Delft University of Technology

FACULTY MECHANICAL, MARITIME AND MATERIALS ENGINEERING
Department Marine and Transport Technology

Mekelweg 2
2628 CD Delft
the Netherlands
Phone +31 (0)15-2782889
Fax +31 (0)15-2781397
www.mtt.tudelft.nl

Specialization:	Transport Engineering and Logistics
Report number:	2016.TEL.7996
Title:	**IoT and Big Data in Transport Systems**
Author:	M.D. Spekreijse

Title (in Dutch)	Het IoT en Big Data in transportsystemen

Assignment:	literature
Confidential:	no
Initiator (university):	prof.dr.ir. G. Lodewijks
Initiator (company):	
Supervisor:	prof.dr.ir. G. Lodewijks
Date:	23-02-2016

IoT and Big Data in Transport Systems

A literature survey

By

M. D. Spekreijse
4041712

In partial fulfilment of the requirements for the degree of

Master of Science

At the Delft University of Technology

Student number: 4041712
Supervisor: Prof. dr. ir. G. Lodewijks

LIST OF ABBREVIATIONS

Term	Abbreviation
Basic Service Set	BSS
Bluetooth Low-Energy	BLE
Direct Attached Storage	DAS
Food Supply Chain	FSC
Full Function Device	FFD
Industry 4.0	I4.0
Information Technology	IT
Infrastructure as a Service	IaaS
Internet of Things	IoT
Internet Protocol	IP
Internet-0	I0
Line of sight	LOS
Local area network	LAN
Near Field Communication	NFC
Network Storage	NS
Personal Area Network	PAN
Platform as a Service	PaaS
Radio Frequency Identification	RFID
Reduced Function Device	RFD
Role Based Access Control	RBAC
Service Oriented Architecture	SOA
Smart Objects	SO
Software as a Service	SaaS
Ultra-Narrow Band	UNB
Wireless Fidelity	Wi-Fi
Wireless Identification and Sensing Platform	WISP
Wireless Local Area Network	WLAN
Wireless Sensor Networks	WSN

ABSTRACT

The Internet of Things (IoT) is a novel paradigm which envisions autonomous intelligent networks of everyday objects. The IoT field is relatively young, but its developments have raised a lot of interest from various industries. The IoT community believes that a broad range of activities will have substantial waste and cost reduction when these smart objects start acquiring and sharing information in their environment.

This literature survey will try to explain the current and predicted role of the IoT within intelligent transport systems. The IoT subject is becoming more popular in scientific literature and there are already some existing surveying studies, but this paper is unique in its specific scope and hopes to contribute to the community with new insights. The survey starts with an introduction of the IoT and its definition in the scientific community. Thereafter the different technologies enabling the IoT are listed and discussed, these form the technical composition of the IoT value chain. Like the IoT, Big Data has seen the same rise in popularity over the past years and it will be introduced similarly. After these subjects have been properly discussed, an analysis of a selection of IoT applications in transport systems will be surveyed and compared.

It will be concluded that while there are some roles for the IoT in these systems, their presence is still meagre. Most applications stand in contrast with the IoT ideology and were implemented from a bottom-up approach. Still these innovations show that results are found in reducing waste and costs, improved process analysis and increased security. The current trends in technological innovation, together with the predictions made in the scientific community, make the IoT a very interesting field for future research.

TABLE OF CONTENTS

1 INTRODUCTION

The developments of the Information Technology (IT) in the past decade has enabled continuous growth in connecting different entities to the internet and according to (Evans, 2011) the term 'the Internet of Things' (IoT) was born when more devices than people were connected to the web. Data acquisition equipment used to be complete heteronomous and therefore it was clear that a lot of information could not be acquired yet due to a limited capacity in resources. This uncovered data could prove useful if new relations were found, which would give a better understanding to processes within our surroundings. The IoT paradigm aims to capture and share data from everyday objects via autonomous means and use this data to enhance the quality of life (Ashton, 2009). It is predicted that the amount of devices being connected to the internet will keep on rising steadily and thus human interaction will account for the minority of internet traffic in the near future. This paradigm is supported by a community which believes that with increased information gathering, waste and costs can be greatly reduced in a broad range of activities.

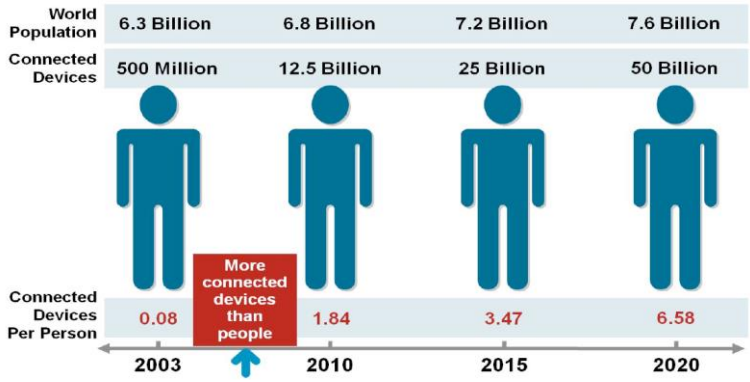

Figure 1-1The IoT was 'born' around 2009 (Evans, 2011)

This IoT paradigm is currently being implemented in various environments like households, traffic situations, manufacturing- and transport environments. In 2013 the Economist made a report (Witchalls, 2013) in which they surveyed over 750 business leaders about their perspectives on IoT in future businesses. It was concluded that most businesses have the IoT on their agenda and expect to be using it within 3 years' time. However, not all industries are completely convinced on how the IoT can be successfully implemented in their industry and there is probably need for the IoT to mature a bit more.

This is a literature survey on the IoT, Big Data and applications of these technologies within transport systems. The goal of this literature survey is not to contribute to research in this area, but to represent the different views, technologies and discussions of these subjects. Most of the technical aspects will be approached from a 'intelligent control for transport systems' perspective i.e. how the systems work, of which components it consists and how these interact. This research is set up to answer the following research question:

'What is the (predicted) role of the Internet of Things within intelligent transport systems, according to literature and relevant practices in industry?'.

In order to answer this question several sub questions have been derived and these are:

1. What is the Internet of Things?
    a. How is the Internet of Things defined in scientific literature?
    b. Which technologies constitute the Internet of Things?
2. What is meant by ‘Big Data’ and what is its relation to the Internet of Things?
    a. Which technologies constitute Big Data?
3. What are the current roles of the IoT in introduced IoT solutions for intelligent transport systems?

The survey is structured according to these questions. In chapter 2 the different perspectives on the IoT will be investigated and compared. When the understanding of the paradigm is established, the different technologies enabling the IoT will be presented in chapter 3. Chapter 4 will list the structure and current research concerning Big Data and in the final chapter a best practices abstraction will be presented, which are derived from case studies concerning IoT applications in transport systems.

2 THE INTERNET OF THINGS

The IoT term is not well defined in scientific literature and is used as a buzz word for marketing purposes, it serves more as a subject where the meaning is open for debate. There are multiple definitions in the scientific community and these differ on their primary focus. To give an example, the following definitions are a selection found in literature and this selection shows that each definition has a different perspective while the fundamental idea stays the same:

- It is explained by Giusto (cited in (Atzori, Iera, & Morabito, 2010), p.1) as "things or objects, which through addressing schemes interact with each other and cooperate with their neighbours to reach common goals".
- According to (Miorandi, Sicari, De Pellegrini, & Chlamtac, 2012) the IoT are "interconnecting physical objects with computing and communication capabilities across a wide range of services and technologies".
- (Gubbi, Buyya, Marusic, & Palaniswami, 2013) perceives the IoT as "Interconnection of sensing and actuating devices providing the ability to share information across platforms through a unified framework…with Cloud computing as the unifying framework."

It is clear that the first explanation comes from a networking perspective, whilst the second uses physical attributes as the base for the IoT definition and the third focusses on the use of platforms and the cloud. This observation means that there is no consensus in literature, however they all aim for connecting devices via a large network with the ability to process information and to autonomously decide whether it should take action.

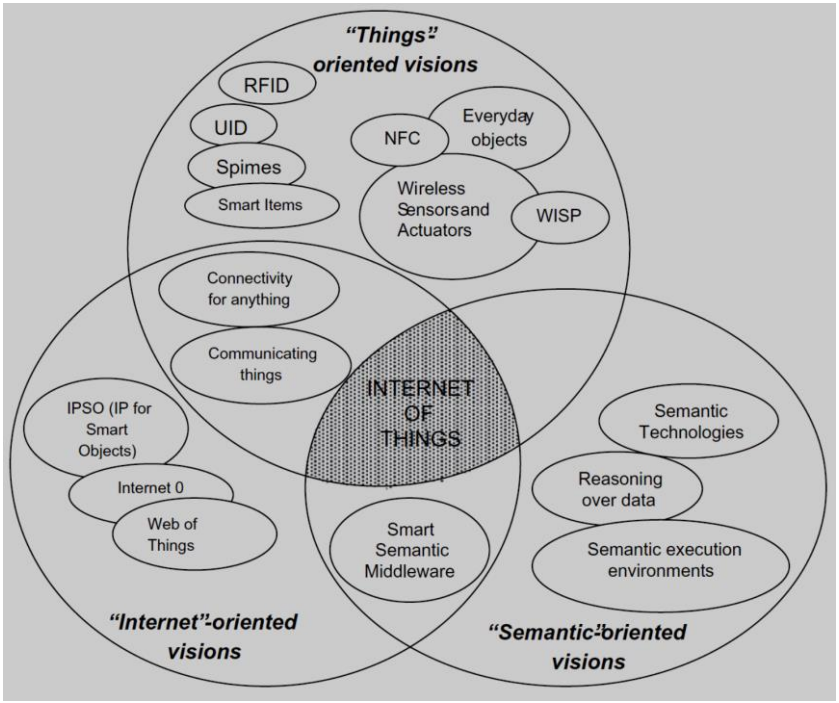

Figure 2-1 The IoT as a result of different visions (Atzori et al., 2010)

The IoT paradigm can thus be approached from several directions, due to its disciplinary nature, these directions or visions are clearly identified by (Atzori et al., 2010) and represent different scientific communities. These different scientific communities started research within their own area and while the IoT literature is maturing slowly these communities are starting to overlap and merge. The usefulness of the IoT can be used only in application domains where these three visions intersect (Gubbi et al., 2013), see Figure 2-1, and these visions are called:

- 'Internet oriented' vision
- 'Things oriented' vision
- 'Semantic oriented' vision

In the following sections each vision shall be discussed in its view towards establishing the IoT.

2.1 THE "INTERNET ORIENTED" VISION

The 'Internet oriented' vision embodies the need for a standardized communication architecture which should allow the IoT to become more widespread. Several studies have focussed on this vision and they all aim for the Internet Protocol (IP) to be promoted as the network technology for connecting objects in the IoT. According to (Gershenfeld, Krikorian, & Cohen, 2004), the costs and complexity of setting up a global network out of heterogeneous local networks are currently too high and have to be dramatically reduced. To get there a set of rules was introduced by the name 'Internet-0' (I0) and devices which are a part of it embody seven principles:

1. Each I0 device uses IP as the connection standard, which removes the need for costly and complex translation interfaces.
2. Communication protocol software is simplified and non-segregated.
3. Each set of I0-deviced is able to work independently, thus there are no client/server relations.
4. An I0-device keeps track of its own identity.
5. I0 uses bits which are bigger than the network[1].
6. Big bits allows data to be represented in the same way, no matter what medium conveys them[2].
7. An I0-device will use open standards in order to make optimal use of available resources

These principles allow everyday objects, given that they are equipped with the needed technology, to seamlessly connect to a data network with communication, computation, sensing and storage functionalities. By allowing nodes to share information in the same 'language' in any network, locally or globally, the needed system can be designed based on the needed functionality rather than constrained

[1] Bits have a physical size, the broadcast time multiplied by the bit speed represents this size. If the bit size is smaller than the network, two computers that transmit simultaneously may not discover data collision (Gershenfeld et al., 2004).

[2] Take Morse code as an example, it is possible to communicate with Morse through multiple media like sound, light, writing etc. This principle allows the IoT data to be transferred through multiple media and thus allowing more objects to participate.

by boundaries. The technologies used in this perspective are accounted to the middleware of the IoT, which will be later on discussed in section 3.3.

2.2 THE 'THINGS ORIENTED' VISION

The 'things oriented' vision sees the IoT as a network of smart objects with extended internet technologies and at the same time the set of technologies which realises this (Atzori et al., 2010; Miorandi et al., 2012). The focus lies on the physical embodiment of the IoT. According to this vision the IoT concept has three conditions, which apply to the active objects in the network:

1. **Anything identifies itself**: smart things are identified with a unique digital name to establish relationships in the domain.
2. **Anything communicates**: smart things form ad hoc networks of interconnected objects.
3. **Anything interacts**: smart things interact through sensing and actuation with their environment.

Developing the solutions and technologies to realise these three pillars is the foundation of the 'things oriented' perspective.

This IoT perspective differs from known networking visions in that everything should be able to interact based on its own decision making; intelligence should even exist at the edge of the network. Each single component is called a Smart Object (SO) and these SO's are physical objects which have at least basic communication and computation functionalities. An SO is also uniquely identified with one name and address within the network and it may possess means to sense physical phenomena. This is the key feature which distinguish SO's from nodes normally used in networking systems.

