Improving Data Access for Smart World

Tariq Lasloum(✉) and Ahmad S. Almogren

Computer Science Department, College of Computer and Information Sciences,
King Saud University, Riyadh, Saudi Arabia
lisloom@hotmail.com, ahalmogren@ksu.edu.sa

Abstract. Devices are becoming increasingly interconnected and increasingly linked to humans beings. The Internet of Things (IoT) concept was developed from the following technologies: the internet, wireless networks, and micro-electromechanical systems (MEMS). It is currently employed for home and industrial applications. Because of differing requirements, different protocols are used. It works on IP, TCP, and HTTP on TCP protocols through the MQTT, XMPP, DDS, and AMQP protocols. IoT evolved from the convergence of MEMS wireless technologies (like RFID and NFC) and the internet. The IoT concept is used in M2M applications like power, gas, and oil utilities' transmission and transport. In this paper, we use OPNET simulation to look at two scenarios and gather traffic data - received and average - for DB query, FTP and Email. We propose an optional addressing method for smart-things to make up the smart world enabling the transmission and analysis of data automatically.

Keywords: The Internet of Things · Sensors · RFID · OPNET

1 Introduction

As technology moves forward, probably the most important advances are in its applications to business and everyday life; information and communication are fields in which innovation has proceeded in a very short time - totally changing how people communicate, interact and do business. Within most organizations, and in everyday living, information travels through familiar routes and pathways. Proprietary data and information is stored in databases and can be analyzed and then shared with other parties, also data and information may be sourced from outside. Medical data, for example, is stored in medical records and can be shared through a secure network with authorised personnel - e.g. doctors.

In some instances, the physical world has become a form of information system: with physical objects taking part via their sensors and their ability to communicate; thus, creating a new kind of information network. These new information networks have the potential to improve communications, create new business models, and improve business processes. They also have the potential to increase convenience and reduce communications costs.

In the IoT, actuators, sensors, and data transmitters are components of physical objects. These physical objects range from pacemakers, to fridges, to roadways, and are connected through a series of wireless and wired networks. These networks often use the Internet protocol (IP) which connects the World Wide Web (www). The physical objects have the

© ICST Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2016
Y. Zhang et al. (Eds.): CloudComp 2015, LNICST 167, pp. 200–210, 2016.
DOI: 10.1007/978-3-319-38904-2_21

ability to sense the environment around them and to communicate - generating huge volumes of data to be analysed by computers. The IoT holds great promise for the future and will no doubt have many applications. This paper evaluates the concept of IoT: looking at its evolution, history, protocols, its simulation, and via this its capacity for throughput. After that, conclusions are presented. Relevant peer-reviewed and/or otherwise credible sources of literature are used as sources of information.

The Internet of Things is made up of Internet-linked devices: at any time, and in any place - as shown in Fig. 1. Examples of 'things' are: your mobile, or a device which remotely starts your car or turns on or off your air-conditioner.

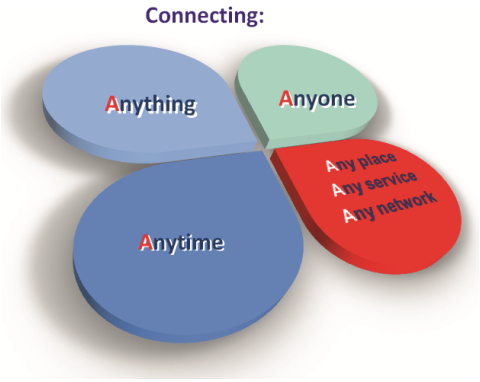


Fig. 1. Connected anything, anytime and anyplace.

The IoT is a phenomenon in which uniquely identifiable objects, including human 'objects' are represented in a virtual internet-like structure. The participants in this network are able to communicate and transfer data and information over a network automatically without human or computer mediation. A 'Thing' in the IoT framework refers to any physical object, even a human being, which has been allocated a unique identifier: a human being, for instance, might have a tiny monitor in their blood intestinal tract which scans and transmits data. In general, a 'thing' is any device or entity with a unique identifier to which an IP address can be assigned and which can transmit information over a network. Entities or devices with component parts which are chips that can automatically transmit information and have IP addresses are termed 'smart devices' [1].

