CHAPTER 1

The Internet of Things: Definitions, Key Concepts, and Reference Architectures

Theo Lynn, Patricia Takako Endo, Andrea Maria N. C. Ribeiro, Gibson B. N. Barbosa, and Pierangelo Rosati

Abstract This chapter introduces the Internet of Things (IoT) and presents definitions and a general framework for conceptualising IoT. Key concepts and enabling technologies are summarised followed by a synthesis and discussion of the current state-of-the-art in IoT Reference Architectures.

Keywords Internet of things • IoT • IoT Reference Architecture

T. Lynn • P. Rosati
Irish Institute of Digital Business, DCU Business School, Dublin, Ireland
e-mail: theo.lynn@dcu.ie; pierangelo.rosati@dcu.ie

P. T. Endo
Irish Institute of Digital Business, Dublin City University, Dublin, Ireland

Universidade de Pernambuco, Recife, Brazil
e-mail: patricia.endo@upe.br

Andrea Maria N. C. Ribeiro • G. B. N. Barbosa (✉)
Universidade Federal de Pernambuco, Recife, Brazil
e-mail: andrea.maria@gprt.ufpe.br; gibson.nunes@gprt.ufpe.br

T. Lynn et al. (eds.), *The Cloud-to-Thing Continuum*, Palgrave Studies in Digital Business & Enabling Technologies,
https://doi.org/10.1007/978-3-030-41110-7_1

1.1 Introduction

The Internet has evolved in a series of waves (Cisco 2012). The first three waves were device-centric. In the first wave, we went to a device, typically a desktop PC, to access the Internet. As mobile computing evolved, soon we brought our own devices with us and could access the Internet anywhere anytime. Today, we are in the midst of the so-called Internet of Things (IoT) where devices (things) are connected to the Internet and each other. These things comprise a multitude of heterogeneous devices ranging from consumer devices, such as mobile phones and wearables, to industrial sensors and actuators. Gartner (2017) estimated only 8.4 billion things were connected in 2017 representing just over 0.5% of the total estimated connectable physical objects worldwide.

This objective of this chapter is to introduce readers to the Internet of Things. The remainder of the chapter is organised as follows. First, we will explore perspectives on the definition of the Internet of Things (IoT) followed by key constructs and concepts underlying IoT including a general research framework for conceptualising IoT. Then, we will delve into a further level of granularity and present a selection of IoT Reference Architectures before concluding.

1.2 Defining the Internet of Things

The Internet of Things (IoT) has rapidly grown in prominence in the last ten years and, yet, it means different things to different people. Indeed Whitmore et al. (2015) note that there is no universal definition of IoT. Two main conceptualisations exist—the technical and socio-technical perspectives. The first, the pure technical perspective, views IoT as an assemblage and ecosystem of technical artefacts. It is defined by reference to these artefacts and their capabilities. These range in detail. For example, Weyrich and Ebert 2016, p. 1) define IoT as being "*[…] about innovative functionality and better productivity by seamlessly connecting devices.*" In contrast, Tarkoma and Katasonov (2011, p. 2) is significantly more detailed defining IoT as a "*global network and service infrastructure of variable density and connectivity with self-configuring capabilities based on standard and interoperable protocols and formats [which] consists of heterogeneous things that have identities, physical and virtual attributes, and are seamlessly and securely integrated into the Internet.*" Similarly, Whitmore et al. (2015, p. 1) define the IoT as "*a paradigm where everyday objects can* *be equipped with identifying, sensing, networking and processing capabilities that will allow them to communicate with one another and with other devices and services over the Internet to achieve some objective.*" Unsurprisingly, given the nature of these definitions, they dominate Computer Science literature.

The socio-technical perspective of IoT recognises not only the technical artefacts but also the associate actors and processes with which the IoT interacts. For example, Haller et al. (2009) recognises the role of the connected objects as active participants in business processes. They define the IoT as "*a world where physical objects are seamlessly integrated into the information network, and where the physical objects can become active participants in business processes. Services are available to interact with these 'smart objects' over the Internet, query their state and any information associated with them, taking into account security and privacy issues*" (Haller et al. 2009, p. 15). Shin (2014, p. 25) argues that the IoT is part of "*wider, socio-technical systems, comprising humans, human activity, spaces, artefacts, tools and technologies.*" Indeed, Shin et al. note that in some instances, a biological entity may, in fact, be considered the connected thing, for example a human with a heart monitor implant or a farm animal with a biochip transponder.

This perspective taken in this book is not particularly concerned with a specific IoT-related definition or problem. Figure 1.1 below presents a

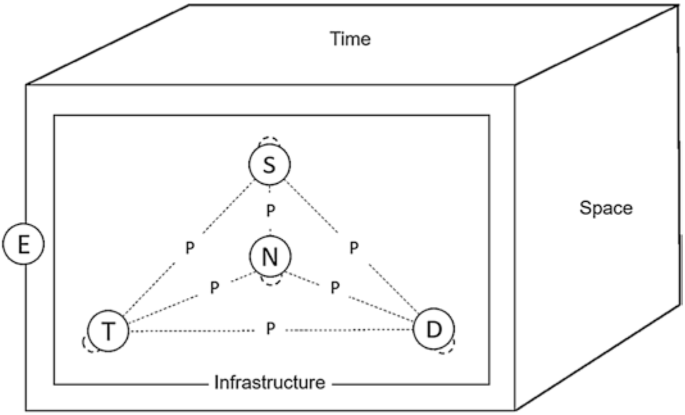

Fig. 1.1 A general framework for conceptualising big data research in the Internet of Things

general research framework for conceptualising IoT research. It is general in that it is capable of being used to understand IoT related problems and research questions in conjunction with widely accepted levels of generalisation (abstraction) in both the social sciences (nano, micro, meso, macro) and computer sciences (computation, algorithmic/representational, physical/implementation). Furthermore, it provides a sufficiently general abstraction of the IoT in that it facilitates sense making without getting in to a non-generalisable level of granularity.

