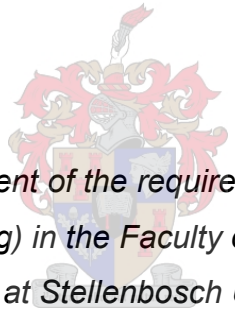
BUSINESS IMPACT, RISKS AND CONTROLS ASSOCIATED WITH THE INTERNET OF THINGS

By

Anja van Niekerk



Thesis presented in partial fulfilment of the requirements for the degree of Master of Commerce (Computer Auditing) in the Faculty of Economic and Management Sciences at Stellenbosch University

Supervisor: Riaan Rudman

March 2017

DECLARATION

By submitting this thesis electronically, I declare that:

- the entirety of the work contained therein is my own, original work,
- I am the sole author thereof (save to the extent explicitly otherwise stated),
- reproduction and publication thereof by Stellenbosch University will not infringe any third party rights, and
- I have not previously in its entirety or in part submitted it for obtaining any qualification.

March 2017

ACKNOWLEDGEMENTS

I would like to thank the following people:

- My husband, Ruan, for all his support, love and motivation.
- My parents, for always believing in me and teaching me that I can do anything I set my mind to.
- My study leader, Riaan, for guiding me through the course and sharing his knowledge.

Abstract

Modern businesses need to keep up with the ever-evolving state of technology to determine how a change in technology will affect their operations. Adopting Internet of Things to operations will assist businesses in achieving the goals set by management and, through data integration, add additional value to information. With the Internet of Things forming a global communication network, data is gathered in real time by sensor technologies embedded in uniquely identifiable virtual and physical objects. This data gathered are integrated and analysed to extract knowledge, in order to provide services like inventory management, customised customer service and e-learning as well as accurate patient records. This integrated information will generate value for businesses by, *inter alia,* improving the quality of information and business operations. Business may be quick to adopt the Internet of Things into their operations because of the promised benefits, without fully understanding its enabling technologies. It is important that businesses acquire knowledge of the impact that these technologies will have on their operations as well as the risks associated with the use of these technologies before they deploy the Internet of Things in their business environment. The purpose of this study was to identify the business impact, risks and controls associated with the Internet of Things and its enabling technologies. Through the understanding of the enabling technologies of Internet of Things, the possible uses and impact on business operations can be identified. With the help of a control framework, the understanding gained on the technologies were used to identify the risks associated with them. The study concludes by formulating internal controls to address the identified risks.

It was found that the core technologies (smart objects, wireless networks and semantic technologies) adopt humanlike characteristics and convert most manual business operations into autonomous operations, leading to increased business productivity, market differentiation, cost reduction and higher-quality information. The identified risks centred on data integrity, privacy and confidentiality, authenticity, unauthorised access, network availability and semantic technology vulnerabilities. A multi-layered approach of technical and non-technical internal controls were formulated to mitigate the identified risks to an acceptable level. The findings will assist information technology specialists and executive management of industries to identify the risks

associated with the implementation of Internet of Things in operations, mitigate the risks to an acceptable level through controls as well as assist them to determine the possible uses and its impact on operations.

Opsomming

Moderne ondernemings moet tred hou met die voortdurende ontwikkeling van tegnologie om te bepaal hoe ’n verandering in tegnologie hulle bedrywighede sal beïnvloed. Inkorporering van Internet van Dinge in bedrywighede sal besighede help om die doelwitte wat deur bestuur gestel is te bereik en, deur data integrasie, additionele waarde te voeg tot inligting. Met Internet van Dinge wat ’n globale kommunikasienetwerk vorm, word data in regte tyd versamel deur sensortegnologieë wat ingebed is in unieke identifiseerbare virtuele en fisiese voorwerpe. Hierdie versamelde data word geïntegreer en ontleed om kennis te onttrek om sodoende dienste te lewer, soos voorraadbestuur, pasgemaakte kliëntediens en e-leer sowel as akkurate pasiënt rekords. Hierdie geïntegreerde inligting sal waarde genereer vir ondernemings deur, *inter alia,* die gehalte van inligting en sakebedrywighede te verbeter. Ondernemings mag vinnig Internet van Dinge in hulle bedrywighede inkorporeer as gevolg van die beloofde voordele, sonder om die instaatstellende tegnologieë ten volle te verstaan. Dit is belangrik dat ondernemings kennis inwin oor die impak wat hierdie tegnologieë sal hê op hulle bedrywighede sowel as die risiko’s wat geassosieer word met die gebruik van hierdie tegnologieë voordat Internet van Dinge in hulle sakeomgewings ontplooi word. Die doel van hierdie studie was om die besigheidsimpak, risko’s en kontroles wat geassosieer word met Internet van Dinge en die instaatstellende tegnologieë te identifiseer. Deur die instaatstellende tegnologieë van Internet van Dinge te verstaan, kan die moontlike gebruike en impak daarvan op sakebedrywighede geïdentifiseer word. Met behulp van ’n kontroleraamwerk, is die begrip van die tegnologieë gebruik om die risiko’s wat geassosieer word met hulle te identifiseer. Die studie sluit af met die formulering van interne kontroles om die geïdentifiseerde risko’s aan te spreek.

Daar is gevind dat die kerntegnologiekomponente (slim voorwerpe, draadlose netwerke en semantiese tegnologieë) menslike eienskappe aanneem en die meeste handsakebedrywighede omskakel na outonome bedrywighede, wat lei tot verhoogte sakeproduktiwiteit, markdifferensiasie, kostebesparing en hoërgehalte-inligting. Die geïdentifiseerde risiko’s is toegespits op data integriteit, -privaatheid en -vertroulikheid, egtheid, ongemagtigde toegang, netwerkbeskikbaarheid en semantiese tegnologiekwesbaarhede. ’n Multilaagbenadering van tegniese en nie-

tegniese interne kontroles is geformuleer, om sodoende die geïdentifiseerde risiko's tot 'n aanvaarbare vlak te versag. Die bevindinge sal inligtingstegnologie-spesialiste en uitvoerende bestuur van industrieë help om die risiko's verbonde aan implementering van Internet van Dinge te identifiseer, risko's te versag tot 'n aanvaarbare vlak met kontroles sowel as hulle te help om moontlike gebruike en hulle impak op bedrywighede vas te stel.

TABLE OF CONTENTS

LIST OF FIGURES, TABLES AND APPENDICES

Figures

Tables

Appendices

CHAPTER 1:
INTRODUCTION, RESEARCH OBJECTIVE, MOTIVATION, SCOPE LIMITATIONS AND METHODOLOGY

1.1 INTRODUCTION

Information technology (IT) and the Internet are classified by organisations as business tools that generate business value by increasing productivity, providing market differentiation, reducing costs or providing higher-quality information (Vermesan & Friess, 2014:30, 41; Melville, Kraemer & Gurbaxani, 2004:286). The Internet has become the main source of communication worldwide, with an estimated usage growth rate of 741% over the last 14 years (Internet World Stats, 2014; Jara, Ladid & Skarmeta, 2013:103). With the increasing growth rate of Internet usage, the enabling technologies and protocols supporting the infrastructure of the Internet are continuously evolving (Farooq, Waseem, Mazhar, Khairi & Kamal, 2015:1). Communication interactions can be classified as human to human or human to machine, but the Internet of Things will bring forth machine to machine communication interactions in the future (Farooq *et al.*, 2015:1). More devices are continually being connected to the Internet. This forms the basis of Internet of Things, as Internet of Things creates an integrated global information network where the key enablers, namely smart objects, will become active participants in a network environment (Sundmaeker, Guillemin, Woelfflé & Friess, 2010:43). Smart objects will be able to uniquely identify objects and gather data on their surrounding environment through sensors (López, Ranasinghe, Harrison & McFarlane, 2012:293–295). Gathered data, communicated through wireless networks, will be processed and integrated in order to extract knowledge to provide services or command objects (Sundmaeker *et al.*, 2010:43; Zorzi, Gluhak, Lange & Bassi, 2010:47).

The evolution of the Internet of Things will impact business operations and bring forth new business opportunities by integrating relevant information from various environments to improve the quality of business operations (Atzori, Iera & Morabito, 2010:2793). Organisations will generate value through integrated data and recognise information as an asset that needs to be managed and protected (Tarrant, Hitchcock & Carr, 2011:165–167).

Despite the new opportunities and advances that the Internet of Things promises, businesses must be prepared and gain knowledge with regard to the impact of Internet of Things on business operations as well as ways to identify risks arising from its use (Jara, Varakliotis, Skarmeta & Kirstein, 2014:3; Melville *et al.*, 2004:286). The implementation of Internet of Things by businesses will largely rely on the protection of the information asset (Farooq *et al.,* 2015:5). Data and information will be exposed to attacks mainly due to the limited capabilities of smart objects, unprotected wireless networks as well as unauthorised access to data and information (Nurse, Erola, Agrafiotis, Goldsmith & Creese, 2015:6; Atzori *et al*., 2010:2801; Wang, Attebury & Ramamurthy, 2006:2). The amount of information gathered and processed by a business will impact on the level of protection and control applied over it (Middleton, Halbert & Coyle, n.d.). Businesses should consider how to address these risks through the implementation of control procedures.

1.2 RESEARCH PROBLEM AND MOTIVATION

IT specialists and executive management of businesses are eager to adopt Internet of Things in their operations due to the promised benefits of cost reduction, market differentiation, increased business productivity and higher quality business information (Vermesan & Friess, 2014:30, 41). By adopting Internet of Things too quickly in business operations, the enabling technologies of Internet of Things won't fully be understood. IT specialists and executive management of businesses need to gain knowledge on the enabling technologies of Internet of Things in order to understand how these technologies can be applied in business operations as well as its impact on business industries.

Businesses rely on timely, accurate and valid information to make strategic business decisions and recognise that information must be protected and kept confidential. Information gathered and processed by Internet of Things are vulnerable to attacks due to the variety of technologies used by it on a large scale in a network (Nurse *et al.*, 2015:6). Businesses will be exposed to new unknown risks when Internet of Things are deployed in operations. These risks are directly linked to a lack of knowledge of the enabling technologies of Internet of Things. Before Internet of Things can be deployed in a business, IT specialists and executive management must be made aware of the risks, associated with the enabling technologies, on their business

information and operations. It is the responsibility of management to mitigate the risks associated with the enabling technologies of Internet of Things to an acceptable level through technical and non-technical control measures as well as a policy component. The volume of business information will impact the level of control needed and to achieve effective control, a best-practice framework is required, which takes the enabling technologies of the Internet of Things into account, to identify and address the risks.

1.3 RESEARCH OBJECTIVE

Before IT specialists and executive management can implement Internet of Things in a business environment, they should be informed of the implications it will have on business operations. The study aims to provide information to businesses on the impact of Internet of Things on current business operations, risks associated with the implementation of Internet of Things as well as formulate controls to address these risks.

It is impossible to define a universal business model for the Internet of Things due the diversity of its applications as well as the different driving forces behind them (Vermesan & Friess, 2014:41). Even though a one-size-fits-all business model cannot be applied to businesses, the adoption of Internet of Things by businesses will bring them economic advantages as well as improve their quality of business operations (Atzori *et al.*, 2010:2793). Through the identification and understanding of the architecture and enabling technologies of the Internet of Things, the objectives of this study were to:

1. identify possible applications of Internet of Things in business operations; and
2. identify the impact of these applications on current business operations or the creation of new business opportunities in specific business industries.

Implementing Internet of Things in businesses will lead to them being exposed to new unidentified risks. This is due to the Internet of Things being a new, poorly understood technology. Through the understanding gained of the architecture and enabling technologies of the Internet of Things, the study further aimed to:

1. identify the risks related to the architecture and enabling technologies of the Internet of Things; and

2. formulate appropriate internal controls to mitigate the risks to an acceptable level in order to govern a business in using Internet of Things appropriately.

1.4 SCOPE LIMITATIONS

The focus of this study was to identify and define the enabling technologies of the Internet of Things in detail in order to formulate an architecture for Internet of Things. The purpose of this research was not an in-depth technical study of the design, development or programming of the enabling technologies, but rather on following a structured approach to explain the process of identifying an object, gathering and processing data as well as transmitting information over networks using Internet protocols.

The investigation further focused on identifying risks specifically linked to the identified enabling technologies of the Internet of Things and did not propose to create a comprehensive list of pre-existing risks associated with the Internet, its infrastructure and enabling technologies. Therefore, by only taking risks associated with the enabling technologies of the Internet of Things into account, specific internal controls were formulated in line with the identified risks. The internal controls were focussed on the protection of gathered and processed information as well as on ensuring continuous network availability.

Although business strategies differ between organisations and industries, there are certain general business operations that occur in all of them. The research further investigated possible applications, identified through the enabling technologies of the Internet of Things, in business operations. The impact of these possible applications on business industries was investigated. The focus of the impact study was only on business operations in specific business industries, and the study does not propose an exhaustive list of all possible business industries.

1.5 METHODOLOGY

In order to accumulate knowledge, a systematic review of relevant historic literature must be undertaken to create a foundation for advancing research in information systems. The information systems field is critiqued on having limited theoretical

studies, as the compilation of a review in this field is complex (Webster & Watson, 2002:1–2).

A non-empirical, qualitative study was performed to address the research problem. An extensive literature review was conducted by reviewing popular press articles, electronic sources, accredited articles in local and international journals, white papers, theses and books. In order to develop an effective literature review, the three-stage framework, shown in Figure 1.1 below, following a systematic data-processing approach, was continuously followed throughout the research, as recommended by Levy and Ellis (2006:181–204).

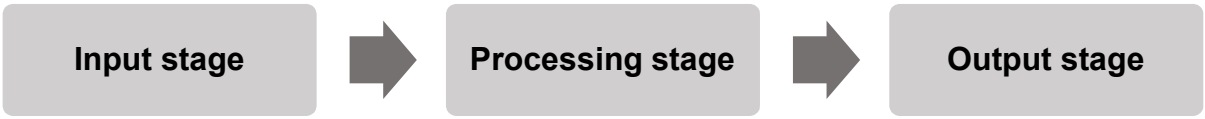


Figure 1.1: Three-stage framework for the study's literature review

(Source: Adapted from Levy and Ellis)

1. **Input stage:** During the input stage, relevant and applicable data were gathered from quality literature databases (such as *Elsevier®/ScienceDirect®*, *IEEE, Google Scholar* and *Emerald*) with initial search terms selected to include broad-based results, which included, *inter alia,* 'Internet of Things', 'Technologies driving Internet of Things', 'Impact of Internet of Things on business industries', 'COBIT 5' and 'IT governance'. The search output was 440 000 articles and website entries.
2. **Processing stage:** The data gathered during the input stage were processed according to a sequential process, where a given process serves as a foundation for the following process.
    - *Knowledge and comprehension process:* During this process, the original selection terms were reduced by selecting readings with similar issues so that relevant information was identified and extracted. The similarities in the selection included the following issues, *inter alia*: 'Internet of things impact on business industries', 'smart objects', 'communication networks', 'communication protocols', 'semantic web', 'risks associated with Internet of Things' and 'COBIT 5'. The initial search output of 440 000 articles and website entries was narrowed down to 223.

- *Application and analysis process:* An in-depth reading of the narrowed-down articles and websites identified applicable information that enabled the researcher to develop a concept of the Internet of Things, its enabling technologies, its possible applications and its impact on business operations in specific industries, risks associated with them and a possible control framework to mitigate risks to an acceptable level. The different concepts were annotated within 143 readings.
- *Synthesis and evaluation process:* The recorded annotations and concepts identified in the previous processes were assembled by the researcher to create her own integrated and generalised information in a supporting and explaining document.

3. **Output stage:** The output stage is the final argumentative literature review with a logical structure produced by the researcher, providing the reader with what the researcher did during the input stage and what was learned during the processing stage.

The stages described above assisted the researcher to gain a better understanding of and expand on, *inter alia,* the following topics:

- Definition of the Internet of Things
- Architecture and enabling technologies of the Internet of Things
- Possible uses and impact of the Internet of Things on business industries
- Risks associated with enabling technologies of the Internet of Things
- IT governance
- Control frameworks: COBIT 5.

The literature review formed the basis of the initial findings of the research. Using this as a basis; the following structured steps were used to address the research problem:

1. **Define the Internet of Things and its enabling technologies.** In chapter 2, a definition of Internet of Things had to be formalised, and its enabling technologies had to be identified and defined in order to formulate an architectural framework in chapter 3. Available definitions of the Internet of Things are inconsistent, as only limited research on the topic has been conducted. The aim was to create a definition from generally accepted literature.

2. **Identify the impact that the enabling technologies of Internet of Things will have on business operations of business industries.** In chapter 4 possible applications of Internet of Things were derived from gaining an understanding of the enabling technologies of Internet of Things. The impact of these possible applications of Internet of Things on business operations will influence current business operations or create new business opportunities.
3. **Perform an in-depth analysis of the COBIT 5 control framework and its processes.** By taking the knowledge gained on the enabling technologies of Internet of Things into account, the control framework and processes of COBIT 5 were evaluated in detail. Through the evaluation of COBIT 5, the applicable processes needed to govern Internet of Things were identified. The applicable processes are set out in appendix A.
4. **Identify risks associated with Internet of Things.** In chapter 5, the relevant processes of the COBIT 5 framework were used to identify risks with regards to each process and the related enabling technologies of Internet of Things (appendix A). A risk-technology matrix was prepared, linking the enabling technologies to their associated risks.
5. **Formulate internal controls to mitigate risks.** In chapter 6 safeguards and controls, based on the risks identified in chapter 5, were formulated to mitigate Internet of Things risks. A risk-control matrix was compiled, linking risks identified to the controls that need be implemented in order to mitigate risks to an acceptable level.

This methodology assisted in gaining a better understanding of the Internet of Things and its enabling technologies in order to identify its possible applications and their impact on business operations. The methodology also assisted in identifying the risks associated with the enabling technologies of Internet of Things and formulating internal controls, by using a control framework, to mitigate identified risks to an acceptable level.

CHAPTER 2:
LITERATURE REVIEW

2.1 INTRODUCTION

Internet of Things is a new technology that consists of many different technologies (Zhang, Sun & Cheng, 2012:294). It is being called the third wave of the IT world, after the computer and the Internet, and will establish humanlike device-to-device communication (Farooq *et al.*, 2015:1; Lui & Zhou, 2012:197). The different technologies of device-to-device communication will have a significant impact on current business operations and give rise to new business opportunities. For a business to realise these opportunities, it should obtain a clear understanding of the Internet of Things and its enabling technologies. Most of the risks associated with the Internet of Things are due to a lack of knowledge of these new technologies.

2.2 HISTORIC REVIEW AND BACKGROUND

The concept of Internet of Things was first established in 1982 when a modified Coke machine was connected to the Internet, which reported the temperature and type of drinks in the machine. In 1991, Mark Weiser had a vision of the Internet of Things in the form of ubiquitous computing (Farooq *et al.*, 2015:1). Bill Joy elaborated on this idea in his taxonomy of the Internet about device-to-device communication in 1999, but the term 'Internet of Things' was first used in 1999 by Kevin Ashton. The concept was made popular over the years by the Auto-IT Centre (Farooq *et al.*, 2015:1; Lui & Zhou, 2012:197; Zhang *et al.*, 2012:294). At this stage, the Internet of Things was only based on wireless sensor networks and radio-frequency identification (RFID) technology to describe a system of interconnected devices (Farooq *et al.*, 2015:1; Zhang, 2011:4109). In 2005, the International Telecommunication Union released a report formally proposing the concept of Internet of Things at the World Summit on the Information Society in Tunis (Lui & Zhou, 2012:197; Zhang, 2011:4109). The report expanded the definition, scope and coverage of the Internet of Things to include a ubiquitous communication network, where objects are embedded with RFID, sensors, nanotechnology and intelligent technology in order to exchange information (Zhang, 2011:4109). Advances made in barcodes, smart phones, social networks and cloud computing technologies contributed to the further development of a supporting network for Internet of Things (Da Xu, He & Li, 2014:2234).

Although there is no standard definition for Internet of Things to date, by 2009, a general understanding of its basic theory, technologies and applications could be found; however, the literature mainly focused on the technical components of Internet of Things (Lui & Zhou, 2012:197; Zhang, 2011:4109). At this point, a broad description of Internet of Things explains that by integrating RFID, sensors and communication technologies, physical objects and devices can interact and communicate with each other through the Internet in order to reach common goals (Da Xu *et al.*, 2014:2233).

The interest in using the enabling technologies of Internet of Things grew in various business industries due to their promise of providing high-quality services to its end users (Da Xu *et al.*, 2014:2233–2234). Even though only a few applications are currently available in the market, the latest research on Internet of Things focuses on the potential advantages that the development of Internet of Things applications will bring to its end users as well as possible uses to help improve the quality of business operations (Farooq *et al.*, 2015:4; Atzori *et al.*, 2010:2793).

The success of Internet of Things will depend on the standardisation of the technical design of information exchange, processing and communications between objects in order to achieve a global interoperable, compatible, reliable and effective functioning (Da Xu *et al.*, 2014:2233). Many organisations are involved in the development of Internet of Things technologies and it is necessary to coordinate and govern these developments through widely accepted standards (Da Xu *et al.*, 2014:2234). With no framework in place to identify and control risks arising from the use of Internet of Things, current studies show a governance problem for businesses adopting the Internet of Things and a lack of confidence with regard to the security and privacy of their data (Farooq *et al.*, 2015:5; The Security Ledger, 2013).

A study that focuses on the possible uses of Internet of Things and its impact on business operations in industries, identifying risks that arise from the use of the enabling technologies of Internet of Things as well as the creation of a comprehensive control framework to mitigate these risks, has as yet not been conducted; hence the gap identified by the researcher. However, before further reporting on this study, the concepts of Internet of Things and governance need to be understood.

2.3 CONCEPT OF THE INTERNET OF THINGS

The concept of the Internet of Things has been viewed from several different perspectives in the research society, leading to various definitions. The motivation for the unclear definition originates from the fact that Internet of Things is composed of two concepts, namely 'Internet' and 'Things'. When these two concepts are combined, it introduces a new innovation in the IT environment, the third concept of semantics (Bandyopadhyay & Sen, 2011:50–52). In order to define the Internet of Things, each of the three concepts needs to be evaluated to formulate a comprehensive definition of Internet of Things.

2.3.1 Concept of 'Things'

The concept of 'Things' in an Internet of Things environment places its focus on the integration of virtual and physical generic objects in a global IT infrastructure (Bandyopadhyay & Sen, 2011:50–51). Each object is issued a unique identification number in order to specifically identify it, as well as to assist in distinguishing between different objects. This helps with improving the traceability of an object in the global IT infrastructure (Zhang *et al.*, 2012:295; Bandyopadhyay & Sen, 2011:51; Zhang, 2011:4111). The information source of the Internet of Things is the data that are identified and collected in real time from objects through various sensor technologies embedded in the objects, thereby improving the objects' awareness of their status and current location (Lui & Zhou, 2012:198; Zhang *et al.*, 2012:295; Zhang, 2011:4111).

Objects will communicate with one another as well as the Internet of Things infrastructure in order to exchange data between the real physical world and the digital virtual world by making use of the connectivity and communication technologies of the 'Internet' concept (Lui & Zhou, 2012:198; Bandyopadhyay & Sen, 2011:51).

