

Charith Perera
PhD, MBA

Sensing as a Service for Internet of Things

A Roadmap



PUBLISHED BY LEANPUB

Brand names, logos and trademarks used herein remain the property of their respective owners. This listing of any firm or their logos is not intended to imply any endorsement or direct affiliation with the author.



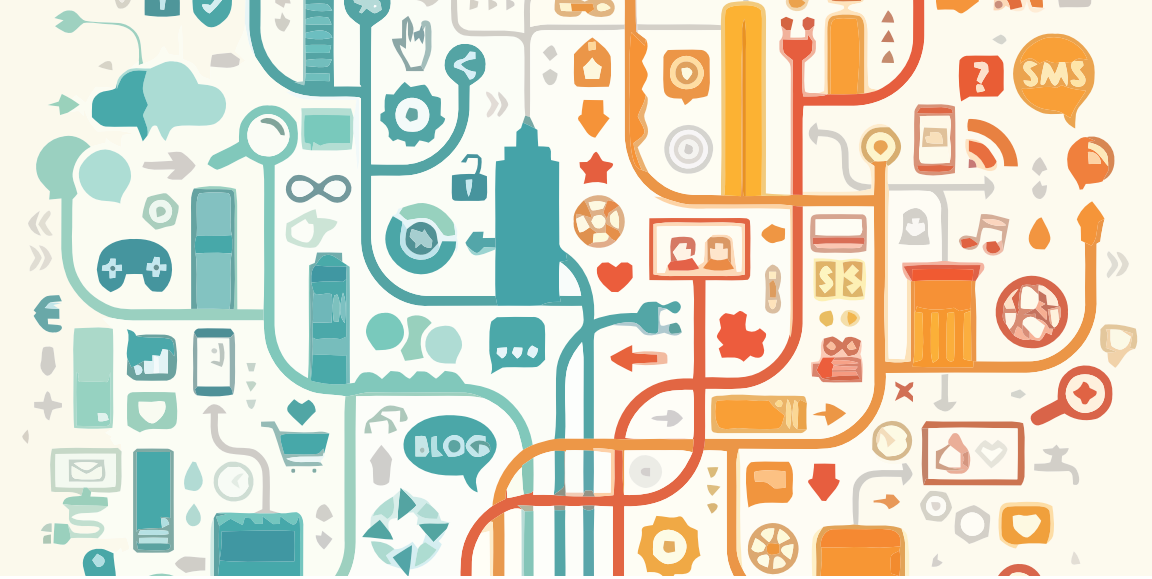
How to cite this book

*Charith Perera, Sensing as a Service for Internet of Things: A Roadmap,
Leanpub Publishers, 2017*

Version 0.9, November 2016

Version 1.0, February 2017

Version 1.1, June 2018 (Latest)



Contents

	Preface	5
1	Introduction	7
1.1	History	7
1.2	Internet of Things	8
1.3	Marketplace	14
1.4	The Problem	30
2	Sensing as a Service (S²aaS)	39
2.1	Smarter Cities	39
2.2	Everything as a Service	41
2.3	Sensing as a Service Model (S ² aaS)	43
2.4	Data Ownership	46
2.5	Motivational Use Cases	49
2.6	Sensing as a Service in Action	50

- 2.7 Advantages and Benefits 55
- 2.8 The solution: S²aaS 58
- 3 The Ecosystem 61**
- 3.1 IoT Solutions and Infrastructure 62
- 3.2 Configuration and Personalization 70
- 3.3 The Marketplace and Data Trading 78
- 3.4 Architectural Components 86
- 3.5 Edge Computing for Smart Cities 93
- Looking Ahead 97

Preface

Few years back, I wrote about the Sensing as a Service (S²aaS) in two scholarly publications [200] [142]. Since then, these publications have been well cited and discussed by different research communities. After receiving number of inquires from interested readers, I decided to write this book to explain the topic of S²aaS in detail, specially without being restricted into number of pages allowed by conferences and journals. This book aims to expand on previous ideas and to present a much detailed vision that would be useful to both general (non-scientific) and advance (scientific) readers.

This book is written in a easy to understand non-technical language to help general readers to grasp the content quickly. However, I also wanted to make sure that this book useful for advance readers who are interested in additional reading material on the topic. In order to facilitate them, throughout this book, I have presented additional material using different types of notes.

Research Challenges This type of notes are used to highlight research challenges. Research questions are identified and briefly discussed in order to provide insights and directions towards addressing them. General readers may skip these notes. ■

— **Further Reading.** This type of notes provide links to web resources, technical documents, white paper, and multimedia material. However, it is important to note that this book is intended to be self-contained and do not expect readers to read all these additional material provided. They are provided to browse at leisure time, if readers are eager to find more information on a particular topic. Additionally, relevant citations are embedded into the text to help advance readers so they can easily follow additional content. General readers should ignore such citations and should not intimidated by them. Such additional information is not necessary to understand the content of this book.



These types of notes are used to provide remarks, highlights, warnings, cautions, hints, practical tips, statistics or any other important advice to the readers.

- ❗ Over the years, many individuals have contributed to develop and shape up the vision of S²aaS. In order to acknowledge their contributions, narration is changed to first person plural throughout the book.

— **Who Should Read This Book.** This book is primarily aimed at following audiences:

- Are you a undergraduate student, masters student, PhD student, or a researcher interested in Internet of Things ?
- Are you a hobbyist or a maker who is bored building typical automation and monitoring solutions for Internet of things domain and looking something new ?
- Looking for some novel ideas or research challenges in the field of Internet of Things ?
- Have heard about Sensing as a Service, but not sure what it is ?

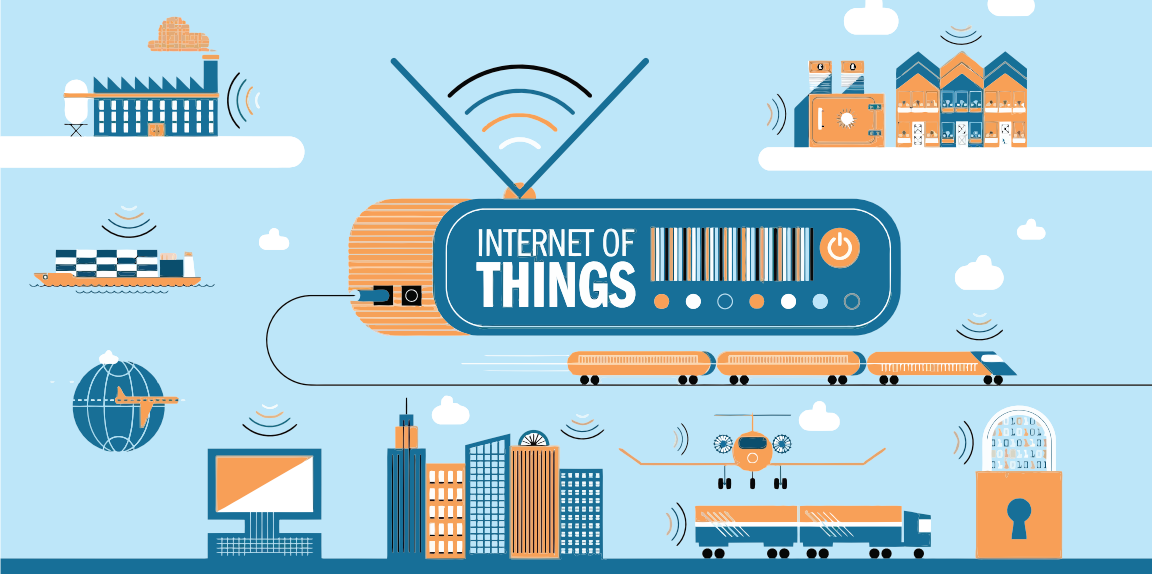
This book is for you.

— **Future of This Book and Updates.** This is not a typical computer science text book, instead a roadmap. The primary objective of this book is to introduce you to the topic of S²aaS and the research challenges around it, so as a community we can address them together.

This book is primarily written to be published on-line as an eBook. However, I understand some of you may like to have a hard copy. To accommodate such readers, this book is available through *Lulu* as well. It is important to note that, as time goes by, roadmaps need to be updated. Some of the content presented in this book may become outdated very quickly due to research and development happens over time.

My aim is to keep this book up-to-date. I'm planning to update this book multiple times per year. Please refer the version number in order to find out the latest version. This is why I chose to publish in *Leanpub*.

Finally, I would love to hear your feedback. That is why I made this book freely available to everyone. I'm more than happy to update this book and add more content depend on your feedback. Please send your feedback to charith.perera@ieee.org.



1. Introduction

This chapter introduce you to the Internet of things (IoT), its history, why IoT has become a buzz word, current IoT marketplace and the major weaknesses in IoT. If you are well aware of IoT, you may directly move to Section 1.4. This chapter aims to create a foundation for upcoming chapters.

1.1 History

Before we investigate the IoT in depth, it is important to look at its evolution. In the late 1960s, communication between two computers was made possible through a computer network [124]. More specifically, in 1969, The first message is sent over the ARPANET, the predecessor of the Internet. The first patent for a passive, read-write RFID tag was granted in 1973. A year later, in 1974, a Universal Product Code (UPC) label is used to ring up purchases at a supermarket for the first time.

In the early 1980s the TCP/IP stack was introduced. Then, commercial use of the Internet started in the late 1980s. Later, the World Wide Web (WWW) became available in 1991 which made

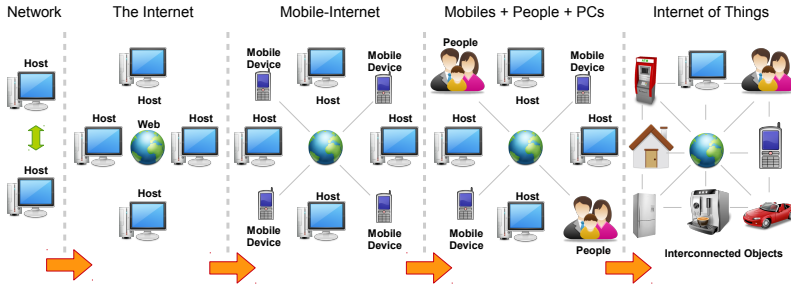


Figure 1.1: Evolution of the Internet of Things (IoT)

the Internet more popular and stimulate the rapid growth. Web of Things (WoT) [75], which based on WWW, is a part of IoT. Later, mobile devices connected to the Internet and formed the mobile-Internet [33]. With the emergence of social networking, users started to become connected together over the Internet. The next step in the IoT is where objects around us will be able to connect to each other and communicate via the Internet [58]. Figure 1.1 illustrates five major phases in the evolution of the Internet of Things.

The term ‘*Internet of Things*’ was coined by Kevin Ashton executive director of the Auto-ID Center in 1999 [15]. Therefore, the term itself is over a decade and half old. However, the ideas of connected devices are more than three decades older [103]. Pervasive computing and ubiquitous computing are the term commonly used at the time.

— **History of the Internet of Things.** In-depth historical reviews are presented here: A look back at the history of the Internet of Things [17], History of the Internet of Things [103], Why it is called Internet of Things [150], A Very Short History of The Internet of Things [152].

1.2 Internet of Things

The Internet of Things (IoT) does not have a well accepted definition. Instead, IoT has been described and defined by many different parties from many different perspectives. In this section, we will introduce you to a wide variety of definitions.

Definition — (1). Things have identities and virtual personalities operating in smart spaces using intelligent interfaces to connect and communicate within social, environment, and user contexts [102].

Definition — (2). The Internet of Things allows people and ‘things’ to be connected Anytime, Anyplace, with Anything and Anyone, ideally using Any path/network and Any service [74].

Definition — (3). Internet of Things is the network of physical devices, vehicles, buildings and other items embedded with electronics, software, sensors, actuators, and network connectivity that enable these objects to collect and exchange data [90].

Definition — (4). Sensors and actuators embedded in physical objects are linked through wired and wireless networks, often using the same Internet Protocol that connects the Internet. [103].

Definition — (5). The Internet of Things is a network of networks where, typically, a massive number of objects / things / sensors / devices are connected through communications and information infrastructure to provide value-added services [84].

In parallel to the term *Internet of Things (IoT)*, Cisco has been driving the term *Internet of Everything (IoE)*. Intel initially called it the *Embedded Internet*. Some other terms used are M2M (Machine to machine) communication Web of Things, Industry 4.0, Industrial internet (of Things), Smart systems, Pervasive computing, Intelligent systems [103]. These terms are interrelated to each other as summarized in Figure 1.2.

— **Machine-to-Machine (M2M).** The term Machine to Machine (M2M) has been in use for more than a decade, and is well-known in the Telecoms sector. M2M communication had initially been a one-to-one connection, linking one machine to another. But today’s explosion of mobile connectivity means that data can now be more easily transmitted, via a system of IP networks, to a much wider range of devices [94].

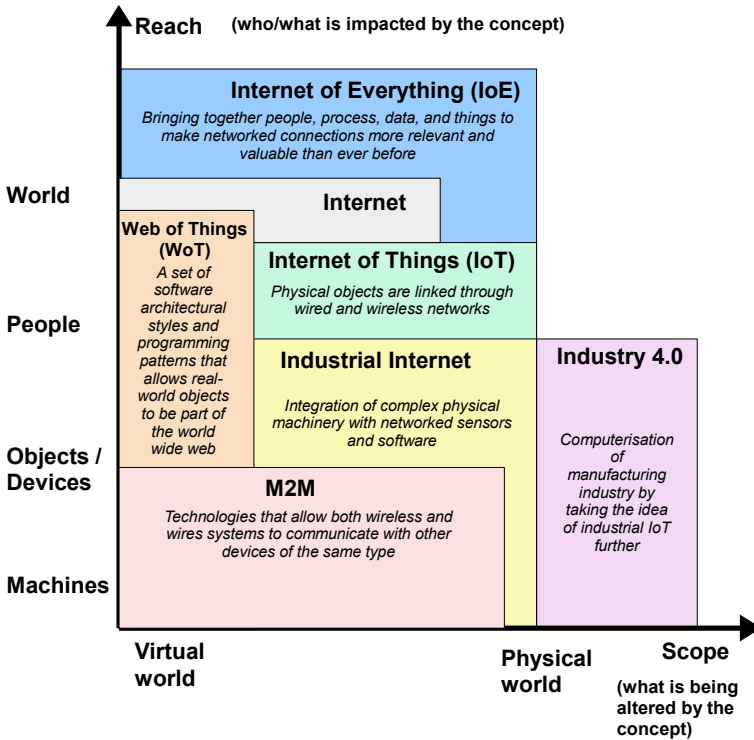


Figure 1.2: Concepts Related to IoT. Reproduced from [103].

— **Sensor Networks.** Wireless sensor networks (WSN), sometimes called wireless sensor and actuator networks (WSAN), are spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location [6].

— **Industrial Internet of Things.** The term industrial internet is strongly pushed by General Electric. It goes beyond M2M since it not only focuses on connections between machines but also includes human interfaces.

— **Internet.** In the above graph, the internet is a fairly small box. In its core it connects only people.

— **Web of Things (WoT).** The Web of Things is much narrower in scope as the other concepts as it solely focuses on software architecture.

— **Internet of Everything (IoE).** Still a rather vague concept, IoE aims to include all sorts of connections that one can envision. The concept has thus the highest reach.

— **Industry 4.0.** The term Industry 4.0 that is strongly pushed by the German government is as limited as the industrial internet in reach as it only focuses on manufacturing environments. However, it has the largest scope of all the concepts. Industry 4.0 describes a set of concepts to drive the next industrial revolution. That includes all kinds of connectivity concepts in the industrial context. However, it goes further and includes real changes to the physical world around us such as 3D-printing technologies or the introduction of new augmented reality hardware.

— **More IoT Definitions and Descriptions.** Definitions collected and synthesized by the IEEE Internet of Things community are documented here [112].

IoT Devices (*Things*) on the Internet of Things

As you may have understood by now, *Things* play a significant role in Internet of Things paradigm. There isn't any formal definition to describe a *Thing* in IoT paradigm. We have illustrated variety of different *Things* that can be part of IoT paradigm in Figure 1.3.



Figure 1.3: A *Thing* can be any object around us from refrigerators to bottles to watches to mobile phones to electrical plugs to sensors.

- ! It is important to note that terms such as objects, smart objects, internet connected objects (ICOs), nodes, devices, IoT devices, smart devices are also used interchangeably in IoT related documentations in order to refer to *'Things'*.

Let us now explore the major characteristics of a *'Thing'*. First, it is important to understand that, any object can become part of the IoT. One major characteristics is computational capability. Each *'Thing'* show have some kind of computational capabilities. Next, each *'Things'* should be be able to communicate with the Internet. This does not mean that each object should have a direct or permanent connection to the Internet. For example, a *'Thing'* may communicate with a near-by mobile phone using Bluetooth and the phone may forward the data to the Internet using its WiFi capabilities. In another example, a *'Thing'* may connect to the Internet using its GPRS communication capability once a week. In Figure 1.4, we illustrate how an everyday object may be converted into an IoT device in IoT. Typically, IoT devices have both sensing and actuation capabilities as well.

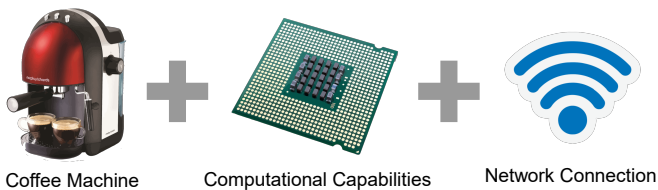


Figure 1.4: An everyday object embedded with some amount of computational and network communication capabilities can be identified as an IoT Device

Common Internet of Things Solutions Architecture

There is no consensus on constitutes a suitable architecture for an IoT solution. Systems have varying requirements that affect the choice of architecture. For example, in a centralised architecture, sensors lie on the periphery and are only concerned with data acquisition. These peripheral devices feed data to a centralised entity, which processes, analyses, stores and disseminates the data. This architectural pattern has many well documented benefits including

reliability, scalability and interoperability [161]. This is in contrast to a distributed IoT architecture where processing occurs on the periphery at the device level, and data may or may not then be sent to a centralised server or other peripheral devices. The distributed approach still has many issues that needs to be addressed but provides more fine grain control over the data produced. We can categorise different types of IoT solutions architecture into four segments [161]: 1) centralised, 2) collaborative, 3) connected intra-net of Things, and 4) distributed IoT.

Out of these architectures, centralised architecture is the most widely used in IoT solutions. The centralised architecture, as shown in Figure 1.5, consists of three components: 1) IoT devices, 2) Gateway devices, and 3) IoT cloud platforms. Today, there are many different vendor who provides both hardware and software components in order to support rapid IoT solutions development. We can see these components in the IoT solutions marketplace as well though though they may not be clearly visible to the end-users.

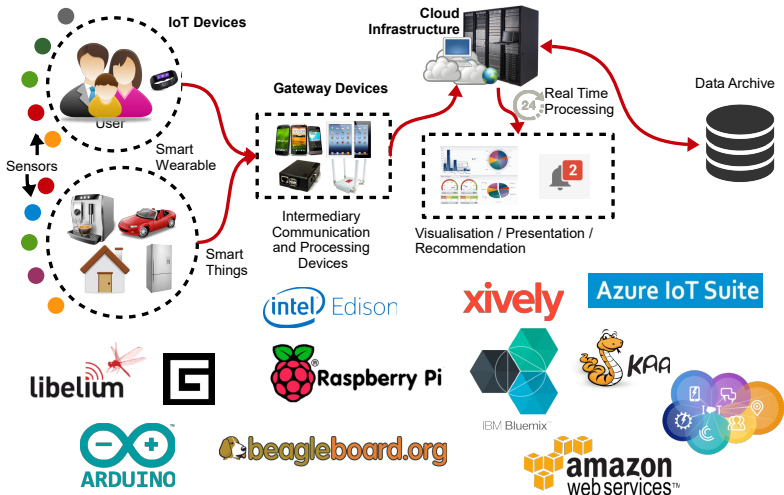


Figure 1.5: Common Internet of Things solutions architecture comprises with three components: 1) IoT devices, 2) Gateway devices, and 3) IoT cloud platforms.

1.3 Marketplace

In the remainder of this section is focused on giving an overview of IoT marketplace. Therefore, if you are familiar with IoT marketplace, please feel free to skim through this section and move to the Section 1.4. The interconnection and communication between everyday objects, in the IoT paradigm, enables many applications in many domains. Asin and Gascon [16] have listed 54 application domains under 12 categories: smart cities, smart environment, smart water, smart metering, security and emergencies, retail, logistics, industrial control, smart agriculture, smart animal farming, domestic and home automation, and eHealth. After analysing the industry marketplace and careful consideration, we classified the popular existing IoT solutions in the marketplace into five different categories: smart wearable, smart home, smart city, smart environment, smart enterprise.

❗ In many IoT related documentation, IoT is being introduced as *a domain* or *a paradigm*. Therefore, we have used those words interchangeably in this book as well. The term *IoT domain / paradigm* is often used as a umbrella term to encapsulate large number of *smart-**domains (e.g., smart cities, smart environment, smart water, smart metering, and so on).

❗ Throughout this section, we have cited number of interesting IoT products and product ideas. We have provided the web-links for you to look at further. However, by the time you are looking at these products, they may not available due to various reasons such as re-branding, going out of business, failed to secure initial funding, and so on.

In case of such unavailability, we suggest you to use the name of the IoT solution and related key terms to locate them using your favourite search engine. You should be able to find some trace of their existence in the past. The objective of introducing number of IoT products is to give you an idea on possibilities in IoT domain and highlight what people have developed in the past.

Smart Wearable

Wearable solutions are diverse in terms of functionality. They are designed for a variety of purposes as well as for wear on a variety of

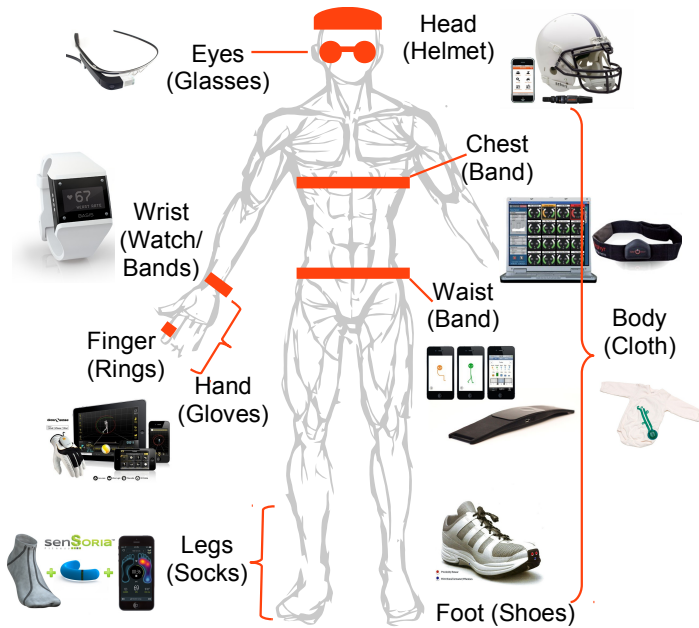


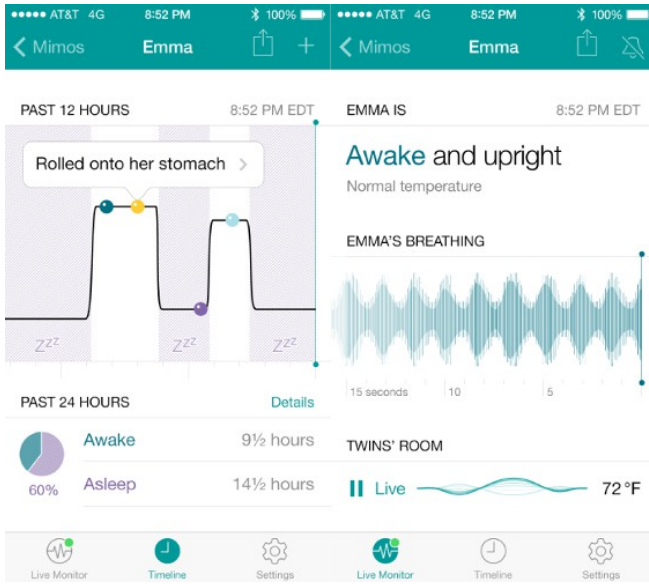
Figure 1.6: Different body parts popularly targeted by wearable IoT solutions in the industry market-place.

parts of the body, such as the head, eyes, wrist, waist, hands, fingers, legs, or embedded into different elements of attire. In the remaining of this section, we summarise popular wearable IoT solutions. The following list includes a brief description of each solution, context information gathered, similar solutions, and the context-aware functionality provided by the solution. The IoT solutions are categorised by the body part on which the solution must be worn, as illustrated in Figure 1.6. In addition to the industry IoT solutions, academic solutions in the wearable computing area are discussed in [95, 131]. Challenges and opportunities in developing smart wearable solutions are presented in [176].

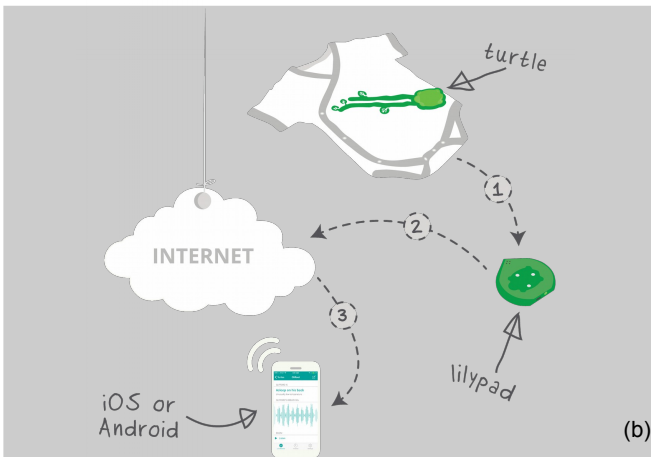
Cloth

- Monitor respiration, body position, activity level, skin temperature, and audio of a baby using pressure, stretch, noise, and temperature sensors, and provide notification through a smart phone regarding any situation that parents need to attend to (Baby Monitor: *Mimobaby* [159]). Some user interface of

Mimobaby is presented in Figure 1.7).



(a)



(b)

Figure 1.7: (a) User interface provided to the users, in this case parents by *Mimo Smart Baby Monitor* (*mimobaby.com*). All the raw information collected are presented to the users, using graphs, figures and icons, after generating secondary context information. (b) Illustrates how primary context has been collected and transferred through the infrastructure to discover secondary context information.