In this framework, five core entities are identified and defined—social actors, things, data, networks, and events. Each of these entities has a myriad of characteristics that may change and evolve over time and inflect our understanding of how value can be generated and captured at different units of analysis:

- *Social Actors (S)*, while typically human, need not be; the framework is flexible enough to accommodate the emerging concept of computers as social actors (Lynn et al. 2015; Zhao 2003).
- *Things (T)* are primarily physical however they may also be virtual and exist in augmented and/or virtual reality. Two key functional requirements of things in IoT and IoE are data sensing (collating data) and network connectivity.
- *Data (D)* here are discrete artefacts that can connect to other entities including other data and may be sourced from first party, second party, or third party sources. It recognises the existence of an IoT data chain. For example, Radio frequency identification (RFID) enables the tracking of objects through an electronic product code (EPC) serving serves as a link to data about the object that can queried over the Internet (Haller et al. 2009).
- *Networks (N)* are systems of interconnected entities and are both conduits and entities in themselves. Our framework accommodates networks between different types of IoT entities and those of the same type, for example machine-to-machine (M2M) networks.
- *Events (E)* are occurrences of interest at given time and/or physical or virtual space.
- *Processes (P)* are obviously critical to how entities interoperate in the IoT and comprise general (e.g. communication) and domain-specific processes. They are essential to how value is created, captured, and delivered in the IoT.

All entities and processes take place in an infrastructural setting and the framework recognises that in the IoT, additional data and metadata is created and collated at the infrastructural level. For example, depending on the networking, processing, and storage capabilities of a given device, these activities may be centralised (in the cloud), at the edge (at the device), or in an intermediary layer (the fog) and not only store or process this data but also may extract other hardware, software, functional use, or other ambient data that can provide different and/or new insights. Finally, each IoT use case is situated in space (physical or virtual) and time and it is against this context that different types of events occur and impact the IoT.

As the IoT can be explored from numerous perspectives, we argue that such a research framework can play an important role for researchers to make sense of a complex and dynamic environment and isolate the major constituents of the IoT experience. In addition, the proposed framework can be used as a general-purpose scaffold for crafting research agendas on the IoT and avoiding duplicated and unfocussed research endeavours.

1.3 Key Concepts and Constructs

IoT revolves around a number key concepts and enabling technologies including object (thing) identification (e.g. IPv6), information sensing (e.g. RFID, sensors, GPS, etc.), communications technologies for data exchange, and network integration technologies (Shin 2014).

It is important to note that legacy computing and telecommunications architectures were not designed with the IoT in mind. The scale of heterogeneous devices and an unprecedented volume, variety and velocity of data combined with an extreme variation in use context require new paradigms in computing. Depending on the use case and service level requirements, IoT devices may require processing and storage locally, in the cloud or somewhere in between. In addition cloud computing, edge, fog, and dew computing are three new computing paradigms designed to support IoT. While beyond the scope of this chapter, it is useful to be aware of these concepts and technologies when consider the architectures in Sect. 1.4. Table 1.1 provides a brief definition for technology.

Table 1.1 Definitions of key technologies in IoT

Construct	*Definition*
Cloud computing	A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction (Mell and Grance 2011, p. 2).
Dew computing	Dew computing is an on-premises computer software-hardware organisation paradigm in the cloud computing environment where the on-premises computer provides functionality that is independent of cloud services and is also collaborative with cloud services (Wang 2016).
Edge computing	Edge computing is the network layer encompassing the end devices and their users, to provide, for example, local computing capability on a sensor, metering or some other devices that are network-accessible (adapted from Iorga et al. 2017).
Fog computing	Fog computing is a layered model for enabling ubiquitous access to a shared continuum of scalable computing resources. The model facilitates the deployment of distributed, latency-aware applications and services, and consists of fog nodes (physical or virtual), residing between smart end-devices and centralised (cloud) services (adapted from Iorga et al. 2017).
IPv6	Internet Protocol version 6 (IPv6) is the most recent version of the Internet Protocol (IP). It is an identification and location system for computers on networks and routes traffic across the Internet. It dramatically expands the addressing space (IPv6 2003) thus facilitating the identification of smart objects.
Machine-to-machine communication (M2M)	M2M communication technologies provide capabilities for devices to communicate with each other through wired and wireless systems (Tsai et al. 2012, p. 1).
Radio frequency identification (RFID)	RFID is a form of automatic identification and data capture (AIDC) technology that uses electric or magnetic fields at radio frequencies to transmit information. Each object that needs to be identified has a small object known as an RFID tag affixed to it or embedded within it. The tag has a unique identifier and may optionally hold additional information about the object. Devices known as RFID readers wirelessly communicate with the tags to identify the item connected to each tag and possibly read or update additional information stored on the tag. This communication can occur without optical line of sight and over greater distances than other AIDC technologies (Karygiannis et al. 2007, p. ES-1).
Wireless sensor and actuator networks (WSAN)	WSANs are networks of large numbers of minimal capacity sensing, computing, and communicating devices and various types of actuators (Stankovic 2008).

1.4 IoT Reference Architectures

IoT devices are being used in a wide range of domains such as health, agriculture, smart cities, and process automation. The 'things' used can be characterised by their heterogeneity in terms of computing resources (processing, memory, and storage), network connectivity (communication protocols and standards) and software development (high degree of distribution, parallelisation, dynamicity). While such heterogeneity enables the depth and breadth of applications and use cases, it also introduces complexity, particularly with respect to expected service level requirements, for example, user and device mobility, software dependability, high availability, scenario dynamicity, and scalability. As such, an abstraction layer to promote interoperability amongst IoT devices is needed. However, lack of standardisation means that such interoperability is lacking (Cavalcante et al. 2015). Reference Architectures can help IoT software developers to understand, compare, and evaluate different IoT solutions following a uniform practice.

