SEMIOTICS

Deliverable D2.1
Analysis of IoT Value Drivers

Deliverable release date	30/04/2018
Authors	1. Iason Somarakis, George Spanoudakis (Sphynx) 2. Volkmar Döricht (Siemens) 3. George Hatzivasilis (FORTH) 4. Jordi Serra, Luis Sanabria, Angelos Antonopoulos, David Pubill, Christos Verikoukis (CTTC) 5. Tobias Marktscheffel (Uni Passau) 6. Icie Chomski, Urszula Rak (BlueSoft) 7. Prodromos Vasileios Mekikis (IQUADRAT)
Responsible person	George SPANOUDAKIS (Sphynx)
Reviewed by	George SPANOUDAKIS (Sphynx)
Approved by	TMC Members (Siemens, FORTH, ST-I, ENG, CTTC) PCC Members (Vivek Kulkarni, Dr. Ioannis Askoxylakis, Dr. Verikoukis Christos, Prof. Georgios Spanoudakis, Domenico Presenza, Danilo Pau, Prof. Dr. Joachim Posegga, Darek Dober, Dr. Kostas Ramantas)
Status of the Document	Final
Version	1.0
Dissemination level	Public

Table of Contents

LIST OF ACRONYMS

AAD Azure's Active Directory

AI Artificial Intelligence

AMQP Advanced Message Queuing Protocol

CoAP Constrained Application Protocol

DDS Data Distribution Service

DoS Denial of Service

DPWS Devices Profile for Web Services

ESIM embedded SIM

GDPR General Data Policy Regulation

HSM hardware Security Modules (

HVAC Heating, Ventilation and Air Conditioning

IDS Intrusion Detection Systems

IIoT Industrial Internet of Things

IMSI International Mobile Subscriber Identity

IoT Internet of Things

IPS Intrusion Prevention Systems

LWC Lightweight Cryptography

MEMS Microelectromechanical systems

ML Machine Learning

MQTT MQ Telemetry Transport

NEMS Nanoelectromechanical systems

NFV Network Functions Virtualization

NGSI Next Generation Service Interfaces

ODL Opendaylight

OPNFV Open Platform for NFV

PaaS Platform as a Service

PLC Programmable Logic Controllers

PVRV Pressure Vacuum Relief Valve

QoS Quality of Service

S&D Security and Dependability9

SCA SDN Controller Applications

SCADA Supervisory Control and Data Acquisition

SDN Software Defined Networking

SIM Subscriber Identification Modules

SPDI Security, Privacy, Dependability, and Interoperability

SSN Semantic Sensor Network

TPM Trusted Platform Modules

UPnP Universal Plug and Play

XMPP eXtensible Messaging and Presence Protocol

EXECUTIVE SUMMARY

The purpose of this deliverable has been to provide a review of related issues and technologies at the start of SEMIOTICS that can help the consortium make informed decisions about the direction and priorities of the subsequent work, based on the current technological possibilities and challenges. The conducted review covered common types of smart objects (e.g., devices, sensors and actuators) and IoT platforms that are available for developing IoT applications. It also covered key quality properties that need to be addressed in such applications including security, privacy, dependability, and interoperability. Within these areas, we identified some key issues that will need to be addressed by SEMIOTICS. These relate to IoT Platforms, Security, Privacy, Analytics and Edge Intelligence and Interoperability and are summarized below.

IoT Platforms: Existing platforms vary both in regards to the functional and non-functional capabilities that they offer and the ways in which they realise them. Important limitations relate to the absence of support for edge computing, weak AI and the varying degrees of support for analytics and machine learning capabilities. Enhancements in both these areas constitute a key objective of SEMIOTICS. Furthermore, SEMIOTICS will develop mechanisms supporting the interoperability required for IoT applications that make use of devices and capabilities of different platforms.

Security: Establishing a secure IoT system is not a trivial task. Despite the evolution of the various technologies and platforms there are still open issues that must be considered during the design of a modern IoT application setting. Open issues relate to: (1) the constrained computational and communicational capabilities of many IoT devices and sensory equipment that makes mainstream security solutions not always applicable. Lightweight primitives must be installed, providing an adequate level of protection based on the inherited security perspectives of specific application domains; (2) the lack of comprehensive support in establishing the trustworthiness of users and components of IoT applications; (3) the concurrent handling of security at different layers (application, platform, infrastructure, device) that may leave holes or create incompatibilities making necessary the integration of all mechanisms at different levels (from the device to the backend) and the validation of the joint behaviour of these mechanisms to ensure a secure operation. For (1) SEMIOTICS will use Lightweight Cryptography (LWC) and make use of field IoT gateways (GW) facilitating the communication of information to the upper layers (knowledge integration, mainstream cryptographic protocols, embedded machine learning, etc.). For (2), SEMIOTICS will use Machine Learning (ML) to detect anomalies and indicators of non-trustworthy behaviour. This will be applied at several system layers, ranging from embedded intelligence at the device end to business intelligence at the cloud. For (3), SEMIOTICS will develop a pattern-based approach to verify that adequate protection mechanisms are in place and operate according to the designed principles.

Privacy: Whilst privacy-preserving mechanisms are offered in existing IoT platforms, the extent of the coverage of requirements arising from recent legislation (GDPR) is not clear. SEMIOTICS will investigate the relevant mechanisms and controls of the IoT platforms that it targets to establish the extent of their compliance with current regulation and the data minimization principles. This will cover user’s rights from the data collection on the device to the information processing on the cloud and the big data analysis. It will also cover scenarios arising from the needs of different IoT applications, in the selected domains of the project. Finally, it will introduce a systematic privacy-by-design approach based on the concept of security, privacy, dependability, and interoperability (SPDI) patterns.

Analytics and edge intelligence: Support for analytics varies in different IoT platforms, especially when it comes to field and edge devices. SEMIOTICS will develop specialized and lightweight algorithms for weak artificial intelligent analysis to enable local semi-autonomous operation, tailored to the resources and constraints of field-level objects. It will also develop mechanisms to fuse local intelligence for enhanced intelligent behaviour at higher layers. Intelligence analytics will enable the detection and analysis of the effects of past adaptations. The adaptation mechanisms will be informed by monitoring and intelligence analytics, which will also provide the basis for accountability.

Interoperability: SEMIOTICS will focus on semantic interoperability. The main goal is to establish interoperability patterns that will facilitate the modelling and real-time management of the underlying IoT ecosystem. This will be based on the formal analysis of the five main interoperability settings suggested by the Big IoT project in order to address interoperability and compatibility issues for composing services from inter- to cross-domain topologies.

The immediate direct use of this deliverable will be in producing the requirements specification for the SEMIOTICS framework, i.e., the usage requirements (D2.2) and the system requirements (D2.3) of the SEMIOTICS framework and in developing the high-level architecture of the SEMIOTICS framework (D2.4 and D2.5). In addition, the review of the technological capabilities documented in this deliverable will inform subsequent work in the consortium, particularly in the work packages WP3 (development of SEMIOTICS smart network and object capabilities), WP4 (development of SEMIOTICS security and privacy patterns and capabilities) and WP5 (system integration).

1 INTRODUCTION

This deliverable presents a review of the state-of-the-art of the technical landscape for developing IoT applications/systems and the key drivers that enable the creation of value out of them. To do so, the review covers common types of smart objects (i.e., devices, sensors and actuators) and IoT platforms that are available for developing IoT applications. It also covers key quality properties that need to be addressed in such applications including security, privacy, dependability, and interoperability.

The purpose of this document is to provide a review of related issues and technologies at the start of SEMIOTICS that can help the consortium make informed decisions about the direction and priorities of the subsequent work, based on the current technological possibilities and challenges.

Methodologically, the review that is presented in this document has been based on an analysis of the relevant literature and experiences of the very members of the SEMIOTICS consortium arising from using related technologies and IoT platforms.

Our review has also been based on (and assumes) definitions of some key concepts which arise in IoT applications, namely the concepts of IoT ecosystem, IoT platform and IoT applications. These, for the purposes of this review, are defined as follows:

- *IoT ecosystem:* The term "IoT ecosystem" denotes a community of vendors and enterprises linked together through data and monetary flows, to monetize IoT applications and middleware. Different IoT ecosystems are often centered around an IoT platform, particular IoT technology or IoT consortia.
- *IoT platform:* The term "IoT platform" is used to denote the middleware that is needed to enable communications between the different smart objects (i.e., devices, sensors and actuators and IoT gateways) and the back-end data processing components of an IoT application, and to support some key common capabilities required by such applications (e.g., data storage, data analytics, security controls etc.).
- *IoT application:* An IoT application (or system) is an IT application that involves inter-connected smart objects, including devices, sensors, actuators and IoT gateways, and back-end data processing components (typically deployed on some cloud infrastructure), which together provide IoT services to end users. A key characteristic of IoT applications is that their smart objects are embedded in "things" in the physical world, collecting/passing information from/to them and possibly exercising forms of control upon them. IoT applications exist in different domains including smart homes and buildings, manufacturing and industry automation, transportation, healthcare, energy, smart cities, wearables, farming and agriculture. IoT applications are typically built using IoT platforms.

Within the areas covered by our review, we identified some key issues that will need to be addressed by SEMIOTICS. These are related to the IoT Platform capabilities, Security, Privacy, Analytics and Edge Intelligence and Interoperability. A detailed discussion of issues in these areas is provided in the different chapters of the deliverable, whilst a summary of the main open issues that will be addressed by SEMIOTICS is provided in Chapter 5. The rest of this deliverable is structured as follows:

- Chapter 2 provides an overview of the business value drivers for IoT applications.
- Chapter 3 provides a review of the technical landscape of IoT applications including IoT devices, IoT connectivity and networks, IoT platforms, and other key IoT products.
- Chapter 4 provides a review of the state-of-the-art in addressing key quality properties in IoT applications including security, privacy, dependability and interoperability.
- Chapter 5 summarises some key open issues that arise in the development and use of IoT applications and discusses such issues in the context of the general objectives of SEMIOTICS.
- Finally, Chapter 6 provides some concluding remarks.

2 BUSINESS VALUE DRIVERS AND ENABLERS FOR IOT

In this chapter, we review different business drivers and business models for creating value in IoT ecosystems (i.e., plans of the way in which an organisation can create, capture and deliver business value in an IoT ecosystem, which includes the customers, value chains and revenue models) and the role that technology plays in this creation. Our review considers also different types of stakeholders in the IoT ecosystem as well as regulatory aspects (e.g., related to privacy and security) that may affect the operation of the IoT ecosystem, platforms and application and the creation of value.

The value of IoT lies in connecting the real world with the virtual world of data. Digitalisation technologies offer new business models. In the Internet of Things, billions of things have addresses and are linked to the Internet. They can transmit data to the cloud for processing and be managed and controlled via applications. This scenario will become a reality thanks to increasingly miniaturized computers, affordable sensors, ubiquitous networking, and the increasing availability of “smart” devices in many areas. With well-designed IoT solutions, one can harness data from already owned machines and physical infrastructure to find transformative insights across the entire business. And the users can immediately develop, deploy and run digital services, create own applications, or even new business models. In the following, we examine the above factors in more detail.

2.1 Value Driver Business Model

IoT platform of the ecosystem: This is the key building block of the ecosystem; the enabler on which ecosystem partners build their services. The quality of the IoT platform as perceived by the ecosystem is decisive. For example, high availability and reliability, full integration capability and secure data exchange are highly valued by potential partners. This is due to how potential users perceive the operator of an IoT platform as having the potential to become a leading IoT player in the long term. Obviously, neither users nor ecosystem partners would want to commit themselves to a platform that may not exist in a few years' time. An important element is the necessary self-sustaining cycle of user and partner recruitment. More partners and applications on the platform attract more users. Also more users attract more partners and applications. Supporting an IoT ecosystem requires more than just providing an IoT API. Companies that offer platforms must be able to create the right incentives (financial and other types of incentives), support partner participation with appropriate support systems and define how they – and non-competitive actors – can create more value for their partners (IBM, 2016).

Application Programming Interfaces (**APIs)** are the basic building blocks of an IoT platform, and operators must therefore develop a strong API strategy. This strategy should be based on a deep understanding of the IoT markets, which the operator wants to target. It is not practical to design APIs for all segments, which means that a focused approach is recommended. The operator should also develop an API roadmap that is consistent with its general IoT strategy, while the API pricing model and API support model must be consistent with the operator's ecosystem revenue model. APIs can promote or prevent network effects. If an operator's APIs is too costly or does not create enough value, ecosystem partners will be reluctant to invest time or effort. It is therefore of crucial importance that the operators design APIs with a view to the needs of the partners (IBM, 2016).

Revenue models are an important aspect for the successful development of IoT ecosystems. Operators seeking to attract ecosystem partners need to define the right model for generating and distributing revenue. What is needed is business models encouraging partners to join the ecosystem, reducing the risks for innovation partners and be consistent with each partner's business model. Some partners are attracted by a *revenue-sharing model*, while others prefer a *licensing model* or a *fixed royalty-based model*. This means that operators need to support multiple revenue and partnership models, which in turn requires new decision-making and management systems.

Users of IoT technologies will capture most of the potential value over time. McKinsey estimates that customers will use more than 90 percent of the value added generated by IoT applications. In many situations, customers (such as factory owners using machines guided by IoT technology, operators of transportation fleets, and consumers) will achieve added value both directly and indirectly, such as the ability to purchase more efficient machines based on IoT data from older products. Of the value-enhancing opportunities offered by the IoT available to technology providers, services and software, rather than hardware, are generally likely to account for the largest share (McKinsey, 2015).

Business Value from Predictive maintenance: An important way in which IoT can create value in factories is improved maintenance. With sensors and connectivity, it is possible to monitor production plants in real time. By avoiding breakdowns, you can not only save costs but also improve the capacity utilization and productivity of the factory. Essentially, IoT can transform the maintenance model from a repair and spare parts model. It is important that it is possible to systematically monitor the performance of all machines with networked IoT devices. For example, if a downstream machine detects that the workpieces it receives are constantly switched off in a certain dimension, this can be an indication that the upstream system needs to be serviced. The machine can be repaired and adjusted before the factory sends defective products or the upstream machine fails (CSIRO, 2016).

Business Value from Inventory optimization: Factory operators also have the opportunity to create value through improved inventory management. With the help of sensors for weight or height measurement, it is possible to set up stateful, automatic re-ordering routines that are far more precise than current rule-based systems, which estimate the need for replenishment and are not based on actual data. McKinsey estimates that such inventory optimization measures can save up to 20 to 50 percent of the factory inventory (McKinsey, 2015). Warehousing ties up capital and reduces margins. With the help of sensors for weight or height detection, stateful, automatic ordering routines can be set up that are far more precise than today's rule-based systems, which estimate replenishment requirements and do not rely on actual data. Plant tracking also helps improve plant utilization and employee performance in production and hospital environments (McKinsey, 2015).

Value Driver Organization and talent management: IoT connects the physical and digital worlds and challenges traditional notions of organizational responsibilities. Traditionally, an IT organization was separate from the operational organizational structure that is responsible for managing the physical environment. In an IoT world, IT is embedded in fixed assets and has a direct impact on the business metrics against which operations are measured. Hence, these functions need to be much more closely coordinated. In addition, companies need not only access to knowledge about the functioning of IoT systems (at employee level or through a partner-supplier relationship), but also the ability and mentality to use IoT for data-driven decision-making and to adapt their organization to new processes and business models (PWC, 2016).

Business Value from productivity and safety benefits: IoT applications can track and improve human performance in the workplace. This includes, among other things, the provision of qualification training, the collection of data for redesigning workplaces and the administration of performance. The introduction of IoT technologies to track and control worker activity can significantly increase productivity in both the advanced and developing economies. For example, a worker equipped with an advanced reality device could be taught how to perform a highly skilled task, such as repairing an industrial robot. The new IoT applications that can increase productivity and improve employee health and safety.

Business Value from IoT Systems Interoperability: According to McKinsey, the total potential value that can be released by the use of IoT is interoperability. In the world of work, 60 percent of potential value requires the ability to integrate and analyse data from different IoT systems. Interoperability is needed to unlock more than 4 trillion dollars a year of potential economic impact through the use of the Internet of Things in 2025, out of a total of 11.1 trillion dollars in the nine scenarios analysed by McKinsey (2015). Most of the **IoT data collected today is not used at all, and the data used is not fully exploited**. For example, in factory automation systems, most data is used for real-time control or anomaly detection only. Much remains to be done to add value by using more data and more sophisticated IoT applications, such as using performance data for preventive maintenance or analysing workflows to optimize efficiency. In fact, IoT can be an important source of large amounts of data that can be analysed to capture values and freely accessible data that can be used by more than one entity (McKinsey, 2015).

2.2 Value Driver technology

Sensing, sensors are becoming ubiquitous: The growing popularity of smartphones and tablets in recent years has led to the fact that low cost high volume touchscreens, proximity sensors, acceleration sensors and camera modules have been used as some of the first sensors on consumer markets. The range of sensors is now rapidly expanding beyond motion and image sensor technology to include those measuring moisture, calorie composition of food and human health indicators because of the increasing diversity of consumer IoT applications such as wearables. Advances in sensor technology and falling average selling prices (5G-PPP, 2017). Advanced manufacturing technologies such as MEMS[1] (Microelectromechanical systems) and NEMS (Nanoelectromechanical systems) combine electronics and mechanical components on a micro and nano scale by integrating the functionality of sensors, actuators and integrated circuits into small form factors for a wide range of applications. In addition to these technological advances, intense competition in the fragmented sensor market with many new entrants has led to a steady decline in sales prices, which has led to increased acceptance of the sensors. While smartphones, tablets and portable devices continue to be the main drivers of MEMS sensor growth, other IoT applications such as healthcare and automotive are increasingly being used by miniaturized sensors. It is expected that the total number of sensor nodes or "endpoints" will increase to hundreds of billions when IoT-like devices become ubiquitous.

Data protection and confidentiality: The nature, quantity and specificity of the data collected by billions of devices create concerns among individuals about their privacy and among organisations about the confidentiality and integrity of their data. Providers of IoT enabled products and services must create meaningful added value for the collection and use of data, create transparency about what data is used and how it is used, and ensure that the data is adequately protected.

Augmented Reality: Employers can use augmented reality devices such as electronic glasses or goggles to place computer-generated graphics in an employee's field of vision to provide real-time support for performing a task, such as machine adaptation. This approach has potential for surgeons, mechanics, surveyors, firefighters and others who cannot easily view manuals or other reference materials in real time. Augmented Reality technology can also be used in conjunction with cameras and sensors for rainfall to show the worker how to perform a task and use the data feed to correct errors. Such a system can help to train relatively unskilled workers for high-quality work.

Increased decentralized intelligence: Portable devices will no longer only perform monitoring and reporting functions, but also other sophisticated functions such as remote control of other devices in the IoT, automatic control, and learning and adapting to situations such as local Augmented Reality. In order to cope with the increasing intelligence required to process complex stimuli in real time, extended processing options such as voice control or gesture recognition are required. For this reason, the proportion of semiconductor elements in portable computer equipment will increase sharply.

Advanced Analytics: Maximizing the benefits of IoT-based systems in factories also depends on analytical improvements - algorithms that can interpret and influence the flow of real-time data from many machines. In today's world, only a small portion of the data generated by production machines is used for decision making. Better analysis would help companies to use more information they collect for optimization and forecasting purposes.

Pre-sales analysis: Capturing real-time usage data gives device manufacturers a unique insight into customer operations. This may also include knowledge of the customer's need for upgrades, extensions, other machine types or replacement equipment. As a rule, such pre-sales analyses can increase the turnover of equipment manufacturers by up to 2 percent. According to McKinsey, this could be 10 billion dollars per year for device manufacturers in 2025 (McKinsey, 2015).

Autonomous robots are intelligent high integrated machines with a high density of functions capable of performing tasks independently and without explicit human control. Examples range from autonomous

[1] http://semieurope.omnibooksonline.com/2014/semicon_europa/International_MEMS_Forum/13_Romain_Fraux_System_Plus_Consulting.pdf

helicopters to Roomba, the robot vacuum cleaner. Autonomous robots and Internet of Things devices will soon become as commonplace as PCs and smartphones are today. Robots are therefore machines that can perform measurements, plan and take measures to achieve the desired results. These systems are widely used to automate a manufacturing and supply chain in which physical goods and virtual goods are controlled by computer-aided and algorithmic control mechanisms. However, there is a significant risk when these systems are used in real-world Internet-connected applications. In particular, an autonomous robot with many "users" has to address many of the same interactive streams that people experience when handling Internet-based entities: Authentication, authorization, claim verification, etc. In both cases, these systems must demonstrate transparency, consistent offline behaviour, high security, high availability, self-availability, independence and self-healing.

This transition to ubiquitous devices that can feel, think and act independently will open up many new opportunities for peer-to-peer transactions. This applies in particular to collaborative, mobile, skillful and social robots located in human-centred environments that are used to bridge interactions between real and virtual worlds. Across the spectrum, ownership, control and security of personal and legal identity and digital information are becoming increasingly important. The challenge before us is to design and implement technological systems that can support a skilled person and their digital equivalent.

2.3 Value Driver Regulations

Security: Enterprises that capture data from billions of devices must not only be able to protect that data from unauthorized access but must also deal with the risk categories inherent in IoT. The extension of IT systems to new devices opens up much more opportunities for potential violations that need to be dealt with. When IoT is used to control property, be it water treatment plants or motor vehicles, the consequences of a security breach go beyond the unauthorised disclosure of information - it can potentially lead to physical damage.

Privacy (Intellectual property): A common understanding of the ownership rights to data generated by various connected devices will be needed to tap the full potential of the Internet of Things. A number of indicative, yet important questions arise in this context. For example, who has what rights to the data of a sensor manufactured by a company and part of a solution used by another company in an environment owned by a third party is an important question. As another example, consider the question of who has the rights to data generated by a medical device that is implanted into a patient's body. Is it the patient, the manufacturer of the device or the healthcare provider who implanted the device and manages patient care?

Public policy: Certain IoT applications cannot be performed without regulatory approval. Even though IoT technology is evolving rapidly and many car and technology companies are investing in this area, it remains unclear where and when self-propelled cars can be used. In addition, regulators must establish rules on liability. Policy makers often also play a role in shaping market rules that influence IoT adoption, such as creating appropriate incentives in the health care system. Finally, the government can play a role in establishing rules for data practices regarding the collection, sharing and use of IoT data.

2.4 A Key Technical Enabler for IoT Business Value: Multi-layered Embedded Intelligence

2.4.1 EMBEDDING INTELLIGENCE AT THE EDGE

Converting data into useful information without spending too much money on data plans requires embedded intelligence on the edge of the network. And the current view that "clouds" are infinite and free will not withstand an era of large amounts of data. As more and more Machine-to-Machine (M2M) connections use the reach and bandwidth of 4G LTE, it will be important to develop applications that know when to switch on and off. It will not always make sense to work through a mobile data plan, for example. There will be a variety of diagnostic and remote monitoring applications that should only transmit video if there is something valuable to report. As always, it will be exciting to have new tools available. But, as always, we must learn how to use them effectively.

2.4.2 5G NETWORK AS FUTURE INDUSTRIAL NETWORK

The fifth generation of wireless communications technology is bringing a lot of movement and disagreement to the telecommunications industry. Some see 5G as the next evolution in wireless data communication that promises higher bandwidths and data rates, with significantly fewer transmission delays. Others, on the other hand, say that the technology will be revolutionary and enable a variety of new applications, including humanoid robots, networked cars and the Internet of things with its tens of billions of devices equipped with embedded sensors.

Mobile operators have begun to build 5G networks, although issues such as defining standards to ensure interoperability and setting security requirements are still outstanding. As the first 5G networks, which are expected to start in 2020, are being built, it is important to note that they will have an impact on mobile operators and multimedia services.

Throughout the history of mobile communications, data speeds have increased incrementally within each generation of the network. This will also be the case with 5G, but much more is expected, including improved performance, capacity and speed, and a network that works globally, no matter where and from which device a user connects.

Communications companies will work to reduce delays in transmission time. The 5G latency is estimated to be less than 1 millisecond; whereas 4G networks have a latency of 25 milliseconds (latency is the time a packet takes to move from one forwarding point to another). Low latency is particularly important for real time critical applications such as self-propelled cars and robotic operations where the shortest delay in transmission time can mean life or death.

But updating hardware and software with the latest technologies is not enough. The new networks must be scalable handling billions of devices expected from the Internet of things and other new applications. It must provide connections that are 100 times faster than the current network speeds.

This is where software-defined networks (SDNs) and the virtualization of network functions (NFV) come into play. They support the flexibility and dynamics of the growing number of modern terminals and intelligent machines on the periphery of the network. SDNs offer improved speeds and latency while eliminating bottlenecks.

SDNs decouple hardware (which for example forwards IP packets) from software (the control level that transports signal traffic for routing through network devices). Software is not necessarily executed in the system, but perhaps in the cloud or in clusters of distributed servers. This means that networks can be set up and reconfigured centrally and automatically, instead of network managers jumping from device to device to make manual changes.

NFV is often paired with SDNs. The concept utilizes CPU and resource virtualization and other cloud computing technologies such as orchestration, network slicing and mobile edge computing to migrate networking capabilities from dedicated hardware to virtual machines running on all-purpose hardware. NFV can increase speed, flexibility and efficiency when used with the new services expected to be introduced by 5G. The components can be upgraded as required by the service provider.

2.4.3 DATA OWNERSHIP WITHIN PRIVATE AND PUBLIC CLOUD

With increasing performance and variety of offerings, more and more companies are deciding to bring their services into the cloud. However, there are concerns about the storage of data in the cloud, such as backups, data security, data protection and data transfer. Despite the benefits of cloud services, a company must answer the most important question of who owns the data when choosing a cloud hosted service. Ownership of data in the cloud may depend on the type of data stored and its origin.

A private cloud hosting solution, also known as an internal cloud or enterprise cloud, is located on the company's intranet or hosted data center, where all your data is protected by a firewall. This can be a good option for companies that already have expensive data centers because they can use their existing infrastructure. However, the biggest disadvantage of a private cloud is that the entire management, maintenance and updating of data centres is the responsibility of the company. Over time, it is expected that your servers will have to be replaced, which can be very expensive. On the other hand, private clouds offer a higher level of security and share very few, if any, resources with other organizations.

The main difference between public and private clouds is that you are not responsible for managing a public cloud hosting solution. Your data is stored in the provider's data center and the provider is responsible for managing and maintaining the data center. This kind of cloud environment is attractive to many companies because it shortens the lead times for testing and implementing new products. The downside, however, is that many companies believe that security could be lacking in a public cloud. Even if you don't control the security of a public cloud, all your data remains separate from others and breaches of security by public clouds are rare.

There are two types of data stored in the cloud. The first category is the data the user creates before uploading it to the cloud, and the second category is data created on the cloud platform itself. Data generated in a cloud platform prior to the upload is copyrighted, depending on the cloud server, while data generated after storage represents a whole new dimension of ownership.

A number of cloud services typically collect and store user data, while the user is unable to retrieve all data once it is made available. For example, LinkedIn does not allow other services to access all user data. In this case, personal data such as the e-mail address of the user or friends cannot be viewed by third parties via the linked API.

A number of companies are trying to stay relevant by keeping access to customer data private. Some free services reserve the right to store user data on their platforms, while others store only part of the data uploaded to their servers. It is therefore advisable not to use a cloud service that retains ownership of all or part of a user's data.

Regardless of the online service used, it is important to use data encryption for all data stored in the cloud to maximize security and provide a form of control over your data. So far there are no regulations for cloud computing and all that has a partial governance of cloud providers are the local rules.

All questions arising from the process of storing data in the cloud must be precisely defined. It is therefore advisable to clearly define all the advantages, disadvantages and costs of a particular cloud platform. This will help to better understand and evaluate the cloud operations around data management.

3 TECHNICAL LANDSCAPE

3.1 Overview

Whilst in Chapter 2, our focus was to review the key drivers, enablers and challenges for generating business value out of the IoT ecosystem, in this chapter we review the key technologies that are necessary or typical for IoT applications and platforms. The purpose of this review is to provide an overview of the capabilities and limitations of such technologies and, through this, enable SEMIOTICS to tune its work programme accordingly.

