Chapter 11
The Internet of Things: Promise of a Better Connected World

George R.S. Weir

11.1 Introduction

In recent years, progress in network-based applications has allowed a move beyond the staple asynchronous communication of email in which each party takes turns to compose and send a digital variation on traditional postal mail. Increasingly, synchronous (live) interaction between parties is possible through audio, video and typed digital channels by means of applications such as *Skype*, Facebook *Messenger* and Apple *Facetime*.

Although email remains a prevalent medium, users have also come to embrace social networking as a basis for selective broadcast and group interaction. These innovative applications are widely adopted across sectors, age groups and nations, in the take-up of laptops, smartphones and tablets. Of course, the increased use of networked devices reflects an associated growth in networking infrastructure. Wireless communication is normal practice in the use of mobile devices as well as a convenient basis for local area networks.

Increasing Internet use and the ready availability of connected information is often regarded as a natural step toward a greater degree of interconnectivity in which many of the devices in our homes, offices and factories become linked and capable of communication and control via local networks. In this chapter, we consider how the current context gives rise to the ideas behind the *Internet of Things* (IoT), look at how such extensive systems would function, and consider what benefits and disadvantages we may expect from such developments. As well as considering the present state of play, we will review the key ingredients, likely applications, ecosystem requirements, potential issues and prospects for a happy future enabled by IoT.

G.R.S. Weir (✉)
University of Strathclyde, Glasgow, UK
e-mail: george.weir@strath.ac.uk

P. Hehenberger and D. Bradley (eds.), *Mechatronic Futures*,
DOI 10.1007/978-3-319-32156-1_11

11.2 Impetus

There are several factors in our current technological context that naturally direct developments toward the extended integration and enhanced data exchange that is core to the Internet of Things. On the one hand, there is familiarity with increasingly functional and immediate communication facilities, with the associated expectation that other information systems will be equally immediate and responsive. On the other hand, rising service costs are an impetus toward wider deployment of networked devices, since such developments are seen as a means to cheaper service provision and, especially, service monitoring. Thus, there is growing anticipation of integrated systems that afford greater convenience, new services and more economical provision of existing services. We may assume that '*A typical home will soon contain a network of gadgets designed to make life easier*' [1].

11.2.1 Government Initiatives

In the UK, a report entitled '*The Internet of Things: making the most of the Second Digital Revolution*' [2] was prepared by the UK Government Chief Scientific Adviser. In the USA:

> … the Federal government is working now to direct development and testing of such systems with an eye toward a variety of future applications. The US government calls such technology "Cyber-Physical Systems" (CPS) and is looking for ways they can be used to improve safety, sustainability, efficiency, mobility and the overall quality of life [3].

In a similar vein:

> The Singapore government has introduced a slew of initiatives as part of its goal to become the world's first smart nation, including a smart nation operating system, Internet of Things scheme targeted at homes, and pilot trials at a designated residential-business estate. [4]

Nations with developing economies are also rising to the IoT opportunity. For instance in India:

> One of the top most initiatives in the form of Digital India Program of the Government which aims at 'transforming India into digital empowered society and knowledge economy', is expected to provide the required impetus for development of the IoT industry ecosystem in the country" [5]

Each of these national perspectives reflects the view that engaging with IoT developments will enhance the welfare of the population and the economic benefit of the country. What then are the required ingredients for such progress in any nation?

11.2.2 Key Ingredients

The UK government report [2] identifies three key ingredients in the Internet of Things ecosystem:

(i) Communication;
(ii) Integration;
(iii) Data analysis.

First among these ingredients is the present and evolving communication infrastructure, comprising existing '*fixed*' network facilities, in addition to wireless technologies, such as Wireless LAN (WLAN), Bluetooth, GPRS (GSM) mobile telephony standards and anticipated new standards for '*near-field*' and close-proximity device interaction.

Integration is considered essential since the scope for IoT will depend upon the consolidation of diverse systems and standards, with '*local*' systems talking to each other and to '*upper level*' systems. Finally, data analysis appears in two roles. First, such analysis serves as a means of monitoring and managing the quality of interaction between devices (e.g. for fault detection), and second, as a value-added ingredient that provides insight on usage and performance. (e.g. for targeting bandwidth and premium enhancements). The expectation is that integrated systems will support widely distributed data gathering as well as centralised synthesis and analysis of data.