2.3.2 Concept of 'Internet'

The concept of 'Internet' focuses on the various types of network access technologies available to objects in order for them to connect, communicate and exchange collected data with one another as well as the Internet of Things infrastructure (Lui & Zhou, 2012:199; Zhang *et al.*, 2012:295; Bandyopadhyay & Sen, 2011:51). Existing mobile, wired and wireless, Internet, private and other networks are used as mediums to transmit data (Lui & Zhou, 2012:199; Zhang *et al.*, 2012:295; Zhang, 2011:4110). Each

object will be assigned a unique Internet Protocol (IP) address, which refers to the address of the object within a communication network (Al-Fuqaha, Guizani, Mohammadi, Aledhari & Ayyash, 2015:2350; Sousa & Oz, 2015:196). The 'Internet' concept is built on the IP at its core and establishes an efficient, interconnected and reliable communication infrastructure that integrates information resources into an intelligent network for objects to connect, communicate and exchange collected data with one another as well as the Internet of Things infrastructure (Lui & Zhou, 2012:199; Zhang *et al.*, 2012:295).

With the combination of the 'Things' and 'Internet' concepts, a global network of uniquely addressed and identifiable objects is formed. These objects collect and exchange a great amount of data based on standard communication protocols, and these data need to be managed, controlled and analysed by the 'semantic' concept (Al-Fuqaha *et al.*, 2015:2352; Lui & Zhou, 2012:198; Bandyopadhyay & Sen, 2011:50).

2.3.3 Concept of 'Semantics'

The concept of semantics focuses on an infrastructure that can perform complex actions for its users. It forms a web of machine-understandable and interoperable services, where intelligent agents can discover data, execute actions, integrate information and create knowledge automatically (Ghaleb, Daoud, Hasna, ALJa'am, El-Seoud & El-Sofany, 2006:63). Intelligent agents are computer systems that consist of specialised programming and computer architecture that are programmed to function in a similar way as people when browsing the Web (Bruwer & Rudman, 2015:1044).

The semantic infrastructure will be able to manage and control the vast amount of data and objects in the communication network in real time (Lui & Zhou, 2012:199; Zhang *et al.*, 2012:295). Furthermore, semantic technologies will have the capability to reorganise, filter and integrate gathered data in order to analyse and reason over them in order to extract knowledge from them to provide a given service or command an object (Al-Fuqaha *et al.*, 2015:2352; Zhang *et al.*, 2012:295; Bandyopadhyay & Sen, 2011:51).

2.3.4 Definition of the Internet of Things

Da Xu *et al.* (2014:2233) define the Internet of Things as "*a dynamic global network infrastructure with self-configuring capabilities, based on standard and interoperable communication protocols, where physical and virtual 'Things' have identities, physical attributes and virtual personalities and use intelligent interfaces, and are seamlessly integrated into the information network*". Asghar, Negi and Mohammadzadeh (2015:427) envision the Internet of Things as an "*Internet with billions of objects connected to it, that generates large amounts of data gathered by sensors which need to be analysed, interpreted and utilised*". Kraijak and Tuwanut (2015:26) associate the Internet of Things with "*real-world objects becoming part of the Internet, where every object is uniquely identified, and accessible to the network, its position and status is known, where numerous services and intelligence are added to effectively expand the Internet, seamlessly combining the digital and physical world*".

After taking the above definitions into account as well as the discussed three concepts of Internet of Things, the following definition for Internet of Things can be formulated: The Internet of Things is a global communication network containing various sensor technologies embedded in uniquely identifiable virtual and physical generic objects that gather real-time data from their environment, which results in data being integrated and analysed to extract knowledge from them to provide a service, command objects as well as exchange information with other objects.

The illustration in Figure 2.1 below shows how the three concepts that define the Internet of Things interlink.

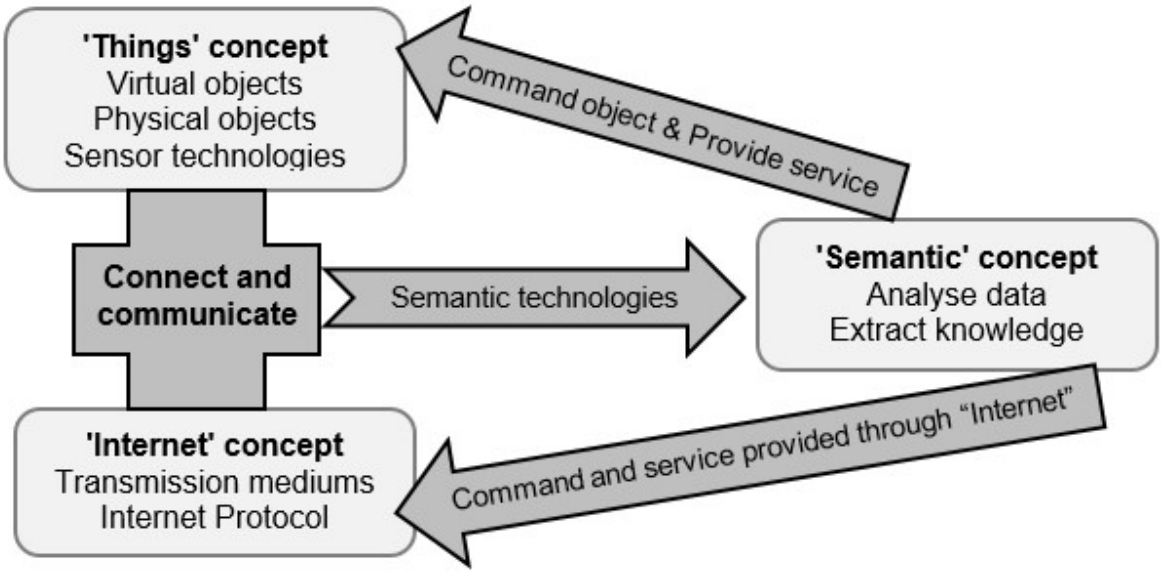


Figure 2.1: Interlinking between the concepts underlying Internet of Things

(Source: Author's own)

Understanding the underlying concepts of Internet of Things is only the start; the Internet of Things needs to be governed appropriately.

2.4 CORPORATE GOVERNANCE

Management aims to align business objectives and strategies with planning, developing, operating and monitoring activities. Business strategies are realised through governance by assessing stakeholder prospects and needs, establishing guidance through regulation and prioritisation, and monitoring achievement, compliance and progress against predetermined guidelines (ISACA, 2012a). Due to a series of managerial misconduct, negligence cases and corporate fraud, corporate governance has taken precedence over the last two decades, emphasising it to ensure that a business reaches its strategic goals and controls its risks (Krechovská & Procházková, 2014:1145; Zalewska, 2014:1).

Corporate governance consists of policies, procedures and processes that are used to direct and control a business (Krechovská & Procházková, 2014:1145; Zalewska, 2014:2). The corporate governance objective of fairness, accountability, responsibility and transparency should be included in these policies, procedures and processes in

order to achieve effective governance over a business (IODSA, 2009:6). Corporate governance stipulates the rules and procedures for the decision-making process and takes the link between good governance and compliance with laws and regulations into account (Krechovská & Procházková, 2014:1145; IODSA, 2009:6).

Corporate governance includes the activities of the board as well as the distribution of responsibilities and rights between the board, shareholders, managers and other stakeholders (Krechovská & Procházková, 2014:1145). The relationship between the board and managers, shareholders, auditors, regulators and other stakeholders should be managed proactively, taking their interests and expectations into account during decision-making processes (Krechovská & Procházková, 2014:1145; IODSA, 2009:47).

Corporate governance structures should be able to adapt to changes in the business environment as well as the growing impact that IT has on business operations. The King Code of Governance for South Africa (2009) (King III) explains why IT should be addressed as a corporate governance responsibility (Posthumus & Von Solms, 2004:643). King III argues that in the past, IT was only used as an enabler by a business to meet its strategic goals, but has now become a pervasive and integral part of a business's fundamental operations, thereby becoming a strategic asset that requires governance (IODSA, 2009:14; Posthumus & Von Solms, 2004:644).

2.5 IT GOVERNANCE

For a business to create higher values for all stakeholders and remain successful, it has to evolve with the ever-changing business environment and the process of globalisation, as well as keep up with new developments and trends in IT (Krechovská & Procházková, 2014:1145). With the importance of corporate governance emphasised in recent years, the vital role that IT plays in improving corporate governance practices has been recognised with the automation of critical business processes and the board relying on decision-making information generated by IT systems (National Computing Centre, 2005:4). IT governance forms part of corporate governance as a whole, but has its own specific focus on the strategic alignment of IT with business objectives through the development and maintenance of effective, accountable and transparent IT control and management in order to maximise

business value as well as control and mitigate IT-related risks (Brisebois, Boyd & Shadid, 2007:1–2; Hardy, 2006:56; Webb, Pollard & Ridley, 2006:7; National Computing Centre, 2005:5).

IT has become an integral and pervasive part in business operations, where inadequate management of IT can lead to significant financial loss and legal risks and negatively impact the business's performance and competitiveness as a whole (IODSA, 2009:15; Webb *et al.*, 2006:3; National Computing Centre, 2005:4). It is the responsibility of the board of directors and executive management to effectively manage IT resources and risks through the application, development and implementation of IT structures, frameworks, processes, procedures and policies, thereby enabling the business to measure, monitor and evaluate the IT resources and risks against predefined factors, criteria or benchmarks (Hardy, 2006:56; Webb *et al.*, 2006:4). Furthermore, the responsibility rests with the board to ensure that IT is governed according to the following five objectives of IT governance (IODSA, 2009:36; Brisebois *et al.*, 2007:4–5; Hardy, 2006:56–57; National Computing Centre, 2005:6):

- **Strategic alignment:** Maximising the use of available IT resources to ensure that IT and business strategies are aligned as well as balancing IT investments between systems that support the current business as is and those that help the business expand
- **Value delivery:** Investing in an IT infrastructure that is designed to maximise business value, achieve business expansion, increase overall revenue, improve customer satisfaction and gain competitive advantage
- **Risk management:** A risk-management policy and plan, embedded in the responsibilities of the board, to adequately identify, manage, assess and address significant risks linked to IT investments
- **Performance management:** Provides accurate, timely and relevant information regarding the achievement of identified IT investment objectives by measuring IT's performance to its contribution to business value in order to identify which goals have been reached and which shortfalls needs to be addressed

- **Resource management:** Ensures that IT has sufficient, competent and relevant IT resources, such as people, infrastructure and information, to support current and future business expectations.

In order to meet the stated objectives of IT governance, the board needs to commit to the continuous management and control of IT, taking into account the benefits that will be gained through implementing IT governance principles as well as the risks associated with not implementing them.

2.5.1 Benefits of implementing IT governance principles

The National Computing Centre (2005:6–7) identified the following main benefits that arise from IT governance principles, which can also be used as a benchmark to subsequently monitor the success thereof:

- Strategic alignment between IT and business objectives to improve stakeholder returns and create competitive advantage
- Greater external compliance with legal and regulatory requirements
- Improved transparency and understanding of overall IT investments and processes
- Definition and clarification of decision-making accountabilities of IT resource users
- Positioning of IT as a business partner to realise opportunities and facilitate new ventures with other businesses as well as enhance relationships with current partners.

2.5.2 Risks associated with not implementing IT governance principles

According to IODSA (2009:15, 40), if IT governance principles are not implemented, it could lead to the following risks:

- Operational risks, where the confidentiality, reliability and authenticity of information is threatened
- Questioning of the assurance given that the IT system is functioning correctly and is beneficial to the business
- Unauthorised access, use and changes to the information system, which impair the integrity of the system

- A going-concern risk during failure or disruption of the IT system if no disaster-recovery plan is in place.

With the Internet of Things entering the business environment, additional IT, regulatory and business risks will arise, which need to be identified and governed through corporate governance structures implemented by a business. A control framework needs to be selected and implemented by the board that is tailored to the specifications of Internet of Things technologies deployed by the business.

2.6 CONTROL FRAMEWORKS

Management implements best practices, critical success factors and performance drivers into business goals in order to gain a competitive advantage in the market. Businesses then use a structured framework to assess their performance and identify areas where improvements need to be made (Guldentops, 2002:115–116). Structured IT control frameworks are designed to align the best practices, critical success factors and performance drivers of a business with its use of IT, which in turn promotes efficient and effective IT governance (Ridley, Young & Carroll, 2004:1). Businesses will be exposed to new risks when implementing the Internet of Things and in order to comply with regulatory governance, businesses must implement a control framework to assist the board in governing the technologies of Internet of Things as well as to address the risks associated with them (IODSA, 2009:39).

According to Nicho and Fahkry (2011:55–59), Control Objectives for Information and Related Technology (COBIT), IT Information Library (ITIL) and ISO 27002 are the most applicable and widely recognised best-practice IT control frameworks or standards used by businesses to maintain, govern, protect and manage their IT services. As per their study, each of the above-mentioned frameworks or standards focuses on a different area of governance and can shortly be described as follows:

- **COBIT:** COBIT is a benchmark governance and control framework, with its focus on the complete lifecycle of IT investments and resources. It consists of a set of process, practice and control guidelines for IT auditing.

- **ITIL:** ITIL is a framework that enables managers to define strategies, plans and processes to assist them in facilitating the delivery and support of effective management and control of IT services.
- **ISO 27002:** ISO 27002 is a standard that establishes guidelines and general principles to address security issues in order to mitigate risks. It focuses on initiating, implementing, maintaining and improving operational, application, computing platform, network and physical security with regard to information within a business.

The discussed three frameworks and standards were each considered as a potential basis to use to identify and control risks arising from the adoption of Internet of Things by a business. With ISO 27002 only focusing on security controls associated with information and ITIL focusing on service delivery, COBIT was selected as the most appropriate IT governance framework to identify and control risks relating to the Internet of Things, as it covers the entire lifecycle of information systems. COBIT combines IT security, IT audit and IT assurance in a governance framework, with the processes of ITIL and ISO 27002 stated as broad controls in COBIT (Nicho & Fahkry, 2011:59).

2.6.1 An overview of COBIT

COBIT offers a worldwide and generally recognised IT control framework that enables diverse organisations to implement a structure throughout the organisation to govern IT (Guldentops, 2002:115–116).

COBIT is built on the foundation that IT supplies the business with the information it needs to achieve its goals and provides comprehensive guidance to management with regard to the following (Hardy, 2006:59–60; Ridley *et al.*, 2004:1–2; Guldentops, 2002:115–116):

- Helps to balance the organisation's IT risks against its investment in IT controls
- Assists in bridging the gaps between business risks
- Provides basic principles to create IT value
- Addresses IT control needs
- Provides assistance in technical issues.

COBIT is the IT control framework most appropriate to assist a business in aligning its IT use with its business goals, as it highlights the business need that is satisfied by each control objective (Ridley *et al.*, 2004:1). ISACA (2012a) identified the five principles on which COBIT is based as follows:

- **Meeting stakeholder needs:** Stakeholder needs are associated with the goals of the organisation, which in turn are converted into executable IT-related goals.
- **Covering the enterprise end to end:** COBIT focuses on seamlessly integrating IT governance into the corporate governance structure of the entire organisation.
- **Applying a single integrated framework:** COBIT provides an overarching simple framework that aligns and integrates effectively with other relevant standards and frameworks.
- **Enabling a holistic approach:** In order to achieve a maximum effective and efficient governance framework, IT-related goals must divide the IT governance enablers into categories.
- **Separating governance from management:** There is a clear difference between governance and management, but to reach an efficient and effective governance system, interaction between the two is required.

IT governance and management are divided into five domains in the COBIT framework. Each of the five domains contains processes that support the business in achieving its control objectives (ISACA, 2012b). The five domains are as follows:

1. **Evaluate, direct and monitor (five processes):** This domain ensures that a structured approach is followed to determine whether the business's objectives and strategies are aligned with its IT-related decisions, that IT processes are monitored effectively and that there is compliance with governance, legal and regulatory requirements in order for the business to achieve its goals;
2. **Align, plan and organise (thirteen processes):** This domain ensures that a management approach is followed to enable the business to effectively manage information and to guarantee that IT resources are used and infrastructure is developed to achieve governance objectives.
3. **Build, acquire and implement (ten processes):** This domain ensures alignment between IT investments and business strategies by identifying, developing,

acquiring and implementing IT resources. This includes the maintenance and controlling of IT investment modifications.

4. **Deliver, service and support (six processes):** This domain ensures the delivery of the actual planned IT services, which include day-to-day operations, security and continuity management as well as supporting its users.
5. **Monitor, evaluate and assess (three processes):** This domain ensures the monitoring of processes and evaluating their performance against pre-determined business and IT processing goals. Any fluctuations between performance and goals are investigated in a systematic and timely manner.

Each of the above-mentioned five domains will help a business in implementing the controls needed to mitigate the identified risks associated with the adoption of any technology.

2.6.2 Benefits of implementing COBIT

Radhakrishnan (2015:1–2), Oliver and Lainhart (20011:1) and Rudman (2008:22–24) summarised the following benefits of the adoption of COBIT as an IT control framework:

- COBIT improves the alignment of business objectives with IT processes and controls.
- The framework has the ability to meet local and international regulatory and compliance requirements.
- The framework is adaptable, meaning it can be applied to any size business or industry. It is the responsibility of the business to apply only the applicable processes of the domains.
- COBIT serves as a principle framework that can integrate with other internationally accepted control frameworks, models and standards to provide a more technical and comprehensive guidance framework.

2.6.3 Limitations of COBIT

Radhakrishnan (2015:1–2) and Rudman (2008:22–24) underline the following limitations to take into account when adopting COBIT as an IT control framework:

- The framework is complex and written at a high level and lacks detail on how control processes should be implemented.
- Additional focus should be placed on IT security, as COBIT does not provide strong security guidelines.
- Although COBIT can be applied to any size business, it is more suited to larger businesses due to it being resource-intensive in terms of time, money, paper and human resources.
- The framework must be adapted to the specific requirements of the business and lacks guidance on how to execute such adaptation.

2.7 CONCLUSION

Insight gained from literature on the concept and definition of Internet of Things was used to formulate an architecture for Internet of Things as well as to understand its underlying technologies. The risks that arise from this new technology can be mitigated by using a relevant control framework, such as COBIT, to govern the IT-related risks in such a manner that it meets the objectives of a business.

CHAPTER 3:
ARCHITECTURE AND ENABLING TECHNOLOGIES OF THE INTERNET OF THINGS

3.1 INTRODUCTION

According to Farooq *et al.* (2015:2), by 2020 more than 25 billion objects are expected to be connected to the Internet, which led to the conclusion that the existing Internet architecture will not be able to accommodate a network as big as the Internet of Things. Their study proposed a new six-layered architecture that will be able to support existing network applications as well as Internet of Things. The architecture is based on a network hierarchical structure, where the output of the previous layer becomes the input to the following layer. This architecture will be used to identify and categorise the enabling technologies of Internet of Things.

Figure 3.1 below illustrates the proposed six-layered architecture with the categorised enabling technologies of Internet of Things. The layers are discussed according to the following section numbers.

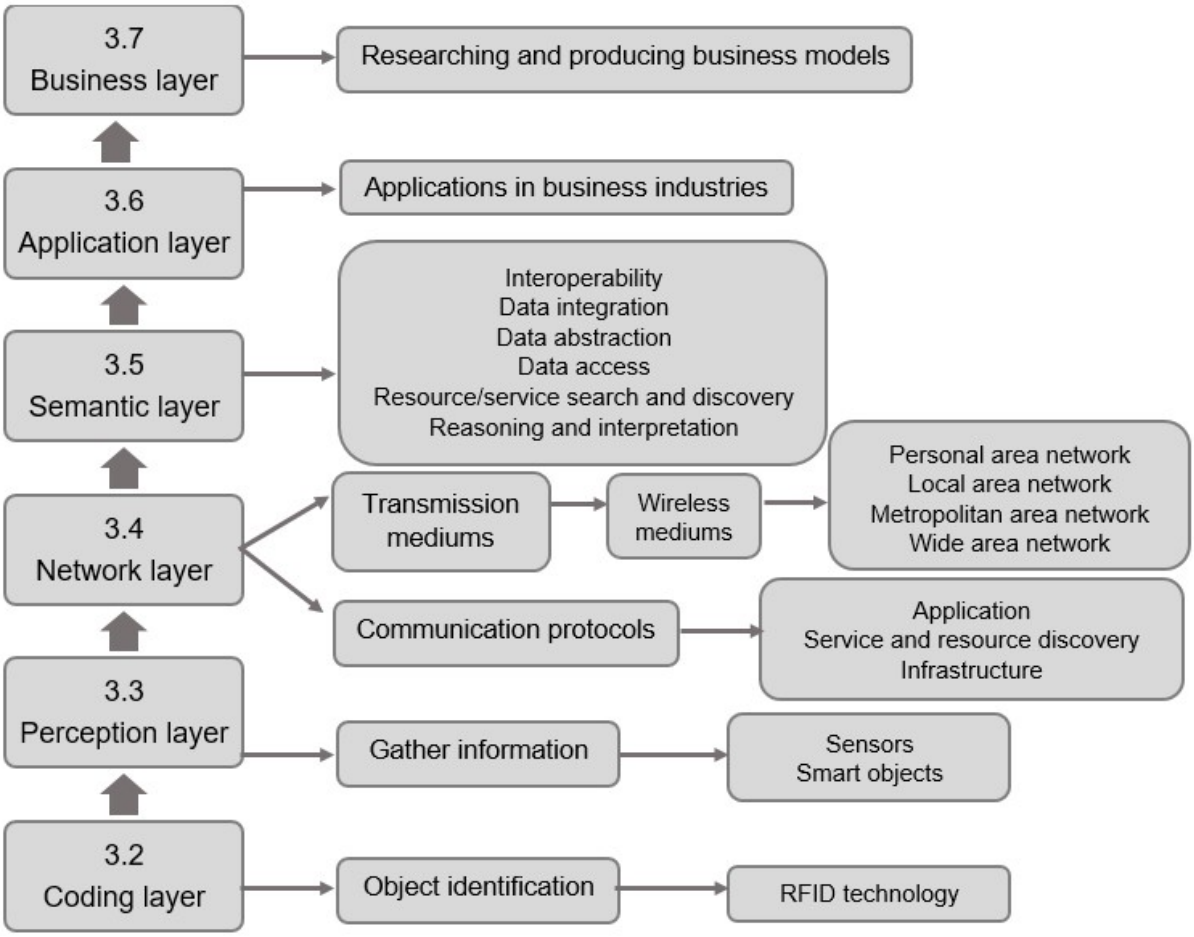


Figure 3.1: Proposed six-layer architecture of the Internet of Things

(Source: Adapted from Farooq *et al.*)

3.2 CODING LAYER

The coding layer is the foundation on which the Internet of Things is built and its main objective is to assign an identification number to each object (Farooq *et al.*, 2015:2). This unique identification number will identify objects in an Internet of Things environment as well as assist in distinguishing between objects (Zhang *et al.*, 2012:295).