3.2 IoT Devices

The IoT domain has a very broad scope, potentially encompassing every physical device that runs computational algorithms and has network connectivity. In the framework of SEMIOTICS we will primarily focus in the Industrial IoT (IIoT) domain, hence in what follows the state-of-the-art in industrial and smart building related IoT devices will be presented. However, it must be noted that even state-of-the-art industrial plants and factories typically follow a simple "monitor and respond" strategy, where sensor values are integrated in a Supervisory Control and Data Acquisition (SCADA) controller, which controls system operations. SCADA systems are typically vertically integrated "black box" solutions with little opportunity for expandability or adaptive behaviour. SEMIOTICS is instead aligned with the Industry 4.0 vision, which goes beyond the "monitor and respond" paradigm and deterministic control and is expected to revolutionize manufacturing. SEMIOTICS will follow a predictive and proactive approach, where IoT devices will be sending Production data in a factory cloud, which will be processed by data analytics and edge intelligence services. These will form the basis of an adaptive IIoT deployment, which will be able to optimize production in real time, manage inventory and even predict failures. In must be noted that SEMIOTICS ecosystem can build upon existing SCADA systems and IIoT devices, which will be presented in the following sections, augmenting their functionality with data analytics functionality and combining data from many different sources and many different vendors. These include IIoT devices for Process and Manufacturing automation, devices for vibration and stress monitoring in proactive / predictive maintenance scenarios, devices for health and safety monitoring, devices for asset tracking and inventory monitoring, and devices for building automation and energy management.

3.2.1 PROCESS INDUSTRY AUTOMATION

IoT devices that target real-world automation scenarios in the *process industry*, which is concerned with the processing of bulk resources into end products as, for example, in oil refineries chemical plants, etc., have been introduced to the market by leading vendors.

The most common use case for IIoT devices is for the real-time monitoring of process parameters, which are transmitted to the control room. These parameters are critical for decision making and can be used directly for the control of actuators (e.g., for electric valves and turbines) by SCADA controllers. Siemens offers a complete suite of IoT devices for process automation (SITRANS IIoT, 2018). These include IoT devices for keeping track of process parameters, including pressure measurements (*SITRANS P* series), temperature measurements (*SITRANS T* series), flow measurement (*SITRANS F* series) and level measurement (*Siemens level* series S). Sensor readings can be transmitted to the gateway via legacy wired connections, or via wireless connections. Self-organizing wireless mesh networking based on IEC 62591 (WirelessHART®) is the industry standard for wireless communication in factories. The process industry is supported by most leading vendors, such as Siemens, P+F, Emerson, Honeywell, and many others Figure 1 (a).

Finally, IoT gateways such as the Siemens SIMATIC IOT2000 (SIMATIC IOT2000, 2018), shown in Figure 1 (b), aggregate sensor data from multiple sources and communication technologies. The IoT gateway is responsible for harmonizing communication between data sources from different manufacturers that could use different communication technologies, protocols and data models.

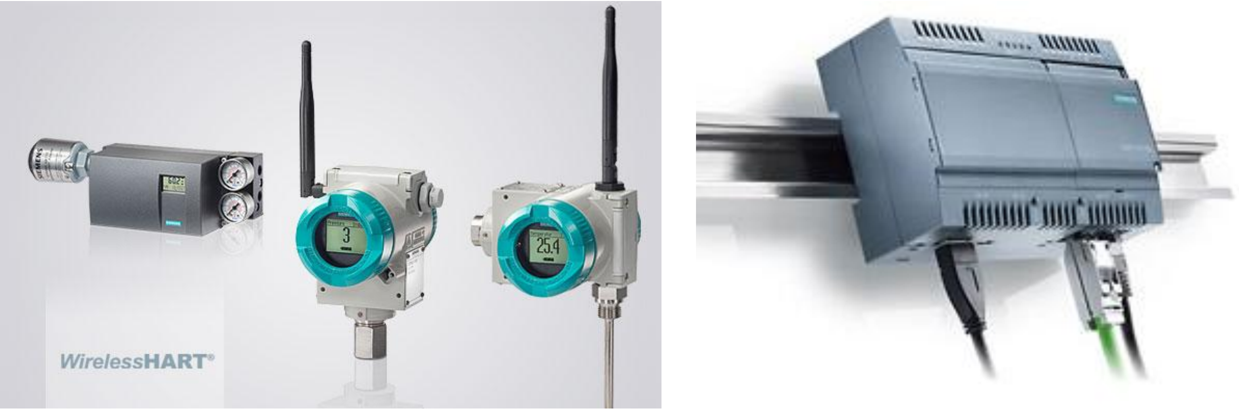


Figure 1. (α) Wireless Hart Temperature /Pressure sensors, (b) Siemens IIoT gateway

3.2.2 DEVICES FOR PREDICTIVE MAINTENANCE

Predictive maintenance is a compelling use case for IIoT. Industries are increasingly considering the deployment of cost-effective IoT devices attached to machines for preventive maintenance.

Wireless IoT devices for vibration sensing are a very useful instrument for predictive maintenance in motors. A state-of-the-art solution from ABB is attached on the motor frame, and automatically calculates and relays information about the motor's health, reducing motor downtime by up to 70 percent (ABB Ability Smart Sensor, 2018).

A similar system from Fluke, shown in Figure 2 (a), can be attached to all types of equipment, sensing vibration data continuously and can help train a predictive maintenance IIoT system regarding equipment performance before, during and after an event (Fluke Condition monitoring, 2018). IoT sensors are also employed for oil and gas pipeline integrity, to report early formations of cracks or deformations. For example, such a device is deployed for continuous monitoring in a section of gas pipeline in Germany as mandated by regulations, because it is laid next to a river valley. This device relies on a 4G modem, and a chain of Fiber-optic sensors, shown in Figure 2 (b), to monitor the pipeline structural integrity and transmit data wirelessly in real time (Pipeline Fiber Optic Strain Sensors, 2018).

Finally, another good example of predictive maintenance system is VAF's TT-Sense (VAF TT-Sense, 2018), which monitors ship engine torque via a wireless non-contact optical sensor and can predict problems when the engine thrust puts too much stress on the main shaft. The same or other similar IoT devices can monitor stresses on the shafts of wind turbines.

Predictive maintenance is a key SEMIOTICS use case, aimed at improving further the anomaly detection process. SEMIOTICS will not rely on static rule-sets to identify problems, but rather employ machine learning and predictive analytics models to implement a truly adaptive behaviour. Predictive analytics models exploit the real-time sensor data to extract patterns that signal abnormal operation, which allows a proactive response as well as discovering the root cause of the problem. Hence, the system accuracy is expected to increase over time, as data points on system parameters during expected and abnormal behaviour are accumulated.

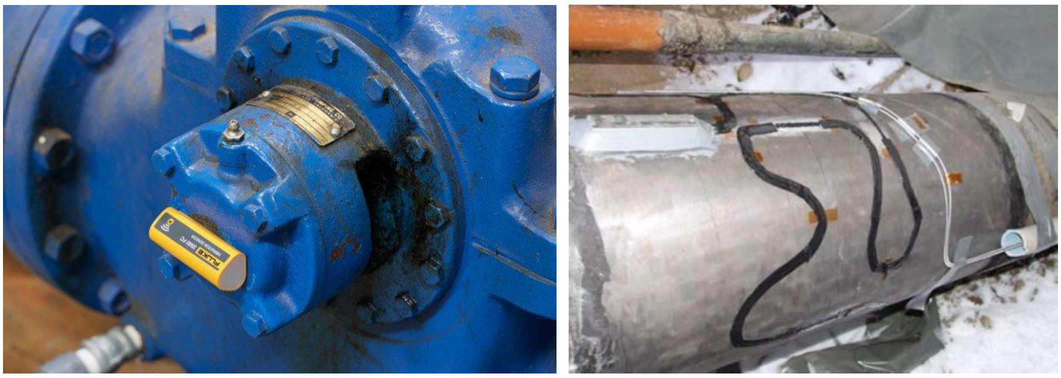


Figure 2. (a) IoT Vibration sensing (b) Fiber optic sensor for pipeline integrity

3.2.3 DEVICES FOR HEALTH AND SAFETY

Most health and safety issues in factories and the process industry are caused by undetected maintenance issues and alarms that failed to reach the control room and lead to actions. Keeping track of Process parameters as detailed in section 3.2.1 significantly increases safety, as alerts can be generated whenever a certain parameter (e.g., pressure in a tank) exceeds a predefined threshold. To further reduce control latency, self-actuating IoT devices can also take action, such as the Smart Wireless Pressure Vacuum Relief Valve (PVRV) from Emerson (Tank Storage System, 2018) shown in Figure 3 (left), which sends an alert and simultaneously opens to relieve excessive pressure. Another representative example of an IoT device for health and safety is the Vanguard Toxic and Combustible Wireless Gas Detector (Vanguard Wireless Gas Detector, 2018) which detects toxic and combustible gases produced (or generated as a by-product) from industrial processes.

Finally, smartGAS Gmbh offers smart NDIR sensing devices for CO2 monitoring (Smart EVO CO2, 2018) in industrial environments, shown in Figure 3 (right), to ensure health and safety of personnel. In industrial environments with significant CO2 generation, for example in breweries, the soft drinks industry, freezer storage industries etc., the maximum permitted CO2 concentration according to most standards can be as high as 5,000 ppm during an 8-hour working period. CO2 gas monitoring in this case is required to ensure air quality monitoring and control (e.g., ensuring appropriate ventilation via the Heating, Ventilation and Air Conditioning (HVAC) system) and compliance with industrial health and safety requirements.

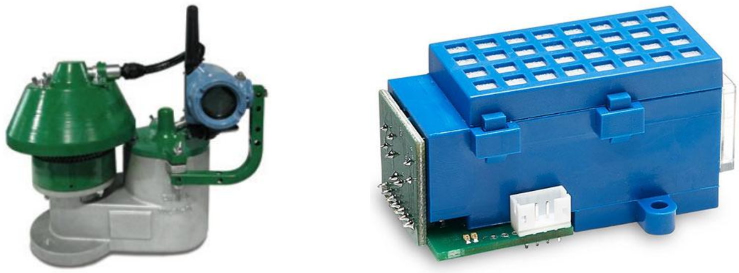


Figure 3. (left) Wireless Pressure Vacuum Relief Valve, (right) CO2 sensing device

3.2.4 DEVICES FOR REAL TIME TRAFFICING OF ASSETS AND INVENTORY

IoT devices are not only involved in primary industrial operation and control, but also for secondary inventory and asset-related measurements. Hence, industries can keep track of supply chain interdependencies, material flow and manufacturing cycle times. IIoT systems can be configured for location tracking, remote monitoring of inventory and reporting of products as they move through the supply chain. IIoT devices based on Passive and Active RFID for supply chain tracking are offered by many vendors, including Siemens' SIMATIC RF line (SIMATIC RF, 2018), shown in Figure 4 (a). RFID devices (or transponders) attached on parts or finished products can be read in bulk from a distance from an RFID reader, ensuring supply chain visibility and tracking in real time. For indoors positioning of assets (e.g., tools, forklifts, etc.) IoT devices based on state-of-the-art Indoor positioning with Ultra-Wideband (UWB) technology report the distance of UWB tags, attached to assets that must be tracked, from fixed anchors, as shown in Figure 4 (b). Assuming that a tag is within range of at least 3 anchors, an accuracy of 10-30 cm (Indoor Positioning with UWB, 2018) can be achieved. Finally, outdoors positioning, such as fleet or container tracking typically relies on IoT devices that combine a GPS unit and a 3G or 4G modem (Orbcomm Asset Tracking, 2018).

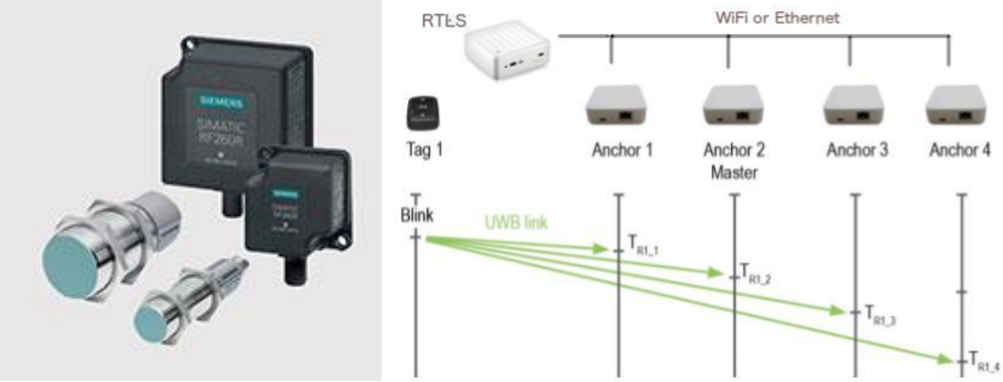


Figure 4. (a) RFID tracking devices, (b) indoors positioning based on UWB.

3.2.5 DEVICES FOR BUILDING AUTOMATION AND ENERGY MANAGEMENT

Building automation ("smart buildings") is relevant for both industrial and commercial uses, and its benefits are increased efficiencies, security, and cost reduction via efficient energy management. Smart lighting solutions by Philips, Siemens, and many other vendors, are implemented by IoT-enabled lights, shown in Figure 5(left), that cut down on energy use by implementing lighting zones with different dimming levels, as well as exploiting occupancy sensors (Philips LED lighting, 2018) to turn down lighting in unused zones. Moreover, IoT sensors in smart buildings can be used as a reference for controlling the HVAC. These may include sensors for temperature, humidity, CO2 and Volatile Organic Compounds (VOC) (Siemens Building solutions, 2018). These sensors allow the HVAC system to adjust the amount of outside air coming in based on the levels of CO2, in the building. To increase energy-efficiency, control algorithms should allow as little outdoor air as possible to enter the building, which saves energy costs during times of lower occupancy levels. Literature (Apte, 2006) indicates a significant potential for energy savings, particularly in buildings with a variable occupancy, of up to 25% and can also contribute to occupant comfort and productivity. Moreover, smart IoT thermostats like Tado (Tado Smart Thermostat, 2018), shown in Figure 5(right), allow remote control of internet-connected thermostats, and offer learning algorithms that automatically adapt to user preferences. Finally, accurate multi-zone control can be achieved with IoT-based actuating valves, that can individually shutoff fluids in domestic hot-water or chiller plants (Siemens Acvatix, 2018).

Figure 5. (left) Philips smart lighting, (right) Tado smart thermostat

3.3 IoT Connectivity/networks

3.3.1 CONNECTIVITY

The connectivity in IoT is characterized by different heterogeneous technologies and a fragmented market (Akpakwu et al., 2017). Probably, the main reason is due to the high diversity of IoT devices and IoT platforms covering a plethora of use cases. Thereby, these diversity in IoT devices, use cases and IoT platforms leads to different requirements in terms of connectivity. The market fragmentation due to the heterogeneous technologies used for connectivity can lead to interoperability problems as well. The heterogeneity, market fragmentation and interoperability issues of current IoT landscape are a good opportunity for the proposed approach in SEMIOTICS. Next, an overview of IoT scenarios in terms of connectivity is provided.

The connectivity in IoT typically refers to provide IoT devices a means of communication to the Internet, which paves the way to IoT platforms developed at the cloud to access globally the data generated by IoT devices for data analytics and storage. To this end, the connectivity can be split in two blocks.

- Connectivity between IoT devices and IoT gateway.
- Connectivity between the IoT gateway and the core network or Internet, which connect to the IoT platforms at the cloud.

Usually, the heterogeneity mentioned above, is found in the connectivity between the IoT devices and the IoT gateway. And from the IoT gateway to the Internet the connectivity is based on either the next wireless or wired technologies:

- Wireless Cellular technologies: 2G, 3G, 4G, LoRa, Sigfox, WiFi.
- Wired: DSL, Optical-based fiber (FTTX).

In other words, an end-to-end technology providing the connectivity between the IoT device to the Internet was not available for some time. More recently, however, LoRa and Sigfox provided this end-to-end solution through proprietary networks called LoRa network and Sigfox low power wide area network, respectively (Akpakwu et al., 2017). Furthermore, the 3GPPis integrating IoT devices within the LTE cellular wireless framework through the LTE-M technology (LTE-M, 2018). Also, in this regard the GSMA technology NarrowBand IoT (NB-IoT) will permit IoT devices to coexist with 2G, 3G and 4G cellular networks (NB-IoT,2018).

In terms of connectivity between IoT devices and the IoT GW the technologies can be divided into wireless and wired communications. Technologies belonging to each of these technology types are reviewed next.

3.3.1.1 WIRELESS CONNECTIVITY

The technologies within this group can be categorized depending on the coverage that they provide, i.e., either short-range, medium-range or long-range.

- **Short range**
  - **Z-Wave:** Z-Wave is primarily used for home automation and it is based on a mesh network topology (Z-Wave, 2018). Z-Wave permits to control residential appliances such as lighting systems, thermostats, windows. It is designed to provide low-latency and reliable transmission of packets with a maximum data rate of 100 Kbit/s. It also supports ranges of up to 40 meters, and operates at 868 MHz in Europe. The PHY and MAC layers rely on ITU-T G.9959 (ITU-T G.9959, 2018).
  - **Bluetooth Low Energy (BLE):** It operates at 2.4 GHz and has a maximum coverage range of 100m. The data rates it can provide are 125 Kbit/s, 1Mbit/s or 2Mbit/s. It provides a significant lower latency and lower power consumption than classical Bluetooth. Namely, in terms of latency, BLE offers 6 ms vs Bluetooth which offers 100 ms. In terms of power consumption, classical Bluetooth consumes 1 W, whereas BLE between 0.01-0.50 W depending on the use, (BLE, 2016).

- **Medium range**
  - **IEEE 802.15.4:** This standard has a maximum coverage of 750m (using a maximum transmit power of 10 dBm) or 1600m (using a maximum transmit power of 18 dBm). It operates at a central carrier frequency of 2.4 GHz. It is a low-rate personal area network (LR-WPAN) with a maximum data rate of 250 Kbits/s. Thereby it has been mainly used to communicate Wireless Sensor Network (WSN) nodes containing sensors which require low data rate such as temperature, humidity or CO_2 concentration levels in scenarios such as smart buildings. It defines the physical and medium access layers. Thus, on top of it other popular technologies such as Zigbee or 6LoWPAN have been proposed to define the upper layers. 6LoWPAN is the technology proposed to let low power and resources constrained devices to support IPv6, (Akpakwu et al., 2017).
  - **Low Power WiFi or IEEE 802.11ah:** This technology extends WiFi to the needs of IoT, i.e., large number of connected devices, enhanced coverage and energy constraints (LowPower-WiFi, 2018). Its aim is to achieve a power consumption of 100's of mW.
  - **DigiMesh:** This is a proprietary technology developed by Digi International. It is a peer-to-peer wireless networking technology and operates at 2.4 GHz. It is envisaged for low power battery-powered nodes. Its range is 1500m operating at a maximum transmit power of 18 dBm (DigiMesh, 2018).

- **Long range**
  - **LoRaWAN:** It specifies the PHY and MAC layers. At the PHY level it uses a proprietary Chirp Spread Spectrum modulation and Frequency Hopping Spread Spectrum. At the MAC layer it relies on the well-known ALOHA protocol. It is based on a start network topology, where each LoRa node reaches the LoRa gateway by means of a single hop link. It has been demonstrated that it can provide coverage ranges of 15 Km in urban environments, see (Akpakwu et al., 2017). It uses the 868 MHz and 915 MHz frequency bands and the maximum data rate is 50 kbps. Besides LoRa provides the connection of the Gateway to a network server, which can be used remotely by the user applications. Thereby, it provides and end-to-end solution.
  - **Sigfox:** Provides an end-to-end connectivity solution based on a patented ultra-narrow band technology. They use proprietary base stations, which connect to backend servers via IP networks. Sigfox devices use the ISM bands of 868MHz or 915 MHz to connect to the base stations. The coverage between Sigfox devices and base stations is 30-50 Km in rural areas and 3-10 Km in urban areas. The main restriction is that only 140 messages per day can be sent in the uplink, each of them has only 12 bytes. Whereas in the downlink only 8 messages per day are allowed (each of 8 bytes).
  - **LTE-M or eMTC:** It has been introduced by 3GPP in release 13 to support machine to machine traffic in LTE networks. It reduces significantly the complexity of the modems, cost and power consumption and extended coverage. It is expected to have a maximum throughput of 1Mbps, both uplink and downlink. It is designed to allow battery lifetimes of 10 years in massive IoT deployments with a 5 W per hour system (Akpakwu et al., 2017).

- **NB-IoT**. Narrowband IoT (NB-IoT) is a technology introduced by 3GPP in release 13, released to the market in 2017. NB-IoT is intended to permit a massive number of IoT devices to fit within LTE cellular networks, i.e., Beyond 4G technologies. Namely, the idea is to let the operator to use its available spectrum and portion of the network to accommodate the IoT devices. To this end, the bandwidth of NB-IoT is 180 KHz both for downlink and uplink. The downlink peak data rate is 34 kbps and 66 kbps in the uplink. It is designed to reuse LTE technology to reduce its incorporation in the market. Thereby, it uses SC-FDMA in the uplink and OFDMA in the downlink for the multiple access, similar rate matching, interleaving or channel coding (NB-IoT, 2016). Its Key Performance Indications (KPI) are to support massive number of IoT devices, guarantee low latency, or extended coverage. It is one of the technologies pioneering the development of 5G.

3.3.1.2 WIRED CONNECTIVITY

Wired connectivity is supported by three main protocols and standards:

- **Modbus.** Modbus is a de-facto standard in many Industrial applications that permits to transmit data between electronic devices via serial lines, using a master slave model (Modbus, 2018).
- **BACnet.** BACnet is a communication protocol widely used in building automation and control networks (BACnet, 2018). E.g. it is used to control HVAC or lighting systems. It uses and object discovery mechanism to communicate between devices and basic read and write functions to share data.
- **OPC.** The Open Platform Communications (OPC Foundation, 2018) is an interoperability standard for the secure and reliable exchange of information among devices from multiple vendors in industrial and building automation. It is based on a server-client software architecture. The OPC server receives generic read and write commands from OPC clients, e.g. SCADA) systems. Then, it translates those read and write requests into device specific format, e.g. into Modbus protocol, to interact with the devices such as Programmable Logic Controllers (PLCs).

3.3.2 NETWORKS: SDN/ NFV TECHNOLOGIES

SDN propose a centralized control of the data plane via a SDN Controller. Network devices under this scheme lack local intelligence or routing protocols (i.e., control plane), instead, forwarding strategies are defined in software at the SDN Controller.

The most prominent open source SDN Controllers as, for example, Opendaylight (OpenDaylight, 2018), or ONOS (ONOS, 2018,), propose southbound and northbound interfaces, known as SBI, and NBI, respectively. .SBI provides an API for interaction with the network devices (SBI). NBI provides an API for interaction with User Applications running on top of the SDN Controller (Toghraee, 2017). SBI implements protocols such as Openflow (Opennetworking, 2018) or NetCONF (Enns, 2006), the former to inject forwarding rules to forwarding devices, while the latter is used to configure parameters of the devices themselves. NBI opens the way for user applications to interact with the data plane, or to retrieve network information via the SDN Controller.

SDN forwarding strategies are specified via SDN Controller Applications (SCA). These SCA may define different aspects of the communication, such as routing or virtual networks, but also can base forwarding decisions on relevant metrics obtained from the network devices (via SBI), such as: link state information, port statistics, flow statistics, and so (Opennetworking, 2018). These instantaneous metrics can be provided to SCAs, which in turn may use them to select alternative directives, e.g.: calculate alternative paths based on a Security and Dependability (S&D) network pattern (Petroulakis et al. 2016).

The use of instantaneous metrics from network devices opens the way for the more dynamic context-aware forwarding strategies, which take advantage of the SDN Controller’s centralized view of the network to rewrite forwarding decisions in real time. This ability is especially relevant for heterogeneous networks, where computing nodes or other network destinations are connected through links with different or varying characteristics (Raschellà et al. 2017).

The Opendaylight (ODL) SDN Controller provides standardized southbound interfaces, such as: OpenFlow, NetCONF, RESTCONF, BGP LS PCEP, OVSDB, OF-CONFIG, OpFlex, and SNMP4SDN. Furthermore, ODL's NBI acts as a Model-Driven Service Abstraction Layer (MD-SAL), through which application developers rely on for automatic detection of the appropriate SBI (Toghraee, 2017). That is, if an application requires to modify a parameter of a network device using NetCONF SBI, ODL automatically communicates with such device using the appropriate protocol. The aforementioned characteristics of ODL (which are also supported in ONOS, both of then sponsored by The Linux Foundation) reveal its strong inclination towards standardized protocols and open APIs.

To ensure dynamic provisioning and security, chaining Virtual Network Functions (VNF or NFV) allows for great flexibility and configurability. NFV are the virtual equivalent of network devices, such as Routers, Firewalls, or Load Balancers. Conventional networks needed to be built following a predefined chain of devices in other to provide services like firewalls, or Intrusion Prevention Systems (IPS). An example can be derived from the case of securing a data base by forcing traffic to go through a firewall device. On the other hand, employing standard platforms such as the Open Platform for NFV (OPNFV), promotes the transition towards cross-compatible virtualized network functions, where services such as a firewall, are defined in software.

By implementing NFV, SDNs gain flexibility. A NFV orchestrator such as ODL, may open NBI that allows user applications to define Flow Policies detailing the flow of specific traffic through several NFV in a specific order, that is, NFV chaining (Moens and De Turck, 2016). Furthermore, the SDN/NFV combination provides gains regarding scalability, mostly due to the software nature of the NFVs, the implementation of NFV replicas, and load balancers. This means that a Flow Policy composed of several NFVs can be recreated (in part or in whole) on other parts of the network when it is required.

Both, SDN and NFV represent an important step towards dynamic, scalable networks. Moreover, NFV chaining via Flow Policies in ODL is an efficient way of providing advanced services, yielding way lower OPEX than in traditional networks. Further, SCA are able to open APIs to user applications requiring on-demand network reconfiguration, ensuring specific Quality of Service (QoS) limits. Even more, the provisioning of computing nodes closer to the generation of data in an IoT setting enables lightweight virtualization (Morabito et al., 2018), potentially alleviating the traffic going up the network topology towards the more computing-heavy core.

3.4 IoT Platforms

IoT platform market is growing fast and already offers plethora of tools out of which some are complex solutions supporting vast number of IoT applications while others do specialise in one or only few domains and use cases. This section provides an overview of IoT platforms available in the market, including both the open source and commercial ones. The purpose of providing this overview is to give answers to questions about what the current landscape of the IoT platform market is and what are the typical application of the platform. Our review provides general comparison of the top 10 IoT platforms based on the current capabilities of each platform. It also describes their strengths and weaknesses.