A system of a large number of SO's is seen as a dynamically distributed network, these SO's produce and consume information and they are able to trigger actions which have an impact on the physical realm (Miorandi et al., 2012). Challenges lie in how these functionalities and resources can be integrated in multiple services spanning the network, which should result in an "always responsive service" for the end-user. Key system-level features, as identified from the 'things oriented' perspective, are:

- Connected devices should be heterogeneous
- Scalable addressing and information management
- Data exchange should be ubiquitous through proximity wireless technologies
- Energy-optimized solutions, minimizing the energy spent for communication and computation
- Devices should be track- and traceable
- Device should be autonomous, the network should distribute intelligence
- Data formats should be standardized
- Adequate security and privacy mechanisms

As is stated above, the IoT from a "things oriented" perspective emerges from how the nodes should work and how they should interact in the network. This perspective will be used later on in this literature study to comprehend the usefulness of IoT application in transport systems.

2.3 THE 'SEMANTIC ORIENTED' VISION

The 'Semantic oriented' vision is related to how to represent, store, interconnect, search and organize information generated by the IoT (Atzori et al., 2010). This visions promotes the use of smart connectivity and context-aware computation; these features should allow the technology to 'disappear' from the consciousness of the user. Raw sensor data has no real value if there is no understanding of its context, the challenge lies in the reasoning of the collected data (Perera, Zaslavsky, Christen, & Georgakopoulos, 2014). IoT envisions that an enormous amount of sensors will be connected to the internet and it is infeasible to process all the data that is being collected, which ultimately leads to the generation 'Big Data'. This demands the IoT to have a shared understanding of the situation of the users, solid software and communication architectures and analytic tools which aim for autonomous and smart behaviour (Gubbi et al., 2013). The general idea is to embed technology into the background of everyday life, this ideology is accompanied by the ideologies of Big Data and Cloud Computing, which will be further discussed in chapter 4.

2.4 DISCUSSION

As was stated in this section's introduction the usefulness of the IoT comes forward when these three visions intersect. What this scientific community lacks is that these different views have not worked out yet how to define one solid meaning for the IoT and therefore current research is segregated. According to the publication analysis of (Yan, Lee, & Lee, 2015) the growth trend of IoT relevant publications has experienced faster growth since 2009, which was stated in the Introduction chapter as the period that the IoT was 'born'. Papers written before this period are limited to one view or a brief introduction of the ideology. Perhaps it is necessary for the IoT scientific community to 'mature' in order to form a generalized understanding.

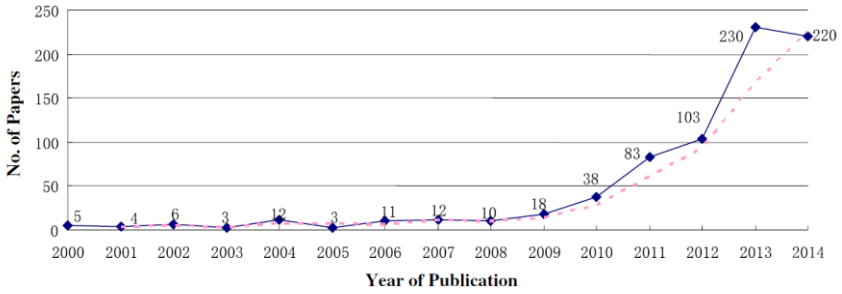

Figure 2-2 Publication analysis on relevant IoT publications (Yan et al., 2015)

Still these visions can be combined and summarized as followed, representing the IoT definition as it is covered in literature: *The Internet of Things consists of a heterogeneous network in which autonomous nodes are able to identify, communicate and interact intelligently. This heterogeneous network is connected via wireless or wired communication, which should be standardized in its naming, addressing and configuration. These technologies should be able to interpret the right context of the end-user and they should be seamlessly integrated into the background of everyday life.*

Not every IoT application will be the same and there are endless possibilities in which it can be envisioned. Still the different explanations of the paradigm show that a broad range of studies intersect here and that there is still research needed for the IoT to become one standardized field. On the other hand, it could be questioned if the IoT is actually a field of study and not, as a conclusion of the different views, merely used as a promotional hype for these applications.

3 ENABLING TECHNOLOGIES

As is discussed in the previous chapter, the IoT holds several disciplines and consists of multiple technologies. In this section the fundamental technologies will be covered and compared when it is relevant to do so. The technologies are structured in such a way that they form a chain between a SO and an end-user, these are:

- Data acquisition
- Identification and tracking
- Communication and networking
- Middleware
- Data storage and analytics
- Applications

The value chain represents the technological structure of the IoT. This chapter is aimed to explain the range of available technologies without going into too much detail, it is only meant to create a survey of what is currently being used and researched by the IoT community. Data acquisition technologies will be left out of the scope since it acts as an extension of the system. This also means for the applications, since it is not the aim of this survey to discuss the various ways data can be represented by applications. The chapter will be concluded by the topic of Privacy, Security and Trust, which is more a topic of policy discussion than a list of available technologies and it forms the foundation of the IoT value chain.

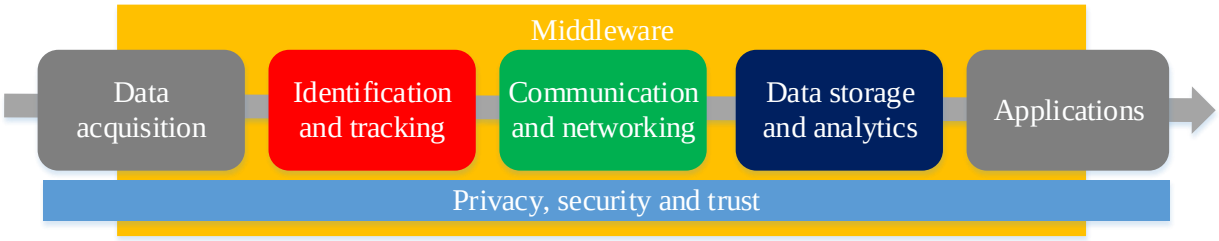

Figure 3-1 Value chain of the IoT

3.1 IDENTIFICATION- AND TRACKING TECHNOLOGIES

To respect the first pillar of the IoT, as described in 2.2, several technologies with means for identifying and tracking are researched, improved and used in the IoT. In this section some key identification- and tracking technologies will be discussed. Key building blocks are represented by Radio Frequency Identification (RFID) and Wireless Sensor Networks (WSN) (Atzori et al., 2010; Miorandi et al., 2012). These building blocks have three limiting factors which are to be improved in order to have a successful IoT implementation:

- Expected heterogeneous support of any device
- The need for equipping a battery to SO's and their limited or short battery life
- Current state-of-the-art electronics dimensions are insufficient for complete IoT realization

The most dominant technology is the **RFID** system (Finkenzeller, 2003), which can be used for real-time object identification and monitoring with no line-of-sight requirements. A RFID tag is a small antenna connected to a microchip which can receive and send its unique ID via radio signals depending on its configuration. There are **passive RFID** tags, which can be placed on an adhesive sticker and do not need an on-board power supply, their power is generated from incoming radio signals and therefore they only interact when they are in contact with a reader. The **active RFID** tags are distinguished from the passive RFID tags due to their power supply, resulting in a limited lifespan, better radio coverage, relative larger memory capacity, higher production costs and larger size. Both tags are used for the (relative) location determination and object identification, whereas active RFID tags can transmit real-time location.

Figure 3-2 Size comparison for a passive and an active RFID tag (source: Atlas RFID Store)

Next to RFID systems there are IoT implementations where **WSN** are used, which can also track object status next to its ID and location (Akyildiz, Su, Sankarasubramaniam, & Cayirci, 2002). These networks consist of a high number of sensing nodes which communicate wirelessly in a multi-hop fashion. Multi-hop wireless networks use two or more nodes to convey information from the source to the destination, two nodes are able to communicate whilst there is no direct connection. The advantages of WSN are the high radio coverage, which is about 100m per node (Atzori et al., 2010), and communication is possible without the presence of a reader: it is peer-to-peer. However, WSN have a limited lifetime due to relying on battery power as a primary source.

The integration of sensing technologies into passive RFID tags result in a well applicable IoT technology: Wireless Identification and Sensing Platform (**WISP**), which is a project of Intel Research Seattle (Smith, Sample, Powledge, Roy, & Mamishev, 2006). The WISP represents a platform which can sense and compute with a programmable flash controller which is powered via a passive (ultra-high frequency) RFID antenna. With the increasing availability of Near Field Communication (NFC) commodities, for instance in smartphones, more opportunities are enabled to create a more widespread IoT network (Sample, 2015). However, the reading range of passive RFID tags is constrained to a few meters.

These three technologies can be compared in Table 3.1, it depends upon the system which technology is the best choice and even combinations of these technologies are possible. Other identification and tracking technologies like GPS and barcodes were not considered in the scope due to their ‘one way’ communication.

Table 3.1 Comparison of Identification and Tracking technologies for IoT implementation

	Sensing	Range	Battery	Lifetime[3]
RFID Passive	None	Medium	None	Indefinite
RFID Active	Possible	Long	Yes	2-3 years
WSN	Yes	Long	Yes	2-3 years
WISP	Yes	Short	None	Indefinite

3.2 COMMUNICATION AND NETWORKING

In this section several working technologies for inter-device connectivity and communication will be listed and discussed. To respect the condition 'anything communicates', only bidirectional communication will be treated, meaning that communication is possible in both directions. This section will be in two parts, the first handles all the technologies which are currently used in Personal Area Networks (PAN) or Local Area Networks (LAN) like in domestic and industrial environments. The latter part covers the Wide Area Network (WAN), resembling networks covering larger areas. Finally, the described technologies shall be briefly discussed and thereafter a comparison will be presented in tabular form.

3.2.1 PAN and LAN technologies

6LoWPAN is an acronym which stands for 'IPv6 over Low power Wireless Personal Area Networks', it envisions that nodes with limiting processing power and low power options also should be connected to the IoT (Mahmood, Javaid, & Razzaq, 2015; Shelby & Bormann, 2011). It is applied in embedded devices which need to communicate with Internet-based services. IPv6 stands for Internet Protocol version 6 and offers 10^{28} unique addresses in order to allow any embedded object or device to connect directly to the internet, meaning that it could be accessed from anywhere if properly configured. An embedded device is a device which has a specific functionality and thus it is needed for one or a few purposes, while being a part of a larger system. Embedded devices have hardware which is designed to be low power consuming, small and cheap. The 6LoWPAN network uses a mesh networking topology to support high scalability and this allows the network to be 'self-healing'[4].

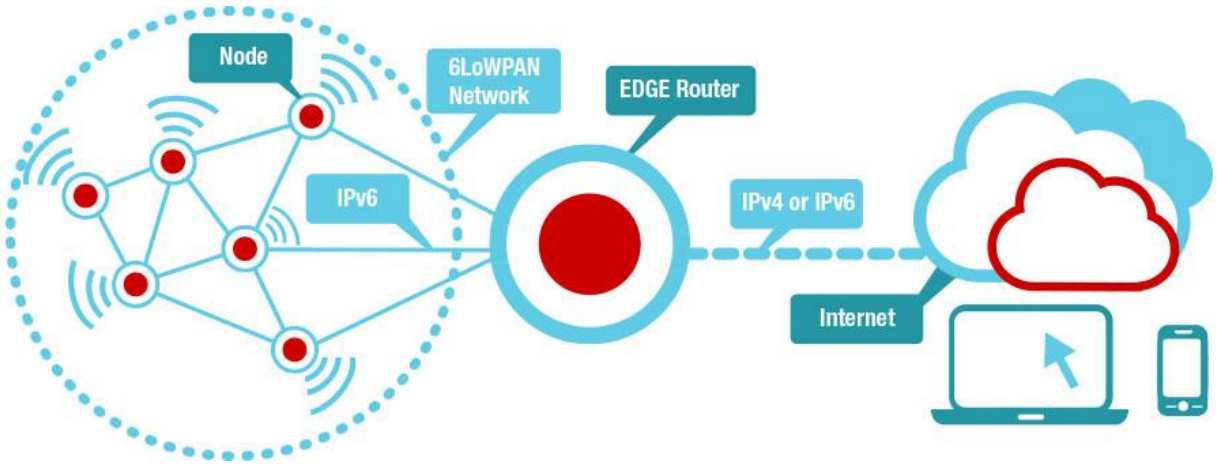

Figure 3-3 Visualization of a 6LoWPAN Network (TexasInstruments, 2015)

[3] Amount of time it would serve without need for intervention

[4] From network topology, a self-healing ring is a network with bidirectional links and therefore it will keep functioning if one is broken (Quattrociocchi, Caldarelli, & Scala, 2014)

Bluetooth communication exchanges data over short distances, approximately 10 to 20 meter, and is characterized by its low power consumption, fast data exchange of 1Mbps and widespread availability (Ferro & Potortì, 2005; Jin-shyan Lee, Su, & Shen, 2007; Mahmood et al., 2015). In a Pico-net, a synonym for a Bluetooth- PAN, a maximum of 8 devices work actively in a Master-Slave relation with 1 device being the Master node. If two or more Pico-nets are interconnected a Scatter-net is formed. As is showed in Figure 3-4, a Bluetooth device can only be a Master in one Pico-net, but it is possible to be a Slave of multiple Pico-nets. If there is no direct connection between two nodes, because two nodes are not within the same range or Pico-net, it still is possible to communicate through multi-hop communication (Ferro & Potortì, 2005). Newer developments have introduced Bluetooth Low-Energy (BLE) as a significant protocol for the IoT (Tamura & Masuda, 2013), built as a power- and application friendly version. BLE has an extended range of 50 to 150 meters, much lower power consumption and its architecture allows for easier connectivity.