RFID is the main technology associated with the automatic identification of objects and uses radio waves to transfer data and track objects (López *et al.*, 2012:292; Zhang *et al.*, 2012:294). RFID consists of the following three-part system (López *et al.*, 2012:292; Zhang *et al.*, 2012:294; CNRFID, n.d.[b]):

- **RFID tag:** The RFID tag contains the identification number of the object and stores the object's information. The RFID tag is attached to an object and can

pick up radio-frequency (RF) signals emitted from the RFID reader and relay signals back to it.

- **RFID reader:** The RFID reader interrogates and triggers the RFID tag through wireless communication mediums and is used to track and identify objects (see Section 3.4).
- **Central computer system**: RFID tag data are transferred to a central computer system to be organised and processed (see Section 3.5).

RFID tags can be classified into three categories, namely passive tags, semi-passive tags and active tags. The classification of tags is done according to the following tag properties (Farooq *et al.*, 2015:2; Atzori *et al.*, 2010:2790; CNRFID, n.d.[a]; Impinj, n.d.):

- **RF emitters**: It must be determined whether the tag is equipped with an RF emitter to emit a signal to the RFID reader without being interrogated by the reader.
- **Battery power**: It must be determined whether the tag is equipped with its own power source or whether it only generates power when it is interrogated by a reader.

Table 3.1 below classifies RFID tags in their three categories according to their battery power and RF properties. The table also indicates the communication range between tags and readers as well as the tags' capability to transfer data to the reader (Farooq *et al.*, 2015:2; Atzori *et al.*, 2010:2790; CNRFID, n.d.[a]; Impinj, n.d.).

Table 3.1: Three categories of RFID tags

	Passive tag	Semi-passive tag	Active tag
Embedded RF emitters in tag	**No**: Tags emit no RF signal.	**No**: Tags emit no RF signal.	**Yes**: Tags act as RF beacon that sends RF signals to reader without being triggered.
Battery power embedded in tag	**No**: Tag generates required power to transmit identification only when triggered by a signal transmitted from reader.	**Yes**: Battery power is used to supply energy to the tag's internal circuitry.	**Yes**: Battery power is used to emit an RF signal.
Communication range between tag and readers	Maximum of 10 metres	Between 10 and 100 metres	Greater than or equal to 100 metres
Sensor capability (refer to Section 3.3)	Capable of reading and transferring sensor data only when tag is triggered by reader	Capable of reading and transferring sensor data only when tag is triggered by reader	Capable of continuously reading and transferring sensor data

(Source: Author's own)

3.3 PERCEPTION LAYER

The perception layer consists of the objects associated with Internet of Things and its main function is to collect, capture and recognise useful information from sensors embedded in objects (Farooq *et al.*, 2015:2; Zhang, 2011:4110).

The latest trend is to combine RFID tags (see Section 3.2) with sensor technologies in order to create an object that can be identified through its RFID tag number and has the capability to gather information on its surrounding environment through sensors (López *et al.*, 2012:293–295). The main purpose of these sensors is to identify and collect information as well as implement control over objects (Zhang, 2011:4110). Sensor technologies, with incorporated transducers, use computing applications (micro electro mechanical systems) to collect real-time data on the object's surrounding environment (Farooq *et al.*, 2015:2; López *et al.*, 2012:293). Sensor technologies are categorised according to their properties and include, but are not limited to, the following (EngineersGarage, n.d.):

- **Temperature:** Thermistors and thermocouples

- **Pressure:** Fibre optic, vacuum and elastic liquid-based manometers
- **Flow:** Electromagnetic, differential pressure and thermal mass
- **Level:** Differential pressure, ultrasonic RF and radar
- **Proximity and displacement:** Photoelectric, capacitive, magnetic and ultrasonic
- **Biosensors:** Resonant mirror, electrochemical and surface plasmon resonance
- **Image:** Charge-coupled devices
- **Gas and chemical:** Semi-conductor, infrared, conductance and electrochemical
- **Acceleration:** Gyroscopes and accelerometers
- **Other:** GPS, moisture, humidity, speed, mass, tilt, force and viscosity.

By combining RFID tags and sensor technologies in a single device, the key enablers of Internet of Things are created, smart objects (López *et al.*, 2012:295). The concept of a smart object can be defined as single platform for assessing, creating, processing and sharing object information through networks and the Internet (López *et al.*, 2012:294; Kortuem, Kawsar, Fitton & Sundramoorthy, 2010: 44). Each smart object consists of a computational unit (microcontroller), a memory unit for program and data storage, read-only memory (EEPROM), static random access memory (SRAM), a power source, radio transceiver and/or transmitter (RFID tag) as well as an actuator to carry out necessary instructions (Liu & Wassell, 2011:1). Smart objects need to be small in size and by integrating nanotechnology techniques into their structure and material, they can be built on nanoscale with more processing power and memory (Bidgoli, 2015:299).

Smart objects are created to fit an intended purpose in order to perform specific functions in business industries (see Section 3.6). Just as business operations vary between industries, so will the composition of smart objects with regard to the material of which they are made, their software, programming and sensors. Even though smart objects differ from one another, they are all built on the following underlying principles (López *et al.*, 2012:294):

- Own a unique identifier

- Sense and save data gathered from sensor technologies
- Identifier and sensor data revealed to other objects and network systems
- Allow communication between different smart objects
- Make decisions with regard to themselves and their interaction with other objects and network systems.

3.4 NETWORK LAYER

The purpose of the network layer is to receive data gathered by smart objects in the perception layer (Section 3.3) and transfer it through transmission mediums (Section 3.4.1) with communication protocols (Section 3.4.2) to the semantic layer (Section 3.5) for processing and storage (Farooq *et al.*, 2015:2).

3.4.1 Transmission mediums

Data are transferred through transmission mediums between sender and receiver objects. Diverse sender and receiver objects are connected to one another and transmit data through the following two communication mediums (Bidgoli, 2015:114–115; Cisco, n.d.):

- **Wireless medium:** Devices and objects use an antenna to transmit data through radio waves to one another.
- **Wired medium:** Devices and objects communicate with one another through cables, where a physical path is provided along which signals can be transmitted.

Wired and wireless communication mediums can be placed into four major types of network structures (Bidgoli, 2015:117; Sousa & Oz, 2015:193–194):

- **Personal Area Network (PAN):** PAN is a wireless network designed for portable and handheld devices, with a maximum distance between devices of 10 metres.
- **Local Area Network (LAN):** A LAN connects workstations of a single business in close proximity to one another within a radius of six kilometres.
- **Metropolitan Area Network (MAN):** A MAN connects multiple LANs of multiple organisations with one another, within a city or nearby cities, across a distance of up to 50 kilometres.

- **Wide Area Network (WAN):** A WAN is a far-reaching system composing of multiple LANs or MANs, across a distance of more than 48 kilometres.

The focus of transmission mediums in Internet of Things lies more in wireless networks than wired networks, as the Internet of Things will form a self-regulating wireless sensor network, containing smart objects (Section 3.3) that monitor the physical environment and collect useful information (Gubbi, Buyya, Marusic & Palaniswami, 2013:1657; Matin & Islam, 2012:4; Zhu, Wang, Chen, Liu & Qin, 2010:348). Table 3.2 below lists the types of wireless communication mediums that are associated with Internet of Things:

Table 3.2: Wireless communication mediums associated with the Internet of Things

	Wireless medium		Network structures	Transmission range
Short-range	Bluetooth	NFC	PAN	<= 10 m
	Bluetooth low-energy	RFID reader	LAN	<= 6 km
	WIFI			
Long-range	WiMAX		MAN	<= 50 km
	LTE-A		WAN	>= 48 km

(Source: Author's own)

The above-mentioned types of wireless communication mediums can be shortly described as follows (Al-Fuqaha *et al.*, 2015:2350; Link-labs, 2015; Sousa & Oz, 2015:197–200):

- **Near-field Communication (NFC):** NFC supports communication between RFID readers and RFID tags within a range of up to 10 centimetres.
- **Bluetooth:** Objects communicate with each other through Bluetooth over short radio wavelengths of up to 10 metres.
- **Bluetooth low-energy:** This was developed to use less energy than standard Bluetooth and transfers data at high speeds within a range of up to 100 metres and is equipped with IP connectivity.
- **RFID reader:** The RFID reader emits a signal to an RFID tag (see Section 3.2) and receives an identification signal back from the RFID tag. The RFID reader

transfers the identification signal to a database that connects to a processing centre (see Section 3.5) to identify objects within a range of up to 200 metres.

- **Wireless Fidelity (WiFi):** WiFi allows wireless data exchange between objects within a range of 100 metres to a wireless router.
- **Worldwide Interoperability for Microwave Access (WiMAX):** WiMAX is a wireless MAN technology with a range of up to 50 kilometres.
- **Long-term Evolution Advanced (LTE-A):** Long-term evolution (LTE) uses Global System for Mobile Communications (GSM) network technologies to transfer data at a high speed between mobile phones. LTE-A is an improved version of LTE, with long-term infrastructure durability as well as scalability that is appropriate for the Internet of Things.

3.4.2 Communication protocols

Data gathered by smart objects are converted into digital signals and transferred through transmission mediums (Section 3.4.1) with communication protocols. Table 3.3 below classifies the communication protocols associated with Internet of Things into three broad categories (Al-Fuqaha *et al.*, 2015:2353):

Table 3.3: Communication protocols associated with the Internet of Things

<table>
<tr><td colspan="2">3.4.2.1
Application protocols</td><td>DDS</td><td>AMQP</td><td>MQTT</td><td>XMPP</td><td>REST on top of HTTP</td><td>CoAP</td></tr>
<tr><td colspan="2">3.4.2.2
Service and resource discovery</td><td colspan="4">mDNS</td><td colspan="2">DNS-SD</td></tr>
<tr><td rowspan="2">3.4.2.3
Infrastructure protocols</td><td>Routing Protocol</td><td colspan="6">RPL</td></tr>
<tr><td>Internet Protocol</td><td colspan="2">6LoWPAN</td><td colspan="2">IPv4</td><td colspan="2">IPv6</td></tr>
</table>

(Source: Adapted from Al-Fuqaha *et al.*)

These above-mentioned protocols do not have to be applied together to execute Internet of Things applications and each category is discussed below.

3.4.2.1 Application protocols

The focus of application protocols is on connecting people, objects, devices and servers with one another in order to transfer data accurately and efficiently. The

following application protocols are associated with the Internet of Things (Al-Fuqaha *et al.*, 2015:2353–2357; Schneider, 2013; Micrium Embedded Software, n.d.):

- **Data Distribution Service (DDS):** DDS provides real-time machine-to-machine communication. It is responsible for delivering information to devices and promotes the sharing of data between dispersed objects. Its main purpose is to connect devices and objects with one another in an Internet of Things environment.
- **Advanced Message Queuing Protocol (AMQP):** AMQP provides reliable exchanging of messages from point to point by routing them to the appropriate queues. Its main purpose is to act as a queuing system to connect servers with one another in order to share Internet of Things information.
- **Message Queue Telemetry Transport (MQTT):** MQTT facilitates optimal connection with remote objects and transfers data to an IT infrastructure for monitoring. Its main purpose is to collect device data and transfer the data back to a server for analysis and storage.
- **Extensible Messaging and Presence Protocol (XMPP):** XMPP allows near-real-time user communication through instant messaging over the Internet, irrespective of the operating system of the device being used. Its main purpose is to connect people to people, devices to people and servers to people for real-time Internet of Things communication.
- **Representational State Transfer (REST) on top of Hypertext Transfer Protocol (HTTP) functionalities:** REST can be interpreted as a cacheable connection protocol needing a stateless client-server architecture. REST is applied within social and mobile network applications, were data are transferred over HTTP between objects and servers in a simpler way. HTTP is a set of rules used for transferring information over the Internet. Taking this into account, it can be deducted that REST on top of HTTP is a software architecture that consists of a set of rules used for creating scalable web services for the Internet of Things.
- **Constrained Application Protocol (CoAP):** CoAP is a web transfer protocol aimed at the small resource-constrained smart objects of Internet of Things. CoAP is designed on REST on top of HTTP and allows objects to communicate interactively over the Internet.

3.4.2.2 Service and resource discovery

In an Internet of Things environment, a smart object that can gather data or perform a required action is called a resource, with a service referring to software that identifies the functionality of its corresponding resource. Search and discovery mechanisms are mandatory in Internet of Things, as they locate resources and services that provide data with regard to an entity of interest in the physical world (Barnaghi, Wang, Henson & Taylor, 2012:4). These mechanisms should be able to locate and record resources and services in a self-configuring and effective manner, enabling smart objects to join or leave an Internet of Things environment without affecting the whole system (Al-Fuqaha *et al.*, 2015:2357).

Domain Name System (DNS) Protocol is the main protocol used for resource and service discovery. It is an organised system of domains, where computers and network services are identified by their IP addresses and no external administration and configuration are needed to connect devices (Al-Fuqaha *et al.*, 2015:2357). The following two DNS protocols can discover resources and services offered by Internet of Things:

- **Multicast Domain Name System (mDNS):** An mDNS sends an IP multicast message to all objects in its nearby domain, requesting these objects to respond back if they comply with the specific enquiry that was sent out. When the target object receives the enquiry that was sent out, it multicasts a reply message, identifying itself as well as its IP address.
- **Domain Name System Service Discovery (DNS-SD):** DNS-SD performs a paring function for locating services needed in a network and matching them with IP addresses of objects using mDNS.

3.4.2.3 Infrastructure protocols

In Internet of Things, each object will have an identification number (see Section 3.2) as well as an address embedded in it. The object's identification number refers to its name, with the address referring to the IP address of the object within a communication network. Due to different global identification methods, it is important to differentiate between an object's identification number and its IP address, as the IP address can provide additional assistance in identifying objects (Al-Fuqaha *et al.*, 2015:2350).

Taking into account that an object has a name and an IP address, each physical object will own a corresponding virtual object within a communication network (Zhang *et al.*, 2012:294). The following infrastructure protocols will assist in addressing Internet of Things objects in low-power wireless communication networks:

- **Internet Protocol version 4 (IPv4):** IP is responsible for efficient data packet delivery between devices. Every device on the Internet has an IP address that uniquely identifies a device by a numerical number. IPv4 comprises of a 32-bit ($2^{\wedge 32}$) numerical address (Sousa & Oz, 2015:196). With the increased number of devices connected to the Internet over the last 14 years, IPv4 was depleted by 2011 (Internet World Stats, 2014; Jara *et al.*, 2013:97, 103).
- **Internet Protocol version 6 (IPv6):** IPv6 was deployed in 2012 to extend the addressing space to 128-bit ($2^{\wedge 128}$) numerical addresses to support the rising number of Internet-enabled devices (Sousa & Oz, 2015:196). IPv6 is deemed appropriate for the Internet of Things, as it offers scalable, flexible, ubiquitous and global end-to-end communication (Jara *et al.*, 2013:98, 103–104).
- **IPv6 over Low Power Wireless Personal Area Network (6LoWPAN):** Characteristics of smart objects in wireless sensor networks (Section 3.3) include low energy supply, restricted bandwidth as well as constrained connectivity and communication capacity. 6LoWPAN integrates IPv6 into smart objects to extend the Internet to smart devices over low-power wireless networks. 6LoWPAN offers low-power wireless networks the flexibility, scalability and end-to-end connectivity of IP (Jara *et al.*, 2014:9; Jara *et al.*, 2013:104; Mulligan, 2007:78).
- **Routing Protocol for Low Power and Lossy Networks (RPL):** A router routes data along the best path through connected networks to their destination (Sousa & Oz, 2015:195). None of the existing protocols were appropriate for 6LoWPAN, and as a result RPL was created (Ko, Terzis, Dawson-Haggerty, Culler, Hui & Levis, 2011:98). RPL is a routing protocol based on IPv6, designed for resource-constrained smart objects in Internet of Things wireless sensor networks (Al-Fuqaha *et al.*, 2015:2357).

3.5 SEMANTIC LAYER

Semantic technologies of the Internet of Things have the capability to extract knowledge from data gathered by smart objects in order to provide specific services or send demands to the correct resources or objects. Extracted knowledge refers to discovering and using resources, analysing and restructuring information and recognising relevant information (Al-Fuqaha *et al.*, 2015:2352). According to Barnaghi *et al.* (2012:4–5), the functions of the semantic layer include the following:

- **Interoperability:** Different users can access, exchange and interpret data among one another unambiguously.
- **Data integration:** Collected data from smart objects in physical environments are merged with other relevant data to create a more rounded picture of the environment, or collected data can be integrated into an existing analysis application to provide a better service to users.
- **Data abstraction:** Data abstraction focuses on how the data gathered from the physical environment are managed and represented.
- **Data access:** Data access refers to users gaining direct access to stored information in databases via the network layer (see Section 3.4).
- **Resource/Service search and discovery:** Refer to Section 3.4.2.2.
- **Reasoning and interpretation:** New knowledge is created by applying logical reasoning to gathered data with existing assertions and rules.

Table 3.4 below identifies the enabling technologies of the semantic layer to perform its functions.

Table 3.4: Enabling technologies of the semantic layer

		Enabling technologies to perform functions							
		RDF	RDFS	DNS	OWL	SPARQL	SSN	BD	CC
Functions	Interoperability	X							
	Data integration							X	
	Data abstraction						X		
	Data access								X
	Resource / Service search and discovery			X			X		
	Reasoning and interpretation	X	X		X	X		X	X

(Source: Author's own)

The above-mentioned enabling technologies can be shortly described as follow:

- **Resource Description Framework (RDF):** RDF is a general-purpose language for the semantic web where machine-readable metadata are added to web resources to provide interoperability between applications and conceptual structured knowledge (Menemencioglu & Orak, 2014:298; Barnaghi *et al.*, 2012:6).
- **Resource Description Framework Schema (RDFS):** RDFS represents the data typing vocabulary for RDF data (Menemencioglu & Orak, 2014:298).
- **Domain Name System (DNS):** Refer to Section 3.4.2.2.
- **Web Ontology Language (OWL):** OWL is an ontology language for web documents and applications that defines their intrinsic classes and connection to one another (Menemencioglu & Orak, 2014:298).
- **Simple Protocol and RDF Query Language (SPARQL):** SPARQL is a query language for databases that are able to retrieve and manipulate data stored in RDF (Menemencioglu & Orak, 2014:298; Barnaghi *et al.*, 2012:5).
- **Semantic Sensor Network Ontology (SSN ontology):** SSN ontology focuses on describing the physical characteristics and operations of sensor devices, their abilities, data gathered, methods for gathering data as well as the life expectancy of devices (Compton *et al*., 2012:27).
- **Big data (BD):** Smart objects with Internet connectivity gather data from their physical surrounding environment. When all the gathered data are put together, they generate big data. Big data demand intricate analysis to extract knowledge from them and require smart and efficient storage (Al-Fuqaha *et al.*, 2015:2351, 2364–2365). Data-modelling software is applied to data in order to analyse them as well as identify possible relationships between gathered data (Sousa & Oz, 2015:235). Data-mining software selects, explores and models large amounts of data, searching for previously unknown patterns in information that can support decision-making (Sousa & Oz, 2015:360).
- **Cloud computing (CC):** Cloud computing platforms provide access to a network of shared configurable computing resources that facilitates the transfer and storage of smart object data, almost-real-time big data analysis as well as user access to extracted knowledge upon request. Cloud computing resources are used and maintained remotely, and include data warehouses, networks, applications, servers and services (Al-Fuqaha *et al.*, 2015:2351, 2364–2365).

Cloud computing has four deployment models and a business must select a model based on its security needs as well as the level of involvement required from its IT managers. The deployment models are as follows (Bidgoli, 2015:297–299):

- Public cloud: A large number of users connect over the Internet to the cloud services and infrastructure. The public cloud carries a higher security and privacy risk for information.
- Private cloud: Cloud services and infrastructure are exclusively used by one business on a private network. The private cloud carries a lower security and privacy risk for information than the public cloud.
- Hybrid cloud: Hybrid cloud users use both private and public clouds. A business will operate its sensitive data on the private cloud and its public information on the public cloud.
- Community cloud: Community cloud infrastructure is used by a group of associated businesses that share common interests and concerns.

3.6 APPLICATION LAYER

The application layer specifies how Internet of Things technologies can be applied to business industry environments, based on the characteristics of its technologies and the data analysed by the semantic layer (Farooq *et al.*, 2015:2; Wu, Lu, Ling, Sun & Du, 2010:487). This layer supports the expansion of Internet of Things to a big-scale development in business industry environments. Possible applications of Internet of Things were derived from gaining an understanding of the enabling technologies of Internet of Things and can broadly be divided into the following categories:

- By authentically identifying an object, the validity of a smart object can be confirmed, thereby ensuring the legitimacy of the information gathered by it and its identity (see Section 3.2)
- Tracking an object's location through real-time identification of a smart object in motion through GPS co-ordinates (see Section 3.3)
- Monitoring environments with sensors embedded in smart objects (see Section 3.3)
- Gathering information on the location, identity and environment of an object (see Section 3.3)

- Making deductions from analysed gathered information (see Section 3.5), and
- Autonomously making decisions and giving instructions based on the deductions made (see Section 3.5).

The applications of the Internet of Things and their impact on business operations in specific business industries were an objective of this research.

3.7 BUSINESS LAYER

The business layer manages the applications and services of Internet of Things. This layer is responsible for researching and producing business models for effective business strategies (Farooq *et al.*, 2015:2; Wu *et al.*, 2010:487). Business models for effective business strategies were however not an objective of the research.

3.8 CONCLUSION

A better understanding has been gained of the Internet of Things through the identification and categorising of its enabling technologies. This knowledge will assist in the investigation of the possible applications and their impact on business operations in specific business industries.

CHAPTER 4:
APPLICATIONS AND IMPACT OF THE INTERNET OF THINGS ON BUSINESS INDUSTRIES

4.1 INTRODUCTION

In the last few years, technology has evolved in such a way that it provides economic advantages for businesses. If the Internet of Things is adopted by businesses, it will offer the following benefits (Vermesan & Friess, 2014:30, 41):

- Increase a business's productivity, which has a direct effect on the success and profitability of the business
- Provide market differentiation to businesses in a market that might already be saturated with similar products and services
- Enable businesses to be more cost-efficient by utilising resources better and reducing business operation downtime
- Provide higher-quality information to be used in the decision-making process.

It will not be possible to define a universal business model for the Internet of Things due the diversity of its applications as well as the different driving forces behind it (Vermesan & Friess, 2014:41). The rest of this chapter briefly outlines the applications of Internet of Things and the impact it will have on selected industries.

Table 4.1 below illustrates how the applications of Internet of Things (see Section 3.6) are applied to selected business industries. The applications can broadly be classified as:

- tracking an object's location
- authentically identifying an object
- monitoring environments with sensors
- gathering information on the location, identity and environment of an object
- making deductions from analysed gathered information, and
- autonomously making decisions and giving instructions based on the deductions made.