Based on the initial review and summary, selected number of platforms will be described deeper to trigger understanding of each platform's usability within the SEMIOTICS framework

General comparison:

Name	**AWS IoT platform (Amazon)**	**Microsoft Azure IoT Hub**	**Google Cloud Platform**	**IBM Watson Internet of Things**	**FIWARE**	**SOFIA -> SOFIA 2**	**Mind Sphere (middleware)**	**GE Predix**	**ThingWorx PTC**	**Oracle IoT Cloud Service**
Solution type	IoT platform	IoT platform	IoT platform	IoT platform	IoT platform	partner IoT platform and middleware	partner IoT platform and middleware (Amazon AWS partner)	IoT platform	IoT platform (Amazon AWS partner)	IoT platform
Main Application	generic purpose	general purpose (but mainly dedicated to Windows Servers - other <e.g. debian> systems are slower)	general purpose (especially for small innovative projects)	industry applications	general purpose	general purpose	IIoT, Healthcare, Energy	IIoT	IIoT + AR games	general purpose
Licence type	Amazon	Microsoft Azure	Google	IBM	opensource	Indra / opensource	Siemens	GE	ThingWorx	Oracle
Instant provisioning	YES	YES	YES	-*(<10 min)	configuration needed and choosing correct IoT Agents	-*	plug and play connectivity for quick connection	(zero touch provisioning)	+/- (building reusable connectors)	-*(user self-provisioning)
Installation model	cloud	cloud / on-premise	cloud	cloud / on-premise	on-premise	cloud / on-premise	cloud	cloud	cloud/on-premise	cloud
Autoscaling	YES	YES	YES	(it is build on IBM SoftLayer which enables to scale up and down when required)	-*	horizontal scalability	-*	+/- (scalable applications)	-*	(Cloud solution: Automatic Scaling)
Serverless computing	serverless computing (Lambda), computing (EC2)	serverless computing (Azure Functions)	serverless computing (Cloud Functions)	YES (IBM Cloud Functions, IBM Bluemix OpenWhisk)	-*	-*	-*	YES (severless runtime engines)	-(scalability)	-*

Name	AWS IoT platform (Amazon)	Microsoft Azure IoT Hub	Google Cloud Platform	IBM Watson Internet of Things	FIWARE	SOFIA -> SOFIA 2	Mind Sphere (middleware)	GE Predix	ThingWorx PTC	Oracle IoT Cloud Service
Analytics	Amazon Machine Learning (help for devs to create ML models): Polly (text to speech), AWS Rekogniton (image recognition), Lex (powers Alexa - voice service)	Microsoft Azure ML Studio (build and deploy algorithms) + APIs, asure-iot-sdks	Cloud Machine Learning Engine (based on opensource TensorFlow), machine learning API for natural language processing, translation, computer vision	Watson Cognitive Analytics	BigData Analysis Cosmos	SOFIA 2 ML	Analytics Services with anomaly detection and trend prediction	rich industrial-grade analytics library and framework	ThingWorx Analytics	Oracle's Big Data Analytics
Support for Hadoop	YES (Elastic Map Reduce)	YES (HDInsight)	YES (Dataproc)	YES(BigInsights)	+/- (Cygnus conntector, Cosmos is based on Hadoop cluster)	YES (BDH)	-*	+/- (Hadoop v2 - it is possible via Apache, but there is no dedicated solution)	-*	(Cloud solution: Big Data Cloud Service)
Relational DB	Amazon Relational Database Service, Amazon DynamoDB	Azure SQL Database, Azure DocumentDB	Redshift and Google Cloud SQL, Google Bigtable	YES	YES (MySQL by Cyngus)	YES (BDRT)	YES (SAP HANA)	YES(PostgreSQL)	YES (databases connectors extension)	YES
Edge computing support	-*	YES	-*	YES	YES (new GE FogFlow for edge computing)	-*	YES	YES (analytics deployment at the edge, edge-to-cloud deployment model)	YES	-*
Supported place for analytics	only in cloud	cloud / local	only in cloud	cloud / local	local	cloud / local	only in cloud	cloud / very limited local	cloud / local	only in cloud

Name			AWS IoT platform (Amazon)	Microsoft Azure IoT Hub	Google Cloud Platform	IBM Watson Internet of Things	FIWARE	SOFIA -> SOFIA 2	Mind Sphere (middleware)	GE Predix	ThingWorx PTC	Oracle IoT Cloud Service
CONCEPTUAL OVERVIEW	Device management	*list of connected devices *their status connections *error reporting and handling, firmware	YES	YES	YES	YES	YES (IDAS)	YES	YES (predictive)	YES (with Predix Edge Manager)	+/-*	YES (status, device model)
	Integration	.	REST API	REST API	REST API	HTTP REST API, HTTP Messaging APIs (secure posting)	REST API	REST API, CRUD access (Java, Python..)	REST API	REST API	REST API	REST API/(Java, Javascript, Android iOS)...
	Security	*encryption mechanisms	YES (encryption TLS, authentication)	YES (security PATTERNS - TLS or IPSec)	YES	device and application authentication	Identity Based Data encryption	YES (authorization, autentication, encryption)	Multilayer security + SSL/TLS encryption, only HTTPS connection on port 443 supported	secure by design, defence-in-depth across every layer, security of data flow, two-party encryption, end-to-end	two sets of security permissions: for design and for run time - authorization and triggering events on a Thing	digital identity (even biometrics) on all layers
	Protocols for data collections	*lightweight protocols: application, payload, messaging, legacy	MQTT, HTTP	AMQP, MQTT, HTTP + mechnism of adaptation for others (IoT Protocol Gateway)	MQTT, HTTP	MQTT, HTTP	MQTT, HTTP	HTTPS, MQTTS	HTTP/HTTPS, TCP, VNC, MQTT/MQTT+TLS, REST, SmartRest, OPC-UA... Device specific prtocols	SSL/TLS	HTTP/HTTPS, TCP	MQTT (Cloud solution: MQTT Bridge)
	Visualisation	*meaningful insights	YES (AWS IoT Dashbord)	YES	YES	YES	YES (SpagoBI, FIWARE Lab)	YES (available in both IoT and analytics edition)	(MindApp Visual Analyser)	YES	YES	YES
	Real-time/Periodic analytics	*on-the-fly	real-time analysis (Amazon Kinesis)	real-time (Azure Stream Analytics)	real-time (Google Functions)	real-time	-* (not found info about real-time analytics apart from real-time CEP)	-*	-*	-*(real-time access to industrial data only)	YES	YES (real time, streaming analytics)

Summarising:

Presented comparison shows current landscape of IoT platforms. Some functionalities are achievable by few of them only, according to documentation of platforms. This is, among others things, a possibility of serverless computing which is available via AWS, Google, IBM, Azure and GE Predix only, according to information available at the time of comparison. The information about edge computing support provided by AWS, Google, Oracle nor SOFIA, haven't been found. The only supported place of AWS, Google, MindSphere or Oracle is cloud, which is a significant limitation. Every of mentioned platforms support some kind of analytics, but they are not equally advance. The real time analytics is achieved by AWS, Azure, Google, IBM, ThingWorx and Oracle. The conclusion from this tally is that the platform satisfying all IoT requirements hasn't been created yet.

3.5 Description of selected IoT platforms

The IoT platforms FIWARE, Amazon, Azure and MindSphere have been chosen from the presented comparison as the most promising candidates for the SEMIOTICS multi-platform approach and will be described in more detail in this section. The reasons and selection criteria for choosing these IoT platforms are as listed below:

- FIWARE is an open source IoT platform that is a good candidate for SEMIOTICS because it offers generic enablers for a broad range of areas. Due to its generality, it also does not limit the SEMIOTICS solution to one specific domain.
- The Amazon IoT CORE platform (Amazon Web Services, 2018a) has been chosen because of its high availability
- The Microsoft Azure IoT platform provides mature analytics tools and "on-premise" deployment.
- Amazon and Microsoft Azure platforms are also highly auto scalable and both allow serverless computing (Lambda and Azure Functions respectively).
- The main reason of choosing MindSphere is its industrial readiness. Also MindSphere allows increasing productivity of businesses in different domains.

All the information given bellow is based on product websites and should be treated as producer information, during comparison we didn't check if the features are really present in the software and working correctly.

3.5.1 AWS IOT CORE

3.5.1.1 OVERVIEW

AWS IoT CORE (presented in the Figure 6) is an IoT platform built by Amazon (Amazon Web Services Inc, 2018a). AWS IoT CORE is one of the leaders of the market. The platform provides bi-directional communication between sensors or other devices, actuators, smart appliances and the AWS Cloud. This functionality enables collecting data from multiple sources, as well as storing and analysing the data. The platform also gives the opportunity to create applications that interact with control and actuation process. All of the platform components are deployed in the AWS cloud. The limitation is that the most of these components can be deployed only in the AWS cloud. The big advantage of this platform is that it offers embedded scalability. AWS IoT CORE can support almost unlimited number of devices and messages and can process and route messages to AWS endpoints and to other devices in a reliable and secure way according to documentation of this platform.

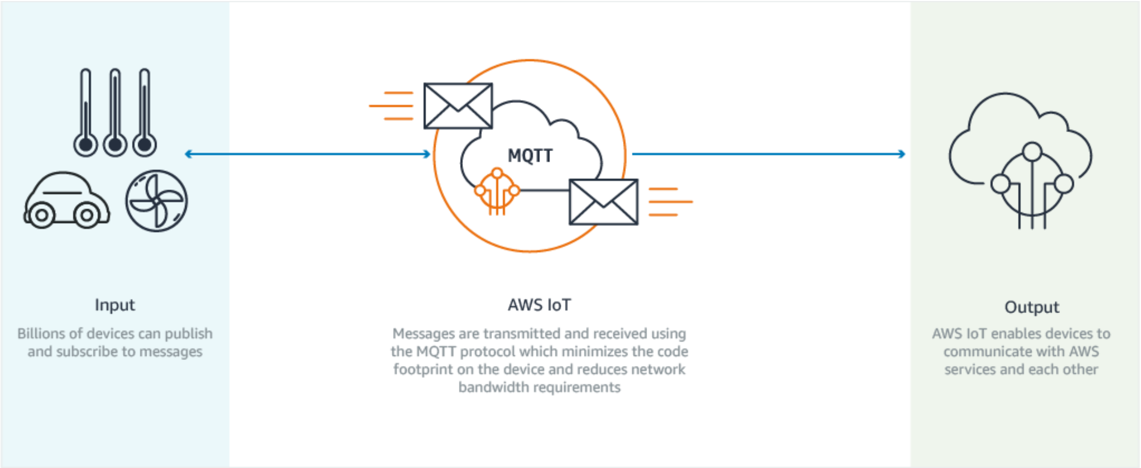

MQTT
Input
Billions of devices can publish and subscribe to messages
AWS IoT
Messages are transmitted and received using the MQTT protocol which minimizes the code footprint on the device and reduces network bandwidth requirements
Output
AWS IoT enables devices to communicate with AWS services and each other

Figure 6 AWS IoT Core (source: Amazon Web Services, Inc. (2018a))

3.5.1.2 ARCHITECTURE

The architecture of AWS IoT CORE (Docs.aws.amazon.com, 2018) can be seen on the image below (Figure 7). The diagram presents generic structure of IoT environment, where the central element is AWS IoT CORE and is connected with devices and sensors as well as end users. Optional elements are on the right hand side and can be used for calculations that are more significant or advanced analytics. Presented AWS Lambda allows serverless computing (Amazon Web Services, Inc. (2018c)), Amazon DynamoDB provides NoSQL database service (Amazon Web Services, Inc. (2018d)), while Kinesis enables to easily collect, process and analyse data in real time (Amazon Web Services, Inc. (2018e)), according to AWS documentation.

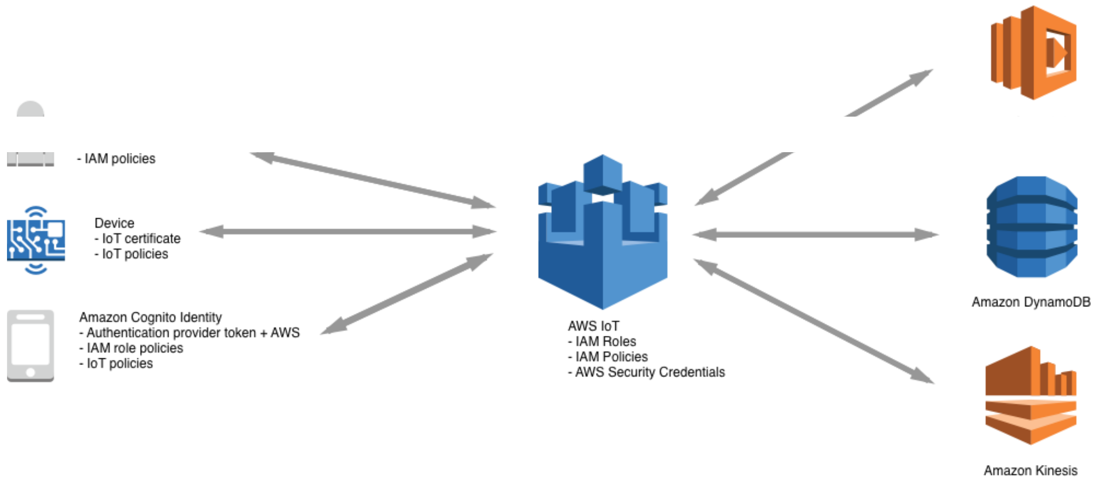


Figure 7 AWS IOT (source: Docs.aws.amazon.com, 2018)

The basic components of the AWS IOT CORE architecture are (Amazon Web Services, Inc. (2018f)):

Message broker – This component is responsible for provide secure mechanism for communication between devices and the platform. The component makes available the following protocols: MQ Telemetry Transport (MQTT) (Mqtt.org, 2018) which is standard IoT protocol and HTTP REST interface to publish events, which is also a standard and it was described widely by Massé (Massé, 2012).

Device gateway – This component is responsible for secure and efficient device communication with platform. Serves the entry point for devices via MQTT and HTTP protocols with low latency. This component is automatically managed and scaled to support a huge number of devices without changing environment infrastructure. This component supports bidirectional communication and allows devices control.

Rules engine – This component provides a message processing mechanism and integration with other AWS services or devices. The engine is based on the SQL language described in literature (Melton, 1996) to select data from message and sends data for further processing to other AWS services such as Lambda function, Dynamo DB or Kinesis described before.

Jobs Service – This component/service is used to define operations that need to be executed on devices connected to AWS IoT. The service allows optimization of remote command executing, for example firmware installation or perform programmable operations. It can also be used for the periodic execution of scripts/commands on devices.

Device Shadow service – This component represents the current state of a device, even when this device is not currently available. Synchronization of current state should be done periodically or when device is connected again. Device shadow represent current state in JSON format (device metadata).

3.5.1.3 KEY PROPERTIES

Security, Privacy & Dependability:
AWS IoT CORE has been built from AWS blocks that are greatly scaled out of the box. According to AWS all critical components of the platform have high dependability. In AWS IoT CORE, user trust and data privacy are one of main priority. Users can manage access to their own resources and services, and data are stored in selected region. AWS claims that without user acceptance, data content can't be shared or copied. This platform provides also dedicated frameworks in order to secure systems based on ASW components and access to data according to documentation of the platform (Amazon Web Services, Inc. (2018a)).

Scalability:
AWS IOT uses advanced networking technology, which is designed for scalability (Amazon Web Services, Inc. (2018a) and high availability. Most of the platform components can be clustered or multiplied. Additionally, processed events can be filtered or terminated on message broker before sending them forward to analysis. This functionality is one of the most important advantage of AWS IoT CORE and makes the platform stand out from the others.

3.5.1.4 SEMIOTICS VIEW

IIoT Components

This platform doesn't have components that could directly support IIoT. AWS IoT platform is a very generic solution with a well-developed part of the cloud services. Flexible reports, monitoring and analytics can be well rated by industrial needs, for rapid and frequent changes. Very important tool mentioned before, IoT device SDK, allows to quickly connect hardware device or software application. This property can be very helpful and crucial because one of the project goals is to achieve easy connectivity framework for devices

Local (Edge) IIoT Application & Smart Object Management & Analytics

AWS IoT CORE analytics is well integrated with the platform and automates all steps required for setting up, configuring and performing data analysis. The first step to start data analytics is to define MQTT topic and filters to process only selected events. AWS IoT Analytics stores the device data in an IoT optimized time-series data store for analysis and provides a built-in query engine that allow searching MQTT messages by using Syntax similar to SQL with ability to search by JSON payloads. The engine also supports time-series analysis. This can be used to analyse the performance of devices over time and understand how and where they are being used.

IIoT Enhanced SDN/NFV networking support

Devices are directly connected to IoT platform endpoint what is not aligned with SEMIOTICS framework where IoT Gateway routes the communication between devices and IoT platforms. AWS approach doesn't assume direct use of SDN or NFV hence for the purpose of the SEMIOTICS project, additional network layer would have to be added to restart the traffic from devices to IoT Gateway e.g. from SDK software layer.

Discovery & Semantic Interoperability

All connected devices can be provisioned, activated and deactivated from the level of IoT Core and such actions are available through SDK. This meets the requirement of SEMIOTICS project where provisioning and smart actuation process is one of the main goals. Additionally, leveraging of JSON data format allows processing of every type of the event message ("Thing event") what gives a vast opportunity and flexibility.

Control & Adaptation

The platform is resistant to situations, where devices or sensors are unavailable and do not emit events. In this situation device shadow service can hold an image of last device state and improves stability of data processing. The platform provides many ways to interact with devices:

- AWS Command Line Interface (AWS CLI) – This helps running AWS IoT commands on Windows, macOS and Linux system.
- AWS IoT API – API is designed for creating and managing things, certificates, roles and context security policies via HTTP/HTTPS protocol.
- AWS SDKs – These SDKs wrap Http(s) API and allow to program IoT applications in any supported language
- AWS IoT Device SDKs – These SDKs allow building applications to install and run on devices. This software publishes events to IoT platform and starts "Thing" processing.

Connecting new devices to AWS IoT requires: connection to Wi-Fi network and identification files (private key, root CA) to establish secure data exchange. After this step, device is ready and can publish messages to AWS IoT. Described procedure seems to be easy but moves responsibility for connecting to device layer.

Learning & Evolution

The platform offers two components for this purpose: (1) DynamoDB (NoSQL database provides fast and predictable performance) and (2) Amazon Kinesis (software for data stream processing). The latter can really improve the "machine learning" aspect, where events are processed in on-line mode (stream processing) and off-line mode, basing on archived data stored in database. AWS provides also the SageMarker service that is used for machine language. It's very quick, easy to build and deploy a ML model which is based on high performance algorithms. ML processing is described below on the diagram (Figure 8) according to documentation (Amazon Web Services, Inc., 2018):

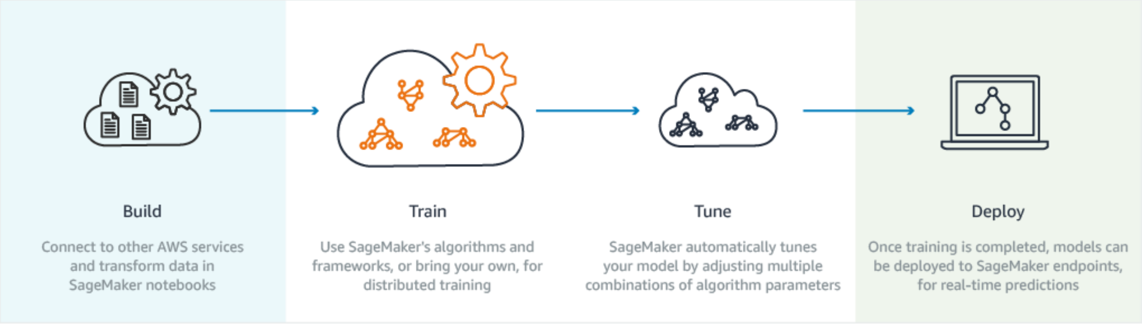

Build
Connect to other AWS services and transform data in SageMaker notebooks
Train
Use SageMaker's algorithms and frameworks, or bring your own, for distributed training
Tune
SageMaker automatically tunes your model by adjusting multiple combinations of algorithm parameters
Deploy
Once training is completed, models can be deployed to SageMaker endpoints, for real-time predictions

Figure 8 Machine Learning [source: Amazon Web Services 2018]

Monitoring Management & Adaptation

All devices, which publish events to IoT platform, have their own unique identifier. This property allows monitoring all connected devices, finding faults or identifying source of problems in monitored environment. In addition, all infrastructure components are monitored in CloudWatch (Amazon Web Services, Inc. (2018g)) – native AWS monitoring component with a graphical console.

Additionally, this monitoring component gives a full access to collected metrics and presents them in a graphical mode. This data came from different AWS components like Amazon Elastic Compute Cloud - Amazon EC2 - instances providing secure resizable cloud-computing (Amazon Web Services, Inc. (2018h)), Amazon Elastic Block Store - Amazon EBS - block store volumes which can be used as physical hard drive after attaching to EC2 instance (Amazon Web Services, Inc. (2018i)), Elastic Load Balancers handling varying application load traffic (Amazon Web Services, Inc., (2018j)), Amazon Relational Database Service (RDS) Instances allowing easy management of relational database (Amazon Web Services, Inc., (2018k)) . Next advantage is that device data monitor can predict issues, monitor sensors to predict and react to environmental conditions.

Time is another important element for monitoring, so in response to this need Amazon introduced new service. Time Sync Service (Amazon Web Services, Inc., (2018l)) allows to continuously monitoring time infrastructure and is based on a fleet of satellite-connected and atomic reference clocks enabling to deliver current time readings of the global standard UTC. This particular service is natively accessible from Amazon EC2 instances enabling cloud computing, according to AWS.

End-to-end Security

All the devices connected with broker or Device Shadow service must have credentials to connect. All traffic between AWS is secure and encrypted over Transport Security Level (TLS version 1.2) (Tools.ietf.org, 2018). Device credentials are kept safe to ensure confidentially data transmission to the broker. AWS offers many clippers for encrypting MQTT and TLS protocols. The platform provides also an end-to-end authentication framework, so transmitted data cannot be exchanged between devices and the platform without proven identity. Certificates management is available from the platform's console or API.

Limitations & Opportunities

The platform is a typical cloud solution and all of data are stored and processed in the public cloud. This approach can generate issues for many companies where an "on premise" model is the corporate standard. An alternative to this could be a hybrid model, where **events** from devices are routed to some module on premise and then routed to cloud for further processing, as UC3 proposes. Another disadvantage is that most of used components of this platform cannot be run on another cloud supplier because they are custom AWS services. In this case, SEMIOTICS framework could leverage mixed components, but all AWS services have to be deployed in Amazon Cloud. Amazon components (not only used in AWS IoT platform) can be used as a good support for any system, since AWS guarantees auto scaling on demand, and secure and stable functioning.

3.5.2 AZURE IOT SUITE **(MICROSOFT)**

3.5.2.1 OVERVIEW

Microsoft Azure IoT Suite (Docs.microsoft.com (2018a)) is a solution that allows to get started quickly through a set of extensible pre-configured solutions. These solutions address common IoT scenarios such as remote monitoring, asset management and predictive maintenance. The Azure IoT suite enables you to connect a broad range of devices types and operating systems, so there is no need to replace technology that you already have. The platform gives the possibility to connect entire chains of devices from the factory floor to the field and to capitalise on device-generated data using advanced analysis capabilities to uncover new insights. This solution is designed to quickly create both proof of concept IoT applications and fully-fledged industry ready IoT solutions in a quick and easy manner, and with broad scaling. This platform also supports gradual expansion to avoid pitfalls during project progress. The data processing mechanism is described below on the diagram (Figure 9).

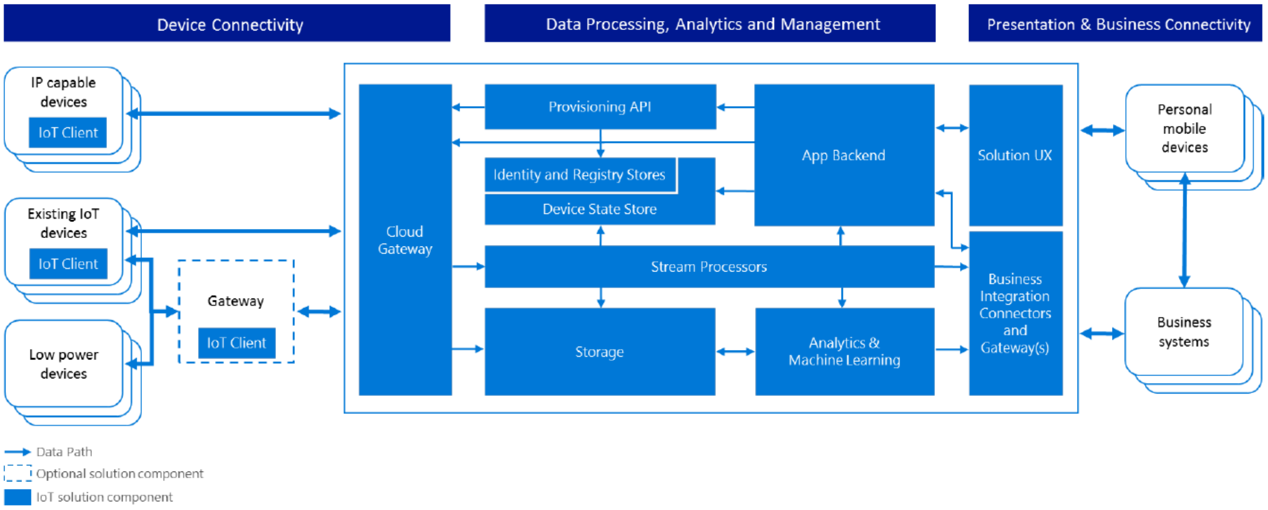


Figure 9 Processing diagram (source: Download.microsoft.com, 2018)

Devices may be connected directly or indirectly via gateways, and they can implement edge data computing with different levels of processing capabilities in both cases. The main interface for devices is provided by Cloud Gateway and facilitates bidirectional communication with backed system or 3rd party systems. The backend is composed of components responsible for discovery, data collecting, message transformation and analytics. These provide the possibility for implementing business applications and visualisation dashboards.

3.5.2.2 ARCHITECTURE

This platform supports various device connection models, what can be seen on the image below (Figure 10). These include:

- Direct connection with IoT Cloud Gateway - This type of communication can be established for IP capable devices that can make secure connections over the Internet.
- Connection via field gateway – This type of communication is for devices that use specific protocols (Constrained Application Protocol (CoAP, Vishwesh, J. and Rajashekar, M. 2017), OPC (OPC Foundation, 2018)) or short range communication via Bluetooth (Bluetooth.com, 2018) or ZigBee(Zigbee.org, 2018), devices not connected directly to internet or not capable of communication encryption (TLS/SSL(Sans.org, 2018)).
- Connection via a custom cloud gateway – This type of communication is used when the data or transition protocol require translation or pre-processing, to adapt to the IoT gateway standard.
- Connection via a field gateway and a custom cloud gateway – This type of communication is used when the data or used protocol require some customization and when the connection to cloud gateway must be established via network tunnels or Virtual Private Network (VPN) technology.

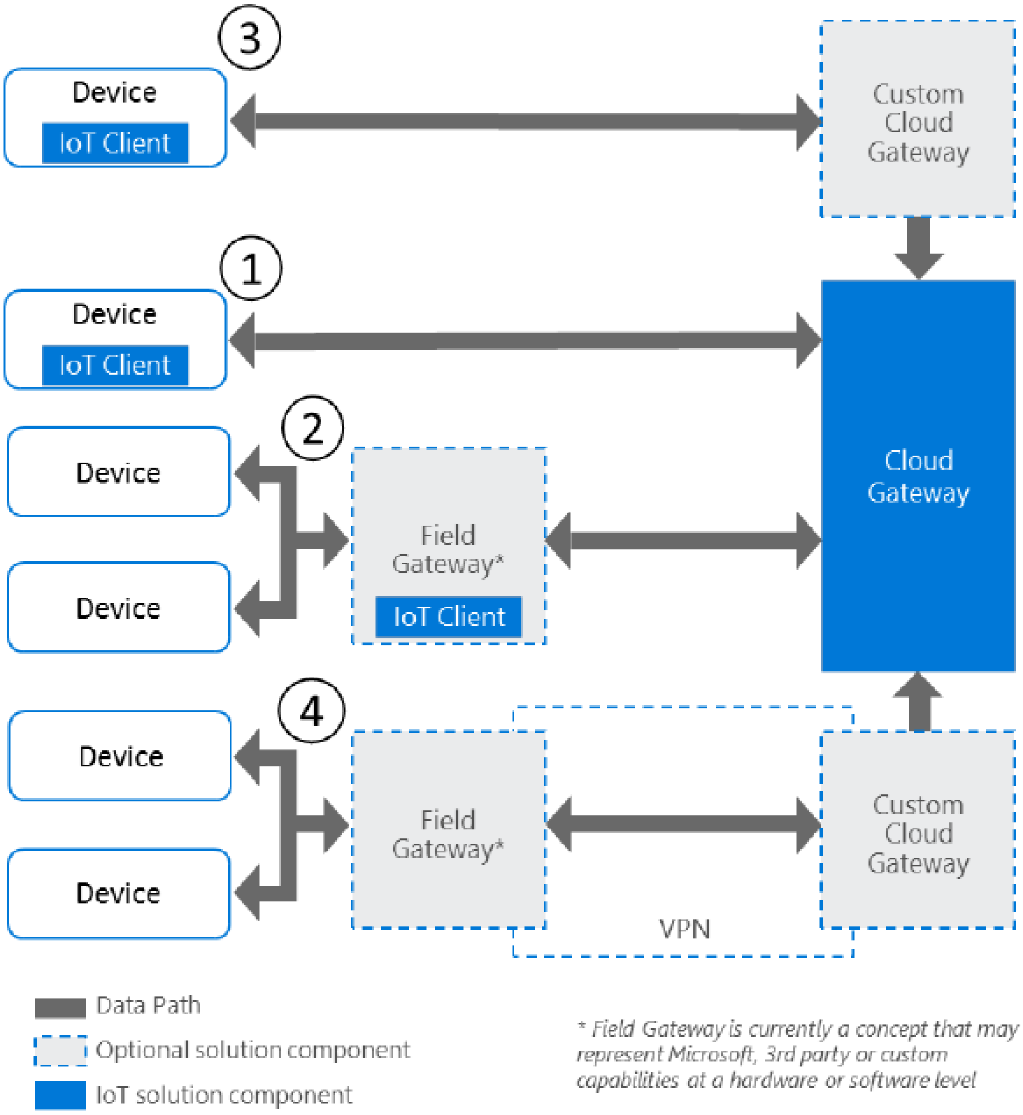


Figure 10 Communication Diagram (source: Download.microsoft.com 2018)

The basic components of the AZURE architecture are:

Field Gateway – component is responsible for establishing communication between device and back end, it has functionality, which is designed for network processing, steering devices and filtering messages. One of important functionality is aggregating data to maintenance traffic and reducing unwanted data transfer to cloud back end. This part of system can be deployed as a specialized device-appliance or dedicated software for general purpose. The usage of this component is optional and focused on local analytics.

Cloud gateway–this is main part of cloud-based system, providing remote communication between field gateway and devices which usually reside at several different sites. To isolate cloud gateway with all devices from other network traffic, the cloud gateway is reachable over the public internet, network virtualization overlay (i.e., VPN) or private network connections into Azure datacentres. This component addresses transport, device connection limits, authorization, authentication and all security aspects. In addition, system processes data for billing, provisioning and monitoring tasks over event-driven architecture and common communication patterns.

