

Phillip Rowe

by Phillip Rowe

FILE	7557_PHILLIP_ROWЕ_PHILLIP_ROWЕ_177757_5752162.DOCX (346.28K)		
TIME SUBMITTED	27-APR-2020 01:07PM (UTC+0100)	WORD COUNT	2996
SUBMISSION ID	125244938	CHARACTER COUNT	16099

Course: BSc (Hons) Electrical and
Electronic Engineering

Module: SGEE6000 – Electronic
Design

Assignment: Internet of Things

Name: Phillip Rowe

University number: 1602827

Date submitted: 27/04/2020

Word count: 2969

Contents

Table of figures	3
1. Executive summary	4
2. Research.....	5
2.1 The basics of the IoT	5
2.2 The origins of the IoT	6
2.3 Driving forces of the IoT.....	6
Interconnectivity of devices.....	6
Storage capacity.....	6
Analytics	6
Marketing Automation	7
2.4 Key concepts of the IoT.....	7
IoT definitions	7
Enabling Technologies	7
Connectivity models.....	7
Transformational potential.....	7
3. Security and privacy challenges	8
3.1 Insufficient testing and updating	8
3.2 Brute forcing and default passcodes	9
3.3 IoT ransomware and malware	9
3.4 Phishing Attacks	9
3.5 Data security and privacy concerns (mobile, web, cloud)	9
4. Consumer choice.....	9
5. Conclusion	10
6. Harvard Referencing	11

Table of figures

Figure 1- Example of IoT system - (Rouse, 2016).....	5
Figure 2- (GOYAL, 2019)	8

1. Executive summary

In this assignment an investigation will be made into the concept of the internet of things. Numerous sources will be used in order to develop sound knowledge of what the internet of things is, its first origins and also its driving forces. The key concepts of the IOT will be discussed and the ways in which the IOT will face security challenges upon its installation and life span. The privacy challenges the IOT will face shall also be discussed and also the different consumer choices customers can make. Conclusions will then be drawn on the IOT and the whole concept of the IOT evaluated.

2. Research

2.1 The basics of the IoT

In the broadest sense, the term IoT encompasses everything connected to the internet, but it is increasingly being used to define objects that "talk" to each other. (Burgess, 2018) To put it in simple terms, the internet of things is made up of devices which are all connected together. This could be like how simple motion sensors can be connected to smartphones, in order to give alerts to the mobile user. The concept of the IoT would be to allow multiple devices on a private internet connection to communicate to one another. The IoT allows all of these devices which are connected together to generate, collect and exchange data with as little human intervention as possible. The internet of things, or IoT, is a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers (UIDs) and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction. (Rouse, 2016) The IoT also can use artificial intelligence and also machine learning in order to aid the data collecting process in order to make collecting data easier, more efficient and more dynamic. Following below in figure 1 is a block diagram of what a normal IoT system can be constructed of.

Example of an IoT system

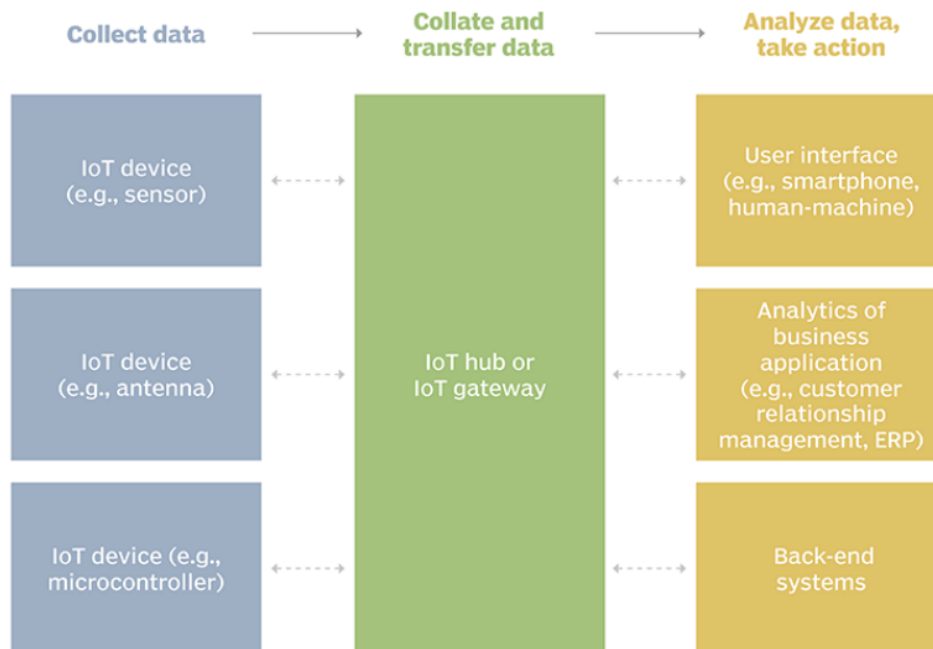


Figure 1- Example of IoT system - (Rouse, 2016)