Table 4.1: Applications of Internet of Things applied to specific business industries

			Internet of Things applications					
			1. Tracking	2. Identification	3. Monitoring situations	4. Gathering information	5. Making deductions	6. Giving instructions
Industries	4.2	**Automotive**						
		Vehicle design	X		X		X	X
	4.3	**Transport**						
		Locating vehicle	X	X			X	
		Ticket payment				X		X
		Commuter analysis				X	X	
		Traffic analysis			X		X	X
	4.4	**Supply chain management, logistics and manufacturing industry**						
		Supply chain management and logistics	X		X		X	X
		Manufacturing process	X		X			
		Inventory records		X		X	X	X
		Warehouse protection			X		X	X
	4.5	**Retail**						
		Consumer needs		X			X	
		Inventory control	X		X	X	X	X
	4.6	**Healthcare**						
		Patients	X	X			X	
		Patient medical history		X		X	X	
		Medical equipment	X		X		X	
		Medical products and materials	X				X	
		Hospital staff		X				X

			Internet of Things applications					
			1. Tracking	2. Identification	3. Monitoring situations	4. Gathering information	5. Making deductions	6. Giving instructions
Industries	4.7	**Pharmaceutical**						
		Supply chain management	X	X				
		Authenticity	X	X				
		Product side effects		X			X	X
	4.8	**Advertising and marketing**						
		Brand awareness and credibility				X	X	X
		Cost-reduction benefits				X	X	X
		Increased quality of leads		X			X	X
	4.9	**Telecommunication**						
		Merging market segments and technologies			X	X	X	X
	4.10	**Education**						
		Adapting to needs		X		X	X	
		Supporting teachers and learners		X		X	X	X
		Module restructuring				X	X	X
	4.11	**Agriculture**						
		Ecological farming environment			X		X	
		Greenhouses			X		X	X
		Animals	X		X		X	
		Agricultural equipment			X		X	X

(Source: Author's own)

4.2 AUTOMOTIVE INDUSTRY

Global warming, depleted non-renewable energy resources, safety, affordability and connectivity are some of the main areas that impact the design of vehicles in the automotive industry (Aris, Sahbusdin & Amin, 2015:2). Sensors embedded in vehicle parts will be able to monitor fuel usage and emissions in an effort to preserve the environment (Aris *et al.*, 2015:1). Vehicles should be equipped with sensors that monitor fuel levels, tyre pressure, acceleration levels and brake conditions, in order to warn their users in advance to a possible breakdown (Agrawal & Das, 2011:5). Safety features should include sensors and actuators that ensure that a safe distance is kept between vehicles in order to avoid accidents as well as to enable the vehicle to automatically make calls in cases of emergency, which provide its GPS location, the damage to the vehicle and the type of load it is carrying (Agrawal & Das, 2011:5; Sundmaeker *et al.*, 2010:51).

4.3 TRANSPORT INDUSTRY

Transport has become part of our daily lives and a necessary infrastructure for our modern society. The optimal functioning of the transport industry is vital for human mobility, business trading and the economic growth of a country (Guerrero-ibanez, Zeadally & Contreras-Castillo, 2015:122). Public transport, on which many people depend, can be improved by the following Internet of Things technologies (Bojan, Kumar & Bojan, 2014:174–176; Chunli, 2012:361; Yongjun, Xueli & Shuxian, 2012:1–2):

- **Vehicle tracking:** Users of public transport can trace the current location of a specific vehicle with their mobile devices by integrating an RFID tag with the vehicle's GPS system. The estimated time of arrival will be calculated for the commuter based on the information received of the vehicle's location, weather conditions and traffic.
- **Ticket payment:** Transport payment is made simpler and easier through a virtual ticketing system based on NFC technologies. NFC-enabled mobile devices of commuters (sender) will authorise transport payment via a smart label at the beginning of a journey by tapping the sender device to the NFC reader of the transport provider (receiver), which will initiate the applications for

the payment process. This is a safer alternative for transport providers than cash transactions.

- **Commuter analysis:** Bus transport will make use of RFID technologies to record the flow of people getting on and off the bus. This gathered information can be used by bus companies to reconcile the payments received to the number of commuters getting on the bus as well as informing other commuters to use alternative transport if a specific bus is full to capacity.
- **Traffic analysis:** Sensors embedded in all vehicles on the road provide comprehensive traffic data to public transport providers on the amount of vehicles on the route, the type of road being used and any accidents in the nearby vicinity. This information will ensure that alternative routes are calculated in congested traffic in order to maximise the efficiency of their service.

4.4 SUPPLY CHAIN MANAGEMENT, LOGISTICS AND MANUFACTURING INDUSTRY

Manufacturers and suppliers of products that use RFID technologies in an Internet of Things environment will be able to reduce inventory production up to 30%, reduce transport costs up to 13%, shorten the delivery cycle of products up to 50% as well as assert better control over inventory movement by tracking the flow of products through the supply chain (Ma, Shang, Fu & Luo, 2013:466; Yan & Huang, 2009:168). By using the analysed traffic data of the transport industry (refer to Section 4.3), routes for delicate products can be controlled to protect products from damage as well as high-value products from heists. Internet of Things technologies will also benefit the manufacturing process by providing real-time data in the following areas (Vermesan & Friess, 2014:36–37; Liu, Yuan & Chang, 2012:232; Agrawal & Das, 2011:6; Sundmaeker *et al.*, 2010:50;):

- **Process management:** RFID and wireless technologies provide real-time locating and monitoring capabilities that support manufacturers in managing, testing and verifying the products going through the assembly line, thereby improving the quality of the product and reducing failure rates.
- **Inventory management:** Detailed inventory records are made possible by the product information stored in RFID tags embedded in products. The complete

history of a product will be available from production to disposal, including manufacturer details, production and expiry date, warranty period and details on after-sales service. Furthermore, Internet of Things semantic technologies will pick up when inventory levels are low and automatically order parts from pre-approved suppliers.

- **Warehouse management:** Sensors in production and storage will monitor for possible threats of temperature fluctuations, water and fire, and send out warning messages to management in threat situations.

4.5 RETAIL INDUSTRY

With consumers demanding a personalised experience in today's digital environment, the Internet of Things will ensure that businesses tie everything together, from ensuring that the right consumer receives the right product at the correct time and place, to tracking inventory through the supply chain as well as visibility in the logistic operations (refer to Section 4.4) (Vermesan & Friess, 2014:69–70; Zhang, Chen, Bergarp, Norman, Wikström, Yan & Zheng, 2009:1).

Through smart identification when customers enter a store, better customer service can be provided at the point of sale according to the shopping habits and preferences of customers (refer to Section 4.8) (Vermesan & Friess, 2014:33). Loss of income from shoplifting can be prevented by embedding an RFID tag in products to track them (Farooq *et al.*, 2015:5). Furthermore, through proper inventory management (refer to Section 4.4), no out-of-stock situations will occur that may lead to the business losing valuable customers (Farooq *et al.*, 2015:5; Agrawal & Das, 2011:6). The sale status of products will be available in real time to manufacturers to accurately plan production quantities, thereby avoiding over- and under-production of inventory (refer to Section 4.4) (Yan & Huang, 2009:168)

4.6 HEALTHCARE INDUSTRY

Internet of Things technologies will meet the growing demand for a ubiquitous healthcare system that will improve human health and well-being (Rahmani, Thanigaivelan, Gia, Granados, Negash, Liljeberg & Tenhunen, 2015:826). Through smart objects embedded in patients as well as mobile and wearable devices, patients and their caregivers will be able to continuously monitor patients' vital signs and health

conditions, gain access to medical information stored and analysed in databases, control medical appliances and communicate in emergency situations (Ali & Abu-Elkheir, 2015:9; Rahmani *et al.*, 2015:826). The benefits that Internet of Things technologies will provide to hospitals through smart objects embedded in patients and facilities can be grouped as follows (Asghar *et al.*, 2015:428–429; Atzori *et al.*, 2010:2795; Sundmaeker *et al.*, 2010:52):

- **Tracking** can be applied in the following areas in a healthcare environment:
  - Patients: By monitoring the position of patients, the workflow in hospitals will be more efficient.
  - Medical equipment: By continuously tracking the medical equipment in hospitals, its availability and location can be checked when needed, and its usage can be monitored to ensure maintenance is done according to regulations.
  - Medical products and materials: Tracking is crucial in a surgery environment, as it confirms and calculates the estimate time of arrival of needed surgery products, blood and transplant organs that are en route to the theatre for the surgeons.
- **Smart authentication** can be applied in the following areas in a healthcare environment:
  - Patients: It includes patient identification to ensure that the patient receives the correct procedure or medicine at the stipulated time and provides a comprehensive up-to-date electronic medical record. Implantable wireless devices could store health records of patients, which could save their lives in emergency situations when they are unable to communicate themselves.
  - Hospital staff: Access to restricted areas in hospitals can be granted only to authorised staff.
- **Data collection from sensors:** Automatic data collection from sensors in smart objects reduces data entry times of patient records and minimises data input errors. Collected data on patients' health indicators are transferred to the semantic layer for analysis, which in return will diagnose a patient's condition.

4.7 PHARMACEUTICAL INDUSTRY

The safety and security of medicine in the pharmaceutical industry are crucial to prevent compromising the health of patients (Sundmaeker *et al.*, 2010:53). Smart labels attached to medicine containers will identify the medicine, provide information on its composition and track it through the supply chain (refer to Section 4.4) (Jara, Belchi, Alcolea, Santa, Zamora-Izquierdo & Gómez-Skarmeta, 2010:809; Sundmaeker *et al.*, 2010:53).

Patients can have harmful side effects and adverse reactions to medicine due to incompatibilities between the ingredients in the drugs and the patients' medical profile. The Internet of Things can provide a solution to this problem by checking the suitability of the medicine to patients' medical history. Wearable or mobile devices of patients will identify medicine in close proximity to the patients through NFC. Before medicine is administered to patients, their electronic allergy profile and medical history are compared to a database that provides a description of the medicine, its active ingredients and side effects, in order to check the patients' compatibility with the medicine (Jara *et al.*, 2010:809).

Before medicine products can be sold on the market, they have to satisfy generally accepted quality standards. Counterfeit medicine, which are of inferior quality, has increased over recent years and jeopardises the health of patients. By tracking and identifying medicine through RFID technologies, counterfeit products can be detected and the supply chain kept free of fraudsters (Ting, Kwok, Albert & Lee, 2010:1, 3).

4.8 ADVERTISING AND MARKETING INDUSTRY

Businesses that use traditional marketing strategies are inclined to blindly market their products to consumers, not taking into account whether the consumers might be interested in the product or not. The focus of traditional marketing lies on the number of consumers that are reached and not on the consumers interested in the products (Prescott, 2012). Traditional marketing includes sales flyers, spam e-mails, telemarketers as well as advertisements on television and radio and in magazines (Wikipedia, 2016). The enabling technologies of Internet of Things will shift the focus of marketing to target specific consumers in a market segment, who will value the information even if they are unaware of the product, thereby building trust and

confidence between the consumer and the business (Prescott, 2012). This electronic format of advertising is distributed through blogs, podcasts, e-books, videos, whitepapers and social media marketing (Wikipedia, 2016).

Data gathered by smart objects on the daily lives of consumers and processed by the semantic layer will be used by marketers to identify consumer preferences of individuals. This information will be used to target consumers in specific market segments and build an electronic relationship with them. According to Optify (2013), the following benefits can be expected when incorporating Internet of Things technologies with marketing:

- **Brand awareness and credibility:** The more advertising mediums – blogs, social media, videos, etc. – a business has, the greater the likelihood of it being visited by a consumer. Furthermore, the presence on multiple advertising mediums will create brand awareness, which will lead to increased consumer trust and strengthen the credibility of the business's brand.
- **Cost-reduction benefits:** By making use of Internet of Things resources for marketing, advertising costs can decrease by up to 60% by cutting costs on traditional marketing.
- **Increased quality of leads:** Due to the target-specific marketing of products, relevant information is provided to consumers, thereby increasing the quality and sale ratio of consumers visiting the business.

4.9 TELECOMMUNICATION INDUSTRY

Revenue streams of traditional telephony and short message services are threatened by next-generation communication services and applications provided by Internet companies at minimal costs (Carriedo & Beltrán, 2015:211). Currently, the telecommunication industry aims to merge the different market segments of telecommunications, IT and electronic media as well as unify its technologies and synchronise its regulations. This merger process is driven by the large-scale development of digital technology in the last few years and will evolve further through the adoption of Internet of Things (Sallai, 2013:13).

Digital information content currently transmitted over networks include, but are not limited to, voice, data, text, audio-visual programs and multimedia. This information has been linked to separate networks, services and user terminals, and their markets have been managed separately. The Internet of Things will create an integration structure for processing, storing, accessing and distributing all digital information, including combining this information with relevant smart objects' data within a network (Sallai, 2013:14).

Businesses should take into account that the line that divides the Internet of Things and traditional telecommunication networks will blur in the long run, as objects will form part of networks and facilitate object-to-object communication as well as increase robustness of communication channels (Sundmaeker *et al.*, 2010:51). With Internet of Things creating the possibility of merging different telecommunication technologies to create additional new services, telecommunication companies should adjust their strategic and technical focus in order to stay in business (Carriedo & Beltrán, 2015:212; Sundmaeker *et al.*, 2010:51). Telecommunication businesses can adjust their focus to provide electronic content services and applications in specific industries, such as e-health, e-learning, intelligent transportation and energy systems (Sallai, 2013:14).

4.10 EDUCATION INDUSTRY

The most significant change to the education process in the last 200 years was that books moved from printed form to online content, thereby creating the concept of e-learning. Although online content made the learning process easier, knowledge is still passed on to learners by a single person (Janitor, 2011:89). The Internet of Things will change the learning environment by introducing an e-learning framework with ontology-based properties and hierarchical semantic associations with the capabilities of adapting and intelligently supporting learners based on their individual needs (Ghaleb *et al.*, 2006:64). The hierarchical semantic associations will be able to show the complete structure of an educational topic and its available sequence of learning, as well as the semantic relationship between the educational contents, in order to provide information for the intelligent e-learning system. Furthermore, the created ontologies will specify the conceptualisation of the educational domain in terms of concepts, attributes and relationships, thereby enabling the e-learning system to

represent, process, share and reuse knowledge between applications (Ghaleb *et al.*, 2006:64–65). The following impact can be expected when e-learning is integrated with the semantic technologies of Internet of Things (Janitor, 2011:89; Koper, 2004:6):

- Flexible web-based courses will be developed that incorporate multimedia and interactive parts to adapt to a smartly identified learner's specific characteristics and needs.
- By identifying and integrating relevant module information gathered from a variety of authors and sources, effective learning and teaching patterns can be shared among piers.
- The time, effort and cost of continuously manually updating the learning-management system of a module will be reduced due to the system autonomously adapting the module to the individual learner's characteristics and needs.
- Semantics and ontologies built into the modules will support learners and staff in better managing teaching and learning activities and workflow as well as ensuring that all relevant resources are used during these activities.
- The semantic structure creates a more advanced and complex learning design that autonomously compare a variety of resources with ease, for the consistent performing of effective and relevant research.

4.11 AGRICULTURE INDUSTRY

Currently in the agricultural industry there is a lack of good-quality information to address farmers' production needs, including the fact that more focus is placed on machinery hardware than software. The Internet of Things and RFID technologies can address these issues by creating an automated smart agriculture environment (TongKe, 2013:210, 213).

In the ecological farming environment, sensors placed in fields will be able to monitor water quality, soil composition, humidity, sunlight as well as air pollution. Farmers will receive timely and accurate data to improve the quality of water, save money on fertilisers and plan their field work more effectively (Farooq *et al.*, 2015:5; Agrawal & Das, 2011:6). Furthermore, the conditions inside a greenhouse can be monitored by sensors and analysed by the semantic layer in order to maximise production and save

water through automatic temperature adjustment and irrigation by actuators in smart objects (Farooq *et al.*, 2015:5; TongKe, 2013:215).

Tracking animals with the help of RFID technologies minimises the risk of them being stolen and allows farmers to better care for the animals (Agrawal & Das, 2011:6; Sundmaeker *et al.*, 2010:55). Also, by adding sensors to RFID technologies, the health status of herds can be monitored in order to control, survey and prevent animal diseases (Sundmaeker *et al.*, 2010:55).

Smart objects placed within agricultural equipment will be able to monitor farm machinery for possible breakdown, with the semantic layer in return diagnosing the problem through gathered information from the machine. Internet of Things technologies will enable farmers to remotely control machinery from another location, thereby lightening their work load (TongKe, 2013:216).

4.12 CONCLUSION

The main theme present through this chapter is the ability of Internet of Things technologies to convert most manual business operations into autonomous operations. With Internet of Things technologies adopting humanlike characteristics through their ability to gather and process information at a high speed and with great accuracy, value will be added to the products and services that businesses deliver to their consumers. Businesses will be quick to adopt the Internet of Things based on the benefits and opportunities that it offers, but will fail to recognise the threats associated with it.

CHAPTER 5:
RISKS ASSOCIATED WITH THE ENABLING TECHNOLOGIES OF INTERNET OF THINGS

5.1 INTRODUCTION

The unique nature of Internet of Things with its numerous devices makes it vulnerable to attacks. This is compounded by the limited capabilities of the constantly interacting devices that make use of a variety of technologies on a large scale in a network (Nurse *et al.*, 2015:6). With the Internet of Things identifying and locating devices and humans, as well as gathering information on them, the acceptance of Internet of Things by businesses will largely rely on the protection of gathered information and data (Farooq *et al.*, 2015:5). Due to the deployment, mobility and complexity of Internet of Things, the protection of information and data creates problems for the following reasons (Nurse *et al.*, 2015:6; Atzori *et al.*, 2010:2801; Wang *et al.*, 2006:2):

- Smart objects are vulnerable to physical attacks and prone to failures due to device limitations and mostly because they are left unattended in harsh environments.
- Intensive communications between smart objects themselves, data storage centres and the semantic layer rely mainly on wireless networks, making unauthorised access to transferred information and data easy, because in some instances unsecured communication channels are used.
- The components of smart objects are characterised by low capabilities in terms of energy and computing resources, which makes the implementing of complex methods supporting security of information difficult.

Table 5.1 below shows the categories in which the threats associated with Internet of Things technologies are discussed.

Table 5.1: Threats associated with Internet of Things technologies

			Threats associated with Internet of Things technologies																		
			Collisions	Denial of service	Man-in-the-middle	Data loss	Sinkhole	Message tampering	People tracking	RFID tag cloning	Eavesdropping	Sniffing	Smart object tampering	Node impersonation attack	Sybil	Spoofing	Replay	Jamming	Selective forwarding	Semantic query languages	Semantic ontology development
Categories	5.2	Data integrity	X	X	X	X	X	X													
	5.3	Data privacy			X				X	X	X	X	X								
	5.4	Data confidentiality			X					X	X	X	X								
	5.5	Authenticity	X											X	X	X	X				
	5.6	Unauthorised access			X	X		X			X	X	X	X	X	X	X				
	5.7	Network availability		X														X	X		
	5.8	Semantic layer vulnerabilities																		X	X

(Source: Author's own)

5.2 DATA INTEGRITY

Data integrity is the fair and consistent representation of information, including the capability to confirm that data have not been changed or corrupted (Bidgoli, 2015:76; Matin & Islam, 2012:18; Boritz, 2005:262). Data integrity includes the characteristics of validity (refer to Section 5.5), accuracy, completeness and timeliness as well as their relationship with one another (ISACA, 2012a; Boritz, 2005:262, 265). These characteristics explained in an Internet of Things context are as follows:

- **Accuracy**: This is the quality of exactness to the real-world event of data gathered by smart objects on their surrounding environment (Boritz, 2005:265; Farooq *et al.*, 2015:2; Zhang, 2011: 4110).
- **Completeness:** With the combination of RFID tags and sensor technologies, a complete dimensional picture of the smart object's location and surroundings can be formed (López *et al.*, 2012:292–295; Boritz, 2005:265).
- **Timeliness:** Data are gathered and transferred over the network for analysis in real time to provide services in a timely manner (Matin & Islam, 2012:18).

Data integrity of Internet of Things are exposed to the following threats:

- **Collisions:** A collision takes place when two objects try to transmit data and information on the same RF at the same time. When the data packets collide with each other, a change in data will occur, which leads to a checksum mismatch at the receiving end of the data. Repeated collisions, if not discovered or prevented, will also lead to energy exhaustion of objects (Wang *et al.*, 2006:5).
- **Denial of service (DOS):** The main goal of a denial-of-service attack is to flood a service with false requests in an attempt to exhaust its resources, and due to the large number of requests, the service reaches its threshold capacity after which it cannot service legitimate requests anymore, making the service unavailable to the intended user in a timely manner. When denial-of-service attacks are executed from different locations by several attackers, it is called a distributed denial-of-service attack (Matin & Islam, 2012:19; Misra, Krishna, Agarwal, Saxena & Obaidat, 2011:115). Different types of denial-of-service attacks are focused on the following components of the Internet of Things:
  - Network: A large amount of network traffic is flooded to the network, preventing legitimate network traffic (Farooq *et al.*, 2015:5; Matin & Islam, 2012:19; Wang *et al.*, 2006:7).
  - Smart objects: The attacker targets the connections between two nodes repeatedly with new connection requests until its becomes vulnerable to memory exhaustion and ignores legitimate connection requests (Farooq *et al.*, 2015:5; Matin & Islam, 2012:19; Wang *et al.*, 2006:7).
  - Data storage: This entails flooding a server with service requests in order to prevent legitimate users to gain access to the information (Bidgoli, 2015:80).
- **Man-in-the-middle:** This is an account-hacking threat in which the attacker has the ability to capture and manipulate data communications in real time between smart objects themselves, the semantic layer and cloud computing servers. Man-in-the-middle has a high success rate if the adversary can impersonate the smart objects or resources to the satisfaction of one another (Farooq *et al.*, 2015:5; Ashktorab & Taghizadeh, 2012:237).

- **Data loss:** Data loss is the threat that data are modified, deleted or lost without a backup thereof and never recovered. Businesses rely on information and data as economic drivers and lost data will have critical consequences for any business. Data can be lost through various means (Farooq *et al.*, 2015:5; Ashktorab & Taghizadeh, 2012:236–237; Rotter, 2008:72; Smith, 2003:1–2):
  - Intentional action: This refers to intentional modification or deletion of data by malicious attackers who are either authorised or unauthorised users of the Internet of Things as well as physical smart object destruction.
  - Unintentional action: This includes accidental modification or deletion of data by individuals who have access rights to them, database administration errors and semantic technologies being unable to read unknown data formats.
  - Failure: This refers to smart object power failure resulting in data in the volatile memory not being saved to permanent memory, hardware failure, a software crash or freeze, business failure of the cloud service provider and data corruption during data transmission.
  - Disaster: This includes natural disasters such as earthquakes, floods and fires that destroy physical Internet of Things resources.
  - Crime: Crime refers to the theft of smart objects, malicious acts of worms, viruses, hacking or unauthorised access to data on smart objects, networks and databases.
- **Sinkhole:** Sinkhole attacks take place when an attacker attracts network traffic to a compromised node by making it look more appealing to nearby nodes through forged routing information. The end result of sinkhole attacks is that the malicious node will lure all network traffic of surrounding nodes through the compromised node, with the attacker at the centre of the network flow, enabling him/her to remove or modify the received data before transmitting it to the receiver (Mejri, Ben-Othman & Hamdi, 2014:61; Matin & Islam, 2012:19; Wang *et al.*, 2006:7; Karlof & Wagner, 2003:300).
- **Message tampering:** Message tampering consists of the modifying, deleting, constructing or altering of data through the following methods:

- RFID tag content changes: When an RFID tag is writable, it is easier for attackers to change the content of the tag, alter its characteristics or insert modified tag data (Rotter, 2008:72).
- Masquerading attack: In the masquerading attack, the adversary is hiding behind valid identification measures of objects, either its IP address or RFID identity number, thereby making it possible to generate false data that appear to come from a legitimate object (Mejri *et al.*, 2014:62).
- Illusion attack: The illusion attack fabricates data by placing sensors in a network that generates false data. The false data of the sensors move normally in the network and require object interaction to make decisions or provide a service (Mejri *et al.*, 2014:62).