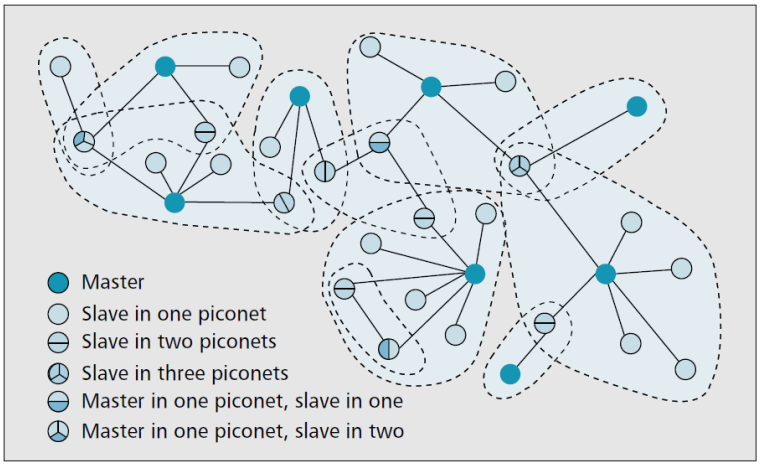

Figure 3-4 Example of a complex scatter-net configuration
(Ferro & Potortì, 2005)

EnOcean is an energy harvesting wireless technology as a 'green' and smart solution to buildings and industrial systems (EnOcean, 2015). An EnOcean module harvests its energy from motion, solar power or change in temperature; this will generate enough energy for the module to transmit wireless radio frequency signals via the low power electronics. The constraint to this technology is that the module is required to be able to convert energy. The modules do not require a battery and therefore the module should be maintenance free, apart from this the technology stands out for its lifetime of 25 years and the range of 30-300 meters, depending on interference from the surroundings.

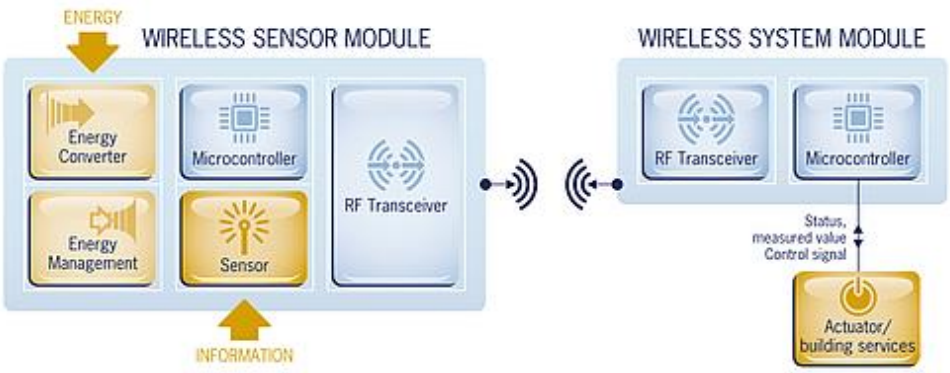

Figure 3-5 EnOcean works with a sensor and a system module
("EnOcean – Technology," https://www.enocean.com/en/energy-harvesting-wireless)

Near Field Communication (NFC) technology is a short-distance wireless communication standard, communication that is simply activated by bringing two NFC devices close to each other (Tamura & Masuda, 2013). The technology is currently being incorporated in the newest smartphones, smartcards and portable devices; it will serve a future purpose for reading, writing, saving and exchanging data more easily. The communication is characterized by its limited range of 10 centimetres with a maximum data rate of 424 kbps and it supports active-to-active as active-to-passive communication (Want, 2011). NFC is a specialized subset of the RFID technology, it differs from RFID through its secure form of data exchange and NFC can act either as a reader or a tag.

Wireless Fidelity (Wi-Fi) provides wireless connectivity between devices in a wireless local area network (WLAN) through the IEEE 802.11 standard[5] (Ferro & Potortì, 2005; Mahmood et al., 2015). The connectivity between devices is set up via a wireless access point, which routes the data traffic via the internet. The network is established through a cellular configuration where each cell is called a basic service set (BSS), which consists of one or multiple access points and devices. The networking range differs from 20 meters inside buildings up to 100 metres outside with a relative high data transfer rate of 54 Mbps, newer IEEE standards are even allowing higher data rates up to 300Mbps. Through wireless mesh concepts a self-organizing and self-healing network can be established, which leads to a high coverage and power saving solutions. Studies have showed that Wi-Fi may be a valuable option for the IoT if a solid power saving plan will be implemented (Tozlu, Senel, Mao, & Keshavarzian, 2012).

ZigBee is a wireless communication protocol and is designed by the ZigBee Alliance to compete with Bluetooth and Wi-Fi through a simple design, reliable, low power requirement and lower costs (Baronti et al., 2007; Gomez & Paradells, 2010; Mahmood et al., 2015). The PAN are created with small digital radios transmitting coded radio signals which are focussed on low power consumption. It is based on a standardized wireless networking protocol for industries operating at 2.4GHz. It requires relatively infrequent data exchange together with low bitrates, from 20 to 250 kbps, in a 30 meter. Multi-hop functioning allows the range to be 'unlimited'. The network identifies two different device types: Full Function Devices (FFD) and Reduced Function Devices (RFD), the latter one is a reduced FFD which is only able to act as an end-device equipped with sensors or actuators and communicates only with a single FFD. FFD's can either act as a ZigBee Router or a ZigBee coordinator, the first one routes the data between the nodes and the second one manages the PAN alone. It is possible to implement multiple network topologies like Star, Tree and Mesh networks[6], for a visual representation see Figure 3-6.

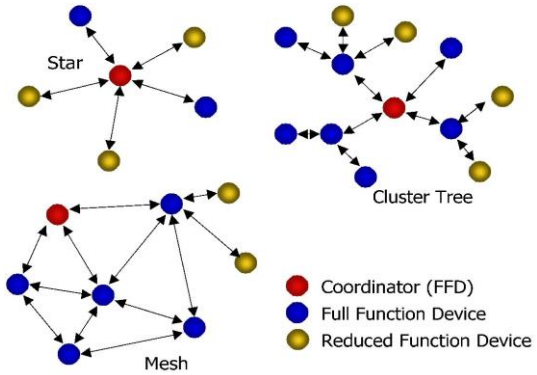

Figure 3-6 Zigbee devices types and network topologies
(Le, 2005)

[5] In short: the standard for a wireless internet connection (http://standards.ieee.org/about/get/802/802.11.html)
[6] In a star network every host is connected to a central hub, in a tree network two or more star networks are connected and a mesh network resembles a fully connected network.

Z-Wave is a wireless network topology for automation of residential environments, allowing devices to communicate small data packages from 10 kbps up to 200 kbps, lower bitrates allow a longer battery life, through a mesh network of maximum 232 nodes (Gomez & Paradells, 2010; Mahmood et al., 2015). The network is characterized that every node has routing capabilities, the network architecture has constrained the data packages to be transmitted a maximum of four times in the network. Each node has an indoor range of 30 meters which can be extended to 100 meters and so the transmittable range is constrained to 120 – 400 meters, depending on the environment. The mesh network consists of controllers and slaves, the controllers try first to reach the destination directly and if this fails the most optimal route is calculated. These optimal routes will be remembered by the routing slaving as 'static routes' and it is allowed to communicate over these routes without the need for the slave to request for permission.

3.2.2 WAN technologies

A **Cellular network** is commonly used in mobile communication and is defined as a network where the final link is wirelessly connected, where the antennas distribute the network in a cellular structure. Through a high area coverage, a large number of portable receivers, like mobile phones and tablets, can communicate with entities via antennas. This network is favoured by systems in need of a higher data transfer and high area coverage, the range differs from 35 kilometres for GSM standards (2G) to 200 kilometres for HSPA standards (3G) (Networks, http://www.privatemobilenetworks.com). However, these networks are owned by third parties and apart from building a dedicated cellular network operating costs through leasing have to be paid.

As an answer to cellular being over engineered for IoT application, **Sigfox**[7] is installing a cellular network based on Ultra-Narrow Band (UNB) technology (SigFox, 2014). It uses the same networking technology as a cellular network, but has constrained the data transfer to lower levels of 10 to 1000 bps. The lower data transfer is possible because the system only allows small data packages of approximately 12 bytes to be sent between nodes. This allows the device to have a greater lifespan, 20 years stand-by, since these lower bitrates consume up to a 100 times less energy. The company has covered the city of San Francisco with just 20 suitcase sized base stations, meaning it has a range of 6-10 kilometres in urban environments[8], and is allowing consumers to use the network for 1$ per device per year (Tilley, 2015).

3.2.3 Discussion and comparison

The above discussed technologies all differ in their characteristic way of working, range, network architecture and bandwidth. There is no optimal networking technology for the IoT, it all depends on the desired configuration and the environment it is supposed to work in, it may not even work properly. **6LoWPAN** catches the eye by its extensive scale- and operability through the IP, which is an interesting feature if the destined IoT network is for instance to be controlled from an external environment. But is it always necessary to put your IoT network on the internet itself and thus making it accessible from anywhere? **Bluetooth** excels in its accessibility and secure short range communications, but the limited amount of active nodes in a Pico-net and the short range may constraint the use of this technology in larger IoT applications. On the contrary, **Cellular technologies** may be an answer if higher areas need to be covered. There is ample bandwidth and area coverage available, but these networks need to be leased

[7] http://www.sigfox.com/en/#!/technology
[8] It is assumed the range can be up to 50 kilometres in a rural environment

or a complete new network needs to be build. The **Sigfox** company is a more fit solution for the IoT, if looked at the specifications, still the same 'leasing' problems arise when compared to a cellular network. **EnOcean** is a green and smart solution through its energy harvesting techniques, but the scale and data rates are probably too small for industrial- and transportation environments. The **NFC** is already widespread used in smartphones and –cards and will probably not be a core technology of an IoT network, but it is an interesting technology for secure proximate identification. With the scale that **Wi-Fi** is already implemented in so many devices, it is a very serious option to be at the base of an IoT network. The high area coverage, which can be easily extended, widespread availability and seamlessly interaction via the IP promote this method. **Zigbee** is a technology which is characterized to have its focus on IoT applications, it accommodates a lot of nodes in a superior networking technique at a low cost and power consumption. However, the 2.4GHz band is a popular bandwidth for wireless devices to work on and so interference may occur. **Z-Wave** is a similar solution like Zigbee, but has a different network topology by limiting the 'hopping' range to four nodes. It is intended for very small data packages and within domestic environments and probably not so for industrial ones.

To determine which is the most suitable to implement when designing a IoT network these technologies have to be compared, which is done in Table 3.2. In this table the advantages and constraints and some characteristic details are listed.

3.3 MIDDLEWARE

The IoT needs a software platform in order to fulfil the required capabilities like self-configuration, scalability and interoperability. In literature middleware is defined by (Atzori et al., 2010) as "..a software layer or a set of sub-layer interposed between the technological and the application levels" and it will play a "major role in simplifying the development of new services and the integration of legacy technologies into new ones". In sum, middleware forms a bridge between the technological and application side of the IoT via software layers. A study carried out by (Bandyopadhyay, Sengupt, Maiti, & Dutta, 2011) surveyed multiple middleware solutions, they stated that the functional components of middleware consists of:

- Interoperation
- Context detection
- Device discovery and management
- Security and privacy
- Managing data volumes

Most middleware solutions which are introduced by researchers are focussing only on one or a few of these aspects and an ideal middleware solution which covers all of these aspects is yet to be designed (Bandyopadhyay et al., 2011; Perera et al., 2014). This is due to the maturity of the IoT and that most middleware is written for a specific project, it is expected that with time a more generalized middleware will become dominant.