- A sleep-tracking device that uses a thin-film sensor strip placed on a mattress in combination with smart phone to help to create a nightly rest profile. It helps to improve user's sleep over time (Sleep Tracking: *Beddit* [24]).
- Jacket relieves anxiety and stress from those diagnosed with autism spectrum disorder (ASD) or attention-deficit / hyperactivity disorder. Built-in motion sensors and pressure sensors track the frustration and activity levels of the child throughout the day and generate custom notification alerts based on that information (Medical Assistant: *MyTJacket* [182]).

Waist / Chest

- Tracks posture and daily activities in real time. It provides advice on posture issues so users can improve their posture (Daily Activity and Fitness Monitor / Medical: *Lumoback* [104]).
- A device that updates Twitter when a baby in the womb kicks its mother (Medical Assistant: *kickbee* [108]).
- A chest band that tracks heart rate, speed, distance, stress level, calories, and activity level. It allows recommended working out within certain heart rate zones to achieve goals such as weight loss or cardiovascular improvement. (Personal Sports Assistant: *BioHarness* [201]).

Wrist

- A wrist band that tracks steps taken, stairs climbed, calories burned, and hours slept, distance travelled, and quality of sleep and provides recommendation for a healthier lifestyle (Daily Activity and Fitness Monitor: *MyBasis* [23], *BodyMedia* [29], *Lark* [181]).
- Open wearable sensor platform, a wrist band that comprises number of different sensors such as pulse, blood flow sounds, blood oxygen saturation, blood flow waveform, pulse, acceleration, type of activity, calories burned and number of steps taken, skin temperature (Open Platform: *AngelSensor* [169]).
- *EMBRACE+*, a wrist band that connects to the user's smart-phone via Bluetooth and displays any notifications user may receive as ambient light notifications (Personal Assistant: *EmbracePlus* [56]).
- Electrocardiogram technology (ECG), Bluetooth connectiv-

ity and a suite of sensors are used to recognize users' heart rhythm uniquely and securely and continuously log into users' nearby devices (Secure Authentication: *nymi* [155]).

- A watch that helps athletes to keep track of their training. Context information such as mapping, distance, speed, heart rate, and light are collected and fused to generate athletes' training profile (Personal Sports Assistant: *Leikr* [2]).

Eyes

- Sports-specific (skiing) goggles that monitor jump analytics, speed, navigation, trip recording, and peer tracking (Personal Sports Assistant: *Oakley Goggles* [122]).
- A pair of glasses that consist of camera, projector, and sensors to support functionalities such as navigation calendar notification, navigation, voice activated, voice translation, communication and so on. It also acts as an open platform where different context-ware functionalities can be built using provided sensors and processing capabilities (Open Platform: *Google Glass* [67]).

Head

- Sports-specific (American football) helmet that determines when to take a player off the field and seek medical advice through impact detection and analysis (Personal Sports Assistant: *TheShockBox* [87]).
- A bicycle helmet that detects a crash. If the user's head hits the pavement (or anything hard (ice, snow, dirt)), a signal will be sent to the smartphone automatically to generate a call for help (Emergency Accident monitor: *ICEdot* [83]).

Hands

- Monitor, analyze and improve golf swing through motion sensors embedded in gloves (Personal Sports Assistant: *Zepp* [202])
- A ring that monitors and keeps track of the user's heart rate (Medical Assistant: *ElectricFoxy* [54]).

Legs / Foot

- A sock that combines an accelerometer with textile sensors to measure steps, altitude and calories burnt. It helps runners to avoid potentially dangerous techniques: heel striking or

excessive forefoot running that could lead to back pain or Achilles ten-don injuries. (Daily Activity and Fitness Monitor / Medical: *Heapsylon* [168])

- A pair of shoes that provides feedback through vibrations in an intuitive and non-obstructive way. The shoes suggest the right direction and detect obstacles (Disability Assistance: *LeChal* [52])

Internal

- A small patch worn on the body working together with 1mm sensor-enabled pills and a back-end cloud service to collect and process real-time information (e.g. heart rate, temperature, activity and rest patterns throughout the day) on the user's medication adherence (Medical: *Proteus Digital Health* [156]).

Multi

- A device that can be worn on multiple body parts tracks steps taken, stairs climbed, calories burned, and hours slept, distance travelled, quality of sleep (Daily Activity and Fitness Monitor: *Fitbit* [61]. Some web user interfaces related to *Fitbit* are presented in Figure 1.8).
- An ultra-small GPS unit and five in-built sensors are used to collect data and fused to tell the camera exactly the right moment to take photos (Leisure: *Autographer* [19]).
- Remote monitoring system that collects data through devices that can be worn on different body parts on a patient's physiological conditions to support physicians (Health Monitoring: *Preventice BodyGuardian* [153]).

Smart Home

Solutions in this category make the experience of living at home more convenient and pleasant for the occupants. Some smart home [189] solutions also focus on assisting elderly people in their daily activities and on health care monitoring [3]. Due to the large market potential, more and more smart home solutions are making their way into the market. From the academic point of view, smart energy and resource management [79, 86], human-system interaction [196], and activity management [43], have been some of the major foci.

Platforms: *Smarthings* [163] is a generic platform that consists

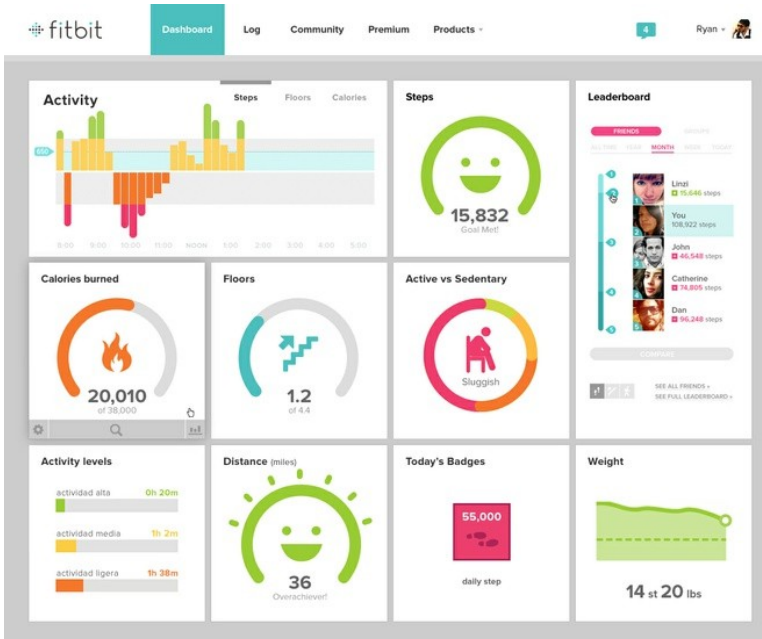


Figure 1.8: The *Fitbit* web based dashboard displays recent activity level and lots of other statistics using graphics, charts, and icons.

of hardware devices, sensors, and software applications. Context information is collected through sensors and injected into applications where reasoning and action are performed accordingly. For example, the sprinkler installed in the user's garden can detect rain and turn itself off to save energy. *Ninjablocks* [118] and *Twine* [180] provide similar functionalities. These solutions were mainly developed to support smart home and building domains, but they can be customised to other domains. *HomeOS* [50] is a platform that supports home automation. Instead of custom hardware (e.g. a *smarthings* hub), *HomeOS* is a software platform which can be installed on a normal PC. As with the *smarthings* platform, applications can be installed to support different context-aware functionalities (e.g. capturing an image from a door camera and sending it to the user when someone rings the doorbell). *Lab-of-things* [30] is a platform built for experimental research. It allows the user to easily connect hardware sensors to the software platform and enables the collection of data and the sharing of data, codes, and participants.

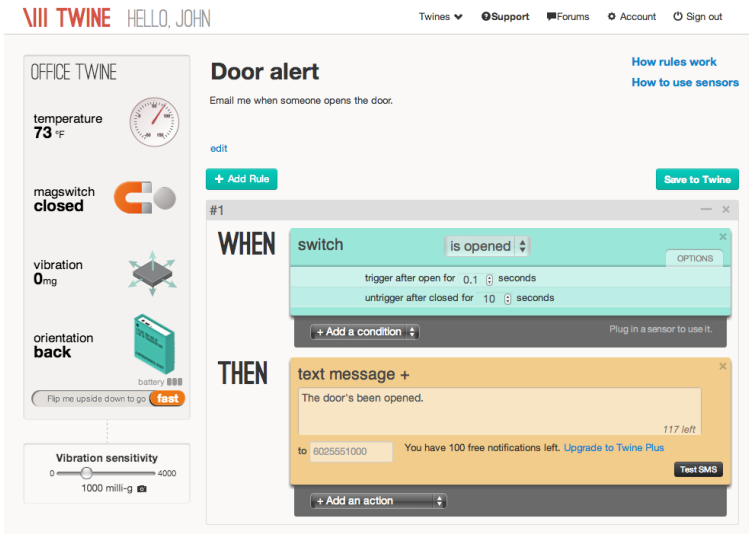


Figure 1.9: *Twine* [180] provides a user interface to define scenarios by combining sensors and actuators in a WHEN-THEN fashion which is also similar to the IF-THEN mechanism. *Twine* will trigger the actuation accordingly when conditions are met.

Virtual Assistance: *Ubi* [184] supports residents by acting as a voice-activated computer. It can perform tasks such as audio calendar, feed reader, podcast, voice memos, make lighting-based notifications to indicate the occurrence of certain events, weather, stock, email, and so on. *Ubi* has a microphone and speakers. It also has sensors to monitor the environment, such as monitoring the temperature, humidity, air pressure, and ambient light. *Netatmo* [81] is an air quality monitoring solution for smart homes. In order to determine air quality, it collects context information from sensors such as temperature, humidity, and CO₂. The solution monitors the home environment and sends an alert when the residents' attention is required. *Meethue* [149] is a bulb which can be controlled from mobile devices. The bulb reacts to the context and can change its colour and brightness according to user preferences, time / day / season, and activity (e.g. resident enters home) and is also sensitive to changes in the weather during the day.

Smart Objects: *WeMo* [26] is a Wi-Fi enabled switch that can be used to turn electronic devices on or off from anywhere.

Context-aware schedules are also supported, where turning on or off is performed automatically according to the time of day, sunrise, or sunset. Enabled with WeMo [26], the *Mr. Coffee 10-Cup Smart Optimal Brew Coffeemaker* [25] makes it easy to schedule, monitor, and modify your brew from anywhere. Sleep in a little longer by setting up a brewing schedule in advance. *Tado* [66] is an intelligent heating control that uses a smart phone. It offers context-aware functionalities such as turning down the heating when the last person leaves the house, turning the heating back up before someone gets home, and heats the house less when the sun is shining. *Nest* [72] is a thermostat that learns what temperatures users like and builds a context-aware personalised schedule. The thermostat automatically turns to an energy-efficient ‘away temperature’ when occupants leave the home. If it senses activity, such as a friend’s coming over to water the plants, Nest could start warming up the house. The thermostat can be activated remotely through the Nest mobile app.

Lockitron [101] is a door lock that can be opened and closed by a phone over the Internet. Residents can authorise family and friends to open a given door by providing authorisation over the Internet, so that others can use their smart phones to unlock doors. *Blufitbottle* [123] is a water bottle that records drinking habits while keeping the users healthy and hydrated. If the user starts to fall behind with hydration, the bottle has customisable sounds and lights to alert them. *Maid* [166] is a smart oven that knows what to cook and how. *Maid* is connected to a sizable recipe store in the internet and can lead you through them. *Maid* also learns your calorie requirements and delivers personalized recipe suggestions. *OpenSprinkler* [127] free users from their sprinkler or irrigation control box, enabling you to program, run, or stop zones at any time from anywhere. Some user interfaces related to *OpenSprinkler* is presented in Figure 1.10.

Digital Relationships: *Wheredial* [107] offers a way to make a personal connection with family members or friends. It retrieves a person’s location from Foursquare, Google Latitude, and a variety of other services. Then it rotates the dial (like a clock) to show where the person is at a given moment. *Goodnightlamp* [49] is a family of connected lamps that let the user remotely communicate the act of coming back home to their loved ones easily and in an ambient way by fusing location-aware sensing. The objective of

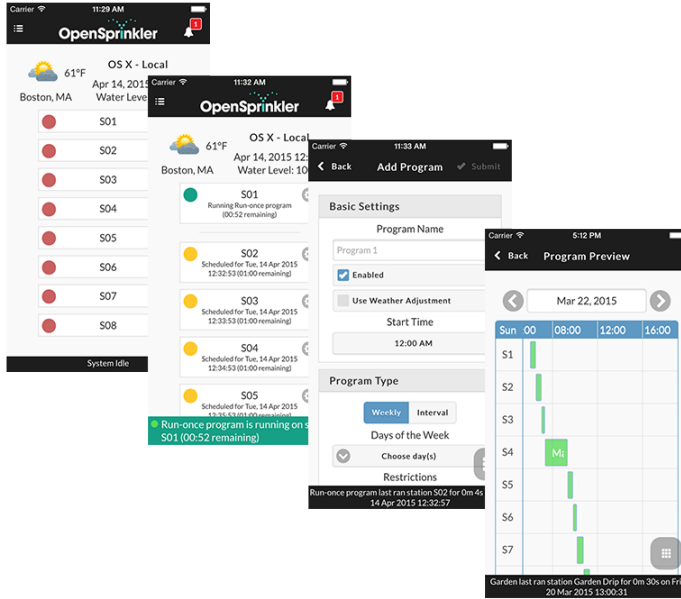


Figure 1.10: *OpenSprinkler* automates irrigation needs.

Wheredial and *Goodnightlamp* is the same: helping to build and maintain family relationships and further strengthen friendships by mitigating the fact that the users are apart from each other. Such solutions are extremely important in terms of social, psychological, and mental well-being.

Legacy Devices: Most of the IoT products in the marketplace comes with own hardware components and software stacks. However, we have increasingly seen that IoT solutions attempt to enrich legacy devices with smart capabilities. One very popular solution is *Nest* [72] thermostat. It has the capability to learn from users over time about their behaviour and preferences and control the temperature more efficiently and pro-actively. This thermostat can be installed by replacing the existing non-smart traditional thermostats. Everything else connected to the heating systems would work seamlessly. *ShutterEaze* [171] is another example for enriching legacy devices. This example is more into home automation. *ShutterEaze* makes it easy for anyone to add remote control functionality and automate their existing interior plantation shutters. No shutters changing is required.

A slightly different example is *Leo* [96]. As illustrated in Figure 1.11, *Leo* keeps track of smoke alarms, carbon monoxide alarms, and the climate in home. If something is not right, it sends notifications straight to the users phone. It is important to note that, there is no communication between the legacy smoke detection devices / alarms and the *Leo* device. They are completely two different systems without any dependencies. *Leo* get triggered by the sound that may produce by other traditional alarms. This is a very good examples to demonstrate how to embed smartness to our homes without replacing existing legacy systems. More importantly, any kind of replacing cost a significant amount to the consumers. This kind of solutions eliminates such unnecessary and extra costs that may put consumers away from adopting IoT solutions. The lesson we can learn is that if the legacy devices cannot understand the context it operates and act intelligently, the new devices can be incorporated to embed smartness to the overall system where new devices helps to mitigate the weaknesses in the legacy devices.

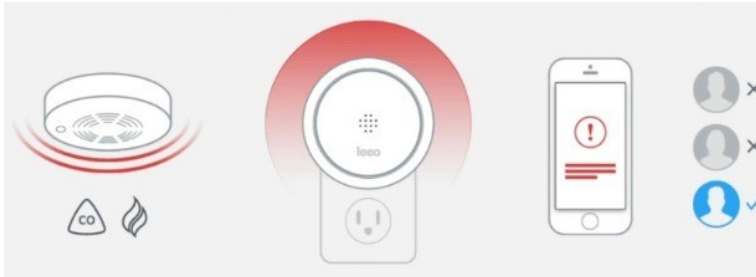


Figure 1.11: Enriching smartness to legacy devices: Legacy devices may monitor fire and smoke. Once these legacy devices detect any abnormalities, they will trigger their alarms and start to make sounds. *Leo* is designed to listen to such alarm sound. Once *Leo* detects such sound, it triggers its reaction mechanisms such as sending notification to the users, neighbours, and government authorities such as fire brigade in a predefined order.

Smart City

Towns and cities accommodate one-half of the world's population, creating tremendous pressure on every aspect of urban living. Cities have large concentrations of resources and facilities [178]. The

enormous pressure towards efficient city management has triggered various Smart City initiatives by both government and private sector businesses to invest in information and communication technologies to find sustainable solutions to the growing problems [142]. Smart grid is one of the domains in which academia, industry, and governments are interested and invested significantly [76, 77].

Smart Traffic: *ParkSight* [177] is a parking management technology designed for cities. Context information is retrieved through sensors (magnetometers) embedded in parking slots. Application support is provided via location and map services to guide drivers to convenient parking based on real-time context analysis. *Uber* [183] allows users to request a ride at any time. The company in a particular place sends a cab. In contrast to transitional taxi services, no phone call or pick-up location is required. A mobile application shows the cabs close to the users and their movement in real time. A cab can be requested by means of a single smartphone tap. *Alltrafficsolutions* [7] collects traffic data through sensors and visualises it on maps in order to provide drivers with traffic updates. Further, it provides remote equipment management support related to traffic control (e.g. changes in digital road signs, speed limit boards, variable message signs (e.g. ‘event parking’) to drivers, and changes in the brightness of digital signs based on the context information). *Streetbump* [42] is a crowd-sourcing project that helps residents to improve their neighbourhood streets. Volunteers use the *Streetbump* mobile application to collect road condition data while they drive. The data are visualised on a map to alert residents regarding real-time road conditions. The collected data provide governments with real-time information with which to fix problems and plan long-term investments.

Platforms: *Libelium* [98] provides a platform of low-level sensors that is capable of collecting a large amount of context information to support different application domains [9]. *Thingworx* [157] and *Xively* [197] are cloud-based IoT platforms, specifically focus on IoT domain, that process, analyse, and manage sensor data retrieved through a variety of different protocols. Since then, most of the major IoT companies have developed their own cloud IoT platforms by extending their existing cloud services: Microsoft Azure IoT Suite [109], Amazon AWS IOT [11], Google Cloud IoT [70], Oracle IoT [128], GE Predix [62], Autodesk Fusion Connect

[18]. Additionally, number of open source IoT platforms are also being developed by the community: Kaa [46], macchina.io [14], OpenIoT [126]. The exact functionalities provided by each platform varies from platforms to platform. However, in high level they all aims provide functionalities such as device and identity management, device discovery, data storage, data analytics, data management, security, mobility, scalability and so on. On top of that, each company provides value added services based on their core competencies such as machine learning, images recognition, artificial intelligence, and so on.

— **IoT Platforms Review.** Comprehensive reviews on IoT platforms are presented in [111, 158]. A list of cloud IoT platforms are presented in [151].

Resource Management: *SmartBelly* [28] is a smart waste management solution. It provides a sensor-embedded trash can that is capable of real-time context analysis and alerting the authorities when it is full and needs to be emptied. Location information is used to plan efficient garbage collection. *Echelon* [53] has developed a smart street lighting solution transforming street-lights into intelligent, energy-efficient, remotely managed networks. It schedules lights to be turned on or off and sets the dimming levels of individual lights or groups of lights so a city can intelligently provide the right level of lighting needed by analysing the context such as time of day, season, or weather conditions.

Activity Monitoring: *Livehoods* [113] offers a new way to conceptualise the dynamics, structure, and character of a city by analysing the social media its residents generate. This is achieved through collecting context information such as check-in patterns. *Livehoods* shows how citizens use the urban landscape and other resources. *Scenetap* [165] shows real-time info about the city's best places. It shows the context information of a given location such as how many people are there, the male to female ratio, and the average age of everyone inside. This helps users to find the best places to hang out (e.g. cinema, bar, restaurant) at a given time and gives information such as availability.

Smart Environment

Air Quality Monitoring: *Airqualityegg* [4] is a community-led sensor system that allows anyone to collect context information such as the carbon monoxide (CO) and nitrogen dioxide (NO₂) gas concentrations outside their home. Such data are related to urban air pollution. *Communitysensing* [40] is also an air quality monitoring system which provides both hand-held devices and a platform to be fixed into municipal vehicles such as street sweepers. *Aircasting* [78] is a platform for recording, mapping, and sharing health and environmental data using smart phones and custom monitoring devices. Context information includes sound levels, temperature, humidity, carbon monoxide (CO) and nitrogen dioxide (NO₂) gas concentrations, heart and breathing rate, activity level, and peak acceleration.

Water Quality Monitoring: *Floating Sensor Network* [187] collects real-time, high-resolution data on waterways via a series of mobile sensing ‘drifters’ that are placed in the water. It collects context information such as water quality, water flow movement, and speed, temperature and water pollution. *Intelligentriver* [39] is also an observation system that supports research and provides real-time monitoring, analysis and management of water resources. A similar solution has been developed by *Roboshoal* [170]. The difference is that their station is a mobile fish-shaped robotic device whose movement is controllable. *Dontflush* [134] is designed to enable residents to understand when overflows happen and reduce their waste-water production before and during an overflow event. Context information is processed in order to determine real-time sewage levels and advise users regarding safe flushing through a context-aware light bulb and SMS.

Natural Disaster Monitoring: *AmritaWNA* [133] is a wireless landslide detection system that is capable of releasing alerts about possible landslides caused by torrential rain in the region. Context information is collected by sensors such as strain gauge piezometers, vibrating wire piezometers, dielectric moisture sensors, tilt meters, and geophones. This is a station-based solution. *Insightrobotics* [88] is a solution that detects forest fires by fusing context information collected through various kinds of sensors (i.e. temperature, wind, and so on) and networked cameras.

Smart Farming: *Microstrain* [110] has developed a wireless

environmental sensing system to monitor key conditions during the growing season in vineyards. Context information such as current temperature and soil moisture conditions, leaf wetness, and solar radiation is collected and fused in order to monitor vineyards remotely and alert farmers regarding critical situations. The collected data are used to support both real-time context-aware functionalities and historic data analysis. *Bumblebee* [164] monitors the lives of bumblebees by collecting and processing context information such as visual, audio, temperature, sunlight, and weather. It automatically tweets the current situation of the colony and well-being of the bees. *Hydropoint* [82] retrieves context information through 40,000 weather stations and automatically schedules irrigation based on individual landscape needs and local weather conditions, resulting in lower water bills and energy savings.

Smart Enterprise

In general, enterprise IoT solutions are designed to support infrastructure and more general purpose functionalities in industrial places, such as management and connectivity.

Transportation and Logistics: Senseaware [167] is a solution developed to support real-time shipment tracking. The context information such as location, temperature, light, relative humidity and

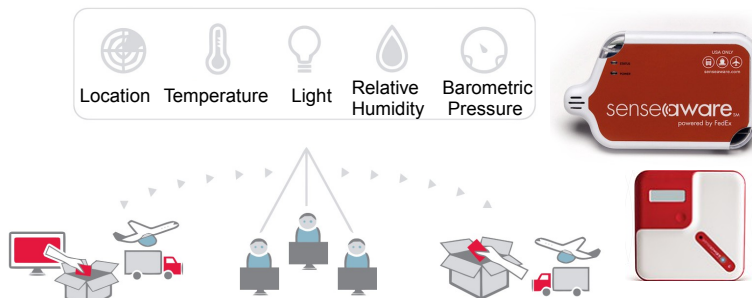


Figure 1.12: *SenseAware* [167] uses small smart devices that comprises five different built-in sensors with limited computational and communication capabilities. It reports the status of the packages in real time to the cloud. These smart devices comes in different sizes and form factors in order to support different types of packaging methods. Two types of smart devices are shown in the figure.

biometric pressure is collected and processed in order to enhance the visibility of the supply chain. HiKoB [80] collects real-time measurements such as temperature gradients within the road, current outdoor temperatures, moisture, dew and frost points from sensors deployed in roads and provides traffic management, real-time information on traffic conditions, and services for freight and logistics. Cantaloupesys [31] allows the user to keep track of stocks in vending machines remotely. Timely and optimal replenishment strategies (i.e. the elimination of unnecessary truck travel and smaller loads per truck) are determined from context information related to usage patterns.

Infrastructure and Safety: SmartStructures [173] collects data from sensors embedded within concrete piles in foundations which enables post-construction long-term load and event monitoring. Yanzi [199] is a solution that enables the user to monitor, maintain, and manage lifts, elevators, heating systems, energy consumption, motion detection, and surveillance. Context information is retrieved through sensors such as video, temperature, motion, and light. Engaugeinc [57] is a remote fire extinguisher monitoring system. Multiple sensors are used to collect context information that allows the user to determine when a fire extinguisher is blocked, when it is missing from its designated location, or when its pressure falls below safe operating levels. Alerts are sent out via email, phone, pager, and a software-based control panel.

Energy and Production: Wattics [192] is a smart metering solution that manages energy consumption at the individual appliance and machine level. Context information is used to understand usage pattern recognitions of each appliance through software algorithms which predict and load balance to reduce the energy cost. Sight-machine [172] continuously processes context data gathered from sensors, lasers, and network cameras, makes assessments in real time, and allows the user to stop problems before they happen with regard to industrial manufacturing machines and equipment.

Resources Management: Onfarmsystems [125] is an IoT solution designed to facilitate smart farming through accommodating increasingly complex and interconnected farming equipment. Context information such as energy, pesticide, mapping/ location, soil moisture, telemetry, weather, and monitoring are used to support efficient real-time decision-making. HeatWatch [63] is a cattle mon-

itoring solution that records the activities of each animal. Recorded context information includes such information as movement, time of day of the mount, and duration of the mount. Such information enables farmers to breed more cows and heifers earlier, obtain better results (more pregnancies), use less semen, spend much less time, and be more efficient. Motionloft [116] is a solution that monitors pedestrian and vehicle movements in real-time by collecting activity data. It enables boutique retailers, large chains, restaurants, and bars to understand the impact which vehicle and pedestrian traffic has on their revenue.

— **IoT Solutions Review.** A comprehensive review on IoT solutions is presented in [136]. Further, industrial IoT solutions are surveyed and analysed from context-aware perspective in [135].

1.4 The Problem


So far we explained what IoT is and what it could bring to our lives. Each of the IoT solution in the marketplace today is designed and developed to make our live much easier and convenient in some way.

