ELEN 7046– Software Technologies and Techniques

Assignment 2: The Internet of Things

May 2015

Name	Student Nr
Adrian Freemantle	1307968

Abstract

The Internet of Things (IoT) is the extension of the internet into new areas of our lives through smart devices and sensors (things) that have the ability to communicate and interact with their environments, infrastructures and other things to generate data. This will lead to the Internet being ubiquitous in every aspect of our lives and in present in all technology. These connected things differ from traditional “command and control” technologies in that they are able to leverage off the power Big Data analytics and remote computing. New technologies will need to be developed to deal with the increased volume of connections and data collected while issues such as security, privacy and common standards pose significant challenges to the adoption of IoT.

Table of Contents

1 Introduction

The Internet of Things (IoT) is the introduction of affordable sensors and devices (things) that are able to connect directly to the internet in order to gather more data from a wider variety of sources than before. It represents a merging of the physical and digital worlds and will change the way we interact with technology and will affect nearly every aspect of our lives.

Section two of this paper will provide a detailed description of what the Internet of Things is and what makes it different from traditional remote “command and control” type systems. The evolution of the internet and its expansion into every aspect of our lives will be explored and the way data is acquired, processed and analysed locally and remotely will be discussed.

Section three of this paper will provide an overview of Big Data and the analytics behind it. The relationship between the Internet of Things and Big Data will be explained and the difference between Big Data and a normal data solution will be discussed.

Section four of this paper will look at some real-world applications of the Internet of Things and the author proposes that most use cases can be broken down into either automation focused or people focused solutions. The differences between these two categories will be expanded upon.

Section five of this paper looks at the problem posed by a lack of common standards and proposes that the existing standards used by the World Wide Web are a potential solution to the problem.

Finally, section seven looks the technological, security and privacy challenges facing the adoption of IoT and provides examples of various risks posed and the potential for abuse of personal information.

2 The Internet of Things

The Internet of Things (IoT) represents the merging of the physical and digital worlds. It has been defined by ARM and Freescale as the use of smart devices and sensors (things) that interact and communicate with their environments, infrastructures and other things to generate data which result in actions to “command and control” things, inform decision making and enhance the quality of life for human beings [1].

Billions of these things will be connected to the Internet to form a *“universal global neural network”* in ways that will profoundly affect our lives [1] and lead to the next evolution of the Internet [2]. Large volumes of data will be created and stored as these things interact with human beings, each other and their environments, leading to the emergence of so called ‘Big Data’ [3] solutions.

Much of the technologies used in IoT are already familiar to us. “Smart Homes” in which thermostats, digital timers and light sensors are used to control and regulate our living areas while communicating via protocols such as Bluetooth and Wi-Fi have been around since the last century [4].

While the concept of IoT and most of the technologies used by it are not new, Cisco Internet Business Solutions Group estimates that IoT only came into existence between 2008 and 2009. They define that as the point in time where the number of things connected to the Internet exceeded the number of people connected to it [2].

2.1 The difference between IoT and Traditional Solutions

The primary differences between traditional and IoT solutions are the way in which things make decisions and the way in which data are used to support the decision-making processes [4]. As an example, we will consider the difference between a traditional and an IoT based climate control solution.

In the traditional solution, a thermostat sensor will be used to monitor the temperature within a room. This sensor data will be provided to an embedded controller within an air conditioner. The embedded controller will make a binary decision against a pre-set value as to whether to warm or cool the room. The decision-making process operates in isolation of other systems and does not take historical trends into account. [4].

An IoT solution would consider factors such as whether anyone was home, which rooms are normally occupied at a specific time of day and may incorporate information from motion sensors used in security systems. It will be able to learn what settings are preferred and will proactively adjust a room's temperature. A local or remote data repository can be used to support this decision-making processes and to store current sensor data. The important aspect here is that the embedded controller can communicate and integrate with a variety of sensors and smart devices as well as the ability to use historical data detect trends [4].

2.2 The Evolution of the Internet

The Internet is a physical interconnected-network of networks that globally connects devices through hardware such as routers, switches, cables, wireless transmitters and other equipment using the Internet Protocol (IP). It is used for the rapid and reliable transfer of information between one connected device and another [2].

While the Internet is a physical network, it differs from the Word Wide Web (WWW) which is a logical application-layer that uses the Internet to transport information using protocols such the Hyper-Text-Transfer-Protocol (HTTP) [2].

While the WWW has undergone extensive change since its inception the Internet has maintained a relatively stable rate of change. Its current functionality does not differ significantly from original functionality developed in the ARPANET era [2].

IoT is significant in that can be the first major change to the Internet's reach and infrastructure. Small Internet-capable things are extending the range of the Internet into new areas such as the human body, animals, plants, cars and nature [2]. It has been predicted that this evolution of the internet will have a larger impact on the computing world than *the fixed Internet wave and the mobile wave combined* [5].

2.3 Smart Devices

Almost every electrical device is now manufactured with some form of embedded-processing and sensing capabilities. This is combined with programmability allows the execution of basic “command and control” functionality [1]. The prevalence of this embedded processing, sensing and programmability in modern devices is the foundation for enabling the transition to smart devices [2].

Embedded processing alone is not sufficient for a device to be classified as “smart”. Remote communication and the ability for the device to uniquely identify itself are key properties of a smart device. Radio-Frequency-IDentification (RFID) is proving to be a popular technology for the identification of smart devices within the IoT [5].