2.2 The origins of the IoT

The term “Internet of Things” (IoT) was first used in 1999 by British technology pioneer Kevin Ashton to describe a system in which objects in the physical world could be connected to the Internet by sensors. (Rose, 2015) Whilst the actual term IoT is fairly new, the general idea of combining computers and networks in order to control devices has been around for decades. In the late 1970s, there were already systems in place which could remotely monitor electric meters on the electrical grid via telephone lines in commercial use. By the 1990s there were major advances in wireless technology which enabled machine to machine enterprise which provided industrial solutions for equipment monitoring. These developments were based on closed purpose built networks, compared to internet protocol networks. The idea of using internet protocol in order to link devices to computers is not a modern day idea, back in 1990 a conference took place in which a toaster was able to be turned on and off over the internet. In the years to follow other things were also enabled by IP such as a soda machine and a coffee pot.

2.3 Driving forces of the IoT

There are many driving forces behind the IoT. These all pose an aspect of the IoT which is needed in order to make it efficient and work in the best way possible.

Interconnectivity of devices

This driving force is currently receiving vast investment in order to accelerate the use of the IoT. This driving force addresses how each individual sensor or device will need to be connected together in order to make the best use of the IoT. The majority of devices used with the IoT, such as laptops, computers, tablets and smartphones are all able to talk to each other and exchange data, things like televisions, lights, showers, fridges and washing machines are being developed also. These other devices are being developed in order to exchange and accept data in order to execute actions with little or no human involvement.

Storage capacity

With all these numerous devices connected to the same network, constantly exchanging and collecting data over time it generates mass volumes of data. This data will then need to be stored and processed. When processing enormous data volumes there is only one storage facility that is capable of processing that data flawlessly and that is the cloud computing. When millions of intelligent devices send important health parameters to doctors all over the world, huge volumes of data are generated and only the cloud is capable of processing such data. (Pal, 2016) Over recent years very important developments have taken place in order to make cloud computing into the most powerful drivers of the IoT. Identity management solutions are under development in order to secure data security. There are constantly developments being made in order to make the cloud more scalable and efficient, this will coherently make the development of multi-platform – compliant devices excel. Since the IoT is over numerous devices and not just computers and laptops, the development of the cloud will make data exchange between other devices much easier.

Analytics

With the appearance of analytics as a service, it has given a big boost to the marketing campaigns. This is service which is sold to customers, they do not need a big setup or massive infrastructure in order to use the service. Analytics as a service is sold to the customer as a web application which

only needs a browser in order to work. This service is economic and convenient for the customer, whilst also benefiting marketing campaigns which need the continuous data being generated.

Marketing Automation

Many multinational giants are sponsoring the development of the IoT, these are mostly down to the commercial gains. With all the data that the IoT collects, if users allow data sharing then companies can use that data and tailor their marketing campaigns to user's desires. The IoT can use customer's preferences, hobbies and professions in order to produce robust customer focused products and services. There is mass development into software which is able to automate marketing processes such as, customer data integration, customer segmentation and finally campaign management. Due to all of this, there is massive investment being made into creating and manufacturing intelligent marketing automation systems. These systems will be able to capitalize on key information in which devices of the IoT collect. The intelligent marketing automation applications need true, key and actionable customer data which the IoT is able to provide. Therefore the IoT and marketing automation are both dependant on each other.

2.4 Key concepts of the IoT

There are many concepts of the IoT, they each serve as a foundation for exploring each opportunity and also each challenge that is presented to the IoT.

IoT definitions

The term IoT refers to situations in which network connectivity and also computing capability is extended to things such as objects and sensors which everyday items but are not considered computers. These everyday items will be allowed to consume, generate and share data with little human intervention. There isn't a single, universal definition for the IoT.

Enabling Technologies

The idea of merging computers with sensors and putting them on the same network in order to control and monitor devices has been around for decades. There are however things which such as IP based-networking, computing economics, miniaturization, advances in data analytics and the rise of cloud computing have excelled the close reality of using all of these devices on the same network and making them one system which shares data together.

Connectivity models

There are a wide range of technical communication models in which the IoT implements, each of this will have their own characteristics. There are 4 common communication models which are described by the internet architecture board. These include Back-end data sharing, device to device, device to cloud and finally device to gateway. These 4 common models show how flexible the IoT can be when choosing a way in which to connect its network. Any of the 4 models can be used in order to provide value to the user.