5.3 DATA PRIVACY

Privacy can be defined as a specific state of life characterised by being excluded from public attention as well as being free from being observed (Britz, 2010). Privacy is regarded as a natural right that is deeply rooted in our civilisation and provides the foundation for legal rights. Privacy is also constitutionally protected in most democratic countries through legislation (Atzori *et al.*, 2010:2802; Britz, 2010).

The right to privacy of personal information is threatened by the projected invasiveness of Internet of Things, which violates the privacy of human individuals by targeting their real-time identification, indicating their immediate environment as well as reflecting their personal profiles on social spaces on the Web (Oteafy & Hassanein, 2012:491; Chan & Perrig, 2003:104). These individuals have no control over which personal data are collected, by who they are collected and when the collection is taking place (Oteafy & Hassanein, 2012:491; Atzori *et al.*, 2010:2802).

Types of personal information that can be collected through Internet of Things are *inter alia* (Phelps, Nowak & Ferrell, 2000:27–41):

- **Demographic data:** Age, marital status, occupation, educational qualification
- **Lifestyle interests:** Favourite hobbies, television programmes, charities, leisure activities
- **Media habits:** Magazines, newspapers, web browsing

- **Personal identification data:** Name, address, telephone number, ID number
- **Financial data**: Annual income, internet banking details, credit information
- **Geographical data:** Location, latitude longitude.

By implementing the Internet of Things in our daily lives, laws may be broken in the process of making the position and movements of individuals known as well as gathering their personal information without their consent. It also has to be taken into account that ethical standards set by civilisation may be breached. The privacy of human users in an Internet of Things environment is exposed to the following threats:

- **People tracking:** Tracking the movements of individuals without their consent through GPS and smart object identification represents a violation of their privacy (Mejri *et al.*, 2014:62; Rotter, 2008:72).
- **RFID tag cloning:** The original RFID tag is cloned, with the duplicated tag being the same size or larger than the original tag, but containing the same characteristics and functionalities as the original tag. Adversaries will use duplicate tags to access restricted areas and abuse private and confidential data (Rotter, 2008:72).
- **Eavesdropping:** This is where attackers gain unauthorised real-time access to private data by secretly monitoring data transmissions between an RFID tag to a reader over the communication channel or data transference over the network between smart objects, the semantic layer and cloud storage. Eavesdropping is difficult to detect, because it is a passive attack where the adversary does not emit any signal (Rotter, 2008:71; Chan & Perrig, 2003:103).
- **Sniffing:** Sniffing is the capturing, decoding, inspecting and interpreting of data transmitted in a network. Sniffing is mostly used to steal information, but can be used for legitimate reasons, such as monitoring networks' performance. It is difficult to detect a sniffing threat due to the attacker being silent in the network (Bidgoli, 2015:60).
- **Smart object tampering:** Tampering is a form of attack where information is extracted from a smart object through physical access to the object. The node may also be altered or replaced to create a compromised node which the attacker controls (Farooq *et al.*, 2015:5; Wang *et al.*, 2006:5).
- **Man-in-the-middle:** Refer to Section 5.2.

5.4 DATA CONFIDENTIALITY

Confidentiality involves a set of rules that limits or places restrictions on access to information, and where the focus of data privacy lies with the violating of human information, the focus of data confidentiality lies with the violating of business information and processes (Bandyopadhyay & Sen, 2011:59). The confidentiality of business information is a fundamental security requirement for most businesses and it is critical to the success of a business that its information is not made available to unauthorised individuals and other businesses (Karygiannis & Owens, 2002). Business information that needs to be protected includes trade secrets, inventions, discoveries, data, formulas, business methods, processes and employees.

In an Internet of Things business environment, the risk exists that databases are breached by attackers and that information communicated on a network is not concealed from them or is understood by anyone other than the desired recipients (Jara *et al.*, 2013:104; Matin & Islam, 2012:18; Wang *et al.*, 2006:4). RFID tag cloning, eavesdropping, sniffing, smart object tampering and man-in-the-middle attacks pose a threat to the confidentiality of data (refer to sections 5.2 and 5.3).

5.5 AUTHENTICITY

Authentication is the determining of the validity of the data transferred and presented by an Internet of Things object, ensuring that the data are indeed collected by the stated object, at its stated location and at its stated time, proving that the data are a true representation of a captured event (Matin & Islam, 2012:18; Boritz, 2005:266). The authenticity of data and smart objects in an Internet of Things environment is exposed to the following threats:

- **Collisions:** Refer to Section 5.2. The data packet that reaches the receiving end will be discarded as invalid due to the checksum mismatch of the collision (Wang *et al.*, 2006:5).
- **Node impersonation attack:** Every object in the Internet of Things environment has an IP address, which helps to distinguish between objects in the network. The adversary in an impersonation attack obtains a valid IP address of an object and passes for a legitimate object in the network (Farooq *et al.*, 2015:5; Mejri *et al.*, 2014:61; Wang *et al.*, 2006:5).

- **Sybil:** Sybil attacks is where a single node represents several identities in a network by fabricating or stealing the identities of legitimate nodes. With the Internet of Things identifying the location of its objects, Sybil attacks pose a threat to geographic routing protocols, as it is expected that an object cannot be in more than one place at any singular time (Matin & Islam, 2012:19; Wang *et al.*, 2006:7; Karlof & Wagner, 2003:301).
- **Spoofing:** A spoofing attack is when an adversary attempts to gain access to a service or resource by impersonating an authorised user or node in order to find sensitive information, launch attacks against networks or bypass access controls (Bidgoli, 2015:60). Three types of spoofing that have an impact on the Internet of Things environment include the following:
    - GPS spoofing: Each smart object is equipped with a GPS system that indicates the location of the object. GPS spoofing happens when false location data are provided through a transmitter that generates a fake stronger signal than signals generated by real GPS satellites (Mejri *et al.*, 2014:61).
    - Acknowledgement spoofing: Routing algorithms implemented in sensor networks need acknowledgments from nodes that they are active and able to form a strong link with the network before they can connect to the communication network. A malicious node can spoof the acknowledgements of overheard packets intended for nearby nodes in order to deliver incorrect information to those nearby nodes. The goal is to convince the sender of the data that a weak connection is strong or that a node that is out of order is alive, thereby losing the data that are sent (Wang *et al.*, 2006:7; Karlof & Wagner, 2003:302).
    - IP address spoofing: Each object has an IP address within a communication network. IP spoofing refers to a technique that attackers use to falsify the return address of a data packet to make it seem as if the data had come from a legitimate node by spoofing the address of that node (Chang, Yoon & Park, 2013:1; Chen & Yeung, 2006:1).
- **Replay attack:** An attacker broadcasts data that have already been sent through the network in order to abuse their authentication sequence at the

moment of data submission. This attack can be used to manipulate the location and the nodes' routing tables (Mejri *et al.*, 2014:62; Rotter, 2008:72).

5.6 UNAUTHORISED ACCESS

Unauthorised access is the viewing of and access to data, information and resources when one has not been granted permission from the legitimate owner to do so. Vulnerabilities in the Internet of Things environment can be abused to gain unauthorised access to data and networks. According to Kumar, Prajapati, Singh and De (2010:920–921), the following commonly known vulnerabilities of data and networks are linked to password access controls:

- No authentication password is used to gain access.
- Even though basic authentication procedures are deployed, the data are transmitted over an unencrypted communication channel.
- A system accepts pre-set default passwords to allow access.

Unauthorised access is linked to following security threats already discussed (Mejri *et al.*, 2014:60):

- The integrity of data is under attack when unauthorised users gain access to data in databases or intercept the data during transmission over a communication channel in order to modify and delete the data. Threats include man-in-the-middle attacks, data loss as well as RFID tag content changes, as discussed in Section 5.2.
- Confidential business information as well as private information of individuals may only be accessed and read by authorised parties who have access rights to it. Threats include eavesdropping, sniffing, smart object tampering and man-in-the-middle attacks, as discussed in sections 5.3 and 5.4.
- Authenticity also includes that all objects in the network must be authenticated before accessing available resources as well as the ability to verify that the sender and receiver objects are who they claim to be. Threats include node impersonation, Sybil attacks, spoofing and replay attacks, as discussed in Section 5.5.

5.7 NETWORK AVAILABILITY

Network availability is the ability of smart objects to access, exchange and retrieve information in a usable form through a network as well as provide an uninterrupted communication channel on which data can move. The importance of network availability is highlighted by the fact that transferred data need to be up to date and recent to provide services and make timely decisions (see Section 5.2) (Matin & Islam, 2012:18; Boritz, 2005:266). Network availability is under threat in the following instances:

- **Jamming:** Jamming is a form of attack where there is interference with the RF that sensor nodes use. A powerful jamming source can disrupt an entire network and less powerful jamming sources may only affect smaller parts of a network. If lesser-powerful jamming sources are strategically distributed in the network, it could also bring the network to a halt and not only disrupt a small part of the network (Farooq *et al.*, 2015:5; Wang *et al.*, 2006:5). The most efficient jamming attacks can be categorised into four types (Wang & Wyglinski, 2011:809):
  - Constant jamming: Repeatedly sends random and worthless signals to the communication channel
  - Deceptive jamming: Repeatedly sends valid data to the communication channel, with no gap between the data being sent
  - Random jamming: Attack is either a constant jamming or a deceptive jamming attack for a random period of time, where the jamming switches off at any given time
  - Reactive jamming: If no data are being transmitted over a communication channel, no jamming attack will take place, but it will interfere with data reception when there is activity on the channel.
- **Selective forwarding:** A selective forwarding attack influences network traffic by assuming that all participating nodes in a network will accurately and reliably forward all the data that they receive. An attacker creates malicious nodes in a network, which selectively forward certain data and simply drop other data instead of forwarding them. Selective forwarding attacks are most effective when the malicious node of the attacker is included in the path of the data flow as well as close to the base station where data are relayed between the

transmitting and receiving nodes. Selective forwarding is made easier through sinkhole attacks (refer to Section 5.2) (Matin & Islam, 2012:19; Wang *et al.*, 2006:7; Karlof & Wagner, 2003:300).

- **Denial of service:** Refer to Section 5.2.

5.8 SEMANTIC LAYER VULNERABILITIES

The semantic layer is capable of extracting knowledge from integrated data gathered by different smart objects in order to provide services (Al-Fuqaha *et al.*, 2015:2352). Old vulnerabilities of the Web reappear in the semantic layer of Internet of Things. With the added flexibility and power of new semantic mechanisms, malicious attackers exploit vulnerabilities in the applications responsible for discovering and using resources, analysing and restructuring information and recognising relevant information that provides a given service (Al-Fuqaha *et al.*, 2015:2352; Orduña, Almeida, Aguilera, Laiseca, López-de-Ipiña & Goiri, 2010).

5.8.1 Semantic query languages

The semantic layer of the Internet of Things is based on various languages to perform its main functions, each with its own unique characteristic. In general, the attack on semantic languages is mostly targeted at the subset of query/update languages, because the query strings of the concatenated user inputs permit the attacker to control the executed query, thereby forcing an unwanted behaviour in the application (Orduña *et al.*, 2010). SPARQL is the most commonly used query language in the Internet of Things. There are three types of query injections that will be associated with SPARQL query language:

- **SPARQL injections:** SPARQL injections are a method used by malicious attackers to gain unauthorised entry to the back end of the database by transmitting SPARQL commands that have not been validated through an application. Attackers manipulate the application command execution by structuring directed queries to gather information in the applications' database (Su & Wassermann, 2006:372; Hotchkies, 2004:3).
- **Blind SPARQL injections:** The query languages used by Internet of Things technologies will use high-level configurations, making it challenging to retrieve information through injection attacks (Orduña *et al.*, 2010). With blind SPARQL

injections, the attacker formulates queries that result in Boolean results by repeatedly querying the database to gather information from it through true and false error messages (Orduña *et al.*, 2010; Hotchkies, 2004:5).

- **SPARUL injections:** SPARUL is an updated version of SPARQL and allows reading as well as writing query capabilities. A new risk is created for modifying and extracting data from the database, as the whole ontology can be altered through queries (Orduña *et al.*, 2010).

5.8.2 Semantic ontology development

Ontologies are the carriers of the meaning contained in the gathered data of Internet of Things. Ontology vocabulary and semantic annotations will have to be developed to be able to understand the meaning of gathered data in order to integrate the information from several sources in order to extract knowledge from it (Benjamins, Contreras, Corcho & Gomez-Perez, 2002:7).

There will always be inefficient knowledge of the subject when a new technology such as ontologies is created, which in turn creates weaknesses due to inexperience with the technology. This will pose an exploitation threat to ontologies, where script writers will take advantage of their vulnerabilities (Bruwer & Rudman, 2015:1048). Vulnerabilities include, but are not limited to, hidden malicious scripts within ontologies as well as gaining unauthorised access to data through the manipulation of ontologies (Bruwer & Rudman, 2015:1048).

5.9 CONCLUSION

Many of the risks identified in this chapter already existed in the separate components of the Internet of Things, but when the components are combined in an Internet of Things environment, new risks will arise due to the addition of new technologies or the combination of technologies. Businesses will be quick to adopt Internet of Things based on the benefits and opportunities that it has, but will fail to recognise the threats associated with it. New controls will need to be adopted in order to address the identified risks. Table 5.2 below shows a risk-technology matrix, where the enabling technologies of Internet of Things identified in Chapter 4 are linked to the relevant threats it gives rise to.

Table 5.2: A risk-technology matrix: linking the enabling technologies of Internet of Things to the relevant threats it gives rise to

		Architecture layers and enabling technologies of the Internet of Things							
		Coding layer (3.2)	Perception layer (3.3)		Network layer (3.4)		Semantic layer (3.5)		
		RFID	Sensors	Smart objects	Transmission mediums	Communication protocols	Data access	Query language	Ontologies
Risks									
5.2 Integrity	Collisions				X				
	Denial of service			X	X		X		
	Man-in-the-middle				X				
	Data loss	X	X	X	X		X		
	Sinkhole				X	X			
	RFID tag content changes	X							
	Masquerading attack			X		X			
	Illusion attack		X						
5.3 & 5.4 Privacy & Confidentialit	People tracking	X	X	X					
	RFID tag cloning	X							
	Eavesdropping				X				
	Sniffing				X				
	Smart object tampering			X					
	Man-in-the-middle				X				
5.5 Authenticity	Collisions				X				
	Node impersonation					X			
	Sybil	X				X			
	GPS spoofing		X						
	Acknowledgement spoofing			X	X				
	IP address spoofing					X			
	Replay attack						X		

		Architecture layers and enabling technologies of the Internet of Things							
		Coding layer (3.2)	Perception layer (3.3)		Network layer (3.4)		Semantic layer (3.5)		
		RFID	Sensors	Smart objects	Transmission mediums	Communication protocols	Data access	Query language	Ontologies
Risks									
5.6 Unauthorised Access	Man-in-the-middle				X				
	Data loss	X	X	X	X		X		
	RFID tag content changes	X							
	Eavesdropping				X				
	Sniffing				X				
	Smart object tampering			X					
	Node impersonation					X			
	Sybil attacks	X				X			
	Spoofing		X	X	X	X			
	Replay attacks						X		
5.7 Network availability	Jamming				X				
	Selective forwarding			X	X				
	Denial-of-service attack				X				
5.8 Semantic layer vulnerabilities	SPARQL injections						X	X	
	Blind SPARQL injections						X	X	
	SPARUL injections						X	X	X
	Ontology development								X

(Source: Author's own)

CHAPTER 6:
SAFEGUARDS AND CONTROLS TO MITIGATE INTERNET OF THINGS RISKS

6.1 INTRODUCTION

The Internet of Things forms a platform for integrating information from various environments. Organisations can generate value through integrated data and recognise information as an asset that needs to be managed and protected (Tarrant *et al.*, 2011:165–167). The amount of information gathered and processed by an organisation will affect the level of control required (Middleton *et al.*, n.d.).

Many of the existing safeguards and controls listed to address risks are inherited from the separate components that make up Internet of Things, but because these components are recombined, with the addition of new technologies, these safeguards and controls need to be revisited in order to manage the risks identified in the previous chapter. The risks can be mitigated through the use of technological and non-technological control measures as well as a policy component. This chapter discusses controls that should be implemented in order to mitigate the risks associated with Internet of Things.

The risks identified in the previous chapter can mostly be linked to the enabling technologies of the perception layer (Section 3.3), network layer (Section 3.4) and semantic layer (Section 3.5) of the Internet of Things' architecture. The controls are mostly centred on 1) protecting a smart object's identity, location and gathered data; 2) ensuring network availability and protecting data transmissions over networks; 3) the development of semantic ontologies; and 4) protecting processed information in databases.

6.2 PERCEPTION LAYER SECURITY

The key technologies of the perception layer in an Internet of Things environment are the RFID and sensor technologies embedded in smart objects. Smart objects with limited capabilities and resources are placed in a network without manual supervision and gather data autonomously on their users and their environment. Due to the smart objects being an important building block for the Internet of Things, the object itself, its data, identity and location need to be protected.

6.2.1 Smart object protection: Physical

Due to smart objects being left unattended most of the time, they are vulnerable to physical attacks by malicious attackers that physically destroy objects as well as environmental destruction by wind, water, sun, etc. Smart objects can physically be protected against this damage with the help of electrostatic screening. This is where a faraday cage constructed of metal will provide protection against destruction as well as block out unauthorised signals in a specific frequency (Li, 2012:375-376).

6.2.2 Smart object protection: Identity and location

Smart objects possess identification capabilities that infringe on the privacy of their users. In addition, the unique frequency between the RFID tag and reader needs to be concealed from unauthorised parties. The following security methods are available to conceal the identity and location of the smart objects in order to ensure that the privacy of Internet of Things users are protected (Li, 2012:375-376; Wang *et al.*, 2006:5; Garfinkel, Juels & Pappu, 2005:40; Juels, Rivest & Szydlo, 2003:104–107):

- **Electrostatic screening:** Refer to Section 6.2.1.
- **Blocker tag:** A blocker tag creates a hostile RF environment for unauthorised RFID readers by sending out a constant frequency range of fake tag numbers, making it incapable of singling out individual tags. The blocker tag prevents unauthorised scanning by attackers, but still allows authorised scanners to proceed normally.
- **Active jamming:** This is where a device actively broadcasts radio signals in order to interfere or interrupt with the operation of any nearby RFID readers, thereby shielding tags from detection.
- **Frequency-hopping Spread Spectrum (FHSS):** This is a method of transmitting signals by rapidly switching between frequency channels using a random sequence known to both the RFID tag and the receiver, thereby preventing an attacker from jamming the frequency being used at any given moment in time.
- **Kill order mechanism:** When a smart object is created for a specific purpose and it has completed its task, an object can be deactivated by sending a command to the object or by physically destroying it. A killed tag will not emit any frequency and can never be re-activated, making it useless to attackers.

6.2.3 Smart object protection: Data

Protection of smart object data refers to the authentication of data-gathering sources; confirming data integrity through their accuracy, completeness and timeliness; and ensuring gathered data are kept private and confidential and that no unauthorised users can gain access to them (refer to sections 5.2–5.6). Data security is challenging to design and develop due to the limited capabilities and resources of smart objects. Data-protection program codes developed to address specific threats can be directly integrated into the smart object design and require minimal user interaction or regulatory enforcement. The following code schemes and security mechanisms are designed to comply with smart object data security requirements (Mejri *et al.*, 2014:63; Garfinkel *et al.*, 2005:40; Pisarsky, 2004:4; Juels *et al.*, 2003:105; Li, 2012:376):

- **Hash-lock protocol:** The hash-lock approach focuses on authenticating the RFID tag with its corresponding reader by locking a tag with a value. Access to the tag can only be granted by the presentation of a personal identification number (PIN) to confirm positive identification of the reader;
- **Re-encryption mechanism:** Encryption is an information-processing algorithm, based on mathematical functions, where a plaintext message is combined with a pre-loaded encryption key embedded in the smart object, which can only be read by deciphering it with a corresponding decryption key. To ensure the integrity of data, smart objects should undergo periodic re-encryption to reduce the possibility of attackers deciphering the decryption key due to frequent data encryption before they are transmitted.
- **Silent tree-walking algorithm:** When multiple RFID tags attempt to communicate with an RFID reader at the same time, the multi-access communication can cause data collisions. The silent tree-walking algorithm supports multi-access communication by providing an access protocol to isolate RFID tag identification numbers from one another.

6.3 NETWORK LAYER SECURITY

The goal of network and data transmittance security is to guarantee the confidentiality, integrity and authenticity of data during the transmission process as well as continuous network availability. To protect the data transmittance in a network, a comprehensive security plan needs to be in place that integrates different security mechanisms.

Integrated security mechanisms include a key-management scheme, secure routing of data, restrictions on the broadcasting range of data, monitoring the network for possible attacks and multipath routing of data.

6.3.1 Key management

The goal of key management is to provide procedures for controlling cryptographic keying material (Fumy & Landrock, 1993:785). Key management is a core mechanism that ensures network security (Sun, Wu, Wu, Li, Zhang, Zhang, Xu & Xiong, 2015:119). Security is provided by distributing the required cryptographic keys to the communicating smart objects and Internet of Things infrastructure prior to communication, enabling them to exchange data securely over a network (Wang *et al.*, 2006:9; Fumy & Landrock, 1993:785). A variety of key types exists and these include, but are not limited to, keys for data privacy and confidentiality, keys for data integrity and keys for authentication (Fumy & Landrock, 1993:786).

Cryptography keys enable users or objects to hide the content of data from all but the intended recipient. According to Mejri *et al.* (2014:63), cryptographic keys can be divided into two categories:

- **Symmetric key cryptography:** In symmetric key cryptography the decryption key is deduced from the encryption key. Security in symmetric cryptography is founded on the principle that the key is kept secret between communication parties.
- **Asymmetric key cryptography:** In asymmetric key cryptography each user and/or object has two keys: one private and one public. The private key is kept secret and the public key is made available to the public. If a message is encrypted with a private key, only the public key can decrypt it and vice versa.

6.3.2 Secure routing of data

In an Internet of Things environment, it is not sufficient to only protect data transmission over a network, it is also important to secure the routing protocols (Zapata, 2002:106). A secure routing protocol should aim to achieve the integrity, authentication and availability of messages in the presence of attackers. Through a proper key-management scheme, all objects in the network are preloaded with the

appropriate keys to achieve the above-mentioned goals before a routing protocol can start (Wang *et al.*, 2006:13).