Several Reference Architectures have been proposed in order to standardise concepts and implementation of IoT systems in different domains. Breivold (2017), for instance, conducted a comparative study with eleven different Reference Architectures. This chapter focuses on the those Reference Architectures that enable IoT integration with cloud computing and/or fog and edge computing i.e. across the cloud to thing (C2T) continuum. Figure 1.2 shows the timeline containing the main Reference Architectures that support IoT across the C2T continuum, namely IoT Architectural Reference Model (IoT ARM), IEEE P2413 (IEEE P2413 2014), Industrial Internet Reference Architecture (IIRA) (Lin et al. 2019), WSO2 IRA, Intel SAS, Azure IRA, and SAT-IoT.

Each of the architectures below can be explored through the lens of the framework presented in Sect. 1.2 and embodies the key concepts and constructs discussed in Sect. 1.3.

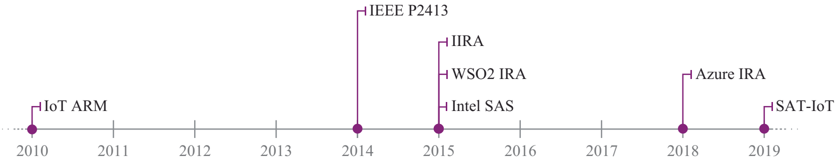

Fig. 1.2 Timeline of selected IoT Reference Architectures

1.4.1 *Internet of Things Architectural Reference Model (IoT ARM)*

The IoT-A project (IoT-A 2019) groups the specificities of IoT functionalities and defines the IoT Architectural Reference Model (IoT ARM) to support the usage, the development and the analysis of different IoT systems, from communication to service level.

According to Bauer et al. (2013), the main contributions of the IoT ARM are twofold: (a) the Reference Model itself, which contains a common understanding of the IoT domain and definitions of the main IoT entities and their basic relationships and interactions; and (b) the Reference Architecture *per se*, which provides views and perspectives to generate IoT architectures adapted to one's specific requirements. This way, the Reference Model and the Reference Architecture provide abstraction levels (models, views and perspectives) to derive concrete IoT solutions (i.e. IoT ARM compliant IoT architectures and systems) (Fig. 1.3).

The Reference Architecture is independent from a specific use-case or application and includes three views: (a) functional, (b) information, and (c) deployment and operation. The functional view describes the function components of a system; these include components' responsibilities, default functions, interfaces, and interactions. The architecture is composed of five longitudinal functionality groups (FGs), namely service organisation, IoT process management, virtual entity, IoT services, communication, and two transversal FGs, namely management and security.

The information view covers the information life cycle in the IoT system, providing an overview of the information structures and flows (i.e. how information is defined, structured, exchanged, processed, and stored), and the list of the components involved in the process.

Lastly, the deployment and operation view has an important role in the realisation of IoT systems as they are bringing together a number of devices, each of which has different resources and connection interfaces, which can be interconnected in numerous ways. The deployment and

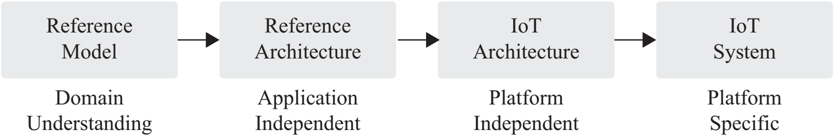

Fig. 1.3 Derivation from each IOT ARM step

operation view provides a set of guidelines for system design, covering different aspects of technologies, communication protocols, services, resources, and information storage.

According to Bauer et al. (2013), evolution and interoperability, availability and resilience, trust, security and privacy, and performance and scalability are the most important for perspectives for IoT systems.

Bauer et al. (2013) also present a reverse mapping to demonstrate how the concepts of the IoT ARM can be presented to existing architectures and to validate their proposal. One of the use cases was based on the use of RFID for tracing the towels before, during, and after the surgery to avoid towels being left on the patient's abdomen. This use case was also based on the use of a cloud infrastructure for data storing. Even though the authors argue that the IoT ARM mapping was successfully done, there is no way to say that it can be applied to any existing concrete architecture.

1.4.2 IEEE Standard for an Architectural Framework for the Internet of Things (P2413)

To avoid silos in domain-specific standards, P2413 is a unified architectural framework for IoT. As well as defining the framework, it includes descriptions of various IoT domains, definitions of IoT domain abstractions, and identification of commonalities between different IoT domains (energy, media, home, transport etc.). It provides a reference model that defines relationships among various IoT verticals and common architecture elements. In this way it has similar design principles to IoT ARM. The Reference Architecture covers the definition of basic architectural building blocks and their ability to be integrated into multi-tiered systems. The Reference Architecture also addresses how to document and mitigate architecture divergence. P2413 also includes a blueprint for data abstraction and addresses the need for trust through protection, security, privacy, and safety. Applying P2413, the architectural transparency of IoT systems can be improved to provide benchmarking, safety, and security assessments.

The P2413.1 is the Standard for a Reference Architecture for Smart City (RASC) (P2413.1 2019). The RASC provides an architectural design for the implementation of a smart city, enabling interaction and interoperability between domains and system components. The smart city applications may include water management, waste management, street lighting, smart parking, environmental monitoring, smart community, smart campus, smart buildings, e-health, e-government, etc. The RASC includes the Intelligent Operations Center (IoC) and IoT.

The P2413.2 is the Standard for a Reference Architecture for Power Distribution IoT (PDIoT) (P2413.2 2019). Following a similar idea of RASC, the PDIoT also provides an architectural design but for implementing power distribution systems, covering different domains, such as legacy grid systems, IoT and cloud computing. This standard defines a cloud based power distribution which supports microservices and migration from legacy systems to IoT based platforms.

