management of railway CPS," 5th EUROMICRO/IEEE Workshop on Embedded and Cyber-Physical Systems (ECYPS), IEEE, Bar Montenegro, June 2017.

[58] G. Hatzivasilis, I. Papaefstathiou, D. Plexousakis, C. Manifavas, N. Papadakis, "AmbISPDM: managing embedded systems in ambient environment and disaster mitigation planning," Applied Intelligence, Springer, pp. 1–21, 2017.

[59] IDC FutureScape, "Worldwide Internet of Things 2017 Predictions," Nov 2016.

[60] Forrester, "IoT Applications Require Distributed Analytics, Centralized Analytics Won't Work For Many IoT Use Cases," March 29, 2017, online at: https://www.forrester.com/report/IoT+Applications+Require+Distributed+Analytics/-/E-RES133723

[61] Gartner, "7 Technologies Underpin the Hype Cycle for the Internet of Things, 2016, The challenges of creating, implementing and preparing for the IoT," Nov 2016, online at: http://www.gartner.com/smarterwithgartner/7-technologies-underpin-thehype-cycle-for-the-internet-of-things-2016/

[62] Forbes and Moor Insights & Strategy, "The Internet of Things and Machine Learning," 2016, online at: https://www.forbes.com/sites/moorinsights/2016/03/16/the-internet-of-things-and-machine-learning/#a83d2d13fb16

[63] L, Pino, G. Spanoudakis, "Finding Secure Compositions of Software Services: Towards A Pattern Based Approach," 5^{th} IFIP Int. Conference on New Technologies, Mobility and Security, Istanbul, Turkey, May 2012.

[64] L. Pino, G. Spanoudakis, A. Fuchs, S. Gurgens, "Discovering Secure Service Compositions," 4^{th} International Conference on Cloud Computing and Services Sciences (CLOSER 2014), Barcelona, Spain, April 2014.

[65] J. Domanska, E. Gelenbe, T. Czachorski, A. Drosou, D. Tzovaras Research and Innovation Action for the Security of the Internet of Things: The SerIoT Project, to appear in Proceedings of the ISCIS2018 Security Work- shop, Springer CCIS, 2018.

[66] E. Gelenbe, Zhiguang Xu, and Esin Seref, Cognitive packet networks, Tools with Artificial Intelligence 1999. Proceedings. 11th IEEE International Conference on, pp. 47–54, 1999.

[67] E. Gelenbe, Cognitive Packet Network, US Patent 6,804,201, 2004.

[68] E. Gelenbe, Steps toward self-aware networks, Commun. ACM 52(7): 66–75, 2009.

[69] O. Brun, L. Wang, and E. Gelenbe, Big Data for Autonomic Intercontinental Overlays, IEEE Journal on Selected Areas in Communications 34(3): 575–583, 2016.

[70] L. Wang and E. Gelenbe, Real-Time Traffic over the Cognitive Packet Network, Computer Networks Conference 2016: 3–21

[71] F. Francois and E. Gelenbe, Towards a cognitive routing engine for software defined networks, ICC 2016: 1–6, IEEE Xplore, 2016.

[72] E. Gelenbe and T. Mahmoodi, Energy-aware routing in the cognitive packet network, ENERGY, 7–12, 2011.

[73] E. Gelenbe and C. Morfopoulou, A Framework for Energy-Aware Routing in Packet Networks, Computer Journal 54(6): 850–859, 2011.

[74] M. Jammal, T. Singh, A. Shami, R. Asal, and Y. Li, Software defined networking: State of the art and research challenges, Computer Networks, vol. 72, pp. 74–98, Oct. 2014.
[75] W. Stallings, Foundations of modern networking: SDN, NFV, QoE, IoT, and Cloud, Pearson Education, 2015.
[76] Y. Liu, A. Hecker, R. Guerzoni, Z. Despotovic, and S. Beker, On optimal hierarchical SDN, Proc. IEEE Int. Conf. on Communications (ICC), pp. 5374–5379, June 2015.
[77] N. Zhang, S. Demetriou, X. Mi, W. Diao, K. Yuan, P. Zong, F. Qian, X. Wang, K. Chen, Y. Tian, C. A. Gunter, K. Zhang, P. Tague, Y. Lin, Understanding IoT Security Through the Data Crystal Ball: Where We Are Now and Where We Are Going to Be, CoRR, arXiv:1703.09809, 2017.
[78] Symantec Internet Security Threat Report, vol. 23, Symantec Corporation, Tech. Rep., March 2018.
[79] E. Gelenbe, Reseaux neuronaux aleatoires stables, Comptes Rendus de l'Academie des Sciences. Serie 2, 310 (3): 177–180, 1990.
[80] E. Gelenbe, Learning in the recurrent random neural network, Neural Computation, 5 (1): 154–164, 1993
[81] Ahto Buldas, Andres Kroonmaa, Risto Laanoja, "Keyless Signatures' Infrastructure: How to Build Global Distributed Hash-Trees", In: Hanne Riis Nielson, Dieter Gollmann., Secure IT Systems – 18th Nordic Conference, NordSec 2013, Proceedings. LNCS 8208, Springer, 2013.
[82] https://ec.europa.eu/digital-single-market/en/internet-of-things
[83] https://www.sofie-iot.eu
[84] https://www.fiware.org/
[85] https://mydata.org
[86] https://www.sovrin.org
[87] http://estfeed.ee/en/analyses/
[88] BRAIN-IoT Project website,http://www.brain-iot.eu/ (last access June 2018).