Transformational potential

If current projections and trends become a reality, there may be a shift as to what implications and issues may arise from a world that is becoming so interconnected. There are some predictions that the IoT will become "hyper connected" to the world where every day basics will be controlled by AI and other devices. There are no known limitations as to where the IoT can go. As people become more inclined to let technology into their lives and homes, the market for Internet of Things (IoT) devices flourishes. (Sargent, 2019) Following recent articles written, as more and more people use

IoT systems in their homes such as Amazon's Alexa, the transformational potential is astronomical. With the investment and development from big commercial companies into things like cloud computing, marketing automation and more high tech everyday machines, the growth is likely to be massive within the next decade. In recent years the transformation of the IoT in the agricultural industry has grown massively, with predictions of even more growth to come. IoT solutions' adoption for agriculture purposes is growing constantly, like there is BI Intelligence that has predicted that number of agriculture IoT device installations will hit 75 million by the year 2020. (GOYAL, 2019). As seen in figure 2 is a flow diagram of how the IoT works in the agricultural sector. There are many other sectors which are expecting exponential growth such as the manufacturing industry, food processing industry and also the medical industry.



Figure 2- (GOYAL, 2019)

3. Security and privacy challenges

There are many different challenges the IoT is facing. Security and privacy are two of the most challenging things to achieve. When purchasing a device which is part of the IoT, the customer will want a certain level of security and privacy in order to protect the data the device is collecting. According to (Harper, 2017) There are over 23 billion IoT connected devices worldwide. The astonishing number of IoT connected devices brings numerous challenges.

3.1 Insufficient testing and updating

Since the market is so competitive to sell the most amount of IoT devices, some companies can make careless errors which taking on the topic of device related security risks. Most of the devices made will not get enough updates and some not get any updates at all. This will then mean that when the device was initially bought, it was secure. As time goes on the device without updates, becomes outdated and will be prone to hacker and other security issues. This fact was actually demonstrated in early computer systems, until automatic updates were made available. Most manufactures actually only offer firmware updates for a short period of time until their own newer device is being made, shifting all of their focus to it.

3.2 Brute forcing and default passcodes

In recent years there was a DDoS attack called “The mirai botnet”. This was referenced as the best example of the issue which comes from IoT devices being sold with default passwords, and the customers not being told to change these when they receive their device. There needs to be a massive shift to the instructions which are sent with IoT devices, stressing the security issues that can occur if default credentials aren’t changed.

3.3 IoT ransomware and malware

According to (Shah, 2017) The rapid rise in the development of IoT products will make cyberattack permutations unpredictable. Modern day cyber criminals have become much more advanced, they are now able to lock out consumers from using their device. Once the hackers have hacked say a security in a private home and lock the user out, they are then able to access personal data. The hackers could then ask the victim to pay large sums of money for the safe return of their data, this is what ransomware is.

3.4 Phishing Attacks

The term phishing is already known well across the enterprise technologies, the IoT is on the uptrend with regards to phishing. Hackers could send a signal to an IoT device that triggers numerous complications. (Lerner, 2019) The most common type of phishing is false emails. The user thinks the email is legit when it asks them to enter their personal credentials, once they have done this the hacker now has access to the whole network of IoT connected devices. This is down to the fact that most users use the same password for multiple devices.

3.5 Data security and privacy concerns (mobile, web, cloud)

Data security and privacy are one of the most important issues in the modern world. With the IoT data is constantly being transmitted, stored, harnessed and processed by large companies, they use a wide variety of devices such as smart TV’s, lighting, smart thermostats and connected printers. During normal operations, all data collected is shared or even sold to numerous companies which violates privacy rights furthering public distrust. There is a blatant need for better legislation, this would include rules of how personal data is able to be cached, used for the correct purpose and then disposed of when not needed in order to protect the consumer. There are a wide range of devices available which can connect to the IoT. Whilst the production of these devices is booming, once these devices become outdated, updates tend to stop once the device becomes older or the manufacturing company shifts focus to a newer device.

4. Consumer choice

There is a wide range of existing and upcoming devices to choose from to integrate into a customer IoT system. There are common devices that can be bought individually such as cameras, door bells and smart TV’s however, some companies however offer package deals where they sell a totally integrated system. The totally integrated system offers the consumer a wide range of advantages

such as they are easily integrated, easy set up guides, cost savings with package deals and also a good customer service program. There are many other devices which can be bought on their own however, there are some issues with some devices being able to connect to the other. Some of the set up guides may prove too much for certain consumers and could be off putting. This is why more and more companies are trying to push the sale of “totally integrated systems.”