1.4.3 Industrial Internet Reference Architecture (IIRA)

The term 'Industrial Internet' is largely attributed to General Electric (GE). In a joint report, Accenture and GE (2014, p. 7) define the industrial internet as an architecture that:

> *[…] enables companies to use sensors, software, machine-to-machine learning and other technologies to gather and analyse data from physical objects or other large data streams—and then use those analyses to manage operations and in some cases to offer new, value-added services.*

Today, the Industrial Internet has evolved in to the Industrial Internet of Things (IIoT). IIoT is defined Boyes et al. (2018, p. 3) as:

> *A system comprising networked smart objects, cyber-physical assets, associated generic information technologies and optional cloud or edge computing platforms, which enable real-time, intelligent, and autonomous access, collection, analysis, communications, and exchange of process, product and/or service information, within the industrial environment, so as to optimise overall production value.*

Somewhat like IoT ARM and P2413, the Industrial Internet Reference Architecture (IIRA) (Lin et al. 2019) is an architecture framework to develop interoperable IIoT systems for diverse applications across industrials verticals.

IIRA is composed of one frame and different representations (Fig. 1.4). According to (Lin et al. 2019), a frame is a collection of concepts represented by stakeholders (individual, team, organisation having interest in a

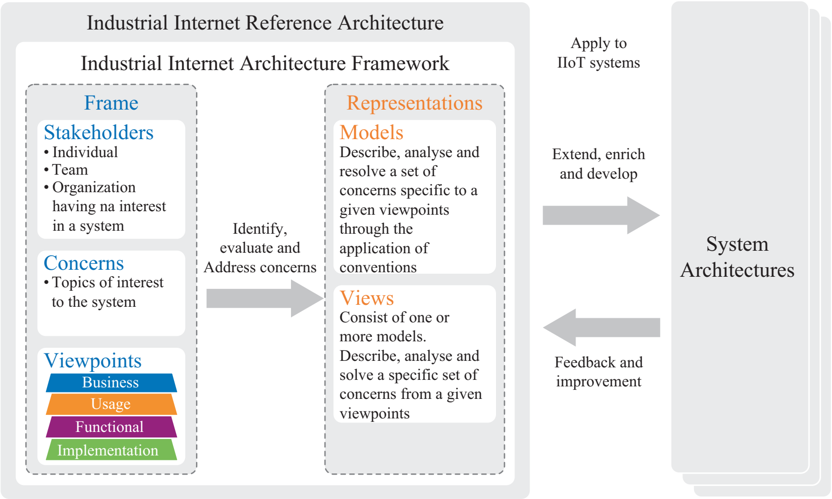
Industrial Internet Reference Architecture
Industrial Internet Architecture Framework
Frame
Stakeholders
• Individual
• Team
• Organization having na interest in a system
Concerns
• Topics of interest to the system
Viewpoints
Business
Usage
Functional
Implementation
Identify, evaluate and Address concerns
Representations
Models
Describe, analyse and resolve a set of concerns specific to a given viewpoints through the application of conventions
Views
Consist of one or more models. Describe, analyse and solve a specific set of concerns from a given viewpoints
Apply to IIoT systems
Extend, enrich and develop
Feedback and improvement
System Architectures

Fig. 1.4 Industrial internet Reference Architecture. (Adapted from Lin et al. 2019)

system), concerns (any topic of interest pertaining to the system), and viewpoints (conventions framing the description and analysis of specific system concerns). Representations are defined as views and models, which are collections of the results obtained through the application of the architecture frame to abstracted or concrete systems. These models and views are chosen for addressing a specific concern at an appropriate level of abstraction (Lin et al. 2019).

The IIRA identifies the main architectural concerns found in IIoT systems and classifies them into viewpoints related to their respective stakeholders. Viewpoints are critical components in the IIRA; there are four different viewpoints (Fig. 1.5). Firstly, the Business Viewpoint is responsible for inserting the vision, values, and objectives of business stakeholders in the commercial and regulatory context. Secondly, the Usage Viewpoint describes how an IIoT system realises its key capabilities, by providing the sequence of activities that coordinates the system components. Thirdly, the Functional Viewpoint relates the functional and structural capabilities of an IIoT system and its components. It is decomposed into five main functional domains: control domain, operation domain,

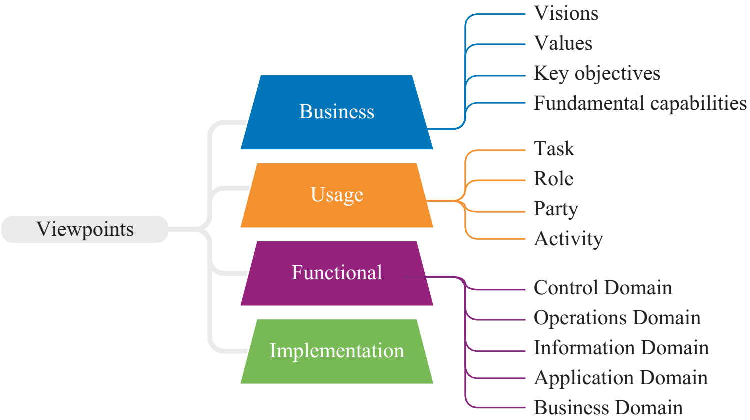

Fig. 1.5 IIRA viewpoints. (Adapted from Lin et al. 2019)

information domain, application domain and business domain. Finally, the Implementation Viewpoint provides (1) a description the general architecture of an IIoT system, (2) a technical description of its components, (3) an implementation map of the activities identified in the Usage Viewpoint; and (4) an implementation map for the key system characteristics (Lin et al. 2019).

By adopting IIRA, industries can integrate best practices into their processes, use a generic architecture and common framework and as a result reduce operation expenditure. It should be noted that IIRA provides architectural patterns for both cloud and edge computing.