The following security routing protocols can achieve normal routing functions as well as effectively guard against common routing attacks simultaneously:

- **Secure Ad hoc On-demand Distance Vector (SAODV):** SAODV is a routing protocol that protects the route discovery mechanism of data and makes use of asymmetric key cryptography. The following two mechanisms of SAODV are used to secure messages (Zapata, 2002:107):
  - Digital signatures: It is the digital equivalent of a handwritten signature used to validate data by verifying the sender of the data (Zhou, Zhao, Zhu & Wei, 2006:1503).
  - One-way hash function: It provides a digital fingerprint of a message's contents, ensuring that a message has not been altered by an attacker during transmission (Zhou *et al.*, 2006:1503–1504).
- **Broadcast authentication:** A fundamental security service in a sensor network is broadcast authentication, where the base station is able to broadcast authenticated data to the whole network, enabling the receiving objects to confirm that the received data originated from the claimed sender object as well as that they have not been modified during the transmission. TESLA broadcast authentication protocol uses asymmetric key cryptography and authenticates routing messages through a one-way hash Message Authentication Code (MAC). Combining a MAC key with a message offers secure authentication in point-to-point communication between objects (Wang *et al.*, 2006:14; Hu, Perrig & Johnson, 2005:23).
- **Secure Routing Protocol (SRP):** SRP protects the route discovery by providing a set of diverse paths that enables the sender object to choose an optimal route as well as preloading the sender and receiver objects with appropriate keys to ensure a secure connection between them (Papadimitratos & Haas, 2002:4).

6.3.3 Restrictions on broadcasting range

Because of the way protocols and algorithms are developed, legitimate objects follow the shortest and easiest route to transfer data over a network. In return, malicious objects placed in a network will follow a longer deviated route to transfer data in order to avoid detection. Taking this into account, a fixed broadcasting range to transfer data in a network is set, which is limited to a specific geographical area. Distance-bounding protocols are used to gain knowledge about the distance between an RFID tag embedded in a smart object and a tag reader by means of a time-critical challenge-response mechanism (Peris-Lopez, Hernandez-Castro, Tapiador, Palomar & Van der Lubbe, 2010:46). Distancing-bounding protocols based on cryptographic techniques include the following:

- **Bit commitment:** A bit commitment is a means of requiring an object to commit to a value by sending out a challenge, keeping the value hidden until a later point in time when the corresponding correct answer is sent back to the sender. The timing delay between sending out a challenge bit and receiving back an answer could be determined and used to calculate the distance between the RFID tag and reader (Peris-Lopez *et al.*, 2010:46, 49).
- **Zero-knowledge:** Zero-knowledge is an identification time-verifying protocol where the amount of information transferred between a receiving and a sender object is initially limited because receivers first need to demonstrate their knowledge of an assertion given by senders before all the information can be transferred. Zero-knowledge also calculates the time delay as described in bit commitment (Dwork, Naor & Sahai, 2004:852; Feige, Fiat & Shamir, 1988:77).

6.3.4 Monitoring network for attacks

An intrusion-detection system is software that is an additional security measure for sensor networks and is an automated process that provides protection against internal and external attacks by monitoring the activities occurring in a network or device and analysing them for behaviours that show signs of attack or violation of acceptable use policies or standard security policies (Sun *et al.*, 2015:118; Scarfone & Mell, 2007). Intrusion-detection systems are based on the following classes of methodologies, either separately or integrated, to identify possible attacks (Scarfone & Mell, 2007):

- **Signature-based detection** is where known threat features are compared to monitored activities in the network in order to identify attacks. This methodology is only effective at detecting known threats and ineffective at detecting variations of known threats or unknown threats.
- **Anomaly-based detection** compares predefined activities that are considered normal for a network against its monitored activities in order to identify attacks through deviations from the norm. Activities considered normal are developed over a period by observing the characteristics of typical activities in a network.
- **Stateful protocol analysis** provides more accurate detection information than signature-based and anomaly-based detection by comparing predetermined universally accepted definitions of protocol activities for each protocol state against monitored activities in a network, thereby identifying any deviations from the norm. It differs from anomaly-based detection by focusing on universal protocol profiles and not on network-specific profiles.

The following intrusion-detection solutions are also available (Sun *et al.*, 2015:118; Wang *et al.*, 2006:18–19):

- **Honeypot:** Honeypots are designed to assist other security mechanisms by operating as a normal computing system resource to be probed, attacked or compromised by attackers. A honeypot's goal is to distract the attention of attackers from the critical system resources in order to analyse their behaviours, thereby creating threat signatures for intrusion-detection systems. The real network services and data are protected by the honeypot that absorbs the damage and logs the attack data.
- **Interleaved Hop-by-hop authentication scheme (IHOP):** IHOP ensures that the base station, which relays data, can detect injected false data from compromised objects. To guarantee that false data are identified, the sensor network has to have a structured hierarchy through which data will flow, where each object in the network needs to be authenticated with message authentication codes (MACs). If an object in the network cannot be authenticated through its MAC, it is assumed that the object is compromised and injecting false data in the network.

- **Statistical En-route Filtering mechanism (SEF):** Through the SEF mechanism, false data can be detected and dropped through the MACs of objects. An object will collect and summarise the results of a detected activity in a report and broadcast the report to all detecting objects. If the other objects agree with the report, they will broadcast their pre-installed MAC to all objects in their network and en-route objects will receive multiple MACs, thereby verifying the probable correctness of the MACs and dropping the objects with invalid MACs immediately from the network.
- **Intrusion-tolerant routing in wireless sensor network (INSENS):** INSENS is a routing protocol where the base station generates the forward routing table of data, which is constructed from the collected network topology information received from the objects in the network. Data may only flow through the network according to the approved routing table generated by the base station. If data are routed through another, unapproved routing table, it will indicate a possible threat.

6.3.5 Multipath routing of data

Multipath routing is the creation of multiple paths for dataflow between smart objects, databases and the semantic layer in a network. By sending multiple copies of data along different paths in a network, an alternative path will be available between the sender and receiver if the shortest path has a failure. Multipath routing will address isolated object failures where only a single object in a network failed as well a cluster failure where numerous objects simultaneously failed in a fixed radius. Multipath routing divides the network traffic across multiple paths, thereby splitting the energy consumption across objects in a network, leading to a longer lifespan of objects. By sending duplicate data along different paths, the likelihood of reliable data delivery increases (Ganesan, Govindan, Shenker & Estrin, 2001:10–13). Two types of multipath structures will provide greater resilience in the presence of network failures (Ganesan *et al.*, 2001:10–14):

- **Disjoint multipath:** This consists of a small number of alternative paths that are connected with the main path, as well as with one another. Data will be able to flow through the alternative path in cases where the main path has failed, as

they are unaffected by it, but the alternative route will be less desirable due to its longer response time.

- **Braided multipath:** This consists of several partially disjoint multipath schemes. The braided multipath need not circumvent the main path as in the disjoint multipath scheme, as each object on the main path will find the best possible path for dataflow through the several partially disjoint multipath schemes as well as main path, thereby excluding the failed object from the route.

6.4 SEMANTIC LAYER SECURITY

The semantic layer consists of a wide variety of enabling technologies, and it is vital to maximise security mechanisms in the semantic environment, which is lacking in security mechanisms on which businesses have relied in the past for security assessment. It is imperative that businesses communicate their security information in a transparent and concise way so that its meaning is unambiguous (Kagal, Finin & Joshi, 2003:3). The risks associated with businesses relying on third party cloud computing resources, the developing of new ontologies and the structuring of a security policy language need to be addressed.

6.4.1 Data analysis and storage

The large quantities of data gathered by devices and smart objects require big storage spaces and additional processing power to be analysed (Farooq *et al.*, 2015:3–4). Cloud computing provides the virtual infrastructure that Internet of Things needs and is the only intelligent technology available to integrate its smart objects, storage spaces, analysing tools, visualisation platforms and service delivery. Cloud computing enables end-to-end service delivery for businesses to access applications on demand from anywhere (Gubbi *et al.*, 2013:1645).

It is economically beneficial for businesses to make use of service providers to provide cloud computing resources. To address the risks associated with businesses relying on third parties for important business functions, the following needs to be in place:

- **Service provider agreement:** According to Mirobi and Arockiam (2015:753–756), a service provider agreement is an agreement between the cloud

computing provider and the business (consumer), stipulating both parties' involvement as well as the method for measuring, monitoring and reporting on the usage of the cloud computing resources. The agreement should also include the following:

  - Availability of resources: This entails ensuring that a resource is available for the agreed level of functional performance at a given period, thereby limiting downtime of the resource to provide a continuous service.
  - Confidentiality of business information: This implies that security measures must be in place to ensure that only authorised users have access rights, right to use and modification privileges to information (Kandukuri & Rakshit, 2009:519).
  - Privacy of personal information: Information must be categorised as private and personal in the database, with security measures in place to ensure access and use only by authorised users. A detailed explanation, entailing the purpose of the information as well as a description of the compilation procedures to ensure the accuracy of information, should be stipulated (Kandukuri & Rakshit, 2009:519).

- **Disaster-recovery plan:** A disaster-recovery plan, also referred to as a business continuity plan, describes how a business will minimise the effect of a cloud failure or a service provider going out of business, enabling the business to maintain or quickly resume critical operations (Bidgoli, 2015:91).
- **Backups:** Regular backups of all business and financial information should be made and stored at a secure location (Bidgoli, 2015:91).

6.4.2 Design methodologies of developers

Designers must be made aware of any risks or challenges before they start developing semantic ontologies. The three challenges that needs to be addressed in order to manage the risks with regard to the development of semantic ontologies are as follows:

- Constructing of kernel ontologies for all domains to act as a common unified top-level dictionary
- Providing methodical and technological support for the ontology development process, focusing on the following:

  - Conceptual modelling and ontology coding of new semantic layer languages
  - Seamless alignment, mapping and integration of existing ontologies with new ontologies
  - Ontology tools for re-engineering and consistency checking, if existing ontologies are to be used.
- Configuration management in order to govern the different versions of ontologies, as well as the interdependencies between the ontologies and annotations (Benjamins *et al.*, 2002:8).

Technical solutions to address risks must be integrated into the design of the ontology during the development stage to ensure the secure and accurate execution of ontologies.

6.4.3 Structuring a semantic policy language

Kagal *et al.* (2003:6–10) recommend that every business should implement a distributed policy-management approach through the use of a semantic policy language. The semantic policy language will be based on ontologies written with the specific security and privacy requirements of the business in mind, and will require domain-independent ontologies as well as specific domain ontologies. The composition of ontologies to create the policy language should include the following four aspects:

- **Representation of actions and conditions:** Representing data gathered by the smart objects through the contextualising of the information, thereby providing a better understanding of the smart object data and their parameters
- **Modelling speech acts:** Focuses on decentralising security control as well enabling policies to be more adaptive to real-time changes of delegating, revoking, cancelling and requesting access rights to Internet of Things resources
- **Meta-policies:** Policies on how policies are interpreted, including resolving conflicts between more than one applicable policy, by selecting the one that enjoys priority

- **Policy engine:** Interprets and reasons over policy ontologies, associated speech acts and domain information in order to make decisions about applicable rights, exclusions, responsibilities and allowances.

6.5 TRAINING AND AWARENESS ABOUT EMERGING RISKS

Many of the identified risks associated with the Internet of Things are directly correlated with a lack of knowledge of the technology. The development of new technology always coincides with new unknown risks, and developers as well as businesses must be made aware and educated about possible risks.

According to Aldossary and Zeki (2015:256–257) as well as Heath, Domingue and Shabajee (2006:9–14), users and developers must be educated on the technologies and risks associated with a new technology such as the Internet of Things. Technology and risk education, addressed through continuous long-term learning and maintenance workshops, should include technical understanding, identifying potential threats, laws and regulations, as well as policies and expectations relating to the privacy of personal information. It is essential for users to be educated on the key safeguards associated with the adoption of Internet of Things technologies, which includes, but are not limited to, refraining from interacting with suspicious objects and information as well as using security features embedded in the underlying infrastructure. A joint partnership should be formed between users and developers to guarantee that technical solutions are implemented, including developers assisting users in ensuring ease of use of smart objects and user-friendly database interfaces.

6.6 POLICY, GUIDELINES AND LEGISLATION CONTROLLING USE

In addition to technical solutions, it is necessary to also address threats through policies, guidelines and legislation (Garfinkel *et al.*, 2005:41). Adequate policy and legislation documents need to be developed, including their implementation guidelines, which take the underlying technology into account. These documents should be easily adjustable and created according to the specific needs of the private business sector. The contents of the policies and legislation must support businesses' strategic objectives and make reference to information rights; provisions prohibiting, restricting or supporting the use of Internet of Things mechanisms; IT-security rules; compliance with regulatory governance; and the establishment of a task force doing

research on the risks and safeguards associated with the Internet of Things (Weber, 2010:23).

To ensure that users of all levels in a business accept the legislation and policies, top management should inspire a positive continuous commitment in accepting rather than merely describing them. Users should be provided with training in a clear and non-technical manner on all the applicable written as well as automated policies (refer to Section 6.4.3) and legislation, including guidelines for implementing them (Singh, 2010:2).

6.7 CONCLUSION

When considering the adoption of Internet of Things in a business environment, business leaders will be eager to accept the new technology based on the prospects it may offer. New risks will arise with the acceptance of Internet of Things and will not be taken into account by business leaders when deciding on the new technology. The risks associated with the adoption of Internet of Things as stated in Chapter 5 will be mitigated to an acceptable level by implementing the controls stipulated in Chapter 6. Table 6.1 is a risk-control matrix for the Internet of Things. The table links the significant threats to the relevant mitigating safeguards and controls. The threats will only be addressed once in the table below, even if they are present in more than one risk category (refer to Table 5.1).

Table 6.1: Risk-control matrix for the Internet of Things

Controls and safeguards				Significant threats in their security risk categories																											
				5.2 Data integrity										5.3 & 5.4 Data privacy & confidentiality					5.5 Authenticity						5.7 Network availability		5.8 Semantic layer vulnerabilities			
				Collisions	DOS: Network	DOS: Smart objects	DOS: Data storage	Man-in-the-middle	Data loss	Sinkhole	RFID tag content changes	Masquerading attack	Illusion attack	People tracking	RFID tag cloning	Eavesdropping	Sniffing	Smart object tampering	Node impersonation	Sybil	GPS spoofing	Acknowledgement spoofing	IP address spoofing	Replay attack	Jamming	Selective forwarding	SPARQL injections	Blind SPARQL injections	SPARUL injections	Ontology development
	6.2 Perception layer security (smart objects)	6.2.1 Physical	Electrostatic screening						X					X																	
		6.2.2 Location & Identity	Electrostatic screening								X			X				X													
			Blocker tag								X			X												X					
			Active jamming								X			X																	
			FHSS																							X					
			Kill order								X			X	X																
		6.2.3 Data	Hash lock protocol			X						X	X		X																
			Re-encryption mechanisms													X	X															
			Silent tree-walking algorithm	X																												
	6.3 Network layer security	6.3.1 Key management	Symmetric key cryptography													X	X															
			Asymmetric key cryptography		X	X	X	X		X		X				X	X			X	X	X		X								

Controls and safeguards				Significant threats in their security risk categories																											
				5.2 Data integrity										5.3 & 5.4 Data privacy & confidentiality					5.5 Authenticity						5.7 Network availability		5.8 Semantic layer vulnerabilities			
				Collisions	DOS: Network	DOS: Smart objects	DOS: Data storage	Man-in-the-middle	Data loss	Sinkhole	RFID tag content changes	Masquerading attack	Illusion attack	People tracking	RFID tag cloning	Eavesdropping	Sniffing	Smart object tampering	Node impersonation	Sybil	GPS spoofing	Acknowledgement spoofing	IP address spoofing	Replay attack	Jamming	Selective forwarding	SPARQL injections	Blind SPARQL injections	SPARUL injections	Ontology development
	6.3 Network layer security	6.3.2 Secure data routing	Digital signatures		X	X	X	X		X		X								X	X		X							
			One-way hash function					X		X						X				X											
			Broadcast authentication		X	X	X	X		X		X								X		X		X							
			SRP							X																					
		6.3.3 Broadcasting range restrictions	Bit commitment			X				X			X						X	X	X		X								
			Zero-knowledge					X		X			X						X	X			X	X							
		6.3.4 Network monitoring	Honeypot		X		X																		X	X					
			IHOP		X								X						X	X	X	X	X								
			SEF										X						X	X		X	X								
			INSENS		X					X																X					
		6.3.5 Multipath routing	Disjoint multipath	X																						X					
			Braided multipath	X																						X					

				Significant threats in their security risk categories																											
				5.2 Data integrity										5.3 & 5.4 Data privacy & confidentiality					5.5 Authenticity						5.7 Network availability		5.8 Semantic layer vulnerabilities			
				Collisions	DOS: Network	DOS: Smart objects	DOS: Data storage	Man-in-the-middle	Data loss	Sinkhole	RFID tag content changes	Masquerading attack	Illusion attack	People tracking	RFID tag cloning	Eavesdropping	Sniffing	Smart object tampering	Node impersonation	Sybil	GPS spoofing	Acknowledgement spoofing	IP address spoofing	Replay attack	Jamming	Selective forwarding	SPARQL injections	Blind SPARQL injections	SPARUL injections	Ontology development
Controls and safeguards	**6.4 Semantic layer security**	**6.4.1 Data analysis and storage**	Service provider agreement						X					X																
			Disaster-recovery plan						X																						
			Backups						X																						
		6.4.2 Design methodologies of developers																													X
		6.4.3 Structuring a semantic policy language		X	X	X	X	X		X		X	X	X		X	X		X	X	X	X	X	X	X	X	X	X	X		
	6.5 Training and awareness about emerging risks			X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
	6.6 Policy, guidelines and legislation controlling use			X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X

(Source: Author's own)

CHAPTER 7:
CONCLUSION

Modern businesses need to keep up with the continuous evolving of technology to ensure that business goals set by management are supported and achieved. They also recognised information as an important asset that needs to be managed and protected. The deployment of Internet of Things technologies will improve the quality of business operations and create new business opportunities that will assist businesses in achieving their goals and add additional value to information by integrating relevant data from various sources.

Due to the benefits that Internet of Things promises, businesses are eager to adopt Internet of Things in their operations, without fully understanding its enabling technologies and their functions. This will result in risks associated with Internet of Things technologies not being identified. When investigating the impact and benefits of these technologies on operations, businesses should also identify the risks that they create and implement controls to mitigate these risks to an acceptable level.

The concept of Internet of Things and its enabling technologies need to be understood by businesses in order for them to identify risks associated with the technologies as well as how it is applied to operations. A six-layered architecture with the categorised enabling technologies of Internet of Things was compiled. The research found that Internet of Things consists of compilation of new and existing technologies that revolves around three core technology components:

- **Smart objects:** These uniquely identifiable objects are the key enablers of Internet of Things. They gather data, through embedded sensors, on their surrounding environment as well as carry out any necessary instructions, thereby creating a platform to assess, create, process and share Internet of Things information.
- **Wireless networks:** The functioning of Internet of Things relies mostly on wireless networks to transfer gathered data and analysed information in real time over networks with communication protocols.

- **Semantic technologies:** These technologies have the capability to discover and use resources as well as analyse, restructure and recognise relevant gathered data of objects in order to provide specific services or send instructions to objects.

Research was conducted on the impact that these enabling technologies have on the automotive, transport, retail, healthcare, pharmaceutical, advertising and marketing, telecommunication, education, agriculture as well as supply chain management, logistics and manufacturing industries. It was found that most manual business operations were converted into autonomous operations by:

- tracking an object's location;
- authentically identifying an individual object;
- monitoring environments with sensors;
- gathering information on the location, identity and environment of an object;
- making deductions from analysed gathered information; and
- autonomously making decisions and giving instructions based on the deductions made.

This leads to increased business productivity, market differentiation, cost reduction and higher-quality information.

The opportunities created with the deployment of Internet of Things in business environments are accompanied by risks directly linked to the enabling technologies. COBIT 5 was used as an IT governance framework to identify the risks associated with Internet of Things technologies and control procedures to address these risks appropriately. The following risks were identified with regards to the applicable COBIT 5 process and the related enabling technologies of Internet of Things:

- **Data security:** The integrity, privacy, confidentiality and authenticity of data are compromised by collisions, denial of service attack, sinkhole, masquerading attack, illusion attack, people tracking and RFID tag cloning. Data security are also compromised by attackers gaining unauthorised access to data through man-in-the-middle attacks, data loss, RFID tag content changes, eavesdropping, sniffing, smart object tampering, node impersonation, Sybil attacks, spoofing and replay attacks.

- **Network availability:** Real-time data transference for timely decision-making is hampered due to the network being interrupted by jamming, selective forwarding and denial-of-service.
- **Semantic vulnerabilities:** A lack of knowledge of new Web ontologies and languages increases the probability that technology weaknesses are exploited through malicious script, unauthorised access to information and SPARQL injections.

A multi-layered approach of technical and non-technical controls needs to be implemented by businesses before Internet of Things technologies can be deployed in operations to ensure that risks associated with the technologies are mitigated to an acceptable level. This approach includes the following:

- A policy, guidelines and legislation controlling the use of the technologies should be implemented that allocate responsibility to users and stipulate their expected actions when using Internet of Things technologies.
- Non-technical controls include formulating a service provider agreement with third parties, formulating a disaster-recovery plan, making regular backups of information as well as educating users and developers on the risks associated with Internet of Things technologies.
- Technical controls include physical and logical access controls, encryption, cryptography techniques, network monitoring, multipath data routing and structuring a semantic policy language based on the specific security needs of the business.

The research showed that it is important for businesses to understand the underlying architecture of any new technology in order to determine its impact on current business operations and possible new opportunities that they create. After gaining knowledge of the enabling technologies of the Internet of Things, businesses need to identify risks associated with the implementation of these technologies in business operations and implement controls to mitigate risks to an acceptable level.

Because the full deployment of Internet of Things technologies in business environments are still in the beginning stage, the opportunities for future research are

infinite. Current technologies make the Internet of Things concept feasible, but the scalability, interoperability and efficiency of technologies still remain a problem. Given the interest shown by business industries in Internet of Things applications, addressing these issues will be a powerful driving force behind future research. Further research is needed on the enabling technologies of Internet of Things in order for it to operate on a global scale and includes, but are not limited to, managing and cross-referencing multiple identifiers of the same object or location, semantic-based discovery of objects and solutions to effectively support mobility of billions of smart objects. Research should also focus on the ownership and control exercised over the vast amount of data gathered and processed in an Internet of Things environment.

References

Agrawal, S. & Das, M.L. 2011. Internet of Things: A paradigm shift of future Internet applications. *2011 Nirma University International Conference on Engineering*, 8–10 December, 1–7, Achmedabad, Nirma University. Available at: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6153246&tag=1 [accessed 19 July 2016].

Aldossary, A.A. & Zeki, A.M. 2015. Web user's knowledge and their behaviour towards security threats and vulnerabilities. *2015 4th International Conference on Advanced Computer Science Applications and Technologies (ACSAT)*, 8–10 December, 256–260, Kuala Lumpur, Malaysia. Available at: http://ieeexplore.ieee.org/document/7478754/ [accessed 30 October 2016].

Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M. & Ayyash, M. 2015. Internet of Things: A survey on enabling technologies, protocols, and applications. *IEEE Communications Surveys & Tutorials*, 17(4):2347–2376. Available at: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=7123563 [accessed 1 July 2015].