Typically, each of these IoT solutions are designed to perform a single or limited number of tasks. We identify them as primary usage. For example, a smart sprinkler [127] may only be activated if the soil moisture level goes below a certain level in a garden. Further, smart plugs allow users to control electronic appliances (including legacy appliances) remotely or create automated schedules [26]. Undoubtedly, such automation not only brings convenience to the users but also reduces the resource wastage. For example, a smart sprinkler [127] may automatically creates optimal watering schedules, keeping its owner's lawn looking it's best. Such result may save an average of 35% on watering.

The data collected by each of these IoT solutions is used by themselves and stored in access controlled silos. Typically, data may either stored locally or within their respective cloud services. After the primary usage, data is either thrown away or locked down in independent data silos. The IoT solutions manufacturers and providers collect data through their products for number of reasons. They may collect data:

- In order automatically trigger actuations based on event.
- In order to visualise and present them to the IoT solution owners.
- In order to analyse data, identify trends / patterns / behaviours / habits, and provide recommendations / actionable advice to the IoT solution owners.
- In order provide recommendations to IoT solution owners through analysis of other similar IoT solution owners.

In summary, the ideology of IoT solutions marketplace is “*We (IoT solution providers) sell you (IoT solutions owners) the IoT solution. You install it at your place. You receive the benefits: 1) automation, 2) reduces wastage, and 3) actionable advice that will help you to change your bad / unhealthy / inefficient behaviours and habits. In return, we get your data so we can learn more about you. We can also learn to predict about other similar IoT solution owners. More we learn about you, better the service we provide to you.*” The question is: “IS THIS A FAIR DEAL..”?

 At the first sight, above approach (or the business model) looks fair and reasonable. However, there is a PROBLEM. We can also identify it as a WEAKNESS of IoT paradigm as well. Let us carefully walk you through the PROBLEM.

Let consider a smart home scenario as illustrated in Figure 1.13. *Jane* is a restaurant manager who works in different shifts. She lives alone in her own house. She has few different IoT products in her house. These products are manufactured by different companies and work independently. They independently bring different benefits to *Jane* (e.g. convenience and waste reduction through automation and efficient resource usage). Overtime, *Jane* has bought number of IoT solutions as follows.

- A context-aware thermostat (e.g., *Nest* [72]) that controls indoor temperature based on *Jane*'s preferences.
- A smart coffee machine (e.g., *Mr. Coffee Coffeemaker* [25]) that automatically brews coffee when she gets up in the morning so by the time she arrives in the kitchen coffee is ready for her.

- A smart activity monitor (e.g., *Fitbit* [61]) that monitors her exercise patterns, food intake, step counts, and fitness goals.
- A smart oven (e.g., *Maid* [166]) that knows what Jane likes to cook and how. It keeps track of what ingredients available at home, possible recipes, past meals and so on.
- A sleep monitoring solution (e.g., *Beddit* that tracks Jane's sleeping patterns, quality of sleep, heart rate and breathing.

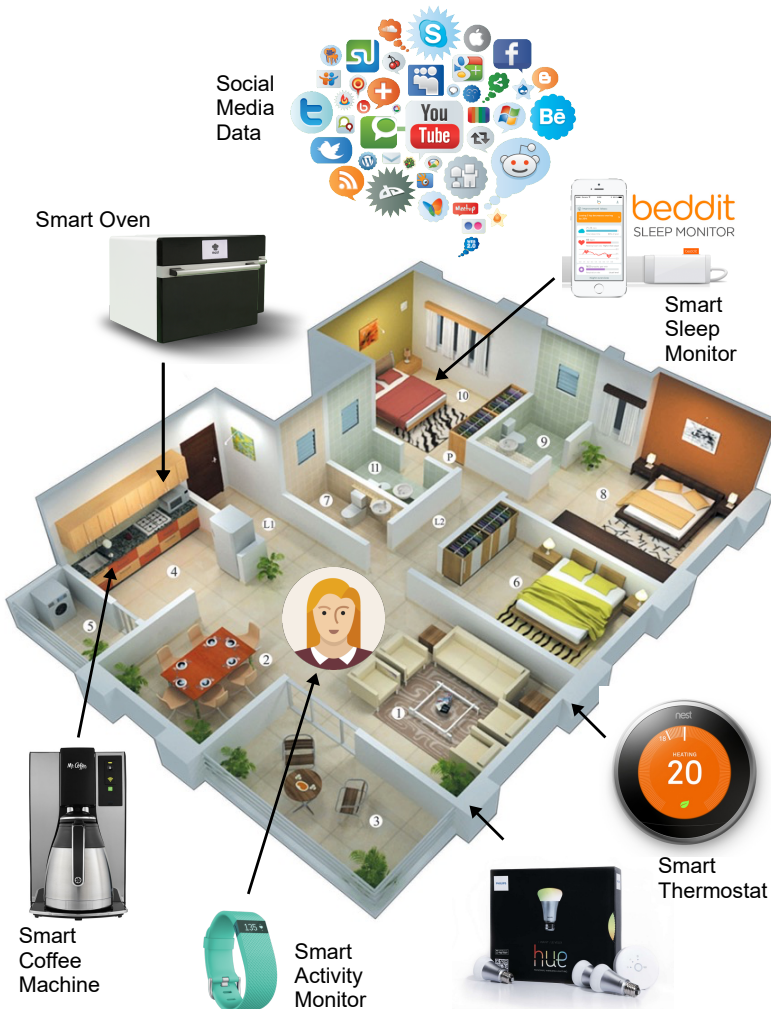


Figure 1.13: Jane's smart home augmented with multiple independent IoT solutions.

- A smart lighting system (e.g., *Meethue* [149]) that reacts to the context and can change its colours and brightness according to Jane's preferences, time / day / season, and activity (e.g. resident enters home) and is also sensitive to changes in weather during the day.

There are two problems in this current approach: 1) *Unification of IoT solutions* (i.e., interoperability) and 2) *Unification of data management* (i.e., sharing and control). The problem one, unification of IoT solutions, is reasonably being addressed by different parties using different approaches as discussed in the next section. The main problem in current the IoT paradigm is *unification of data management*. For the sake of completeness, we briefly discuss the problem of *Unification of IoT solutions*, before we discuss the major problem.

— **Unification of IoT solutions.** Interoperability is a critical factor to be successful in IoT domain. Consumers typically do not want to stick into a single manufacturer or a service provider. They always go for their preferences and for the factors which are more important to them such as cost, look and feel, customer service, functionality and so on. Interoperability among different IoT products and solutions allows consumers to move from one product to another or combine multiple products and services to build their smart environments as they like in a customize fashion. Further, interoperability [93] is also important to eliminate market domination of large companies that increase the entry barriers for the small IoT product and service providers.

In IoT marketplace, interoperability is mainly achieved using different methods: 1) partnerships among IoT Solutions developers, 2) open and close standards, and 3) adaptors and mediator services. We have seen that major industrial players in the IoT marketplace stablish strategic partnerships with each other in order to enable interoperability among their product and services. However, this is not a scalable strategy to widely enable interoperability among IoT devices. Similarly, large corporations such as Apple (e.g. *HomeKit* [13], *HealthKit* [12] and *Google* [68] are also attempting to build their own standards and interoperability certifications. This kind of interoperability may lead to corporate domination of IoT marketplace which could also hinder the

innovation by small, medium, and start-up companies.

To address the interoperability, there are some alliance have been initiated. For example *AllSeen Alliance* [100] has been created to promote some kind of interoperability among IoT consumer brands. *AllSeen* has developed a standard software platform called *AllJoyn* [100]. *AllJoyn* is a system that allows devices to advertise and share their abilities with other devices around them. A simple example would be a motion sensor

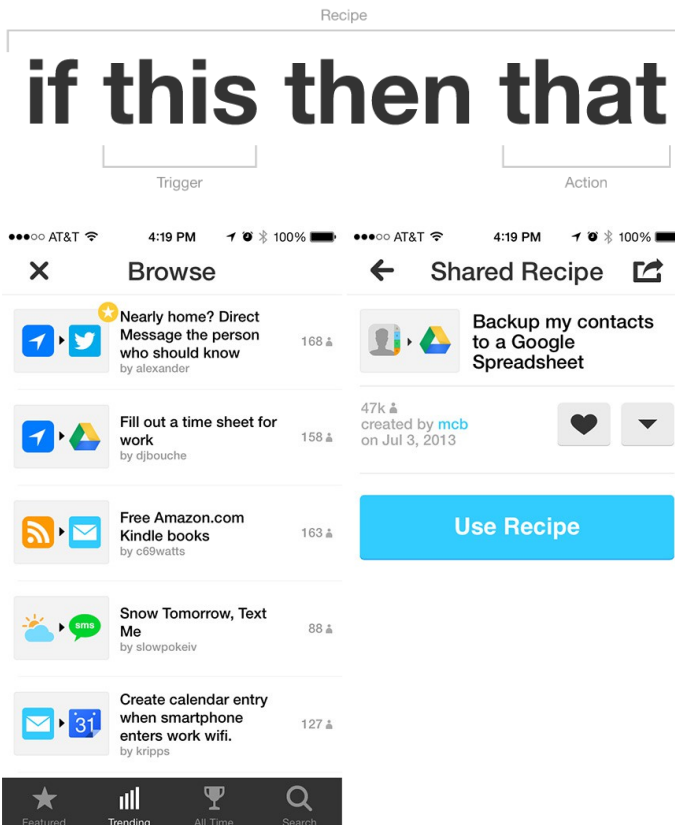


Figure 1.14: User Interface of IFTTT IoT service [85]:(a) shows how a recipe is structured using conditional statements and actions. (b) shows how recipes are built combining different triggers, actions, and channels.

letting a light bulb know no one is in the room it is lighting. This is the ideal approach the interoperability among IoT products. However, security [92] and privacy in this framework need to be strengthened to avoid using interoperability features to attack IoT products by hackers or evil parties.

Another approach to enable interoperability among different IoT solutions is through adapter services. For example, *IFTTT* [85], If This Then That, is a web based service that allows users to create powerful connections, chains of simple conditional statements. One simple statement is illustrated in Figure 1.14. Channels are the basic building blocks of *IFTTT*. Each Channel has its own *Triggers* and *Actions*. Some example Channels could be *Facebook*, *Twitter*, weather, *Android Wear*, and so on. Channel could be both hardware or software. Service providers and product manufactures need to register their services with *IFTTT* once. After that anyone interested can use that product or service as a channel to compose any recipe. Example list of channels are listed here: ifttt.com/channels. Personal recipes are combinations of a *Trigger* and an *Action* from active Channels. Example recipes are shown in Figure 1.14. For example, first recipe is defined to send a twitter message to a family member when the user reaches home. This kind of recipe can be used to offload responsibility from a child so the system automatically act on behalf of the child and sent a tweet to their parents. Context-aware recommendation can also help users to quickly configure channels in *IFTTT*. Context could be location, time, family members around, IoT products located near by and so on. Context-aware recommendation [51] can also be done by analysing similar users with similar smart environments.

Unification of data management

As explained earlier, the current IoT solutions mostly work in independent fashion with occasional interactions with each other through different unification approaches. Obviously, such unification brings new set of values to the IoT paradigm. For example, a smart microwave oven may talk to a smart activity monitor and a sleep monitor to decide what to cook on a particular day based on how much calories that Jane has burnt. As you can see, interactions and inter communication between IoT solutions can offer better value

for their owners. However, even with unification of IoT solutions, we are still missing a significant opportunity due to lack of a unified data management approach.

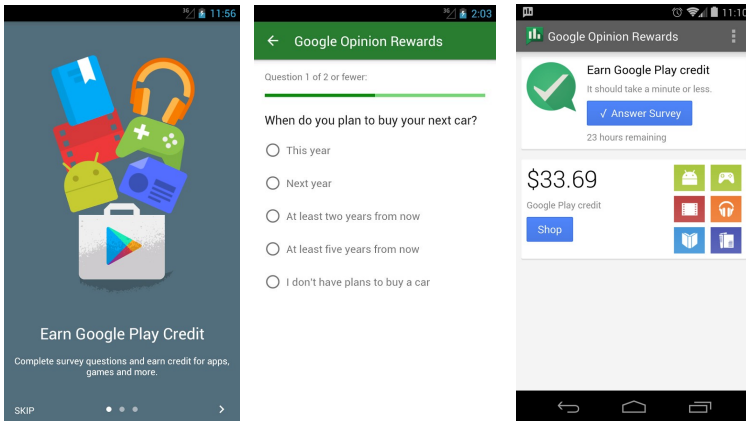
— **Weakness of IoT Ecosystem.** Currently, each IoT solution maintains its own data silo with limited access to external parties. There is a significant amount of knowledge hidden in these silos that can be used to improve our lives (including behaviours, habits, life patterns and so on) and reduce wastage through efficient resource consumption. To discover such knowledge and insights, it is essential to analyse data stuck in independent silos *together* in *large-scale*. However, within current IoT ecosystem, there is no way to manage (i.e., collect, store, share, analyse) data collected by different IoT solutions in a unified fashion. Further, data owners only have access to their own data which has little value when it comes to knowledge discovery. Finally, data owners do not know how to discover knowledge from raw data.

Let us now explain why the data collected by IoT solution has a significant value. Today, in a market driven society, personal information has a significant value. Today, business entities spend substantial amount of money to conduct market analyses and consumer surveys. A sample of 1,000 respondents, which would give a statistical accuracy of $\pm 3.1\%$ costs around \$8,000 [114]. Recently, different third party companies started offering consumer surveys on behalf of businesses. One such solution is Google Consumer Surveys [73]. Google Consumer Surveys allows businesses to target user groups with specific criteria and conduct the survey. Currently, one user response cost around \$0.10, 1/10th of the cost of similar quality research conduct using traditional methods. Even though such approaches have reduced the cost of surveys, they still have deficiencies such as latency, inaccuracies, and so on.

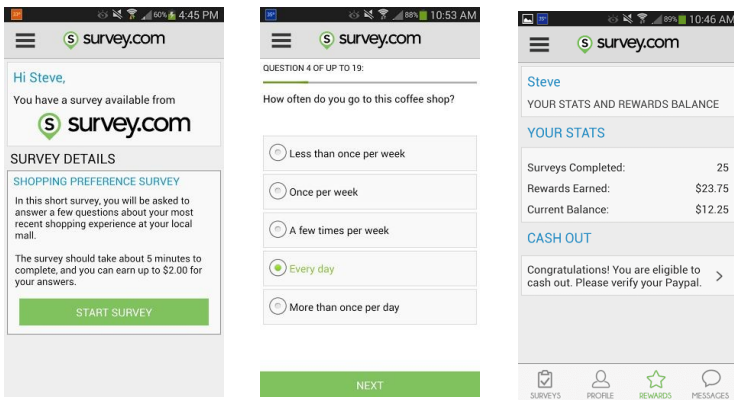
Taking such personal data collection approaches further, companies have introduces mobile app based services that pay money to their participant in return for providing personal opinions using multiple choice questions. For example, *Google Opinion Reward* [71] and *Survey.com* are applications that selectively present survey questionnaires to the users. Users get paid for answering questionnaire surveys. Sometimes, Amazon Mechanical Turk [10] is also used to gather user preferences and opinions. Reward is varied

based on the number of questions answered. Figure 1.15 shows a sequence of user interfaces that demonstrate how participants offer their personal opinions. It is important to note that users are getting paid just for answering surveys. Surveys like this have issues by their nature such as accuracy of the answers, difficulty in asking lot of questions (i.e., users get bored quickly despite being paid), difficulty in getting answers to data that users may not remember (e.g., how many times did the user drank coffee over the last month), personal biases, and so on.

 The data collected by IoT solutions are owned by IoT



(a) User Interface of the Google Opinion Reward



(b) User Interface of the survey.com

Figure 1.15: User interface of the personal opinion gathering apps

solution owners. For example, when *Jane* bought her smart coffee machine, *Jane* owns the data collected by the smart coffee machine.

We hope, by now, you agree with the fact that personal data has a significant value. In current IoT ecosystem, personal data collected by different IoT solutions stuck in separate data silos. More importantly, today, IoT solution owners do not have much control over their data and their data is locked in silos managed by products and services companies with limited access to them. IoT solutions may allow their owners to download data in some way with various kinds restriction (e.g., allows only to download last four weeks worth of data). However, there is no way to share such data with a third party. Downloading own personal data has no value to data owners unless there is a way to analyse and extract useful information out of them. It is very difficult and very time consuming task for a non technical data owner, even for a technical expert, to analyse and extract useful information from raw data. Additionally, each data owner will only have access to their own data from multiple IoT solutions. However, speaking from data analytics point of view, in order to conduct advance analytics and extract useful information, data from large number of data owners need to be processed and analysed together. From individual data owners point of view, this is not possible in current IoT ecosystem. The solution to this problem can be formulated by identifying its characteristics as follows.

- Data owner should have unrestricted access to the data collected by their IoT solutions.
- Data owner should be able to decide with whom they want to share their data under what conditions.
- The ideal solution should motivate data owners to share their data and receive some benefits in return.
- At the same time, it should also motivate third parties to offer data analytics services so even non technical data owners may benefit by sharing their data.

In the next chapter, we present the solution that has the above characteristics. We call it '*The Sensing as a Service model*'.



2. Sensing as a Service (S²aaS)

In the previous chapter, we introduced you to the Internet of Things paradigm and related concepts. We also explained the current IoT marketplace. Subsequently, we highlighted the main weakness of the Internet of Things paradigm. In this chapter, we introduce the solution, the Sensing as a Service model, to overcome the weakness. Throughout this chapter, we discuss the S²aaS ecosystem in detail.

2.1 Smarter Cities

In the previous chapter, we conducted our discussion from IoT point of view. Let us now introduce the concept of Smart Cities, more broadly smarter planet. The Internet of Things (IoT) [179] and Smart Cities (SC) [32, 190] are recent phenomena that have attracted attention from both academia and industry. While both ideas consolidate similar ideology, they have different origins. Both IoT and SC do not have clear and concise definitions due to their short history and broadness. Examining the origins of both ideas in brief allows us to understand their potentials.

Definition A smart city is an urban development vision to integrate multiple information and communication technology (ICT) and Internet of Things (IoT) solutions in a secure fashion to manage a city's assets – the city's assets include, but are not limited to, local departments information systems, schools, libraries, transportation systems, hospitals, power plants, water supply networks, waste management, law enforcement, and other community services [195].

The goal of building a smart city is to improve quality of life by using technology to improve the efficiency of services and meet residents' needs. ICT allows city officials to interact directly with the community and the city infrastructure and to monitor what is happening in the city, how the city is evolving, and how to enable a better quality of life. Through the use of sensors integrated with real-time monitoring systems, data are collected from citizens and devices - then processed and analyzed. The information and knowledge gathered are keys to tackling inefficiency.

As you may observe, IoT is primarily driven by technological advances, not by the applications or user needs. In contrast SC [37] originated to solve the problems in modern cities. As a result of rural migration and suburban concentration towards cities, the urban living has become a significant challenge to both citizens and to the city governance. Waste, traffic, energy, water, education, unemployment, health, and crime management are some of the critical issues [178]. SC are expected to address these challenges efficiently and effectively using information and communication technologies (ICT). By definition, Smart Cities have six characteristics: smart economy, smart people, smart governance, smart mobility, smart environment and smart living [65]. As illustrated in Figure 2.1, SC and IoT, which have different origins, are moving towards each other to achieve a common goal. We believe that the Sensing as a Service model resides in between these two with many other technological and business models.

It is important to understand that data is the key in any Smart City solution. In order to address critical challenges in different aspects (e.g., water, air, living spaces, parking, and so on) of modern cities, data need to be collected and analysed in large scale. In order to perform large scale data analytics towards building smart

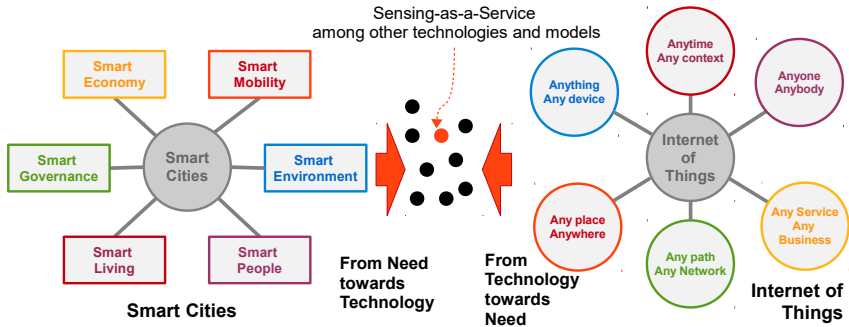


Figure 2.1: Relationship among S²aaS model, SC and IoT

city solutions, there are three important ingredients that need to be put together: 1) data, 2) computation, and 3) analytics.

Building analytics is not only a scientific and engineering task but also a creative task [144]. It is very inefficient to hand over the responsibility of building analytics into few large companies or groups. Ideally, anyone with some data science capabilities enriched by creativity should be able to develop novel data analytics solutions that would address smart city challenges. However, collecting data could be expensive and time-consuming. Further, most of the individuals and groups who are interested in building smart city solutions do not have access to large volumes of data or computational infrastructure.

Therefore, the only way to democratize both data and computational capabilities is to follow the path of *Everything as a Service* (XaaS) [22]. Such an approach will motivate a large number of capable individuals and small groups to engage in building analytics and open up a lot of opportunities and a creative IoT solutions marketplace.

2.2 Everything as a Service

Everything as a Service (XaaS) [22] is a category of models introduced with cloud computing [132]. Similar to IoT, cloud computing also has a short history. It became popular with a number of industry initiatives such as Salesforce.com (1999) and Amazon Web Service (2002). The basic idea behind cloud computing is to concentrate resources such as hardware and software into few physical locations and offer those resources as services to a large number of consumers

who are located in many different geographical locations around the globe over the Internet in an efficient manner. There are three major service models that are closely bound to cloud computing from its initial stage: infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS), and software-as-a-service (SaaS). The commonality among these models is that they all provide resources as a service. With the popularity of these models, several similar type models are also proposed. The service models offered in cloud computing are discussed in [204] with popular industry based examples.

Let us briefly discuss the reasons behind the success of everything as a service model in the cloud paradigm. One major reason is the cost effectiveness. XaaS model promotes the ‘*pay as you go*’ method or in other terms ‘*pay only for what you use*’. This allows the consumers to consume a service from a service provider by paying only for the amount of resources they use. This is an efficient way compared to the traditional methods of consuming resources where consumers need to buy resources in predefined discreet quantities with higher expenses. For example, consider a retail online business which has peak and off-peak seasons.

In traditional method, the business has to buy significant amount of compute servers (and other resources) to facilitate the customer needs during the peak season. However, these resources become idle during the off-peak season which makes the business process inefficient. In XaaS, online retail applications are hosted in servers facilitated by cloud service provider where the business is only required to pay for the resource it consumes. This model works similar to the utility services such as electricity. Further, cloud computing service models provide many other benefits such as business agility, scalability and elasticity, reliability, green initiatives, less maintenance work including backup and disaster recovery. Ultimately, XaaS allows businesses to focus more on core competency and innovation instead of ICT [106]. As we later discussed in this chapter, the S²aaS model follows the ideology of XaaS where it makes data available to the interested parties on demand.

Further explanation on characteristics, features and benefits of cloud computing are presented in [132, 160].

2.3 Sensing as a Service Model (S²aaS)

Previously, we introduced the S²aaS model as a solution based on IoT infrastructure. It has the capability to address the challenges in Smart Cities. Today, many everyday objects are embedded with sensors though the usage is restricted to the object itself. Let us discuss the S²aaS model and architecture in detail. As depicted in Figure 2.2, the S²aaS model consists of four conceptual layers:

1. Sensor Data Owners
2. Sensor Data Publishers
3. Extended Service Providers
4. Sensor Data Consumers

! It is important to note that sensors does not necessary means physical sensors but also virtual sensors. In S²aaS model, any source that generates data can be considered as a virtual sensor. For example, weather APIs, quantified self apps (e.g. Lifesum [99]), social media accounts, and man more can be considered as virtual sensors.

In this section, we explain the S²aaS model in a generic conceptual form. In Section 2.5, we present a real world scenario based on this model. At the end of Section 2.5, we map the real world scenario into the conceptual model in order to provide a practical understanding.

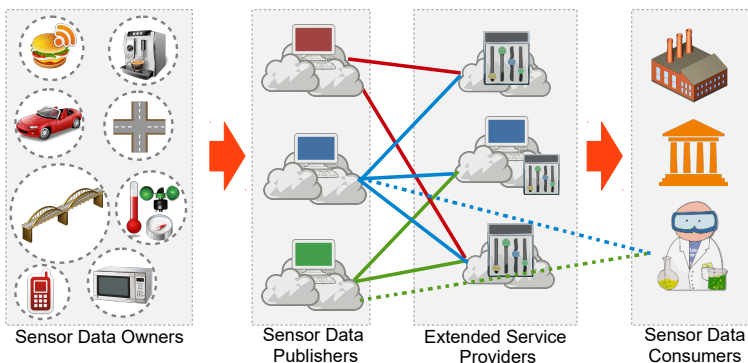


Figure 2.2: The Sensing as a Service model

1) Sensor Data Owners Layer

This layer consists of sensors and sensor data owners. A sensor is a device that detects, measures or sense a physical phenomenon such as humidity, temperature, etc. [5]. Multiple sensors can be attached to an object or device. For example, microwaves or coffee machines may have sensors that can be used to detect events (e.g. the number of times it is used per day and related context information). Such information can be used to understand user behaviour and user preferences more accurately. A road may have sensors that can detect the weather and traffic conditions. Today, large varieties of different sensors are available. They are capable of measuring a broad range of phenomena [98]. Further, they have the capability to send sensor data to the cloud. On the other hand, a sensor owner has the ownership of a specific sensor at a given time. Ownership may change over time. We discuss data ownership in Section 2.4.

2) Sensor Data Publishers Layer

This layer consists of sensor data publishers (SP). The main responsibility of a sensor data publisher is to detect available sensors, communicate with the sensor owners, and get permission to publish the sensors in the cloud. Sensor data publishers are separate business entities. When a sensor owner registers a specific sensor, SP collects information about the sensor availability, owner preferences and restriction, expected return, etc. All this information needs to be published in the cloud. Once the registration is done, a SP waits until a sensor consumer makes a request. When a SP receives such a request, it forwards all the details including the offer to the corresponding sensor owner(s) to accept or reject. If the sensor owner accepts the offer, the corresponding sensor data consumer will be able to acquire data from that sensor through the SP during the period mentioned in the agreement (offer). The same interaction explained above can take place between SPs and ESPs. SPs entirely depend on the payments (e.g. commission) receives from sensor owners, sensor data consumers or both.



In the next chapter, we introduce you to *Data Markets*. A Data Market is a type of sensor data publisher.