Table 3.2 Comparison of network topologies for the IoT

	Battery	Range [m]	Power consumption	Data rates	Characteristic	Frequency	Advantage	Constraint
6LoWPAN	Yes	Indefinite	Low	High	IP interoperability	Multiple	Global addressing Low power Self-healing	Requires an additional communication platform to reach the cloud
Bluetooth / BLE	Yes	10	Low	1 Mbps	Master/Slave Pico-nets and scatter-nets Multi-hop	2.4 GHz band	Accessibility Fast data exchange Low power consumption	Maximum of 8 devices per pico-net Power saving methods lead to weaker signal Interference on the 2.4GHz band
Cellular	Yes	35-200 km	Moderate	1 – 100 Mbps	Cellular structured Extensive coverage Pre-existing network	Multiple	High data rates Large area coverage	Placement of transmitters Simcard-like verification Possible subscription requirements
Sigfox	Yes	6 - 10 km	Very low	10 – 1000 bps	Cellular structured Extensive coverage Pre-existing network	900MHz	Large area coverage Long lifespan	Placement of transmitters
EnOcean	No	30 - 300	Low	125 kbps	Energy is harvested	315 / 868 MHz	No battery needed	Must be able to convert energy into electricity
NFC	No	0,1	None	424 kbps	Reading, writing and exchanging data	13.56 MHz	Secure form of data exchange	Short range
Wi-Fi	Yes	20 - 100	Low / High	54 – 300 Mbps	Communication via wireless access point	2.4 / 5 GHz	Strong signal High data rate Large network	Larger networks require more access points Battery powered devices and access points
Zigbee	Yes	10 - 30	Very low	20 kbps (868 MHz) 40 kbps (915 MHz) 250 kbps (2.4 GHz)	Multi-hop communication ZigBee end-device, router and coordinator	868 MHz 916 MHz 2.4 GHz	Low-power Low costs Networking Signal security	Short range Interference on the 2.4GHz band
Z-Wave	Yes	30	Low	40 kbps 200 kbps (400series)	Every node has routing capabilities Static routing	868 MHz 2.4 GHz (400 series)	Considerable range Slaves can act without permission	Low data rates Packages can only be transmitted over 4 nodes Interference on the 2.4GHz band

The Service Oriented Architecture (SOA) is often proposed as the common architecture for middleware (Atzori et al., 2010; Miorandi et al., 2012; L. Xu, He, & Li, 2014). While there is no commonly accepted SOA solution, they all abstract the device functionalities and aim to provide a common set of services. (Stankovic, 2014) concludes that with the current growth of devices being connected to the IoT "it is necessary to have an adequate architecture that permits easy connectivity, control, communication and useful applications".

The different structures which are proposed in before mentioned literature consists of multiple layers, (L. Xu et al., 2014) has made a clear overview of the different SOA compositions and generalizes it to:

- Sensing layer – integrated with existing hardware to sense and control
- Networking layer – Basic networking and data transfer support
- Service layer – Creates and manages services for the end-user
- Interface layer – Provides interaction for end-users and other applications

In order for the IoT to work to its fullest potential, autonomous communication is needed, but this represents also a future danger (Atzori et al., 2010). Devices could unknowingly be triggered and share sensitive information, this should be prevented by including functions related to the management of privacy, security and trust of the data. It is preferred that these functionalities are distributed throughout the complete layered stack, in order to not affect system performance for devices which run on low resources.

This approach allows complex systems to be decomposed into several well defined components with the use of standardized interfaces and standards. By using standardization, the system is organized on a horizontal level, this reduces the time needed for parts of the system to adapt to each other during interaction. According to the insights of (Zhong et al., 2013) SOA is a flexible set of design principles, making functional building blocks widely accessible.

Middleware propositions are numerous and most of them are specifically designed for one type of system, like the e-SENSE software which is designed for WSN (Atzori et al., 2010). For a more in depth explanation and comparison of the possible solutions, readers will be referred to the work of (Bandyopadhyay et al., 2011) where the focus lies on middleware.

3.4 DATA STORAGE AND ANALYTICS

When more devices are connected to the IoT and start delivering data, it is an unavoidable consequence that more efficient and effective methods have to be implemented for its government. (Gubbi et al., 2013) states that policies concerning storage, ownership and expiry of the data will become critical during the growth of interconnectivity. Data should be monitored and correct action has to be taken after the data is placed in the right context. It is expected by (Miorandi et al., 2012) that applications have to adapt to the user's context, but this kind of flexibility is still too far away.

The main challenge lies in the amount of noise in the generated data, it is not standardized and should be filtered first before it can be categorized (Stankovic, 2014). In the beginning a lot of data can be considered uncertain, when the system's learning curve is still steep, and this will cause the users not to fully trust the system. It is expected that after the system matures, when better data association is possible, the IoT will be far more effective.

Cloud Computing will be used to store and analyse Big Data and is defined by the National Institute of Standards and Technology (NIST) as follows:

"Cloud computing is a pay per use model for enabling available, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction." (Talia, 2014)

Cloud Computing is normally being deployed for:

- Handling highly intensive computing workloads
- Providing very large data storage facilities
- Potentially reducing management and use costs

There are several known Cloud deployment models, ranging from private clouds to shared or public clouds. These deployment models differ in the accessibility and privacy of the cloud. In Chapter 4 a more in-depth survey and discussion concerning Big Data will be made.

3.5 PRIVACY, SECURITY AND TRUST

While the IoT is being developed within domestic-, healthcare- and enterprise systems, a full scale deployment will be publically resisted as long as it lacks confidence that it holds no threat to Privacy, Security and Trust (Atzori et al., 2010; Miorandi et al., 2012). Data that is collected around individuals, enterprises or governments is considered confidential and sensitive; the management of fully using this data while keeping all actors satisfied is discussed in this section. The location of the IoT intelligence and service provisioning is considered to exist at the edge of the network (Roman, Zhou, & Lopez, 2013). These entities that operate on the edge are expected to heterogeneously retrieve and process the acquisitioned data, thus it is not preferred to completely limit and control the edge activities. In this section the current state of affairs and challenges concerning these three topics will be surveyed and discussed.

IoT providers aim for increasing the network´s scale, however security concerns arise with a higher level of heterogeneity and wireless networking scale (Gubbi et al., 2013; Sicari, Rizzardi, Grieco, & Coen-Porisini, 2014). Wireless communication can be attacked relatively easy and current effective countermeasures cannot be applied due to the limiting computing power constraints and the scalability of the IoT. If cloud computing is shared by multiple businesses or individuals, the security and identity protection is critical, solutions are expected to be found in cryptography and digital forgetting. Digital forgetting refers to the discussion how and when data should be considered expired and ultimately deleted from the IoT.

3.5.1 Privacy

The challenges and solutions concerning privacy within the IoT are referring to the norms under which data of individuals may be accessed and used (Miorandi et al., 2012). Some applications will require localization or tracking of the individual and in literature there is no consensus under which conditions this data could be accessed. In (Atzori et al., 2010; Sicari et al., 2014; Stankovic, 2014) it is proposed that privacy policies should be defined, because it is impossible for individual users to disclose their personal information, which should be guaranteeing that:

- Collected information cannot be linked to the identities of individual users
- Individual users should be informed on the way they are tracked
- Individual users should be able to set which data is private and which is not
- After it has served its purpose, the collected data is deleted

It is suggested that the above proposed policies should be open to dynamic changes, in order to prevent any future rejection.

Due to the edge intelligence, which was discussed earlier in this section, every edge entity is supposed to have relatively more control over the generated data (Roman et al., 2013). Therefore, it is possible for this entity to share only the essential part of the data, satisfying both the identity of the tracked individual and the data request of the system. This does sound promising, but if edge entities would be programmed to act without consent of the individual user, or if it is infected with malicious software, the benefit of a distributed IoT is misused and privacy cannot be guaranteed.

The in literature stated privacy requirements all aim for the same direction with different proposals. An IoT environment is considered dynamical and it is mandatory that such a system is able to constantly adapt to the user's needs. The bulk of the privacy proposals aim for strict policies for entities or SO's when considering data management and expiration; current research challenges lie in how to govern these kind of policies when the IoT keeps growing in scale.

3.5.2 Security

The different wireless components of an IoT network spend most of the time unattended and are vulnerable for unauthorized external access (Atzori et al., 2010; Miorandi et al., 2012). The discussion around the security of the IoT concerns the authentication, confidentiality and access control of the SO's and their processed data. Due to low energy requirements and constrained computing resources, it is impossible to implement complex security schemes which are currently used in the Information Technology (IT). The security issues are also a bit more complex, since both users and SO's should be able to gain authorization to access data. The danger lies in the situation that either sensitive data is collected illegally or that raw data is interpreted wrongly[9]. Solutions are not straightforward due to the amount of data that is collected and the need for everything to be online constantly.

In (Sicari et al., 2014) different studies were analysed on the security topic and it was concluded that a unique and well-defined solution for the IoT context is missing, questions lie in how and where the security should be handled. Most studies aim for the solution to encrypt the data and secure it with a security key or a decryption algorithm at routing points within the system. There are also some suggestions from (Roman et al., 2013) to work with Role Based Access Control (RBAC) so that SO's can earn, or lose, their credentials by (dis)approval of users and other entities in the system. While independent systems will be able to work out a decent solution, a standardized security method is still far away.

[9] Would an unauthorized individual be able to interpret, for instance, environmental monitoring data of an earthquake early warning system without an appropriate risk management strategy?

3.5.3 Trust

The notion of trust is a complex one and it misses a definitive consensus in literature (Miorandi et al., 2012; Sicari et al., 2014). Trust can be explained as a negotiation language in which both privacy and confidentiality is satisfied for both parties. Trust exists around questions if SO's are processing and handling data in compliance with the end-users needs and rights, but also in the notion if two SO's can authorize each other. Different proposed solutions have been analysed in literature (Roman et al., 2013; Sicari et al., 2014) and direct towards a hierarchical model or reputation mechanisms. In the same study it is concluded that the current research of trust is mature enough, but solutions to a fully distributed and dynamical approach are hard to find.

3.6 DISCUSSION

In this chapter the availability of the enabling technologies for the IoT in literature were discussed and presented. The technologies can be categorized in either hardware or software and the literature study showed that on each technology layer multiple solutions exist. For almost all layers, there is no optimal choice and per IoT implementation a separate study could research the ideal set. As was concluded in the previous section, there is no standardized consensus of the IoT and currently there are not indications that this will be formed in the near future.

In section 3.1 and 3.2 a tabular overview was presented to give a representation of the available hardware technologies for identification, tracking and networking. In section 3.3 and 3.4 the discussion around middleware architecture and big data analytics was surveyed and in the final section 3.5 the different view on security policies were listed. The challenge of standardization recurred in every topic and potentially this issue will remain. The IoT is envisioned as a distributed and heterogeneous system and a lot of technological issues arise when such a system is implemented on an enormous scale.

4 BIG DATA

Every day more data is generated by Enterprises, Social Media, Multimedia and the IoT (Kambatla, Kollias, Kumar, & Grama, 2014). As an example, a few hundred Terabytes of operational information are stored by Boeing's jet engines during a Transatlantic flight, to be analysed and compared to all the historical data. Every minute over a 100 hours of video material are uploaded and around 135.000 hours are streamed on YouTube and complex data analysis tools are running to find new correlations of behavioural mechanisms. These two examples show that an overwhelming amount of data is generated and analysed, but questions may arise if this data could be useful. Individually it can be considered valueless, but when accumulated data is exploited useful information can be identified and potential forecasts can be made (M. Chen, Mao, & Liu, 2014). A paper published (McKinsey & Company, 2011) shows an extensive research on the value of Big Data in different sectors like Retail and Manufacturing, they concluded that Big Data can contribute economically to enterprises and public sectors and that it will create benefits for end-users.

The subject of Big Data concerns the need for real-time analysis of enormous datasets and masses of unstructured data, which are gathered in various fields(Hashem et al., 2014). The data is numerous, it cannot be categorized within standard relational databases and the capturing- and processing processes are executed rapidly. The underlying engine of Big Data is supported by the service called Cloud Computing, which has been briefly introduced in the previous chapter. With Cloud Computing a much larger scale and more complex algorithms can be employed to meet the, continuously growing, demands of Big Data.

However, the rapid evolution of Big Data left little time for the subject to mature in academic literature and there exist little consensus of the fundamental question when data is qualified as Big Data (Gandomi & Haider, 2015). Still a substantial part of the found literature (multiple authors, cited in Chen et al., 2014; Gandomi & Haider, 2015; Hashem et al., 2014)) direct towards the same meaning and they distinguish Big Data from normal analytics via four V's:

- Volume : The massive data volumes which are processed
- Variety : The data is collected from a great variety of sources in multiple formats
- Velocity : Data is acquired, sent and analysed with high data transfer rates
- Value : Value is found in, first considered, unstructured and uncorrelated data

The growth of these two fields further promote the growth of the IoT (M. Chen et al., 2014), according to the paradigm sensors all over the world transmit their collected data and there would be need to store and process this data in the cloud. This chapter will cover a basic overview of Big Data and Cloud Computing with their related technologies and challenges.