11.2.3 Applications

Within the UK government report, five core sectors are identified as having major potential to boost the UK economy through IoT developments

(i) Home automation
(ii) Agriculture
(iii) Energy
(iv) Healthcare
(v) Transport

For each of these sectors, we can anticipate IoT applications with significant economic potential. Home automation should have wide appeal and would apply not only to individual dwellings but also in the context of larger-scale building management systems designed to coordinate multiple interior systems, such as air conditioning, temperature and lighting. Small-scale automation facilities are already available for home use. These include '*smart thermostats*' that are network-accessible for remote control. Production and yield management in agriculture and other manufacturing contexts stand to benefit from the introduction of sensor-based feedback and automation.

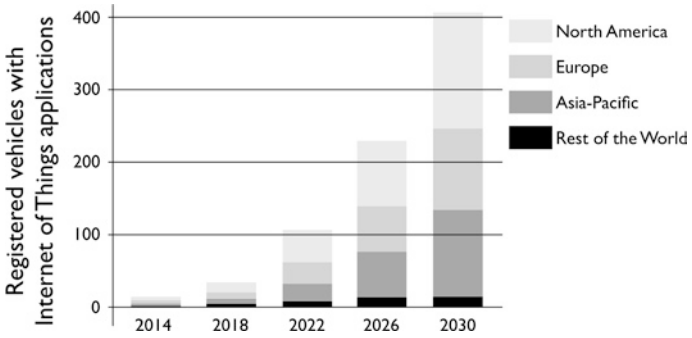

Fig. 11.1 Anticipated growth of in-car IoT applications (after *Smart Cars and the IoT* [10])

The energy sector has already shown movement in the direction of IoT through introduction of smart metres. These systems go beyond mere recording of total energy consumption to reporting consumption and usage patterns to the provider. Healthcare is an important application sector for IoT primarily from a cost efficiency perspective. The prospect of reduced cost health services through remote delivery (eHealth) is an eagerly anticipated economic boon for a presently overstretched and cash-strapped National Health Service.

In the transport sector government advisers predict significant growth in the use of in-car sensors, telemetry and inter-vehicle communication, as a basis for self-driving vehicles (Fig. 11.1). Progress in such smart transport is illustrated by the *Cooperative ITS Corridor*, an EU project to manage cars from Rotterdam via Munich, Frankfurt and on to Vienna [6].

Roads equipped with cameras every 100 m and WiFi antennas every 500 m, combine with short-range '*car-to-road*' communication, in order to measure the exact position of vehicles 10 times per second, within 1 m accuracy. Among the perceived benefits are improved flow management, such as addressing the '*braking shockwave*' problem on motorways, warning drivers of upcoming roadwork and other obstacles. Such initiatives also aim to harmonize smart-road standards among different countries. At first, such systems only employ '*car-to-roadside*' communication, with plans to extend this later to '*include car-to-car*' interaction.

While these anticipated economic benefits are central to IoT promotion by governments, we can already see relevant devices and technologies entering the marketplace that will contribute to the adoption and growth of IoT. The prevalence of home WiFi networks affords a convenient infrastructure for introducing the so-called '*smart*' devices with network communication capabilities. These vary from domestic appliances such as toasters and kettles, through wirelessly controlled light switches and multi-room digital music systems, to toothbrushes that report the effectiveness of their use through Bluetooth connectivity. In the home context, control facilities are readily afforded through mobile telephone apps or apps for Android and iOS tablets. These examples illustrate the potential integration of seemingly disparate systems.

In the realm of mobile systems, smartphones already support WiFi, Bluetooth and near-field connectivity. In conjunction with in-built GPS capability and suitable software applications, these phones can seamlessly interact with the local environment, registering their presence (or the presence of the telephone user), registering relevant localized data for presentation to the user and reacting to personalized settings or user preferences, based upon time of day and geographical position. Increasingly appearing as supplements to the ever-present smartphone, we find smart watches, fitness trackers and other wearable devices, such as clothes with in-built sensors. In keeping with domestic device development, these wearable devices build upon the functionality embedded in telephones and tablets to engage data processing and communication facilities. A case in point is the wearable PoloTech™ smart shirt from Ralph Lauren that measures the wearer's heart rate and respiration, distance travelled and calories burned, with data transferred to smartphone or tablet via Bluetooth.