3) Extended Service Providers Layer

This layer consists of extended service providers (ESP). This layer can be considered as the most intelligent among all the four layers which embed the intelligence to the entire service model. The services provided by ESPs can be varied widely from one provider to another. However, there are some fundamental characteristics of ESPs. To become an ESP, they have to provide value added services [117] to the sensor data consumers. However, in some instances a single business entity can perform both sensor data publisher and extended service provider roles. Each SP has access (only) to the sensors which are registered with it. When a sensor data consumer needs sensor data from multiple sensors where each sensor has been registered with different SPs, ESPs can be used to acquire data easily. ESPs communicate with multiple SPs regarding sensor data acquisition on behalf of the sensor data consumer.

The ESPs depend on the payments (e.g. commission) similar to SPs. ESPs receive payments for the value added service they provided to their customers (i.e. sensor data consumers). An example value added service can be selecting sensors based on customer's requirements [140]. Customers will provide their requirements in high-level (e.g. measure environmental pollution in Canberra) instead of selecting the sensors by themselves. In return, ESP will select the appropriate sensors (e.g. pH, temperature, humidity, CO₂, etc.) located in Canberra.

4) Sensor Data Consumers Layer

This layer consists of sensor data consumers. All the sensor data consumers need to register themselves and obtain a valid digital certificate from an authority in order to consume sensor data. Some of the major sensor data consumers would be governments, business organizations, academic institutions, and scientific research communities. Sensor data consumers do not directly communicate with sensors or sensor owners. All the communication and transactions need to be done through either SPs or ESPs. If a sensor consumer has the required technical capability, they can directly acquire data from sensor data publishers. However, this could be very challenging. For example, selecting which sensors to use out of billions of sensors available could be an overwhelming task [119, 120, 121, 138, 141, 147]. Further, sensor data consumers may need

to communicate with multiple sensor data publishers to acquire the required data. However, the cost of sensor data acquisition would be lower as they are not required to pay for ESPs' value added services. Scientific research communities may be interested in such methods.

The sensor consumers with less technical capabilities and expertise can acquire required sensor data through ESPs where most of the difficult tasks such as combining sensor data from multiple sensor data publishers and selecting appropriate sensors based on the consumer requirements are handled. Further, sensor consumers can register their interests with both SPs, and ESPs. For example, they can express their interest by using a number of constraints. A coffee manufacturer who expects to start its business in Canberra may be interested to access the sensor data produced by coffee machines located in Canberra for a fee. Depending on the expression of interest, ESPs/SPs will notify the coffee manufacturer when a matching deal is available. In simple terms, sensor owners define what they are expecting as return for the sensor data from one end of the S²aaS model. On the other end, sensor consumers define what kind of sensor data they want and how much are they willing to pay (offer). SPs and ESPs are platforms that enable these transactions (deals) to take place. The S²aaS model shares common characteristics of an auction [203].

2.4 Data Ownership

We classify sensors into four categories based on ownership as depicted in Figure 2.3:

1. Personal and Household
2. Private Organizations and Places
3. Public Organizations and Places
4. Commercial Sensor Data Providers



Sensor owners can also be considered as data owners in most of the situations unless there is an explicit agreement says otherwise. Therefore, in this book, we assume sensor owner is same as sensor data owner and the IoT solution owner.

1) Personal and Household

All personal items, such as mobile phones, wrist watches, spectacles, laptops, soft drinks, food items and household items, such as televisions, cameras, microwaves, washing machines belong to the personal and household category. In simple terms, all items (and also all sensors) not own by private or public organizations belong to this category. We expect that all of these items (also called things, objects, and devices) would be equipped with sensors in the future.

2) Private Organizations and Places

The private organizations and places category consists of all items own by private organizations. The same items we listed under personal and household category can be listed under here as well depending on the ownership. If a private company owns a coffee machine and a microwave which cannot be attributed to a single person, then those items can be listed under this category. Therefore, the private business organization has the right to take the decision whether to publish the sensors attached to those items to the cloud or not. As another example, if a private business organization owns a sport complex or a hospital, all the sensors deployed in those properties are also owned by them. When a company manufactures and sells a product that comprises sensors, the ownership get transferred to that customer. As a result, a customer will decide whether to publish those sensors in the cloud or not. The same process will occur when physical properties (e.g. land, building) are sold from one party to another. This category would be the second largest sensor owner after the personal and household category.

3) Public Organizations and Places

The public organizations and places category is similar to the private organizations and places category we discussed above. However, this category also includes public infrastructure such as bridges, roads, parks, etc. All the sensors deployed by the government will be published in the cloud depending on government policies.

4) Commercial Sensor Data Providers

Commercial sensor data providers are business entities who deploy and manage sensors by themselves by keeping ownership. They earn by publishing the sensors and sensor data they own through sensor data publishers. They may deploy sensors across all places



Figure 2.3: Sensor classification scheme based on ownership

such as households, private and public owned properties depending on demand and strategic value by also complying with legal terms. Mostly, they will focus on public and private places. They will also make a payment to the property owner as an exchange for giving permissions for sensor deployment. For example, commercial sensor data provider may deploy sensors in a children’s park owned by state government (under government permission) to detect motion and measure the micro climate (e.g. temperature, humidity, wind speed, wind direction). Such monitoring allows to detect and predict potential crowd movements. The sensor data that can be used to predict such movements can be sold to sensor data consumers such as mobile stall businesses and children’s product retailers who may be located in nearby areas.

A sensor owner makes the final decision on whether to publish the sensors he owns in the cloud or not. If the owner decides not to publish, no sensor data publisher would be able to get access to those sensors which significantly protect the security and privacy of the sensor owner. If the sensor owner decides to publish the sensors he owns, he needs to register himself with a sensor data publisher. Sensor owners can define restrictions and conditions such as who can request permission and the expected return (offer). It is important to note that each sensor may send data to a different SP in the cloud (similar as we use Internet service providers). However, a single sensor only sends data to a single SP (in order to save energy). Data will be shared between SPs if necessary depending on consumer requirements. Even though all four categories perform the same task (i.e. sensor deployment and publication), the deci-

sion making processes can be quite different especially in term of objectives, financial goals, approval processes, privacy and policy concerns.

2.5 Motivational Use Cases

A futuristic scenario can be used to explain the S²aaS model. The scenario illustrated in Figure 2.4 is based on smart home domain which also plays a significant role in the Smart Cities. Our intention is to highlight the interactions between different parties explained earlier in high-level.

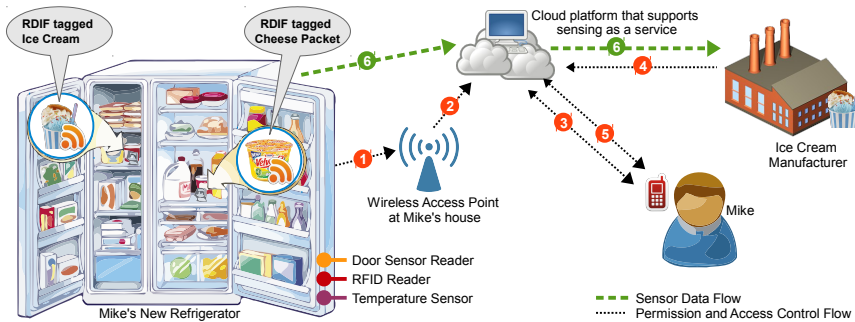


Figure 2.4: A futuristic scenario that explains the interactions in S²aaS model

Mike bought a new refrigerator for his new home. He brought it home and plugged it to the power. The fridge automatically identifies the availability of Wi-Fi in the house as shown in step (1). Further, the refrigerator communicates with a sensor data publisher and informs about its presence by providing information such as the available sensors (e.g. RFID reader, temperature, door sensors) as shown in step (2). Next, in step (3), the SP communicates with *Mike* to check whether he likes to publish the sensors attached to the refrigerator in the cloud (step 3). We assume that *Mike* has already registered with the SP in a previous transaction. *Mike* is allowed to define which sensors to publish, what kind of consumers are allowed to bid, and what kind of return (fee or any other offer) is expected. Later, *Mike* receives an email from a company called *DairyIceCream* (via a SP called *EasySensing*), an ice cream manufacturer, with an offer as shown in step (4). *DairyIceCream* is

interested to have access to the RFID reader and the door sensor attached to the freezer in *Mike's* refrigerator. As a return, *DairyIceCream* is willing to offer either 3% discount on every product purchased from *DairyIceCream* or a monthly fee of \$2. As *Mike* likes *DairyIceCream* products, he agrees to the 3% discount offer instead of the monthly fee as shown in step (5). A week later, *Mike* receives an email from a company called *ProductiveAnalytics* which has been sent on behalf of the *GoldenCheese* company, a cheese manufacturer, with an similar offer. This request also comes through *EasySensing*. However, the offer is either 4% discount on every product purchase by *GoldenCheese* or a monthly fee of \$1. As *Mike* does not like *GoldenCheese* products, he decides to accept the monthly fee option.

Scenario from S²aaS Model Perspective

Previously, we explained the S²aaS model in a generic perspective and now we describe it from the above mentioned scenario perspective. In the scenario, *Mike* is the sensor owner. Therefore, he and his sensors represent the *sensors data owners* layer. Further, in ownership categorization, *Mike* represents the *Personal and households* scheme. Both the *DairyIceCream* and *GoldenCheese* companies represent the *sensor data consumers* layer. *EasySensing* is a SP who enables the communication and transactions between *Mike* and the *DairyIceCream*. *EasySensing* is responsible for matching the sensor owners expectations with the requirements of sensor data consumers. *DairyIceCream* retrieves the data from *EasySensing* directly and conducts the data analysis with the help of in-house experts. *ProductiveAnalytics* is an ESP who works on behalf of *GoldenCheese*. *GoldenCheese* has hired *ProductiveAnalytics* to perform the data analysis as they do not have the required technical skills within the company. *ProductiveAnalytics* collects the data by handling all the deals and transaction with the sensor owners though their partner SPs.

2.6 Sensing as a Service in Action

In the previous section, we discussed a scenario related to the smart home domain in S²aaS perspective. This section presents three different use case scenarios that explain different aspects of the sensing as a service model: (1) waste management, (2) smart agriculture,

and (3) environmental management. All three scenarios share common a sets of characteristics as well as few unique characteristics. Waste management has a direct impact on cities. Environmental management has direct, indirect, and long term impact on the entire human life-cycle both in urban and rural living. Further, smart agriculture makes indirect impact on sustainability towards SC.

Waste Management

Waste management is one of the toughest challenge that modern cities have to deal with. Waste management consists of different processes such as collection, transport, processing, disposal, managing, and monitoring of waste materials. These processes cost significant amount of money, time, and labour. Optimizing waste management processes help to save money that can be used to address other challenges that smart cities need to deal with. In Figure 2.5, we illustrate how the S²aaS model works in the waste management domain. In a modern smart city, there are several parties who are interested in waste management (e.g. city council, recycling companies, manufacturing plants, and authorities related to health and safety). Instead of deploying sensors and collecting information independently, the S²aaS model allows all the interest groups to share the infrastructure and bare the related costs collectively. The most important aspect of such a collaboration is the cost reduction that individual groups need to spend otherwise. All the interested parties can retrieve and process sensor data in real time in order to achieve their own objective. The cost depends on the data requirement of the interest group.

For example, a city council may use sensor data to develop optimized garbage collection strategy, so they can save fuel cost related to garbage trucks. Additionally, recycling companies can use sensor data to predict and track the amount of waste coming into their plants to be processed so they can optimize their internal processes. Further, health and safety authorities can monitor and supervise the waste management process without spending substantial amount of money for manual monitoring inspections. The phenomenon of sharing sensor data using a S²aaS model creates a synergy effect (i.e. interaction of multiple elements in a system to produce an effect greater than the sum of their individual effects). The S²aaS model ensures the long term sustainability of the IoT infrastructure.

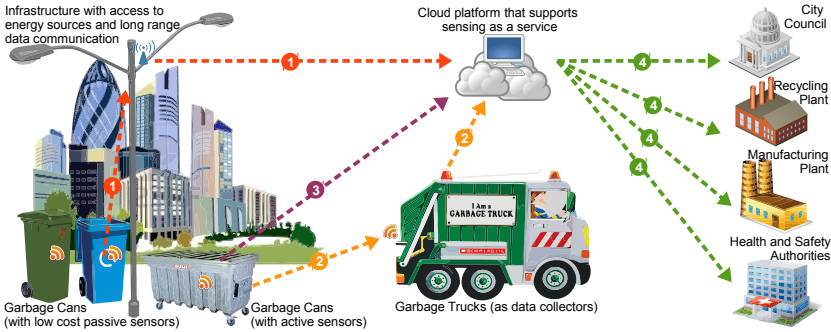


Figure 2.5: Efficient waste management in Smart Cities supported by the S²aaS model

Let us discuss how this technology can be used to support the S²aaS model in financially viable manner. In order to perform waste management, different types of sensors need to be deployed in different places such as garbage cans and trucks. These sensors need to detect information such as the amount of garbage, types of garbage, and so on. As we have depicted in Figure 2.5, direct and indirect communication strategies can be used to collect and communicate sensor data to the cloud. Sensors with energy harvesting capabilities are important in this domain [8]. As represented in step (1) in Figure 2.5, low powered [191] and low capable sensors can be used to sense and data can be uploaded to the cloud with the help of nearby infrastructure (e.g. through communication devices attached to street lights or similar infrastructure that have access to rich energy sources and communication capabilities). Additionally, when long range communication is not available, data can be uploaded to the cloud with the help of auto-mobiles, as depicted in step (2) in Figure 2.5, such as garbage trucks, city council vehicles, buses that operate in the areas and so on. Furthermore, both active and passive sensors can be used to sense the environment [34]. Direct communication can be done via technologies such as 3G which makes this approach less dependant on third parties (as depicted in (3) in Figure 2.5).

Smart Agriculture

Currently, the authors are actively involved in designing and developing open platforms for sensor data collection, processing and

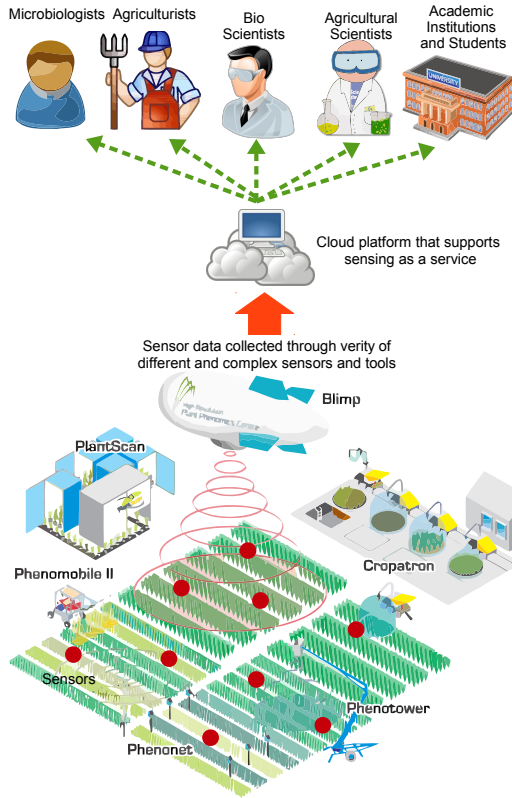


Figure 2.6: Efficient and effective collaborative agricultural research supported by S^2aaS model

sharing in the domain of agriculture through two projects: *Phenonet* [41] and *OpenIoT* [126]. In this scenario, the general public is not directly involved as in the smart home domain. In Figure 2.6, we illustrate how the S^2aaS model works in the smart agriculture domain. Agriculture is an important part of smart cities as it contributes to the food supply-chain that facilitates a large number of communities concentrated into cities.

The S^2aaS model allows to conduct scientific research and exploration more efficiently and effectively. Further, it opens up different research opportunities which are unlikely to occur in a traditional research model. Let us explain the *Phenonet* project in details and the applicability of the S^2aaS model towards agricultural research. *Phenonet* describes the network of sensors collecting information

over a field of experimental crops. Researchers at the High Resolution Plant Phenomics Centre are testing a network of smart sensor nodes able to monitor plant growth and performance information and climate conditions. Even though the main research goal of deploying sensors and collecting data is to understand plant growth under different climate conditions, the same set of sensors can be utilized to perform a verity of different research activities in different domains. The data can be shared among different research organizations and institutions located around the world. Due to limited funding, most of these research institutions may not be able to maintain large scale sensor deployments (e.g. academic institutions, specially in developing countries). However, the S²aaS model allows all these interest groups, who are unable to set-up their own sensor deployments, to perform research using actual data with significantly less costs. Further, the S²aaS model creates opportunities across different domains. For example, the above mentioned sensor data can be used to understand pest control and related phenomenon. Additionally they can be used to understand soil conditions where bio-scientist may be interested. More importantly, the S²aaS model allows researchers to share resources across borders and understand phenomenon which are not available in their own countries.

Environmental Management

This domain has the unique ability of utilizing existing sensors that are deployed for different reasons. Most of the sensors used in environmental monitoring are commonly used in other domains such as climate, wild fire detection, and structural health monitoring. Using the S²aaS model, interest groups can acquire relevant sensor data without deploying sensors by themselves. Further, environmental management is a large domain where a single organization cannot deal with (e.g. wild fire). A model like S²aaS stimulates innovative solutions that use the same data but produce different results using different processing and analysing techniques (e.g. prediction, visualization, simulation). As we discussed in Section 2.3, ESPs can help the sensor data consumers to orchestrate existing services into different data processing [162] and analysis work-flows [36].

2.7 Advantages and Benefits

Some of the major advantages and benefits in the S²aaS model are discussed below:

Built-in cloud computing

It is modelled around cloud computing. Therefore, it inherits all the benefits of the fundamental cloud computing models such as IaaS, PaaS, and SaaS. Scalable and widely accessible processing and storage resources are available to facilitate S²aaS software platforms (SPs and ESPs). Sensor data consumers only need to pay for the data they use. Therefore, the cost of data acquisition reduces significantly due to sharing, participatory / crowd sourcing, and reusing nature (i.e. sense once and use by many). The workload is distributed among different players in the model. This enables rapid deployment of sensors across wider geographical locations that capture various phenomena.

Sharing and reusing

In traditional methods, each party (group or person) who wants to collect sensor data needs to visit the field and deploy the sensors manually by themselves. Further, there is no easy way to share sensor data collected by one party with others. S²aaS is a model that stimulates by concept of sharing. In simple terms, if someone has already deployed the sensors, others can have access to them by paying a fee to the sensor owner. One of the major arguments that could arise regarding S²aaS model is that “*How to convince a manufacturer to embed sensors and communication capabilities into devices we use in everyday life (e.g refrigerator in the use-case presented in Section 2.5)*”. This question can be answered in two different perspectives.

First, IoT envisions to have sensor embedded into objects around us. The goal of IoT is to allow devices to communicate with each other. Naturally, such a goal forces next generation devices to be embedded with rich sensing and communication capabilities. Therefore, the motivation is given to the manufacturers not by the S²aaS model but the vision of IoT. The S²aaS model is designed to provide incentives to users which motivate them to purchase next generation devices that supports both IoT envisioned interactions as well as the S²aaS model. The additional cost that contributes to

increase the prices of the devices (due to embedding rich sensing and communication capabilities) can be easily covered by participating in the S²aaS model itself. Even today, state of the art devices such as refrigerators and televisions comprise communication and sensing capabilities.

Reduction of data acquisition cost

Due to the shared and collaborative nature, data acquisition cost will be reduced significantly. Such a sustainable business model stimulates more and more sensor deployments. Further, technological advances and higher demands allow to produce sensors in mass volumes using cheap materials by reducing the cost per unit. Further, this helps to collect data from sensors which was impossible previously.

Collect data previously unavailable

This model allows to collect sensor data which is impossible to collect using traditional non-collaborative methods. This business model promotes and stimulates the sensor deployments by companies at commercial level. As we explained earlier in Section 2.3, dedicated business entities will deploy sensors in public places such as parks and bridges so government authorities can have access to those sensors by paying only for the data they need in real-time or archived. Today business entities spend substantial amount of money to conduct market analyses and consumer surveys. A sample of 1,000 respondents, which would give a statistical accuracy of +/-3.1% costs around \$8,000 [114]. Recently, different third party companies started offering consumer surveys on behalf of businesses. One such solution is Google Consumer Surveys [73]. Google Consumer Surveys allows businesses to target user groups with specific criteria and conduct the survey. Currently, one user response cost around \$0.10, 1/10th of the cost of similar quality research conduct using traditional methods.

Even though such approaches have reduced the cost of surveys, they still have deficiencies such as latency, inaccuracies, and so on. In the S²aaS model, all the data is directly coming from the sensor without user intervention. This also helps to reduce the cost of data acquisition. Due to privacy concerns it is important to anonymise the sensor data collected. We discuss privacy matters later. In the

smart home scenario we discussed in Section 2.5, we explained how a single sensor attached to a refrigerator, and cheap passive RFID tags attached to consumer products, produce valuable information of consumer behaviour that can be used by thousand of companies. This drastically reduces the consumer survey cost as well as pay off the cost of attaching sensors to the products.

Innovations

Due to a reduction in sensor data acquisition cost, larger number of interest groups will be able to access to them. Further, the availability of sensor data which was not available previously can also significantly stimulate innovation . S²aaS model itself provides space for innovation in the ESP layer. The cloud-based value added services provided in the ESP layer allows the sensor data consumers to achieve their objective easily and faster in many different application domains.

Applications

Easily accessible sensor data allows government authorities, academia, research institutions, and businesses to address different challenges in Smart Cities such as traffic, energy, water, education, and unemployment, health, and crime management. For example, accurate data on energy consumption in a city allows managing electric grids efficiently by analysing and predicting energy consumption behaviours, patterns, future trends, and needs.

Real-time data for decision making and policy making

This model enables collecting sensor data in real-time, from a variety of different domains, which facilitates the decision making processes. Such data is expensive to collect and usually unavailable for decision making in traditional sensor deploying environments. For example, data collected from sensors deployed in vehicles and roads allow the authorities to monitor and manage traffic in real-time. Further, sensor data collected over a period of time (archived) can be used to make policy decisions. For example, traffic data over a period on a specific city will help a city governance to make long term strategic decisions such as whether to invest on a tram service across the city or not. In addition to the points discussed above, there are many other direct and indirect benefits in the S²aaS model.

Direct and indirect benefits

The S²aaS model creates a win-win situation for all the parties involved. Based on the scenario we presented in Section 2.5, *Mike* (sensor owners' perspective) is getting a return (a valuable offer). In *DairyIceCream* perspective, now they have real-time data about product consumer behaviour (e.g. when *Mike* eats ice cream, how frequent, whether *Mike* use substitutions and so on). Therefore, *DairyIceCream* is no longer required to conduct manual surveys and market analyses.

Privacy preservation

Finally and more importantly, this model provide complete control of the privacy of sensor owners in their own hands. The final decision of whether to publish their sensors or not is taken by the sensor owners. It allows the sensor owners to control and protect their privacy. Additionally, the S²aaS model needs to be supported by anonymization techniques. For example, lets consider security and privacy challenges [64] related to the smart home scenario we presented in Section 2.5. During the configuration process, it is important to identify the information and preferences related to *Mike*. In order to protect the privacy of the users, SPs and ESPs should not provide personal information to the sensor data consumers. Such approach helps to preserve user privacy. Additionally, once the deal between the sensor owner, sensor consumer and the sensor provider is done, data retrieves from *Mike's* sensors should be explicitly anonymized. It is important to develop new algorithms and security devices that can anonymize sensitive information (such as exact location).

2.8 The solution: S²aaS

In section 1.4, we explain the main weakness in IoT ecosystem. So far until now, we explain the S²aaS model in detail as a potential solution to address that weakness. Let us recall what we mentioned about IoT ecosystem.

— **Weakness of IoT Ecosystem.** Currently, each IoT solution maintains its own data silo with limited access to external parties. There is a significant amount of knowledge hidden in these silos

that can be used to improve our lives (including behaviours, habits, life patterns and so on) and reduce wastage through efficient resource consumption. To discover such knowledge and insights, it is essential to analyse data stuck in independent silos *together* in *large-scale*. However, within current IoT ecosystem, there is no way to manage (i.e., collect, store, share, analyse) data collected by different IoT solutions in a unified fashion. Further, data owners only have access to their own data which has little value when it comes to knowledge discovery. Finally, data owners do not know how to discover knowledge from raw data.

— **Strength of S²aaS Ecosystem.** The S²aaS model, which would be built on existing IoT infrastructure, creates a data sharing architecture that allows data owners and data consumers to share and trade data for mutual benefits [139]. In S²aaS model, data owners have the full control of their data and they get to decide when and with whom they want to trade their data under what conditions. It creates a win-win situation for both data owners and data consumer, and encourages both parties to engage in S²aaS ecosystem. Further, due to data sharing nature, data consumers can acquire IoT data from a larger number of data owners through the data trading process, so they can use data analytics at scale to discover useful knowledge and insights. Finally, with the support of SPs and ESPs, data owners do not need to know how to analyse data or discover knowledge. Data consumers (i.e. third party services) will do it for them.



3. The Ecosystem

In the previous chapter, we introduce you to the S²aaS model, in a more conceptual and generic way, as a solution to address the major weakness in the IoT paradigm. This chapter takes the discussion further by exploring the S²aaS model in more practical point of view. Specifically, we demonstrate how S²aaS model can be deployed, configured, and used by everyday users in a smart home environment. In this discussion, we primarily focus on two main stakeholders: 1) *Data Owners* and 2) *Data Consumers* and their interactions with the S²aaS model.

- ❗ It is important to note that S²aaS model is still in its *infancy* where real world deployments and adoptions are yet to be seen. Therefore, most of the ideas and concepts that we discuss in this chapter does not exist in the real world. Our goal is to demonstrate how S²aaS model can be built by using and, but also more importantly, extending existing IoT solutions. As a result, we will highlight lots of research challenges and gaps in the exiting IoT marketplaces where we invite you all to address them.

3.1 IoT Solutions and Infrastructure

The S²aaS model is expected to be built on top of the typical IoT infrastructure. Therefore, the first step towards engaging with the S²aaS model is to acquire IoT solutions and build the infrastructure. We discussed IoT solutions marketplace earlier in Section 1.3. There are many different types of IoT solutions. Some solutions are more generic in nature and some are designed to perform specific tasks [135, 136]. For example, IoT solutions such as Fitbit [135] focuses on tracking users' activity, exercise, food, weight and sleep towards improving users' health. On the other hand, IoT solutions such as *SmartThings* [136] focuses on providing a generic platform that different types of products can be connected to them.

