

1602836 Assignment 2 DI

by Daniel Ince

FILE	14401_DANIEL_INCE_1602836_ASSIGNMENT_2_DI_177757_1895965265. PDF (608.7K)		
TIME SUBMITTED	18-MAY-2020 11:49PM (UTC+0100)	WORD COUNT	3856
SUBMISSION ID	128182270	CHARACTER COUNT	22761

Assignment Title: Internet of Things

Module: SGEE6000 – Electronic Design

Course: BSc Electrical and Electronic Engineering

University number: 1602836

Name: Daniel Ince

Date Submitted: 18/05/2020

Word count: 3199

Contents

1. Executive Summary	3
2. Research	4
2.1 Origins and driving forces	4
2.1.1 Definition	4
2.1.2 IoT Paradigm	5
2.2 Key concepts, models and technologies	6
2.2.1 IoT Architecture	6
2.2.2 Industry 4.0	7
2.2.3 IoT Models	7
2.3 Security challenges.....	10
2.3.1 Personal devices.....	10
2.3.2 National infrastructure.....	10
2.4 Privacy challenges	12
2.4.1 Convenience.....	12
2.4.2 Privacy classification	13
2.5 Consumer choice.....	14
3. Conclusions	15
Works Cited	16

1. Executive Summary

The research conducted in this assignment investigated the origins and concepts surrounding the Internet of Things and how technology has developed to become interconnected. Potential issues surrounding privacy and security have been reviewed whilst evaluating the current methods of risk reduction in these area with forethought to future improvements. The nature of the IoT growth has resulted in a lot of current privacy laws becoming insufficient to deal with this new scenario. Whilst the pace has left issues with legacy equipment and systems becoming out of date and vulnerable to the fast changing security threat that comes with the IoT.

2. Research

2.1 Origins and driving forces

2.1.1 Definition

The internet of things is a vision that stems from the idea that networking can encompass almost all aspects of life and technology within our world. Keyur K Patel states *“The Internet of things refers to a type of network to connect anything with the Internet based on stipulated protocols through information sensing equipment to conduct information exchange and communications in order to achieve smart recognitions, positioning, tracing, monitoring, and administration.”* (2016)

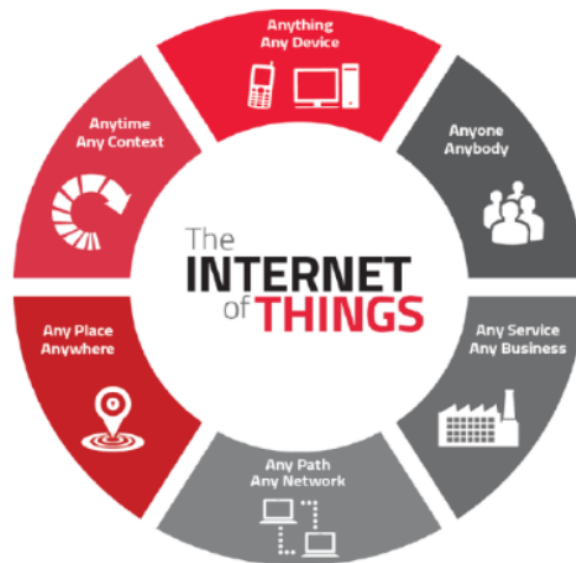


Figure 1: IOT (Patel & Patel, 2016)

The first concept of the internet of things began in 1999 within the RFID community by Kevin Ashton, where information sharing between devices was first starting to take a hold. The aim is that all manner of devices will have an IP address and be connected to each other, sharing information and analysing it in order to make many processes automated. It is described by Knud L. Lueth (2014) on the IoT Analytics website, that during 2010, information was leaked that 360 degree image data for Google's StreetView was being stored across domestic WiFi networks. The development of the internet and mobile devices has pushed this theme into many companies' priorities, the prediction in October 2013 being that in 2020 the IoT would be a \$8.9 trillion market. As explained by Karen Rose (2015) Many early systems in the 1970s had machine to machine communication but were mainly localised and were not connected to the internet. The Internet of Things system will encompass all industries and domestic applications across the globe.