1.4.4 WSO2 IoT Reference Architecture (WSO2 IRA)

WSO2 is a US-based open source integration vendor. The WSO2 IoT Reference Architecture (WSO2 IRA) is illustrated in Fig. 1.6 and supports IoT device monitoring, management, and interaction, covering the communication process between the IoT and the cloud (Fremantle 2015). The WSO2 IRA comprises five horizontal layers (client/external communication, event processing and analytics, aggregation layer, transports, and devices) and two cross-cutting layers (device management and identity and access management). Table 1.2 provides a brief definition of each layer.

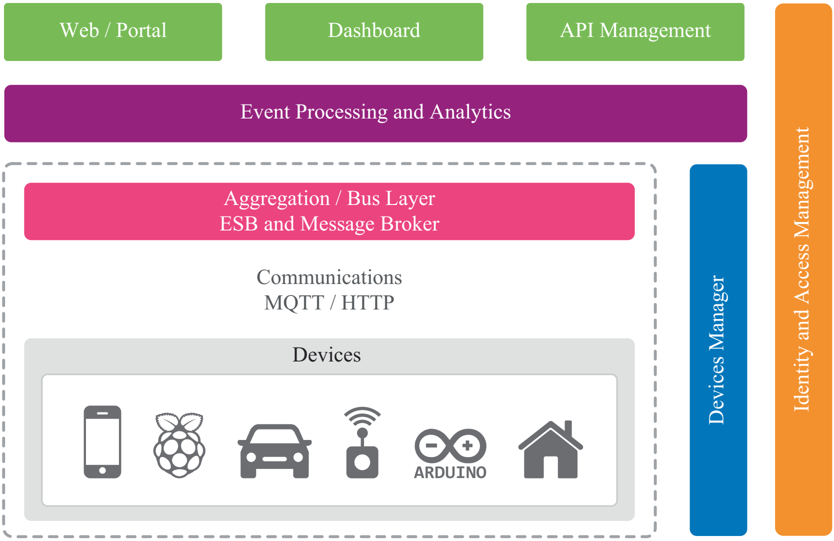

Fig. 1.6 WSO2 IoT Reference Architecture. (Adapted from Fremantle 2015)

Table 1.2 WSO2 IoT Reference Architecture layers

Layer	*Description*
Communication	Enables the devices to communicate outside of the device-oriented system web-based front-ends and portals, dashboards, and APIs.
Event processing and analytics	Takes the events from the bus and provides the ability to process and act upon these events.
Aggregation	Aggregates and brokers communications between devices, aggregates and combine communications from different devices and routes communications to a specific device, and bridges and transforms between different protocols.
Transport	Supports the connectivity of the devices.
Devices	IoT devices, they must have some communications that either indirectly or directly attaches to the Internet.
Device management	• Communicates with devices via various protocols and provides both individual and bulk control of devices. It also remotely manages software and applications deployed on the device. • Maintains the list of device identities and map these into owners. It must also work with the identity and access management layer to manage access controls over devices.
Access management	Provides identify and access management services.

1.5 Intel System Architecture Specifications (Intel SAS)

The purpose of the Intel System Architecture Specifications (SAS) is to connect any type of device to the cloud considering five key items: (1) C2T management, (2) real time analytics, (3) interoperability, (4) service and device discovery and provisioning, and (5) security (Intel 2015). Intel SAS has two distinct versions that co-exist in order to cover different infrastructure maturity levels: version 1.0 for connecting the unconnected and version 2.0 for smart and connected things. Version 1.0 specifies how legacy devices that were not originally designed to be connected to the cloud can use an IoT gateway to be online. Version 2.0 specifies how to integrate heterogeneous smart things focusing on security, manageability and real time data sharing between things and cloud (Fig. 1.7).

Intel SAS recommends a layered architecture that encompasses horizontal layers (users, runtime, and developers) and vertical layers (business and security). The data flow involves through eleven steps including analogue-to-digital conversion (ADC), gateways and reaching the cloud. Intel also recommends software components and interfaces to connect legacy devices with no connectivity functionality. The software components are located at endpoint devices and in the cloud. Basically, the cloud software components receive data collected by on-premise components and are responsible for analysis, storage, and service orchestration.

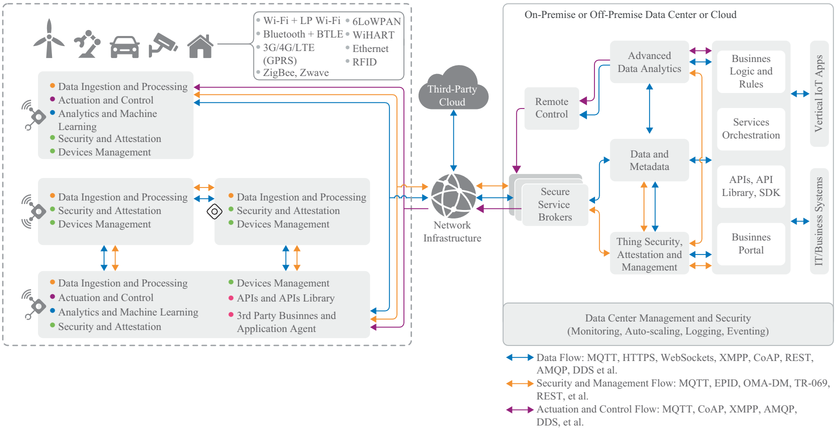
Wi-Fi + LP Wi-Fi
Bluetooth + BTLE
3G/4G/LTE (GPRS)
ZigBee, Zwave
6LoWPAN
WiHART
Ethernet
RFID
Data Ingestion and Processing
Actuation and Control
Analytics and Machine Learning
Security and Attestation
Devices Management
Data Ingestion and Processing
Security and Attestation
Devices Management
Data Ingestion and Processing
Security and Attestation
Devices Management
Data Ingestion and Processing
Actuation and Control
Analytics and Machine Learning
Security and Attestation
Devices Management
APIs and APIs Library
3rd Party Businnes and Application Agent
Third-Party Cloud
Network Infrastructure
On-Premise or Off-Premise Data Center or Cloud
Remote Control
Advanced Data Analytics
Data and Metadata
Secure Service Brokers
Thing Security, Attestation and Management
Businnes Logic and Rules
Services Orchestration
APIs, API Library, SDK
Businnes Portal
Vertical IoT Apps
IT/Business Systems
Data Center Management and Security (Monitoring, Auto-scaling, Logging, Eventing)
Data Flow: MQTT, HTTPS, WebSockets, XMPP, CoAP, REST, AMQP, DDS et al.
Security and Management Flow: MQTT, EPID, OMA-DM, TR-069, REST, et al.
Actuation and Control Flow: MQTT, CoAP, XMPP, AMQP, DDS, et al.