- *Message broker* - This component allows decoupling the edge from the cloud components, smooth-following processing and scaling runtime environment. Received events are permanently stored in the broker and they are available for multi consumers of data (topic pattern). This communication model is supported in both directions and when a device is unavailable; the broker stores the message (command) and delivers it when the device is reachable. Every message has set time to live duration (TTL).
- *Custom gateway* – This is a dedicated layer, which supports standardisation/adoption of protocols and messages transformation before reaching final cloud gateway endpoint. In this component, custom message processing is possible. This may, for example, involve injecting some data, compression/decompression messages. In this solution, data processing can be very fast.
- *Device identity store* – This component is a typical registry of information for all integrated devices. The component can be used for client authentication or getting cryptographic information about devices. The identity store does not provide searching facility; it only supports getting information by device identifier. The cloud gateway (see above) is looking regularly for the authentication device purpose, in this way that component has very fast access interface.

IoT Edge – This component allows making some custom logic and analytics on device side and can focus the cloud layer only for business logic and data processing. This software layer is very important in situation when system is able to make decision on the device very fast without sending stream of events to cloud. IoT Edge helps to respond as quickly as possible to emergencies and can reduce bandwidth costs and transferring not necessary events (reducing network traffic and data transfer costs). Azure IoT Edge is composed by 3 components: IoT Edge modules, runtime and interfaces.

IoT Edge modules – These are containers to run Azure services and 3rd party or custom code. All of these containers are compatible with Docker (Docker, 2018) platform enabling distributed computing, and can be connected to each other to create a pipeline of data processing. Custom service implementation can wrap with container or run as Azure service. Thanks to this solution, it is possible to deploy complex data processing and machine learning. Without any problem on the edge, it can be installed Azure services like Azure Functions, Azure Stream Analytics, and Azure Machine Learning.

IoT Edge runtime – This is a runtime environment runs on each IoT Edge device, manages all deployed containers for each device. It enables custom cloud logic and analytics. The environment performs several functions, including:

- Installing and updating workloads on the device.
- Maintaining Azure IoT Edge security standards on the device.
- Ensuring that IoT Edge modules are always running.
- Reporting module health to the cloud for remote monitoring.
- Facilitating communication between downstream leaf devices and the IoT Edge device.
- Facilitating communication between modules on the IoT Edge device.
- Facilitating communication between the IoT Edge device and the cloud.

The IoT Edge runtime scheme is presented in the Figure 11.

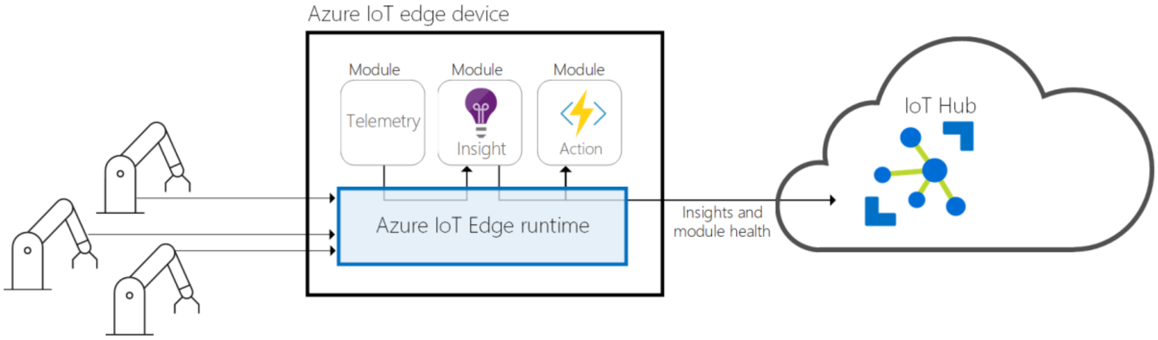


Figure 11 Edge runtime (source: Docs.microsoft.com, (2018b))

IoT Edge cloud interface – This component enables to monitor and manage remotely of connected devices to IoT Edge. The component realises very important and difficult task - managing lifecycle millions of different heterogeneous devices. Workloads are created and configured for particular type of devices, periodically deployed and monitored to find any misbehaved device. The IoT Edge cloud interface is presented in the Figure 12.

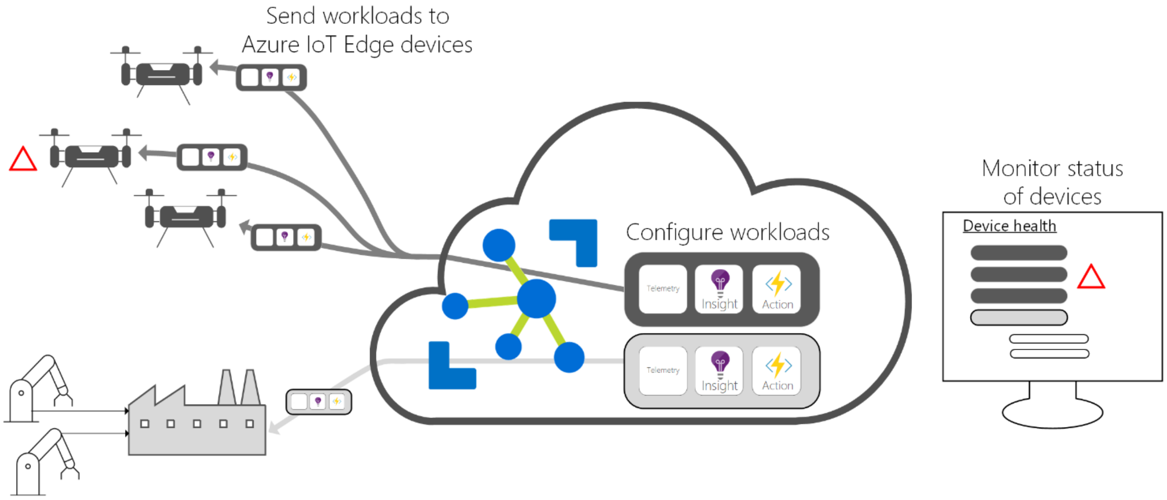


Figure 12 Cloud Interfaces (source: Docs.microsoft.com, (2018b))

3.5.2.3 KEY PROPERTIES

Security, Privacy & Dependability:

Azure ensures secure connectivity devices and cloud, device provisioning and confident data management in the cloud. This platform provides authentication mechanisms for end users and devices and protects them from cyber and physical attacks.

Scalability: This platform is one of the many cloud–based solutions where scalability and stable data processing are the main advantages. IoT Azure is platform designed to process over 300 million messages per day and can support about 1 million of simultaneously connected devices. This is impressive but sometimes it may not be enough. In very particular situation, where high performance is required or other speed-processing characteristic cannot be guaranteed by a single IoT platform, a sharing approach should be used. In this case, it is recommended to partition of devices into multiple IoT hubs, what can ensure right data processing time and system reaction for changed environment behaviour. To properly scale solutions, an initial analysis is required where volume and numbers of exchanged messages between devices and cloud, volume of identity registry operations are gathered and analysed.

3.5.2.4 SEMIOTICS VIEW

IIoT Components:

This platform has dedicated component that can really improve support for IIoT. IoT Edge supports local analytics and devices management, can be used to fast data processing in the edge. Additionally, this platform gives a full play in setup connectivity in field and network layer. A few configurations to establish connectivity are supported and very well documented.

Local (Edge) IIoT Application & Smart Object Management & Analytics:

The platform supports local analytics on device side by dedicated IoT Edge component. This is very important matter from the point of view of this project. Used solution can be a good pattern and shows benefit of this usage.

IIoT Enhanced SDN/NFV networking support:

This platform supports device management by mentioned before IoT Edge runtime component, so local data management, pre-processing and analytics is provided out of the box. Because platform provides some functionality out of the box, development process should be shorter than in other platforms.

Discovery & Semantic Interoperability:

Azure IoT Hub provides functionality for full management of devices including bulk configuration changes and firmware updates, creating devices metadata information and monitoring. Below some typical management patterns supported by Azure:

- Reboot – command initiated from backend, charge device to reboot and register in platform when will be available again.
- Factory reset – command initiated from backend, charge device to reset software setting to factory setting.
- Configuration – command initiated from backend using desired properties to configure software on device. In that case can be changed device behaviour or data message content.
- Firmware update – command initiated from backend, to start firmware update procedure.
- Reporting progress and status – command initiated from backend as a query for current device status and progress of running tasks on the device.

Control & Adaptation: Azure allows using field gateway component at network level when devices cannot directly integrate with Cloud Gateway. An additional layer is a right place for data or network translation and provide a good opportunity to integrate device with cloud Gateway if is not possible to make it directly (for example when is not possible to install software on the device). Azure delivers dedicated tools for remote device management for operators, to changing software configuration and parameters and manage software updates.

Learning & Evolution: Azure stream processing is a central component, which is responsible for real-time and on-demand analytics. This allows developing and running very fast massive parallel analysis from one or more IoT streams of data. The engine provides possibility to analyse and predict some devices behaviour (basing on trends). One of the most important feature is that this service can be run on Azure IoT Edge component, performs local analysis and **real-time intelligence closer IoT devices**. This service usage allows to significantly decreasing volume of device-generated data to cloud. Microsoft provides also Azure Machine Learning service, for easy and fast creating and deploying predictive models. Both ML Studio and ML service are available only as cloud, so to create their own model only internet access from PC is required. Studio has a set that is ready to use algorithms and models as well as it gives tools and possibility to build custom predictive model (math formulas/algorithms to analyse historical and current data to identify trends). Microsoft Machine Learning is a mature solution, where developer can very fast (drag and drop options) prepare test, verify and deploy model on runtime environment. Basic workflow of Azure Machine Learning is presented in the Figure 13.

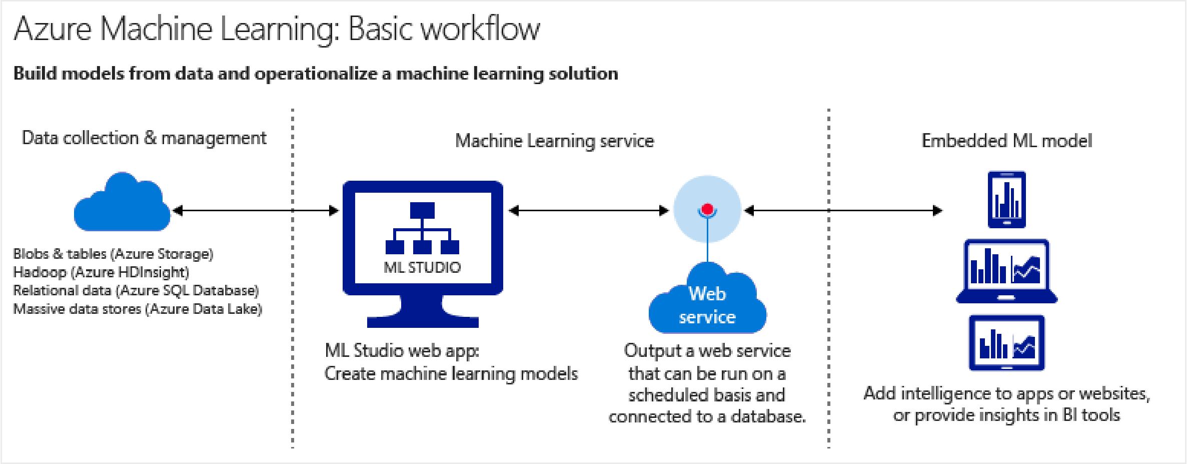

Azure Machine Learning: Basic workflow
Build models from data and operationalize a machine learning solution
Data collection & management
Machine Learning service
Embedded ML model
Blobs & tables (Azure Storage)
Hadoop (Azure HDInsight)
Relational data (Azure SQL Database)
Massive data stores (Azure Data Lake)
ML STUDIO
ML Studio web app:
Create machine learning models
Web service
Output a web service that can be run on a scheduled basis and connected to a database.
Add intelligence to apps or websites, or provide insights in BI tools

Figure 13 Machine Learning (source: Docs.microsoft.com, (2018c))

Monitoring Management & Adaptation: Azure provides dedicated monitoring for 6 aspects:

- Device identity operations
- Device telemetry
- Cloud to device messages
- Connections
- File uploads
- Message routing

Monitoring does not affect data processing and it does not change messages order. Overall, it offers a valuable aspect because it can inform about broken connections or field connection attempts. Such information can have a huge impact on calculations where algorithm requires current state/data from a couple devices (lack of one data can change the result completely). The monitoring system of Azure is based on a REST API and a micro-services approach. This is meant to ensure scalability and stable processing.

End-to-end Security: Azure has a strong focus on security patterns in device - cloud communication bases on security model standard: Detect Assess, Diagnose, Stabilize and Close (Docs.microsoft.com, 2018a). Azure is secured not only inside the platform, but also for the end user. This platform also allows interoperating securely with devices which support or not the IP protocol. Every device has their own unique identifier, which is part of the token used by the IoT infrastructure. The communication path between devices and IoT hub is secured by standard TLS and authentication using X.509 protocol (Tools.ietf.org, 2018). Azure's Active Directory (AAD) manages additional access to data in the cloud. AAD provides authentication and authorization functionality and easy access to resource management. Data in the cloud can be stored in Azure Cosmos DB or other databases, which support definition of the level of security, desired. The communication of security and privacy is described on picture below (Figure 14).

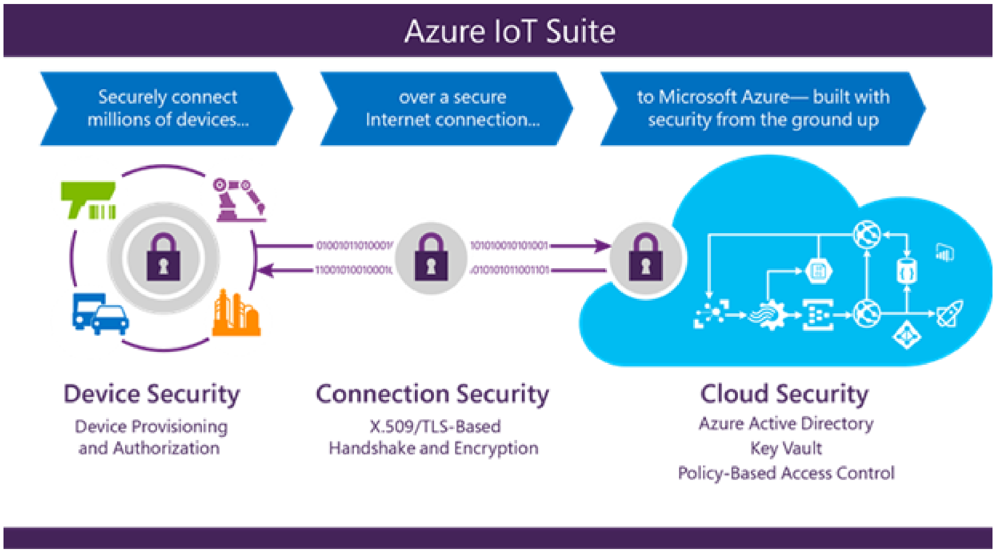

Azure IoT Suite
Securely connect millions of devices...
over a secure Internet connection...
to Microsoft Azure— built with security from the ground up
Device Security
Device Provisioning and Authorization
Connection Security
X.509/TLS-Based Handshake and Encryption
Cloud Security
Azure Active Directory
Key Vault
Policy-Based Access Control

Figure 14 AZURE IoT Suite (source: Docs.microsoft.com (2018a))

Limitations & Opportunities: The Azure platform is a typical cloud solution, which does not support a hybrid architecture (where some components are deployed on premise). Another limitation is that most of components are based on the .NET platform (Docs.microsoft.com, 2018c) and it could be a difficult for those using Java based solutions. A very positive aspect of Azure is its architecture that uses a micro services approach – currently very popular architecture pattern for developing an application as a set of small independent components (Tanaserri, N. (2017)). Hence, building dedicated APIs to integrate the platform with other systems is not problematic.

3.5.3 MINDSPHERE (SIEMENS)

3.5.3.1 OVERVIEW

MindSphere (Cache.industry.siemens.com (2018a)) is an operation system for Internet of Things, which is based on open standards and interfaces, and organises and connects devices regardless of suppliers. This platform (see Figure 15) is responsible for collecting and suitable selection of data for further processing and analysis. MindSphere provides security standards for all elements of the system starting from devices, across the network layer to the cloud backend and authorized access for end users. The platform supports usage of Siemens, 3rd party suppliers and custom-made services as MindApp components. Another advantage is that end user can use application data to get and manage resources/things/systems in real time. All gathered data can be combined together and provide completely new insights, which is of crucial business value.

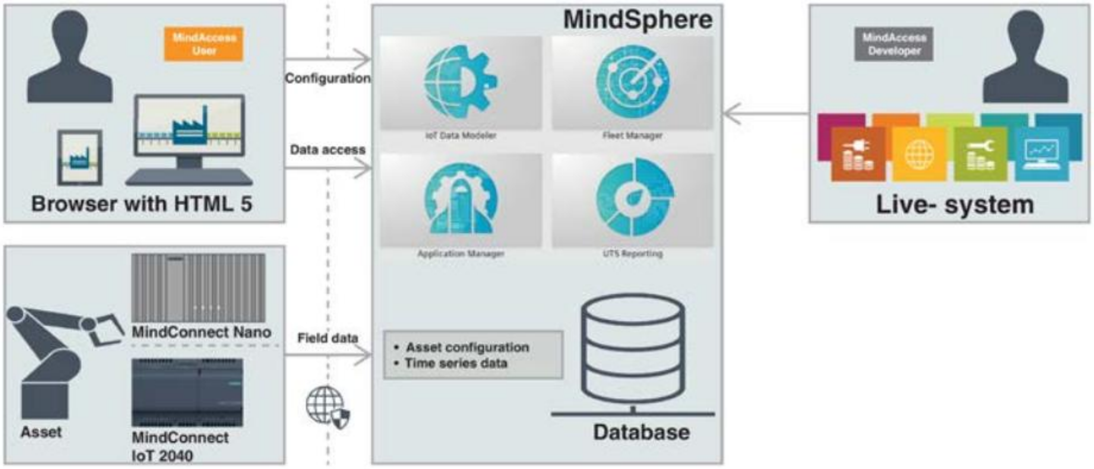


Figure 15 MindSphere (source: Cache.industry.siemens.com (2018a))

3.5.3.2 ARCHITECTURE

MindSphere (Cache.industry.siemens.com (2018b)) is another commercial IoT platform developed by Siemens Company. The MindSphere layers architecture is presented in the Architecture - Developer Documentation. The platform consists of two distinct layers:

- First layer: This layer provides a managed Platform as a Service (PaaS) to host your applications directly on MindSphere, service platform which allows you to use our services via public APIs in your own solutions and
- Second layer: This layer includes MindConnect Elements which provide the plug and play hardware and customizable software components to get application data into the platform

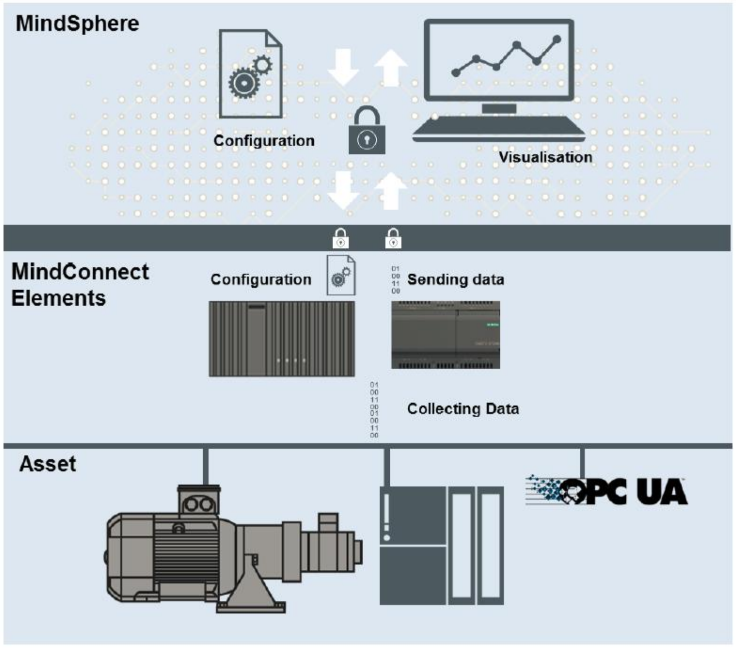


Figure 16 MINDSPHERE LAYERS (source: Cache.industry.siemens.com (2018b))

Description for most important components can be found bellow.

Mind Access (Developer): Mind Access is web-based application portal, where authorized users can manage resources (Assets), deploy and test applications. Work with this tool starts from creation of individual account and granting appropriate roles. One of them is the “MindAccess Developer” role, which is required to start creation of assets, configuration, access to applications and saving data. One of Mind Access part is IoT Data Modeler. This tool is used for user or organization management and assets configuration. Organization management allows granting and revoking rights to manage Assets and create configurations. User management works through a typical simple administrator panel, where managing users and assets is their main functionality.

Mind Connect: This component (hardware and software) enables collecting data from devices and transferring date to MindSphere for future processing and analysis. For example, one of hardware tools can be MindConnect Nano (Support.industry.siemens.com, 2018a) or MindConnect IoT2040 (Support.industry.siemens.com, 2018b), which are responsible for collecting and secure data transferring over the Internet. Such dedicated connectors enable data encryption, and fast and easy connectivity of machines/sensors to MindSphere. They also support data collection via standard protocols (and additionally Siemens S7, OPC UA), free maintenance and up-to-data software. The software approach to connect devices with platform is based on MindSphere SDK - MindConnect LIB - native library (Siemens PLM Community, 2018).

Applications for MindSphere: Mind Applications (MindApp) constitute a crucial part of MindSphere, where Siemens or 3rdparty applications can process collected data and visualize the result of analysis. This is the right place for installation of custom-made applications, which are focused on special (end-user/business) processing of data. This core platform element is based on Cloud Foundry, open source and multi cloud application PaaS.

MindConnect API: This platform exposes a set of different APIs for collecting and sending data to the cloud. The platform also provides APIs for main functionality like customer, user, and agent and asset management, file services and so on. Most of these APIs provide the possibility to configure resources and manage users skipping the MindSphere Portal (web) layer. Another service is the Trigger/Rule Engine, which enables to add new rules to process, for example, new request events.

This platform supports two approaches in device integration with platform:

- Using hardware – there is an additional layer between device and MindSphere, which is based on physical device. Actually 2 types of devices are supported by mentioned: MindConnect IoT2040 and MindConnect Nano. In the first approach to ensure secure and rapid data transmission in environment, there should be installed physical devices, which support interaction between devices and network layer.
- Using software – this approach requires building software integration layer which bases on provided libraries: MindConnect FB (Cache.industry.siemens.com, 2018c) and MindConnect LIB

The main functionality of MindSphere is based on Cloud Foundry. All custom services (applications) and Siemens native services are deployed on Cloud Foundry, which ensure horizontal (load balancing) and vertical (changing CPU, RAM allocation) scaling out of the box.

3.5.3.3 KEY PROPERTIES

Security, Privacy & Dependability:
MindSphere is running on SAP HANA Cloud Platform and this property guarantee that dependability, stable and fast processing within the one of MindApplication. During the construction of this platform, the privacy aspect was one of most important aspect. All steps that have to be done for import data to MindSphere platform are controlled and managed by MindAccess User. MindSphere provides also set of roles, that can be assigned to user and offers them some functionalities (for example "MindAccess Developer"). Security data transmission/communication devices/sensors/actuators are provided by mentioned before MindConnect component.

Scalability: Data processing is directly dependent on services deployed on CloudFoundry. The system is scalable if the used custom service will support scaling and are free of internal bottlenecks. MindConnect (IoT gateway layer) is scalable due to hardware specification and its functional responsibility.

It should also be noted that, as of 2018, MindSphere will be able to use Amazon (AWS) services like Kinesis (Amazon Web Services, Inc. (2018e)) or other databases and components. That future will be available in next version of MindSphere.

3.5.3.4 SEMIOTICS VIEW

IIoT Components: MindSphere is an IoT platform that specializes in industrial implementations. The key component is MindConnect Nano, i.e., a dedicated device allows for fast, secure connectivity devices/sensors with IoT infrastructure. This hardware-based component can be connected with many different sensors and actuators. The device sends data to MindSphere with protocols: Siemens S7 (Cache.industry.siemens.com (2018a)), OPC UA (Cache.industry.siemens.com (2018a)).

Local (Edge) IIoT Application & Smart Object Management & Analytics: Currently this platform does not support local analytics. Locally gathered data by MindConnect are sent do MindSphere for future processing

IIoT Enhanced SDN/NFV networking support: MindConnect can be used as an element controlled by an SDN/NFV component, as envisaged by the SEMIOTICS architecture.

Discovery & Semantic Interoperability: MindSphere is a very heterogeneous system platform, although this is not obvious. On one side, device integration with the platform requires the MindConnect component. On the other side, the architecture of MindSphere gives an opportunity to use 3rd party components. Connecting with other supplier components require some development, but this approach should be acceptable for most of project budgets.

Control & Adaptation: New devices/sensors can be to the network or a MindConnect device Device control is guaranteed by an integration procedure and resources management that can be carried out through mentioned one of Applications for MindSphere *MindApp* (Cache.industry.siemens.com (2018b)). If a device is connected directly to *MindConnect* (described in an architecture section).

Learning & Evolution: MindSphere provides a simple rule engine (i.e., the Trigger/Rule Engine (Cache.industry.siemens.com (2018a))) and gives the possibility to define a few types of rules such as user-defined rules, action rules, and user-defined filtering rules. Furthermore, *MindAp*p provides a few helpful applications, including:

- Trend Prediction – This is an application that can analyse asset and machine time series data (including multiple data series), providing the ability to make algebraic and statistical calculations.
- Demand Prediction – According to information in MindSphere websites, this advanced application will be available in the future. It will be able to predict demand based on time-series data using pretrained neural network analysis,
- Sequential Pattern Mining – According to information in MindSphere websites, this advanced application will be available in the future. This application will be able to predict failures by pattern and sequence search in event logs.

Monitoring Management & Adaptation: MindSphere offers a monitoring application, called MindApp MyMachines (Legal.apps.mindsphere.io, 2018), which provides monitoring dashboards with information about configured tools and machine parameters, as well as information about critical machine data, machine status and history. Another application of the platform is Fleet Manager (Cache.industry.siemens.com, 2018d) that can be used for analysis, visualisation and assets monitoring. This application is a native application for making analytic task and create rules. Fleet Manager offers:

- Assets management and monitoring (limited by access rights)
- Data presentation

- Combining of data for an analysis
- Creating simple rules and queries

End-to-end Security: MindSphere meets IoT security standards. In particular, it offers two ways to connect a device with the IoT platform, i.e., through MindConnect hardware and MindConnect LIB. Both these mechanisms provide secure and encrypted connection to MindSphere. MindSphere has a separate environment for testing and production. Every registered platform user has own account and rights. Platform sensor connection is secure; sensors need to be fully configured before they can communicate with the platform.

Limitations & Opportunities: MindSphere IoT platform is a relatively new cloud-based solution and many of parts of it needs improvement. The platform can have only 10,000 monitored assets and does not support typical remote management operations on devices such as start, stop, restart and device software management (getting device software version, starting software upgrade). Nevertheless, MindSphere gives the possibility to develop custom app and integrate them with existing ones.

3.5.4 FIWARE (OPEN SOURCE)

3.5.4.1 OVERVIEW

Unlike the platforms reviewed in previous sections, FIWARE is not commercial, but an open-source cloud-based infrastructure for IoT platforms. This solution can be regarded as an IoT platform or as a platform for platforms. It is a different approach than other providers because it enables not only to build your own solution from scratch thanks to the generic enablers that it offers, but also to build new solutions upon existing components using multiplatform approach (Gemein, 2018). The FIWARE project is part of the *Future Internet Public Private Partnership* programme funded and created by the European Commission in collaboration with the information and communication technology industry (Future Internet Public Private Partnership (FI-PPP) 2018).

FIWARE is built upon the OpenStack-based cloud infrastructure (OpenStack 2018) and is enhanced by offerings from FIWARE Catalogue (Catalogue.fiware.org. (2018a); Guth 2016). What distinguishes this solution from the others is a rich library of components called *Generic Enablers*. Reference implementations allow easy development of functionalities such as the connection to the Internet of Things or Big Data analysis. FIWARE follows approach to represent *Device* with integrated specific entities as a whole and do not distinguish between *Sensors* and *Actuators*.

3.5.4.2 ARCHITECTURE:

The overall architecture of FIWARE solution is presented in Figure 17 (Martínez et al. 2018a), whereas more specific architecture of services enablement is in the Figure 18 (Guth et al. 2016). As it is shown in the figures FIWARE Generic Enablers are spread over two different domains, i.e., *IoT Backend* and *IoT Edge*, which are described below.