2.1.2 IoT Paradigm

Figure 1 supports the aim for the IoT, to have all people, devices and machines connected across all locations, and within all industries, at any one time. This is the driving force for the IoT, the vision that all industries can co-operate seamlessly across all platforms. Information shared from one area of society will benefit others and allow a faster automated system. This includes all objects not normally associated with being electronic or 'smart', such as clothing, food and the environment. All this technology will be able exchange and store information on the 'cloud'. What this interconnectivity means is time efficiency, an example is when supplies are running low on an appliance, the device automatically orders more, meaning less interaction from humans and less time spent empty. Stated by Keith D. Foote, part of Kevin Ashton's presentation in 1999 stated *"The problem is, people have limited time, attention and accuracy. All of which means they are not very good at capturing data about things in the real world."* (2016)

The internet of things also requires the implementation of a certain level of intelligence into devices, allowing them to identify the optimum outcome and act accordingly in an efficient and autonomous manner without human interaction. As explained by Lampropoulos et al. (2019), The IoT aims to achieve autonomous, secure connectivity between the devices and the real world applications, whilst also integrating intelligence into the systems.

This intelligence and automation in processes allows for the increased output of a system, for example a manufacturing plant. As this means more profit, corporations are keen to push for a more interconnected world, to reduce running costs, reduce manpower, and increase output. Veronica Scuotto states, *"Thanks to the business opportunities arising from the application of IoT in urban services, many firms are currently involved in smart city projects."* (2016)

2.2 Key concepts, models and technologies

2.2.1 IoT Architecture

According to IoT Analytics, the official definition for the internet of things is, “Sensors and actuators embedded in physical objects are linked through wired and wireless networks, often using the same Internet Protocol (IP) that connects the internet.” (2014)

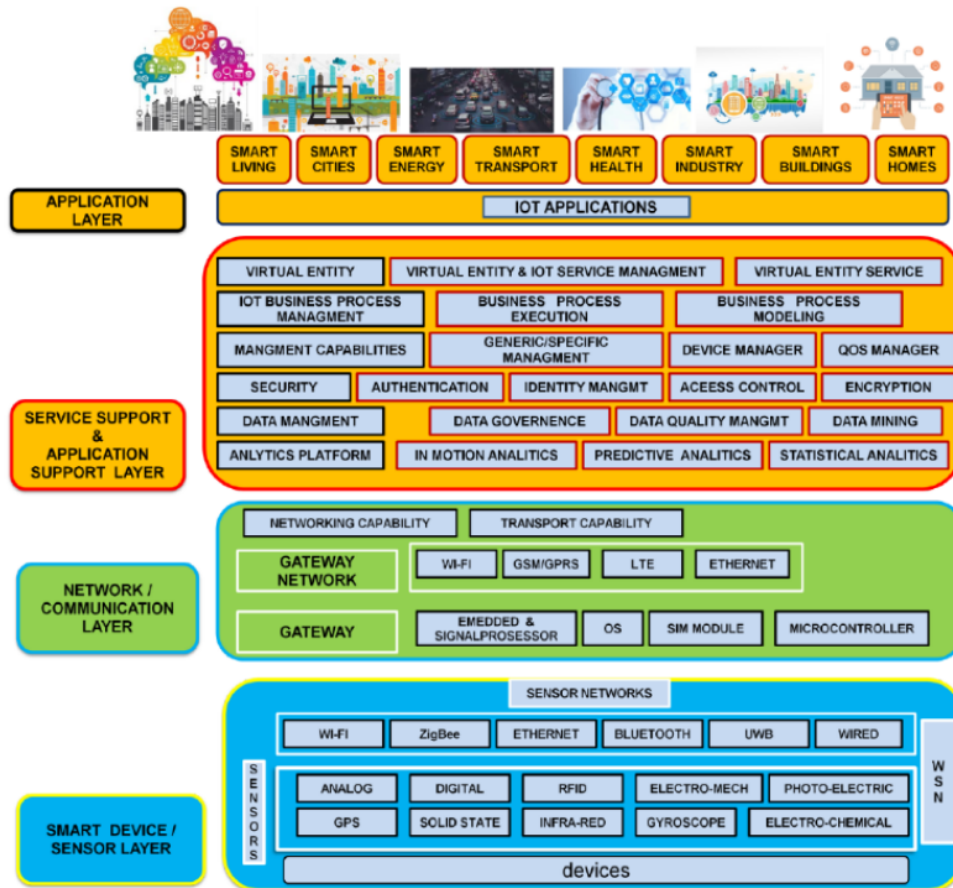


Figure 2: IoT Architecture (Patel & Patel, 2016)