4.1 THE BIG DATA VALUE CHAIN

The processes which are employed in order to extract information from Big Data fall under the Value Chain and these are explained differently in literature by (F. Chen et al., 2015; M. Chen et al., 2014;

Gandomi & Haider, 2015; Philip Chen & Zhang, 2014), in this section a consensus will be portrayed. It depends on the requirements of the system if some of the following functions are outsourced or not, this can be decided from either a confidential or financial perspective, therefore only the processes will be explained how they should work. The fundamental steps are as follows:

- Data generation
- Data preparation
- Data storage
- Data analysis
- Data visualisation

Current main sources of Big **Data generation** are from various directions like traders, enterprises, IoT and scientific research. It is estimated by (McKinsey & Company, 2011) that the business data volume of companies worldwide doubles every 1.2 years, which shows that means for having an effective value chain are grounded. This papers focusses on the shared interests between the IoT and Big data, the generated data from the IoT can be characterized as:

- Being immensely scaled since the IoT is deployed in a distributed manner
- Having a great variety in data types, due to the variety in IoT devices
- Being correlated in both space and time
- Having only a small portion of valuable data, due to potential noises in acquisition and transmission of the data

This means that decent management of the following step, **Data preparation**, is needed. Data preparation stands for all the necessary steps which are employed before data is stored in the cloud and these consist of data collection, transmission and pre-processing. Data collection and -transmission for the IoT happen at component level and the different enabling technologies are introduced in the previous chapter. The data which is sent by the SO´s vary in consistency and noise and it is considered a waste to store all this data in the cloud. Various techniques for pre-processing are discussed by (F. Chen et al., 2015; M. Chen et al., 2014) and these target to:

- Integrate correlating data from multiple sources to provide a uniform view of the data
- Cleanse data from inaccuracies and incompleteness by either deleting or modifying this data set
- Eliminate redundancies via recognizing repetition or surplus of data

Prepared data is then send towards a **Data Storage** centre, storage systems for Big Data are classified as Direct Attached Storage (DAS) or Network Storage (NS). In DAS data is connected through peripheral devices and is commonly used in small sized data storage centres. NS provides via a network ubiquitous data access via a union interface and is characterized for a strong expandability. (Hashem et al., 2014) notes that most storage systems are limited in their computational- and/or storage capacity and should not be considered useful for Big Data. The exact hardware and technical features of storage centres will be left out of the scope for this literature survey.

The **Data Analysis** functionality refers to the intelligence extracted from applying complex algorithms to Big Data. In literature several techniques concerning data analysis are discussed and reviewed (F. Chen et al., 2015; Gandomi & Haider, 2015; Kambatla et al., 2014). There exists a general consensus that multiple intelligent learning tools exist which can derive intelligence from (un)structured data within numerical- and text files, web and mobile data, recorded audio, video and social media. If these learning tools do not show direct results, complex data mining models will be created which will further analyse the big data for new associations, behaviour and classifications.

Data Visualisation is the graphical representation of the learned knowledge via analysis in a more intuitive and effective way (Philip Chen & Zhang, 2014). To have the necessary effect of the visualisation the information has to be conveyed graphically in both aesthetic- and functional form. Current known data visualisations are done separately and these serve only their own purposes, the main challenge of creating a general solution lies in the immense size and dimension of Big Data.

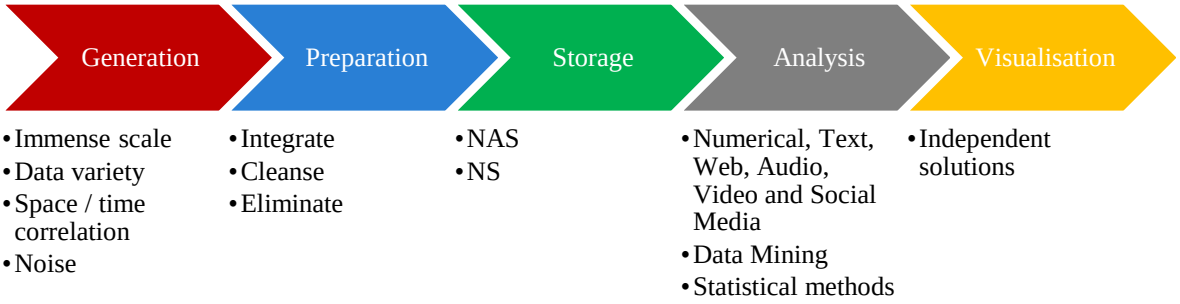

Figure 4-1 The Big Data Value Chain

In order to have an ubiquitous and on-demand access to the Big Data Storage, Analysis and Visualisation the technology of **Cloud Computing** is adopted in IoT literature (M. Chen et al., 2014; Gubbi et al., 2013; Hashem et al., 2014; Jin, Wah, Cheng, & Wang, 2015), see Figure 4-2 . Due to the limited resources in computational power, battery lifetime and storage capacity of IoT devices, outsourcing of these functionalities is a welcoming solution. There are various Cloud Computing services which offer multiple services: first of all, there are Platforms as a Service (PaaS) like the millions of applications for mobile devices found in ‘app-stores’, then there are Software as a Service (SaaS) available as on-line software applications (Gmail, Windows Live, Google Docs) or Infrastructure as a Service (IaaS) which refer to on-line hardware applications providing computational power or storage capacity. Services provided by Cloud Computing can be seen as the underlying engine of the IoT.

4.2 DISCUSSION

In this chapter the subject of Big Data was introduced and the essential features were discussed. Like the IoT, Big Data is becoming a popular term in scientific literature, see Figure 4-3, but it can be concluded that current research is not matured yet(Hashem et al., 2014). There are still some open research challenges, which are defined by (M. Chen et al., 2014; Hashem et al., 2014; Philip Chen & Zhang, 2014), these are expected to further enhance the development of Big Data and therefore also the IoT:

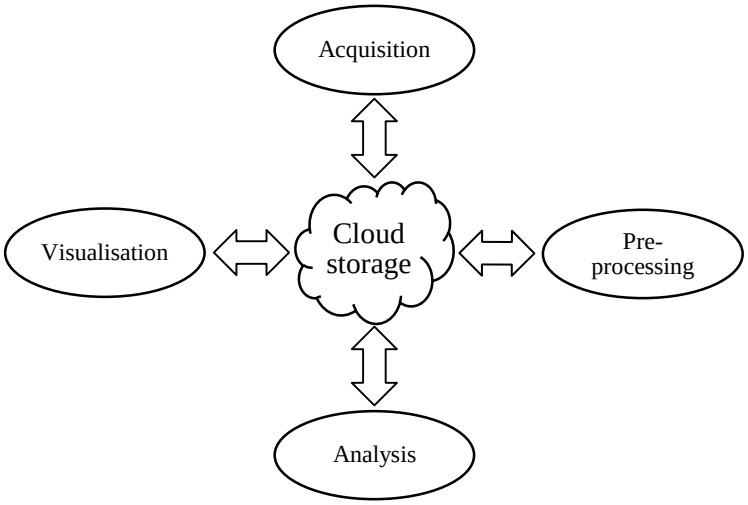

Figure 4-2 Cloud Computing as the underlying engine of the Big Data in the IoT

- Data life cycle management, when to keep or discard data
- Scaling solutions, how to cope with current data growth
- Data quality and integrity, how to verify and ensure consistent data with the rise of possible data sources
- Data uncertainty, how to deal with incomplete but important data
- Data security and online access, how to ensure operation during a security breach

Still it shows already a lot of promise in the applications of Smart Grids, Predictive Manufacturing Systems, Enterprises and Social Media (M. Chen et al., 2014; Jay Lee, Lapira, Bagheri, & Kao, 2013; Mahmood et al., 2015; McKinsey & Company, 2011).

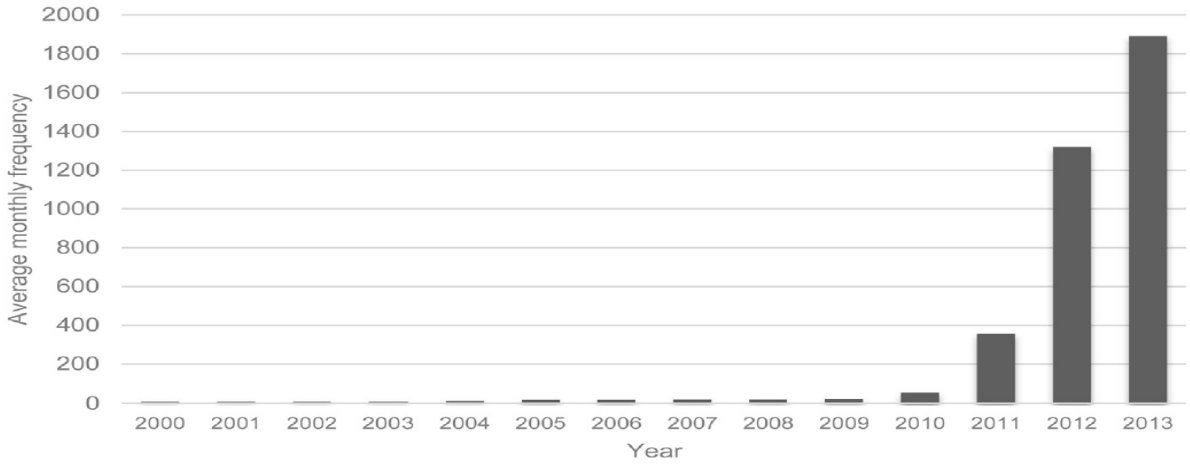

Figure 4-3 Frequency distribution of the term "big data" in literature (Gandomi & Haider, 2015)

5 APPLICATION OF THE IOT IN TRANSPORT SYSTEMS

Case studies regarding IoT implementation and application in transport systems will be discussed in this section, which should give a better understanding of the potential impact. With the IoT's evolution of physical objects to SO´s new markets are opened (Miorandi et al., 2012). Businesses will be able collect more data and knowledge via digital means, allowing vertical markets to bridge knowledge and to further improve their supply chains. RFID technology has been around for a while, but with the current trends these environments are equipped with primitive intelligence and require substantial upgrades before it can contribute to the IoT. In literature and on the internet there are high expectations of the IoT, but its widespread adoption will only be driven when the public has fully accepted it.

5.1 SELECTION AND ABSTRACTION OF BEST PRACTICES

There are numerous examples of IoT implementations around, but in this survey it has been limited to two topic areas: Logistics and Industry. These subjects are chosen in order to fit the survey's scope 'intelligent control for transport systems'. Within these subjects several implementation cases have been found and in this section they have been categorized dependent on their application. The created overview is meant as a best practices summary, giving a clear overview of the driving factors for IoT implementation. The abstracted categories are as follows:

- Real-time optimisation
- Fault prediction
- Safety and security
- Improved life cycle analysis

Each category will be treated with one or several examples from either literature or industry, it is aimed to give the readers tangible insights and hopefully some inspiration.

5.1.1 Real-time optimisation

Optimisation models could be further improved if the response time to sudden changes within the standard operations could be minimized. There are existing optimisation models which have been proven to be very efficient, but through the IoT it should be possible to provide a more real-time response model. In (Liu & Sun, 2011) it is proposed that through the current developments in the IT, businesses can evolve from intra-enterprise to cross-enterprise and bridge vertical markets. If these vertical markets will be connected to an overlapping IT infrastructure, in which they will project their supply and demands, **enhanced planning, forecasting and inventory models** are created. These models allow to be adapted constantly to drastic changes within a supply chain through joint visibility whilst considering each of the actor's interests.

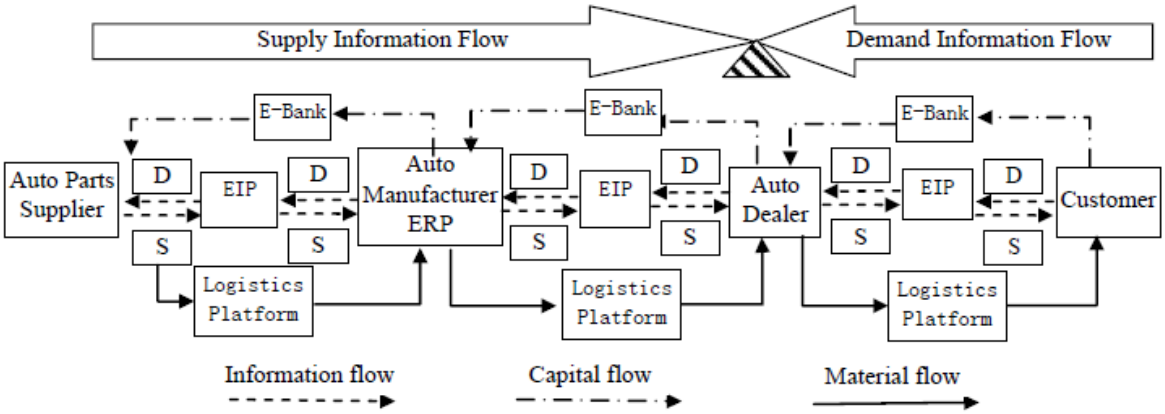

Figure 5-1 Logistics within an automotive manufacturers supply chain (Liu & Sun, 2011)

Collaborative planning, forecasting and replenishment (CPFR) is used for supply chain integration and concentrates on enhanced information sharing in vertical businesses, current CPFR models only share information between neighbouring actors. In this paper this approach is combined with the IoT in enhancing the inbound logistics of automotive manufacturers, providing quick and on-time service for each actor within the supply chain. Figure 5.2 shows the foreseen change in the supply chain, giving smart capabilities to the system as a whole. Each link in the chain is able to analyse the current trends in the market through the ubiquitous access of data and is therefore able to adapt to sudden changes, realising lower safety stocks and more transparent scheduling.