Fig. 1.7 Intel system architecture specifications. (Adapted from Intel 2015)

1.5.1 Azure IoT Reference Architecture (Azure IRA)

The Azure IoT Reference Architecture (Azure IRA) represented in Fig. 1.8 relies on Microsoft Azure platform to connect sensors to intelligent services at the cloud. The main goal of Azure IRA is to take actions on business insights that are generated through gathering data from IoT applications ('things') (Microsoft 2018). The reference document proposes a recommended IoT architecture, describing foundational concepts and principals, IoT subsystems details and solution design considerations. Azure IRA is focused on flexibility. As such, IoT solutions are cloud native and microservice-based. As deployable services are independent of each other, they suggest that it is better for scaling, updating individual IoT subsystems, and flexibility in the selection of technologies per IoT subsystem.

Figure 1.8 shows the recommended Azure IRA covering both hybrid cloud and edge solution integration. In orange, one can see the core IoT subsystems: IoT devices, cloud gateway (IoT Hub), stream processing, and user interface. The IoT device should be able to register with the cloud gateway, which is responsible for managing the devices. The stream processor consumes and stores the data, and integrates with the business process. For each subsystem, the Azure IRA recommends a specific technology based on Azure services. There is also a set of optional IoT

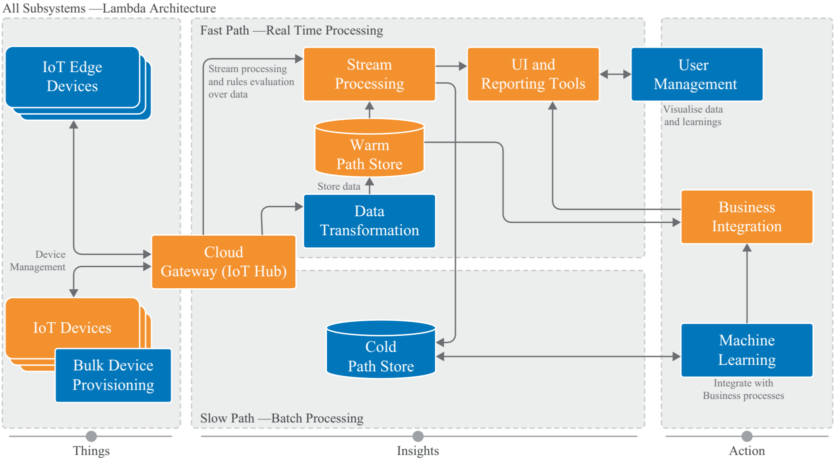

Fig. 1.8 Azure IoT Reference Architecture. (Adapted from Microsoft 2018)

subsystems (in blue): IoT edge devices, data transformation, machine learning, and user management. The edge devices are able to aggregate and/or transform and process the data on premise, while the data transformation (at the cloud) can manipulate and translate telemetry data. The machine learning subsystem allow the IoT system to learn from past data and act properly, such as firing alert to predictive maintenance. Finally, the user management subsystem provides functionality for users to manage the devices.

1.5.2 SAT-IoT

SAT IoT is a platform (Fig. 1.9) developed by Spanish company, SATEC, as part of the Horizon 2020 RECAP project.[1] Smart cities is a primary use case for SAT IoT. As such it needed an architecture that could (1) manage the smart city data network topology at run time, (2) use optimisation techniques that support processing aggregated data by geographical zones, and (3) monitor the IoT system and the optimisation process in run time (Peña and Fernández 2019).

Edge/cloud computing location transparency is a core feature of the platform allowing data to be shared between different zones (geographically and from the cloud to the edge), and thus to be processed at any of the edge nodes, mid nodes, or cloud nodes. This is realised by two of the entities in the SaT IoT architecture—the IoT Data Flow Dynamic Routing Entity and the Topology Management Entity. Together, they enable SAT IoT to manage the network topology at run time while also providing the necessary monitoring capabilities to understand the usage pattern and capacity limitations of the infrastructure. The IoT Data Flow Dynamic Routing Entity and the Topology Management Entity are augmented by the integration of the RECAP Application Optimiser in to SAT IoT, which derive the best possible placement of the data processing logic. Figure 1.9 shows the SAT-IoT architecture composed of Physical Layer, Smart Device Entity, IoT Data Flow Collector Entity, IoT Data Flow Dynamic Routing Entity, IoT Topology Management Entity, IoT Visualisation Entity, IoT Cloud Entity, Platform Access Entity, Security and Privacy, and Embedded IoT Applications.