Patel explains that there are three categories of information sharing within the IoT; People to people, people to machines, and machines to machines, all interacting through the internet. (2016) The architecture is shown in figure 2, very similar to the hierarchy of the internet. At the lowest level we can see the primary elements of the system, the sensors, the purpose is to convert physical information of the real world into a signal of various forms. This information can then be passed onto devices such as computers or transmitters where it can be processed. At this level there are different networks for the sensors themselves such as ethernet, wired or Bluetooth. The network and communication layer contain the gateways and interfaces between the sensors and onto the network.

The service and application support levels is where this information is processed and managed, having large amounts of memory and processing power. It is here where encryption and access controls are implemented to protect the information before it is sent on to the application layer. Final elements such as actuators are present across a large range of industries and areas make up the application layer and it is here actions are carried out based upon the information given. The result being that all the applications across the different domains are interconnected and exchanging information.

2.2.2 Industry 4.0

The internet of things also aims to achieve Industry 4.0, a next level phase of industry for the information age. Industry 4.0 will involve automation and intelligence in processes, as mentioned earlier. To achieve this it will use a plethora of new or developing technologies such as cooperative robotics, augmented reality, virtual data processing and real-time simulations. Additionally, Lampropoulos et al., state, *"it seeks to address the dynamic global market and the competitive nature of today's industries in line with the continuously changing customers' and market needs."* (2019) The rapid development of social media has resulted in a large amount of data stored online and digital content. Companies are recognising this data stored, including the frequency of websites visited, how long content was viewed and that it can be used for marketing or business purposes. Information like this can be taken and used to tell the business what the consumer is likely to purchase, enabling these items to be targeted towards specific individuals. When applied at a global scale, this severely increases the advertising power of a company. However, with this data, comes a number of security and privacy risks and challenges to overcome. As Lampropoulos et al. (2019) explain, standardization, interoperability, identity management and confidentiality are all issues that need to be dealt with. From an operational perspective, devices will all have different manufacturers and will require some form of standardisation between manufacturers in order to function correctly. Service providers will be needed for systems such as cloud storage and these will face the same issues.

2.2.3 IoT Models

There are four different models for the IoT, this communication framework is highlighted by Rose et al., (2015) and sets out how the IoT will operate.

- Device-to-Device Communication

Where a minimum of two devices are directly connected and share information. This is direct and requires no server or cloud storage. There will be a common communication protocol for these devices and typically this will be used for small data packets in an automated home lighting system for example. A weakness of this model is that these devices will use device

specific communication and built in security measures. Therefore, these systems may become outdated, redundant and incompatible with newer units.

- Device-to-Cloud Communications

These IoT devices will be able to send and receive information from a storage cloud. The communication will be achieved through existing methods such as ethernet to send data to an external cloud service. This data can be analysed separately and sent back to the devices, whilst also supporting software updates as these devices are connected to the internet, an example is voice activation software used in smart speakers and televisions. A disadvantage is that users may be tied into a subscription with a certain service provider, making it difficult to homologate multiple manufacturers of devices.