— **Motivation to buy IoT solutions.** In most cases, S²aaS model does not expected to become the motivational factor for anyone to buy IoT solutions. Following reasons are by far the most critical motivational factors [55].

Efficiency: *With one button or smart-phone application, you can control multiple devices or systems. That means you can easily set back the thermostats and turn off the lights simultaneously. You'll also get out of the house faster and save electricity.*

Convenience: *Having a smart home allows you to manage several electronic devices and/or systems from across the house or across the world. Draw the shades, turn on lights, and check in on security; having that sort of convenience alone is enough to inspire many people to automate.*

Comfort: *Having a smart home allows you to maximize comfort, from temperature to lighting to entertainment. Everything is at your fingertips!*

Peace of Mind: *A smart home system can prevent potentially bad things from happening. Of course, you can use a smart home system to monitor cameras, doors, and windows, but also items such as water leak sensors. You can even check in from a smart phone to make sure the garage door is closed and the TV is off.*

! People who are buying IoT solutions are referred to as ‘buyers’. However, once they started engaging with the S²aaS model, they are referred to as ‘data owners’.

There are number of decisions that need to be taken by the buyers when purchasing IoT solutions. First, they need to decide what types of IoT solution is required in a given circumstance (i.e., *what is the requirement they are trying to fulfil by purchasing an IoT solution?*). Some example types are smart coffee machines, smart activity monitors, smart sleep monitors, smart baby monitors, smart lighting, smart irrigation, and so on. Next, the buyers need to choose which IoT solution to buy when multiple different solutions manufactured by different companies are available. In Figure 3.1, we have illustrated few different types IoT solutions and few alternative solutions for each type that exists in the IoT marketplace.

! Large number of IoT solutions are listed here:
<http://ioemarket.blogspot.co.uk>

The buyers will also need to look at specific features that each of the IoT solution provides to make sure that the they fulfil the requirements at hand. For example, a smart coffee machines typically provide feature such as automated coffee making based on owners’ behavioural patterns (e.g. make coffee in the morning based on the owners calender appointments and predictive awaking time.). However, some buyers may looking for more specific features in addition to primary expectations (e.g., automated ordering of coffee and milk using on-line service).

In S²aaS model, there are few more factors that buyers may need to consider. Buyers will need to look at the **Privacy Label** as well as the **Privacy Ratings** to verify whether a particular solution provides acceptable level of privacy protection.

— **What is Privacy.** *Privacy is far too vague a concept to guide adjudication and lawmaking, as abstract incantations of the importance of ‘privacy’ do not fare well when pitted against more concretely stated countervailing interests [174]. One widely accepted definition, presented by Alan F. Westin [194], describes information privacy as “the claim of individuals,*

Smart Irrigation


 OpenSprinkler


 blossom⁸


Smart Lighting


 PHILIPS


Smart Sleep Tracking



Figure 3.1: Smart Irrigation, Smart Lighting, and Smart Sleep Tracking solutions developed by different vendors.

groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others”. Roger Clarke [38] has mentioned that “privacy is the interest that individuals have in sustaining a ‘personal space’, free from interference by other people and organisations”.

Sometimes privacy is explained with the help of different dimensions. Privacy of the person, privacy of personal behaviour, privacy of personal communications, privacy of personal data [38] are the four main dimensions of privacy. In the Oxford Dictionary [129], *privacy* is defined as “a state in which one is

not observed or disturbed by other people". More importantly, privacy has been identified as a human right by the European convention [44] as well as by the Universal Declaration of Human Rights [186]. Further, the Charter of Fundamental Rights of the European Union defines the "*respect for private and family life*" in its Article 7 and adds a specific article on "*protection of personal data*" in Article 8. Additionally, Article 12 of the Universal Declaration of Human Rights protects an individual from "*arbitrary interference with his privacy, family, home or correspondence,*" and "*attacks upon his honour and reputation*" [185]. This evidence strongly justifies the need to protect user privacy while we are attempting to harness the power of data trading and knowledge discovery to generate stakeholder value.

In parallel to the security protection goals, three goals have been proposed as privacy protection goals, namely *unlinkability*, *transparency*, and *intervenability* [47]. *Unlinkability* explains that data should not be combined from multiple data sources in such a way that together they would violate user privacy. *Transparency* means that stakeholders need to be informed about the data life cycle and what happens to each data item over time. This can be achieved through both technical and non-technical means such as auditing, laws, regulations, etc. The data owners should know what type data will be accessed, what kind of data sources will be combined, where the data will be processed, what kind of analytics will be used, what kind of results would be generated, and so on. A step going forward, *intervenability* says that data owners should be able to intervene at any time during the data life cycle so they can withdraw or change their consent over time. More importantly, data owners should have control over their data.

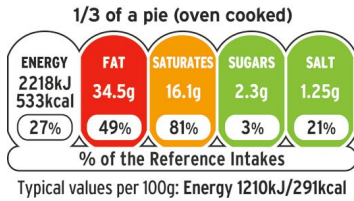
The amount of data captures by IoT solutions has been significantly increased over the last few year. Such data has substantial value as for business and other similar organization once collected and fused in large scale as they contains information related to user behaviours and consumptions. The knowledge that can be derived from such data will help business to steam line their business activities such as supply chain management and reduce wastage. On the other hand, business may be able to help

individual households to change their behaviour and consumer patterns much more efficient ways by allowing them to save financially. However, due to the extremely personal nature of the knowledge that can be derived from such data and the potential risks involved, data owners are often reluctant to provide access to their data to third parties despite the reward they may receive in return.

Research Challenges — Privacy Label. Such a label should consists of information that impact the IoT solution owners' privacy. We can think of this label in parallel to a nutrition or ingredients label attached to food packages. In Figure 3.2, we illustrate couple of different types of labels presented on food packing today. Some of the important research questions are:

- What types of information does a *Privacy Label* should contain?
- How do you derive / produce such information specific to each IoT solution?
- How can we present such information to a potential buyer, specially to non-technical personnel, in a simplified and easy to understand manner?
- What type of visualization techniques can to be used to structure *Privacy Labels*: graphics / icons based or textual based (including numbers)?
- How can a potential buyer determine which IoT solution accommodates his privacy preference better, by looking at the information presented in a *Privacy Label*?

— Privacy Label. Some preliminary steps have been taken to develop privacy labels in web domain [91]. However, developing such labelling scheme for IoT solutions is much more complicated and difficult due to the fact that IoT collect large volumes of data in continuous manner in comparison to website where limited types of data being collected when visited.



NUTRITION	GDA			
	per 100g	per pack	adult	per pack
Typical values				
Energy kJ	450	1345		
Energy kcal	105	315	2000	16%
Protein	7.9g	23.7g	45g	53%
Carbohydrate	8.8g	26.4g	230g	11%
of which sugars	1.2g	3.6g	90g	4%
Fat	4.2g	12.6g	70g	18%
of which saturates	2.7g	8.1g	20g	41%
Fibre.	1.2g	3.6g	24g	15%
Sodium	0.24g	0.72g	2.4g	30%
Equivalent as salt	0.60g	1.80g	6g	30%

GDA = Guideline daily amount

Figure 3.2: Different ways to present nutrition information on food packaging: Will the future *Privacy Labels* on IoT solutions may look like something similar?

Research Challenges — Privacy Ratings. We think about *Privacy Ratings* in-line with widely used product ratings. Product ratings are widely used by the industry for many different purposes. Some times ratings are produced through crowd-sourcing techniques. In other times, ratings are given by an authoritative entity after evaluating a product or service from a certain perspective (e.g. energy rating for houses or washing machines). Typically, each IoT solution combines few different types of components: smart objects, gateway device, and cloud service [136]. Some of the interesting research questions are:

- What types of information does a *Privacy Rating* should contain?
- How do we evaluate a given IoT solution in order to offer a *Privacy Rating*?
- How can we present such information to a potential buyer, specially to non-technical personnel, in a simplified and easy to understand manner?
- What type of visualization techniques can be used to structure *Privacy Ratings*: graphics / icons based or textual based (including numbers)?
- How can a potential buyer determine which IoT solution accommodates his privacy preference better, by looking at the information presented in a *Privacy Rating*?



Figure 3.3: Product rating are widely used in the industry for different purposes: How can we rate an IoT solution from privacy perspective?

- What would be best approach to produce a *Privacy Rating* for an IoT solution: crowd sourcing or authoritative process or any other?

As we mentioned earlier, today, most of the IoT solutions work independently. However, limited number of solutions can interact with each other using different techniques such as partnerships, open and close standards, and adapters and mediator services. These numbers are getting increased due to consumer demand towards unification of IoT solutions. As a result of unification, IoT solutions are expected to work as a single ecosystem by following *hub-and-spoke star networks* within each smart home. This means that there will be a device at homes where other IoT solutions are get connected to. Such devices will act as mediators between different IoT solutions.

Within IoT ecosystem, we identify these devices as *Home Hubs*. We will discuss more about *Home Hubs* in the next section. However, it is important to note that each household will also be required to acquire a *Home Hubs* which will play a central role in the S²aaS model. *Home Hubs* and IoT solutions may developed by different companies where they need work together using some unification techniques. Within S²aaS ecosystem, *Home Hubs* will play an additional role as well.

We identify this role as being a *Databox* [ValorisingtheIoT]. The *Databox* is responsible for managing and protecting data produced by different IoT solutions. The *Databox* will act as a gate keeper by only providing access to authorized parties. We discuss *Databox* in more detail in the next section.

In relation to S²aaS model, another factor to look for is ***Supported Markets***. In Chapter 2, we introduced you to the S²aaS marketplaces where IoT data will be bought and sold. In S²aaS, we envision not to have one single market, instead to have multiple markets similar to today's mobile app market ecosystem (e.g., Google Play, Apple app store, Windows app store). Each *Home Hubs* manufacture, with *Databox* role included, will decide how many markets and which markets they are going to support based on both business, economic and technological reasons.

Finally, buyers will also need to check ***Partner Compatibility***. Certain IoT solutions may only work with certain *Home Hubs*. Similarly, if a potential buyer have few different independent IoT solutions already deployed in their households and looking to enable interactions cross them, it is important to buy a *Home Hub* that is compatible with the existing IoT solutions. Such compatibility allows different IoT solutions to connect together and enable advance interactions between each other.

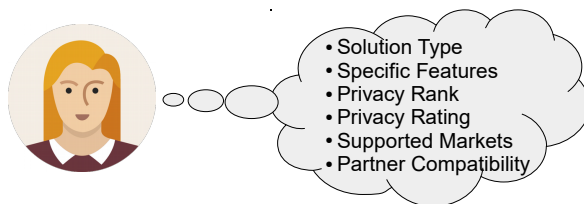


Figure 3.4: Decisions that potential buyers need to make

Once all the decisions are made, buyers may purchase the IoT solutions. Figure 3.4 summarises the whole process. This process may repeat over time as the home owners may decide to augment their homes with different IoT solutions as they feel necessary.

3.2 Configuration and Personalization

Once the purchases are done, buyers need to bring them home and install them either by themselves or through a service provider. Once the physical installation is done, the next step is to setup and configure the newly installed IoT solutions as well as the *Home Hub*.

Physical deployment of IoT ecosystem at home (i.e., multiple IoT solutions and a *Home Hub*) may also require deployments of intermediation hubs throughout the house as illustrated in Figure 3.5 (numbered). The reason is that IoT solutions could have components designed to run with battery power for longer durations without recharge or replacements. They are designed to operate using low range low power protocols such as Bluetooth, Zigbee, RFID, NFC, ANT+, and so on [145]. As a result, some IoT solutions may have some components that are unable to communicate with the *Home Hub* via WiFi. Intermediary mini hubs may act as gateways and protocol converters.

— **Towards Home Hubs.** Today, we see different types of smart homes hubs are being built with variety of different features. Some features are common across different manufactures and some are unique due to the unique capabilities of the manufacturers and their existing products and services portfolios. *Home Hubs* typically act as WiFi routers. Two of the major *Home Hub* candidate available on the market today are Amazon Echo and Google Home. However, several companies following them. One of the key functionalities of a *Home Hub* is to enable interoperability among different IoT solutions so they can interact with each other.

Amazon Echo [9] It is a voice-enabled wireless speaker developed by *Amazon.com*. The device is capable of voice interaction, plays music from *Prime Music*, *Spotify*, *Pandora*, *iHeartRadio*, *TuneIn*. It has 360 omni-directional audio

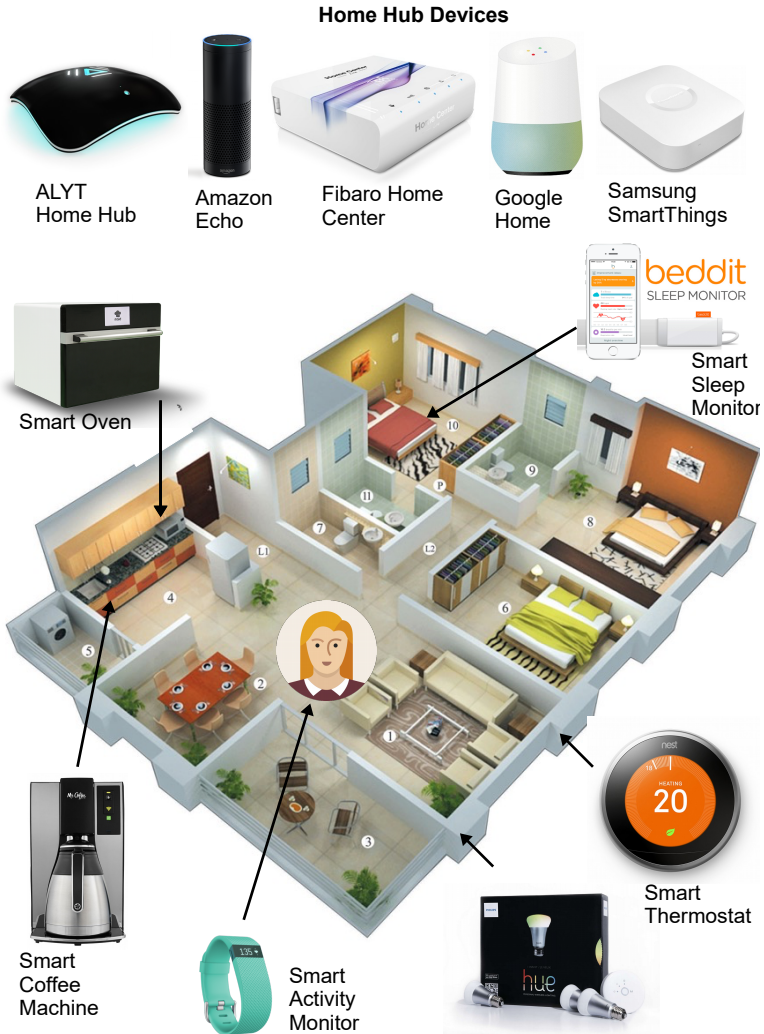


Figure 3.5: Each household that is interested in building an IoT ecosystem requires a Home Hub to be installed. IoT solutions are expected to be connected to the *Home Hub* either directly or via mini hubs. *Home Hubs* are typically connected to permanent power sources and comprise comparatively high computational capabilities. They are also installed with necessary drivers so they can interact with different IoT solutions developed by different vendors.

and allows hands-free convenience with voice-control. It can answer questions, read audio-books and the news, report traffic and weather, give info on local businesses, provide sports scores and schedules, and more using the *Alexa Voice Service*. It can also control several smart devices using itself as a home automation hub. For example, it can control lights, switches, and thermostats with compatible *WeMo*, *Philips Hue*, *Samsung SmartThings*, *Wink*, *Insteon*, *Nest*, and *ecobee smart home* devices. Amazon Echo supports *Uber* bookings, *Domino's pizza* ordering and many more services.

Google Home [69] It is a voice-activated home hub that allows home owners and their family to get answers from Google, stream music, and manage everyday tasks. It is developed by Google. The intelligent personal assistant, Google Assistant, is included as the main and only primary assistant in the software and operating system of Google Home.

Other Some popular *Home Hubs* are *Samsung SmartThings* [163], *ALYT Home Hub* [105], *Fibarò Home Center* [59], *VeraLite Smart Home Controller* [188], *Insteon Hub* [89].

There are three different types of configurations need to be done in order for an household to participate in the S²aaS model: 1) Primary (Vertical) configuration, 2) Secondary (Horizontal) configuration, and 3) Tertiary configuration.

Primary (Vertical) Configuration

This is also called *vertical* or *intra-solution* configuration. Once brought home, each IoT solution needs to be configured as independent solutions. Most of the time, each solution comes with some hardware components, mobile app, and a cloud service. First, owners may be required to register their IoT solutions on-line by creating accounts and providing other necessary details. After that they will also need to perform a series of physical tasks such as pressing and holding a button or calibrating a device in order to connect different components of the IoT solution together. In Figure 3.6, we present an example which demonstrates how to configure a smart scale solution called *Aria* [60].

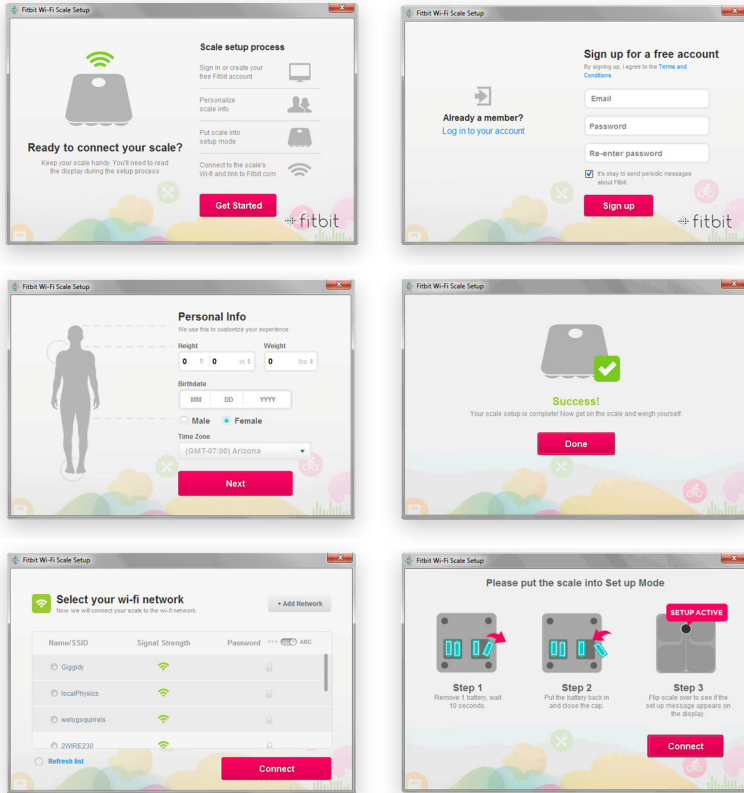


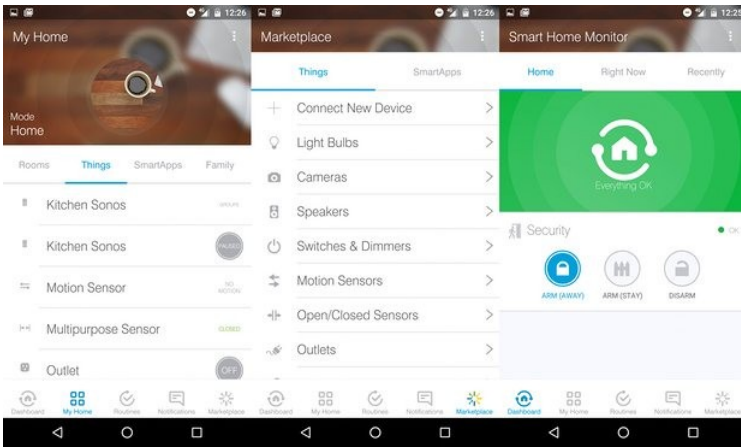
Figure 3.6: Configuration process of Aria Smart Scale

Research Challenges — Primary Configuration. Some of the interesting research questions are:

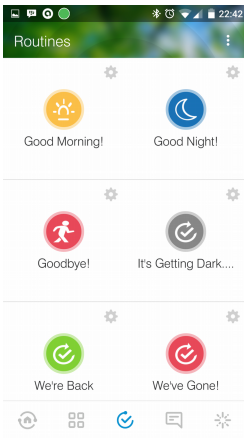
- What are the most common techniques used to configure IoT solutions and why?
- What kind of user interfaces are used to perform configuration?
- How user friendly are these configuration techniques and can we make them more user friendly?
- How long does a typical configuration takes and can it be reduced?
- How secure are these configuration techniques and can we make them more secure?

Secondary (Horizontal) Configuration

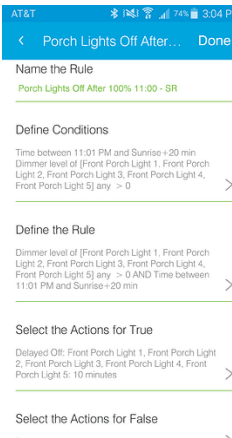
This is also called *horizontal* or *inter-solution* or *Internet of Things* configuration. This type of configuration focuses on building IoT ecosystems within households by connecting different, but also independent, IoT solutions together. This is where true value of IoT comes into life. Value of two IoT solutions together is higher than the value they create independently due to collective synergy. Typically, different IoT solutions are connected together using *Home Hubs*. Then the *Home Hub* provides mechanisms to configure



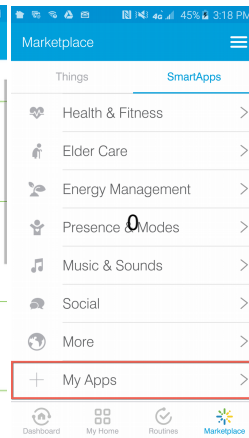
(a)



(a)



(b)



(c)

Figure 3.7: Configuring multiple IoT solution together.

these multiple IoT solutions in a unified manner. Such mechanisms are identified using different terms by different vendors. Some commonly used terms are *IFTTT*, *routines*, *scenes*, and *rules*. In Figure 3.7, we illustrate how a routine can be built in *Samsung SmartThings Home Hub* by combing different IoT solutions. A routine is a sequence of action that would take place due to some kind of trigger. A Trigger could be 1) reaching a time (e.g. 6.00am morning), 2) detecting an event (e.g., home owner gets up from the bed), 3) change in environmental factor (e.g., temperature drops below 5C), and so on. These routines are typically predefined and executed based on triggers. These popular predefined routines are also comes as pre-packaged apps so the home owners can install them instead designing by themselves.

Research Challenges — Secondary Configuration. Configuring multiple IoT solutions together through routines or scenes are typically done manually. This is a tedious task to perform specially when a brand new installation of IoT ecosystem has to be done in a new household. Further, as more and more IoT solutions get installed in a given household, it would be possible to configure new routines which were not possible before. It would be necessary to have techniques put in place in order to keep track of IoT solutions available at a given time. Such techniques will need to identify new types of routines that can be configured using existing IoT solutions. Further, non technical personal may find such configurations difficult, time consuming and cumbersome. Therefore, it critical develop new techniques to perform these configurations automatically with minimum user intervention. Some of the interesting research questions are:

- What are the most common techniques used to perform secondary solutions and why?
- How user friendly are these secondary configuration techniques and can we make them more user friendly?
- How secure are these secondary configuration techniques and can we make them more secure?
- How long does a typical configuration takes and can it be reduced?
- Can the routines already being built by user be shared with

other similar users and is it effective and efficient?

- Is it possible to predict and recommend routines for a given user by analysing similar users?
- What kind of information need to be gathered and analysed in order to provide such recommendations?
- Is it possible to learn new routines by observing owner's behaviour and what kind of observation is required to learn such routines?

Tertiary Configuration

This is also called S^2aaS configuration. In secondary (IoT) configuration, the main focus is to connect multiple IoT solution together so they can work together in order to provide more convenience to their owners. In S^2aaS configuration, the main focus is on *Data*. During S^2aaS configuration, owners will need to pick a data marketplace they would want to join. This is where the data consumers will make data requests and data owners get to trade their data for different types of rewards, as we discussed later in this chapter.

— **More about Privacy.** Privacy would be perceived as a dialectic and dynamic boundary regulation process between the individual (data subject/self), the others (firms and other individuals), and data/information (premise) in contexts [130, 137, 143]. As a dialectic process, privacy could be regulated in situations/contexts such as our own expectations/experiences, those of others with whom we interact and social norms (cultural, social) and regulations (legal). As a dynamic process, privacy could be viewed as being under continuous negotiation and management of 1) disclosure boundary: what (type and amount) information could be disclosed in this context; 2) identity boundary: how much identity related information would be displayed and maintained in this context; 3) temporarily boundary: boundaries associated with time, that is, the disclosure and identity boundary depending upon the interpretations of contexts for the past, present and past.

Due to the variations in privacy expectations, no single privacy profile fits every individual; therefore, privacy need to be negotiated with each and every individual separately. One classi-

figuration identifies four types of users based on their privacy expectations [1, 146, 175]: *privacy fundamentalists*, *profile averse*, *identity concerned*, and *marginally concerned*. Westin [193] has identified three similar main user types based on their attitudes and concerns about privacy. From most to least protective of their privacy are: *fundamentalists*, *pragmatists*, and *unconcerned*.

Preferences: Risk-Reward: Each data owner may have their own privacy preference such as to whom they would like to give access to their data, for what reason, under what conditions, and so on. More importantly, some data owners would be more privacy aware than others and their privacy expectations may also varies based on the opinions, knowledge, financial status, and many other factors [1, 175, 193]. Therefore, it is vital to understand each data owners privacy preferences and expectations so the data requests can be filtered and presented to the data owners accordingly.

Research Challenges — Tertiary Configuration. Understand privacy requirements is significant challenge as most of the data owners may not even know how to express their privacy preference. Some of the interesting research questions are:

- How can we allow data owners to express their privacy preference and what are the pieces of information that need to be captured?
- What are the human computer interaction techniques that can be used to acquire necessary pieces of information in order to understand the data owners' privacy preferences and expectations?
- Can we reduced the information we collect from each data owner in order to understand their privacy preference by predicting through analysing similar users?

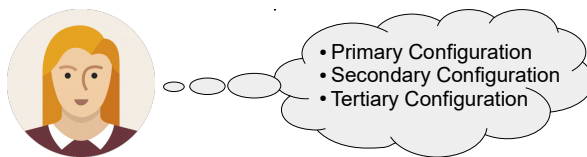


Figure 3.8: Configuration and personalization

Figure 3.8 summarise the whole configuration and personalization processes. These processes may repeat over time as the home owners may decide to augment their homes with more and more IoT solutions as they feel necessary.