- *IoT Backend* – This domain contains the set of functions, logical resources and services hosted in Cloud datacentre. On the one hand, it is connected to the Context Broker (where IoT resources are translated into NSGI Context Entities), on the other hand IoT Backend is connected to the IoT edge elements (physical infrastructure)
- *IoT Edge* – This domain is made of all on-field IoT infrastructure elements needed to connect physical devices to FIWARE applications - typically, it contains: IoT end-nodes, IoT gateways, and IoT networks.

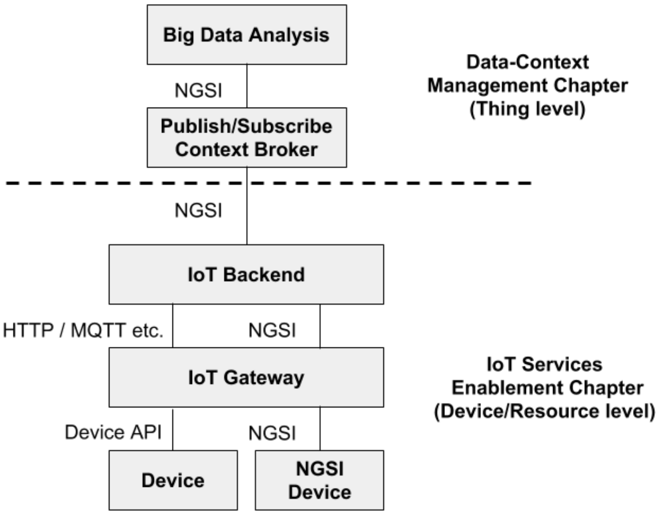

Big Data Analysis
NGSI
Publish/Subscribe Context Broker
Data-Context Management Chapter (Thing level)
NGSI
IoT Backend
HTTP / MQTT etc.
NGSI
IoT Gateway
IoT Services Enablement Chapter (Device/Resource level)
Device API
NGSI
Device
NGSI Device

Figure 17 FIWARE IoT architecture (source: Martínez et al. (2018))

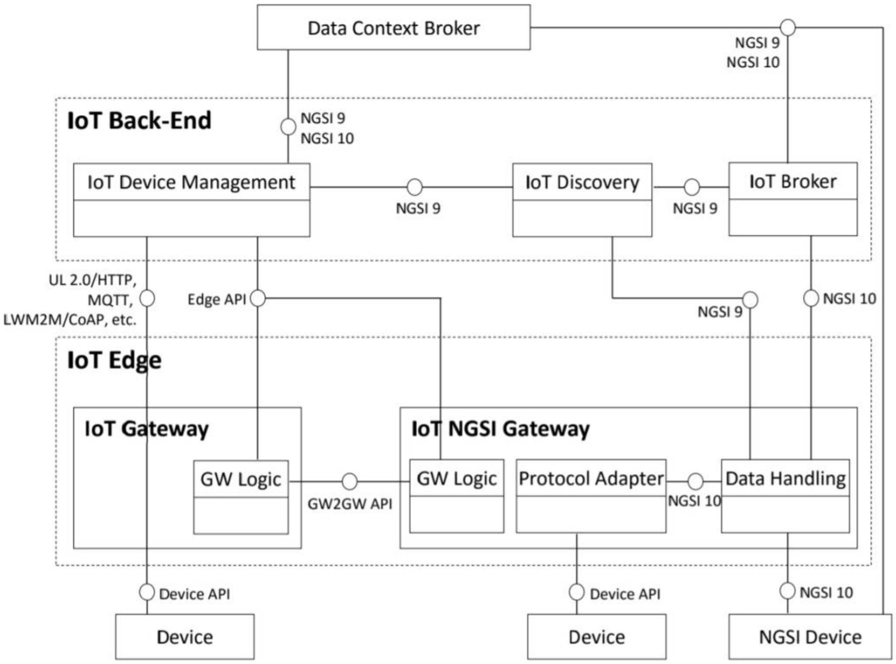


Figure 18. FIWARE IoT Services Enablement Architecture (source: Guth et al. (2016))

The *IoT Edge* contains the *IoT Gateway* and the *IoT NGSI* (*Next Generation Service Interfaces*) responsible for establishing and managing the communication between the devices and the *IoT Backend*. The core functionality of the FIWARE platform is *IoT Integration Middleware* which is located within *IoT Backend* and the *Data Context Broker*. FIWARE architecture is presented on the image. The typical use case scenario is a simple integration of IoT devices into Data chapter Context Broker. This scenario is available at FIWARE Lab for developers. The mandatory Generic Enablers in this case are:

- *Backend Device Management GE* – This GE responsible for translating specific communication protocol into NGSI, handling sensor notifications and some actuations from Context Broker to the device
- *Data Chapter Context Broker GE* – This GE handles all Context entities. It is natural interface for FIWARE app developers for reading IoT information and for triggering commands if it is possible through communication protocol of the device.

Optional Generic Enablers include:

- *Gateway Logic GE* – This GE handles the IoT Edge management API (and gateway-to-gateway API) but needs the corresponding function or module in Backend Device Management GE (Forge.fiware.org. (2018b)).

In full scenario it is possible to handle and combine native NGSI devices/Gateways and any other kind of IoT devices/gateways.

The basic components of FIWARE:

- *Device Backend Gateway* – This component collects data from devices using heterogeneous protocols and translates them into standard NGSI entities
- *Context Broker* – This component retrieves, maintains and deliver Context Information into the platform components and external systems
- *CEP (Complex Event Processing)* – This component analyses event data in real-time, enabling instant and predefined actions
- *Connector Framework* – This component adapts NGSI data from Context Broker to internal or external systems
- *ST (Short Term) Historic* – This component handles raw and aggregated queries based on short-term historic data.
- *Publish/Subscribe Context Broker* – This component is the main component of the architecture. Its function is not only to handle and aggregate context data from different context producers (e.g. devices), but also to be an interface between architecture actors. The information model used in FIWARE architecture is NGSI. In this model, all objects of the real word (sensors / actuators / devices) are represented as Context Entities, while information about these objects is expressed in the form of attributes. The generic architecture of Context Broker is presented in the Figure 19 (FIWARE Forge Wiki 2018).

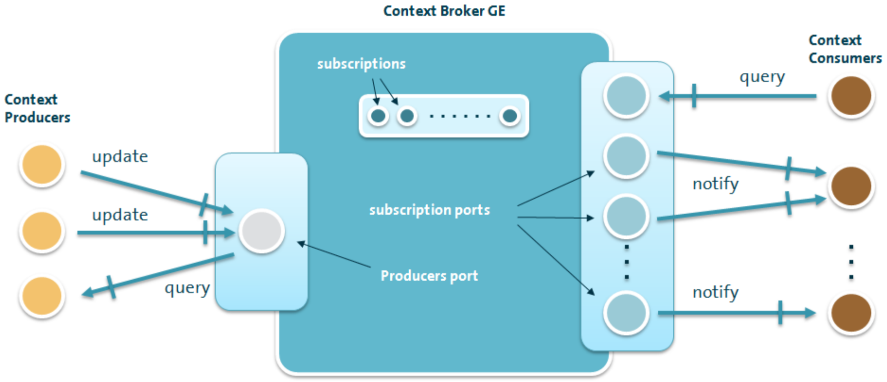


Figure 19 Generic architecture of Publish/Subscribe Context Broker (Forge.fiware.org. (2018a))

3.5.4.3 KEY PROPERTIES

Security, Privacy & Dependability

FIWARE is providing secure by design architecture build aroun*d Identity and Access Management* as well as *Access Control Decision and Enforcement* (Forge.fiware.org. (2018b)). The security architecture consists of three GE:

- *Identity Management GE* – This GE offers a backend domain API is provided by the overall security access mechanism based on industry-standard protocol for authorization Oauth2 (Boyd, 2012)
- *PEP Proxy GE* – This GE provides an enforcement of authorization policy to REST-based backed services in order to allow and restrict access to the available resources
- *Authorization PDP* – This GE can be used when non-REST APIs using PEP Proxy cannot be used.

According to FIWARE (Forge.fiware.org. (2018c)) critical attribute of the platform is enhanced security and dependability achieved by supporting automated Integration, configuration, monitoring and adaptation.

Scalability

There is a possibility to scale up IoT Broker, when the overload of information requests from devices appears, by adding new IoT Broker (slave). It is also possible to scale down in an analogous manner. Performed tests of horizontal and vertical scaling showed that the implementation of FIWARE IoT Agent are unstable and crashes during overload state (for more than 1000 requests per second) according to literature evaluation of the platform (Soto 2017).

3.5.4.4 SEMIOTICS VIEW

IIoT Components

FIWARE IoT platform itself is very generic and therefore it allows creating a platform for different purposes, but it takes time. There is no completely industrial ready components in *FIWARE Catalogue*, but on the other hand, there is an industrial initiative build upon *FIWARE* solution. It is called *FIWARE for Industry* **(**FIWARE For Industry, 2018). *FIWARE for Industry* extends *FIWARE Technologies* giving tools for implementation of *Virtual Factories* through *Academy of Industry 4.0* methods and tools, Lab of Open Source components, a *Hub* of reference architectures and digital platforms and also a *Showcase of Industry 4.0* success stories and best practice. All of this to show how to create your own solution upon *FIWARE* IoT platform.

Local (Edge) IIoT Application & Smart Object Management & Analytics

As it was mentioned before FIWARE is not providing dedicated solutions for IIoT application, but rather generic set of enablers. However, there is a Cepheus (Catalogue.fiware.org (2018c)) – IoT Data Edge Consolidation enabler, which addresses the need to process streams of data in real time, when character of data, requires aggregating and merging real-time data from different source.

Alternative solution is more complex solution FogFlow framework enabling edge analytics. It was created by NEC Laboratories Europe (NEC, 2018) and approved by FIWARE Foundation. It is not directly a part of FIWARE Catalogue. FogFlow is providing a programming model with sophisticated context processing modules and enabling to automatically distribute components to available resources. FogFlow technology can be also used as a cloud-edge platform to dynamically manage various data analytics services over thousands of sensors. The monitoring of abnormalities of things-events and real-time analysis is available with this solution. FogFlow is able to respond to changing environment taking into account availability, locality and mobility of IoT devices. This framework can automatically change orchestration of tasks over cloud and edges in an optimized manner as it stands in the description of this solution.

IIoT Enhanced SDN/NFV networking support

FIWARE provides generic enabler Netfloc that develops advanced elements for SDN networking approach. This is very important from SEMIOTICS point of view as it enables to provide the ability to efficiently manage resources and network configuration problems. This GE takes the form of SDK framework, which supports low-level OpenFlow protocol through transparent Northbound API as it is in documentation. Netfloc with the other two GEs composes the Advanced Middleware and Interface to Networks and Device Reference Architecture. This two others are: NETIC that is used for virtualization of networks, and Advanced Middleware which enables to build efficient and secure applications supporting a wide range of communication scenarios including across FIWARE GEs (Forge.fiware.org, (2018c)).

Discovery & Semantic Interoperability

The FIWARE Catalogue offers the IoT Discovery GE. Its role is to be a meeting point for IoT Context Producers (sensors and devices) and Context Consumers (discovering producers). The semantic interoperability – on of SEMIOTICS objectives – is provided by OMA NGSI-9 messaging protocol – powerful API for contextual information (Catalogue.fiware.org, (2018b)).

Control & Adaptation

One of the most important roles of Context Broker is to control context flow among all attached actors. In order to do that Context Broker has to know every Context Provider in the architecture. An announcement process can achieve it.

Too complicated device provisioning steps are not favorable from the adaptation point of view. The connection of the devices to the platform can be done through Device API where specific information about the device is required. Connection can be realized by provisioning the device itself, by provisioning a Configuration Group or both. If the device actuation is needed, registering IoT device should also be performed. In such a case, there are additional steps required before connecting device (Fiware-iot-stack.readthedocs.io (2018a)).

Learning & Evolution

Although there are tools for analysis of streaming data in Big Data Analysis Cosmos, which is one of proposals in FIWARE Catalogue (Catalogue.fiware.org. (2018d)), there is lack of machine learning algorithms applied to the operational behavior of the platform itself. Currently this area require some improvement and address common ML problems.

Monitoring Management & Adaptation

There is a generic enabler in FIWARE architecture responsible specifically for monitoring. Infrastructure used for this purpose contains of different components. First, there are probes responsible for gathering raw data. Then, there is a Collector, which forwards this data to NGSI adapter. NGSI Adapter is translating the data to common format. Then, there is a Context Broker where transformed monitoring data are published. There is also Connector, which mediates between Context Broker and storage. All collected data are storage in Hadoop. This approach provides the opportunity to get historical data for the specific device or even platform component via native Nagios API (Fiware-monitoring.readthedocs.io. (2018b)).

Monitoring GE is not dedicated to specific framework for gathering data. The owner of the infrastructure decides which tool should be installed. On the other hand, there are more examples for Nagios usage than any other tool in the documentation of FIWARE platform. Nagios is an application, which is ready for monitoring industrial data.

From SEMIOTICS point of view this kind of monitoring can be not be sufficient. There is lack of adaptive aspects on global level (of Context Broker or another) in FIWARE approach. This project can be a great opportunity to fill this gap.

End-to-end Security

One of the SEMIoTISc objectives is security by design. FIWARE claims to provide secure by design architecture and few of generic enablers mentioned earlier (Identity Management GE, Authorization PDP and

PEP Proxy) are used by application in runtime as it stands in documentation (Forge.fiware.org. (2018b)). From the perspective of the project this is a crucial case to provide highest level of security in all possible scenarios.

Limitations & Opportunities

The generic character of this platform can be regarded as an advantage, because of wide horizontal of opportunities of possible usage. However, this approach can be also seen as a disadvantage, because FIWARE as a general-purpose solution is not so ready to use in scenarios dedicated to specific domain (e.g., IIoT, healthcare). Another limitation is scalability of the platform. According to literature (Soto 2017), there is one part of this solution, namely *IoT Agent*, which is not stable and is crushing when overload occurs (>1000 requests per second).

3.6 Other key products

Except from the main devices, networks, and platforms, also other key products can be necessary for a modern IoT ecosystem. These include products related to security protection and solutions for providing tamper resistant in devices including subscriber identification modules (SIM), trusted platform modules (TPM) and hardware security modules (HSM).

Many mobile IoT devices are now equipped with a subscriber identification module (SIM) – an integrated circuit that stores securely the international mobile subscriber identity (IMSI) number and the corresponding key (Palattella et al. 2016). This information is utilized for the subscriber's identification and authentication. However, the SIM data are hardcoded on the chip and cannot be altered. Thus, when the operator of a device is changed, the SIM card must be replaced with a relevant card containing the credentials of the new user.

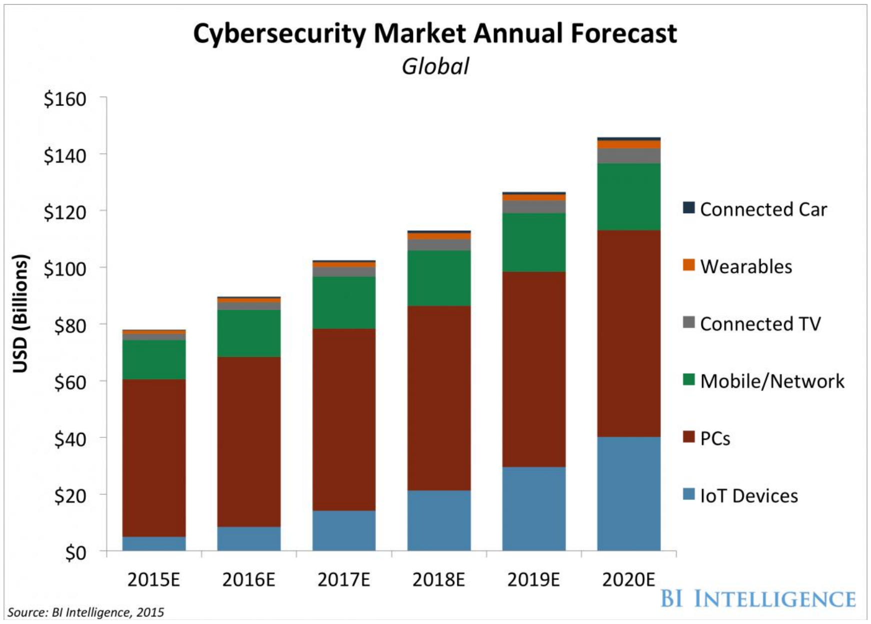
The embedded SIM (eSIM) card solution is proposed in the IoT domain in order to facilitate the M2M communication between devices (Park et al. 2017; Vesselkov et al. 2015). The eSIM module is re-programmable, enabling the remote provisioning of the operator subscription. It is, thus, a vital enabler for M2M connections allowing simple and seamless mobile connection of all types of communicating devices. The card comes in different sizes and shapes. In settings, where there is no need to swap cards, the chip is placed within a device and it is kept protected from heat, humidity, or extreme vibrations. Then, the owner updates the settings remotely when the operator changes, enhancing usability and the physical protection of the equipment. This is a fundamental requirement in several application domains, like precision agriculture, intelligent transportation, and industrial deployments (Hatzivasilis et al. 2017; Woo et al. 2015). Popular eSIM vendors include Gemalto (2015) and GSMA (2017). The provided interfaces support a mode of operation that is virtually identical with the current SIM personalization procedures of mobile operators. Another class of M2M SIM (Gemalto 2015; GSMA 2017) cards safeguards the identities of devices communicating on cellular networks and implements secure authentication and ciphering.

A *TPM c*onstitutes the international standard for secure crypto-processors (Chen et al. 2014). TPM is a dedicated microcontroller that protects cryptographic keys in hardware. It is placed on the motherboard and, once enabled; it provides full disk encryption and becomes the “root of trust” for the system, offering authentication and integrity to the boot procedure. TPM can lock/seal the hard drives until the system completes an authentication check or a system verification. It also includes a unique RSA key hardcoded on the chip that is utilized for asymmetric cryptography. Moreover, TPM can generate, maintain, and protect other keys which are utilized by cryptographic procedures. TPM is standardized by ISO/IEC 11889 (ISO/IEC 2015).

The *HSM* also protects and manages digital keys for strong authentication and offers crypto-processing functionality (Paverd and Martin 2012). In contrast to TPM that is embedded on the motherboard, HSMs are removable. HSMs are deployed as plug-in cards or external devices that are attached to the network server or a computing device. High performance modules are connected to the network using TCP/IP. HSMs are certified by international standards, like Common Criteria (ISO/IEC 15408 1996-2018).

3.7 IoT Security

According to Gartner, the IoT-enabled devices will exceed the 20.4bn by 2020 (Meulen 2017). These high volumes of interconnected devices constitute an increasingly attractive target for attackers. After the demonstration of several IoT vulnerabilities by researchers and their successful exploitation by attackers (e.g. smart vehicles (Woo et al. 2015) and smart lights (Ronen and Shamir 2016)), IoT security has now become an issue of high concern for the main Informatics stakeholders. The figure below depicts the forecasts for the cybersecurity market until 2020, as evaluated by the IoT security report of the Business Insider (Camhi 2015).



Source: BI Intelligence, 2015

Figure 20 Cybersecurity Market Annual Forecasts by Business Insider

Several methodologies and standards are established in order to assist the secure development of a system. Popular and widely used techniques for specifying security include the *Common Criteria Evaluation Methodology (CEM)* (ISO/IEC 15408 1996-2018) and the *Open Source Security Testing Methodology Manual* (ISECOM 1988-2918).

The three main cyber security principles for any type of security control are referred to as the *Confidentiality, Integrity, Availability (CIA) principles*. Confidentiality is the property where information is not disclosed to users, processes, or devices unless they have been authorized to access the information. Integrity is the property whereby information has not been modified or destroyed in an unauthorized manner. Availability is the property of being accessible. Each of these three principles involve relevant protection mechanisms, which are described in the following table, as they are derived from the abovementioned standards and related research efforts (Hatzivasilis et al. 2016).

Table 1 Security aspects and protectIon mechanisms

Aspect	Protection Mechanism	Description
Confidentiality	Confidentiality	Guarantees that a processed asset is not becoming known outside the interacting entities
	Authentication	Challenges credentials on the basis of identification and

		authorization
	Resilience	Preserves protection in case of failure
Integrity	Integrity	Guarantees that the interacting entities know when an asset has been changed
	Subjugation	Guarantees that transactions occur based on a defined process, removing freedom of choice and liability in the case of disclosure
	Nonrepudiation	Prevents the interacting entities from denying their role in an interaction
Availability	Continuity	Preserves interactivity in the case of failure
	Alarm	Informs that an interaction is happening or has happened
	Indemnification	Includes a contract between the asset owner and the interacting entity. It may also involve warnings as a precursor of legal action and public legislative protection

Surveys regarding security, architecture, and enabling technologies in the IoT domain are presented in (Lin et al. 2017; Andrea et al. 2015; Bekara 2014), while a taxonomy of the related security attacks is proposed in (Nawir et al. 2013). The guidelines for secure IoT development, as also suggested by large computer and software vendors (e.g., Microsoft, IBM, Siemens, Gemalto, etc.), include the following three security areas:

- *Device security*, i.e., mechanisms and techniques for protecting the device itself, once it is deployed in the field.
- *Connectivity security,* i.e., mechanisms and techniques for guarantying that the transmitted data between the IoT devices and the IoT Hub/Gateway is confidential and tamper-proof.
- *Cloud security,* i.e., mechanisms and techniques for safeguarding data while it is transmitted to, and is stored in the cloud.

Popular IoT platforms, like the Microsoft Azure IoT suite (Betts et al. 2018) and the IBM Watson IoT Platform (IBM 2018), tackle these issues and provide the mainstream security solutions, as we have described in Section 3.2 of this deliverable. In the following, we provide an overview of state-of-the-art IoT security grouped in under the three main areas listed above.

The next figure illustrates the SEMIOTICS architecture. At the bottom, semi-autonomous IoT devices, like sensors, collect field data and exchange information with the upper layers through a hub or a gateway. Connectivity from this end to the backend cloud services is served by SDN/NFV components that forward the data and administrate the traffic flows.

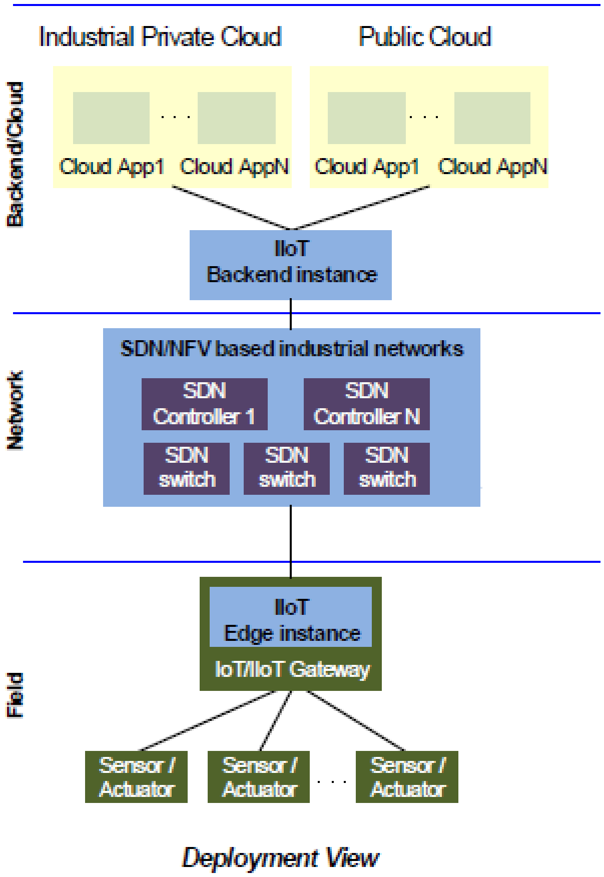


Figure 21 SEMIOTICS architecture and Deployment view

3.7.1 DEVICE SECURITY

Device security implements the different aspects for authenticating a device in an IoT application. Two main components are required for this purpose:

- A *unique identity key* or *security token* for each device. The device utilizes this key in order to authenticate and communicate with the IoT gateway.
- An *on-device X.509 certificate* and *private key* for authenticating the device to the IoT gateway. The authentication procedure must guarantee that this private key is not known outside the device at any time, thus achieving a higher level of protection.

In typical device operation, the device token provides authentication for each transaction that is made by the device to the IoT gateway. Thus, the symmetric key is associated to each transaction. The X.509-based procedure enables the authentication of the device at the physical layer during the establishment of the TLS connection (connectivity security). The certificate contains information that is related to the devices, like its ID, and other organizational details.

The security token can be also used alone, without requiring the X.509 authentication, but in a less secure setting. The choice between the two methods is determined by the availability of the adequate resources on the device end (e.g. store the private key securely) and the level of authentication security that is needed by the application.

3.7.2 CONNECTIVITY SECURITY

Connecting IoT devices over the Internet poses threats for data confidentiality and integrity. It is, thus, important to ensure that all the transmitted data between the devices and IoT gateways and from there to the cloud is encrypted.

The IoT gateway utilizes the security tokens to authenticate devices and services. The process is managed automatically by the IoT platforms. The seamless communication is supported by relevant protocols, such as the Advanced Message Queuing Protocol (AMQP), MQTT, and HTTP (Hatzivasilis et al. 2018), and is safeguarded by the security mechanisms that are implemented by each one of them. Nevertheless, these underlying solutions process the security tokens in different ways and the correct usage should be inspected in each specific case. This is a technical issue and concerns the correct mapping of the token-related information to each protocol’s data format. For example, the MQTT connection request utilizes the device ID in the username and the security token in the password field, while HTTP includes the valid token in the authorization request header. In addition, some application settings need the user to generate the security tokens and use them directly. Examples of these scenarios include the direct use of AMQP, MQTT, or HTTP surfaces.

The IoT gateway maintains an *identity registry* for the secure storage of device identities and security keys. Distinct devices or groups of them can be added to allow or block list, achieving complete control over device access. The high-level device provisioning includes the following steps:

- Associate an identifier at the physical device (i.e., the device identity and/or X.509 certificate) at the manufacturing or commissioning phases
- Create a relevant entry at the gateway’s identity registry
- Securely store the X.509 certificate thumbprint in the registry

On the other hand, the device must also authenticate the gateway. In the ordinary setting, a root certificate, which is included in the device software development kit SDK, is utilized for authenticating the gateway’s credentials. Although the root certificates are long-lived, they can also expire or be revoked. Thus, a secure procedure must be foreseen for updating the root certificate on the device end or, otherwise, the IoT devices may be subsequently unable to connect to the IoT gateway or the cloud services.

Finally, the Internet connection between the devices and the gateway is generally protected by the SSL/TLS 1.2 standards. Old versions of each protocol may also be supported for backward compatibility (i.e., TLS1.1, TLS 1.0).

3.7.3 CLOUD SECURITY

Cloud computing suffers from a number of security issues that overlooking them may lead to catastrophic consequences. As seen on (Jansen and Grance 2011; Fernandes et al. 2014) the main security vulnerabilities can be categorized as bellow

- Shared technologies: As seen in (Kocher et al. 2018; Lipp et al. 2018) attacker can exploit shared memory technologies to gain access to unauthorized content such as encryption keys
- Data breach: Personal data containing sensitive information such as credit card information can be lost or worse can be leaked.
- Account/service hijacking: If login credentials are lost or leaked, this can lead to attackers gaining access to critical areas of services and could potentially compromise confidentiality, integrity and availability.
- Denial of Service (DoS): As seen in (Deshmukh and Devadkar 2015) cloud infrastructure mechanisms cope with DoS attacks[2] by providing scaling up its resources but this firstly provides the

[2] https://readwrite.com/2016/10/22/the-internet-of-things-was-used-in-fridays-ddos-attack-pl4/

attacker with more resources to achieve his malicious goals and secondly can this type of attack can have monetary impacts.

- Malicious insiders: A company's employee can leverage his position to access sensitive information of the hosted services.

As a first line of defence to prevent the physical access attacks is obviously a high-level physical security at the data-centres. Furthermore, a scheme using XACML (OASIS 2005) can be used to limit access of employees to decrease the possibility of an insider attack.

To prevent side channel attacks as proposed in (Gruss et al. 2017) KAISER can be used in order to achieve kernel space isolation. Moreover, Intel trusted execution technology provides a trusted way of loading and executing the Virtual Machine Monitor (VMM) or the OS kernel has a serious limitation as described in (Wojtczuk and Rutkowska 2009) which is that the attacker can easily bypass it if he has physical access to the servers.

Hashizume et al. (2011) use misuse patterns to describe the environment, conditions and sequences of an attack based on co-residence between malicious and legitimate virtual machines. The misuse patterns act as a repository, which may then be used by developers for security measures against the attacks. In addition, Intrusion Detection Systems (IDS) that monitor and detect malicious activity in a system can be used to prevent intrusions. However due to the high complexity of the cloud a Hybrid Intrusion Detection System can be used (Rajendran et al. 2015).