11.2.4 Ecosystem Requirements

To appreciate the variety of prospective applications, we should consider the range of device types, the networking modalities and the methods of communication that are likely to comprise the essential infrastructure or ecosystem for the Internet of Things. One essential aspect of such technologies is the inherent flexibility that arises from multiple scales of device (with differing capabilities), different means of establishing intercommunication with other devices and a variety of alternative network topologies to suit differing needs. In terms of device capability, and associated scale, we may distinguish three device varieties, characterised by the roles that they play:

(i) Location markers (Passive).
(ii) Data gathering and relay (Active).
(iii) Decision-making (Active).

While we may naturally think of computation and data processing as necessary features of IoT devices, considerable utility can be added through the use of 'passive' objects as components within a local network. Such objects are passive in the sense that they have no native facility for generating, sensing or processing data. Instead, they are able to signify their presence through use of '*location markers*'. These markers may be based on Radio Frequency Identification (RFID) tags that can be detected by RFID sensors. Such '*smart labels*' may be battery-powered and actively send their ID by radio waves or simply wait to be read by an active RFID reader. The sole purpose of such tags is to signify the identity and presence (location) of the objects to which they are attached. The objects and the tags may be passive but detectable by other active systems. This allows for detecting or tracking tagged items and transfer of such information to local or remote computers.

The second variety of device has the native facility to capture and relay data. This requires some sensor capability but, while in this sense active may have little or no data processing capacity. The principal role for these sensor-based devices is to gather local data and relay this to other more sophisticated devices where the data from multiple sensor devices will be collated, aggregated and, perhaps, analysed. Our third variety of device covers those that actively process received data. This includes any active device that receives sensor information directly or indirectly, via other sensor systems. Combinations of these three device varieties support a hierarchical structure that allows data to be passed '*upstream*' from multiple sources to be collated and analysed; potentially, from local through district and regional to national and beyond.

This hierarchy of interlinked components will rely upon several types of network topologies. There will be scope for close-proximity communication based upon an ad hoc network topology. This will support interaction from device to device in cases if these devices are at a similar level of data gathering and distribution (i.e. peer to peer). From sensor-based, passive items and mobile devices, data will be communicated to local networks and is likely to rely upon current technologies, such as WLAN and Bluetooth. In turn, LANs have connection through Internet Service Providers to wider area networks. Thereby, the different networking models will integrate and interact to provide an infrastructure at different levels of complexity.

A complementary perspective on these networking models considers the interactions between devices and systems in terms of communication. These models represent the mode of interaction between different devices in the networking context. A common interaction model is client–server (Fig. 11.2). This is the traditional form of Internet communication in which many smaller-scale systems interact via one or more larger-scale systems.

Another 'style' of communication between systems that has become common on the Internet is peer-to-peer interaction. This is characterised by systems or devices communicating directly with other similarly scaled systems (Fig. 11.3).

A less common approach to communication is also feasible. In this case, individual devices communicate with a central system that provides a repository of data and results. This allows each device both to deposit and to query the central