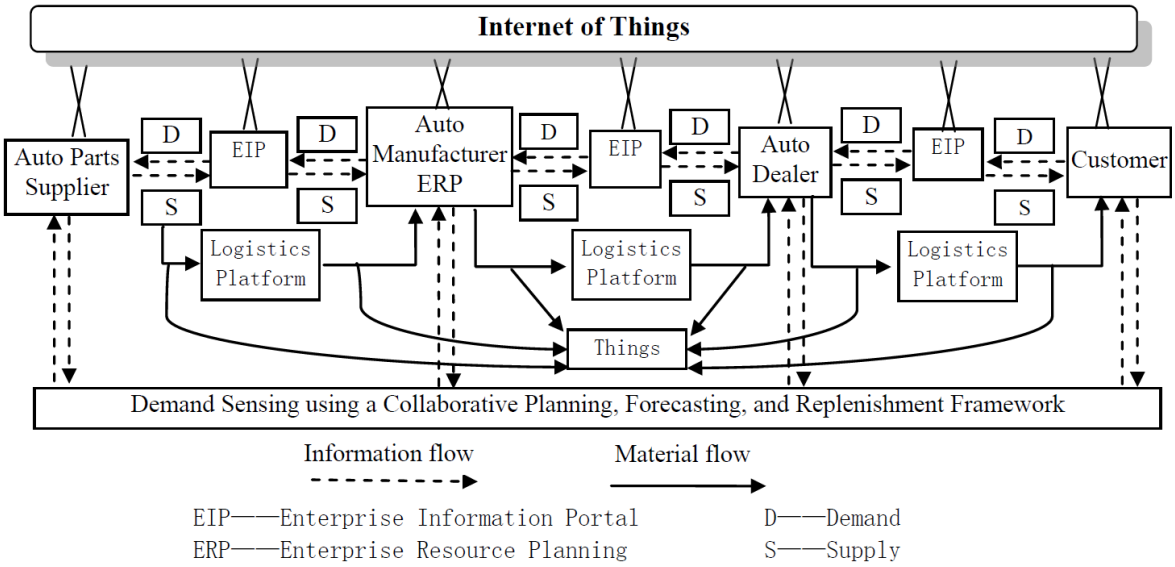

Figure 5-2 Proposed IoT architecture for vertical bridging within a supply chain (Liu & Sun, 2011)

Similar solutions are proposed in the papers of (Zhong et al., 2013; Zhong, Lan, Xu, Dai, & Huang, 2015) but they focus more on joint visibility within a single enterprise. Both papers state that decision making is improved through a clearer understanding of the real-time logistic trends within the facility and this enhances directly the efficiency of production and the operators. The proposed tools and visualisation

methods are currently being tested with industrial collaborators and Zhong's paper from 2015 reports its feasibility by sharing the first results.

An industry which can benefit from real-time optimisation is the field of Food Supply Chain (FSC). In the FSC the goods have a degrading quality and thus **optimal use of these resources** is of upmost importance. There is a huge base of mathematical and modelling solutions or proposals to solve these problems, see for instance the works of (Caixeta-Filho, 2006; Ferrer, Mac Cawley, Maturana, Toloza, & Vera, 2008; Lin & Negenborn, 2015), but the translation to practice is sometimes missing.

In (Pang, Chen, Han, & Zheng, 2015) it is discussed that current IoT application studies are either inadequate in technology alternatives or too general in application[10]. The IoT solution presented by them shows that the entire FSC has been abstracted in a number of scenarios: Produce, Store, Transport, Sell and Consume; each of these scenarios has been abstracted that services within these are similar. For each of the abstracted scenarios an entire IoT system has been set up and is linked with the other scenarios, this is an interesting approach and it allows the designers to optimize the design for each specific scenario.

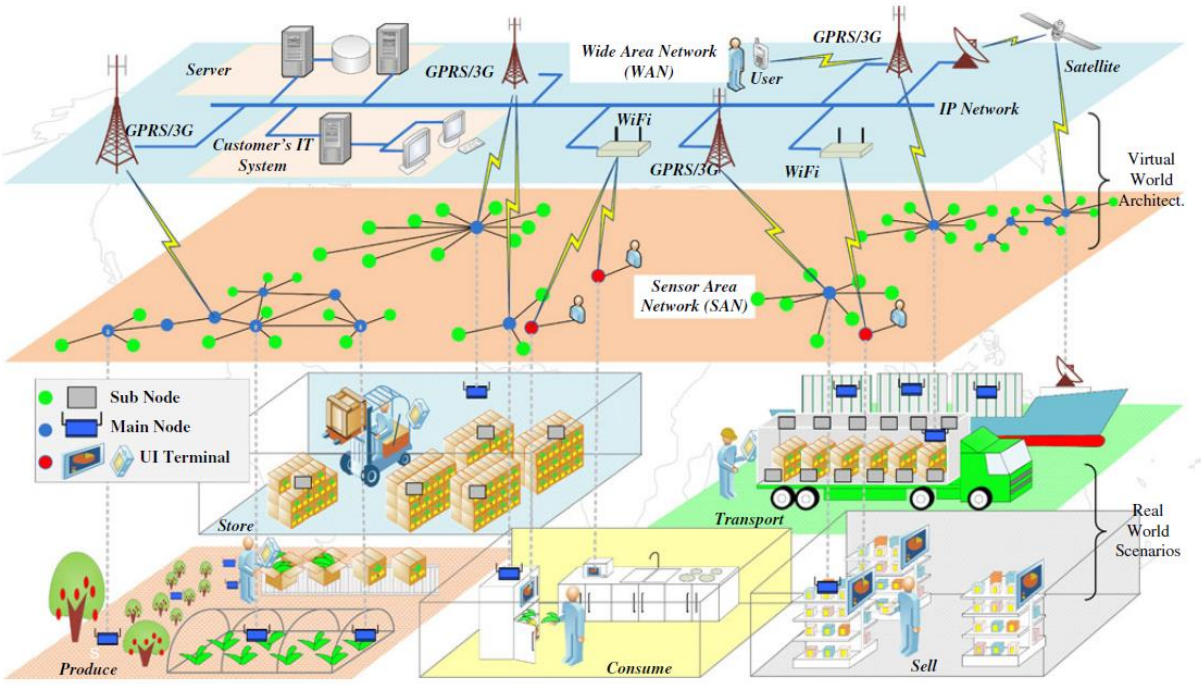

Figure 5-3 Proposed model for IoT implementation within FSC

5.1.2 Fault prediction

Parallel to the developments of the IoT, of changing everyday objects to SO's, there was a rise in interest of implementing similar technologies to industry. This was seen as the fourth industrial evolution, and given a buzz-like term '**Industry 4.0' (I4.0)**, and it has seen already a growing interest in various industrial fields (Bosch, 2015). I4.0 differs in two ways from the IoT in that the general scope is on improving its own supply chain and operations, opposing the IoT which focusses on enhancing the quality of life of most actors in a system. The second difference is that most industries already have a firm base of sensing and actuating technologies, but lack the required IT architecture or cyber-physical system to use them to their full potential.

[10] There is also a very interesting notion concerning the current methodology for IoT solutions. Pang discusses that, in order to have an effective and innovative IoT solution, the design should never be value-centric.

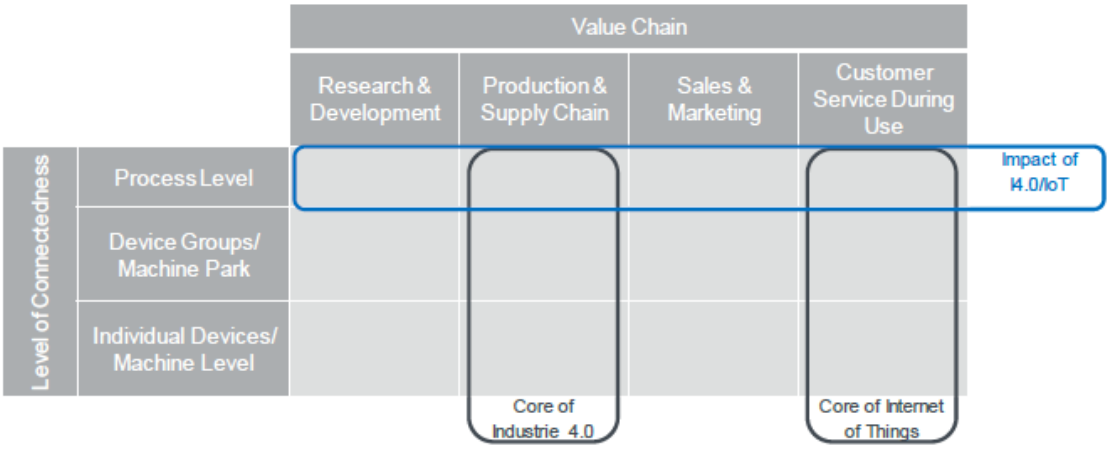

Figure 5-4 Overlap of IoT and Industry 4.0 (Bosch, 2015)

On most agenda's in I4.0 the topic of **predictive maintenance** is listed, which aims to lead to less unscheduled downtimes and potential lower maintenance costs. In (Leitão, Rodrigues, Barbosa, Turrin, & Pagani, 2015; X. Xu, Chen, & Minami, 2012) it is showed how the IoT can improve current maintenance standards, by placing sensors at key machine components and having decent machine-to-man communications. By analysing the behavioural trends of the machine even the slightest disturbances could be noticed and centralized maintenance experts could take decent action depending on their interpretation of the change in behaviour. Companies like Bosch GmbH and SAP are already offering services in predictive maintenance and their reports (Bosch Software Innovations, 2016; SAP, 2016) tell that there is already a lot of promise but even more to achieve in the future.

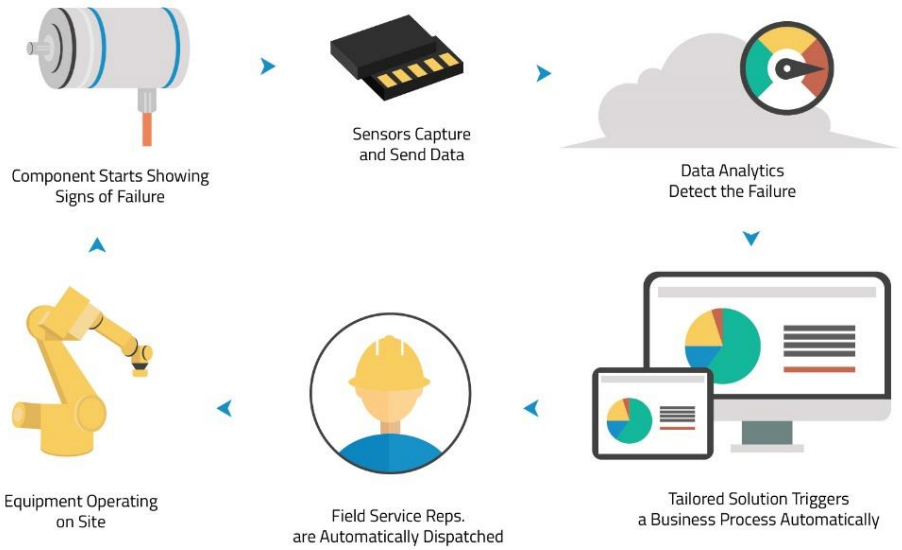

Figure 5-5 IoT predictive maintenance model ideology (Tamburini, 2015)

Machinery is to be equipped with temperature, infrared, acoustic, vibration, battery-level and sound sensors on its critical and wearable parts. These machines will be monitored by an overlapping system which analyses and tracks their behaviour, which can give clearer indications for the need of maintenance. This enables a novel ideology which continuously tracks the current machine status, preventing failure and thus preventing the higher costs of serious breakdowns. This allows companies to:

- Offer comprehensive solutions to their customers
- Optimize their maintenance services
- Higher efficiency of the maintenance processes
- Increase in operation productivity

An example is found in the online article of (Grayson, 2014) in which the effect of predictive maintenance by the company Caterpillar is accompanied with positive financial results. Machine performance, like fuel levels, throughput and maintenance intervals, is tracked via real-time measurements and fed back to both maintenance specialists and Caterpillar itself. The insights that are derived from analysing and harnessing this data, coming from their machinery, engines and services, are shared within their own supply chain. This leads to the anticipation of potential breakdowns and to proactively scheduling of their maintenance, which leads also to a higher productivity at their customer and turnover for their dealers. This shows that not only the IoT enhances Caterpillars own processes, but also of their customers; this will ultimately lead to better customer relations and hopeful an increase in sales.

Whilst not exact configuration details could be found of the overlapping system, similar services are now offered by Microsoft Azure. The offered services address the big data that is generated from the various sources and returns a more comprehensive interpretation in a dashboard, see figure 5.5. This dashboard only shows the product, information which is easily interpreted by the reader, the more sophisticated data analytics are run from the background.