To prevent data breaches and to guarantee data confidentiality and integrity on the channels and so prevent Sniffing and Spoofing Attacks the basic solution is to use an encrypted network protocol that encrypts all the traffic from the source to the destination over the whole trip. SSL and TLS can be used to prevent leakage of sensitive information through communication encryption. Another standard commonly used by CPs is IPsec, a protocol suite for securing IP communications implementing network-level authentication and encryption for each IP packet. Usually these mechanisms protect network traffic to the edge of the cloud network, VPN and its techniques as SSH and IPsec tunnels are used to defend traffic between servers within the cloud network.

3.7.4 CHALLENGES AND SEMIOTICS PROVISION

Establishing a secure IoT system is not a trivial task. Despite the evolution of the various technologies and platforms there are still open issues that must be considered during the design of a modern IoT application setting. These issues are summarised in the following.

Many IoT devices and sensory equipment have constrained computational and communicational capabilities. Therefore, the mainstream security solutions are not always applicable. Lightweight primitives must be installed, providing an adequate level of protection based on the inherited security perspectives of specific application domains. LWC is the main contributor in this design aspect (Manifavas et al. 2013). Compact and lightweight modules in hardware or software provide the main cryptographic functionality. Then, gateways that act as proxies ensure compatibility and uninterrupted communication between the end devices and the rest IoT infrastructure. SEMIOTICS also considers the constrained and heterogeneous nature of different IoT ecosystems, providing seamless operation and enhanced interoperability. IoT gateways will be installed in the field, collecting information from the constrained devices, like sensors, and facilitating the computational intensive communication to the upper layers (knowledge integration, mainstream cryptographic protocols, embedded machine learning, etc.).

Moreover, several IoT settings empower social relationships of users or underlying networking entities. In these cases, the trustworthiness of the different entities must be also established. Examples include resource sharing between the users, ad hoc routing of sensory devices, and service composition from various service providers. The diversity of devices and open connectivity makes it possible for malicious participants or compromised entities to exploit the various mechanisms and attack the system from inside. Reputation and trust-based computing evaluates the fair participation in order to detect and mitigate selfish or malicious behaviour (Hatzivasilis et al. 2017). Each entity's past behaviour is evaluated and misbehaviour is ranked negatively. These schemes act as an intrusion detection mechanism that try to discover known attack tactics.

Nevertheless, the trust schemes are then become the target of more sophisticated attacks. The hackers may remain undetected by performing collaborative attacks while keeping their trust levels slightly higher from the malicious detection threshold. Thus, anomaly detection techniques are suggested to further constrain the attackers' activities (Agrawal et al. 2015; Omar et al. 2013). ML is a promising choice (Omar et al. 2013). Initially, the ML scheme parses traces of normal and malicious traffic. Then, it processes incoming network data at runtime. If attacks or deviations of the normal state are detected, the system administrator is notified respectively. SEMIOTICS poses high research efforts towards the integration of ML and AI in the IoT domain, as well as tools and libraries for efficient mapping onto embedded resource constrained systems. The proposed solutions will not only facilitate the various IoT services but also enhance security at several system layers, ranging from embedded intelligence at the device end to business intelligence at the cloud. SEMIOTICS will develop specialized and lightweight algorithms for intelligent analysis to enable local semi-autonomous operation, tailored to the resources and constraints of field-level objects. It will also develop mechanisms to fuse local intelligence for enhanced intelligent behaviour at higher layers. Intelligence analytics will enable the detection and analysis of the effects of past adaptations. The adaptation mechanisms will be informed by monitoring and intelligence analytics, which will also provide the basis for accountability.

The integration of all these mechanisms from the device to the backend must be validated and the proper operation must be enforced. For these purpose, SEMIOTICS works towards the development of a pattern-based methodology that will verify that the adequate protection mechanisms are in place and operate according to the designed principles (Petroulakis et al. 2016). The proposed approach will evaluate the SPDI properties of each individual component and deduce the outcome of the finally composed system. The management service at the backend infrastructure will be capable not only to evaluate the SPDI features of the underlying system, but also to control and configure it based on SPDI goals and strategies in order to accomplish end-to-end protection and security-by-design.

3.8 IoT Privacy

3.8.1 PRIVATE DATA

In IoT applications, high volumes of personal data are exchanged by the underlying systems, rising serious concerns regarding privacy and deriving the application of relevant protection controls imperative for the end users. Therefore, several standards (like the ISO/IEC standards 27018 (ISO/IEC 2014) and 29100 (ISO/IEC 2011)) and regulation efforts (such as the General Data Protection Regulation of European Union – Regulation (EC) 2016/679 (European Parliament 2016)) are established, trying to tackle these issues.

This type of knowledge that is referred to a person is defined as Personal Identifiable Information (PII) (ISO/IEC 2011). The data may be categorized as personal sensitive, sensitive, and statistical (ISO/IEC 2011), with the first category demanding the highest privacy protection followed by the sensitive data, while statistical data requires moderate protection with such information becoming often publicly known via survey reports.

Moreover, three actuator types are defined, marshalling the ownership of personal data and the related processing rights (ISO/IEC 2011). The *PII principal/owner* is the person to whom the data is referred to and must have the total control and legal rights over the data. The *PII contracted processor* is the entity (e.g. person or service) that has been granted the explicit agreement of the PII principal for processing his/her personal data for a specific purpose. The processor is restricted and cannot use the data in a way that will trespass the common agreement with the principal. Nevertheless, in order to deliver the required functionality, the processor may need to disclose the PII to a *third party*. The processor has to obtain the explicit consent from the principal, with the corresponding processing terms and access rights also restricting the usage for the third party. For every violation, the contracted processor and the different third parties are accountable to the PII owner.

3.8.2 PROTECTION MECHANISMS

Privacy threats include malicious or non-malicious events that affect the protected PII (e.g. exploitation of connection vulnerabilities for smart home equipment (Apthorpe et al. 2016) or private data disclosure from wearable fitness tracking devices (Zhou and Piramuthu 2014). The private data must be protected during the transmission and storage operations. The aforementioned security mechanisms on the previous subsections are deployed for this purpose and ensure the CIA principles.

Nonetheless, there are other specific protection mechanisms for preserving privacy that safeguard the private data during the collection, access, and usage procedures. Typically, the PII owner must be always get informed about the collection of his/her personal data, the entities that can gain access to them, and how this information is going to be used.

The general privacy framework and properties are defined in ISO/IEC standards 27018 (ISO/IEC 2014) and 29100 (ISO/IEC 2011), and the General Data Protection Regulation of European Union – Regulation (EC) 2016/679 (European Parliament 2016). The next table summarizes the main privacy properties and the specialized protection mechanisms, as derived by these initiatives (Hatzivasilis et al. 2016).

Table 2 Privacy aspects and protecTion mechanisms

Aspect	**Protection Mechanism**	**Description**
Data Collection	Consent	Demands the PII owner's freely given, specific, and informed agreement to the processing of the PII. The PII must not be shared or disclosed to a third party without the owner's consent
	Opt-in	Includes a policy or process where the PII owner agrees explicitly to the PII's processing, before relevant consent
	Fairness	Guarantees that the PII is collected, used, or disclosed for only the appropriate purposes, implementing the GDPR features of collected data minimization and accuracy
Data Access	Identifiability	Results in identifying the PII owner, directly or indirectly, based on a given set of PII. It should include identifiability, pseudonymization, or anonymity
	Notification	Informs the PII owner that his/hers data are being collected
	Auditability	Provides adequate means to identify and control the access of PII data
	Challenge compliance (accountability)	Guarantees that the PII owner can hold the PII processors accountable for adhering to all privacy controls, supporting the GDPR properties for lawfulness, fairness, and transparency
Data Usage	Retention	Guarantees that the PII, which is no longer needed, is not maintained, as a precautionary measure towards the minimization of unauthorized collection, disclosure, or use.
	Disposal	Includes mechanisms for destroying or disposing of the PII on demand, including and the 'right to be forgotten' of GDPR
	Report	Informs that an interaction with PII is happening or has happened
	Break or incident	Manages a breach of PII

	response	

3.8.3 IDENTIFICATION AND ANONYMITY

The identification of the user is one of the main concerns of every privacy preserving strategy. An adversary may be able to correlate the exchange data with a specific person by integrating different sources of available information. In some cases, the user may wish to preserve his/her anonymity even from the service provider. Thus, the way that the user has access to an application is important for preserving privacy. In general, three types of user access can be implemented that are also determined by the functionality that is requested:

- An **authenticated user** must login the system and use the provided service using its own identity (real or virtual), for example in e-government services or social-media
- A user that access the system utilizing a **pseudonym**
- **Anonymous** usage

In the first case, the service provider knowns the user's identity and the system may intentionally or non-intentionally track the user's activity. The user is aware of this fact and participates with his/her own will. If this type of knowledge is available, it can be utilized not only by the provider but also by a third party or an attacker that will gain access to it. In such cases, the undesired effects need to be circumscribed by established security and privacy controls (e.g. store encrypted data in the database and minimize the pieces of personal information that has to be maintained).

When pseudonyms are utilized, the user cannot be tracked directly. This provides a higher privacy protection that is considered adequate for many applications. However, context knowledge can still make it possible to infer information about the user. For example, from service requests that are made by users that are located in a hospital, we can infer that these people are either employees, patients, or patients' companions. A user, that uses an IoT application service from the hospital almost every day, could also be identified as faculty stuff. If the same user also accesses the system frequently from another constantly used location, then we could deduce with a high probability that this other location is his/her home and from it try to figure out the true identity of the user and track back all the service activity to the specific person. Thus, extra protection mechanisms must be deployed as a defence measure, especially for the location-based services (LBS) that are usually provided by the different IoT settings (Chen et al. 2013).

The main defence strategies include *cloaking areas* (Buchanan et al. 2013) and *k-anonymity* (Moque et al. 2012; Yanaguchi et al. 2012). In cloaking areas, the users' mobile equipment deploys automatic procedures where the pseudonyms of different people are randomly interchanged when they are passing through a specified area. For example, in an IoT environment with smart cars the anonymization areas may be located in the traffic lights or in road crossing, where many cars are met and decrease their speed, allowing the identity change to take place. However, context knowledge can still be inferred (Niu et al. 2015). The effectiveness of this solution depends on the density of the anonymization areas and the volume of the participating users over time. The higher the density and the volume, the higher the protection. More advanced schemes are proposed to counter such attacks. Semantic obfuscation techniques intermix the data of semantically diverse domains and reduce the deduced amount of context knowledge (Ullah and Shah 2016). Other protection mechanisms can send dummy location data to the LBS provider instead of the accurate location (Sun et al. 2017). Also, the cloaking solution is only applicable to LBS or other services that involve the user's mobility.

With *k-anonymity*, an intermediate entity between the users and the service is responsible for blurring the identities of at least 'k' users with each other. The users may need to subscribe in this entity and access the functionality even through Internet, overcoming the locality restrictions of the cloaking areas. However, the entity must be considered as a trusted participant by the users' community. In other cases, the functionality can be implemented as a peer-to-peer service, running on the user's devices. On the other hand, this option demands the users' active participation and the willingness to consume their own resources for the community's benefit. Nevertheless, one main advantage of k-anonymity for system design is the fact that the protection level can be quantified and configured. Increasing the 'k' factor, enhances the privacy defence.

Combinatorial approaches of both cloaking areas and k-anonymity schemes are also suggested (Yu et al. 2016), taking advantage of the benefits from both approaches.

Anonymous participation requires threshold signature schemes (Alcaide et al. 2013). A community possess valid credentials to a service (i.e., crowdsourcing), which are then processed by the threshold scheme. Each community participant possesses a share of the common secret. In order to decrypt and authenticate the credentials, one would require at least *n* valid shares. Thus, users send their collected data to the service along with their shares. If the service achieves to authenticate the credentials of the group utilizing *n* shares, the data from these specific users are considered authenticated and are further processed. The user provides only partial knowledge to the data collector regarding the credentials of such a group. The collector trusts and processes the data, while the unlink ability with the contributor's identity is retained. These schemes can be centralized, decentralized, or hybrid. The protection level can be configured by changing the *n* parameter of the threshold scheme. One main security concern is the fact that the community signing key dealers must be honest and trustworthy.

On the other hand, anonymous privacy-preserving techniques restrict popular business operations for e-commerce and targeted marketing. Thus, attribute-based credentials (ABC) are proposed as a mean to protect privacy and provide the adequate information to the service provider (Alpar et al. 2016). In ABC, a cryptographic container stores attribute-related data, similarly with an X.509 certificate. The container is issued by a trusted authority and bounds the ABC owner to a secret key. The user can show only his/her attributes and prove that they are signed by the authority. The selective disclosure feature enables the user to send only an arbitrary attribute subset, like his/hers purchase level that determines discounts or other advantages. As the proof is based on zero-knowledge, the service provider does not learn the secret key of the user. Moreover, some ABC schemes offer multi-show unlinkability that prevent the service from correlating two different showings of the same user.

3.8.4 GENERAL DATA PROTECTION LEGISLATION (GDPR)

The development of new technologies, such as the IoT, has somewhat complicated the notion of "personal data" and led to the emergence of various types of data. In the EU, the concept of "personal data" is rather wide-ranging. The GDPR particularly expanded the definition of "data subject" to take account of the online environment and is referred to as:

"An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person" (GDPR, art 4(1)).

The fact that the definition refers to any information relating to an "identified or identifiable" individual basically means that it includes the name of a person, mobile phone number, e-mail, location, contacts, credit card and payment data, browsing history, pictures, videos, temperature, blood pressure, insulin level, etc.

Recital 30 of the GDPR elaborates on the issue as follows:

"Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as Internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them."

3.8.4.1 MAIN BUILDING BLOCKS OF "PERSONAL DATA"

Following the definition provided in EU data protection legislation, four main elements shall be met for data to qualify as "personal". Such elements have been detailed in an Opinion of the Article 29 Working Party (4/2007) of 20 June 2007 (Article 29, Data Protection Working Party). The four building blocks can be summarized as follows:

"any information": This phrase suggests a wide interpretation of the concept, regardless of the "nature" or "content" of the information, as well as the technical "format" in which the data is presented. More specifically, any type of information about an individual – be it objective or subjective – may be considered as personal data. As for the content, the European Court of Human Rights has established that the concept of private and family right (as enshrined in the European Convention on Human Rights (Article 8)) must be interpreted widely. Finally, as for the format of the information or the medium on which it is contained, the Article 29 Working Party confirms that the concept of personal data includes information available in whatever form.

"relating to": In order for information to qualify as "personal data", information must be about an individual, even if such link is not directly established. In its Opinion, the Article 29 Working Party considers that for data to "relate" to an individual, a "content" element, a "purpose" element or a "result" element should be present. The first element is fulfilled when the information is about an individual in the most obvious and common understanding of the word. The existence of the second element (purpose) will depend on whether the information is processed to "*evaluate, treat in certain way or influence the status or behavior of an individual*". Finally, the third element (result) exists when the processing of certain information has an impact on the person's rights and interests.

"an identified or identifiable": The Working Party affirms that an individual is "identified" when he/she can be distinguished from all other members of a group and is "identifiable" when, although the person has not yet been identified, it is possible to identify him/her. The Opinion details the hypotheses where a person is identifiable because "*information combined with other pieces of information (whether the latter is retained by the data controller or not) will allow the individual to be distinguished from others*".

"natural person": The protective legal regime provided in the EU applies to 'natural persons' universally, regardless of their country of residence.

3.8.4.2 SENSITIVE PERSONAL DATA

The GDPR also maintains the distinction between ordinary and special categories of personal data, also known as “sensitive data” (but added genetic and biometric data to the list of such data). The processing of such types of data is – similarly to what already applied under the Data Protection Directive – restricted and prohibited in most cases. Accordingly, in order to process such special categories of data, the data controller must find a proper legal ground exhaustively listed in the GDPR.

3.8.4.3 “PROCESSING” OF PERSONAL DATA

The GDPR will apply when there is a “processing” of personal data. The activities that are considered to constitute a ‘processing’ have not gone through any significant change within the GDPR, which maintains a very broad scope of application.

Accordingly, the GDPR will apply in case of “*any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction*”.

It goes without saying that IoT involving “personal data” necessarily implies that there is a processing within the meaning of the GDPR. Hence, the various principles and obligations set therein will need to be carefully assessed and complied with by the stakeholders involved.

3.8.4.4 ANONYMISATION AND PSEUDONYMIZATION OF PERSONAL DATA

Despite the relatively recent attention for the legal issues related to anonymization, including pseudonymization, the EU Data Protection Directive (95/46/EC) already addressed the subject of anonymization in 1995, putting the following rationale under Recital 26 (Julien Debussche and Benoit Van Asbroeck, 2015):

- The principles of data protection must apply to any information concerning an identified or identifiable person;

- To determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person;
- The principles of protection shall not apply to data rendered *anonymous* in such a way that the data subject is no longer identifiable.

Although this rationale provides some guidance, it is not sufficient to grasp exactly the legal significance of 'anonymization' and, in particular, pseudonymization. Therefore, we will first and foremost contextualize the main concepts of anonymization techniques as they are used in the legal environment.

Legal contextualization

It shall be noted that there is a discrepancy between the legal and technical definitions of anonymization, pseudonymization and encryption.

Anonymization is a process by which information is manipulated (concealed or hidden) to make it difficult to identify data subjects (Ohm, 2010). Common ways to achieve anonymization are deletion or omission of ‘identifying details’, or aggregation of information (Hon et. al, 2011).

Pseudonymization is defined by the GDPR as a technique of processing personal data in such a way that it can no longer be attributed to a specific individual without the use of additional information, which must be kept separately and subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person (GDPR, art 4(5)).

Encryption is a specific technique whereby plain text is changed into unintelligible code. It should not be confused with cryptography, often used interchangeably with encryption, which is the related science dealing with the technicalities of creating encrypted information (Perkins, 2005).

A major difference between the concepts discussed above relates to the goals of the techniques. The goal of anonymization is primarily to remove linking attributes and to avoid or impede the identification of individuals (Article 29, Data Protection Working Party). Pseudonymization and encryption, however, are not aimed at rendering a data subject unidentifiable, given that – at least in the hands of the data controller – the original data are either still available or deducible.

3.8.4.5 PRIVACY – COMPLIANCE OBLIGATIONS UNDER THE GDPR

The data protection principles are at the core of the processing of personal data. Many of them already existed under the Data Protection Directive, as transposed in the laws of the EU Member States, and are now reinforced in the GDPR. Article 5(1) of the GDPR lists the seven key principles relating to the processing of personal data. Article 5(2) provides for a general principle of "accountability", according to which the controller shall be responsible for, and able to demonstrate compliance with, the other six principles.

Those principals are:

1. **Lawfulness, fairness & transparency**
   Personal data must be processed lawfully, fairly, and in a transparent manner in relation to the data subject. The latter "transparency" requirement supplements what already existed in the Data Protection Directive.
2. **Purpose limitation**
   As was already the case under the Directive, personal data must be collected for specified, explicit and legitimate purposes; and must not be further processed in a way incompatible with those purposes.
3. **Data minimization**
   The general principle enshrined in Article 5(1)(c) of the GDPR provides that personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. Also, the period for which the data are stored should be limited to a strict minimum. Finally, personal data should only be processed if the purpose of the processing cannot be fulfilled by other means.

4. **Accuracy**
   Personal data must be accurate and, where necessary, kept up-to-date; every reasonable step must be taken to ensure that inaccurate personal data, having regard to the purposes for which they are processed, are erased or rectified without delay.
5. **Storage limitation**
   Personal data must be kept in a form, which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. Personal data may be stored for longer periods insofar as the data will be processed solely for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 83(1) and subject to implementation of appropriate technical and organizational measures.
6. **Integrity and confidentiality**
   Personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures (see below for further details on the security requirements).
7. **Accountability**
   Controllers are required to demonstrate compliance with the GDPR's principles, notably through the adoption of certain technical measures, the implementation of policies, the keeping of paper trails of decisions relating to data processing, the introduction of staff training programs, the performance of audits and impact assessments, or the adherence to approved codes of conduct. In this context, the GDPR imposes a risk-based approach (Article 29, Data Protection Working Party). Companies are therefore required to comprehend the likelihood and severity of the risk to the rights and freedoms of individuals, taking into consideration the nature, scope, context and purposes of the processing (Article 24 and Recital 76)[3]. The GDPR therefore considers the processing of personal data to be a risk for the rights and freedoms of individuals, which is why the data controller must carry out a continuous assessment of the risks.

3.8.4.6 Requirements under the GDPR

Each organization shall observe the legal obligations related to security and cyber-security. Such obligations not only derive from the GDPR, but also from other legislative instruments at both EU and national level. The advent of the (minimal harmonization) Network Information Security Directive has multiplied the requirements relating to security and cyber-security.

These obligations are however closely linked to those under the NIS Directive, examined below, and are in line with best practices applicable to information society systems that require adequate protection of assets.

Data Governance Obligations

Under the GDPR, any organization must implement a wide range of measures to reduce the risk of non-compliance with the GDPR and to prove that it takes data governance seriously. Such measures create significant operational obligations and costs.

A general obligation is imposed upon data controllers to adopt technical and organizational measures to meet the requirements set in the GDPR (and to be able to demonstrate that they have done so) (GDPR, Article 24). Operating a regular audit program, implementing privacy-by-design measures, running a Privacy Impact Assessment, appointing a Data Protection Officer, etc. are all measures considered to be in line with the data governance obligations, including the security-related requirements. Such measures must be reviewed and updated on a regular basis, taking into account the changing circumstances (GDPR, Article 24).

[3] See also in relation to the risk-based approach Articles 32(1) and 33 to 35

Security of Data Processing

Similarly to the Data Protection Directive, the GDPR requires data controllers and processors to "implement appropriate technical and organizational measures" (GDPR, Article 32).
Such measures shall take into account the following elements:

- State-of-the-art;
- Cost of implementation;
- Nature, scope, context and purposes of the processing; and
- Risk of varying likelihood and severity of the rights and freedoms of natural persons

GDPR goes further than the Data Protection Directive as it provides the following specificsuggestions for what types of security measures might be considered "appropriate to the risk":

- the pseudonymization and encryption of personal data;
- the ability to ensure the on-going confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

3.8.4.7 REQUIREMENTS UNDER THE NETWORK INFORMATION SECURITY DIRECTIVE

The NIS Directive, that was adopted on 6 July 2016 and entered into force in August 2016, imposes (online) security obligations on providers of two different types of services discussed hereunder: essential and digital services.

Essential Service

Article 5 of the NIS Directive defines an essential service as "*a service essential for the maintenance of critical societal and/or economic activities depending on network & information systems, an incident to which would have significant disruptive effects on the service provision*."

EU Member States have to identify the operators of essential services established on their territory by 27 months after entry into force of the Directive. Operators active in the following sectors may be included: energy, transport, banking, stock exchange, healthcare, utilities, and digital infrastructure (NIS Directive, Annex II).

When determining the significance of a disruptive effect in order to identify operators of essential services, the EU Member States must consider the following factors:

- the number of users relying on the service concerned;
- the dependency of (one of) the sectors mentioned above on the service concerned;
- the impact incidents could have on economic and societal activities or public safety;
- the market share of the entity concerned;
- the geographic spread of the area that could be affected by an incident;
- the importance of the entity to maintain a sufficient level of the service, taking into account the availability of alternative means for the provision of that service; and
- any other appropriate sector-specific factor (NIS Directive, art 6).

Digital Service

A digital service is described as "*any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services*" (NIS Directive, art 4(5)).

The NIS Directive covers three different types of digital services, which are defined as follows (NIS Directive, art 4(17)-(19)):

- **Online marketplace**: a digital service that allows consumers and/or traders to conclude online sales or service contracts with traders either on the online marketplace's website or on a trader's website that uses computing services provided by the online market place.
- **Online search engine**: a digital service that allows users to perform searches of, in principle, all websites or websites in a particular language on the basis of a query on any subject in the form of a keyword, phrase or other input, and returns links in which information related to the requested content can be found.
- **Cloud computing service**: a digital service that enables access to a scalable and elastic pool of shareable computing resources.

3.8.5 CHALLENGES AND SEMIOTICS PROVISION

The impact of IoT on privacy has been examined in several studies (e.g. (Caron et al. 2016; Xi and Ling 2016)) and various mitigation techniques are surveyed in (Tank et al. 2016). SEMIOTICS will comply with the current regulation and the data minimization principle (Abhik 2016). Efforts will focus on the preservation of user's rights from the data collection on the device to the information processing on the cloud and the big data analysis (Henze et al. 2016; Henze et al. 2014; Perera et al. 2015).

The different application settings may exhibit specialized privacy concerns (e.g. smart energy systems (Ukil et al. 2015), medical healthcare systems (Gong et al. 2015), and aggregated schemes for Fog computing (Lu et al. 2017)). SEMIOTICS will consider the intrinsic characteristics of the three demonstrated use cases, targeting the maximum privacy protection on the healthcare scenario.

IoT privacy challenges also include privacy-by-design (Porambage et al. 2016; Ziegeldorf et al. 2013) and end-to-end protection (Funke et al. 2016). Similarly with security, SEMIOTICS will tackle these issues based on the SPDI pattern approach.

3.9 IoT Dependability

From an industrial perspective, the IEC 60300 standard [IEC 2006] specifies the main features of dependability. The table below describes the core mechanisms for preserving dependability, as derived by the corresponding standard.

Table 3 Dependability aspects and proteciton mechanisms

Aspect	Protection Mechanism	Description
Safety	Prevention	Prevents faults from being integrated into the system via good development practices and implementation techniques
	Removal during development	Validates the system in order to detect and erase faults before the production phase
Reliability	Tolerance	Guarantees the required functionality's delivery in the presence of faults
	Performability	Guarantees how well the system will perform for a specified period in the presence of faults
	Survivability	Provides degraded but useful functionality that is acceptable by the users for a specified period in case of failure
Maintainability	Forecasting	Foresees possible faults in order to erase them or circumvent their effect

	Removal during use	Records and erases faults via the maintenance cycle, after the production phase

From a research perspective, a very detailed overview of dependability in general is given by [Avizienis et al. 2004]. Dependability considers the aspects of availability, reliability, safety, integrity, and maintainability, whereas security covers confidentiality, integrity, and availability. Thus, in terms of additional concepts, dependability adds reliability, safety, and maintainability. Reliability is defined as the continuity of correct service. Safety is the absence of catastrophic consequences on the user and the environment. Maintainability is the ability of a system to undergo modifications and repairs. Another important concept related to dependability are faults: a fault is the cause of an error, which in turn is something that cause a service to deviate from its correct behaviour. An example a fault in an offshore wind park is a controller failing due to lightning strike. Faults can be classified according to many different criteria:

- Phase of creation or occurrence: Developments faults occur during the development of a system. Operational faults occur during the operation of a system.
- System boundary: Internal faults have their cause within the system, whereas external faults originate outside of the system's boundary.
- Phenomenological cause: Natural faults are caused natural phenomena without explicit involvement of humans. Human-made faults are caused by humans.
- Dimension: Faults can be either software faults or hardware faults.
- Intent: Faults can be classified as either deliberate or non-deliberate. All-natural faults are considered to be non-deliberate.
- Objective: Faults can be either malicious or non-malicious. All malicious faults are deliberate.
- Capability: Accidental faults are introduced inadvertently. Incompetence faults are introduced due to a lack of skills and/or training.
- Persistence: Permanent faults have a defined starting point and last indefinitely unless countermeasures are taken. Transient faults have defined starting point and their duration is random or unpredictable.

Deliberate malicious faults in SEMIOTICS are covered in Section 3.6 on IoT security as they are in other words security issues.

At the field device level, most research on dependability is related to WSN, as dependability plays a particularly important role in harsh environmental conditions, with limited power supply and connectivity between nodes. A major research project in this field is RELYonIT (2012), a FP7 project funded by the European Union. RELYonIT created models for environmental factors, dependability requirements, and platforms, so that they then were able to select and parameterise protocols based on this data (Oppermann et al. 2015). In SEMIOTICS, in particular in the wind park use case, the effects of the environment on dependability of the system will also play a role. Furthermore, wind parks can be hard to reach physically, meaning that maintainability must be achieved via means of software only.

At the network layer, the relationship between dependability and SDNs has been investigated in research. Many features of SDNs benefit dependability, and in particular maintainability and reliability. However, as argued by Kreutz et al. (2013), security and dependability must be considered already in the design of SDNs, because SDNs are both an extremely promising evolution of networking architectures, and a dangerous increase in the threat surface. Thus, they naturally increase reliability since the network can recover from hardware failures (in some cases) by reconfiguring software. On the other side, reliability can also be reduced, if attacks on vulnerabilities in the software of SDN nodes cause them not to be available anymore. Another important concept to improve dependability is fault masking, i.e., the ability to seamless continue execution when a fault occurred (Pullum 2001). Finally, Fonseca et al. (2017) provide a very detailed overview of dependability-related issues in software-defined networks.