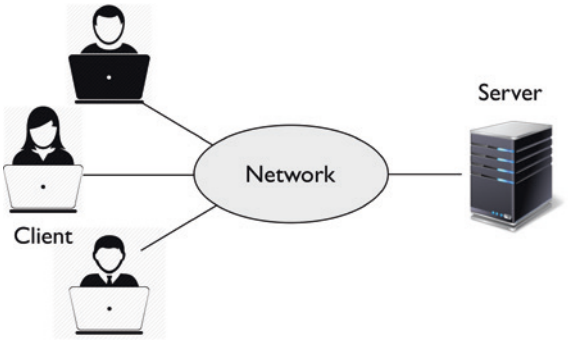

Fig. 11.2 Client–server communication model

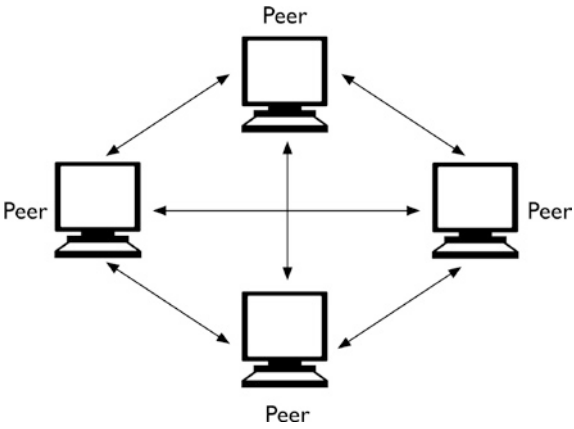

Fig. 11.3 Peer-to-peer communication model

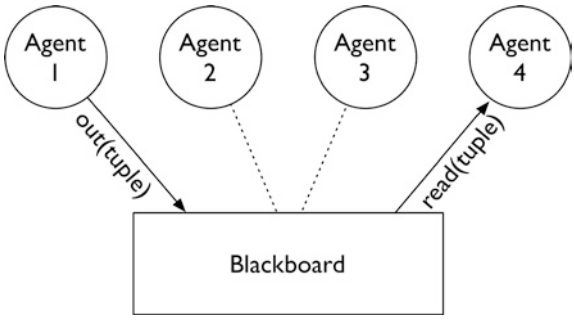

Fig. 11.4 Blackboard communication model

repository. This may be described as a '*blackboard*' model (Fig. 11.4) and shares many features of what has come to be called cloud computing.

The likelihood is that any significant installation associated with IoT would engage several of these communication models, while most individual components may employ a single model, most probably, the client–server or peer-to-peer approach.

With the increasing presence of communications infrastructure and interoperability of mobile devices comes new possibilities in tracking and monitoring of domestic objects outside the home—children, pets, vehicles, mobile phones and people. Of course, this is a double-edged sword that promises utility but also raises issues of civil liberty and personal privacy.

As part of a domestic or commercial IoT ecosystem, we have the promise of smart inventory, regulated service reports and associated ease of auditing and data production (e.g. for insurance purposes or home reports when selling property). Other features in prospect are highly integrated monitoring and control of heating, cooling and energy management at the domestic, district, regional and national level. Such environment monitoring for smart control may embrace ambient features and anticipated changes, e.g. weather forecast affecting thermostat settings.

With more devices becoming '*smart*' and able to register their status with upper-level systems, we should expect increases in device self-monitoring for fault tolerance and timely repair, e.g. as we have currently for vehicle engine status monitoring. Significant cost benefits may arise through better insight on system demand and better understanding of system performance. Allied to this may be quality of service enhancements through optimized device and system design as a result of greater performance feedback.

The costly realm of healthcare may expect to benefit substantially from remote diagnosis and treatment, as well as through operational enhancements. In the short-term, we may look forward to a more accessible, efficient and cheaper health service.

11.3 Issues and Challenges

Among the likely issues that are emerging or will emerge in consequence of wide-scale adoption of Internet of Things are the following:

1. Usability
2. Reliability and robustness
3. Availability
4. Locus of control
5. Privacy
6. Integrity
7. Security

11.3.1 Usability

Inevitably, with developments in ubiquitous technology there will be many difficulties that arise through inherent system complexity, or through system misuse. Some of the issues associated with Internet of Things are already evident in the nature and use of today's infrastructure. Other issues are predicted according to the manner and mechanisms that will sustain the growth in IoT.

From a user perspective, usability is always a major concern but key to progress in IoT is the trend toward '*invisible integration*'. As domestic and commercial items gain connectivity and native '*intelligence*', these facilities may become inherent and unseen, with little or no requirement for user activation or direction. In other words, the essential aspects of IoT may be invisible in their usual operation. If this is accomplished, and this may be more aspirational than realistic, then IoT technology will add little to any usability issues with connected devices.

11.3.2 Reliability and Robustness

Serious concerns associated with the reliability and robustness of devices and systems that constitute the Internet of Things are bound to arise. With greater dependence upon such integration comes greater risk. If complex integrated systems become mission or life critical, we will require assurance of reliability. This may require insight on minimum failure rates for critical devices and their higher-level systems.

With increased complexity we have multiple points of failure. The robustness and reliability factors affect individual devices, communication links, centralised and de-centralised services. Reliability is determined not only by failure rates or how robust are the constituent parts, but also in terms of capacity and associated levels of performance. Quality of service may be critical just as absence of device failure may be critical too. As with present day Internet connectivity, when demand increases, infrastructure capacity has a direct effect upon service performance. If there is a need to assign priorities and manage contention, then some services, and probably, some users, will lose out.

11.3.3 Availability

The issue of availability is closely allied to the concern for reliability and robustness. If system capacity is limited or not entirely reliable, how do we spread the benefits? Unless there is equal service provision (or at least, availability) for all, we risk a new era of ‘haves’ and ‘have nots’, in which the privileged (or the wealthy) have greater access, availability or performance than others. The prospect of emerging social benefits from IoT may herald a new realm of inequality of service availability determined by cost of provision or geographical location.