3.3 The Marketplace and Data Trading

In S^2 aaS model, as illustrated in Figure 3.9, data markets are the places where data owners trade their data with data consumers for rewards in return.

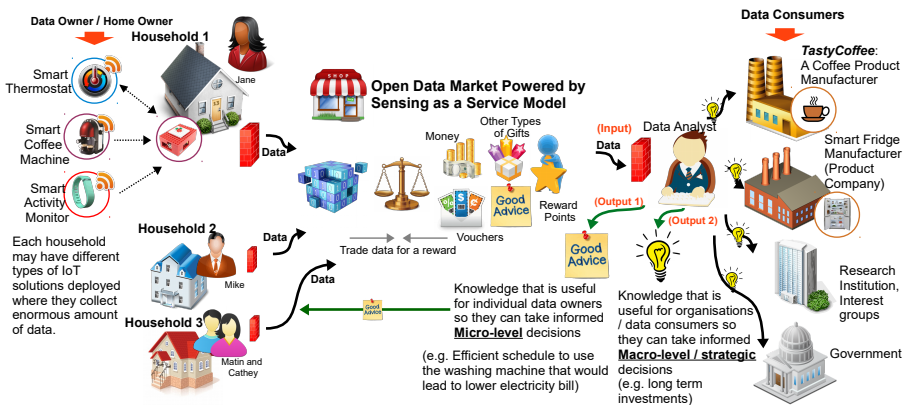


Figure 3.9: Data market for Personal Data

We envision the data marketplaces to be similar to mobile app markets. In today's mobile app markets (e.g. Google Play, Apple App Store), third party developers can sell their apps and phone owners can search and buy them (or install them for free). Figure 3.10 show how apps are listed in Google play app store. In data markets, we envision two different ways that data consumers would request data from data owners.

1) Subscriptions based Data Trading: This would be somewhat similar to today's mobile app market. Data consumers will advertise their expectations (i.e., what kind of data they are looking for and other conditions) and offers (i.e., reward types and value) in their preferred marketplace. Instead of having apps listed, data markets will list *enrolment opportunities*. We can call them *packages* or *subscriptions*. In mobile apps ecosystems, developers build mobile apps and list them in app stores. Similarly, in S^2 aaS ecosys-

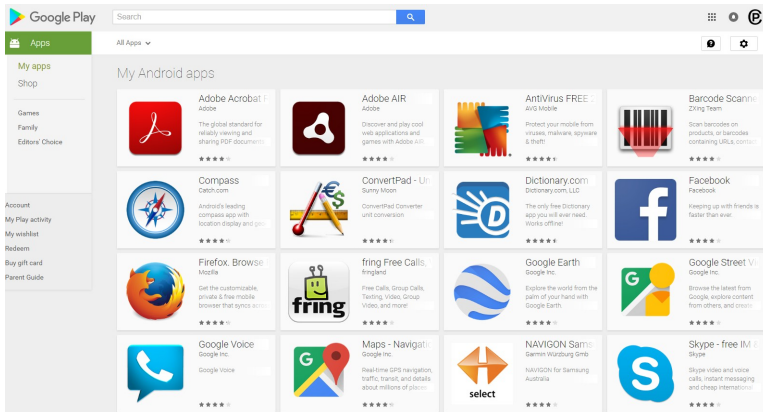


Figure 3.10: Google play mobile app store

tem, data consumers are expected to build data request packages / subscriptions and listed them in the data marketplaces.

However, the difference would be that enrolment packages will provide more freedom to data owners than take-it-or-leave-it approach that traditional apps follow. Data owners will be provided with some configuration parameters to express their preferences. As a result, enrolment will be carried out based on terms that data owners set, so the data owner will be in control all the time. Each enrolment opportunity will specify what data it expects at which levels of granularity, other related conditions, list of IoT products that generate the data they expect, potential reward types and values, an app that is capable of processing and prepare the data to be sent to the data consumer, and so on. For example, once a data owner agreed to enrol, relevant applications need be downloaded to the *Databox* in the *Home Hub*. These apps are responsible for data pre-processing (if that is part of the agreement) and send either raw or processed data to the data consumer as per the enrolment agreement.

In circumstances where data consumers are providing value added service to the data owners as a reward, they may specify different service options trading on different levels of granularity. It is important to note that a single data consumer may offer multiple different services. For example, one service offering may accept data produced by Fitbit [61] and Beddit [24], and will return useful

advice (as the reward) on how to exercise, rest and sleep efficiently. Another service offering may accept not only above mentioned data but also data from smart fridge [115] and kitchen storage [27]. This offering may go beyond the previous service and provide efficient meal planning advice based on the ingredients available at home that would compliment efficient exercise, rest and sleep. Data owners will receive the services correspond to the granularity of personal data they choose to trade.

Based on the data owner's privacy preferences as well as the types of IoT products deployed in a given household, Databox will need to find out what are the best matching enrolment opportunities. Based on the level of automation, Databox may also inform the data owner about the potential opportunities of data trading and present a risk benefit analysis specific to each enrolment opportunity.

2) One-time Data Trading: In this method, data consumers will directly send their offers to selected number of matching data owners after examining their metadata about available data sources (i.e., available IoT solutions). The Databox will be required to examine such requests and present the data owner a risk-benefit analysis report so the data owner can make the final decision on whether to trade data or not.

Individuals have to make privacy decisions by trading off the benefits, cost and risks associated with information disclosure in contexts. We see the privacy preferences of an individual as a changing set of requirements that can be represented using a point in a spectrum where one side is the most restricted and the other side is the most lenient. Li et al. [97] have theorized and empirically tested how an individual's decision-making on information disclosure is driven by competing situational benefits and risk factors. The results of their study indicate that, in the context of an e-commerce transaction with an unfamiliar vendor, information disclosure is the result of competing influences of exchange benefits and two types of privacy beliefs (privacy protection belief and privacy risk belief). In the S²aaS domain, the privacy risks that a data owner might tolerate depend on many different factors such as rewards, reputation of the data consumer, the purpose that data is used for, and so on. For example, Li et al. [97] has found that monetary rewards could undermine information disclosure when information collected has low relevance to the purpose of the e-commerce transaction.

One of the main challenges is to develop a knowledge model that can be used to capture privacy preferences of data owners in contexts, which can later be used when negotiating access to data. Such a model can also be used to model the data consumer's privacy preferences as well. However, much harder challenges would be to understand the contextual privacy preferences of the data owners. *Databox* would allow data owners to provide their preferences on the following parameters 1) what and how much data would be disclosed in this context (peer group; social and cultural rules/norms; legal; history of disclose with the entity requesting; history of disclosure in terms of personal preference and data policy; 2) price/benefits of disclosure; 3) level of disclosure/exposure/openness; 4) level of risk of disclosure. Based on the preferred privacy parameters, privacy preferences of their owner in contexts could be understood.

From *Databox* point of view, understanding of data owner privacy preference is important. First, *Databox* can use those privacy preferences of both data owners and consumers to filter out enrolment opportunities based on incompatibilities. Secondly, from a more advanced view, *Databox* will be able to carry out data trading tasks autonomously or at least semi-autonomously. One of the first steps towards addressing the challenges of understanding privacy preferences is to use recommendation systems to predict each data owners' privacy preference and create a template that conforms to the data owner's privacy expectations. Information such as 1) demographic information, 2) answers provided to very few but critical questions, 3) privacy preferences of similar data owners, can be used to develop privacy preferences predictive models. Incomplete privacy preference knowledge can be acquired by interacting with data owners. However, privacy preferences are not easy to understand through direct questions.

One of the research challenges would be to explore how and what kind of techniques can be used to acquire those preferences. The challenge is to acquire that information without overloading them. One possible direction would be to use techniques such as ContraVision [154] in order to understand users' positive and negative perceptions towards futuristic scenarios and technologies. It is important to notice that data owners are mostly non-technical people whom may have less understanding of the technology. Therefore, privacy preference acquisition needs to employ techniques that are

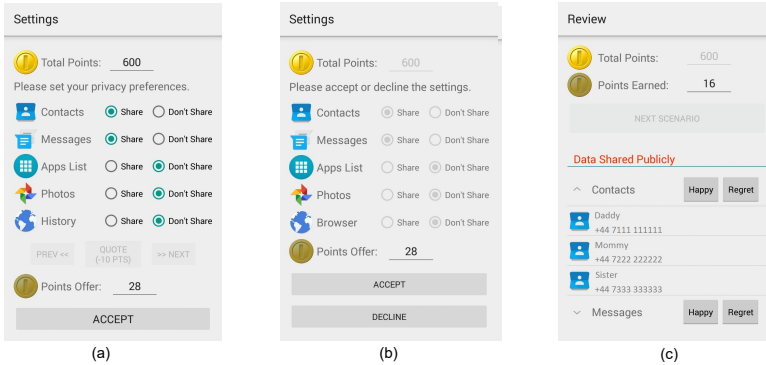


Figure 3.11: These screenshots show how users may interact with permission systems of a mobile app to negotiate personal data usage by having rewards as a trading mechanism [20]. (a) Negotiation design. The user is offered a reward for their contacts and messages, but can change these settings to receive a new quote; (b) Classic take it or leave it design. In this scenario, the user is only able to accept or decline access to contacts and messages in return for a reward; (c) Review design. The user decides how they feel about having publicly shared the contact details of their family members.

more meaningful and understandable to such audiences.

One of the major challenge is to find an appropriate exchange or transaction negotiation model. There are permission negotiation models being proposed with respect to mobile apps domain [20] as show in Figure 3.11. Baarslag et al. [20] allow users to negotiate with mobile apps in an interactive manner in order to find right balance between privacy and pricing.

However, risk-benefit negotiations are much more complex due to difficulties in measuring potential privacy harms and risks with respect to different types of IoT data in a marketplace. In a pervasive setting, a case-based privacy mechanism would be cumbersome and difficult to achieve by users directly. To address this, *Databox* could build upon agent-based techniques that employ software agents to represent data owners in an automated manner. The agent supports the user in their privacy decisions, by advising the user through a interface, while handling autonomous privacy transactions on the user's behalf.

— **Privacy Risk-benefit Analysis and Visualization.** In news media, we see different types of privacy violations or harms. Some of the common privacy harms are surveillance, interrogation, aggregation, identification, insecurity, secondary use, exclusion, breach of confidentiality disclosure, exposure, blackmail, appropriation, distortion, intrusion, and decisional interference [174]. However, these are high-level abstract terms. Identification of how each data item collected by each IoT product may lead to the above privacy harms is a difficult challenge specially due to the heterogeneity of the IoT products.

A factor that makes such identification more difficulty is uncertainty and advances in computational capabilities. Cheap and abundant computational resource mean that, anyone can develop new algorithms that fuse different types of data to discover new knowledge. For example, an algorithm may use energy consumption data to detect the usage of a microwave and to determine the presence of a person in a given household. In another instance, an algorithm may combine lighting and air-conditioner usage data to determine presence in a given household. In these two instances, algorithms employ different types of data.

To add to the complexity, the amount of data needed by each algorithm may also vary. For example, one algorithm may be able to determine human presence using data that is captured at 3 seconds intervals. However, more sophisticated algorithms may do the same with data sampling interval 3 minutes (180 seconds). So the capabilities of knowledge discovery is getting more advanced every day. Therefore, it is very difficult to calculate a risk when it is not 100% sure about what the algorithms can do where the capabilities are changing every day due to the advances in the field. However, some amount of privacy risks (e.g. unauthorised access, un-consented secondary usage) can be reduced by developing privacy-aware sensing infrastructure [137].

Another challenge is how to inform non-technical data owners about benefits and risks. Similar research has been done in the social networking domain where they have analysed the trade-off between privacy risk and social benefit [198]. The exact amount of a reward (e.g., number of loyalty points) that is asso-

ciated with a particular data transaction could be varied depends on the potential value that the data is expected to generate for the data consumer. Informing the reward value of a potential data request is not difficult. However, the complexity adds in as rewards need to be presented in a comparison manner with potential risks.

Representing privacy harms using the above taxonomy is less useful, especially for non-technical data owners. One challenge is to understand how privacy risks are perceived by non-technical users. The next challenge is to identify the probability of each of the privacy harms. For example, how likely is that a house gets burgled given some data is being leaked to a malicious party. The answer would depend on many factors such as the, burglary rate in a given area, security systems deployed in the house, and so on. For example, a data owner living in an area with a high crime rate may be concerned about the possibility of a third party entity inferencing his working patterns thinking that burglary could occur based on such sensitive information. So if the data consumer requesting data that can be used to infer such patterns, user may view it as a significant threat. In contrast, a user living in an area with low crime rate in a high-end apartment complex with 24 hour security will consider burglary as a low risk. Capturing and modelling knowledge related to privacy risks, likelihood of occurrence using different data sources, personalisation (e.g., localisation of threat to each location and individual) is an important challenge to address. Finally, all this information need to be presented to the data owners in a way that is meaningful and usable from their perspective during the engagement of data markets.

Research Challenges — Marketplace and Data Trading.

Some of the interesting research questions are:

- What information need to be provided in subscription or one-time data trading data request?
- How data consumers would find matching data owners ?
- How an app works within *Databox* and what are the main components of such apps ?
- How the data trading would work from user interaction

point of view ?

- What kind of data trading negotiation techniques is required in order for S²aaS model to work effectively and efficiently ?
- How to build reliable and scalable sensing infrastructure that is capable of automatically organizing themselves based on each data owners expectations, when data need to be gathered from large number of data owners ?

Shared Data Ownership

In real world, data ownership could be a complicated matter [45]. Data is relational and it often relates not so much to ‘*me*’ or ‘*you*’ but to ‘*us*’, and with this the coherence of the ‘*my data*’ model starts to break down and break down in challenging ways [45]. For example, data may not own by an individual, but a group of people (e.g., family). In such situations, data access decisions may need to comply with preferences and expectations of all the member in the group. However, data ownership may not always clear. For example, if an individual in not capable of making informed data access decision, who can act on behalf (e.g., children, elderly) is an interesting question to be answered.

Research Challenges — Data Ownership. An interesting research question is:

- How data trading negotiations would work when data is co-owned by multiple parties (e.g., multiple individuals living in a single household)?

Transactions and Earnings

Individual transactions are expected to return very small amount (i.g in pennies). However, this amount will grow up when the number of transactions get increased. Data owners will be able to sell their IoT data not only once but many times to many different data consumers (i.e., companies such as Walmart, Tesco, Google, etc.). For example, a start-up called Datacoup [48] is offering 8 USD¹ per month in return for selling personal data. Even though the success or the long

¹<https://www.technologyreview.com/s/524621/sell-your-personal-data-for-8-a-month/>

term sustainability of this particular company is not known, their approach supports our vision of open data markets.

From a data consumers point of view, collecting data from a few data owners has little value. In order to derive valuable insights, data consumers would be required to collect and analyse data in large scales. For example, collecting operation parameters (e.g., operating temperature, energy usage) as well as user interaction patterns will help manufacturers to better understand how users interact with their devices in the real world. Such data, collected and processed on a large scale, will provide new insights (to manufacturers) to build new types of devices. Manufacturers will be able to predict service intervals and issue useful guarantees on parts as well as automated parts reordering (through real-time monitoring and predictive models).

3.4 Architectural Components

Let us now present the main components of the S²aaS ecosystem. It is important to note that based on reliability, security, and privacy expectations, the actual architecture may varied. Our design thinking is large inspired by today's mobile app ecosystem. We identify five major components: 1) Data Bucket, 2) Data Market, 3) Data Studio, 4) Data Mill, and 5) Data Oven. It is important to note that we use these (somewhat fancy) terms as code names for each component in order to refer to certain functionalities they are expected to perform. Depending on the implementation, these components may be combined to different products and services.

Data Bucket: This service is responsible for gathering data from different IoT solutions. It interfaces with the data owners using a mobile app where it allows data owners to express their privacy preferences, receive recommended data requests, trade data, and negotiate data trading. We will walk you through the Data Bucket app later in this paper in order to demonstrate how data owners may engage with the S²aaS ecosystem. Each data owner has its own data bucket.

Data Market: This service is similar to Google play app store. Instead of apps, Data Market stores, organises, disseminates, and manages data requests. Data Market also organises and manages Meta data provided by individual Data Buckets.

Such Meta data allows Data Market to distribute data requests appropriately to compatible and interested data owners.

Data Studio: This service allows data consumers to create their data requests easily. It provides necessary integrated development environment like interface that allows data consumers to compose data requests efficiently and effectively. Each data request is a package of several pieces of information that includes data requirements, rewards, privacy risks, analytical components, and other information.

Data Mill: This is a technical infrastructure service component where personal data is being processed in combined with the open data (e.g., weather data). No stakeholders involve with this component directly. A brand new milling machine is created in order to gather and process data from a single data owner. It is not allowed to combine personal data from different individuals within a single machine mill. Data Mill either could be located in the cloud or within the local device within smart home (e.g., as part of Amazon Echo or Google Home) [148].

Data Oven: This is also part of the technical infrastructure service. It receives data from the Data Mill where initial data processing occurs. Data from multiple different individuals are processed together within the Data Oven.

Figure 3.12 illustrates the high-level architecture of the S²aaS ecosystem including some of the most important communication aspects. Sensing as a Service model builds on top of the existing IoT ecosystem. The IoT solutions are typically registered and configured by data owners. These IoT solutions communicate with their companion cloud services and data is frequently being pushed back in order to be analysed and knowledge extracted. Data owners need to register themselves by creating and configuring a data bucket account. Once login to the data bucket app, data owners are provided with user interfaces that allows them to connect IoT solutions to the data Bucket. In the example, Jane has connected Fitbit, Beddit and Smart coffee machine to her Data Bucket account. During each of these configuration processes, data owners are allowed to express their preferences in terms of which data items they would like to trade under what conditions, and so on.

Let us now look at the other end of the S²aaS ecosystem, the

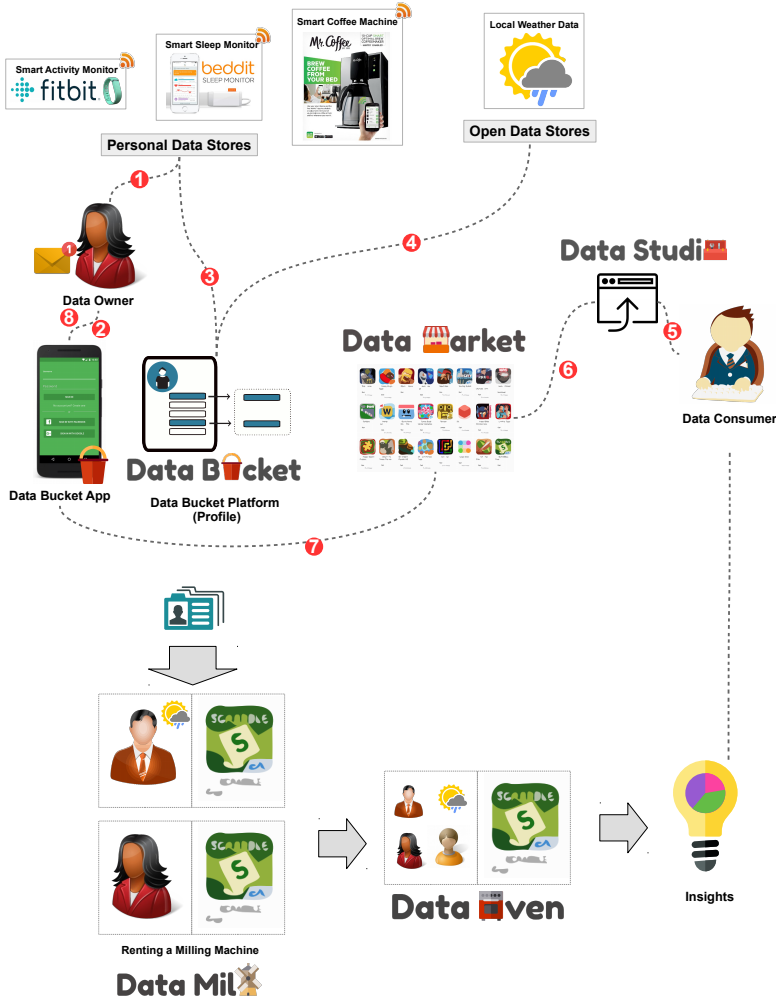


Figure 3.12: Architectural components

data consumers. Data consumers first needs to do some preliminary research and determines kinds of data needs to be gathered in order to support the objective. In sample scenario, the data consumer needs to research about activity, sleep patterns, and there relationship with coffee consumption.

The data consumer then needs to use the Data Studio to create the data request. Data request comprises of several pieces of information including data items requested, intention of data gathering,

knowledge expected to be derived, technologies used to processed and analysed, rewards willing to provide, and so on. The Data Studio package this request and publish in the Data Market place. The Market place then pushed it to the matching data owners.

Depending on the initial configuration, data owners will either receive the data request as a notification or will be listed under recommended data trading section in the in the Data Bucket app. Data owners may open up the request to continue trading data. Data owners can use the Data Bucket app to negotiate with the respective data consumers regarding rewards, and the exact data to be traded (e.g., data granularity, duration, etc.). We present some examples later in the paper. Once the both data owner and the consumer is agreed, a digital contract will be made.

Data market passes the authorization to gather data (as per the agreement) to the Data Mill in order to perform data processing. At the same time, data owners receive agreed reward. In the Data Mill, personal data is processed in combined with the data gathered from open data sources (e.g., public data such as weather). Once completed, processed data is sent to the data oven in order to perform further processing, analysis, and derive expected knowledge. At this stage, data from multiple users are processed together.

— **A story.** You can think of the data consumer as a baker (Joe the friendly baker). Let us assume he wants to make a new coffee cake. He first build the recipe using his recipe book (Data Studio). Once, he is happy with the recipe, he goes to the market (Data Market) and buys coffee beans, wheat, sugar, eggs, and all other ingredients (Data). Then, Joe goes to his village mill (Data Mill) and rent three different milling machines that are designed for different grinding requirements, one for wheat, one for sugar, and one for coffee. Joe had to wait until few other village men finish their grindings and release the milling machines. Important rule in the mill is that each batch from each customer need to be grinded separately. However, depending on the grinding requirements, customers can pick a specialised machine. Once all done, Joe takes all ingredients to his bakery. He combines all the ingredients according the recipe he built earlier. Joe bakes his cake in his oven (Data Oven) until he satisfy with the outcome. Walaaa, coffee cake (insights) is ready

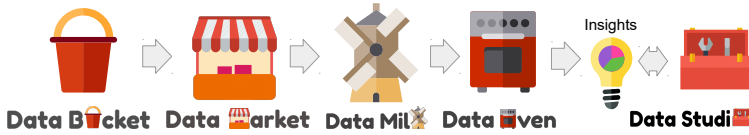


Figure 3.13: Story of data science

Let us now walk you through the major user interfaces provided in Data Bucket app in order to explain how a typical non-technical user may participate with the S²aaS ecosystem. Our intention is not to make the UI designs perfect. Instead, we aim to envision the high-level objectives of each screens. These interfaces allows us to highlight challenges in user interaction design.

Figure 3.14 (a) shows the login screen of the data bucket app. Data Bucket is the central account for data owners who interact with the S²aaS ecosystem. Each of the Data Bucket is registered with one or more Data Markets. Once login, as shown in Figure 3.14 (b), a list of IoT products are shown. Data owners can click the IoT solution they own and configure them. As shown in Figure 3.14 (c), Data Bucket app provides an interface for data owners to enter their credentials related to each IoT solutions (e.g., login details for the Fitbit account). Data bucket knows the exact data items that a particular IoT solution can provide (e.g., Fitbit provides body weight, physical activity, step count, body mass index, and sleep duration). Data owners can select which data items they would like to trade and several other preferences. Using the similar process, data owners can connect different IoT solutions. As a result, Data Bucket knows which data items are available for trade by each data owner.

In a separate screen Figure 3.14 (d), data owners are provided with list of recommended data trading offers. Broadly data trading opportunities can be categorised into two, namely, 1) one-time, and subscriptions. Once data owners decide to explore further with any of the trading offers, they are provided with a secondary screen as shown in Figure 3.14 (e). Data owners are provided with details on a particular data-trading offer (who is the data consumer, what is the intention, what analytics are used, how analytics are certified, what knowledge is expected to derive, and so on). Data owners can negotiation how much data they want to trade under which conditions and how much reward they would expect in return.

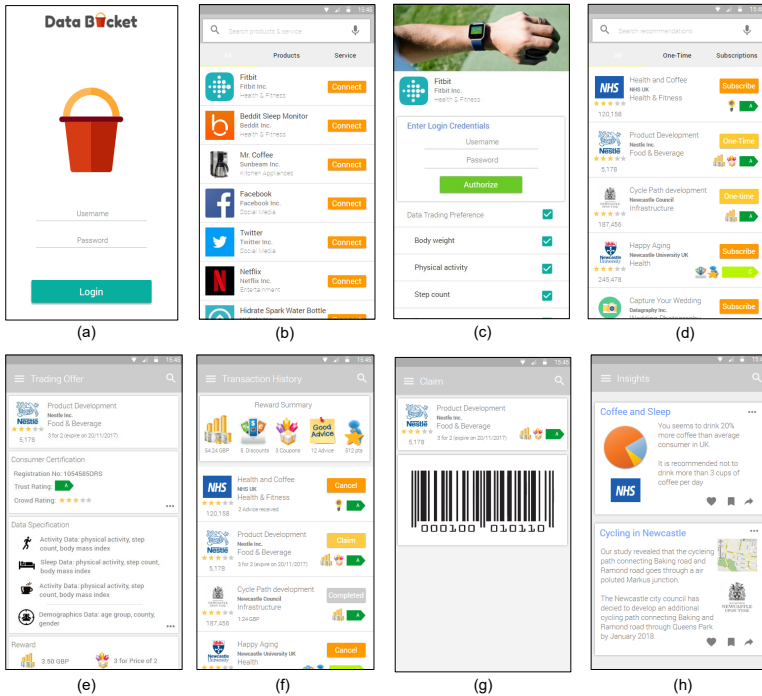


Figure 3.14: Data Bucket envisioned user experience

Once both parties agreed, details can be seen on different screen as shown in Figure 3.14 (f). This screen allows data owners to claim their rewards (see Figure 3.14 (g)) and cancel existing subscriptions. One of the importance types of reward is actionable (useful) advice. Instead of giving financial rewards, data consumers agree to provide useful advice to the data owners through a designated app or through the Data Bucket app's insights screen as show in Figure 3.14 (h).