- Device-to-Gateway

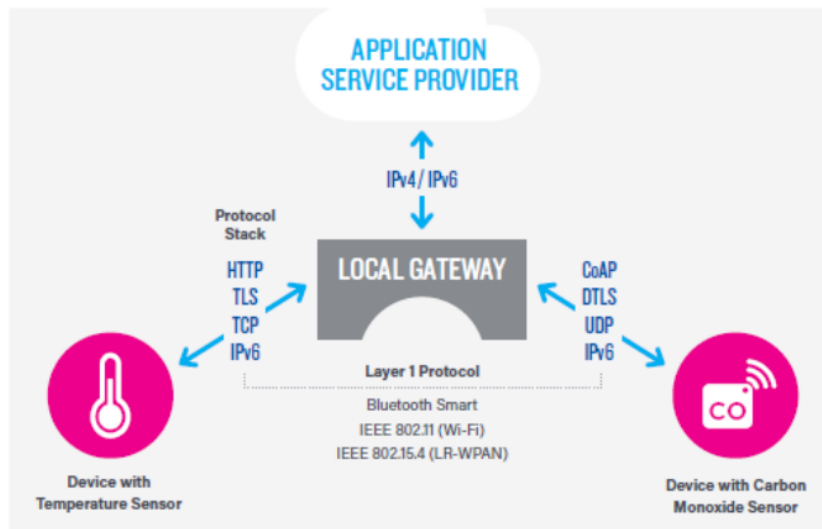


Figure 3: Device to gateway model (Rose, et al., 2015)

A diagram for the device to gateway model is shown in figure 3, here an intermediate gateway is used between the devices and the cloud. This is typically a local gateway that provides security protocols and can be used to allow communication between devices that would have

struggled with interoperability. As explained by Rose (2015), the cost of this system can increase due the necessity to add software for the integration of new devices with old.

- Back-End Data-Sharing

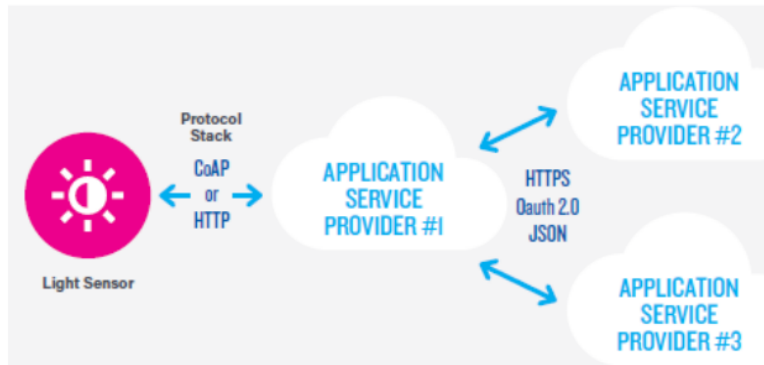


Figure 4: Back-end data-sharing model (Rose, et al., 2015)

The architecture of this model allows multiple cloud services to share data that can be accessed by devices communicating directly with each cloud. Here information can be accessed from a large amount of devices instead of separate groups of information on various standalone servers. Interoperability between these systems is crucial and requires a lot of design and cost upfront.

2.3 Security challenges

2.3.1 Personal devices

The internet of things vision is of a mix of different communication technologies adapted to be energy efficient, reliable and secure. A large challenge is presented through security, as there will be large amounts of personal data required to be stored on the network or cloud. As stated by Norton on their website *"Wearable devices are essentially data collectors. The personal data collected and stored with these devices, such as your name, age, health and location can aid criminals in stealing your identity."* (Norton, 2020) The problem of identity fraud and piracy may increase in magnitude, the issue being that all of the devices and information can be accessed anywhere in the world.

Another vulnerability is through the access to all the devices on the network, as these could be subject to hacking and outside interference. Many devices, protocols and programming languages of all kinds will need to be seamlessly communicating, this creates weak spots for access. Stated by Marie-Helen Maras *"The IoT creates a greater attack surface by forming more access points to the Internet that need to be securely monitored."* (2015) It is predicted that the largest global threat online at the moment is Ransomware, viruses affecting both individuals and companies by locking out sensitive or valuable information until a fee is paid.