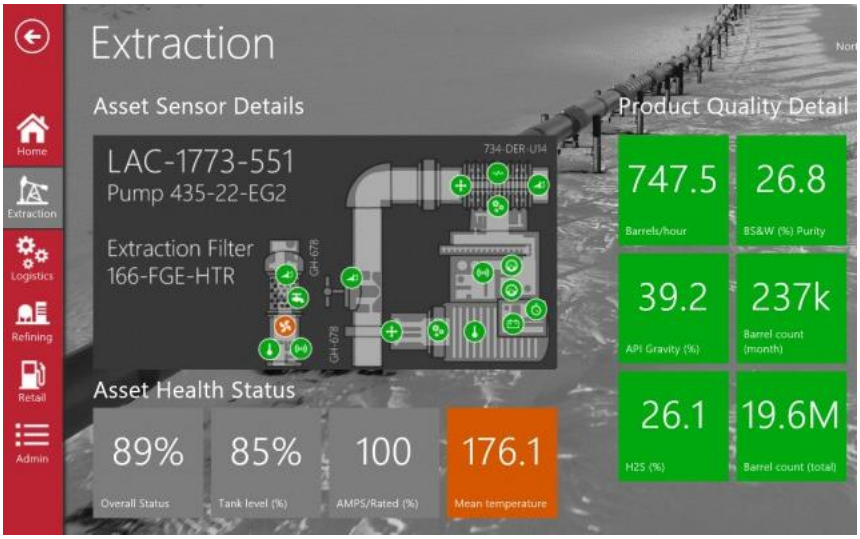

Figure 5-6 Example of predictive maintenance dashboard (Edsons, 2015)

5.1.3 Security and safety of assets

Company assets can be secured via the IoT, since not everything can be completely secured with known security measures like video- and visual surveillance. An early warning system can be installed which can give **improved situational awareness** when unauthorized access has been taken in the system, with the IoT any object within this system could potentially have this authority. Whether the entry of an individual in protected areas is noticed, or a locking mechanism has been opened for no specific reason, an appropriate action can be taken by the system without shutting it down completely. (Shi, Tao, & Voß,

2011) has proposed a RFID container seal which could be used within container terminals. While the seal off course gives physical protection, any actor can track and trace real-time the container's location via the various choke points within the container supply chain. Next to this there is also a financial benefit: (Pang et al., 2015) explains the 'sales premium' condition, which explains that customers are willing to pay more for assets if these are managed via a secure track- and trace system and they even show more interest if they have access to these systems as well.

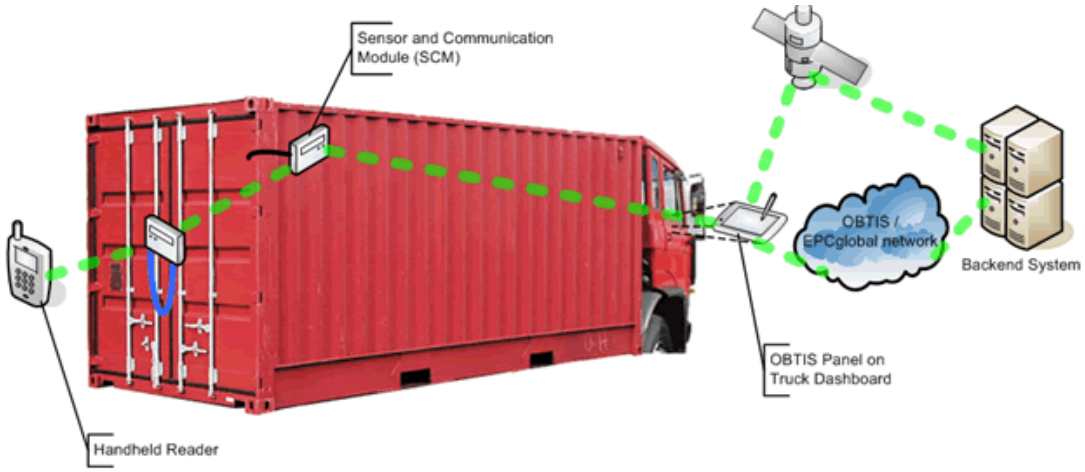

Figure 5-7 Sketch of a RFID container seal system

Next to having a secure environment, the safety of the individuals should also be concerned. A safety system is introduced by (Accenture, 2015; Qiuping, Shunbing, & Chunquan, 2011) for Marathon Oil Refineries[11] and it deploys a WSN via their employee's equipment, these sensors could notify if the environment becomes unstable or unsafe and it is hoped that this will be sufficient to prevent complete disasters. These SO's are equipped with GPS, Oxygen sensors and gas detectors; the industrial site is covered by a WSN. Also managers could trace their employees and others statistics to track their wellbeing, like their ambient oxygen level, the other way around employees could notify their managers if something is wrong by employing a panic button. Problems may arise in environments like underground mines, where these WSN should notify the user of any harmful gasses. But some of these harmful gasses could be ignited by the wireless devices and there is insufficient research on the exact effect of battery powered wireless devices, which can ionize sparks through their electrostatic charge.

[11] Video log made of the Accenture Life Safety Solution: https://www.youtube.com/watch?v=SEVP1of584I

Figure 5-8 The SO implemented for Marathon Oil Refineries by Accenture

5.1.4 Complete life-cycle analysis

While the utilisation of RFID and track- and tracing methods are not new to transport systems, these could be improved via the IoT. Most implementations within logistic systems use passive RFID to track assets within their system, while previously discussed technologies could extend this range such that assets can be tracked (to some extent) until it is end-of-life. There are various publications concerning the combination of RFID and IoT within such systems (Pang et al., 2015; Shi et al., 2011; Zhong et al., 2013, 2015), but these were discussed earlier.

In (Karakostas, 2013) an overlapping architecture is proposed which applies the RFID identification on a larger scale. Current naming systems give 'unique' identifiers but this is limited to the logistic chain. Global standardisation could be useful for intercontinental logistics by implementation a Domain Server Name (DNS) architecture, a DNS implementation would mean that even intercontinental transport could be tracked from end to end. However, this still requires developments in legal and commercial fields before it can become reality.

Another example is that of (Leitão et al., 2015) in which a case is discussed where laundry washing machines are traced until end-of-life, this case is implemented at several Whirlpool factories during this study. In their framework three different levels of intelligence are introduced, where each different level is used at a different stage within the chain. For instance, during production the SO is open to re-routing, customization and traceability whilst during distribution the SO transmits specific conditions which are of interest for tracking the quality of transport and when it is in operation it communicates its condition and functional behaviour. Since it aims to achieve multiple sets of features during its life cycle, these different functionalities have to be provided by multiple agents. Solutions are sought by **encapsulating** these **services** under the SOA, which should operate from an overlapping middleware situated in the cloud. This process is managed through multiple agents, which all have a specific priority on their agenda like quality or productivity. In this multi-agent system these agents negotiate with each other to realise the most ideal outcome for the system as a whole.

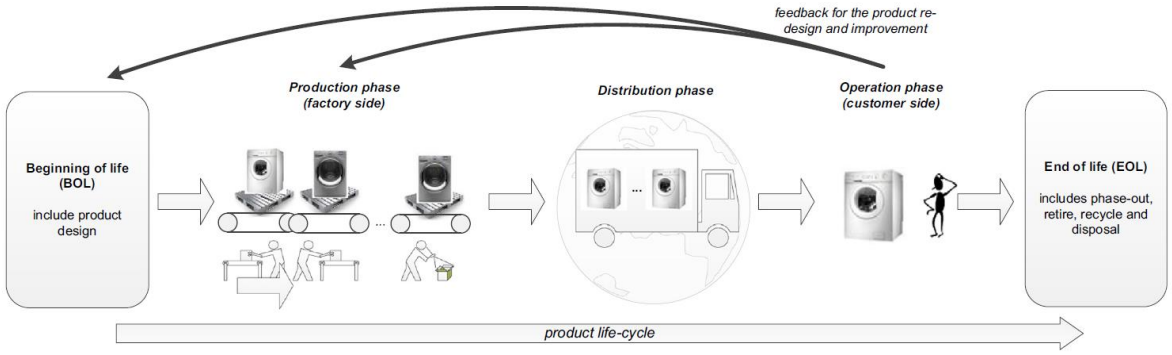

Figure 5-9 Feedback during product life cycle

This information could be later used for newer design, which is actually a new methodology called Business to Many (B2M). With B2M customers can help enhance innovations from their user experience, which is according to e-marketing a promising trend.

5.2 DISCUSSION

The discussed trends are taken from a selection of literature to give an idea how the IoT could be implemented in current logistic and industrial transport systems. The list, which is summarized in Table 5.1, is probably not a complete presentation of all IoT implementations and further research could improve this list.

Table 5.1 Overview of IoT implementation publications per enhancement

Category	Enhancements	Literature
Real-time optimisation	Forecasting Planning Scheduling Optimal use of resources	(Liu & Sun, 2011; Pang et al., 2015; Zhong et al., 2013, 2015)
Fault prediction	Maintenance	(Bosch Software Innovations, 2016; Leitão et al., 2015; SAP, 2016; X. Xu et al., 2012)
Safety and security	Situational awareness	(Accenture, 2015; Pang et al., 2015; Shi et al., 2011; Zhong et al., 2015)
Improved life cycle analysis	Range of logistic chain After sales analysis Service encapsulation Customer relationship	(Karakostas, 2013; Leitão et al., 2015; Pang et al., 2015; Shi et al., 2011; Zhong et al., 2013, 2015)

6 CONCLUSION AND RECOMMENDATIONS

In this literature study it has been tried to answer the scientific questions listed in the introduction, in order to give an organized survey of the IoT. The first section treated the different visions which were present in literature and it was concluded that probably the scientific community for the IoT has not matured yet. These visions could be categorized in three parts: the internet-, the things- and the semantic perspective and each approaches the IoT from that specific angle. In practice these angles intersect, but there was no real overlapping scientific research found which indicates that the IoT is represented in one field. It could be debated if the IoT is indeed a single scientific field, because the term IoT is also frequently used as a buzz word serving marketing purposes, and different 'IoT' implementations are only correlated.

Even if there exist no real consensus on the IoT definition, a lot could be found on the technologies constituting the IoT. Whilst multiple studies gave different technological structures, a consensus was created in chapter 3. Almost all technologies are not new, but the innovation lies in the combined use of these. Next to creating an overview of the commonly accepted technologies for the IoT, a comparison was created for 1) Identification- and tracking technologies and 2) Communication and networking. These comparisons would hopefully give further insights in what is currently available and which technology is probably best suited for a specific application. Still it is recommended to extend this research into known cases of IoT implementation to see if there are specific design considerations, which are not yet listed in the tables presented and should be taken into account. Finally, an overview was shared of the current discussions concerning Privacy, Security and Trust. It is acknowledged that the public only accepts the IoT completely, and thus allowing it to work to its fullest potential, if these three subjects are completely respected.

As with the IoT, Big Data is a subject which has seen increased popularity over the last few years. Through literature, which is also not completely matured, the Big Data value chain was constructed and this gave a clear overview of the technologies needed to constitute Big Data. The specifics of the needed software architecture, different analytical models and data centres were left out, because this would not fit in the scope of this survey. It was also found that Big Data is outsourced, meaning that while Big Data and IoT work together they normally are not worked at the same place. Still the expectations look promising and in actual results are already numerous in literature.

While the first sections covered the theoretical basis for the IoT, the final section tried to give a more practical insight into the IoT. Several application studies have been analysed and finally it was tried to derive the motivating factors for IoT implementation. The factors have been abstracted to four areas, this is merely an interpretation made in this survey and it serves as an overview of what has motivated the Logistic and Industrial community to implement the IoT. These categories were found to be 1) Real-time optimisation, 2) Fault prediction, 3) Safety and Security and 4) Improved life cycle analysis. It could be concluded that the IoT can enhance current transport systems, but these environments should always

consider to first make a solid business case of what they want to achieve with this implementation. A very interesting notion was found in an I4.0 study of (Landrock, 2016) done for Bosch GmbH. In this report the current IoT implementation trends are criticized, for most users pursue a bottom-up approach; they try to implement the IoT on a project basis in order to solve one goal. He stresses that if companies try to pursue a more strategic approach, which is called top-down, more interesting results could be achieved. Perhaps it is still too early for such an approach, but finally industry will be forced to rethink their current value chains.

All these sections covered the content to answer the sub questions to the research question of this literature survey, which was:

'What is the (predicted) role of the Internet of Things within intelligent transport systems, according to literature and relevant practices in industry?'.

The current role of the IoT is still meagre represented within transport systems. Most of the implementations cover existing sensor networks within industrial environments or present some nice tricks within domestic, safety- and energy saving systems. But this only means that the IoT is still in a very early stage of development and the scientific society needs more time to further improve the possible implementations. The biggest constraints of the IoT lay in the technological constraints like battery-life and physical size; furthermore, there is still a lot of debate on security and privacy issues. Still the current representations do show signs of improvement and this means that the IoT has potential.

BIBLIOGRAPHY

Accenture. (2015). *Winning with the Industrial Internet of Things*. *Industrial Internet of Things*. Retrieved from https://www.accenture.com/us-en/insight-industrial-internet-of-things.aspx

Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., & Cayirci, E. (2002). Wireless sensor networks: a survey. *Computer Networks*, *38*(4), 393–422. http://doi.org/10.1016/S1389-1286(01)00302-4

Ashton, K. (2009). That "Internet of Things" Thing. *RFiD Journal*, 4986. Retrieved from http://www.itrco.jp/libraries/RFIDjournal-That Internet of Things Thing.pdf\npapers3://publication/uuid/8191C095-0D90-4A17-86B0-550F2F2A6745

Atzori, L., Iera, A., & Morabito, G. (2010). The Internet of Things: A survey. *Computer Networks*, *54*(15), 2787–2805. http://doi.org/10.1016/j.comnet.2010.05.010

Bandyopadhyay, S., Sengupt, M., Maiti, S., & Dutta, S. (2011). Role of Middleware for the Internet of Things: A Study. *International Journal of Computer Science & Engineering Survey*, *2*(August), 58–63.