Perhaps we should expect differing service options at different costs. One case in point may be the rise of a two-tier national health service with two access modes: personal contact and online. Presumably, the latter will initially be the cheaper option but this might evolve into a more specialized service, e.g. advice and input from world leading medics, at a premium cost.

11.3.4 Locus of Control

Since IoT introduces major scope for data gathering and assimilation, the issue of control will concern many individuals and organizations. Current data gathering points, such as popular search engines, already raise questions of ownership, control and use of information. Similar questions arise regarding state access and use of information. If individuals yield control of information about their online

and offline behaviour, they lose influence on how such information may be used. Optimistically, the information will be used positively to optimize services and minimize costs. Pessimistically, there may be adverse effects upon particular individuals or organizations, such as members of groups that are perceived as radical in their social, political or religious views.

In response, one might suppose that IoT leaves little scope for individual or local control of information. Indeed, one may argue that any 'added value' arising from the synthesis of data depends upon the aggregation of many data sources. Nevertheless, by its nature, the envisaged data aggregation requires authorised access to data that is ultimately derived from individuals or the systems and devices belonging to those individuals—and this naturally leads us to the issue of privacy.

11.3.5 Privacy

In this envisaged context of centralised data collection, we presuppose the application of data analytics across '*big data*'. As well as the aforementioned issue of control, we may ask '*Who owns the information*?' and '*Who determines how it may be used*?' Given that some people may wish to withhold information, can this be accommodated within the wider system? If not, can we secure guarantees that information in which we figure cannot be used in adverse effect against us? Along side the prospective benefits of timely intervention, e.g. based upon an individual's biological data, comes threats to privacy and civil liberty, e.g. through '*timely intervention*' and removal of health insurance benefits based upon an individual's biological data. Likewise, freedom of movement may be devalued if individuals are tracked via their use of mobile systems and have '*nowhere to hide*'.

On a less sinister note, collective data, e.g. associated with product performance and use, may hold great value to device manufacturer but afford little or no direct benefit to individual users. In the absence of incentive to contribute such data, will individuals have scope to opt out? More likely, participation will become a condition of system provision. If you want the service, you contribute the data.

Availability of data may raise questions over who will have access to such information. Increased resources of amalgamated data may generate new scope for data brokers and will certainly herald new avenues for personalized adverts.

11.3.6 Integrity

As we become increasingly dependent upon systems that relay information to higher-level systems, for data integration and analysis, questions may arise in our minds about the conclusions drawn from data that we have contributed. Assuming that the results are actually available for our inspection, can we trust the results

of data analysis? Is there any scope for independent verification? At the domestic level, as well as relaying data to the supplier, smart metres may provide consumer feedback on energy usage. Access to the raw data and the basis for supplier cost calculations should allow us to determine the correctness of any resultant charges. But will all automated data transfer systems afford such transparency to the consumer? Alternatively, will intermediaries, such as industry watchdogs, have a role in policing the integrity and quality of such services?

11.3.7 Security

The security of systems and devices is our final area of concern with the Internet of Things. The preponderance of devices will only be as strong as its weakest point and we may expect many weak points in the explosion of interconnectivity arising from IoT. In anticipation of this issue, some have even dubbed the development '*the Internet of Insecure Things*', with the depressing thought that '*Anything that can be hacked will be hacked*'.

Evidence from existing networked systems and devices reinforces this unfortunate prospect. For instance, malware (allegedly originating in China) has been found on US SCADA (control) systems. Many nation states have growing anxiety over risks to national infrastructure, as evidenced by examples of attacks on the US power grid. A demonstration under Project Aurora, illustrated such vulnerability to attack, with a $1 million diesel-electric generator destroyed as culmination to the experiment. The frequency of data breaches is further indication that interconnections between systems may give rise to weaknesses as well as strengths.

One might suppose that developments in the form and function of newer devices would include protection against such risks. Yet the vulnerabilities persist primarily because the forms of attack are still effective. As previously noted, increasingly complex systems have more potential points of failure. Any party seeking mischief against an IoT installation may target individual devices or target the network and communication infrastructure. Most attacks use standard protocols to overwhelm the target. Since the connectivity and communication protocols are fundamental aspects of the system, they cannot be disabled as a defence. In consequence, any connected device will be vulnerable, by its nature. The inherent risks are unauthorized access (to data or control). With network access to a device, an intruder may retrieve stored data from the device or modify the device behaviour by means of remote commands or re-programming the device's standard behaviour.