At present, very many places have wireless networks and are thus available to the internet - therefore it is possible to include these in the Internet of Things. Clearly, the internet is not only a network for people to communicate with each other using computer but also to connect with those around you from the devices over wireless networks. An IoT is a network that connects all devices with the existing IT infrastructure, that uses sensor technologies, that includes Radio-Frequency Identification (RFID), wireless sensor networks, and also mobile telephony. The IoT concept can help in more than one area. One of these is domestic energy management. As shown in Fig. 2.

In this paper, we first introduce the IoT. In Sect. 2, we describe some related work; Sect. 3 shows a typical IoT architecture. Simulations of the different application environments which can use the IoT are presented in Sect. 4. Finally, our conclusions are discussed in Sect. 5.

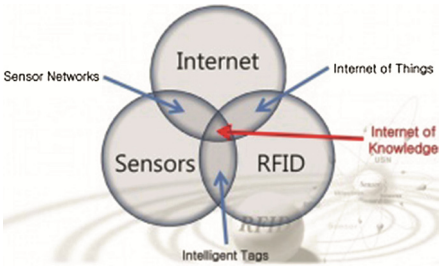


Fig. 2. The internet, sensors and RFID.

2 Related Work

The IoT is sometimes referred to the IoO (The Internet of Objects), and it already affects human life and how animals, humans, and machines interact. The IoT has huge potential for data and information gathering, also for analysis and distribution and thus for turning data into knowledge. IoT projects are being undertaken which will narrow the gap between the rich and poor, and which have the potential to better distribute resources amongst people. With an loT involving sensors planted in many places and connected to computers/software, it will be possible to improve our understanding of the universe and how humans interact with it.

At the present the IoT can be looked on as a 'network of networks'. For example, the cars that we drive today have many sensors which control functions from fuel injection, to engine speed, to braking and in-car temperature. Homes have control systems that handle heating, air conditioning, and indoor humidity. These separate networks will in future be connected, with resultant increased management functionalities - due to the IoT [2].

The IoT has many current applications, and many more potential applications that have the capacity to revolutionize the world. Mobile phones presently account for the highest connected segment, but industries like healthcare, security, financial services, and the car industry hold great potential for further inter connectivity. It is projected that the number of connected devices will be approximately 24 billion by 2020: creating a global new business impact of $ 4.5 trillion [3].

The majority of device source code is based on specific operating systems (for example TinyOS2 and Contiki3) which were developed for resource-controlled platforms. Furthermore, in the wireless sensor networks (WSNs) area, the application source code is conventionally developed directly over the Operating System OS. Mainly the source code is developed in the same language as the OS, statically associated to it, and not, in any effective way, isolated from it. This leads to an efficient application, although

also it may increase the level of errors and make the code more complex, - requiring the developers to understand both the specifics of the OS and the platform [4].

The top ten applications of IoT include connected cars, remote clinical monitoring, assisted living, building and home security, and pay as you drive car insurance. Other areas are smart meters, traffic management applications, charging electric vehicles, and building automation. Home energy monitoring and car sensors are areas with extensive IoT applications. Energy is today a sensitive topic with concerted efforts being made to reduce consumption, use renewable sources, and also use clean energy. Energy monitoring IoT applications exist which use an open network platform working over a wireless system with sensors [5].

The term 'internet of things' was coined in 1999; the development of the IoT has progressed through a number of stages due to the convergence of MEMS (micro-electro-mechanical systems), wireless technologies, and the internet. RFID (radio frequency identification) is also something which falls within the scope of the modern day IoT. The concept was developed from the principle of uniquely identifying objects and people – thus making the network manageable by computers [6].

The development of IoT was, in particular, due to the requirements of critical operations such as oil and gas drilling, and also manufacturing. For instance, drilling a geothermal well requires the use of a constant stream of information which cannot effectively be managed by a human agency. The need for an automatic and reliable method for collecting and transmitting information thus became important [7].

Other applications, for instance tracking and loading passenger luggage, required an automated process as human intervention was tedious and cumbersome. The situation also required occasional human intervention (for managing and identifying items quickly and automatically). These needs have led to the development of RFID and other technologies - including NFC (near field communication), QR codes, barcode, and digital watermarks. In general though, the IoT has been associated more closely with M2M (machine to machine) communications - mainly in power, gas, and oil utilities, and with manufacturing. The IoT can be traced to the early automated devices with internet capability such as the coke machine. Programmers had the ability to check if a cold drink would be available to them if they went to the vending machine. A similar system was developed in relation to a coffee machine that would let people know whether there was coffee available in the machine - remotely. Such initiatives increased interest in enabling devices and humans to communicate more seamlessly in various other application areas including health and industry. The internet is playing a key role in the evolution and development of the IoT as it allows data and information transmission over wired or wireless devices [7].