Typically, data owners are non-technical personal. Therefore, above-mentioned user interfaces and interactions should be built in such a way that they can be used with minimum technical knowledge. The challenge is to evaluate data requests made by data consumers and generate risk-reward analysis reports so the data owners can make informed data trading decisions. Visually representing risk-reward analyses in such a way that they are detailed enough for data owners to be informed accurately, but simple enough to be understood easily and quickly, is an important feature towards the

success of the S²aaS model. One of the challenge is to determine what information is important for each data owner when engaging with data trading and how such information can be presented to them.

Another challenge is to decide what kind of controls should be given to data owners during both the negotiation and post-trading stages. The data buying and selling processes should be simple enough to take place repeatedly without requiring significant amounts of input and time from data owners. Finally, what aspects of a data trading transaction are negotiable and non-negotiable, is also an important question. Baarslag et al. [21] has provided some insights towards data trading negotiations.

Research Challenges — Data Interoperability and Integration. Some interesting research questions are:

- How to enable semantic interoperability among different IoT products and services? For example, temperature could be room temperature, body temperature, etc.
- How to develop techniques (e.g., mathematical models that adjust data) to meaningfully process data collected by the heterogeneity of devices with different specifications? For example, reliability, accuracy may be different from one product to another even though they may semantically capture the same type of data (e.g., room temperature)?
- How to develop an ontology to capture all kinds of data types and contexts within the data marketplace? What are the existing ontologies that can be brought together to develop this ontology?

Research Challenges — Privacy-aware Data Analytics.

Some interesting research questions are:

- How to build a library of privacy preserving techniques that are generic enough so they can be reused for different types of analytics tasks?
- How to develop a framework to evaluate and measure strengths, weaknesses, applicability, computational requirements (and other characteristics) of each technique?

3.5 Edge Computing for Smart Cities

S²aaS vision aims to create ‘rentable infrastructure’ where interested parties can gather IoT data by paying a fee for the infrastructure owners. S²aaS model primarily utilises the existing IoT infrastructure which are being deployed to achieve a primary objective. Let us consider the following use-cases as illustrated in Figure 3.15. This use case can be considered as an extended version of the data market we discussed in Figure 3.9.

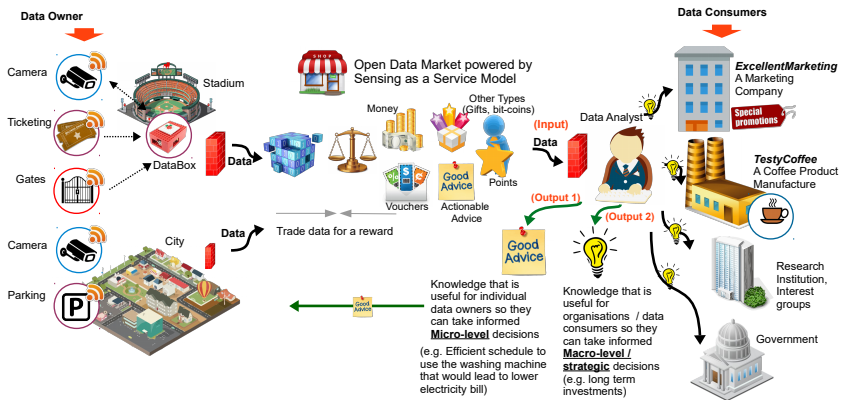


Figure 3.15: Data Market for Sensing as a Service in Smart City

- A shop may deploy a security camera system in order to provide security for its premises (primary objective). However, such cameras (or the data captured by the cameras) can be re-utilised (or re-analysed) to understand the consumer patterns (e.g., analyse demographics such as age, gender, etc. of the people who are passing by).
- A garbage bin may be fitted with sensors in order to monitor and track garbage levels and to support resource management (e.g., truck allocation, recycling facility demand monitoring etc.). Same sensing infrastructure can also be re-utilised to understand crowd in a given day (e.g., understand crowds based on what they throw away).

Let us consider the following scenario as illustrated in Figure 3.16. There is game in the stadium on the weekend. A marketing company, *ExcellentMarketing*, wants to understand the attending crowds better to develop their promotional campaigns specifically

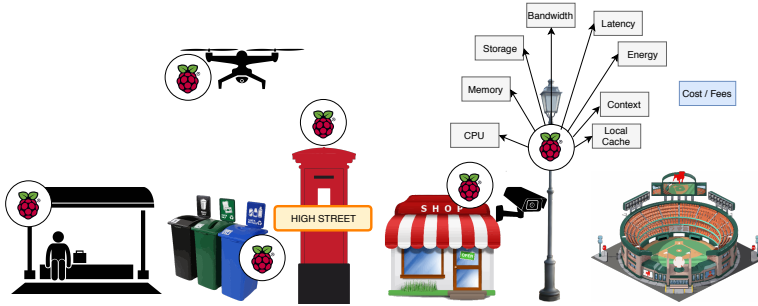


Figure 3.16: Cloud initiated Sensing as a Service

targeting the spectators (market segment). Therefore, they may be interested in collecting data such as demographics (age ranges, gender, sentiments, etc), movement, sentiments, buying behaviours, etc. Through a broker, *ExcellentMarketing* aims to rent the infrastructure over certain period of time (during the game day), so they can gather the data in order to understand the crowd better. *ExcellentMarketing* may be interested to gather variety of data from the streets. Different sensors may be used to gather and infer different types of knowledge: video cameras [demographics]; motion sensors: [number counting, crowd movement identification]; environmental sensors (e.g. temperature, wind, humidity): [identify any influencing factors, buying behaviours, etc].

Knowledge engineering techniques (e.g., semantic technologies) can be utilised to optimally orchestrate IoT resources to facilitate users' requirements. Such orchestrations should also respect user preferences and while managing overall efficiency of the network. In the above context, *ExcellentMarketing* may either interest in gathering data in real-time (e.g., to enrich their promotion in real-time) or in a differed manner (e.g., to enrich future promotional campaigns). The orchestrations need to be performed accordingly to support the two types of sensing requirements. In order to support real-time sensing as a service, orchestration will be required to bring more computational nodes together in order to process data at higher rate to reduce latency. Due to high resource consumption (both computation and network), *ExcellentMarketing* will be required to pay a higher price.

One of the major challenges in edge computing is to reduce

network communication and latency. Knowledge engineering techniques can be used to enrich edge nodes with intelligence (knowledge), so they can make decisions by themselves reducing communication with the cloud. Orchestration also requires discovering IoT resource (e.g. computational nodes, service, sensing capabilities, etc.) efficiently in order to develop optimal plan at runtime. Knowledge engineering techniques are also useful towards performing adhoc resource discovery.

In the above use case, orchestration is triggered via a cloud broker where the BestBrands makes its initial request. However, there is another type of scenarios that could occur as follows where the request initiated by one of the edge nodes. Let us consider the scenario presented in Figure 3.17.

Bob is visiting a tourist attraction and he is interested in using his augmented reality device (AR) (mobile phone, glasses, etc.) to enrich his experience. He is interested in a rich experience, so he would like to rent nearby IoT infrastructure to support the experience. His augmented reality device would discover the nearby infrastructure to share the computation load (computation offloading), so Bob's own AR device can reduce its energy consumption. As a result, Bob can have longer experience. Bob's AR device will orchestrate the different computational tasks to differ nodes (e.g., download and process maps, weather information, audio narration, translation, etc.). Such distribution of tasks will reduce the latency and improve the Bob's experience. Bob is happy to pay for this rich experience. On the other hand, Alice is university student with limited budget. She is less concerned about the experience, but she needs to retain the mobile phones battery until she returns back to the hotel. Based on her priority, the orchestration that Alice's AR device need to perform would be significantly different from Bob's orchestration. Alice may pay less than Bob, but her experience may not as rich as Bob's (e.g., latency, feature limitations).

In this scenario, request is initiated by Alice's and Bob's AR devices (edge devices). As same as in previous scenario, orchestration may need to consider contextual information. Candidate compute nodes may not only have different computational and sensing capabilities, but they may also have other relevant resources already with them. For example, the garbage bin may already have the map in its local cache (that both Alice and Bob needs). Therefore, it is

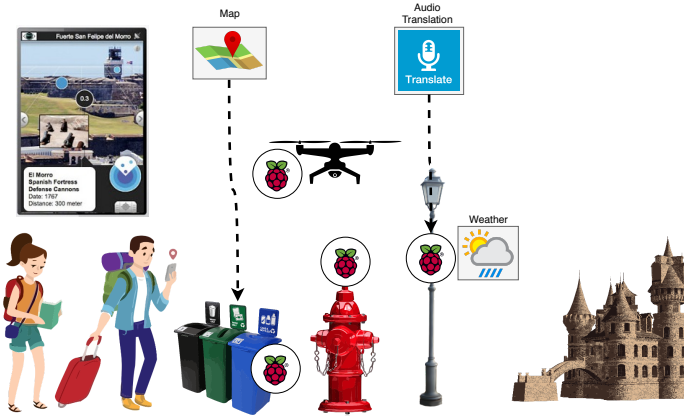


Figure 3.17: Edge Initiated Sensing as a Service

much efficient to assign map processing to the garbage bin node. Similarly, there could be many considerations that the orchestration algorithms need to consider (in addition to user preferences). Knowledge engineering techniques (interoperability, semantics) can play a significant role in edge orchestration activities. Even though service composition for ubiquitous domain is well researched (though mostly in simulations), they all assume nodes and the services are inseparable and static [35].

In contrast, one of the main assumptions in S^2aaS is that infrastructure and associated resources are rentable, and the services are separable from nodes. This means that assignment of services into rented compute nodes happens dynamically. Such separability allows to perform orchestration in a much fine-grained and optimum manner. However, such separability also makes discovery and orchestrating algorithms much more complex (due to increased possibilities) than typical service composition. Therefore, new algorithms will be required to tackle this challenge efficiently. In addition to the rentable infrastructure already deployed across cities, we envision that some service provider may deploy purpose build devices (e.g., drones augmented with rentable infrastructure) in high demand areas.

Research Challenges — Resource Orchestration. Some interesting research questions are:

- How to develop algorithms to orchestrate edge resource optimally to fulfil a given S²aaS requirement?
- What would be the difference between cloud initiated and edge initiated orchestration algorithms?
- What kind of knowledge is needed by the above algorithms and how to store such knowledge in a resources constrained distributed environments?

Looking Ahead

As we said very beginning of this book, we did not intend this book to become a literature review. Our aims was to tell a story. The storing of Sensing as a Service model and how we think it could be built on top of the IoT infrastructure. In this book, we pitched the S²aaS model in parallel to the today's existing technologies so it is easier for anyone understand. Despite the absence of thorough literature review, we wanted this book to be useful for undergraduate and postgraduate students as well as to the members of the scientific community. Therefore, time to time we provided some important references that could be useful for researchers in order to follow up the state of the art research. More importantly we highlighted some of the interesting research questions that need to be addressed in order to build the S²aaS model. We invite you all to become a part of this journey.



Bibliography

- [1] Mark S Ackerman, Lorrie Faith Cranor, and Joseph Reagle. “Privacy in e-Commerce: Examining User Scenarios and Privacy Preferences”. In: *Proceedings of the 1st ACM Conference on Electronic Commerce*. EC '99. New York, NY, USA: ACM, 1999, pages 1–8. ISBN: 1-58113-176-3. DOI: 10.1145/336992.336995 (cited on page 77).
- [2] Acorn Projects ApS. *Leikr*. 2016. URL: <http://www.leikr.com/> (cited on page 18).
- [3] N Agoulmine et al. “U-Health Smart Home”. In: *Nanotechnology Magazine, IEEE* 5.3 (2011), pages 6–11. ISSN: 1932-4510. DOI: 10.1109/MNANO.2011.941951 (cited on page 19).
- [4] *Air Quality Egg*. 2013. URL: <http://airqualityegg.com/> (cited on page 27).
- [5] I F Akyildiz et al. “A survey on sensor networks”. In: *Communications Magazine, IEEE* 40.8 (Aug. 2002), pages 102–

114. ISSN: 0163-6804. DOI: 10 . 1109 / MCOM . 2002 . 1024422 (cited on page 44).
- [6] Ian F. Akyildiz and Ismail H. Kasimoglu. “Wireless sensor and actor networks: research challenges”. In: *Ad Hoc Networks* 2.4 (2004), pages 351–367. ISSN: 15708705 (cited on page 10).
- [7] All Traffic Solutions. *All Traffic*. 2013. URL: <http://www.alltrafficsolutions.com/smartapps-video/smartapps-overview/> (cited on page 25).
- [8] U Alvarado et al. “Energy harvesting technologies for low-power electronics”. In: *Transactions on Emerging Telecommunications Technologies* 23.8 (2012), pages 728–741. ISSN: 2161-3915. DOI: 10 . 1002 / ett . 2529 (cited on page 52).
- [9] Amazon Inc. *Amazon Echo - Amazon Official Site - Alexa-Enabled*. 2016. URL: <https://www.amazon.com/Amazon-Echo-Bluetooth-Speaker-with-WiFi-Alexa/dp/B00X4WHP5E> (cited on page 70).
- [10] Amazon Inc. *Amazon Mechanical Turk - Welcome*. 2016. URL: <https://www.mturk.com/mturk/welcome> (cited on page 36).
- [11] Amazon Inc. *AWS IoT - Amazon Web Services*. 2016. URL: <https://aws.amazon.com/iot/> (cited on page 25).
- [12] Apple Inc. *HealthKit - Apple Developer*. 2016. URL: <https://developer.apple.com/healthkit/> (cited on page 33).
- [13] Apple Inc. *HomeKit - Apple Developer*. 2016. URL: <https://developer.apple.com/homekit/> (cited on page 33).
- [14] Applied Informatics Software Engineering GmbH. *macchina.io - Building Blocks for the Internet of Things*. 2016. URL: <https://macchina.io/> (cited on page 26).
- [15] Kevin Ashton. “That ‘Internet of Things’ Thing In the real world, things matter more than ideas”. In: *RFID Journal* (June 2009) (cited on page 8).

- [16] Alicia Asin and David Gascon. *50 Sensor Applications for a Smarter World*. Technical report. Libelium Comunicaciones Distribuidas, 2012 (cited on page 14).
- [17] Atmel Team. *A look back at the history of the Internet of Things | Atmel Bits and Pieces*. 2015. URL: <http://blog.atmel.com/2015/04/09/a-look-back-at-the-history-of-the-internet-of-things/> (cited on page 8).
- [18] Autodesk. *Autodesk Fusion Connect. Enterprise IoT Software Platform*. 2016. URL: <http://autodeskfusionconnect.com/> (cited on page 26).
- [19] Autographer. *Home - Autographer - The World's First Wearable camera*. 2013. URL: <http://www.autographer.com/%7B%5C#%7Dhome> (cited on page 19).
- [20] Tim Baarslag et al. “Negotiation as an Interaction Mechanism for Deciding App Permissions”. In: *ACM SIGCHI Conference Extended Abstract on Human Factors in Computing Systems*. 2016 (cited on page 82).
- [21] Tim Baarslag et al. *An Automated Negotiation Agent for Permission Management*. 2017. URL: <http://dl.acm.org/citation.cfm?id=3091184> (cited on page 92).
- [22] P Banerjee et al. “Everything as a Service: Powering the New Information Economy”. In: *Computer* 44.3 (Mar. 2011), pages 36–43. ISSN: 0018-9162. DOI: 10.1109/MC.2011.67 (cited on page 41).
- [23] Basis Science Inc. *BASIS*. URL: <http://www.mybasis.com/> (cited on page 17).
- [24] Beddit. *Beddit: Solve sleep without wearing anything*. 2016. URL: <http://www.beddit.com/> (cited on pages 17, 79).
- [25] Belkin International. *Mr. Coffee Smart Optimal Brew 10-Cup Programmable Coffee Maker with Wemo*. 2016. URL: <http://www.mrcoffee.com/coffee-makers/smart-optimal-brew-coffeemaker-with-wemo/mr-coffee-smart-optimal-brew-10-cup-programmable-coffee-maker-with-wemo-bvmc-pstx91we/BVMC-PSTX91WE.html> (cited on pages 22, 31).

- [26] Belkin International Inc. *WeMo Switch*. 2016. URL: <http://www.belkin.com/us/wemo-switch> (cited on pages 21, 22, 30).
- [27] Amel Bennaceur et al. “Feed me, feed me”. In: *Proceedings of the 11th International Workshop on Software Engineering for Adaptive and Self-Managing Systems - SEAMS '16*. New York, New York, USA: ACM Press, 2016, pages 89–95. ISBN: 9781450341875. DOI: 10.1145/2897053.2897071 (cited on page 80).
- [28] Bigbelly Solar Inc. *SmartBelly Components*. 2015. URL: <http://www.bigbelly.com/solutions/stations/smartbelly/> (cited on page 26).
- [29] BodyMedia. *LINK Armband*. 2013. URL: <http://www.bodymedia.com/> (cited on page 17).
- [30] A J Bernheim Brush et al. “Lab of Things: A Platform for Conducting Studies with Connected Devices in Multiple Homes”. In: *Proceedings of the 2013 ACM Conference on Pervasive and Ubiquitous Computing Adjunct Publication*. UbiComp '13 Adjunct. New York, NY, USA: ACM, 2013, pages 35–38. ISBN: 978-1-4503-2215-7. DOI: 10.1145/2494091.2502068 (cited on page 20).
- [31] Cantaloupe Systems. *Seed Platform*. 2012 (cited on page 29).
- [32] Andrea Caragliu, Chiara Del Bo, and Peter Nijkamp. “Smart cities in Europe”. In: *3rd Central European Conference in Regional Science-CERS*. Oct. 2009, pages 45–59 (cited on page 39).
- [33] Casaleggio Associati. *The Evolution of Internet of Things*. Technical report. Casaleggio Associati, Feb. 2011 (cited on page 8).
- [34] Leonardo Weiss Ferreira Chaves and Christian Decker. “A survey on organic smart labels for the Internet-of-Things”. In: *Networked Sensing Systems (INSS), 2010 Seventh International Conference on*. 2010, pages 161–164. DOI: 10.1109/INSS.2010.5573467 (cited on page 52).

- [35] Nanxi Chen, Nicolas Cardozo, and Siobhan Clarke. “Goal-Driven Service Composition in Mobile and Pervasive Computing”. In: *IEEE Transactions on Services Computing* 11.1 (2018), pages 49–62. ISSN: 19391374. DOI: 10.1109/TSC.2016.2533348 (cited on page 96).
- [36] Tung-Hsiang Chou and Jia-Lang Seng. “Telecommunication e-services orchestration enabling business process management”. In: *Transactions on Emerging Telecommunications Technologies* 23.7 (2012), pages 646–659. ISSN: 2161-3915. DOI: 10.1002/ett.2520 (cited on page 54).
- [37] H Chourabi et al. “Understanding Smart Cities: An Integrative Framework”. In: *System Science (HICSS), 45th Hawaii International Conference on*. 2012, pages 2289–2297. DOI: 10.1109/HICSS.2012.615 (cited on page 40).
- [38] Roger Clarke. *Introduction to Dataveillance and Information Privacy, and Definitions of Terms*. 2013. URL: <http://www.rogerclarke.com/DV/Intro.html> (cited on page 64).
- [39] Clemson University. *Intelligent River*. 2013. URL: <http://www.intelligentriver.org/> (cited on page 27).
- [40] Common Sense. *Common Sense Mobile sensing for community action*. 2012. URL: <http://www.communitysensing.org/> (cited on page 27).
- [41] Commonwealth Scientific and Industrial Research Organisation (CSIRO), Australia. *Phenonet: Distributed Sensor Network for Phenomics supported by High Resolution Plant Phenomics Centre, CSIRO ICT Centre, and CSIRO Sensor and Sensor Networks TCP*. 2011 (cited on page 53).
- [42] Connected Bits. *Street Bump*. 2016. URL: <http://www.streetbump.org/> (cited on page 25).
- [43] D J Cook et al. “CASAS: A Smart Home in a Box”. In: *Computer* 46.7 (2013), pages 62–69. ISSN: 0018-9162. DOI: 10.1109/MC.2012.328 (cited on page 19).
- [44] Council of Europe. *Convention for the Protection of Human Rights and Fundamental Freedoms*. 1950. URL: <http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/005> (cited on page 65).

- [45] Andy Crabtree and Richard Mortier. “Human Data Interaction: Historical Lessons from Social Studies and CSCW”. In: *Proceedings of the 14th European Conference on Computer Supported Cooperative Work, 19-23 September 2015, Oslo, Norway*. Edited by Nina Boulus-Rødje et al. Cham: Springer International Publishing, 2015. Chapter Human Data, pages 3–21. ISBN: 978-3-319-20499-4. DOI: 10.1007/978-3-319-20499-4_1 (cited on page 85).
- [46] CyberVision Inc. *Kaa Open-Source IoT Platform 2016 — IoT cloud platform the Internet of Things solutions and applications that set the standard*. 2016. URL: <http://www.kaaproject.org/> (cited on page 26).
- [47] George Danezis et al. *Privacy and Data Protection by Design - from policy to engineering*. Technical report. European Union Agency for Network and Information Security (ENISA), 2014, pages 1–79 (cited on page 65).
- [48] Datacoup. *Unlock the Value of Your Personal Data, Introducing the world’s first personal data marketplace*. 2016 (cited on page 85).
- [49] Alexandra Deschamps-Sonsino. *Good Night Lamp*. 2016. URL: <http://goodnightlamp.com/> (cited on page 22).
- [50] Colin Dixon et al. “An Operating System for the Home”. In: *Symposium on Networked Systems Design and Implementation (NSDI), USENIX*. Apr. 2012 (cited on page 20).
- [51] G Dror, N Koenigstein, and Y Koren. “Web-Scale Media Recommendation Systems”. In: *Proceedings of the IEEE* 100.9 (Sept. 2012), pages 2722–2736. ISSN: 0018-9219. DOI: 10.1109/JPROC.2012.2189529 (cited on page 35).
- [52] Ducere Technologies. *LeChal*. 2013. URL: <http://duceretech.com/products.html> (cited on page 19).
- [53] Echelon Corporation. *Smart Street Lighting*. 2013. URL: <https://www.echelon.com/applications/street-lighting> (cited on page 26).
- [54] ElectricFoxy. *ElectricFoxy*. 2013. URL: <http://www.electricfoxy.com/projects/pulse-stay-in-your-zone/> (cited on page 18).

- [55] Electronic House Staff. *5 Reasons Having a Smart Home Makes Your Life Better - Electronic House*. 2016. URL: <https://www.electronichouse.com/smart-home/5-reasons-having-a-smart-home-makes-your-life-better/> (cited on page 62).
- [56] EMBRACE+. 2013. URL: <https://shop.trycelery.com/page/embraceplus> (cited on page 17).
- [57] ENGAUGE. *Remote Fire Extinguisher Monitoring System*. 2016 (cited on page 29).
- [58] European Commission. *Internet of Things in 2020 Road Map For The Future*. Technical report. Working Group RFID of the ETP EPOSS, May 2008 (cited on page 8).
- [59] FIBAR GROUP. *Fibaro Home Center 2 | Z-Wave Smart Home System*. 2016. URL: <http://www.fibaro.com/us/the-fibaro-system/home-center-2> (cited on page 72).
- [60] Fitbit Inc. *Fitbit Aria Wi-Fi Smart Scale*. 2016. URL: <https://www.fitbit.com/uk/aria> (cited on page 72).
- [61] Fitbit Inc. *Fitbit Official Site for Activity Trackers & More*. 2016. URL: <https://www.fitbit.com/uk> (cited on pages 19, 32, 79).
- [62] GE Digital. *GE Predix*. 2016. URL: <https://www.predix.io/> (cited on page 25).
- [63] GEA Farm Technologies. *HeatWatch including Rescounter II technology: HeatWatch II*. Technical report. 2006 (cited on page 29).
- [64] D Gessner et al. “Trustworthy Infrastructure Services for a Secure and Privacy-Respecting Internet of Things”. In: *Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on*. 2012, pages 998–1003. DOI: 10.1109/TrustCom.2012.286 (cited on page 58).
- [65] Rudolf Giffinger et al. *Smart cities Ranking of European medium-sized cities*. Research Project Report. Centre of Regional Science, Vienna UT, Oct. 2007 (cited on page 40).

- [66] tado GmbH. *Tado: Smart heating control*. 2016. URL: <https://www.tado.com/gb/> (cited on page 22).
- [67] Google Inc. *Google Glass*. 2013. URL: <http://www.google.com/glass/start/> (cited on page 18).
- [68] Google Inc. *Google Fit | Google Developers*. 2016. URL: <https://developers.google.com/fit/> (cited on page 33).
- [69] Google Inc. *Google Home*. 2016. URL: <https://home.google.com/> (cited on page 72).
- [70] Google Inc. *Internet of Things (IoT) Solutions | Google Cloud Platform*. 2016. URL: <https://cloud.google.com/solutions/iot/> (cited on page 25).
- [71] Google Inc. *Introducing Google Opinion Rewards*. 2016 (cited on page 36).
- [72] Google Inc. *Nest Thermostat*. 2016. URL: <https://nest.com/thermostat/meet-nest-thermostat/> (cited on pages 22, 23, 31).
- [73] Google Inc. *Your Surveys - Google Consumer Surveys*. 2016. URL: <https://www.google.com/insights/consumersurveys/home> (cited on pages 36, 56).
- [74] Patrick Guillemin and Peter Friess. *Internet of Things Strategic Research Roadmap*. Technical report. The Cluster of European Research Projects, Sept. 2009 (cited on page 9).
- [75] Dominique Guinard. “Towards the web of things: Web mashups for embedded devices”. In: *In MEM 2009 in Proceedings of WWW 2009*. ACM. 2009 (cited on page 8).
- [76] V C Gungor et al. “Smart Grid Technologies: Communication Technologies and Standards”. In: *Industrial Informatics, IEEE Transactions on 7.4* (2011), pages 529–539. ISSN: 1551-3203. DOI: 10.1109/TII.2011.2166794 (cited on page 25).
- [77] V C Gungor et al. “A Survey on Smart Grid Potential Applications and Communication Requirements”. In: *Industrial Informatics, IEEE Transactions on 9.1* (2013), pages 28–42. ISSN: 1551-3203. DOI: 10.1109/TII.2012.2218253 (cited on page 25).