Baronti, P., Pillai, P., Chook, V. W. C., Chessa, S., Gotta, A., & Hu, Y. F. (2007). Wireless sensor networks: A survey on the state of the art and the 802.15.4 and ZigBee standards. *Computer Communications*, *30*(7), 1655–1695. http://doi.org/10.1016/j.comcom.2006.12.020

Bosch. (2015). *Industry 4.0 Market Study*. Berlin.

Bosch Software Innovations. (2016). Predictive Maintenance: The intelligent way to maximize machine availability. Retrieved January 28, 2016, from https://www.bosch-si.com/solutions/manufacturing/predictive-maintenance/increase-machine-uptime.html

Caixeta-Filho, J. V. (2006). Orange harvesting scheduling management: a case study. *Journal of the Operational Research Society*, *57*(6), 637–642. http://doi.org/10.1057/palgrave.jors.2602041

Chen, F., Deng, P., Wan, J., Zhang, D., Vasilakos, A. V., & Rong, X. (2015). Data mining for the internet of things: Literature review and challenges. *International Journal of Distributed Sensor Networks*, *2015*(i). http://doi.org/10.1155/2015/431047

Chen, M., Mao, S., & Liu, Y. (2014). Big data: A survey. *Mobile Networks and Applications*, *19*(2), 171–209. http://doi.org/10.1007/s11036-013-0489-0

Edsons, B. (2015). Azure IoT Suite predictive maintenance. Retrieved February 22, 2016, from https://blogs.microsoft.com/iot/2015/12/01/azure-iot-suite-predictive-maintenance-now-available/

EnOcean. (2015). EnOcean – Technology. Retrieved November 30, 2015, from https://www.enocean.com/en/energy-harvesting-wireless/

Evans, D. (2011). The Internet of Things - How the Next Evolution of the Internet is Changing Everything. *CISCO White Paper*, (April), 1–11. http://doi.org/10.1109/IEEESTD.2007.373646

Ferrer, J. C., Mac Cawley, A., Maturana, S., Toloza, S., & Vera, J. (2008). An optimization approach for scheduling wine grape harvest operations. *International Journal of Production Economics*, *112*(2), 985–999. http://doi.org/10.1016/j.ijpe.2007.05.020

Ferro, E., & Potortì, F. (2005). Bluetooth and Wi-Fi Wireless Protocols: A Survey and a Comparison. *IEEE Wireless Communications*, (February), 12–26.

Finkenzeller, K. (2003). *RFID handbook Aplications, Technology*. *Jone Willey & Sons*. http://doi.org/978-0-470-69506-7

Gandomi, A., & Haider, M. (2015). Beyond the hype: Big data concepts, methods, and analytics. *International Journal of Information Management*, *35*(2), 137–144. http://doi.org/10.1016/j.ijinfomgt.2014.10.007

Gershenfeld, N., Krikorian, R., & Cohen, D. (2004). The Internet of Things. *Scientific American*, *291*(4), 76–81. http://doi.org/10.1038/scientificamerican1004-76

Gomez, C., & Paradells, J. (2010). Wireless home automation networks: A survey of architectures and technologies. *IEEE Communications Magazine*, *48*(June), 92–101. http://doi.org/10.1109/MCOM.2010.5473869

Grayson, W. (2014). Caterpillar pushes dealers missing out on billions in sales each year to increase use of telematics data. *Equipment World - Construction Equipment, News and Information*, p. 1. Retrieved from http://www.equipmentworld.com/caterpillar-pushes-dealers-missing-out-on-billions-in-sales-each-year-to-increase-use-of-telematics-data/

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, *29*(7), 1645–1660. http://doi.org/10.1016/j.future.2013.01.010

Hashem, I. A. T., Yaqoob, I., Badrul Anuar, N., Mokhtar, S., Gani, A., & Ullah Khan, S. (2014). The rise of "Big Data" on cloud computing: Review and open research issues. *Information Systems*, *47*, 98–115. http://doi.org/10.1016/j.is.2014.07.006

Jin, X., Wah, B. W., Cheng, X., & Wang, Y. (2015). Significance and Challenges of Big Data Research. *Big Data Research*, *2*(2), 59–64. http://doi.org/10.1016/j.bdr.2015.01.006

Kambatla, K., Kollias, G., Kumar, V., & Grama, A. (2014). Trends in big data analytics. *Journal of Parallel and Distributed Computing*, *74*(7), 2561–2573. http://doi.org/10.1016/j.jpdc.2014.01.003

Karakostas, B. (2013). A DNS Architecture for the Internet of Things: A Case Study in Transport Logistics. *Procedia Computer Science*, *19*(Ant), 594–601. http://doi.org/10.1016/j.procs.2013.06.079

Landrock, H. (2016). *Industrie 4 . 0 / Internet of Things Vendor Benchmark 2016*.

Le, K. T. (2005). ZigBee SoCs provide cost-effective solutions | EE Times. Retrieved December 17, 2015, from http://www.eetimes.com/document.asp?doc_id=1273396

Lee, J., Lapira, E., Bagheri, B., & Kao, H. (2013). Recent advances and trends in predictive manufacturing systems in big data environment. *Manufacturing Letters*, *1*(1), 38–41. http://doi.org/10.1016/j.mfglet.2013.09.005

Lee, J., Su, Y., & Shen, C. (2007). A Comparative Study of Wireless Protocols : *IECON Proceedings (Industrial Electronics Conference)*, 46–51. http://doi.org/10.1109/IECON.2007.4460126

Leitão, P., Rodrigues, N., Barbosa, J., Turrin, C., & Pagani, A. (2015). Intelligent products: The grace experience. *Control Engineering Practice*, *42*(0), 95–105. http://doi.org/http://dx.doi.org/10.1016/j.conengprac.2015.05.001

Lin, X., & Negenborn, R. R. (2015). Quality-aware Predictive Scheduling of Raw Perishable Material Transports.

Liu, X., & Sun, Y. (2011). Information Flow Management of Vendor-Managed Inventory System in Automobile Parts Inbound Logistics Based on Internet of Things. *Journal of Software*, *6*(7), 1374–1381. http://doi.org/10.4304/jsw.6.7.1374-1380

Mahmood, A., Javaid, N., & Razzaq, S. (2015). A review of wireless communications for smart grid. *Renewable and Sustainable Energy Reviews*, *41*, 248–260. http://doi.org/10.1016/j.rser.2014.08.036

McKinsey & Company. (2011). Big data: The next frontier for innovation, competition, and productivity. *McKinsey Global Institute*, (June), 156. http://doi.org/10.1080/01443610903114527

Miorandi, D., Sicari, S., De Pellegrini, F., & Chlamtac, I. (2012). Internet of things: Vision, applications and research challenges. *Ad Hoc Networks*, *10*(7), 1497–1516. http://doi.org/10.1016/j.adhoc.2012.02.016

Networks, P. M. (n.d.). Private Mobile Networks. Retrieved November 30, 2015, from http://www.privatemobilenetworks.com/

Pang, Z., Chen, Q., Han, W., & Zheng, L. (2015). Value-centric design of the internet-of-things solution for food supply chain: Value creation, sensor portfolio and information fusion. *Information Systems Frontiers*, *17*(2), 289–319. http://doi.org/10.1007/s10796-012-9374-9

Perera, C., Zaslavsky, A., Christen, P., & Georgakopoulos, D. (2014). Context aware computing for the internet of things: A survey. *IEEE Communications Surveys and Tutorials*, *16*(1), 414–454. http://doi.org/10.1109/SURV.2013.042313.00197

Philip Chen, C. L., & Zhang, C.-Y. (2014). Data-intensive applications, challenges, techniques and technologies: A survey on Big Data. *Information Sciences*, *275*, 314–347. http://doi.org/10.1016/j.ins.2014.01.015

Qiuping, W., Shunbing, Z., & Chunquan, D. (2011). Study On Key Technologies Of Internet Of Things Perceiving Mine. *Procedia Engineering*, *26*, 2326–2333. http://doi.org/10.1016/j.proeng.2011.11.2442

Quattrociocchi, W., Caldarelli, G., & Scala, A. (2014). Self-Healing Networks: Redundancy and Structure. *PLoS ONE*, *9*(2), e87986. http://doi.org/10.1371/journal.pone.0087986

Roman, R., Zhou, J., & Lopez, J. (2013). On the features and challenges of security and privacy in distributed internet of things. *Computer Networks*, *57*(10), 2266–2279. http://doi.org/10.1016/j.comnet.2012.12.018

Sample, A. (2015). NFC-WISP : A Sensing and Computationally Enhanced Near-Field RFID Platform, 105–106.

SAP. (2016). Predictive Maintenance | Internet of Things & M2M Technology | SAP. Retrieved January 28, 2016, from http://www.sap.com/pc/tech/internet-of-things/software/predictive-maintenance/index.html

Shelby, Z., & Bormann, C. (2011). *6LoWPAN: The wireless embedded Internet* (Vol. 43). Retrieved from https://books.google.com.ec/books?hl=es&lr=&id=3Nm7ZCxscMQC&oi=fnd&pg=PT9&dq=6lowpan&ots=xp9oJ7-wHM&sig=Wv1_lYHqw_tYxx0R1fEXgUjtluM

Shi, X., Tao, D., & Voß, S. (2011). RFID Technology and its Application to Port-Based Container Logistics. *Journal of Organizational Computing & Electronic Commerce*, *21*(4), 332–347. http://doi.org/10.1080/10919392.2011.614202

Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2014). Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks*, *76*, 146–164. http://doi.org/10.1016/j.comnet.2014.11.008

SigFox. (2014). M2M and IoT redefined through cost effective and energy optimized connectivity. *Whitepaper*, 1–17.

Smith, J. R., Sample, A. P., Powledge, P. S., Roy, S., & Mamishev, A. (2006). A wirelessly-powered platform for sensing and computation. *UbiComp 2006: Ubiquitous Computing*, 495–506. http://doi.org/10.1007/11853565_29

Stankovic, J. A. (2014). Research Directions for the Internet of Things. *Internet of Things Journal, IEEE*, *1*(1), 3–9. http://doi.org/10.1109/JIOT.2014.2312291

Talia, D. (2014). Towards Internet Intelligent Services Based on Cloud Computing and Multi-Agents. In S. Gaglio & G. Lo Re (Eds.), *Advances onto the Internet of Things* (pp. 271–281). Springer International Publishing Switzerland.

Tamburini, D. (2015). True Value: The Industrial Internet of Things Brings Added Returns to Customers. http://doi.org/10.1017/CBO9781107415324.004

Tamura, T., & Masuda, I. (2013). Device connectivity technologies using short-distance wireless

communications. *Fujitsu Scientific and Technical Journal*, *49*(2), 213–219. Retrieved from http://www.scopus.com/inward/record.url?eid=2-s2.0-84874548206&partnerID=tZOtx3y1

TexasInstruments. (2015). 6LoWPAN | Wireless Connectivity | Overview | TI.com. Retrieved November 30, 2015, from http://www.ti.com/lsds/ti/wireless_connectivity/6lowpan/overview.page

Tilley, A. (2015). San Francisco Now Has Its Own Cellular Network Just For The "Internet Of Things" - Forbes. Retrieved December 8, 2015, from http://www.forbes.com/sites/aarontilley/2015/10/27/samsung-backed-sigfox-has-built-a-wireless-network-for-the-internet-of-things-in-san-francisco-plans-coverage-of-10-us-cities-by-early-2016/

Tozlu, S., Senel, M., Mao, W., & Keshavarzian, A. (2012). Wi-Fi enabled sensors for internet of things: A practical approach. *IEEE Communications Magazine*, *50*(6), 134–143. http://doi.org/10.1109/MCOM.2012.6211498

Want, R. (2011). Near Field Communication. *Pervasive Computing, IEEE*, *10(3)*, 4–7. http://doi.org/10.1109/MPRV.2011.55

Witchalls, C. (2013). *The Internet of Things Business Index*. (J. Chambers, Ed.). The Economist Intelligence Unit Ltd.

Xu, L., He, W., & Li, S. (2014). Internet of Things in Industries: A Survey. *IEEE Transactions on Industrial Informatics*, *PP*(99), 1–11. http://doi.org/10.1109/TII.2014.2300753

Xu, X., Chen, T., & Minami, M. (2012). Intelligent fault prediction system based on internet of things. *Computers and Mathematics with Applications*, *64*(5), 833–839. http://doi.org/10.1016/j.camwa.2011.12.049

Yan, B.-N., Lee, T.-S., & Lee, T.-P. (2015). Mapping the intellectual structure of the Internet of Things (IoT) field (2000–2014): a co-word analysis. *Scientometrics*, *105*(2), 1285–1300. http://doi.org/10.1007/s11192-015-1740-1

Zhong, R. Y., Lan, S., Xu, C., Dai, Q., & Huang, G. Q. (2015). Visualization of RFID-enabled shopfloor logistics Big Data in Cloud Manufacturing. *The International Journal of Advanced Manufacturing Technology*. http://doi.org/10.1007/s00170-015-7702-1

Zhong, R. Y., Li, Z., Pang, L. Y., Pan, Y., Qu, T., & Huang, G. Q. (2013). RFID-enabled real-time advanced planning and scheduling shell for production decision making. *International Journal of Computer Integrated Manufacturing*, *26*(7), 649–662. http://doi.org/10.1080/0951192X.2012.749532