The recent development of more unique addressing capability courtesy of the internet protocol version 6 (IPv6) will greatly enhance the development of the IoT. The address space expansion courtesy of IPv6 implies an almost unlimited number of IP addresses that can be assigned - so IP addresses can be assigned to many more things. For example, a credit card with a smart chip can have an IP address assigned to it. With, in addition, fingerprint sensing, this means that the card could alert the user and the credit card company of any unauthorized use - even before a transaction took place. Such a transaction could then be stopped before it happened, and the card deactivated.

Presently over 5 billion devices have been interconnected. These devices range from home appliances to devices used in manufacturing. Homes now have automated lighting, sprinkler systems, and security systems – all possibly linked to the internet. Industry's needs have led to the requirement for horizontal and vertical balance in making interconnections.

Future developments will require a challenge like multi connectivity, power management, security, rapid evolution and complexity [8].

One of the most important attributes of the IOT is the use of sensors. These are increasing in number and reducing in cost. Sensors can now provide data on almost any physical variable: movement, sound, light, temperature, moisture, location. Some sensors are used only for a few days and then discarded.

Traditional Wi-Fi systems allow the network to be setup by the sensor. Normally, networks are made up of a number of Wi-Fi transceivers that allow actuators and sensors to be linked to the Access Point (AP). Of course, the Access point may be connected to Internet - as shown in Fig. 3.

Fig. 3. Sensors and actuators linked directly to an Access Point (AP).

3 System Architecture

The IoT protocol works on a series of rules including D2D (device to device communication) where devices must communicate with each other. This communication and movement of data uses protocols which include MQTT, XMPP, DDS, and AMQP.

Data from devices must be collected and sent to a server infrastructure (D2S- device to server) which then shares the data from the devices with other servers (S2S – server to server). The data and information can then be sent back to the devices, shared with people, or analysed using programs [6].

We have, so far, identified the high level components needed for the Internet of Things. Each of these components may also be found outside of the IoT. The following are IoT components:

(a) **Hardware** - actuators, embedded communication hardware, and sensors.
(b) **Middleware** - storage and computing utilities for information analytics that are on demand.

(c) **Presentation** - visualization that is clear to understand and implemented in such a way that it can be accessed across different platforms. In addition, these tools may be considered for diverse applications as shown in Fig. 4.

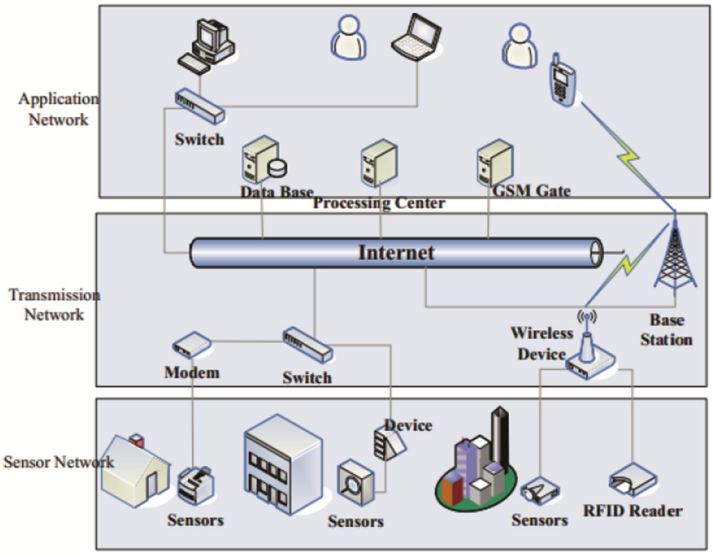


Fig. 4. Typical architecture of IoT.

Radio Frequency Identification (RFID). Important components in embedded communications are represented by RFID technology. This allows the development of microprocessor systems which record data about wireless communications. Passive RFID tags do not need batteries to operate. In addition, the RFID reader can receive an ID by operating on the power of the signal. There are a number of places where such systems can be found: e.g. transportation (instead of tickets, registration labels) and admin/control applications. Furthermore the tags can be used in bank credit cards and on toll roads.

Wireless Sensor Networks (WSN). Autonomous sensors distributed by a wireless sensor network (WSN) of spatially to control the physical and environmental terms, and to cooperatively maintain data flow on a network to a core location.