The nature of technology development means that new device editions are being created all the time. V. Shah explains, that many of the older device editions are left without fresh updates, and whilst were secure at the time of manufacture, are no longer secure as time passes. As these are still connected to the internet, they pose a vulnerability to the whole network. (2019) This is because whilst device technology develops, so does the capability of viruses. Due to the huge technological boom to develop convenient smart devices, a lot of these do not have enough protection and security enabled, often with alternate means of access used by the manufacturer. Maras goes on to state *"Ultimately, the rush to deploy IoT technology has outpaced the creation and implementation of security and privacy protections and standards for these devices."* (2015)

2.3.2 National infrastructure

In the past an attack from a virus would just target the individual's personal information on a home computer. However, with the internet of things, many more areas can be affected, for example in 2010 a virus called Stuxnet was reportedly created specifically to target a uranium enrichment facility in Iran. Symantec (2011) explain that the main purpose of Stuxnet was to target industrial control systems or similar equipment. This virus was able to reprogram the code on PLCs for equipment to operate outside of safe limits within the nuclear facility and hide the changes from the plant operator. This virus poses no threat to normal computers, and instead searches for connections to specific PLCs.

The virus spreads itself amongst devices undetected, until it finds a device connected to an industrial control system. McAfee state *"Anyone monitoring the equipment would have had no indication of a problem until the equipment began to self-destruct."* (2020) What this attack shows is how easily a virus can be spread to target a specific process, with IoT connected devices making that spread easier.

The internet of things will encompass domains such as military and defence technology, energy and oil and gas. IoT technology will be costly to keep secure and will need constant updating, firms such as the above will have the funding to keep systems up to date and secure, whereas smaller businesses may struggle. Lu, et al. (2015) explain that the economic cost of installing and running an IoT system may be substantially more than the benefits, and so it may be impossible to fully install all the privacy protection technologies within the system.

2.4 Privacy challenges

2.4.1 Convenience

With the development of the internet of things, there will inevitably be an increased level of surveillance for the system to function properly. This leads to a large amount of information on individuals stored online. Privacy is controlled within the UK Human Rights Act 1998 and allows individuals the right to keep some sensitive information from others. The introduction of IoT devices will make this harder due to the amount of data these devices can pull from a single person. As explained by Maras (2015), the data stored can include real-time location, financial history, hobbies, activities, and work. These devices can build up a profile of someone's life, whilst also storing data on people they encounter and relatives. This could potentially be a privacy risk to others, even if the individual using the device has agreed to share their own information.

The benefit of having an IoT enabled world is convenience; personal data is automatically processed to provide information such as parked car locations, nearby shops, and tailored digital content online. However, this ease of use and automation must come at the extent to a loss of privacy to some extent. An example of this today is the use of internet cookies that are placed onto personal computers from websites to record information and send it back to a server. Norman Gervais states, *"It not only collects information about which web pages the user visits, but also about the user's activities on the site."* (2014) When applied at a level the IoT aims to achieve, these text files will be documenting real-life activities and real-time location. The addition of extra privacy control measures often reduces the convenience, as features such as multi-step authentication and security questions add time and effort to operating the device. This can detract from the selling point of the device and make it no longer competitive. Therefore, a balance must be found, and manufacturers must strive to achieve sufficient security for the user's data, whilst maintaining ease of use of the device.

2.4.2 Privacy classification

Privacy source (Corby [16])	High security privacy	Medium security privacy	Basic security privacy	Low security privacy
(I) Static				
(A) Who we are				
(1) Bio identity		Age	Weight, height, Race, birth	Blood type, fingerprint
(2) Financial identity			Bank account, credit card	
(3) Legal identity		Identification		Passport, driver's license
(4) Social identity		Affiliation, job, and party	Religion, nation, marriage, and position	
(5) Virtual identity		Phone number, password	Email address, mobile phone	Msn, IP
(B) What we have				
(1) Property		House, car, and property	Investment, stock	Salary
(2) Nonreal property			Insurance	
(3) Relation	Family	Children	Phone book, address book	Spouse
(C) Where we are		Home, company address		
(II) Dynamic				
(A) Transactions	Call records	Shopping	Credit card records	Booking hotel, credit score
(B) How we live	My photo	Travel, disease	Online records, criminal records, and chat	Hobby, drug use
(C) Where we are		Location		

Figure 5: Privacy Classification (Lu, et al., 2015)

Due to the large amount of information stored and analysed by IoT devices, Lu, et al. (2015) have classified the privacy data into categories of confidentiality and security, shown in figure 5. The ideal is to achieve security goals for each type of security privacy.