Several prime examples of remote tampering have come to light recently. A case in point is the Internet-enabled fridges that use email to communicate their status [7]. In one instance, hackers have successfully gained access to the software system in such fridges and changed the programming to send spam emails. Similar remote access problems often affect Internet-enabled devices, including wireless-linked cameras.

Recent press stories report Web sites offering lists of remote cameras that can be viewed from anywhere on the Internet (without the permission, approval or knowledge of the camera owners). In one example, a Web site was found to be offering links to unsecured security cameras in 256 countries [8].

Remote access is often achieved by guessing a factory-set password that allows user control of the facility. Commonly, such devices are installed without change to their pre-set access passwords. Leaving them vulnerable to any remote user who can locate the device on the Internet and determine the required authentication details. The risk that unauthorised individuals may misdirect devices or acquire personal data from associated systems is significant and a realistic concern. In addition, experience shows that simpler remote interference with networked devices can impair or deny the service to legitimate authorised users or disable the normal operation of the device and its associated service.

Such interference is aptly termed '*denial of service*' and attacks of this nature often occur against Web services. In each instance, the attack is designed to fully engage the system and, usually, disable it through overloading its network inputs. Often, the technique will direct network traffic to the target service from many other devices that have been compromised, taken over and controlled remotely, without the knowledge of their owners. Such distributed denial of service attacks may simply overwhelm the limited capacity of the target to handle incoming communication or service requests. The assailed system may simply '*crash*' and cease to operate or fail to perform its normal operation while it is buffeted by the network onslaught. Such attacks may result in service disruption, data loss and associated damage to the public image of the affected organization.

The motivation behind such attacks may be mischief, political alignment or extortion against the owner of the target system. In the IoT context, the risk from denial of service attacks may range from inconvenience through financial loss and public image impairment to physical injury or death. Especially in a setting where we have implanted networked medical devices, the associated health risks from illicit access may be severe. This risk is recognised in the decision by former US Vice-President Dick Cheney, when undergoing heart surgery to have the wireless connectivity disabled on the implanted defibrillator [9].

11.4 The Future Internet of Things

The Internet of Things is not a utopian ambition. Technology exists that will enable many of the applications described in this chapter, and many more to be specified as the vision expands. In addition, the lauded potential social and economic benefits are plausible but not guaranteed.

As with many developments in technology, we may expect benefits and drawbacks. On the positive side, there are clear indications that the extensive integrated communication infrastructure that is fundamental to IoT will afford enhanced services through wider automation, information access and exchange. Those users

who are able to quickly adapt and adopt the new technologies are most likely to benefit from these developments.

On the negative side, for a variety of social, financial or educational reasons, many prospective beneficiaries may be slow or ultimately unable to embrace the new opportunities that arise from IoT. Alongside the social and economic benefits, we may anticipate a new digital divide that arises from limited availability and incompatibility of old and new technologies. This gap may be amplified if some in society are unable to afford or to comprehend the technology and its potential, while others remain relatively unmoved and disinterested. Some may be content to adopt personal applications, such as health and fitness monitors or limited domestic management systems. The majority may rush to join the advance. The significant prospective impact of the Internet of Things lies in its broader application for social change and economic transformation. Achieving this potential depends not solely upon developments in technology but upon equitable access and affordable opportunity.

References

1. Sunday Times (2015) 11 Jan 2015
2. www.gov.uk/government/uploads/system/uploads/attachment_data/file/409774/14-1230-internet-of-things-review.pdf. Accessed 31 May 2015
3. us.sourcesecurity.com/news/articles/co-5188-ga-sb.13927.html. Accessed 31 May 2015
4. www.zdnet.com/article/singapore-unveils-plan-in-push-to-become-smart-nation/. Accessed 31 May 2015
5. deity.gov.in/content/draft-internet-thingsiot-policy. Accessed 31 May 2015
6. c-its-korridor.de/?menuId=1&sp=en. Accessed 28 Dec 2015
7. www.theguardian.com/technology/2014/jan/21/fridge-spam-security-phishing-campaign. Accessed 28 Dec 2015
8. www.networkworld.com/article/2844283/microsoft-subnet/peeping-into-73–000-unsecured-security-cameras-thanks-to-default-passwords.html. Accessed 28 Dec 2015
9. www.bbc.co.uk/news/technology-24608435. Accessed 28 Dec 2015
10. www.abiresearch.com/market-research/product/1019236-smart-cars-and-the-iot/. Accessed 28 Dec 2015