Wireless communications have made available well-organized, low cost, low power, and very small devices which can be used in remote recognition applications. The components that create the WSN monitoring network contain:

(a) **WSN hardware**
A node (WSN core hardware) which uses processers, sensor interfaces, power source, and transceiver units. They are, in effect, a series of several converters for the sensor interface.

(b) **WSN communication stack**
The communication stack at the node needs to link with the external world via the Internet, and to work as an entry to the Internet and the WSN subnet.
(c) **Middleware**
It is a method used to merge cyber infrastructure with a sensor networks and Service Oriented Architecture (SOA) to make available administration to heterogeneous sensor resources in a deployment self-governing.
(d) **The secure Data aggregation**
One of the requirements for prolonging the lifetime of the network and making sure that reliable data collected from sensors is an effective and secure data aggregation method [6].

Data storage. An important element in this area is the development of an unprecedented.

The IoT revolution will result in huge amounts of data from different sources and devices, all requiring huge bandwidths. The information and data are same to be transmitted through the WAN (wide area networks) which already suffers from a bandwidth gap. Limited bandwidth will result in the strangled development and wider adoption of the IoT. New endpoints will be introduced by the IoT, of which endpoints will also be different from what is being used. However, the strategy was adopted for the provision of low bandwidth, high volume data throughput to help keep costs low. This can be achieved through cellular networks using high speed technologies like 3G that will offer higher data rates. Wireless systems that use very low data throughputs as well as low power were developed. Other means for connectivity include satellite M2M that has unique capabilities as it can work nearly everywhere in the world. Satellite M2M can be rolled out fast and on a universal scale without the need for local connectivity for instance, using SIM cards.

Satellite M2M is very scalable with the ability to recover quickly from natural disasters and outages. It can be applied in dual mode devices that have terrestrial and satellite networks. Because of the multi device nature, IoT will require low cost and low power ubiquitous systems to work efficiently. Because of the different protocols and requirements at different stages, the IoT system uses integrated communication links incorporating radio, cable, and fibre optic. Future developments will require fibre connection between servers, satellite M2M and cable or radio between devices and servers.

4 Simulation

The IoT will result in connecting billions of ‘things’, and this requires prior simulation before it can be implemented in real world situations. Simulation will be necessary in order to understand the IoTs various components and operating principles, especially with regard to scale. Simulating the IoT will require the integration of an accurate OS (Operating System) simulation into a generic simulation environment as a first step.

OMNeT++ and Contiki can provide a suitably integrated OS. Contiki has wide support for sensors and hardware actuators embedded into devices, making it suitable

for IoT. OMNeT++ is a simulation library that has been used widely and has a large set of available extension frameworks and simulation models.

For this paper, we use the OPNET program for the simulation of two scenarios in order to deduce traffic - received and average - for DB query, FTP and Email. In scenario 1 we used 30 nodes and in scenario2 we used 40 nodes. This is shown in Fig. 5.

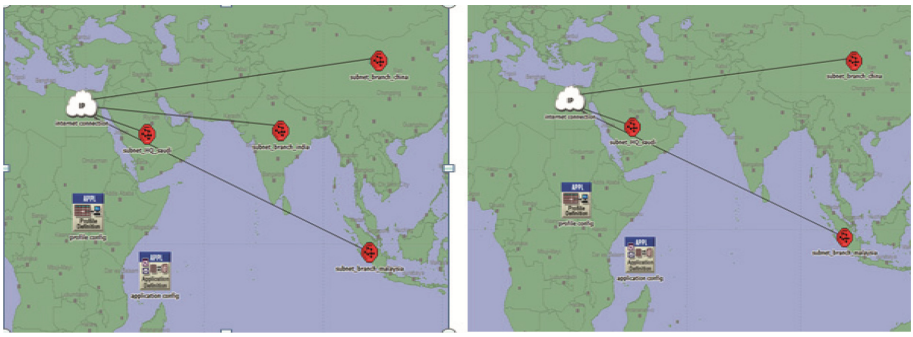
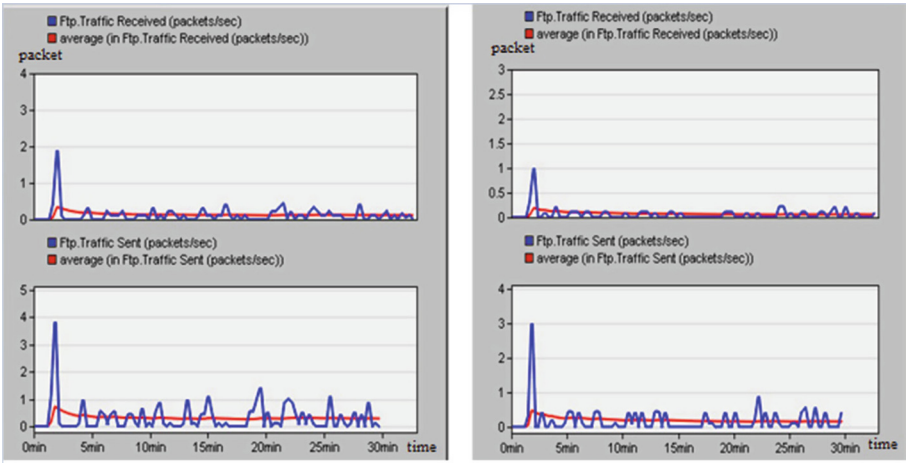