Dependability is also an important issue to consider in backend and cloud systems. Rosa et al. [Rosa et al. 2017] developed on-line prediction models for successful, failing, and evicted jobs in large data centers, e.g. Google data centres. Thus, dependability of cloud platforms can be increased by predicting the success probability of a task. Another important aspect is not failing jobs but failing components. In this case, the cloud system must recover and continue running the job on another (virtual) machine. This is called failover. Yang et al. (2017) developed a novel approach for rapid low-cost failover through a combination of hard state backup and soft state inference; they implemented their approach on Alibaba cloud platforms, demonstrating its real-life effectiveness. Another example of a cluster manager for cloud platforms is Borg, developed by Google. Verma et al. (2015) show how the system design is optimized towards quick fault recovery time and avoiding correlated failures, as examples of measures to improve dependability. They also deploy software-defined networking to allocate ports and IP addresses to Borg systems efficiently. In addition, an important cloud platform used in Infrastructure-as-a-service scenarios is OpenStack. Yuan et al. (2014) compared two techniques, bug analysis and fault injection, and how effective they are for improving dependability of the system. They show that bug analysis has the advantage of having richer features while fault injection yields results that are more precise.

3.10 IoT Interoperability

Interoperability is the ability of a system to work with or use the components of another system; “work” means the capabilities to perform a certain function in a shared and agreed way as, for example, by using same file format, exchanging information via a precisely defined protocol, or using a common encoding-decoding schema. It is easy enough to achieve interoperability of different systems within the same domain or between different implementations within the stack of a specific software vendor (Ganzha et al. 2016). In the current IoT ecosystems, the various devices and applications are installed and operate in their own platforms and clouds, but without adequate compatibility with products from different brands. For example, a smart watch developed in Android cannot interact with a smart bulb without the relevant proprietary gated application provided by the same vendor. Thus, islands of IoT functionality are established that lead towards an Intranet-of-Things rather than the Internet-of-Things. To take advantage of the full potential of the IoT vision we need standards to enable the horizontal and vertical communication, operation, and programming across devices and platforms, regardless their model or manufacturer.

Thus, from bottom-up, four levels of interoperability emerge:

- *Technological:* includes the seamless operation and cooperation of heterogeneous devices that utilize different communication protocols on the transmission layer (e.g. WiFi, ZigBee, 802.15.4).
- *Syntactic:* establishes clearly defined and agreed formats for data, interfaces, and encodings
- *Semantic:* settles commonly agreed information models and ontologies for the used terms that are processed by the interfaces or are included in the exchanged data.
- *Organizational:* cross-domain service integration and orchestration.

Technical, syntactic, and semantic interoperability enable horizontal compatibility between the involved technologies and platforms, while vertical operation is achieved through organizational interoperability. The next figure illustrates these four levels and the relevant state-of-the-art interoperability mechanisms in an IoT ecosystem. Details are provided in the following subsections. SEMIOTICS considers all interoperability scopes but it will focus on *syntactic and semantic* interoperability solutions for administrating services and applying pattern-based management strategies.

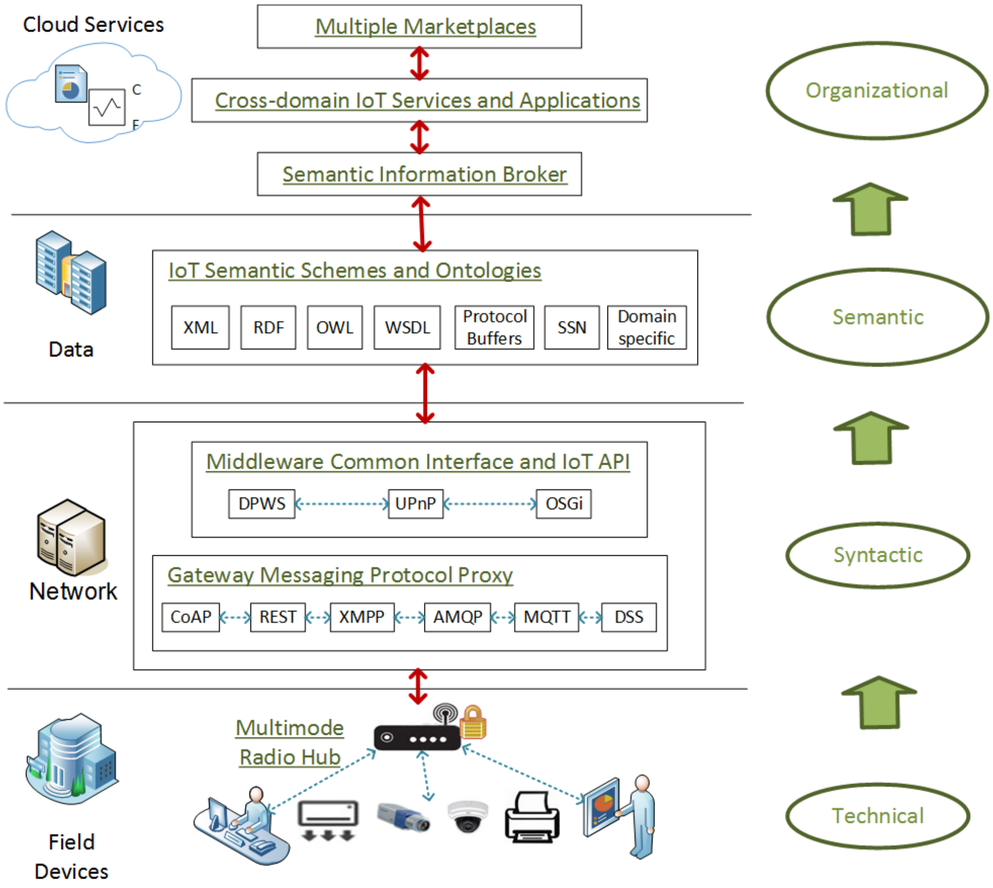


Figure 22 IoT Interoperability Concepts

3.10.1 TECHNOLOGICAL INTEROPERABILITY

Technological interoperability remains a significant barrier in IoT settings as up to 60% of the overall potential value is currently locked due to lack of compatible solutions (Manyika et al. 2015). Multimode radio equipment constitutes the main technical solution towards the integration of the various heterogeneous devices that utilize different networking and communication means.

Smart phones are a representative example. They deploy a cellular modem which supports 7 radio interfaces and enable the connection to GSM, CDMA, or LTE networks. Thus, a smart phone can operate with any cellular network and communicate with any other phone.

A similar approach can be followed in various IoT ecosystems, like a smart house. Home hubs, like routers and gateways, implement multimode radios and support various communication technologies (WiFi, Bluetooth, ZigBee, 802.15.4). These hubs act as bridges and provide the desired interoperable functionality. Thus, modern TVs and thermostats that use WiFi, speakers that communicate with Bluetooth, as well as switches and light bulbs that connect with ZigBee, can interact with each other, providing the user with flexible and convenient ways to interoperate with different smart home ecosystems. For example, a WiFi TV can communicate with ZigBee light bulbs through the home's multimode radio router. This setting can facilitate the installation and synchronization of new devices, and ease the connection to the network.

Once the devices are connected, most of the required interoperability functionality can be implemented in software. For instance, ZigBee can be developed in a networking stack if the devices support the 802.15.4 technology. Software solutions ease manufacturers to update their products, fix bugs, and add new features without requiring redesigning the underlying hardware. This capability addresses diversity and fragmentation, and can reduce replacement and management costs.

However, security issues may raise. Deploying multiple wireless technologies in a device can potentially expose more attack points where malicious entities could inject unauthorized code and sniff network traffic. The aforementioned hardware security protection mechanisms in the previous subsections, such as cryptographic protocols or secure boot and trusted environment execution, can safeguard the system and counter such attacks.

3.10.2 SYNTACTIC INTEROPERABILITY

IoT vendors utilize standardized and widely used technologies and platforms in order to broad the acceptance of their products. Popular solutions include the Devices Profile for Web Services (DPWS), Universal Plug and Play (UPnP), and OSGi, as well as the messaging protocols CoAP, eXtensible Messaging and Presence Protocol (XMPP), AMQP, MQTT, Protocol Buffer and Data Distribution Service (DDS).

However, these solutions offer only inter-domain compatibility and they usually act as closed silos with narrow application focus, imposing specific data formats and interfaces. Mechanisms for resolving these issues and achieving horizontal interoperability include common APIs between the different IoT middleware platforms (Broring et al. 2017) and gateway proxies for the messaging protocols (Al-Fuqaha et al. 2015) respectively.

A common and generic API is established by the EU funded project Big IoT (Broring et al. 2017). The API and the related information models are determined in cooperation with the Web of Things Interest Group at the W3C 8, enhancing the supported standards of this community. The API eases the development of software services and applications for different platforms.

A gateway messaging proxy is suggested in (Al-Fuqaha et al. 2015). The proposal automatically converts messages from one messaging protocol to the compatible format of another protocol. The functionality is offered among RESTful HTTP, CoAP, XMPP, MQTT, and DDS.

All these methods provide the main inter-domain interoperability features at the syntactic level. The devices can communicate seamlessly, but until this point, they cannot understand each other. Thus, additional mechanisms are required to represent and explicate the information semantics in a machine-interpretable format, as described in the following subsection.

3.10.3 SEMANTIC INTEROPERABILITY

IoT is considered as the successor of the Web. Thus, the semantic technologies that enable and facilitate the interoperability in web services are commonly adapted in the IoT domain. This includes widely-used and well-studied XML schemes like the RDF, RDFS, and OWL for ontologies, the WSDL for services, and the protocol buffers for serialized structured data. Such technologies offer common description and representation of data and services, characterize things and their capabilities, and deal with the semantic annotation, resource discovery, access management, and knowledge extraction in a machine-readable and interoperable manner.

Towards these goals, the most notable effort in the IoT field is the Semantic Sensor Network (SSN) ontology by the W3C community (Compton et al. 2012). It models two of the core IoT components: i) the sensors and ii) the sensor networks. The SSN ontology captures the sensor capabilities, usage environment, performance, and enabling contextual data discovery. This also constitutes the standardized ontology for the semantic sensor networks.

More specifically, the SSN ontology is a suite of general purpose ontologies. It embodies the following 10 conceptual modules:

- Device

- Process
- Data
- System
- Deployment
- PlatformSite
- SSOPlatform
- OperatingRestriction
- ContraintBlock
- And MeasuringCapability

The modules consist of 41 concepts and 39 object properties.

The general approach regarding the semantic interoperability that is followed by several IoT initiatives, like the EU funded project OpenIoT (Soldatos et al. 2015), is the usage of the SSN ontology as the semantic base. The ontology is then extended with the additional required concepts to model the targeted application scenarios. Such concepts usually include relevant standards and ontologies for specific application areas, like e-health (Cameron et al. 2015), and less often extensions at the sensor level (as the relevant SSN information is quite complete).

3.10.4 ORGANIZATIONAL INTEROPERABILITY

The common interpretation of semantic information in a globally shared ontology could be quite useful. However, this is not always the case. Although several local systems may utilize popular or standardized ontologies, eventually they extend them and establish their own semantics and interfaces. The direct interaction between these systems is not feasible. Thus, Semantic Information Brokers (SIB) are proposed (Kiljander et al. 2014) which correlate the required information, enabling the interoperability of systems with different semantics and cross-domain interaction.

Moreover, the abovementioned common API permits complex service composition and added value services. The API provide well-defined functionalities that can also implement interoperability on device-, fog-, and cloud-level. The main functionalities include: i) identity management and registration to resources, ii) resource discovery based on user-defined criteria, iii) access to data and meta-data (e.g. publish/subscribe of data streams), iv) command forwarding to things, v) vocabulary management of semantic information, vi) security management (key management, authentication, authorization, etc.), and vii) charging and billing management for using the provided assets.

The manufacturer's resources are advertised on the marketplace. Clients can discover the offered applications and gain access to them. In the near future, it is expected that there will be multiple marketplaces for IoT products (Broring et al. 2017). The marketplaces could be set for each application domain (e-health, smart home, etc.) or there could be multiple marketplaces for a single domain but set by different vendors.

As the developers comply with the defined interfaces, the marketplaces enhance the organizational interoperability. In cooperation with SIBs, the cross-domain IoT vision is further fostered. Thus, a modern IoT application can utilize services from different manufacturers and implement horizontal interoperable solutions that also utilize the three vertical interoperability layers, accomplishing seamless operation from the device end to the backend infrastructure.

3.10.5 CHALLENGES AND SEMIOTICS PROVISION

As aforementioned, SEMIOTICS concerns all four levels of interoperability, but the research efforts will focus on the semantic interoperability. The main goal is to establish interoperability patterns that will facilitate the modelling and real-time management of the underlying IoT ecosystem. SEMIOTICS will formally analyse the five main interoperability settings that are suggested by the related Big IoT project (Broring et al. 2017). These settings cover the compatibility issues for composing services from inter- to cross-domain topologies.

4 OPEN ISSUES

The review of IoT business value drivers and technology enablers have identified some key areas of focus of work in SEMIOTICS. These can be summarised as follows:

IoT Platforms: Existing platforms vary both in regards to the functional and non-functional capabilities that they offer and the ways in which they realise them. Important limitations relate to the absence of support for edge computing (and in particular close to sensors Artificial Intelligence including Machine Learning and Deep learning) and the varying degrees of support for analytics and learning capabilities, especially at the resource constrained embedded field/edge. Enhancements in both these areas constitute a key objective of SEMIOTICS. Furthermore, SEMIOTICS will develop mechanisms supporting the interoperability required for IoT applications that make use of devices and capabilities of different platforms.

Security: Establishing a secure IoT system is not a trivial task. Despite the evolution of the various technologies and platforms there are still open issues that must be considered during the design of a modern IoT application setting. Open issues relate to: (1) the constrained computational and communicational capabilities of many IoT devices and sensory equipment that makes mainstream security solutions not always applicable. Lightweight primitives must be installed, providing an adequate level of protection based on the inherited security perspectives of specific application domains; (2) the lack of comprehensive support in establishing the trustworthiness of users and components of IoT applications; (3) the concurrent handling of security at different layers (application, platform, infrastructure, device) that may leave holes or create incompatibilities making necessary the integration of all mechanisms at different levels (from the device to the backend) and the validation of the joint behaviour of these mechanisms to ensure a secure operation. For (1) SEMIOTICS will use LWC and make use of field IoT gateways facilitating the communication of information to the upper layers (knowledge integration, mainstream cryptographic protocols, embedded machine learning, etc.). For (2), SEMIOTICS will use ML to detect anomalies and indicators of non-trustworthy behaviour. This will be applied at several system layers, ranging from embedded intelligence at the device end to business intelligence at the cloud. For (3), SEMIOTICS will develop a pattern-based approach to verify that adequate protection mechanisms are in place and operate according to the designed principles.

Privacy: Whilst privacy preserving mechanisms are offered in existing IoT platforms the extent of the coverage of requirements arising from recent legislation (GDPR) is not clear. SEMIOTICS will investigate the relevant mechanisms and controls of the IoT platforms that it targets to establish the extent of their compliance with current regulation and the data minimization principles. This will cover user's rights from the data collection on the device to the information processing on the cloud and the big data analysis. It will also cover scenarios arising from the needs of different IoT applications, in the selected domains of the project. Finally, it will introduce a systematic privacy-by-design approach based on the concept of SPDI patterns.

Analytics and edge intelligence: Support for analytics varies in different IoT platforms, especially when it comes to field and edge devices. SEMIOTICS will develop specialized, resource constrained and lightweight algorithms for intelligent analysis to enable local semi-autonomous operation, tailored to the resources and constraints of field-level objects. It will also develop mechanisms to fuse local intelligence for enhanced intelligent behaviour at higher layers. Intelligence analytics will enable the detection and analysis of the effects of past adaptations. The adaptation mechanisms will be informed by monitoring and intelligence analytics, which will also provide the basis for accountability.

Interoperability: SEMIOTICS will focus on semantic interoperability. The main goal is to establish interoperability patterns that will facilitate the modelling and real-time management of the underlying IoT ecosystem. This will be based on formal analysis the five main interoperability settings suggested by the Big IoT project (Broring et al. 2017) in order to address interoperability and compatibility issues for composing services from inter- to cross-domain topologies.

5 CONCLUSIONS

This deliverable presented a review of the state-of-the-art of the technical landscape for developing IoT applications/systems and the key drivers that enable the creation of value out of them. To do so, the review covered common types of smart objects (i.e., devices, sensors and actuators) and IoT platforms that are available for developing IoT applications. It also covered key quality properties that need to be addressed in such applications including security, privacy, dependability, and interoperability.

The purpose of our review has been to help the consortium make informed decisions about the direction and priorities of the subsequent work, based on the current technological possibilities and challenges. The immediate direct use of this deliverable will be in producing the requirements specification for the SEMIOTICS framework, i.e., the usage requirements (D2.2) and the system requirements (D2.3) of the SEMIOTICS framework and in developing the high-level architecture of the SEMIOTICS framework (D2.4 and D2.5). In addition, the review of the technological capabilities documented in this deliverable will inform subsequent work in the consortium, particularly in the work packages WP3 (development of SEMIOTICS smart network and object capabilities), WP4 (development of SEMIOTICS security and privacy patterns and capabilities) and WP5 (system integration).

To facilitate this, this document identified existing capabilities, their maturity and open issues. The latter relate to IoT platform enhancements, IoT security and privacy and interoperability. The key strands of work for addressing issues in these areas have been summarised in Chapter 4.

6 REFERENCES

ABB Ability Smart Sensor 2018 - *ABB Advanced Services (ABB Service for Motors and Generators)*. Available at: http://new.abb.com/motors-generators/service/advanced-services/smart-sensor (Accessed: 23 March 2018).

Adame, T., Bel, A., Bellalta, B., Barcelo, J. and Oliver, M., 2014. IEEE 802.11 ah: the WiFi approach for M2M communications. *IEEE Wireless Communications*, *21*(6), pp.144-152.

Advanced 5G Network Infrastructure for the Future Internet Public Private Partnership in Horizon 2020 “Creating a Smart Ubiquitous Network for the Future Internet” (2017). [online] Available at: https://5g-ppp.eu/wp-content/uploads/2014/02/Advanced-5G-Network-Infrastructure-PPP-in-H2020_Final_November-2013.pdf [Accessed: 2 May 2018].

Akpakwu, G.A., Silva, B.J., Hancke, G.P. and Abu-Mahfouz, A.M., 2018. A survey on 5G networks for the internet of things: communication technologies and challenges. *IEEE Access*, *6*, pp.3619-3647.

Al-Fuqaha, A., Khreishah, A., Guizani, M., Rayes, A. and Mohammadi, M., 2015. Toward better horizontal integration among IoT services. IEEE Communications Magazine, IEEE, vol. 53, issue 9, pp. 72-79.

Alcaide, A., Palomar, E., Montero-Castillo, J. and Ribagorda, A., 2013. Anonymous authentication for privacy-preserving IoT target-driven applications, Computers & Security, Elsevier, vol. 37, issue September 2013, pp. 111-123.

Alpár, G., Batina, L., Batten, L., Moonsamy, V., Krasnova, A., Guellier, A. and Natgunanathan, I., 2016, May. New directions in IoT privacy using attribute-based authentication. In *Proceedings of the ACM International Conference on Computing Frontiers* (pp. 461-466). ACM

Amazon Web Services, Inc. (2018a). AWS IoT Core Overview - Amazon Web Services. [online] Available at: https://aws.amazon.com/iot-core/ [Accessed 22 Feb. 2018].

Amazon Web Services, Inc. (2018b). Machine Learning at AWS. [online] Available at: https://aws.amazon.com/machine-learning/ [Accessed 22 Feb. 2018].

Amazon Web Services, Inc. (2018c). AWS Lambda – Serverless Compute - Amazon Web Services. [online] Available at: https://aws.amazon.com/lambda/ [Accessed 15 Mar. 2018].

Amazon Web Services, Inc. (2018d). Amazon DynamoDB – NoSQL Cloud Database Service. [online] Available at: https://aws.amazon.com/dynamodb/ [Accessed 15 Mar. 2018].

Amazon Web Services, Inc. (2018e). Amazon Kinesis. [online] Available at: https://aws.amazon.com/kinesis/ [Accessed 15 Mar. 2018].

Amazon Web Services, Inc. (2018f). AWS IoT Core Features - Amazon Web Services. [online] Available at: https://aws.amazon.com/iot-core/features/ [Accessed 15 Mar. 2018].

Amazon Web Services, Inc. (2018g). Amazon CloudWatch - Cloud & Network Monitoring Services. [online] Available at: https://aws.amazon.com/cloudwatch [Accessed 15 Mar. 2018].

Amazon Web Services, Inc. (2018h). Amazon EC2. [online] Available at: https://aws.amazon.com/ec2/ [Accessed 15 Mar. 2018].

Amazon Web Services, Inc. (2018i). Amazon Elastic Block Store (EBS) – Block Storage for EC2 – Amazon Web Services (AWS). [online] Available at: https://aws.amazon.com/ebs/ [Accessed 15 Mar. 2018].

Amazon Web Services, Inc. (2018j). AWS | Elastic Load Balancing - Cloud Network Load Balancer. [online] Available at: https://aws.amazon.com/elasticloadbalancing/ [Accessed 15 Mar. 2018].

Amazon Web Services, Inc. (2018k). Amazon Relational Database Service (RDS) – AWS. [online] Available at: https://aws.amazon.com/rds/ [Accessed 15 Mar. 2018].

Amazon Web Services, Inc. (2018l). Introducing the Amazon Time Sync Service. [online] Available at: https://aws.amazon.com/about-aws/whats-new/2017/11/introducing-the-amazon-time-sync-service/ [Accessed 15 Mar. 2018].

Andrea, I., Chrysostomou, C. and Hadjichristofi, G., 2015. Internet of Things: security vulnerabilities and challenges, 3rd IEEE International Workshop on Smart City and Ubiquitous Computing Applications (ISCC), IEEE, 6-9 July, Larnaca, Cyprus, pp. 180-187.

Apthorpe, N., Reisman, D. and Feamster, N., 2016. A smart home is no castle: privacy vulnerabilities of encrypted IoT traffic, Workshop on Data and Algorithmic Transparency (DAT), New York, USA, 19 November.

Article 29 Data Protection Working Party, 'Opinion 4/2007 on the Concept of Personal Data' (2007) WP 136, Available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf

Article 29 Data Protection Working Party, 'Opinion 4/2007 on the Concept of Personal Data' (2007) WP 136, 29, Available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf

Article 29 Data Protection Working Party, 'Statement on the Role of a Risk-based Approach in Data Protection Legal Frameworks' (2014) WP218, Available at: http://ec.europa.eu/justice/data- protection/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf

Avizienis, Algirdas, et al. "Basic concepts and taxonomy of dependable and secure computing." IEEE transactions on dependable and secure computing 1.1 (2004): 11-33.

BACnet [online] Available at: http://www.bacnet.org/ [Accessed Feb. 18].

Bekara, C., 2014. Security issues and challenges for the IoT-based smart grid, International Workshop on Communicating Objects and Machine to Machine for Mission-Critical Applications (COMMCA), Procedia Computer Science, Elsevier, vol. 34, issue 2014, pp. 532-537.

Betts, D., Street, C. and Diogenes, Y., 2018. Internet of Things security architecture. Microsoft Azure documentation. Available on-line: https://docs.microsoft.com/en-us/azure/iot-suite/iot-security-architecture

Bluetooth.com. (2018). Protocol Specifications | Bluetooth Technology Website. [online] Available at: https://www.bluetooth.com/specifications/protocol-specifications [Accessed 15 Mar. 2018].

Boano, C.A., Brown, J., Keppitiyagama, C., Roedig, U., Römer, K., & Zuniga, M. (2014). TempLab: A testbed infrastructure to study the impact of temperature on wireless sensor networks. IPSN-14 Proceedings of the 13th International Symposium on Information Processing in Sensor Networks, 95-106.

Boano, C.A., Rmer, K. and Voigt, T., 2015. RELYonIT: dependability for the internet of things. *IEEE IoT Newsletter Januray*, *13*

Boyd, R. (2012). Getting Started with OAuth2.0. Sebastopol: O'Reilly.

Broring, A., Schmid, S., Schindhelm, C.-K., Kheli, A., Kabisch, S., Kramer, D., Phuoc, D., Mitic, J., Anicic, D. and Teniente, E., 2017. Enabling IoT ecosystems through platform interoperability. IEEE So ftware, IEEE, vol. 34, issue 1, pp. 54-61.

Buchanan, W. J., Kwecka, Z. and Ekonomou, E., 2013. A privacy preserving method using privacy enhancing techniques for location based services, Mobile Networks and Applications, vol. 18, issue 5, pp. 728-737.

Cache.industry.siemens.com (2018e) Architecture - Developer Documentation. Available at: https://developer.mindsphere.io/concepts/concept-architecture/index.html.

Cache.industry.siemens.com. (2018a). MindSphere documentation. [online] Available at: https://cache.industry.siemens.com/dl/files/613/109749613/att_931598/v1/MindSphere_072017_enUS.pdf

Cache.industry.siemens.com. (2018b). MindSphere Getting Started. [online] Available at: https://cache.industry.siemens.com/dl/files/499/109483499/att_937935/v1/201710_Manual_MindSphere_Getting Started_en.pdf_.pdf [Accessed 22 Feb. 2018].

Cache.industry.siemens.com. (2018c). [online] Available at: https://cache.industry.siemens.com/dl/files/170/109746170/att_927150/v1/MindSphere_MindConnectFB1500_GettingStarted.pdf [Accessed 19 Mar. 2018].

Cache.industry.siemens.com. (2018d). [online] Available at: https://cache.industry.siemens.com/dl/files/260/109742260/att_932160/v1/201709_Datasheet_MindAppFM_en.pdf [Accessed 19 Mar. 2018].

Cameron, J. D., Ramaprasad, A. and Syn T., 2015. An ontology of mHealth. 21st Americas Conference on Information Systems (AMCIS), Puerto Rico, pp. 1-11.

Camhi, J., 2015. The IoT Security Report: Securing new connected devices against cyber attacks, BI Intelligence, Business Insider.

Caron, X., Bosua, R., Maynard, S. B. and Ahmad, A., 2016. The Internet of Things (IoT) and its impact on individual privacy: an Australian perspective, Computer Law & Security Review, Elsevier, vol.32, issue 2016, pp. 4-15.

Catalogue.fiware.org. (2018a). FIWARE Catalogue. [online] Available at: https://catalogue.fiware.org [Accessed 26 Feb. 2018].

Catalogue.fiware.org. (2018b). IoT Discovery | FIWARE Catalogue. [online] Available at: https://catalogue.fiware.org/enablers/iot-discovery [Accessed 26 Feb. 2018].

Catalogue.fiware.org. (2018c). IoT Data Edge Consolidation GE - Cepheus | FIWARE Catalogue. [online] Available at: https://catalogue.fiware.org/enablers/iot-data-edge-consolidation-ge-cepheus [Accessed 14 Mar. 2018].

Catalogue.fiware.org. (2018d). BigData Analysis - Cosmos | FIWARE Catalogue. [online] Available at: https://catalogue.fiware.org/enablers/bigdata-analysis-cosmos [Accessed 15 Mar. 2018].

Chaudhuri, A., 2016. Internet of things data protection and privacy in the era of the General Data Protection Regulation. *Journal of Data Protection & Privacy*, *1*(1), pp.64-75 Agrawal, S. and Agrawal, J., 2015. Survey on anomaly detection using data mining techniques. Procedia Computer Science, Elsevier, vol. 60, issue 2015, pp. 708-713.

Chen, C., Raj, H., Saroiu, S. and Wolman, A., 2014. cTPM: a cloud TPM for cross-device trusted applications, 11th USENIX Symposium on Networked Systems Design and Implementation (NSDI), 2-4 April, Seattle, WA, USA, pp. 187-201.

Chen, Z., Xia, F., Huang, T., Bu, F. and Wang, H., 2013. A localization method for the Internet of Things, The Journal of Supercomputing, Springer, vol. 63, issue 3, pp. 657-674.

Compton, M. et al., 2012. The SSN Ontology of the W3C Semantic Sensor Network Incubator Group. Web Semantics: Science, Services and Agents on the World Wide Web, Elsevier, vol. 17, issue C, pp. 25-32.

CSIRO 2016, Advanced Manufacturing - A Roadmap for unlocking future growth opportunities for Australia, CSIRO Futures, form https://www.csiro.au/~/media/CABB4E555E7C4D4C986C4164FCC0214D.ashx

Debussche, J. and Asbroeck, B. Van (2015) ‘Computing and Privacy Series’, part 4, pp. 15–20. Available at: http://www.jus.uio.no/ifp/english/research/news-and-events/events/cloud-privacy-series-brochure_juliendebussche.pdf

Deshmukh, R. V. and Devadkar, K. K., 2015. Understanding DDoS attack & its effect in cloud environment. Procedia Computer Science. Elsevier Masson SAS, 49(1), pp. 202–210.European Parliament, 2016. Regulation (EU) 2016/679, European Union. Available on-line: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

DigiMesh [online] Available at: https://www.digi.com/products/digimesh [Accessed Feb. 18].