[1] https://recap-project.eu/

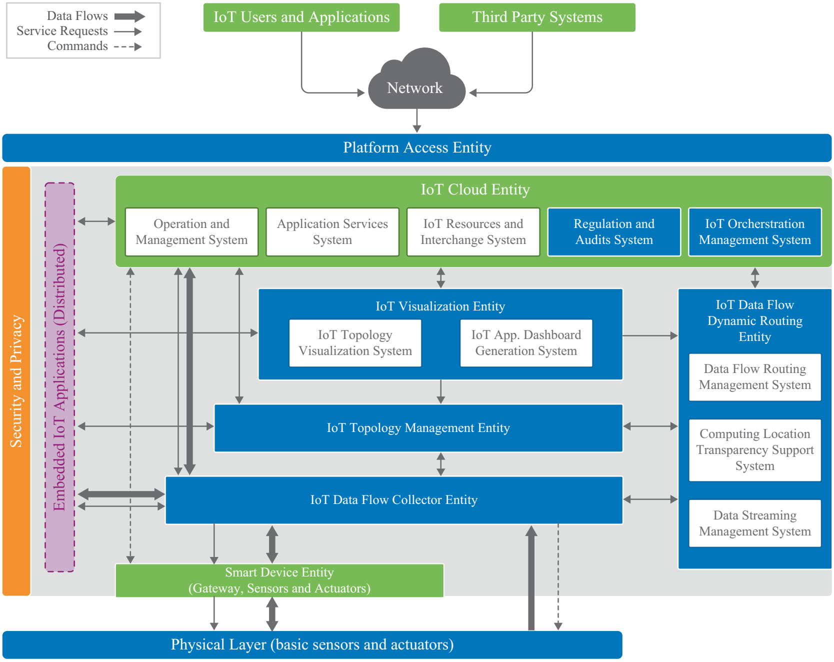
Data Flows
Service Requests
Commands
IoT Users and Applications
Third Party Systems
Network
Platform Access Entity
Security and Privacy
Embedded IoT Applications (Distributed)
IoT Cloud Entity
Operation and Management System
Application Services System
IoT Resources and Interchange System
Regulation and Audits System
IoT Orcherstration Management System
IoT Visualization Entity
IoT Topology Visualization System
IoT App. Dashboard Generation System
IoT Data Flow Dynamic Routing Entity
Data Flow Routing Management System
Computing Location Transparency Support System
Data Streaming Management System
IoT Topology Management Entity
IoT Data Flow Collector Entity
Smart Device Entity (Gateway, Sensors and Actuators)
Physical Layer (basic sensors and actuators)

Fig. 1.9 The SAT-IoT Architecture. (Adapted from Peña and Fernández 2019)

1.5.3 Summary of Architectural Features

Table 1.3 summarises the key functional features addressed in each IoT Reference Architecture, that is interoperability, scalability, security and privacy, data management, analytics, data visualisation and user interface, and supported computing paradigms.

By system interoperability, we mean that the architecture should address connectivity, data management and automatic integration in a transparent way for the end user. Scalability refers to the architecture's ability to handle increases in the number of IoT devices and endpoints. Security and privacy capability ensures that the information be where it should be and prevents data leakage to unauthorised persons. Data management refers to both the management and exchange of data between architectural

Table 1.3 Summary of key features listed by different IoT Reference Architectures

Reference Architectures	*Interoperability*	*Scalability*	*Security and privacy*	*Data management*	*Analytics*	*Data visualisation/ user interface*	*Supported computing paradigm*
IoT ARM	X	X	X	X	–	–	IoT and cloud
IEEE P2413	X	X	X	X	–	–	IoT and cloud
IIRA	X	X	X	X	X	-	IoT, edge and cloud
WSO2 IRA	X	X	X	X	X	X	IoT and cloud
Intel SAS	X	X	X	X	X	X	IoT and cloud
Azure IRA	X	X	X	X	X	X	IoT edge and cloud
SAT-IoT	X	X	X	X	X	X	IoT, fog, edge and cloud

components. Analytics refers to the ability of the architecture to capture useful data from the deluge of data that travels on the network. Data visualisation and user interface is related to whether the architecture provides a human interface. Finally, computing paradigm refers to whether the architecture addresses support for new computing paradigms and specifically cloud, fog, edge, and dew computing.

Table 1.3 summarises the key features of different IoT Reference Architectures. It clearly emerges that only two functionalities are met by all Reference Architecture proposals—interoperability and security and privacy. Another common area of focus, unsurprisingly, is data management. Obviously, the primary value driver in the IoT is data and systems are required to manage the volume, velocity and variety of this data, not least where its stored and processes. The IEEE P2413 Reference Architecture presents less functionality; however this is due to the nature of such a standard. It is however the basis for a related smart cities standard (RASC).

When considering the IoT from a business, technical, or research perspective, each of these architecture features should be considered and addressed.

1.5.4 Conclusion

The chapter introduced two perspectives of the Internet of Things—a purely technical and a socio-technical perspective. The Internet of Things is not merely a technical phenomenon. It has the potential to transform how society operates and interacts. As such, it is critical to have a sufficiently general abstraction of the Internet of Things that facilitates sense making without getting in to a non-generalisable level of granularity. We present such an abstraction organised around five entities—social actors, things, data, networks, and events—and the processes that occur between them, all situated in time and space. We provided a brief overview of some of the key enabling technologies and new computing paradigms. Section 1.4 presented seven Reference Architectures for the Internet of Things and compared them across seven dimensions. This provides a further lens with which to consider the Internet of Things.

References

Accenture and General Electric. 2014. *Industrial Internet Insights Report for 2015*. Accessed April 2020. https://www.accenture.com/us-en/_acnmedia/Accenture/next-gen/reassembling-industry/pdf/Accenture-Industrial-Internet-Changing-Competitive-Landscape-Industries.pdf.

Bauer, Martin, Mathieu Boussard, Nicola Bui, Jourik De Loof, Carsten Magerkurth, Stefan Meissner, Andreas Nettsträter, Julinda Stefa, Matthias Thoma, and Joachim W. Walewski. 2013. IoT Reference Architecture. In *Enabling Things to Talk*, 163–211. Berlin, Heidelberg: Springer.

Boyes, Hugh, Bil Hallaq, Joe Cunningham, and Tim Watson. 2018. The Industrial Internet of Things (IIoT): An Analysis Framework. *Computers in Industry* 101: 1–12.

Breivold, Hongyu Pei. 2017. *A Survey and Analysis of Reference Architectures for the Internet-of-Things*. ICSEA 2017, 143.