- [78] Habitatmap.org. *AirCasting*. 2013. URL: <http://www.aircasting.org/> (cited on page 27).
- [79] Dae-Man Han and Jae-Hyun Lim. “Design and implementation of smart home energy management systems based on zigbee”. In: *Consumer Electronics, IEEE Transactions on* 56.3 (2010), pages 1417–1425. ISSN: 0098-3063. DOI: 10.1109/TCE.2010.5606278 (cited on page 19).
- [80] HiKoB. *PROJECT GRIZZLY*. 2013 (cited on page 29).
- [81] Household Technology. *The Netatmo Weather Station, the weather station designed for iPhone and iPad, wifi weather station, air quality monitoring and wireless weather station*. 2016. URL: <http://www.netatmo.com/en-US/product> (cited on page 21).
- [82] HydroPoint Data Systems Inc. *Home - HydroPoint*. 2016. URL: <https://hydropoint.com/> (cited on page 28).
- [83] ICEdot. *ICEdot | ICEdot Crash Sensor*. 2013. URL: <http://site.icedot.org/site/crash-sensor/> (cited on page 18).
- [84] IEEE. *IEEE INTERNET OF THINGS JOURNAL - Home*. 2015. URL: <http://iot-journal.weebly.com/> (cited on page 9).
- [85] IFTTT Inc. *Learn how IFTTT works*. 2016. URL: <https://ifttt.com/> (cited on pages 34, 35).
- [86] F Iglesias and P Palensky. “Profile-Based Control for Central Domestic Hot Water Distribution”. In: *Industrial Informatics, IEEE Transactions on* 10.1 (2014), pages 697–705. ISSN: 1551-3203. DOI: 10.1109/TII.2013.2275032 (cited on page 19).
- [87] Impakt Protective Inc. *Shockbox - Concussion Management Helmet Sensors*. 2016. URL: <http://www.theshockbox.com/> (cited on page 18).
- [88] Insight Robotics. *Computer Vision Wildfire Detection System*. 2012. URL: <http://www.insightrobotics.com/content/computer-vision-wildfire-detection-system> (cited on page 27).

- [89] Insteon. *Insteon Hub* — Insteon. 2016. URL: <http://www.insteon.com/insteon-hub/> (cited on page 72).
- [90] International Telecommunication Union. *Internet of Things Global Standards Initiative*. 2015. URL: <http://www.itu.int/en/ITU-T/gsi/iot/Pages/default.aspx> (cited on page 9).
- [91] Patrick Gage Kelley et al. “A “nutrition label” for privacy”. In: *Proceedings of the 5th Symposium on Usable Privacy and Security SOUPS 09 1990* (2009), page 1 (cited on page 66).
- [92] Sye Loong Keoh, S S Kumar, and H Tschofenig. “Securing the Internet of Things: A Standardization Perspective”. In: *Internet of Things Journal, IEEE* 1.3 (June 2014), pages 265–275. ISSN: 2327-4662. DOI: 10.1109/JIOT.2014.2323395 (cited on page 35).
- [93] J Kiljander et al. “Semantic Interoperability Architecture for Pervasive Computing and Internet of Things”. In: *Access, IEEE* 2 (2014), pages 856–873. ISSN: 2169-3536. DOI: 10.1109/ACCESS.2014.2347992 (cited on page 33).
- [94] Jaewoo Kim et al. “M2M Service Platforms: Survey, Issues, and Enabling Technologies”. In: *IEEE Communications Surveys & Tutorials* 16.1 (2014), pages 61–76. ISSN: 1553-877X. DOI: 10.1109/SURV.2013.100713.00203. URL: <http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6644332> (cited on page 9).
- [95] O D Lara and M A Labrador. “A Survey on Human Activity Recognition using Wearable Sensors”. In: *Communications Surveys Tutorials, IEEE* 15.3 (2013), pages 1192–1209. ISSN: 1553-877X. DOI: 10.1109/SURV.2012.110112.00192 (cited on page 15).
- [96] Leo Inc. *Leo Smart Alert Smoke/CO Remote Alarm Monitor for iOS and Android*. 2016. URL: <https://shop.leeo.com/> (cited on page 24).
- [97] Han Li, Rathindra Sarathy, and Heng Xu. “Understanding Situational Online Information Disclosure as a Privacy Calculus”. In: *Journal of Computer Information Systems* 51.1 (2010), pages 62–71. DOI: 10.1080/08874417.2010.

11645450. URL: <http://www.tandfonline.com/doi/abs/10.1080/08874417.2010.11645450> (cited on page 80).
- [98] Libelium Comunicaciones Distribuidas. *libelium*. 2006 (cited on pages 25, 44).
- [99] Lifesum AB. *Lifesum Health app - Get healthy, lose weight, or gain muscle*. 2016. URL: <https://lifesum.com/> (cited on page 43).
- [100] Linux Foundation. *AllJoyn Framework*. 2016. URL: <https://allseenalliance.org/framework> (visited on 06/26/2016) (cited on page 34).
- [101] Lockitron. *Lockitron: Unlock Bolt from anywhere*. 2016. URL: <https://lockitron.com/> (cited on page 22).
- [102] Tan Lu and Wang Neng. “Future internet: The Internet of Things”. In: *3rd International Conference on Advanced Computer Theory and Engineering(ICACTE)*. Volume 5. Aug. 2010, pages V5–376—V5–380. DOI: 10.1109/ICACTE.2010.5579543 (cited on page 9).
- [103] Knud Lasse Lueth. *Why it is called Internet of Things: Definition, history, disambiguation*. 2014. URL: <https://iot-analytics.com/internet-of-things-definition/> (cited on pages 8–10).
- [104] Inc. LUMO Body Tech. *LUMOback*. 2016. URL: <http://www.lumoback.com/> (cited on page 17).
- [105] LYT Inc. *ALYT - Link your things*. 2016. URL: <https://www.alyt.com/> (cited on page 72).
- [106] Marketsandmarkets. *Cloud Computing Market: Global Forecast (2010 - 2015)*. Worldwide Market Report. marketsandmarkets, Oct. 2010 (cited on page 42).
- [107] John McKerrell. *WhereDial*. 2013. URL: <http://www.wheredial.com/> (cited on page 22).
- [108] Corey Menscher. *Kickbee*. 2013. URL: <http://kickbee.net/> (cited on page 17).

- [109] Microsoft. *Azure IoT Suite—Connect Devices and Data | Microsoft*. 2016. URL: <https://www.microsoft.com/en-us/cloud-platform/internet-of-things-azure-iot-suite> (cited on page 25).
- [110] MicroStrain Inc. *Shelburne Vineyard Remote Monitoring*. 2013. URL: <http://www.microstrain.com/news/shelburne-vineyard-relies-wireless-sensors-and-cloud-monitor-its-vines> (cited on page 27).
- [111] Julien Mineraud et al. “A gap analysis of Internet-of-Things platforms”. In: *Computer Communications* 89 (2016), pages 5–16. ISSN: 01403664 (cited on page 26).
- [112] Roberto Minerva, Abyi Biru, and Domenico Rotondi. *Towards a definition of the Internet of Things (IoT)*. Technical report. IEEE Internet Initiative, 2015. URL: <http://iot.ieee.org/> (cited on page 11).
- [113] CMU Mobile Commerce Lab. *Livehoods*. 2013. URL: <http://livehoods.org/> (cited on page 26).
- [114] Michaela Mora. “customer Insights: Insightful planning”. In: *Dallas Business Journals* (May 2010) (cited on pages 36, 56).
- [115] Asher Moses. *LG smart fridge tells you what to buy, cook and eat*. The Sydney Morning Herald. Jan. 2012 (cited on page 80).
- [116] Motionloft. *Motionloft property analytics*. 2013 (cited on page 30).
- [117] P J Nesse et al. “Assessment and optimisation of business opportunities for telecom operators in the cloud value network”. In: *Transactions on Emerging Telecommunications Technologies* (2013), n/a–n/a. ISSN: 2161-3915. DOI: 10.1002/ett.2666 (cited on page 45).
- [118] Ninja Blocks Pty Ltd. *Ninja Blocks*. 2013. URL: <http://ninjablocks.com/> (cited on page 20).
- [119] Luiz Henrique Nunes et al. “Multi-criteria IoT resource discovery: a comparative analysis”. In: *Software: Practice and Experience* (Dec. 2016). ISSN: 00380644. DOI: 10.1002/spe.2469. URL: <http://doi.wiley.com/10.1002/spe.2469> (cited on page 45).

- [120] Luiz H Nunes et al. “The Effects of Relative Importance of User Constraints in Cloud of Things Resource Discovery: A Case Study”. In: *Proceedings of the 9th International Conference on Utility and Cloud Computing*. UCC ’16. New York, NY, USA: ACM, 2016, pages 245–250. ISBN: 978-1-4503-4616-0. DOI: 10.1145/2996890.3007867. URL: <http://doi.acm.org/10.1145/2996890.3007867> (cited on page 45).
- [121] Luiz Nunes et al. “A Distributed Sensor Data Search Platform for Internet of Things Environments”. In: *International Journal of Services Computing* 4.2 (June 2016), pages 1–12. arXiv: 1606.07932. URL: <http://arxiv.org/abs/1606.07932> (cited on page 45).
- [122] Oakley Inc. *Oakley Airwave Goggles*. 2013. URL: <http://www.oakley.com/airwave/> (cited on page 18).
- [123] OleoApps Inc. *BlueFit: smart water bottle*. 2013. URL: <http://blufitbottle.com/> (cited on page 22).
- [124] Natalia Olifer and Victor Olifer. *Computer Networks: Principles, Technologies and Protocols for Network Design*. John Wiley & Sons, 2005. URL: <http://au.wiley.com/WileyCDA/WileyTitle/productCd-EHEP000983.html> (cited on page 7).
- [125] OnFarm Systems Inc. *OnFarm*. 2012 (cited on page 29).
- [126] OpenIoT Consortium. *Open Source Solution for the Internet of Things into the Cloud*. Jan. 2012 (cited on pages 26, 53).
- [127] OpenSprinkler. *OpenSprinkler*. 2016. URL: <https://opensprinkler.com/> (cited on pages 22, 30).
- [128] Oracle Corporation. *Internet of Things | Oracle Cloud*. 2016. URL: <https://cloud.oracle.com/iot> (cited on page 25).
- [129] Oxford University Press. *privacy - definition of privacy in English from the Oxford dictionary*. 2016. URL: <http://www.oxforddictionaries.com/definition/english/privacy> (cited on page 64).

- [130] Leysia Palen and Paul Dourish. “Unpacking “Privacy” for a Networked World”. In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. CHI ’03. New York, NY, USA: ACM, 2003, pages 129–136. ISBN: 1-58113-630-7. DOI: 10.1145/642611.642635 (cited on page 76).
- [131] A Pantelopoulos and N G Bourbakis. “A Survey on Wearable Sensor-Based Systems for Health Monitoring and Prognosis”. In: *Systems, Man, and Cybernetics, Part C: Applications and Reviews, IEEE Transactions on* 40.1 (2010), pages 1–12. ISSN: 1094-6977. DOI: 10.1109/TSMCC.2009.2032660 (cited on page 15).
- [132] S Patidar, D Rane, and P Jain. “A Survey Paper on Cloud Computing”. In: *Advanced Computing Communication Technologies (ACCT), 2012 Second International Conference on*. 2012, pages 394–398. DOI: 10.1109/ACCT.2012.15 (cited on pages 41, 42).
- [133] Amrita Vishwa Vidya Peetham. *AmritaWNA: Amrita Center for Wireless Networks and Applications*. 2013. URL: <http://amrita.edu/awna/> (cited on page 27).
- [134] Leif Percifield. *dontflush.me*. 2013. URL: <http://dontflush.me/> (cited on page 27).
- [135] Charith Perera, Chi Harold Liu, and Srimal Jayawardena. “A Survey on Internet of Things From Industrial Market Perspective”. In: *IEEE Access* 2 (2014), pages 1660–1679. ISSN: 2169-3536. DOI: 10.1109/ACCESS.2015.2389854 (cited on pages 30, 62).
- [136] Charith Perera, Chi Harold Liu, and Srimal Jayawardena. “The Emerging Internet of Things Marketplace from an Industrial Perspective: A Survey”. In: *IEEE Transactions on Emerging Topics in Computing* 3.4 (2015), pages 585–598. ISSN: 21686750 (cited on pages 30, 62, 67).
- [137] Charith Perera, Rajiv Ranjan, and Lizhe Wang. “End-to-End Privacy for Open Big Data Markets”. In: *IEEE Cloud Computing* 2.4 (July 2015), pages 44–53. ISSN: 2325-6095 (cited on pages 76, 83).

- [138] Charith Perera and Athanasios V. Vasilakos. “A knowledge-based resource discovery for Internet of Things”. In: *Knowledge-Based Systems* 109 (2016), pages 122–136. ISSN: 09507051. DOI: 10.1016/j.knosys.2016.06.030. arXiv: arXiv:1606.08968v1 (cited on page 45).
- [139] Charith Perera and Arkady Zaslavsky. “Improve the sustainability of Internet of Things through trading-based value creation”. In: *Internet of Things (WF-IoT), 2014 IEEE World Forum on*. Mar. 2014, pages 135–140. DOI: 10.1109/WF-IoT.2014.6803135 (cited on page 59).
- [140] Charith Perera et al. “CA4IOT: Context awareness for Internet of Things”. In: *Proceedings - 2012 IEEE Int. Conf. on Green Computing and Communications, GreenCom 2012, Conf. on Internet of Things, iThings 2012 and Conf. on Cyber, Physical and Social Computing, CPSCoM 2012*. 2012, pages 775–782. ISBN: 9780769548654. DOI: 10.1109/GreenCom.2012.128 (cited on page 45).
- [141] Charith Perera et al. “Context-aware Sensor Search, Selection and Ranking Model for Internet of Things Middleware”. In: *IEEE 14th International Conference on Mobile Data Management (MDM)*. Milan, Italy, June 2013 (cited on page 45).
- [142] Charith Perera et al. “Sensing as a service model for smart cities supported by Internet of Things”. In: *European Transactions on Telecommunications* 25.1 (2014), pages 81–93. ISSN: 1124318X. DOI: 10.1002/ett.2704 (cited on pages 5, 25).
- [143] Charith Perera et al. “Big data privacy in the internet of things era”. In: *IT Professional* 17.3 (2015), pages 32–39. ISSN: 15209202. arXiv: 1412.8339 (cited on page 76).
- [144] Charith Perera et al. “Energy-Efficient Location and Activity-Aware On-Demand Mobile Distributed Sensing Platform for Sensing as a Service in IoT Clouds”. In: *IEEE Transactions on Computational Social Systems* 2.4 (Dec. 2015), pages 171–181. ISSN: 2329-924X (cited on page 41).

- [145] Charith Perera et al. “Fog Computing for Sustainable Smart Cities: A Survey”. In: *ACM Computing Surveys* pp.pp (2016), pp (cited on page 70).
- [146] Charith Perera et al. “Privacy-Knowledge Modeling for the Internet of Things: A Look Back”. In: *Computer* 49.12 (Dec. 2016), pages 60–68. ISSN: 0018-9162. DOI: 10.1109/MC.2016.366. URL: <http://ieeexplore.ieee.org/document/7756262/> (cited on page 77).
- [147] C Perera et al. “Sensor Search Techniques for Sensing as a Service Architecture for the Internet of Things”. In: *Sensors Journal, IEEE* 14.2 (2014), pages 406–420. ISSN: 1530-437X. DOI: 10.1109/JSEN.2013.2282292. arXiv: arXiv:1309.3618v1 (cited on page 45).
- [148] C. Perera et al. “Valorising the IoT Databox: creating value for everyone”. In: *Transactions on Emerging Telecommunications Technologies* 28.1 (2017). ISSN: 21613915. DOI: 10.1002/ett.3125 (cited on page 87).
- [149] Philips. *Meethue Personal Wireless Lighting*. 2016. URL: <http://www2.meethue.com/en-gb/> (cited on pages 21, 33).
- [150] Postscapes.com. *Internet of Things History | Background and Timeline of the Topic*. 2016. URL: <https://postscapes.com/internet-of-things-history/> (cited on page 8).
- [151] Postscapes.com. *IoT Cloud Platform Landscape | 2016 Vendor List*. 2016. URL: <http://www.postscapes.com/internet-of-things-platforms/> (cited on page 26).
- [152] Gil Press. *A Very Short History Of The Internet Of Things - Forbes*. 2014. URL: <http://www.forbes.com/sites/gilpress/2014/06/18/a-very-short-history-of-the-internet-of-things/3/%7B%5C#%7D2506b07543c5> (cited on page 8).
- [153] Preventice Solutions Inc. *BodyGuardian Remote Monitoring System*. Technical report. <http://www.preventice.com/products/bodyguardian/>, 2013 (cited on page 19).

- [154] Blaine A Price et al. “ContraVision: Presenting Contrasting Visions of Future Technology”. In: *CHI '10 Extended Abstracts on Human Factors in Computing Systems*. CHI EA '10. New York, NY, USA: ACM, 2010, pages 4759–4764. ISBN: 978-1-60558-930-5 (cited on page 81).
- [155] Bionym product. *Nymi | Convenient Authentication Anywhere*. 2016. URL: <https://nyimi.com/> (cited on page 18).
- [156] Proteus Digital Health. *Proteus Digital Health*. 2016. URL: <http://proteusdigitalhealth.com/> (cited on page 19).
- [157] PTC. *Enterprise IoT Solutions and Platform Technology : ThingWorx*. 2016. URL: <https://www.thingworx.com/> (cited on page 25).
- [158] Mohammad Abdur Razzaque et al. “Middleware for Internet of Things: A Survey”. In: *IEEE Internet of Things Journal* 3.1 (Feb. 2016), pages 70–95. ISSN: 2327-4662 (cited on page 26).
- [159] Inc. Rest Devices. *Mimobaby: A Baby Monitor*. 2015. URL: <http://mimobaby.com/> (visited on 08/12/2016) (cited on page 15).
- [160] Bhaskar Prasad Rimal, Eunmi Choi, and Ian Lumb. “A Taxonomy and Survey of Cloud Computing Systems”. In: *Proceedings of the 2009 Fifth International Joint Conference on INC, IMS and IDC*. NCM '09. Washington, DC, USA: IEEE Computer Society, 2009, pages 44–51. ISBN: 978-0-7695-3769-6. DOI: 10.1109/NCM.2009.218 (cited on page 42).
- [161] Rodrigo Roman, Jianying Zhou, and Javier Lopez. “On the features and challenges of security and privacy in distributed internet of things”. In: *Computer Networks* 57.10 (2013), pages 2266–2279 (cited on page 13).
- [162] S Sakr et al. “A Survey of Large Scale Data Management Approaches in Cloud Environments”. In: *Communications Surveys Tutorials, IEEE* 13.3 (2011), pages 311–336. ISSN: 1553-877X. DOI: 10.1109/SURV.2011.032211.00087 (cited on page 54).

- [163] Samsung. *No Title*. 2016. URL: <https://www.smartthings.com/uk/> (cited on pages 19, 72).
- [164] Nik Sargent. *Bumblebee nesting project*. 2013. URL: <http://niksargent.com/bumblebee> (cited on page 28).
- [165] SceneTap. *SceneTap*. 2013. URL: <http://scenetap.com/> (cited on page 26).
- [166] SectorQube. *Make All Incredible Dishes*. 2016. URL: <http://maidoven.com/> (cited on pages 22, 32).
- [167] SenseAware. *Be in control: Get ready to transform your supply chain*. Technical report. 2013 (cited on page 28).
- [168] Sensoria. *Sensoria Smart Sock*. 2013. URL: <http://www.heapsylon.com/welcome-to-sensoria/> (cited on page 19).
- [169] Seraphim Sense Ltd. *Angel Sensor – Open Mobile Health Wearable | The future of health and well being*. 2016. URL: <http://angelsensor.com/> (cited on page 17).
- [170] SHOAL Project Consortium. *Shoal*. 2012. URL: <http://www.roboshoal.com/> (cited on page 27).
- [171] *ShutterEaze | Motorized Plantation Shutters Retrofit Solution*. 2016. URL: <http://shuttereaze.com/> (cited on page 23).
- [172] Sight Machine. *Sight Machine*. 2013 (cited on page 29).
- [173] Smart Structures. *Smart Structures, The global leader in wireless Embedded Data Collector (EDC) solutions to improve quality of bridge pilings and deep foundations*. 2014. URL: <http://smart-structures.com/> (cited on page 29).
- [174] Daniel J Solove. “A Taxonomy of Privacy”. In: *University of Pennsylvania Law Review* 154.3 (Jan. 2006), page 477 (cited on pages 63, 83).
- [175] Sarah Spiekermann. *Online information search with electronic agents: drivers, impediments. and privacy issues*. Hochschulschrift, Dissertation, Thesis, Graue Literatur, Non-commercial literature. 2001. URL: <http://www.econbiz.de/Record/online-information-search-with-electronic-agents-drivers-impediments->

- and - privacy - issues - spiekermann - sarah / 10001679229 (cited on page 77).
- [176] T Starner. “The challenges of wearable computing: Part 1”. In: *Micro, IEEE* 21.4 (2001), pages 44–52. ISSN: 0272-1732. DOI: 10.1109/40.946681 (cited on page 15).
- [177] Streetline. *ParkSight*. 2013. URL: <http://www.streetline.com/our-solutions/> (cited on page 25).
- [178] Kehua Su, Jie Li, and Hongbo Fu. “Smart city and the applications”. In: *Electronics, Communications and Control (ICECC), 2011 International Conference on*. 2011, pages 1028–1031. DOI: 10.1109/ICECC.2011.6066743 (cited on pages 24, 40).
- [179] Harald Sundmaeker et al. *Vision and Challenges for Realising the Internet of Things*. Technical report. European Commission Information Society and Media, Mar. 2010 (cited on page 39).
- [180] Supermechanical Limited Liability Company. *Twine*. 2016. URL: <http://supermechanical.com/> (cited on pages 20, 21).
- [181] Lark technologies. *Lark: Meet Lark, your personal weight loss coach*. 2016. URL: <http://www.web.lark.com/> (cited on page 17).
- [182] Tware. *Non-weighted wearable tech hug vest that calms kids and adults with anxiety, stress, sensory overload*. 2016. URL: <http://www.mytjacket.com/> (cited on page 17).
- [183] Uber Inc. *Sign Up to Drive or Tap and Ride | Uber*. 2016. URL: <https://www.uber.com/> (cited on page 25).
- [184] Unified Computer Intelligence Corporation. *Ubi*. 2016. URL: <http://www.ucic.io/> (cited on page 21).
- [185] United for Human Rights. *Privacy Rights Video, Declaration of Human Rights: United for Human Rights*. 2008. URL: <http://www.humanrights.com/what-are-human-rights/videos/right-to-privacy.html> (cited on page 65).

- [186] United Nations. *The Universal Declaration of Human Rights* | United Nations. 1948. URL: <http://www.un.org/en/universal-declaration-human-rights/index.html> (cited on page 65).
- [187] University of California Berkeley. *Floating Sensor Network*. 2012. URL: <http://float.berkeley.edu/> (cited on page 27).
- [188] Vera Control Ltd. *VeraLite Smart Home Controller*. 2016. URL: <http://getvera.com/controllers/veralite/> (cited on page 72).
- [189] F Viani et al. “Wireless Architectures for Heterogeneous Sensing in Smart Home Applications: Concepts and Real Implementation”. In: *Proceedings of the IEEE* 101.11 (2013), pages 2381–2396. ISSN: 0018-9219. DOI: 10.1109/JPROC.2013.2266858 (cited on page 19).
- [190] Meisong Wang et al. “City Data Fusion: Sensor Data Fusion in the Internet of Things”. In: *Accepted for publication in International Journal of Distributed Systems and Technologies (IJDST)* 7.1 (2015), pages 15–36. ISSN: 19473540. DOI: 10.4018/IJDST.2016010102. arXiv: 1506.09118 (cited on page 39).
- [191] Thomas Watteyne et al. “OpenWSN: a standards-based low-power wireless development environment”. In: *Transactions on Emerging Telecommunications Technologies* 23.5 (2012), pages 480–493. ISSN: 2161-3915. DOI: 10.1002/ett.2558 (cited on page 52).
- [192] Wattics. *Smart metering*. 2011 (cited on page 29).
- [193] A Westin. *Privacy on & off the Internet: What consumers want*. Technical report. Tech. Report for Privacy & American Business. Hackensack, NJ: Privacy & American Business, 2001 (cited on page 77).
- [194] Alan Westin. “Privacy And Freedom”. In: *Washington and Lee Law Review* 25.1 (1968). ISSN: 0043-0463 (cited on page 63).
- [195] Wikimedia Foundation Inc. *Smart city*. 2016. URL: https://en.wikipedia.org/wiki/Smart%7B%5C_%7Dcity (cited on page 40).

- [196] Chao-Lin Wu and Li-Chen Fu. “Design and Realization of a Framework for Human-System Interaction in Smart Homes”. In: *Systems, Man and Cybernetics, Part A: Systems and Humans, IEEE Transactions on* 42.1 (2012), pages 15–31. ISSN: 1083-4427. DOI: 10 . 1109 / TSMCA . 2011 . 2159584 (cited on page 19).
- [197] Xively. *Xively-Public Cloud for the Internet of Things*. 2013 (cited on page 25).
- [198] M Yang et al. “Adaptive Sharing for Online Social Networks: A Trade-off Between Privacy Risk and Social Benefit”. In: *2014 IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications*. Sept. 2014, pages 45–52. DOI: 10 . 1109 / TrustCom . 2014 . 10 (cited on page 83).
- [199] Yanzi Networks AB. *Remote Site Management*. 2011 (cited on page 29).
- [200] Arkady Zaslavsky, Charith Perera, and Dimitrios Georgakopoulos. “Sensing as a Service and Big Data”. In: *International Conference on Advances in Cloud Computing (ACC)*. Bangalore, India, July 2012, pages 21–29 (cited on page 5).
- [201] Zephyr Technology Corp. *BioHarness*. 2013. URL: <http://zephyr-technology.com/products/> (cited on page 17).
- [202] Zepp US Inc. *Zepp | Sensors to Take your game to the next level*. 2016. URL: <http://www.zepp.com/en-us/> (cited on page 18).
- [203] Y Zhang et al. “Auction Approaches for Resource Allocation in Wireless Systems: A Survey”. In: *Communications Surveys Tutorials, IEEE* PP.99 (2012), pages 1–22. ISSN: 1553-877X. DOI: 10 . 1109 / SURV . 2012 . 110112 . 00125 (cited on page 46).
- [204] Minqi Zhou et al. “Services in the Cloud Computing era: A survey”. In: *Universal Communication Symposium (IUCS), 2010 4th International*. 2010, pages 40–46. DOI: 10 . 1109 / IUCS . 2010 . 5666772 (cited on page 42).