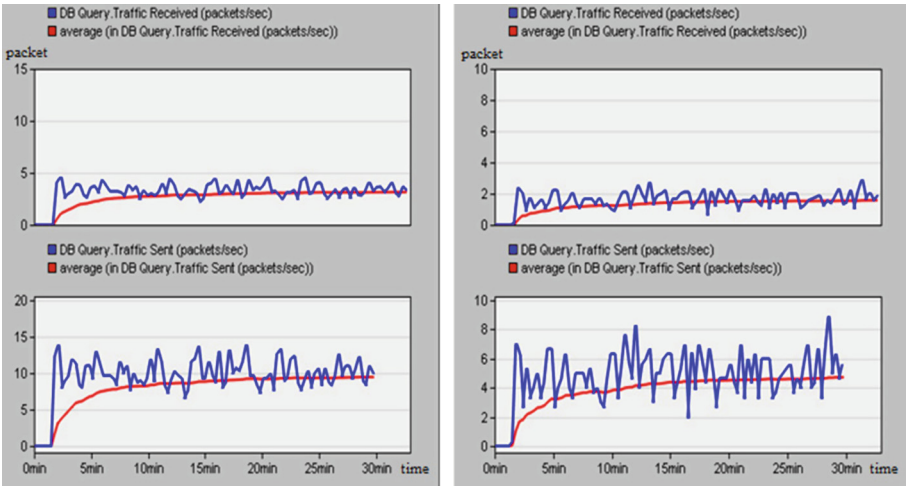
Fig. 5. Two scenarios.

In Fig. 6, we show FTP in terms of packets rate from 30 nodes in the chart (a) and from 40 nodes in the chart (b). In Fig. 7, we show DB query in terms of packets rate from 30 nodes in the chart (a) and from 40 nodes in the chart (b). In Fig. 8, we show the Email in terms of packets rate from 30 nodes in the chart (a) and from 40 nodes in the chart (b).



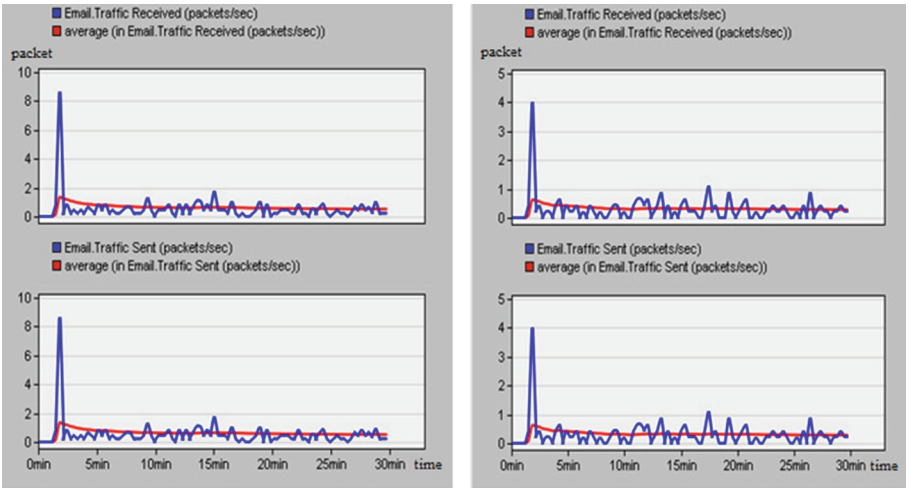
(a) (b)

Fig. 6. (a) Simulation for FTP application, traffic received, sent and average in scenario1, (b) simulation for FTP application, traffic received, sent and average in scenario2 (Color figure online).