Ali, N.A. & Abu-Elkheir, M. 2015. Internet of nano-things healthcare applications: Requirements, opportunities, and challenges. *2015 IEEE 11th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, 19–21 October, 9–14, Abu Dhabi, United Arab Emirates. Available at: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=7347934 [accessed 19 July 2016].

Aris, I.B., Sahbusdin, R.K.Z. & Amin, A.F.M. 2015. Impacts of IoT and big data to automotive industry. *2015 10th Asian Control Conference (ASCC)*, 31 May – 3 June, 1–5, Kota Kinabalu, Malaysia. Available at: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=7244878 [accessed 19 July 2016].

Asghar, M.H., Negi, A. & Mohammadzadeh, N. 2015. Principle application and vision in Internet of Things (IoT). *2015 International Conference on Computing, Communication & Automation (ICCCA)*, 15–16 May, 427–431, Uttar Pradesh, India. Available at:

http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=7148413 [accessed 19 July 2016].

Ashktorab, V. & Taghizadeh, S.R. 2012. Security threats and countermeasures in cloud computing. *International Journal of Application or Innovation in Engineering & Management (IJAIEM)*, 1(2):234–245. Available at: http://www.ijaiem.org/volume1Issue2/IJAIEM-2012-11-3-076.pdf [accessed 24 May 2016].

Atzori, L., Iera, A. & Morabito, G. 2010. The Internet of Things: A survey. *Computer Networks*, 54(15):2787–2805. Available at: http://www.sciencedirect.com.ez.sun.ac.za/science/article/pii/S1389128610001568 [accessed 26 May 2015].

Bandyopadhyayy, D. & Sen, J. 2011. Internet of things: Applications and challenges in technology and standardization. *Wireless Personal Communications,* 58(1):49–69. Available at: http://link.springer.com/article/10.1007/s11277-011-0288-5 [accessed 23 June 2015].

Barnaghi, P., Wang, W., Henson, C. & Taylor, K. 2012. Semantics for the Internet of Things: Early progress and back to the future. *International Journal on Semantic Web and Information Systems (IJSWIS)*, 8(1):1–21. Available at: http://go.galegroup.com.ez.sun.ac.za/ps/i.do?ty=as&v=2.1&u=27uos&it=search&s=RELEVANCE&p=AONE&qt=SP~1~~IU~1~~SN~1552-6283~~VO~8&lm=DA~120120000&sw=w&authCount=1 [accessed 8 July 2015].

Benjamins, R., Contreras, J., Corcho, O. & Gomez-Perez, A. 2002. Six challenges for the semantic Web. *Intelligent Software Components: Intelligent Software for the Networked Economy (iSOCO)*. White paper, 1–15. Available at: http://oa.upm.es/5668/1/Workshop06.KRR2002.pdf [accessed 27 May 2016].

Bidgoli, H. 2015. *MIS²*. Boston, MA: Cengage Learning.

Bojan, T.M., Kumar, U.R. & Bojan, V.M. 2014. An internet of things based intelligent transportation system. *2014 IEEE International Conference on Vehicular Electronics and Safety (ICVES)*, 16–17 December, 174–179, Hyderabad, India. Available at: http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=7063743&url=http%3A

%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D7063743 [accessed 30 July 2016].

Boritz, J.E. 2005. IS practitioners' views on core concepts of information integrity. *International Journal of Accounting Information Systems*, 6(4):260–279. Available at: http://www.sciencedirect.com/science/article/pii/S1467089505000473 [accessed 11 April 2016].

Brisebois, R., Boyd, G. & Shadid, Z. 2007. What is IT governance and why is it important? *5th Performance Seminar of the INTOSAI IT Standing Committee*, 3 March, 1–8, Muscat, Oman. Available at: http://www.intosaiitaudit.org/muscat/Canada-E_Governance.pdf [accessed 7 January 2016].

Britz, J.J. 2010. *Technology as a threat to privacy: Ethical challenges to the information profession*. Research paper. University of Pretoria, Pretoria. Available at: http://web.simmons.edu/~chen/nit/NIT'96/96-025-Britz.html [accessed 30 May 2016].

Bruwer, R. & Rudman, R. 2015. Web 3.0: Governance, risks and safeguards. *Journal of Applied Business Researc*h, 31(3):1037–1056. Available at: http://search.proquest.com/openview/e279f7eb6bb41f72d29c24e3e815a78b/1?pq-origsite=gscholar [accessed 11 October 2016].

Carriedo, F. & Beltrán, M. 2015. Mobile cloud computing to provide Mobiquity as a service on telecommunication vertical clouds. *2015 3rd IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud)*, 30 March – 3 April, 211–220, San Francisco, CA. Available at: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=7130889 [accessed 19 July 2016].

Chan, H. & Perrig, A. 2003. Security and privacy in sensor networks. *Computer*, 36(10):103–105. Available at: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1236475 [accessed 27 January 2016].

Chang, Y.H., Yoon, K.B. & Park, D.W. 2013. A study on the IP spoofing attack through proxy server and defense thereof. *2013 International Conference on Information Science and Applications (ICISA)*, 24–26 June, 1–3, Suwon, Korea. Available at:

http://ieeexplore.ieee.org.ez.sun.ac.za/stamp/stamp.jsp?tp=&arnumber=6579417 [accessed 26 May 2016].

Chen, W. & Yeung, D.Y. 2006. Defending against TCP SYN flooding attacks under different types of IP spoofing. *International Conference on Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies (ICN/ICONS/MCL 2006)*, 1–6 April, 38–38, Morne, Mauritius. Available at: http://ieeexplore.ieee.org/document/1628284/ [accessed 26 May 2016].

Chunli, L. 2012. Intelligent transportation based on the internet of things. *2012 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet)*, 21–23 April, 360–362, Yichang, China Available at: http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=6201865&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D6201865 [accessed 30 July 2016].

Cisco. N.d. *What is a wireless network? The basics.* Available at: http://www.cisco.com/cisco/web/solutions/small_business/resource_center/articles/work_from_anywhere/what_is_a_wireless_network/index.html [accessed 2 July 2015].

CNRFID. N.d.(a). *Features of RFID tags*. French National RFID Centre (CNRFID). Available at: http://www.centrenational-rfid.com/features-of-rfid-tags-article-19-gb-ruid-202.html [accessed 24 June 2015].

CNRFID. N.d.(b). *RFID system technology*. French National RFID Centre (CNRFID). Available at: http://www.centrenational-rfid.com/rfid-system-technology-article-17-gb-ruid-202.html [accessed 24 June 2015].

Compton, M., Barnaghi, P., Bermudez, L., García-Castro, R., Corcho, O., Cox, S., Graybeal, J., Hauswirth, M., Henson, C., Herzog, A., Huang, V., Janowicz, K., Kelsey, W., Le Phuoc, D., Lefort, L., Leggieri, M., Neuhaus, H., Nikolov, A., Page, K., Passant, A., Sheth, A. & Taylor, K. 2012. The SSN ontology of the W3C semantic sensor network incubator group. *Web Semantics: Science, Services and Agents on the World Wide Web*, 17:25–32. Available at: http://www.sciencedirect.com.ez.sun.ac.za/science/article/pii/S1570826812000571 [accessed 9 July 2015].

Da Xu, L., He, W. & Li, S. 2014. Internet of things in industries: A survey. *IEEE Transactions on Industrial Informatics*, 10(4):2233–2243. Available at:

https://www.researchgate.net/profile/Wu_He2/publication/270742269_Internet_of_Things_in_Industries_A_Survey/links/55fc355a08aec948c4b189f6.pdf [accessed 29 September 2016].

Dwork, C., Naor, M. & Sahai, A. 2004. Concurrent zero-knowledge. *Journal of the ACM (JACM)*, 51(6):851–898. Available at: http://web.cs.ucla.edu/~sahai/work/web/2004%20Publications/J.ACM2004.pdf [accessed 13 June 2016].

EngineersGarage. N.d. *Sensors: Different types of sensors*. Available at: http://www.engineersgarage.com/articles/sensors# [accessed 25 June 2015].

Farooq, M.U., Waseem, M., Mazhar, S., Khairi, A. & Kamal, T. 2015. A review on Internet of Things (IoT). *International Journal of Computer Applications*, 113(1):1–7. Available at: http://www.academia.edu/11498044/A_Review_on_Internet_of_Things_IoT_ [accessed 25 May 2015].

Feige, U., Fiat, A. & Shamir, A. 1988. Zero-knowledge proofs of identity. *Journal of Cryptology,* 1(2):77–94. Available at: http://crypto.cs.mcgill.ca/~crepeau/COMP647/2010/TOPIC03/FFS88.pdf [accessed 13 June 2016].

Fumy, W. & Landrock, P. 1993. Principles of key management. *IEEE Journal on selected areas in communications*, 11(5):785–793. Available at: http://ieeexplore.ieee.org/document/223881/?arnumber=223881&tag=1 [accessed 13 October 2016].

Ganesan, D., Govindan, R., Shenker, S. & Estrin, D. 2001. Highly-resilient, energy-efficient multipath routing in wireless sensor networks. *ACM SIGMOBILE Mobile Computing and Communications Review*, 5(4):10–24. Available at: http://dl.acm.org/citation.cfm?id=509514 [accessed 8 June 2016].

Garfinkel, S.L., Juels, A. & Pappu, R. 2005. RFID privacy: An overview of problems and proposed solutions. *IEEE Symposium on Security & Privacy*, 8–11 May, 34–43, Oakland, CA. Available at: https://www.cs.colorado.edu/~rhan/CSCI_7143_001_Fall_2002/Papers/rfid_security_01439500.pdf [accessed 8 June 2016].

Ghaleb, F., Daoud, S., Hasna, A., ALJa'am, J.M., El-Seoud, S.A. & El-Sofany, H. 2006. E-learning model based on semantic web technology. *International Journal of Computing & Information Sciences*, 4(2):63–71. Available at:

https://www.researchgate.net/profile/Fayed_Ghaleb/publication/228853216_E-Learning_Model_Based_On_Semantic_Web_Technology/links/00b7d51660071b9d65000000.pdf [accessed 6 August 2016].

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. Available at: http://www.sciencedirect.com/science/article/pii/S0167739X13000241 [accessed 29 June 2015].

Guerrero-ibanez, J.A., Zeadally, S. & Contreras-Castillo, J. 2015. Integration challenges of intelligent transportation systems with connected vehicle, cloud computing, and internet of things technologies. *IEEE Wireless Communications*, 22(6):122–128. Available at: http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=7368833&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D7368833 [accessed 30 July 2016].

Guldentops, E. 2002. Governing information technology through COBIT. *Integrity, Internal Control and Security in Information Systems,* 83:115–159. Available at: http://www.researchgate.net/profile/Erik_Beulen/publication/243443857_Governance_in_IT_Outsourcing_Partnerships/links/54d0a69c0cf20323c2185774.pdf#page=282 [accessed 29 July 2015].

Hardy, G. 2006. Using IT governance and COBIT to deliver value with IT and respond to legal, regulatory and compliance challenges. *Information Security Technical Report*, 11(1):55–61. Available at: http://www.sciencedirect.com/science/article/pii/S1363412705000774 [accessed 7 January 2016].

Heath, T., Domingue, J. & Shabajee, P. 2006. User interaction and uptake challenges to successfully deploying semantic web technologies. *Proceedings of the 3rd International Semantic Web User Interaction Workshop (SWUI2006),* 6 November, 1-15, Athens, GA. Available at: http://oro.open.ac.uk/23129/ [accessed 30 October 2016].

Hotchkies, C. 2004. Blind SQL injections automation techniques. *Black Hat Briefings USA*, 23 July – 1 August, 1–48, Las Vegas, NV. Available at: http://www.sachin0631.0fees.net/sqlinjection.pdf [accessed 27 May 2016].

Hu, Y.C., Perrig, A. & Johnson, D.B. 2005. Ariadne: A secure on-demand routing protocol for ad hoc networks. *Wireless Networks*, 11(1/2):21–38. Available at: https://www.cs.rice.edu/~dbj/pubs/winet-ariadne.pdf [accessed 10 June 2016].

Impinj. N.d. *The different types of RFID systems*. Available at: http://www.impinj.com/resources/about-rfid/the-different-types-of-rfid-systems/ [accessed 14 July 2015].

Internet World Stats. 2014. *Internet usage statistic*. Available at: http://www.internetworldstats.com/stats.htm [accessed 25 May 2015].

IODSA (Institute of Directors Southern Africa). 2009. *King Code of Governance for South Africa 2009.* South Africa.

ISACA (Information Systems Audit and Control Association). 2012a. *COBIT 5: A business framework for the governance of enterprise IT*. Rolling Meadows, IL.

ISACA (Information Systems Audit and Control Association). 2012b. *COBIT 5: Process reference guide*. Rolling Meadows, IL.

Janitor, J. 2011. Borderless education with high speed networks. *2011 9th International Conference on Emerging eLearning Technologies and Applications (ICETA)*, 27–28 October, 89–94, Stara Lesna, Slovakia. Available at: http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=6112592&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D6112592 [accessed 6 August 2016].

Jara, A.J., Belchi, F.J., Alcolea, A.F., Santa, J., Zamora-Izquierdo, M.A. & Gómez-Skarmeta, A.F. 2010. A pharmaceutical intelligent information system to detect allergies and adverse drugs reactions based on internet of things. *2010 8th IEEE International Conference* on *Pervasive Computing and Communications Workshops (PERCOM Workshops)*, 29 March – 2 April, 809–812, Mannheim, Germany. Available at: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5470547 [accessed 19 July 2016].

Jara, A.J., Ladid, L. & Skarmeta, A. 2013. The Internet of Everything through IPv6: An analysis of challenges, solutions and opportunities. *Journal of Wireless Mobile*

Networks, Ubiquitous Computing, and Dependable Applications, 4(3):97–118. Available at: http://ipv6forum.com/iot/images/jowua-v4n3-6.pdf [accessed 1 June 2015].

Jara, A.J., Varakliotis, S., Skarmeta, A.F. & Kirstein, P. 2014. Extending the Internet of Things to the future Internet through IPv6 support. *Mobile Information Systems*, 10(1):3–17. Available at: http://www.hindawi.com/journals/misy/2014/831974/abs/ [accessed 1 June 2015].

Juels, A., Rivest, R.L. & Szydlo, M. 2003. The blocker tag: Selective blocking of RFID tags for consumer privacy. *Proceedings of the 10th ACM Conference on Computer and Communications Security*, 27–31 October, 103–111, Washington, DC. Available at: https://impact.asu.edu/~mcn/cse494fa05/Juels03.pdf [accessed 8 June 2016].

Kagal, L., Finin, T. & Joshi, A. 2003. A policy based approach to security for the semantic Web. *2nd International Semantic Web Conference (ISWC2003)*, 20–23 October, 1–17, Sanibel Island, FL. Available at: http://www.csee.umbc.edu/~finin/papers/papers/iswc03b.pdf [accessed 27 June 2016].

Kandukuri, B.R. & Rakshit, A. 2009. Cloud security issues. *IEEE International Conference* on *Services Computing (SCC'09)*, 21–25 September, 517–520, Bangalore, India. Available at: http://ieeexplore.ieee.org/document/5283911/?arnumber=5283911 [accessed 13 October 2016].

Karlof, C. & Wagner, D. 2003. Secure routing in wireless sensor networks: Attacks and countermeasures. *Ad Hoc Networks*, 1(2):293–315. Available at: http://users.eecs.northwestern.edu/~peters/references/SecureRoutingKarlof03.pdf [accessed 23 May 2016].

Karygiannis, T. & Owens, L. 2002. Wireless network security. *National Institute of Standards and Technology: Special publication*, November, 800(48):1–5. Available at: http://www.pajhohesh.ir/e-books-m-biabani/computer-en/01.pdf [accessed 27 January 2016].

Ko, J., Terzis, A., Dawson-Haggerty, S., Culler, D.E., Hui, J.W. & Levis, P. 2011. Connecting low-power and lossy networks to the internet. *IEEE Communications Magazine*, April, 49(4):96–101. Available at:

http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5741163&tag=1 [accessed 7 July 2015].

Koper, R. 2004. Use of the semantic Web to solve some basic problems in education: Increase flexible, distributed lifelong learning; decrease teacher's workload. *Journal of Interactive Media in Education*, 2004(1):1–16. Available at: http://jime.open.ac.uk/articles/10.5334/2004-6-koper/ [accessed 6 August 2016].

Kortuem, G., Kawsar, F., Fitton, D. & Sundramoorthy, V. 2010. Smart objects as building blocks for the internet of things. *IEEE Internet Computing*, 14(1):44–51. Available at: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5342399 [accessed 25 June 2015].

Kraijak, S. & Tuwanut, P. 2015. A survey on internet of things architecture, protocols, possible applications, security, privacy, real-world implementation and future trends. *2015 IEEE 16th International Conference on Communication Technology (ICCT)*, 18–21 October, 26–31, Hangzhou, China. Available at: http://ieeexplore.ieee.org/document/7399787/ [accessed 11 October 2016].

Krechovská, M. & Procházková, P.T. 2014. Sustainability and its integration into corporate governance focusing on corporate performance management and reporting. *Procedia Engineering*, 69:1144–1151. Available at: http://www.sciencedirect.com/science/article/pii/S187770581400349X [accessed 7 January 2016].

Kumar, M.S., Prajapati, M.R.K., Singh, M. & De, A. 2010. Realization of threats and countermeasure in semantic Web services. *International Journal of Computer Theory and Engineering*, 2(6):919–924. Available at: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.461.6687&rep=rep1&type=pdf [accessed 25 May 2016].

Levy, Y. & Ellis, T.J. 2006. A systems approach to conduct an effective literature review in support of information systems research. *Informing Science: International Journal of an Emerging Transdiscipline*, 9(1):181–212. Available at: http://www.scs.ryerson.ca/aferworn/courses/CP8101/CLASSES/ConductingLiteratureReview.pdf [accessed 3 June 2015].

Li, L. 2012. Study on security architecture in the Internet of Things. *2012 International Conference* on *Measurement, Information and Control (MIC)*, 14–15 January, 374–377, Harbin, China. Available at: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6273274&tag=1 [accessed 22 June 2016].

Link-labs. 2015. *Types of wireless technology*. Available at: http://www.link-labs.com/types-of-wireless-technology/ [accessed 2 July 2015].

Liu, R. & Wassell, I.J. 2011. Opportunities and challenges of wireless sensor networks using cloud services. *Proceedings of the workshop on Internet of Things and Service Platforms*, 6–9 December, 1–7, Tokyo, Japan. Available at: http://dl.acm.org/citation.cfm?id=2079357 [accessed 29 June 2015].

Liu, T., Yuan, R. & Chang, H. 2012. Research on the Internet of Things in the automotive industry. *2012 International Conference on Management of e-Commerce and e-Government (ICMeCG)*, 20–21 October, 230–233, Beijing: China Available at: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6374914 [accessed 19 July 2016].

Liu, Y. & Zhou, G. 2012. Key technologies and applications of internet of things. *2012 Fifth International Conference* on *Intelligent Computation Technology and Automation (ICICTA)*, 12–14 January, 197–200, Zhangjiajie, Hunan. Available at: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6150221 [accessed 23 June 2015].

López, T.S., Ranasinghe, D.C., Harrison, M. & McFarlane, D. 2012. Adding sense to the Internet of Things. *Personal and Ubiquitous Computing*, 16(3):291–308. Available at: http://link.springer.com/article/10.1007/s00779-011-0399-8 [accessed 23 June 2015].

Ma, Z., Shang, X., Fu, X. & Luo, F. 2013. The architecture and key technologies of Internet of Things in logistics. *International Conference on Cyberspace Technology (CCT 2013)*, 23 November, 464–468, Beijing, China. Available at: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6748635 [accessed 19 July 2016].

Matin, M.A. & Islam, M.M. 2012. Overview of wireless sensor network. *INTECH Open Access Publisher*. Croatia. Available at: http://cdn.intechopen.com/pdfs-wm/38793.pdf [accessed 29 June 2015].

Mejri, M.N., Ben-Othman, J. & Hamdi, M. 2014. Survey on VANET security challenges and possible cryptographic solutions. *Vehicular Communications,* 1(2):53–66. Available at: http://www.sciencedirect.com/science/article/pii/S2214209614000187 [accessed 24 May 2016].

Melville, N., Kraemer, K. & Gurbaxani, V. 2004. Review: Information technology and organizational performance: An integrative model of IT business value. *MIS Quarterly*, 28(2):283–322. Available at: http://dl.acm.org/citation.cfm?id=2017226 [accessed 25 May 2015].

Menemencioglu, O. & Orak, I.M. 2014. A review on semantic Web and recent trends in its applications. *2014 IEEE International Conference on Semantic Computing (ICSC)*, 16–18 June, 297–303, Newport Beach, CA. Available at: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6882044&tag=1 [accessed 9 July 2015].

Micrium Embedded Software. N.d. *Part 3: Internet Usage and Protocols.* Available at: http://micrium.com/iot/internet-protocols/ [accessed 2 July 2015].

Middleton, B., Halbert, J. & Coyle, F.P. N.d. *Security impacts on semantic technologies in the coming decade.* Research paper. Dallas, TX: Southern Methodist University. Available at: http://stko.geog.ucsb.edu/sw2022/sw2022_paper4.pdf [accessed 27 June 2016].

Mirobi, G.J. & Arockiam, L. 2015. Service level agreement in cloud computing: An overview. *2015 International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT)*, 18–19 December, 753–758, Kanyakumari District, India. Available at: http://ieeexplore.ieee.org.ez.sun.ac.za/stamp/stamp.jsp?tp=&arnumber=7475380 [accessed 3 July 2016].

Misra, S., Krishna, P.V., Agarwal, H., Saxena, A. & Obaidat, M.S. 2011. A learning automata based solution for preventing distributed denial of service in Internet of things. *2011 IEEE International Conference on Internet of Things, and Cyber, Physical and Social Computing*, 19–22 October, 114–122, Dalian, China. Available at: http://ieeexplore.ieee.org.ez.sun.ac.za/stamp/stamp.jsp?tp=&arnumber=6142307 [accessed 23 May 2016].

Mulligan, G. 2007. The 6LoWPAN architecture. *Proceedings of the 4th workshop on Embedded Networked Sensors*, 25–26 June, 78–82, Cork, Ireland. Available at: http://dl.acm.org/citation.cfm?id=1278992 [accessed 7 July 2015].

National Computing Centre. 2005. *IT Governance: Developing a successful governance strategy*. The IMPACT programme. Manchester. Available at: http://www.isaca.org/Certification/CGEIT-Certified-in-the-Governance-of-Enterprise-IT/Prepare-for-the-Exam/Study-Materials/Documents/Developing-a-Successful-Governance-Strategy.pdf [accessed 7 January 2016].

Nicho, M. & Fahkry, H. 2011. An integrated security governance framework for effective PCI DSS implementation. *International Journal of Information Security and Privacy*, 5(3):50–67. Available at: http://www.igi-global.com/article/integrated-security-governance-framework-effective/58982 [accessed 29 September 2016].

Nurse, J.R., Erola, A., Agrafiotis, I., Goldsmith, M. & Creese, S. 2015. Smart insiders: Exploring the threat from insiders using the Internet-of-Things. *2015 International Workshop on Secure Internet of Things*, 21 September, 5–14, Vienna, Austria. Available at: http://ieeexplore.ieee.org.ez.sun.ac.za/stamp/stamp.jsp?tp=&arnumber=7411833 [accessed 24 May 2016].