- I. Low security privacy – This information does not need to be encrypted but requires authorisation to access.
- II. Basic security privacy – Required to be encrypted in storage and transmission, also requires authorisation.
- III. Medium security privacy – Encrypted as previous with unique encryption key and authorisation for one time reading/writing.
- IV. High security privacy – Encrypted as previous whilst also having a unique encryption key per individual.

The classification is an example of how this information can be managed and categorised for different levels of security. Difficulty may ensue as some people may prioritise different information to others. As stated by Rose, *“There are social norms and expectations of privacy that differ in public spaces versus private spaces, and IoT devices challenge these norms.”* (2015)

2.5 Consumer choice

Discussed in a journal article by Gervais (2014), many people are not happy with the amount of online tracking, even though these activities can be limited, only 38% of users were aware of how to do so. This means that given the IoT approach, many people may choose to opt out of a large amount of the automated or intelligent systems that utilise personal information. Gervais goes on to state *“Perhaps part of the concern over internet privacy stems from the fact that a user does not need to give away a lot of personal information to a single entity to have his entire identification revealed.”* (2014) This may lead to a large amount of people opting out, rendering some of the IoT systems less effective than if there was cooperation and information sharing of individuals. This is backed up by the statement by Karen Rose et al., *“If people don’t believe their connected devices and their information are reasonably secure from misuse or harm, the resulting erosion of trust causes a reluctance to use the Internet.”* (2015) Firms may attempt to reduce the likelihood of someone opting out once signed up, by making it difficult to or hiding the opt out function.

3. Conclusions

The end goal of internet of things is to have mass device integration and communication between multiple domains to improve efficiency, production, convenience and quality of life. Achieving these goals will come with many challenges highlighted during this assignment.

The IoT will struggle to function as intended without user participation on allowing personal information to be used. Privacy will need to be strictly controlled if people are to opt in consent for the sharing of information. Privacy law will have to be reworked for the large amount of new information taken and shared, for sufficient controls to be implemented. This will encourage corporations to install these otherwise expensive controls and reduce the impact on the individual by limiting how their information is used. These measures will also change the market and may make the cost of IoT systems increase overall where the market is ultimately dominated by large corporations that can afford the research and development.

Security will need to be improved across the range of devices, including older systems with focus on providing security updates for previous generations. This will incur a lot of cost, however firms may resort to a subscription service for exchanging older devices with new with up to date firmware. Weaknesses will have to be prevented by ensuring IoT systems are inherently secure, without old equipment posing security issues. Encompassing security such as this will be essential if a vast majority of national infrastructure and even military technology is to be controlled and managed through the IoT.

Corporations will need to adapt to fast changing technological environment and aim to keep legacy systems up to date if security integrity is to be maintained. A combination of communication models will need to be used, whilst the challenge of interoperability between the devices on these systems will become an apparent issue.

Ultimately, a world with flawless interconnectivity across a broad range of applications will likely enhance the life of the majority. Although some individuals may be caught out by the equally as fast developing security threat, provided it is not dealt with within the development and service of smart technology by manufacturers, government laws and the conscientiousness of those accessing IoT enabled devices.