(a) (b)

Fig. 7. (a) Simulation for DB query application, traffic received, sent and average in scenario1, (b) simulation for FTP application, traffic received, sent and average in scenario2 (Color figure online).



(a) (b)

Fig. 8. (a) Simulation for eMail application, traffic received, sent and average in scenario1, (b) simulation for FTP application, traffic received, sent and average in scenario2 (Color figure online).

The second step in the simulation is the accurate presentation of the various protocols from the different-used network stack layers. Low layer protocols such as ZigBee can be used for protocol representation since it can be modelled accurately in OMNeT++.

By using the actual protocol implementation, we will give better and more accurate results for instance using the NSC (network simulation cradle). Moreover, using real protocols during IoT simulation enable designers and stakeholders unearth concepts not yet understood about IoT.

5 Conclusion

The IoT is a promising phenomenon. Many things are interconnected through networks, and communicate by using various network protocols. IoT is a concept which uniquely addresses 'things', inanimate or human, which are able to gather and transmit information and data automatically. IoT evolved from the convergence of MEMS wireless technologies like RFID and NFC, and the internet. IoT has been used in M2M applications like power, gas, and oil utilities transmission and transport. IoT uses the IP, TCP and HTTP over TCP protocols as its communications backbone. Because of differing requirements, different protocols are used. For this paper, we used OPNET to look at two scenarios and gather traffic data - received and average - for DB query, FTP and Email.

IoT has a bright future and will revolutionize how people do business, communicate, and interact with 'things' - it is a network of networks.

References

1. Castro, D., Misra, J.: The Internet of Things, November 2013
2. Evans, D.: The Internet of Things, How the Next Evolution of the Internet is Changing Everything, April 2011
3. Royer, M.: The Internet of Things (IoT). Ph.D., August 2013
4. Kovatsch, M., Lanter, M., Duquennoy, S.: Actinium: a RESTful runtime container for scriptable Internet of Things applications. In: Proceedings of the 3rd International Conference on the Internet of Things (IoT 2012), Wuxi, China, October 2012
5. Bouhafs, F., Rajabi, D.: Open sensing platform for HomeEnergy monitoring in the Internet of Things. Int. J. Eng. Sci. **2**(1), 53–61 (2013)
6. Gubbi, J., Marusic, S., Buyya, R., Palaniswami, M.: Internet of Things (IoT): a vision, architectural elements, and future directions. Future Gener. Comput. Syst. **29**(7), 1645–1660 (2013)
7. Chase, J.: The Evolution of the Internet of Things, September 2013
8. Links, C.: Sentrollers and The Internet of Things. GreenPeak Technologies, Utrecht, May 2013
9. Guinard, D., Ion, I., Mayer, S.: In search of an Internet of Things service architecture: REST or WS-*? A developers' perspective. In: Proceedings of Mobiquitous 2011 (8th International ICST Conference on Mobile and Ubiquitous Systems), pp. 326–337, Copenhagen, Denmark, December 2011
10. Brown, M., Coughlan, T., Lawson, G., Goulden, M., Houghton, R.J., Mortier, R.: Exploring interpretations of data from the Internet of Things in the home. Interact. Comput. **25**(3), 204–217 (2013)
11. Carretero, J.: The Internet of Things: connecting the world. Pers. Ubiquit. Comput. **18**(2), 445–447. Springer, London (2013)

12. Khriyenko, O., Terziyan, V., Kaikova, O.: End-user facilitated interoperability in Internet of Things. Int. J. Adv. Internet Technol. **6**(1&2), 90–100 (2013)
13. Mattern, F., Floerkemeier, C.: From the internet of computers to the Internet of Things. In: Sachs, K., Petrov, I., Guerrero, P. (eds.) Buchmann Festschrift. LNCS, vol. 6462, pp. 242–259. Springer, Heidelberg (2010)
14. Bin, S., Yuan, L., Xiaoyi, W.: Research on Data Mining Models for the Internet of things (2010)
15. Uckelmann, D., Harrison, M., Michahelles, F.: An architectural approach towards the future Internet of Things. In: Uckelmann, D., Harrison, M., Michahelles, F. (eds.) Architecting the Internet of Things, pp. 1–24. Springer, Berlin Heidelberg (2010)
16. Fleisch, E.: (ETH Zurich/University of St. Gallen) what is the internet of things, January 2010