5. Conclusion

To conclude on the research carried out in this assignment, the IoT is on the upwards trend and will inevitably continue to become more crucial in everyday life. By using analytics and market automation strategies, the IoT is making it easier to use consumer data and turn that data into a brand new product or service. Whilst there are some major concerns with how secure the IoT is, with the development and investment from massive corporations the security will massively improve. There does however need to be legal duties set for companies to comply with, in order to avoid another devastating DDoS attack as seen in previous years. The proof of how effective the IoT is can be seen in the agricultural sector as discussed previously, the agricultural sector has become basically completely automated with the use of smart devices connected to the IoT. Whilst there are concerns with security, the advantages of the IoT massively outweigh the disadvantages. The new integrated devices being brought out are enabling consumers to totally automate everyday life, as well as providing a massive shift with industrial industries. The potential changes the IoT can make to the way in which our data used is huge, if used correctly companies could use the data that consumer devices are collecting and then tailor products and services to customers specific needs. The overall conclusion of the IoT is that providing new software and security protocols are taken, then the with the current investment rate and drive behind the need for new IoT devices, the IoT will develop its way into the majority of the populations normal living conditions.

6. Harvard Referencing

- Burgess, M., 2018. *wired*. [Online]
Available at: <https://www.wired.co.uk/article/internet-of-things-what-is-explained-iot>
[Accessed 18th April 2020].
- GOYAL, A., 2019. *Business of apps*. [Online]
Available at: <https://www.businessofapps.com/insights/internet-of-things-iot-agriculture-sector/>
[Accessed 18th April 2020].
- Harper, A., 2017. *peerbits*. [Online]
Available at: <https://www.peerbits.com/blog/biggest-iot-security-challenges.html>
[Accessed 18th April 2020].
- Higgins, D., 2018. *EY*. [Online]
Available at: https://www.ey.com/en_gl/advisory/how-to-unleash-the-transformational-potential-of-emerging-tech
[Accessed 16th April 2020].
- Kranz, M., 2017. *networkworld*. [Online]
Available at: <https://www.networkworld.com/article/3239298/new-gen-technologies-make-iot-transformational.html>
[Accessed 18th April 2020].
- Latham, M., 2017. *The Internet of Things and the Transformational Power of Data*. [Online]
Available at: <https://blog.recurly.com/iot-and-the-transformational-power-of-data>
[Accessed 17th April 2020].
- Lerner, S., 2019. *Enterprisedigi*. [Online]
Available at: <https://www.enterprisedigi.com/iot/articles/iot-security-challenges>
[Accessed 19th April 2020].
- Pal, K., 2016. *techopedia*. [Online]
Available at: <https://www.techopedia.com/2/31275/trends/big-data/what-are-the-top-driving-forces-for-the-internet-of-things-iot>
[Accessed 18th April 2020].
- Rose, K., 2015. *THE INTERNET OF THINGS*. 1st ed. s.l.:The Internet Society (ISOC).
- Rouse, M., 2016. *Tech Target*. [Online]
Available at: <https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT>
[Accessed 18th April 2020].
- Sargent, J., 2019. *sd times*. [Online]
Available at: <https://sdtimes.com/iot/iot-is-the-next-digital-transformation/>
[Accessed 18th April 2020].
- Shah, V., 2017. *readwrite*. [Online]
Available at: <https://readwrite.com/2019/09/05/9-main-security-challenges-for-the-future-of-the-internet-of-things-iot/>
[Accessed 19th April 2020].

FINAL GRADE

GENERAL COMMENTS

Instructor

55/100

PAGE 1

PAGE 2

PAGE 3

PAGE 4

PAGE 5

PAGE 6

PAGE 7

PAGE 8

PAGE 9

PAGE 10

PAGE 11

GRADING FORM: CSG-RUBIC

PHILLIP ROWE

0



There was evidence of further reading and research with the inclusion of a reference list and appropriate in text referencing. Your interpretation and understanding of the additional research was good. Your references were appropriate to the task and your reference list was of an appropriate length for this assignment.

12/20

KNOWLEDGE AND UNDERSTANDING



The knowledge and understanding of the subject demonstrated by this assignment was reasonably detailed and mainly accurate. There were very few gaps in your knowledge of the basic concepts and your understanding of the higher level concepts was demonstrated to a limited degree. Further work – Your explanations need to be more detailed and written with a greater emphasis on critical evaluation rather than description.

20/40

ANALYSIS



Your analysis of the task was generally satisfactory, both in class and as shown in this assignment, however it did tend more towards descriptive rather than analytical. You have demonstrated some analytical skills and your approach to the task was logical. You wrote a short conclusion that demonstrated some skills in analysing quantitative and qualitative data, however this was generally basic in nature.

16/30

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.

7/10