Docker. (2018). What is Docker?. [online] Available at: https://www.docker.com/what-docker [Accessed 15 Mar. 2018].

Docs.aws.amazon.com. (2018). Security and Identity for AWS IoT - AWS IoT. [online] Available at: https://docs.aws.amazon.com/iot/latest/developerguide/iot-security-identity.html [Accessed 22 Feb. 2018].

Docs.microsoft.com. (2018). Introduction to Azure Security. [online] Available at: https://docs.microsoft.com/en-us/azure/security/azure-security [Accessed 15 Mar. 2018].

Docs.microsoft.com. (2018). Whitepapers. [online] Available at: https://docs.microsoft.com/en-us/aspnet/whitepapers/overview#aspnet4 [Accessed 15 Mar. 2018].

Docs.microsoft.com. (2018a). Azure IoT Suite. [online] Available at: https://docs.microsoft.com/pl-pl/azure/includes/media/iot-security-ground-up/securing-iot-ground-up-fig3.png [Accessed 22 Feb. 2018].

Docs.microsoft.com. (2018b). What is Azure IoT Edge. [online] Available at: https://docs.microsoft.com/en-us/azure/iot-edge/how-iot-edge-works [Accessed 22 Feb. 2018].

Docs.microsoft.com. (2018c). What is Machine Learning on Azure?. [online] Available at: https://docs.microsoft.com/en-us/azure/machine-learning/studio/what-is-machine-learning [Accessed 22 Feb. 2018].

Download.microsoft.com. (2018). Microsoft Azure IoT Reference Architecture. [online] Available at: http://download.microsoft.com/download/A/4/D/A4DAD253-BC21-41D3-B9D9-87D2AE6F0719/Microsoft_Azure_IoT_Reference_Architecture.pdf [Accessed 22 Feb. 2018].

Enns, R., 2006. NETCONF configuration protocolRoman, R., Zhou, J. and Lopez, J., 2013. On the features and challenges of security and privacy in distributed internet of things. Computer Networks, 57(10), pp.2266-2279.

European Parliament, 2016. Regulation (EU) 2016/679, European Union. Available on-line: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

Fernandes, D. A. B. et al., 2014. Security issues in cloud environments: a survey. International Journal of Information Security, 13(2), pp. 113–170.

FIWARE For Industry. (2018). FIWARE Technologies enabling Industry 4.0. [online] Available at: http://www.fiware4industry.com/ [Accessed 26 Feb. 2018].

Fiware-iot-stack.readthedocs.io. (2018a). FIWARE-IOT-Stack. [online] Available at: http://fiware-iot-stack.readthedocs.io [Accessed 21 Feb. 2018].

Fiware-monitoring.readthedocs.io. (2018b). Installation & Administration Guide — FIWARE Monitoring. [online] Available at: http://fiware-monitoring.readthedocs.io/en/develop/manuals/admin/index.html [Accessed 28 Feb. 2018].

Fluke Condition Monitoring. [online] Available at: https://connect.fluke.com/en/condition-monitoring?trck=condition-monitoring [Accessed on 23 March 2018]

Fonseca, P.C.d.R., Souza Mota, E., 2017. A Survey on Fault Management in Software-Defined Networks. IEEE Communications Surveys & Tutorials, Vol. 19, No. 4, pages 2284-2321

Forge.fiware.org. (2018a). Internet of Things (IoT) Services Enablement Architecture - FIWARE Forge Wiki. [online] Available at: https://forge.fiware.org/plugins/mediawiki/wiki/fiware/index.php/Internet_of_Things_(IoT)_Services_Enablement_Architecture [Accessed 21 Feb. 2018].

Forge.fiware.org. (2018b). Security Architecture - FIWARE Forge Wiki. [online] Available at: https://forge.fiware.org/plugins/mediawiki/wiki/fiware/index.php/Security_Architecture [Accessed 21 Feb. 2018].

Forge.fiware.org. (2018c). FI-WARE Security - FIWARE Forge Wiki. [online] Available at: https://forge.fiware.org/plugins/mediawiki/wiki/fiware/index.php/Security [Accessed 15 Mar. 2018].

Funke, S., Daubert, J., Wiesmaier, A., Kikiras, P. and Muehlhaeuser, M., 2015. End-2-End privacy architecture for IoT, IEEE Conference on Communications and Network Security (CNS), IEEE, Florence, Italy, 28-30 September, pp. 1-3.

Future Internet Public Private Partnership (FI-PPP). [online] Available at: http://www.fi-ppp.eu [Accessed 7 Mar. 2018].

Ganzha, M., Paprzycki, M., Pawlowsji, W., Szmeja, P. and Wasielewska, K., 2016. Semantic technologies for the IoT – an Inter-IoT perspective. 1st International Conference on the Internet-of-Things Design and Implementation (IoTDI), IEEE, Berlin, Germany, pp. 271-276.

GDPR, art 24

GDPR, art 24(1)

GDPR, art 32

GDPR, art 4(1)

GDPR, art 4(5)

Gemalto, 2015. Cellular connectivity management solution for consumer electronics devices, Gemalto documentation. Available on-line: https://www.gemalto.com/brochures-site/download-site/Documents/tel-ce-cellular-connectivity.pdf

Gong, T., Huang, H., Li, P., Zhang, K. and Jiang, H., 2015. A medical healthcare system for privacy protection based on IoT, 7th International Symposium on Parallel Architectures, Algorithms and Programming (PAAP), IEEE, Nanjing, China, 12-14 December.

Gruss, D. et al., 2017. KASLR is dead: Long live KASLR. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 10379 LNCS, pp. 161–176.

GSMA-NB-IoT 2018 [online] Available at: https://www.gsma.com/iot/narrow-band-internet-of-things-nb-iot/ [Accessed Feb. 2018].

GSMA, 2017. The importance of embedded SIM certification to scale the Internet of Things, GSMA documentation, pp. 1-12. Available on-line: https://www.gsma.com/iot//wp-content/uploads/2017/02/1038-FM-GSMA-Test-Cert-eBook-V6.pdf

Harris III, A.F., Khanna, V., Tuncay, G., Want, R. and Kravets, R., 2016. Bluetooth low energy in dense IoT environments. *IEEE Communications Magazine*, *54*(12), pp.30-36 Aaron Perkins, 'Encryption Use: Law and Anarchy on the Digital Frontier [comments]' (2005) 41(5) Houston Law Review 1628

Hashizume, K., Yoshioka, N. and Fernandez, E. B., 2011. Three Misuse Patterns for Cloud Computing. Security Engineering for Cloud Computing, pp. 36–53.

Hatzivasilis, G., Fysarakis, K., Soultatos, O., Askoxylakis, I., Papaefstathiou, I. and Demetriou, G., 2018. The Industrial Internet of Things 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.

Hatzivasilis, G., Papaefstathiou, I. and Manifavas, C., 2016. Software security, privacy and dependability: metrics and measurement. IEEE Software, IEEE, vol. 33, issue 4, pp. 46-54.

Hatzivasilis, G., Papaefstathiou, I. and Manifavas, C., 2017. SCOTRES: secure routing for IoT and CPS. IEEE Internet of Things (IoT) Journal, IEEE, vol. 4, issue 6, pp. 2129-2141.

Henze, M., Hermerschmidt, L. Kerpen, D., Haubling, R., Rumpe, B. and Wehrle, K., 2016. A comprehensive approach to privacy in the cloud-based Internet of Things, Future Generation Computer Systems, Elsevier, vol. 56, issue March 2016, pp. 701-718.

Henze, M., Hermerschmidt, L. Kerpen, D., Haubling, R., Rumpe, B. and Wehrle, K., 2014. User-driven privacy enforcement for cloud-based services in the Internet of Things, International Conference on Future Internet of Things and Cloud (FiCloud), IEEE, Barcelona, Spain, 27-29 August, pp. 1-6.

IBM 2016, Evolution of the API economy, from https://www-01.ibm.com/events/wwe/grp/grp308.nsf/vLookupPDFs/Evolution%20of%20API%20economy%20/$file/Evolution%20of%20API%20economy%20.pdf

IBM, 2018. About Watson IoT Platform. IBM Cloud Docs. Available on-line: https://console.bluemix.net/docs/services/IoT/iotplatform_overview.html#about_iotplatform

IEC 60300, 2006. International Standards on Dependability, IEC. Available on-line: https://webstore.iec.ch/preview/info_iec60300-1%7Bed3.0%7Den.pdf

Indoor Positioning with UWB. [online] Available at: https://www.infsoft.com/technology/sensors/ultra-wideband [Accessed 23 March 2018]

ISECOM, 1988-2018. Open Source Security Testing Methodology Manual, ISECOM. Available on-line: www.isecom.org/research/osstmm.html

ISO/IEC 11889, 2015. Trusted platform module library, ISO/IEC. Available on-line: https://www.iso.org/standard/66510.html

ISO/IEC 15408, 1996-2018. Common Criteria for Information Technology Security Evaluation, ISO/IEC. Available on-line: www.commoncriteriaportal.org

ISO/IEC 27018, 2014. Code of Practice for Protection of Personally Identifiable Information (PII) in Public Clouds Acting as PII Processors, ISO/IEC. Available on-line: www.iso.org/iso/catalogue_detail?csnumber=61498

ISO/IEC 29100, 2011. Privacy Framework, ISO/IEC. Available on-line: https://www.iso.org/standard/45123.html

ITU, I., 2012. 9959: Short range narrow-band digital radiocommunication transceivers-PHY and MAC layer specifications. *Geneva, Switzerland: International Telecommunication Union*. Available at: https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-G.9959-201202-S!!PDF-E&type=items.

Jansen, W. and Grance, T., 2011. Guidelines on Security and Privacy in Public Cloud Computing. Director, 144(7), pp. 800–144.

Kiljander, J. et al., 2014. Semantic interoperability architecture for pervasive computing and Internet of Things. IEEE Access, IEEE, vol. 2, pp. 856-873.

Kocher, P. et al., 2018. Spectre Attacks: Exploiting Speculative Execution. Available at: http://arxiv.org/abs/1801.01203.

Kreutz, D., Ramos, F. M.V., Verissimo, P. (2013). Towards Secure and Dependable Software-Defined Networks. HotSDN’13, August 16, 2013, Hong Kong, China, pages 55-60

Kuan Hon and others, 'The Problem of 'Personal Data' in Cloud Computing - What Information is Regulated? The Cloud of Unknowing, Part 1' (2011) 1(4) IDPL 211, 214

Legal.apps.mindsphere.io. (2018). [online] Available at: https://legal.apps.mindsphere.io/legal/documents/documentsEN/MindSphere_MindApp_ManageMyMachines_datasheet_en.pdf [Accessed 19 Mar. 2018].

Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H. and Zhao, W., 2017. A survey of Internet of Things: architecture, enabling technologies, security and privacy, and applications, IEEE Internet of Things Journal, IEEE, vol. 4, no. 5, pp. 1125-1142.

Lipp, M. et al., 2018. Meltdown. Available at: http://arxiv.org/abs/1801.01207.

LTE-M description GSMA [online] Available at: https://www.gsma.com/iot/long-term-evolution-machine-type-communication-lte-mtc-cat-m1/ [Accessed Feb. 2018].

LTE-M description GSMA [online] Available at: https://www.gsma.com/iot/long-term-evolution-machine-type-communication-lte-mtc-cat-m1/ [Accessed Feb. 2018].

Lu, P., Heung, K., Lashkari, A. H. and Ghorbani, A. A., 2017. A lightweight privacy-preserving data aggregation scheme for Fog computing-enhanced IoT, IEEE Access, Special Section: Security and Privacy in Applications and Services for Future Internet of Things, IEEE, vol. 5, pp. 3302-3312.

M.G. Apte, "A Review of Demand Controlled Ventilation", In Proceedings of Healthy Building 2006, 16–19 April 2006, pp. 371–376.

Maharjan, S., 2010. RFID and IOT: An overview. Simula Research Laboratory University of Oslo.

Manifavas, C. et al., 2013. Lightweight cryptography for embedded systems – a comparative analysis. 6th International Workshop on Autonomous and Spontaneous Security (SETOP), Springer, LNCS, vol. 8247, pp. 333-349.

Manyika, J., Chui, M., Bisson, P., Woetzel, J., Dobbs, R., Bughin, J. and Aharon, D., 2015. Unlocking the potential of the Internet of Things. McKinsey Global Institute Report, McKinsey&Company, June 2015, pp. 1-4.

Martínez, R., Pastor, J., Álvarez, B. and Iborra, A. (2018). A Testbed to Evaluate the FIWARE-Based IoT Platform in the Domain of Precision Agriculture.

Massé, M. (2012). REST API design rulebook. Beijing: O'Reilly.

McKinsey 2015, The Internet of Things: Mapping the value beyond the Hype, McKinsey Global Institute, from: https://www.mckinsey.de/files/unlocking_the_potential_of_the_internet_of_things_full_report.pdf, pg. 6

Melton, J. (1996). SQL language summary. ACM Computing Surveys, 28(1), pp.141-143.

Meulen, R., 2017. Gartner says 8.4 billion connected “things” will be in use in 2017, up 31 percent from 2016, Gartner. Available on-line: https://www.gartner.com/newsroom/id/3598917

Modbus [online] Available at: www.modbus.org/ [Accessed Feb. 2018].

Moens, H. and De Turck, F. (2016). Customizable Function Chains: Managing Service Chain Variability in Hybrid NFV Networks. IEEE Transactions on Network and Service Management, 13(4), pp.711-724.

Moque, C., Pomares, A. and Gonzalez, R., 2012. AnonymousData.co: a proposal for interactive anonymization of electronic medical records, Procedia Technology, Elsevier, vol. 5, issue 2012, pp. 743-752.

Morabito, R., Cozzolino, V., Ding, A., Beijar, N. and Ott, J. (2018). Consolidate IoT Edge Computing with Lightweight Virtualization. IEEE Network, 32(1), pp.102-111.

Mqtt.org. (2018). Documentation | MQTT. [online] Available at: http://mqtt.org/documentation [Accessed 13 Mar. 2018].

N. Mangalvedhe, R. Ratasuk, and A. Ghosh (2016) NB-IoT deployment study for low power wide area cellular IoT, in Proc. IEEE 27th Annu. Int. Symp. Pers., Indoor, Mobile Radio Commun. (PIMRC), Sep. 2016, pp. 1–6.

Nawir, M., Amir, A., Yaakob, N. and Lynn, O. B., 2013. Internet of Things (IoT): taxonomy of security attacks, 3rd International Conference on Electronic Design (ICED), IEEE, Phuket, Thailand, 11-12 August 2016, pp. 321-326.

NEC. (2018). NEC Develops a FIWARE-based Fog Computing Framework for Edge-based IoT Services. [online] Available at: http://uk.nec.com/en_GB/press/201711/20171127_01.html [Accessed 26 Feb. 2018].

NIS Directive, Annex II

NIS Directive, art 4(5)

NIS Directive, art 6

NIS Directive, arts 4(17)-(19)

Niu, B., Zhu, X., Li, Q., Chen, J. and Li, H., 2015. A novel attack to spatial cloaking schemes in location-based services, Future Generation Computer Systems, Elsevier, vol. 49, issue 2015, pp. 125-132.

Omar, S., Ngadi, A. and Jebur, H. H., 2013. Machine learning techniques for anomaly detection: an overview. International Journalof Computer Applications, vol. 79,no. 2, pp. 33-41.

OPC Foundation (2018), *What is OPC?* [online] Available at: https://opcfoundation.org/about/what-is-opc/ [Accessed 15 Mar. 2018].

Open Network Operating System. [online] Available at: https://onosproject.org/features/ [Accessed Feb. 2018].

OpenFlow Switch Specification (2015). Available at: https://www.opennetworking.org/wp-content/uploads/2014/10/openflow-switch-v1.5.1.pdf [Accessed: Feb 2018].

OpenStack. (2018). Open source software for creating private and public clouds. [online] Available at: https://www.openstack.org/ [Accessed 7 Mar. 2018].

Oppermann, F. J., Boano, C. A. Zuniga, M.A., Römer , K. (2015). Automatic Protocol Configuration for Dependable Internet of Things Applications. Local Computer Networks Conference Workshops (LCN Workshops), 2015 IEEE 40th. Clearwater Beach, FL, USA.

Orbcomm Asset Tracking. [online] Available at:
https://www.orbcomm.com/en/hardware/devices?gclid=EAIaIQobChMI_-aJ1-Si2QIVGuAZCh0GEgwtEAAYASAAEgL5RfD_BwE [accessed 23 March 2018]

Palattella, M. R., Dohler, M., Grieco, A., Rizzo, G., Torsner, J., Engel, T. and Ladid, L., 2016. Internet of Things in the 5G era: enablers, architecture, and business models. IEEE Journal on Selected Areas in Communications, IEEE, vol. 34, no. 3, pp. 510-527.

Park, J., Lee, J. and Lee, K., 2017. Method for changing MNO in embedded SIM on basis of dynamic key generation and embedded SIM and recording medium therefor, US Patent, US Grant US9775024B2, KT Corp.

Paul Ohm, 'Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization' (2010) 57 UCLA Law Review 1701, 1707

Paverd, A. J. and Martin, A. P., 2012. Hardware security for device authentication in the smart grid, International Workshop on Smart Grid Security (SmartGridSec), Springer, LNCS, col. 7823, pp. 72-84

Perera, C., Ranjan, R., Wang, L., Khan, S. U. and Zomaya, A. Y., 2015. Big data privacy in the Internet of Things era, IT Professional, IEEE, vol. 17, issue 3, pp. 32-39.

Petroulakis, N., Spanoudakis, G. and Askoxylakis, I., 2016. Patterns for the design of secure and dependable software defined networks, Computer Networks, Elsevier, vol 109, issue 1, pp. 39-49.

Philips LED lighting. [online] Available at: http://www.lighting.philips.co.uk/systems/lighting-systems/greenwarehouse [accessed 23 March 2018]

Pipeline Fiber Optic Strain Sensors. [online] Available at: https://www.azosensors.com/article.aspx?ArticleID=602 [accessed 23 March 2018]

Platform Overview - OpenDaylight. [Online]. Available: https://www.opendaylight.org/what-we-do/odl-platform-overview. [Accessed: Feb. 2018].

Porambage, P., Ylianttila, M., Schmitt, C., Kumar, P., Gurtov, A. and Vasilakos, A. V., 2016. The quest for privacy in the Internet of Things, IEEE Cloud Computing, IEEE, vol. 3, issue 2, pp. 36-45.

Pullum, L. L., 2001. Software Fault Tolerance Techniques and Implementation. Artech House, Norwood, Massachusetts, USA

PWC 2016, Industry 4.0: Building the digital enterprise, from: https://www.pwc.nl/en/industries/industrial-manufacturing.html, page 9

Rajendran, P. K., Muthukumar, B. and Nagarajan, G., 2015. Hybrid intrusion detection system for private cloud: A systematic approach. Procedia Computer Science. Elsevier Masson SAS, 48(C), pp. 325–329.

Raschellà, A., Bouhafs, F., Deepak, G.C. and Mackay, M., 2017. QoS aware radio access technology selection framework in heterogeneous networks using SDN. *Journal of Communications and Networks*, *19*(6), pp.577-586.

Raschellà, A., Bouhafs, F., Deepak, G.C. and Mackay, M., 2017. QoS aware radio access technology selection framework in heterogeneous networks using SDN. *Journal of Communications and Networks*, *19*(6), pp.577-586.

Ronen, E. and Shamir, A., 2016. Extended functionality attack on IoT devices: The case of smart lights, IEEE European Symposium on Security and Privacy (EuroS&P), IEEE, Saarbrucken, Germany, 21-24 March 2016.

Rosa, A., Chen, L., Binder, W. (2017). Failure Analysis and Prediction for Big-Data Systems. IEEE Transactions on Services Computing (Volume: 10, Issue: 6, Nov.-Dec. 1 2017), pages 984-998

Sans.org. (2018). [online] Available at: https://www.sans.org/reading-room/whitepapers/authentication/ssl-tls-whats-hood-34297 [Accessed 15 Mar. 2018].

Sans.org. (2018). [online] Available at: https://www.sans.org/reading-room/whitepapers/authentication/ssl-tls-whats-hood-34297 [Accessed 15 Mar. 2018].

Siemens Acvatix. [online] Available at: https://www.siemens.com/global/en/home/products/buildings/hvac/valves-actuators.html. [accessed on 23 March 2018]

Siemens Building solutions. [online] Available at:http://w3.usa.siemens.com/buildingtechnologies/us/en/building-automation-and-energy-management/sensors/Pages/sensors.aspx [accessed 23 March 2018]

SIMATIC IOT2000. [online] Available at: http://w3.siemens.com/mcms/pc-based-automation/en/industrial-iot/Pages/Default.aspx [accessed 23 March 2018]

SIMATIC RF. [online] Available at: http://w3.siemens.com/mcms/identification-systems/en/rfid-systems/transponders/pages/default.aspx [accessed 23 March 2018]

Smart EVO CO2 . [online] Available at: http://www.smartgas.eu/en/ [accessed 23 March 2018]

Soldatos, J. et al., 2015. OpenIoT: Open source Internet-of-Things in the Cloud. Interoperability and Open-Source Solutions for the Internet of Things, Springer, LNCS, vol. 9001, pp. 13-25.

Soto V., 2017, PERFORMANCE EVALUATION OF SCALABLE AND DISTRIBUTED IOT PLATFORMS FOR SMART REGIONS, Luleå University of TechnologyAvaiable at: https://ltu.diva-portal.org/smash/get/diva2:1136272/FULLTEXT01.pdf

Standard, O.A.S.I.S., 2005. extensible access control markup language (xacml) version 2.0. *2008. http://docs. oasis—open. or~/xacmmL2. 0/access_ control-xacml-2. 0 — core· spec—OS. pa1*

Sun, G., Chang, V., Ramachandran, M., Sun, Z., Li, G., Yu, H. and Liao, D., 2017. Efficient location privacy algorithm for Internet of Things (IoT) services and applications, Journal of Network and Computer Applications, Elsevier, vol. 89, issue 2017, pp. 3-13.

Support.industry.siemens.com. (2018). SIOS. [online] Available at: https://support.industry.siemens.com/cs/document/109483500/mindconnect-nano-–-quick-start-–-march-2017?dti=0&lc=en-DE [Accessed 15 Mar. 2018].

Tado Smart Thermostat. [online] Available at: https://www.tado.com/ [accessed 23 March 2018]

Tanaserri, N. (2017). Microservices with Azure. [online] Microserviceswithazure.com. Available at: https://microserviceswithazure.com/Namit.html [Accessed 15 Mar. 2018].

Tank Storage System. [online] Available at: http://www.documentation.emersonprocess.com/groups/public/documents/whitepaper/d352445x012.pdf [accessed 23 March 2018]

Tank, B., Upadhyay, H. and Patel, H., 2016, March. A survey on IoT privacy issues and mitigation techniques. In *Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies* (p. 2). ACM.

Tian, H. et al. (2015) 'Global patterns and controls of soil organic carbon dynamics as simulated by multiple terrestrial biosphere models: Current status and future directions', Global Biogeochemical Cycles, 29(6), pp. 775–792. doi: 10.1002/2014GB005021.

Toghraee, R. (2017). Learning OpenDaylight. Birmingham, UK: Packt Publishing.

Tools.ietf.org. (2018). RFC 4158 - Internet X.509 Public Key Infrastructure: Certification Path Building. [online] Available at: https://tools.ietf.org/html/rfc4158 [Accessed 15 Mar. 2018].

Tools.ietf.org. (2018). RFC 5246 - The Transport Layer Security (TLS) Protocol Version 1.2. [online] Available at: https://tools.ietf.org/html/rfc5246 [Accessed 13 Mar. 2018].

Ukil, A., Bandyopadhyay, S. and Pal, A., 2015. Privacy for IoT: involuntary privacy enablement for smart energy systems, IEEE International Conference on Communications (ICC), IEEE, London, UK, 8-12 June.

Ullah, I. and Shah, M. A., 2016. A novel model for preserving location privacy in Internet of Things, 22nd International Conference on Automation and Computing (ICAC), IEEE, 7-8 September, Colchester, UK, pp. 1-6.

VAF TT-Sense. [online] Available at: https://www.vaf.nl/products-solutions/overview/tt-sense-shaft-power-thrust-meter [accessed 23 March 2018]

Vanguard Wireless Gas Detector. [online] Available at:
http://www.ueonline.com/vanguard/index.html?gclid=EAIaIQobChMI0czMyZ-o2QIVBZPtCh0mQAeHEAAYASAAEgKXqvD_BwE [accessed 23 March 2018]

Verma, A., Pedrosa, L., Korupolu, M., Oppenheimer, D., Tune, E. and Wilkes, J., 2015, April. Large-scale cluster management at Google with Borg. In *Proceedings of the Tenth European Conference on Computer Systems* (p. 18). ACM

Vesselkov, A., Hammainen, H. and Ikalainen, P., 2015, November. Value networks of embedded SIM-based remote subscription management. In *Telecommunication, Media and Internet Techno-Economics (CTTE), 2015 Conference of* (pp. 1-7). IEEE.

Vishwesh, J. and Rajashekar, M. (2017). Internet of Things (IoT): Security Analysis & Security Protocol CoAP. International Journal of Recent Trends in Engineering and Research, [online] 3(3), pp.417-425. Available at: http://www.ijrter.com/papers/volume-3/issue-3/internet-of-things-iot-security-analysis-security-protocol-coap.pdf.

Wojtczuk, R. and Rutkowska, J., 2009. Attacking Intel Trusted Execution Technology. Bios, pp. 1–6. Available at:http://www.intel.com/content/dam/www/public/us/en/documents/white-papers/trusted-execution-technology-security-paper.pdf%5Cnhttp://digitalpiglet.org/teaching/stonybrook/CSE509.2012.F/Attacking.Intel.TXT-slides.pdf.

Woo, S., Jo, H. J. and Lee, D. H., 2015. A practical wireless attack on the connected car and security protocol fir in-vehicle CAN, IEEE Transactions on Intelligent Transportation Systems, IEEE, vol. 16, issue 2, pp. 993-1006.

Xi, W. and Ling, L., 2016. Research on IoT privacy security risks, International Industrial Informatics – Computing Technology, Intelligent Technology, Industrial Information Integration (ICIICII), IEEE, Wuhan, China, 3-4 December.

Yamaguchi, R. S., Hirota, K., Hamada, K. and Takahashi, K., 2012. Applicability of existing anonymization methods to large location history data in urban travel, IEEE International Conference on Systems, Man, and Cybernetics, IEEE, 14-17 October, COEX, Seoul, Korea, pp. 997-1004.

Yang, R., Zhang, Y., Garraghan, P., Feng, Y., Ouyang, J., Xu, J., Zhang, Z., Li, C. (2017) Reliable Computing Service in Massive-Scale Systems through Rapid Low-Cost Failover. IEEE Transactions on Services Computing (Volume: 10, Issue: 6, Nov.-Dec. 1 2017), pages 969-983

Yu, R., Bai, Z., Yang, L., Wang, P., Move, O. A. and Liu, Y., 2016. A location cloaking algorithm based on combinatorial optimization for location-based services in 5G networks, IEEE Access, Special Section on Green Communications and Networking for 5G Wireless, IEEE, vol. 4, issue 2016, pp. 6515-6527.

Yuan, X., Li, Y., Wu, Z., Liu, T., 2014. Dependability Analysis on OpenStack IaaS Cloud: Bug Analysis and Fault Injection. 6th International Conference on Cloud Computing Technology and Science. IEEE, pages 18-25

Z-Wave (2018) [online] Available at: www.z-wave.com/ [Accessed Feb. 2018].

Zhao, K. and Ge, L., 2013, December. A survey on the internet of things security. In Computational Intelligence and Security (CIS), 2013 9th International Conference on (pp. 663-667). IEEE.

Zhou, W. and Piramuthu, S., 2014. Security/privacy of wearable fitness tracking IoT devices, 9th Iberian Conference on Information Systems and Technologies (CISTI), IEEE, Barcelona, Spain, 18-21 June, pp. 1-6.

Ziegeldorf, J. H., Morchon, O. G. and Wehrle, K., 2013. Privacy in the Internet of Things: threats and challenges, SITRANS IIoT. [online] Available at: https://www.siemens.com/global/en/home/products/automation/process-instrumentation.html [accessed 23 March 2018]

Zigbee.org. (2018). White Papers | Zigbee Alliance. [online] Available at: http://www.zigbee.org/zigbeealliance/white-papers/ [Accessed 15 Mar. 2018].