Works Cited

- Cluster of European Research Projects on the Internet of Things, 2010. *Vision and Challenges for Realising the Internet of Things*. Luxembourg: Publications Office of the European Union.
- Foote, K. D., 2016. *A Brief History of the Internet of Things*. [Online]
Available at: <https://www.dataversity.net/brief-history-internet-things/#>
[Accessed 20 April 2020].
- Gervais, N., 2014. Governmental Internet Information Collection Cookies Placing Personal Privacy at Risk. *Bulletin of the American Society for Information Science and Technology*, 40(2), pp. 27-31.
- Lampropoulos, G., Siaskas, K. & Anastasiadis, T., 2019. Internet of Things in the Context of Industry 4.0: An Overview. *International Journal of Entrepreneurial Knowledge*, 7(1).
- Lueth, K. L., 2014. *IoT Analytics*. [Online]
Available at: <https://iot-analytics.com/internet-of-things-definition/>
[Accessed 20 April 2020].
- Lu, X., Qu, Z., Li, Q. & Hui, P., 2015. Privacy Information Security Classification for Internet of Things Based on Internet Data. *International Journal of Distributed Sensor Networks*, p. 8.
- Maras, M.-H., 2015. Internet of Things: security and privacy implications. *Tomorrow's Privacy*, 5(2).
- McAfee, 2020. *What is Stuxnet?*. [Online]
Available at: <https://www.mcafee.com/enterprise/en-gb/security-awareness/ransomware/what-is-stuxnet.html>
[Accessed 20 April 2020].
- Norton, 2020. *Securing the Internet of Things*. [Online]
Available at: <https://uk.norton.com/internetsecurity-iot-securing-the-internet-of-things.html>
[Accessed 20 April 2020].
- Patel, K. K. & Patel, S. M., 2016. Internet of Things-IOT: Definition, Characteristics, Architecture, Enabling Technologies, Application and Future Challenges. *International Journal of Engineering Science and Computing*, 6(5).
- Peppet, S. R., 2014. Regulating the Internet of Things: First Steps Towards Managing Discrimination, Privacy, Security and Consent. *Colorado Law Scholary Commons*, 93(85).
- Rose, K., Eldridge, S. & Chapin, L., 2015. *The Internet of Things: An Overview*. [Online]
Available at: https://s3.amazonaws.com/academia.edu.documents/48790442/ISOC-IoT-Overview-20151014_0.pdf?response-content-disposition=inline%3B%20filename%3DThe+Internet+of+Things+An+Overview+Under.pdf&X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=ASIATUSB6BAMI3BCT
[Accessed 29 April 2020].
- Scuotto, V., Ferraris, A. & Bresciani, S., 2016. Internet of Things: Applications and Challenges in Smart Cities. *Business Process Management Journal*, 22(2).
- Shah, V., 2019. *9 Main Security Challenges for the Future of the Internet of Things*. [Online]
Available at: <https://readwrite.com/2019/09/05/9-main-security-challenges-for-the-future-of-the-internet-of-things-iot/>
[Accessed 20 April 2020].

Symantec, 2011. *W32. Stuxnet Dossier*. [Online]

Available at: <https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-044.pdf>

[Accessed 20 April 2020].

1602836 Assignment 2 DI

GRADEMARK REPORT

FINAL GRADE

GENERAL COMMENTS

Instructor

82/100

PAGE 1

PAGE 2

PAGE 3

PAGE 4

PAGE 5

PAGE 6

PAGE 7

PAGE 8

PAGE 9

PAGE 10

PAGE 11

PAGE 12

PAGE 13

PAGE 14

PAGE 15

PAGE 16

PAGE 17

**DANIEL
INCE**

0

RESEARCH-INFORMED LITERATURE



There was evidence of extensive further reading and research from credible and reliable sources. Your interpretation and understanding of the additional research was very good and demonstrated a deep underlying appreciation of the subject. Your references were consistently applied and appropriate to the task and your reference list was of an appropriate length for this assignment.

16/20

KNOWLEDGE AND UNDERSTANDING



The knowledge and understanding of the subject demonstrated by this assignment was generally excellent. There were very few gaps in your knowledge of the basic principles and your understanding of the higher level concepts was demonstrated to a high degree. You have demonstrated a highly competent critical understanding of the main concepts and expanded your knowledge well beyond that contained in the course notes.

33/40

ANALYSIS



Your analysis of the task was excellent, both in class and as shown in this assignment. You have demonstrated highly competent analytical skills and your approach to the task was highly logical. You carried out a detailed evaluation of the research and included an excellent conclusion. You have demonstrated a capacity for independent thought and your interpretation of the quantitative and qualitative data was excellent with sound judgements based on wholly valid arguments.

25/30

PRACTICAL APPLICATION AND DEP.



N/A

SKILLS FOR PROFESSIONAL PRAC.



In this assignment you have demonstrated skills in working individually and also collaboratively. Your written report was written in a professional and confident style, however you still need to be more efficient with your word count. The report was very well presented, with excellent diagrams in appropriate places, good sentence/paragraph structure and clear calculations.

8/10