Cavalcante, Everton, Marcelo P. Alves, Thais Batista, Flavia C. Delicato, and Paulo F. Pires. 2015. *An Analysis of Reference Architectures for the Internet of Things*. International Workshop on Exploring Component-based Techniques for Constructing Reference Architectures (CobRA).

Cisco. 2012. *The Internet of Everything: How More Relevant and Valuable Connections Will Change the World*. Cisco IBSG, 2012. Accessed December 2019. https://www.cisco.com/c/dam/global/en_my/assets/ciscoinnovate/pdfs/IoE.pdf.

Fremantle, Paul. 2015. *A Reference Architecture for the Internet of Things*. WSO2 White paper.

Gartner. 2017. Gartner Says 8.4 Billion Connected "Things" Will be in Use in 2017, Up 31 Percent from 2016. https://www.gartner.com/en/newsroom/press-releases/2017-02-07-gartner-says-8-billion-connected-things-will-be-in-use-in-2017-up-31-percent-from-2016.

Haller, S., S. Karnouskos, and C. Schroth. 2009. The Internet of Things in an Enterprise Context. In *Future Internet Symposium*, 14–28. Berlin, Heidelberg: Springer.

IEEE P2413. 2014. Standard for an Architectural Framework for the Internet of Things (IoT). *IEEE Standards Association*, 16 September. Accessed December 2019. http://grouper.ieee.org/groups/2413/Sept14_meeting_report-final.pdf.

Intel. 2015. The Intel IoT Platform Architecture Specification White Paper. Intel.

Iorga, Michaela, Larry Feldman, Robert Barton, Michael Martin, Nedim Goren, and Charif Mahmoudi. 2017. The NIST Definition of Fog Computing. *NIST Special Publication* (SP) 800-191 (Draft). National Institute of Standards and Technology.

IoT-A project. 2019. Accessed December 2019. https://cordis.europa.eu/project/id/257521.

IPv6 Addressing Architecture. 2003. https://tools.ietf.org/html/rfc3513.

Karygiannis, Tom T., Bernard Eydt, Greg Barber, Lynn Bunn, and T. Phillips. 2007. Guidelines for Securing Radio Frequency Identification (RFID) Systems: Recommendations of the National Institute of Standards and Technology. *NIST Special Publication*, 800-98.

Lin, Shi-Wan, Brandford Miller, Jacques Durand, Graham Bleakley, Amine Chigani, Robert Martin, Brett Murphy, and Mark Crawford. 2019. The Industrial Internet of Things Volume G1: Reference Architecture V1.90. *Industrial Internet Consortium*, June. Accessed December 2019. https://www.iiconsortium.org/pdf/IIRA-v1.9.pdf.

Lynn, Theodore, Philip Healy, Steven Kilroy, Graham Hunt, Lisa van der Werff, Shankar Venkatagiri, and John Morrison. 2015. *Towards a general research framework for social media research using big data*. In 2015 IEEE International Professional Communication Conference (IPCC), 1–8. IEEE.

Mell, Peter, and Tim Grance. 2011. The NIST Definition of Cloud Computing.

Microsoft. 2018. Microsoft Azure IoT Reference Architecture, Version 2.1. Accessed December 2019. http://download.microsoft.com/download/A/4/D/A4DAD253-BC21-41D3-B9D9-87D2AE6F0719/Microsoft_Azure_IoT_Reference_Architecture.pdf.

P2413.1. 2019. P2413.1 Standard for a Reference Architecture for Smart City (RASC). *IEEE Standard Association*. Accessed December 2019. https://standards.ieee.org/project/2413_1.html.

P2413.2. 2019. P2413.2 Standard for a Reference Architecture for Power Distribution IoT (PDIoT). *IEEE Standard Association*. Accessed December 2019. https://standards.ieee.org/project/2413_2.html.

Peña, Miguel Angel López, and Isabel Muñoz Fernández. 2019. *SAT-IoT: An Architectural Model for a High-Performance Fog/Edge/Cloud IoT Platform*. IEEE World Forum on Internet of Things (WF-IoT), 633–638. IEEE.

Shin, Donghee. 2014. A Socio-technical Framework for Internet-of-Things Design: A Human-Centered Design for the Internet of Things. *Telematics and Informatics* 31 (4): 519–531.

Stankovic, John A. 2008. When Sensor and Actuator Networks Cover the World. *ETRI Journal* 30 (5): 627–633.

Tarkoma, Sasu, and Artem Katasonov. 2011. *Internet of Things Strategic Research Agenda (IoT–SRA)*. Finnish Strategic Centre for Science, Technology, and Innovation: For Information and Communications (ICT) Services, Businesses, and Technologies, Finland.

Tsai, Shin-Yeh, Sok-Ian Sou, and Meng-Hsun Tsai. 2012. *Effect of Data Aggregation in M2M Networks*. In The 15th International Symposium on Wireless Personal Multimedia Communications, 95–99. IEEE.

Wang, Yingwei, and David Leblanc. 2016. *Integrating SaaS and SaaP with Dew Computing*. In 2016 IEEE International Conferences on Big Data and Cloud Computing (BDCloud), Social Computing and Networking (SocialCom), Sustainable Computing and Communications (SustainCom) (BDCloud-SocialCom-SustainCom), 590–594. IEEE.

Weyrich, Michael, and Christof Ebert. 2016. Reference Architectures for the Internet of Things. *IEEE Software* 33, no. 1: 112–116. Accessed December 2019. https://doi.org/10.1109/MS.2016.20.

Whitmore, Andrew, Anurag Agarwal, and Li Da Xu. 2015. The Internet of Things—A Survey of Topics and Trends. *Information Systems Frontiers* 17 (2): 261–274.

Zhao, Shanyang. 2003. Toward a Taxonomy of Copresence. *Presence: Teleoperators & Virtual Environments* 12 (5): 445–455.