Oliver, D. & Lainhart, J. 2011. Delivering business benefits with COBIT: An introduction to COBIT 5. *Cobit Focus*, July, 3:1–3. Available at: http://www.isaca.org/Knowledge-Center/cobit/cobit-focus/Pages/COBIT-Focus-Volume-3-July-2011.aspx#1 [accessed 6 January 2016].

Optify. 2013. How to sell your agency's inbound marketing services. *#Hashdoc.* White paper. Available at: https://www.hashdoc.com/documents/10608/how-to-sell-your-agency-s-inbound-marketing-services# [accessed 7 August 2016].

Orduña, P., Almeida, A., Aguilera, U., Laiseca, X., López-de-Ipiña, D. & Goiri, A.G. 2010. *Identifying security issues in the semantic Web: Injection attacks in the semantic query languages*. Research paper. Spain: DeustoTech. Available at: http://morelab.deusto.es/media/publications/2010/conferencepaper/identifying-security-issues-in-the-semantic-web-injection-attacks-in-the-semantic-query-languages.pdf [accessed 27 May 2016].

Oteafy, S. & Hassanein, H.S. 2012. Resource re-use in wireless sensor networks: Realizing a synergetic internet of things. *Journal of Communications*, 7(7):484–

493. Available at: http://www.ojs.academypublisher.com/index.php/jcm/article/view/jcm07074844 93 [accessed 23 May 2016].

Papadimitratos, P. & Haas, Z.J. 2002. Secure routing for mobile ad hoc networks. *SCS Communication Networks and Distributed Systems Modelling and Simulation Conference (CNDS)*, 27–31 January, 1–13, San Antonio, TX. Available at: http://www.diva-portal.org/smash/get/diva2:429037/FULLTEXT01.pdf [accessed 10 June 2016].

Peris-Lopez, P., Hernandez-Castro, J.C., Tapiador, J.M., Palomar, E. & Van der Lubbe, J.C. 2010. Cryptographic puzzles and distance-bounding protocols: Practical tools for RFID security. *2010 IEEE International Conference on RFID*, 12–14 April, 45–52, Orlando, FL. Available at: http://ieeexplore.ieee.org.ez.sun.ac.za/stamp/stamp.jsp?tp=&arnumber=5467258 [accessed 13 June 2016].

Phelps, J., Nowak, G. & Ferrell, E. 2000. Privacy concerns and consumer willingness to provide personal information. *Journal of Public Policy & Marketing*, 19(1):27–41. Available at: http://www.jstor.org/stable/pdf/30000485.pdf?_=1464598726726 [accessed 30 May 2016].

Pisarsky, G.M. 2004. RFID technology: An analysis of privacy and security issues. *Proceedings of the Computer Science Seminar*, 24 April, 1–5, Hartford, CT. Available at: http://www.ewp.rpi.edu/hartford/~rhb/cs_seminar_2004/SessionA3/pisarsky.pdf [accessed 23 June 2016].

Posthumus, S. & Von Solms, R. 2004. A framework for the governance of information security. *Computers & Security*, 23(8):638–646. Available at: http://www.sciencedirect.com/science/article/pii/S0167404804002639 [accessed 7 January 2016].

Prescott, B. 2012. Business sense: Inbound marketing. *Times Standard*. Available at: http://www.times-standard.com/business/ci_19898286 [accessed 7 August 2016].

Radhakrishnan, S. 2015. 5 Common mistakes in adopting COBIT 5. *COBIT Focus*, May, 1–2. Available at: http://www.isaca.org/Knowledge-

Center/Research/Documents/COBIT-Focus-5-Common-Mistakes-in-Adopting-COBIT-5_nlt_Eng_0515.pdf [accessed 6 January 2016].

Rahmani, A.M., Thanigaivelan, N.K., Gia, T.N., Granados, J., Negash, B., Liljeberg, P. & Tenhunen, H. 2015. Smart e-health gateway: Bringing intelligence to internet-of-things based ubiquitous healthcare systems. *2015 12th Annual IEEE Consumer Communications and Networking Conference (CCNC)*, 9–12 January, 826–834, Las Vegas, NV. Available at: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=7158084 [accessed 19 July 2016].

Ridley, G., Young, J. & Carroll, P. 2004. COBIT and its utilization: A framework from the literature. *Proceedings of the 37th Annual Hawaii International Conference on System Sciences*, 5–8 January, 1–8, Big Island, Hawaii. Available at: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1265566 [accessed 29 July 2015].

Rotter, P. 2008. A framework for assessing RFID system security and privacy risks. *IEEE Pervasive Computing*, April–June, 7(2):70–77. Available at: http://www.computer.org/csdl/mags/pc/2008/02/mpc2008020070-abs.html [accessed 27 January 2016].

Rudman, R.J. 2008. Demystifying COBIT. *Accountancy SA*, April: 22–24. Available at: http://www.accountancysa.org.za/?p=2695 [accessed 6 January 2016].

Sallai, G. 2013. From telecommunications to cognitive infocommunications and internet of things: Phases of digital convergence. *2013 IEEE 17th International Conference on Intelligent Engineering Systems (INES)*, 19–21 June, 13–17, Costa Rica. Available at: http://ieeexplore.ieee.org/document/6632803/ [accessed 11 October 2016].

Scarfone, K. & Mell, P. 2007. Guide to intrusion detection and prevention systems (idps). *National Institute of Standards and Technology: Special publication*, February, 800(94):1–9. Available at: http://ecinetworks.com/wp-content/uploads/bsk-files-manager/86_SP800-94.pdf [accessed 8 June 2016].

Schneider, S. 2013. Understanding the protocols behind the Internet of Things. *Electronic Design*. Available at: http://electronicdesign.com/embedded/understanding-protocols-behind-internet-things [accessed 1 July 2015].

Singh, B. 2010. Network security and management. *2010 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC)*, 28–29 December, 1–6, Coimbatore, India. Available at: http://ieeexplore.ieee.org.ez.sun.ac.za/stamp/stamp.jsp?tp=&arnumber=5705886 [accessed 6 July 2016].

Smith, D.M. 2003. The cost of lost data. *Journal of Contemporary Business Practice*, 6(3):1–9. Available at: http://sirtechnology.com/wp-content/uploads/2012/01/The-Cost-of-Lost-Data-Graziadio-Business-Review.pdf [accessed 24 May 2016].

Sousa K.J. & Oz, E. 2015. *Management information systems*. Stamford, CT: Cengage Learning.

Su, Z. & Wassermann, G. 2006. The essence of command injection attacks in web applications. *ACM SIGPLAN Notices*, January, 41(1):372–382. Available at: http://dl.acm.org/citation.cfm?id=1111070 [accessed 27 May 2016].

Sun, Y., Wu, L., Wu, S., Li, S., Zhang, T., Zhang, L., Xu, J. & Xiong, Y. 2015. Security and privacy in the Internet of Vehicles. *2015 International Conference on Identification, Information, and Knowledge in the Internet of Things (IIKI)*, 22–23 October, 116–121, Beijing, China. Available at: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=7428337&tag=1 [accessed 24 May 2016].

Sundmaeker, H., Guillemin, P., Woelfflé, S. & Friess, P. 2010. *Vision and challenges for realising the Internet of Things*. Luxembourg: Publications Office of the European Union. Available at: http://www.researchgate.net/publication/228664767_Vision_and_challenges_for_realising_the_Internet_of_Things [accessed 25 May 2015].

Tarrant, D., Hitchcock, S. & Carr, L. 2011. Where the semantic Web and Web 2.0 meet format risk management: P2 registry. *International Journal of Digital Curation*, 6(1):165–182. Available at: http://www.ijdc.net/index.php/ijdc/article/view/171/239 [accessed 27 June 2016].

The Security Ledger. 2013. *IT pros: Internet of Things is a governance disaster*. Available at: https://securityledger.com/2013/11/it-pros-internet-of-things-is-a-governance-disaster/ [accessed 13 January 2016].

Ting, S.L., Kwok, S.K., Albert, H.T. & Lee, W.B. 2010. Enhancing the information transmission for pharmaceutical supply chain based on Radio Frequency Identification (RFID) and Internet of Things. *2010 8th International Conference on Supply Chain Management and Information Systems (SCMIS)*, 6–8 October, 1–5, Hong Kong, China. Available at: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5681726 [accessed 19 July 2016].

TongKe, F. 2013. Smart agriculture based on cloud computing and IOT. *Journal of Convergence Information Technology,* 8(2):210–216 Available at: http://www.globalcis.org/jcit/ppl/JCIT2598PPL.pdf [accessed 25 July 2016].

Vermesan, O. & Friess, P. (Eds.). 2014. *Internet of things: From research and innovation to market deployment.* Aalborg: River. Available at: https://www.researchgate.net/profile/Patrick_Guillemin/publication/265689193_IoT-From_Research_and_Innovation_to_Market_Deployment_IERC_Cluster_eBook_978-87-93102-95-8_P/links/541932c10cf203f155adc4f4.pdf [accessed 3 August 2016].

Wang, L. & Wyglinski, A.M. 2011. A combined approach for distinguishing different types of jamming attacks against wireless networks. *2011 IEEE Pacific Rim Conference on Communications, Computers and Signal Processing (PacRim)*, 23–26 August, 809–814, Victoria, Canada. Available at: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6032998&tag=1 [accessed 25 May 2016].

Wang, Y., Attebury, G. & Ramamurthy, B. 2006. A survey of security issues in wireless sensor networks. *IEEE Communications Surveys & Tutorials*, April–June, 8(2):2–23. Available at: http://ieeexplore.ieee.org.ez.sun.ac.za/stamp/stamp.jsp?tp=&arnumber=4109893 [accessed 9 May 2016].

Webb, P., Pollard, C. & Ridley, G. 2006. Attempting to define IT governance: Wisdom or folly? *Proceedings of the 39th Annual Hawaii International Conference on System Sciences*, 4–7 January, 1–10, Kauai, Hawaii. Available at: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1579684&tag=1 [accessed 7 January 2016].

Weber, R.H. 2010. Internet of Things: New security and privacy challenges. *Computer Law & Security Review*, 26(1):23–30. Available at: http://www.sciencedirect.com.ez.sun.ac.za/science/article/pii/S0267364909001939 [accessed 26 May 2015].

Webster, J. & Watson, R.T. 2002. Analyzing the past to prepare for the future: Writing a literature review. *Management Information Systems Quarterly*, 26(2):1–11. Available at: http://aisel.aisnet.org/cgi/viewcontent.cgi?article=2625&context=misq [accessed 3 June 2015].

Wikipedia. 2016. *Inbound marketing*. Available at: http://en.wikipedia.org/wiki/Inbound_marketing [accessed 7 August 2016].

Wu, M., Lu, T.L., Ling, F.Y., Sun, L. & Du, H.Y. 2010. Research on the architecture of Internet of things. *2010 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE)*, 20–22 August, 484–487, Chengdu, China. Available at: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5579493&tag=1 [accessed 23 June 2015].

Yan, B. & Huang, G. 2009. Supply chain information transmission based on RFID and internet of things. *2009 ISECS International Colloquium on Computing, Communication, Control, and Management*, 8–9 August, 166–169, Sanya, China. Available at: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5267755 [accessed 19 July 2016].

Yongjun, Z., Xueli, Z. & Shuxian, Z. 2012. Intelligent transportation system based on Internet of Things. *World Automation Congress (WAC)*, 24–28 June, 1–3, Peurto Vallarta, Mexico. Available at: http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=6321832&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D6321832 [accessed 30 July 2016].

Zalewska, A. 2014. Challenges of corporate governance: Twenty years after Cadbury, ten years after Sarbanes–Oxley. *Journal of Empirical Finance*, 27:1–9. Available at: http://www.sciencedirect.com/science/article/pii/S092753981300100X [accessed 7 January 2016].

Zapata, M.G. 2002. Secure ad hoc on-demand distance vector routing. *ACM SIGMOBILE Mobile Computing and Communications Review*, 6(3):106–107. Available at: http://www2.ic.uff.br/~ejulio/mestrado/estudo_orientado/p106-zapata.pdf [accessed 10 Junie 2016].

Zhang, M., Sun, F. & Cheng, X. 2012. Architecture of internet of things and its key technology integration based-on RFID. *2012 Fifth International Symposium on Computational Intelligence and Design (ISCID)*, 28–29 October, 294–297, Hangzhou, China. Available at: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6406857 [accessed 23 June 2015].

Zhang, Y. 2011. Technology framework of the Internet of Things and its application. *2011 International Conference on Electrical and Control Engineering*, 16–18 September, 4109–4112, Yichang, China Available at: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6057290 [accessed 23 June 2015].

Zhang, Z., Chen, Q., Bergarp, T., Norman, P., Wikström, M., Yan, X. & Zheng, L.R. 2009. Wireless sensor networks for logistics and retail. *2009 Sixth International Conference on Networked Sensing Systems (INSS)*, 17–19 June, 1–40, Pittsburgh, PA. Available at: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5409943 [accessed 19 July 2016].

Zhou, C., Zhao, B., Zhu, G. & Wei, W. 2006. Study of one-way hash function to digital signature technology. *2006 International Conference on Computational Intelligence and Security*, 3–6 November, 1503–1506, Guangzhou, China. Available at: http://ieeexplore.ieee.org.ez.sun.ac.za/stamp/stamp.jsp?tp=&arnumber=4076216 [accessed 12 June 2016].

Zhu, Q., Wang, R., Chen, Q., Liu, Y. & Qin, W. 2010. Iot gateway: Bridging wireless sensor networks into internet of things. *2010 IEEE/IFIP 8th International Conference on Embedded and Ubiquitous Computing (EUC)*, 11–13 December, 347–352, Hong Kong, China. Available at: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5703542 [accessed 25 June 2015].

Zorzi, M., Gluhak, A., Lange, S. & Bassi, A. 2010. From today's intranet of things to a future internet of things: A wireless- and mobility-related view. *IEEE Wireless Communications*, 17(6):44–51. Available at: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5675777 [accessed 25 May 2015].

APPENDIX A: RISK AND CONTROL MATRIX USING COBIT 5

The 37 detail processes of COBIT 5 were reviewed in order to identify the risks associated with the Internet of Things and the relevant controls to address the risks. Only processes that were relevant to the implementation of Internet of Things are listed in the table below.

Domain	Relevant COBIT process	Detail processes' requirements	Risk(s) identified	Impact of the risk	Control(s) to mitigate the risk(s)
Evaluate, direct and monitor	EDM01	Evaluate, direct and monitor the governance system with regard to the privacy of personal information and the confidentiality of business information.	• Laws are broken and ethical standards breached through the real-time identification and locating of individuals. • Confidentiality of business information and processes is critical to the success of the business.	High	• Identify and evaluate the legal, regulatory and contractual obligations associated with protecting the privacy of personal and confidentiality of business information. • Determine how the legal, regulatory and contractual obligations should be applied within the governance of the business. • Ensure users and developers are informed on the relevant guidelines for ethical and professional behaviour. • Establish a task force to monitor compliance with relevant legal, regulatory and contractual obligations. • Third party service providers should also be made aware of privacy and confidentiality obligations through documented service provider agreements.
	EDM03	Evaluate, direct and monitor the business's exposure to risks associated with the Internet of Things.	• All risks with regard to the use of Internet of Things technologies are not identified and mitigated appropriately. • The risk-management procedures and policies do not function effectively.	High	• Develop and implement a risk-management plan that includes the following: ○ Establish a formal risk-management policy that includes an action plan in emergency situations. ○ Document risk-identification procedures to evaluate risk factors in advance. ○ Promote a risk-aware culture through education and training among users and developers to proactively identify risks. ○ Establish mechanisms that addresses the changes in risks. ○ Assign the responsibility for the identification and mitigation of risks.

Domain	Relevant COBIT process	Detail processes' requirements	Risk(s) identified	Impact of the risk	Control(s) to mitigate the risk(s)
Align, plan and organise	APO01	Manage Internet of Things information and the use of its technologies through governance guidelines and policies.	• Individuals in the Internet of Things environment cannot perform their duties effectively due to their uncertainty of their rights and responsibilities. • Ineffective and non-comprehensive policies with regard to the use of Internet of Things technologies. • Policies are not reviewed and updated on a regular basis for adjustments associated with changes in technologies. • Data gathered from smart objects are not managed effectively and classified correctly. • Information stored on cloud computing infrastructure is not secure.	High	• Define the scope, function, capabilities and decision rights of Internet of Things users, developers, management and service providers. • Develop and implement a technology usage policy that includes the following: ○ Educate all relevant individuals on the terms of the policy. ○ Update the policy on a regular basis. • Develop and implement an information-management policy that includes the following: ○ Developers should create a semantic policy language with the specific security and privacy requirements of information in mind. ○ Cloud storage service providers should define and implement procedures to ensure the integrity and consistency of information in their service agreements. ○ Cloud storage service providers should classify, create and maintain information.
	APO03	Determine and define the architecture and underlying technologies of the Internet of Things.	• Internet of Things architecture and underlying technologies are not sufficient for the deployment of the Internet of Things in a business environment.	High	• Determine the full extent of Internet of Things architecture that supports the deployment in a business environment, including the identification of underlying technologies such as smart objects, network specifications, semantic layer, etc.
	APO04	Identify emerging technologies in the technology environments, assess the potential of these technologies and monitor its implementation and use.	• New technologies are adopted in a business without implementing the necessary controls to mitigate the risks they pose.	Medium	• Perform extensive research on the new technology in order to gain knowledge of its applications, benefits and possible threats. • Identify safeguards to address the risks associated with the new technology.
	APO05	Identify required investments and manage investments based on resources, risks and benefits.	Refer to APO04.	Medium	Refer to APO04.

Domain	Relevant COBIT process	Detail processes' requirements	Risk(s) identified	Impact of the risk	Control(s) to mitigate the risk(s)
Align, plan and organise	APO07	Maintain the skills and competencies of employees as well as managing contract staff.	• Employees' and developers' knowledge and experience are insufficient. • Service provider support is insufficient.	High	• Provide continuous long-term learning and workshops for employees and developers on the technical aspects of the Internet of Things. • Formulate a formal agreement with service providers that stipulates the availability of resources and security measures regarding the confidentiality of business information and privacy of personal information.
	APO08	Manage business IT relationships.	Refer to APO04.	High	Refer to APO04.
	APO09	Manage IT service delivery.	• IT services received from external parties do not meet business requirements.	High	• Identify areas of external service provision and determine the services required. • Formulate a formal agreement with service providers that stipulates the availability of resources and security measures regarding the confidentiality of business information and privacy of personal information. • Measure, monitor and report on the service delivery.
	APO10	Manage external service providers.	Refer to APO09.	High	Refer to APO09.
	APO12	Identify, manage and mitigate all Internet of Things risks.	Refer to EDM03.	High	• Refer to EDM03. • Define risks and formulate controls to mitigate the risks associated with investment in and use of the Internet of Things.
	APO13	Develop, implement and maintain an information security management system.	Refer to DSS05.	High	Refer to DSS05.
Build, acquire and implement	BAI02	Analyse and define business requirements for the infrastructure and underlying technologies of the Internet of Things.	• Refer to EDM01, APO03 and APO12. • Insufficient business continuity plan is in place to maintain operations in emergency situations.	High	• Refer to EDM01, APO03 and APO12. • Formulate a disaster-recovery plan and ensure regular backups of data is made.

Domain	Relevant COBIT process	Detail processes' requirements	Risk(s) identified	Impact of the risk	Control(s) to mitigate the risk(s)
Build, acquire and implement	BAI05	Sustain business changes through effective training.	• Developers have inefficient knowledge of new technologies, which leads to script writers taking advantage of ontology vulnerabilities. • Database information is not adequately protected from query injection threats.	High	• Developers must be made aware of risks and challenges. • Semantic policy language must be based on ontologies written with the specific security and privacy requirements of business in mind. • Educate developers through continuous long-term leaning and maintenance workshops on the use and development of new technologies.
	BAI08	Manage information and knowledge gathered in an Internet of Things environment.	• Data gathered from smart objects are not managed effectively and classified correctly.	High	• Composition of ontologies should include: ○ Representation of actions and conditions ○ Meta-policies.
	BAI09	Manage all Internet of Things assets, including smart objects and networks.	• Smart objects are vulnerable to physical attacks and harsh environments. • Smart objects ignore legitimate connection requests in denial-of-service attacks. • Networks are unavailable due to jamming, selective forwarding and denial-of-service attacks. • Database information is not adequately protected from query injection threats.	High	• Implement physical security controls for smart objects such as the faraday cage. • Manage networks' performance through: ○ Secure data routing ○ Monitoring the network ○ Multipath routing ○ Frequency hopping ○ Blocker tags ○ Hash lock protocol. • Composition of ontologies should include: ○ Modelling speech acts ○ Policy engine.
Deliver, service and support	DSS01	Coordinate Internet of Things activities and deliver operational services.	• Refer to APO09. • Data integrity is threatened by collisions, data loss, sinkhole, message tampering, denial-of-service and man-in-the-middle attacks.	Medium	• Refer to APO09. • Manage data integrity through: ○ Secure data routing ○ Restricting broadcasting rage ○ Network monitoring ○ Disaster-recovery plan and backup ○ Smart object protection.
	DSS02	Provide sufficient user support.	Refer to APO07.	High	Refer to APO07.

Domain	Relevant COBIT process	Detail processes' requirements	Risk(s) identified	Impact of the risk	Control(s) to mitigate the risk(s)
Deliver, service and support	DSS04	Establish and maintain a business continuity plan.	• Substantial data loss or interruptions in business operations are experienced. • Current business continuity plans are inadequate or outdated.	High	• Formulate and implement a comprehensive business continuity plan. • Ensure that regular backups of all business information is made.
	DDS05	Implement and manage protective, detective and corrective security controls to ensure security of assets and information.	• Data integrity is threatened by collisions, data loss, sinkhole, message tampering, denial-of-service and man-in-the-middle attacks. • Privacy of personal information and confidentiality of business information are threatened by tracking people, RFID cloning, eavesdropping, sniffing, smart object tampering and man-in-the-middle attacks. • Validity of gathered, transferred and presented data is threatened by collisions, node impersonation, Sybil, spoofing and replay attacks. • Unauthorised access is gained to smart objects, networks and databases. • Network unavailability due to jamming, selective forwarding and denial-of-service attacks.	High	• Implement smart object security controls: ○ Electrostatic screening ○ Blocker tags ○ Active jamming ○ Frequency-hopping spread spectrum ○ Kill order mechanism ○ Hash-lock protocol ○ Re-encryption mechanism ○ Silent tree-walking algorithm. • A combination of the following controls will mitigate information transmission security risks: ○ Key management ○ Secure routing of data ○ Restrictions on broadcasting range ○ Monitoring networks for attacks ○ Multipath routing.
	DDS06	Manage roles, responsibility, access privileges and levels of authority associated with Internet of Things data.	Refer to APO01.	High	Refer to APO01.
Monitor, Evaluate, and Assess	MEA03	Monitor and evaluate Internet of Things compliance with laws, regulations and contractual requirements.	Refer to EDM01.	High	Refer to EDM01.

(Source: Author's own)