2.4 Remote Communication

Smart devices require some form of remote communication to aggregate and analyse the collected data for useful trends and behaviours. This communication can be established directly with cloud-based computing services or relayed via local hubs or gateways that aggregate the data collected from a variety of sensors and smart devices [1].

2.5 Remote Computing

Remote or cloud-based computing is an effective way of dealing with energy constraints and limited processing capacity of embedded processors on battery driven smart devices. The power of cloud-based processing combined with the analytics derived from the aggregation of data from multiple things improve the overall intelligence and automation capabilities of an IoT solution [1].

3 Big Data and Analytics

The phrase Big Data is can be used to describe a situation where the volume, variety and velocity of data are significantly higher than traditional systems. The veracity or quality aspects of the data are also taken into consideration as this has an impact on the reliability of the analysis results [6].

Each thing on the Internet of Things can generate massive volumes of data as the sensors and embedded processing capabilities of these smart devices are able to capture more data at a higher rate than before. The exponential increase in the number smart devices connected to the internet in turn lead to an corresponding increase in the amount, variety and the rate at which digital data is being generated and analysed [3].

3.1.1 Volume

The quantity of data is growing at an exponential rate. This is reflected by the fact that the aggregation of the world’s total data is measured in zettabytes (ZB) with a single zettabyte being equal to a billion terabytes [6].

In 2009 the total amount of data in the world was estimated to be 0.8ZB. This grew to 1.8ZB by the end of 20011 with predictions that 35ZB of data would be reached by the year 2020 [6].

The infrastructure required to store, retrieve and process these volumes of data is significant. Frost and Sullivan estimated that the revenue for European datacentre facilities will grow from $2.83bn in 2013 to $5.27bn in 2018 [7].

3.1.2 Variety

The variety of data sources and formats pose new challenges to analytics. Unstructured and semi structured data such as Twitter feeds can contain valuable data such as customer sentiment or predict trends in customer behaviour. Being able to extract this information will require specialised software and new ways of analysing the resulting data [6].

An example of such a Big Data solution would be performing semantic and tonal analysis of a telephone conversation within a customer in a call centre. Combining this data with the client's history could provide trend analysis on how likely the customer is to remain with the company [6]

3.1.3 Velocity

Velocity is the time it takes from the capture of data to the moment where it is actionable or understandable. This can be quantified as the opportunity cost between the time of data capture to the when the analysis of the data provided valuable or actionable insights [6]. The shorter this time difference, the lower the opportunity cost.

An example of such a Big Data solution would the high-speed analysis of stock market information at a rate of *10 million messages per second with 10 microseconds of latency* [8].

3.1.4 Veracity

Veracity refers to the quality aspects of the data, such as validity, accuracy, reliability and trustworthiness [6]. Larger varieties of data sources combined with the unstructured nature of data can result in a garbage information that is irrelevant or directly misleading.

A Big Data example of this problem would be determining if a Tweet with the word "Clientele" referred to the insurance company or the concept of a customer base.

3.1.5 Context

Context is defined by the Oxford dictionary as "*the circumstances that form the setting for an event, statement, or idea, and in terms of which it can be fully understood*". This is an important aspect of Big Data as the data was captured within a specific context, where the context can include aspects such as a geographical location, time, date, and any other information which provides perspective from which to interpret the data [9].

4 Real World Applications of the Internet of Things

Any attempt at capturing a comprehensive list would be futile as new applications are constantly being invented. It is the authors opinion that most IoT solutions can be categorised into two distinct groups; automation focused and people focused.

4.1 Automation Focused

Automation focused things consist of millions interconnected devices that primarily focus on the automation of processes through “command and control” capabilities as well as the tracking and routing of goods and items [1]. The aim of this type of IoT system is to simplify people’s lives through the automation of tedious, dirty and time-consuming tasks.

Communication in this category tends to focus on, machine-to-machine, machine-to-infrastructure and machine-to-nature communication with use cases including asset tracking, home automation, environmental monitoring and smart traffic management.

4.2 People Focused

People focused IoT is centred around the analysis of personal data with the intention of gaining insights into the behaviour of people, their social connections, socio-economic status, health and even sexual orientation [10].

Given that some smart-phones contain sensors such Global Positioning Systems, accelerometers, microphones, cameras, biometrics monitors and data such as call logs and message logs, activity history and installed applications, it is easy to see the value and potential for abuse posed by the data made available by these devices.

This is a contentious area of IoT as it raises many ethical questions and blatant violations of privacy are not uncommon [10], however the argument can be made that this type of data can be used by governments to provide better service-delivery and identify crime hot-spots [10]. None the less it is easy to see how this data can be used to assign “category” to an individual or group of individuals [1] for discrimination purposes.

4.3 Use Cases

The number of applications are nearly limitless, these include; Smart Cities, Smart Environment, Smart Water, Security & Emergencies, Smart Retail, Smart Logistics, Industrial Control, Smart Agriculture, Smart Animal Farming, Smart Homes and eHealth [4]. Two use cases will be examined in detail to provide an overview of the vast potential of the IoT.

4.3.1 eHealth

Electronic Health, eHealth or Tele-Health is the *remote or real-time pervasive monitoring of patients, diagnosis and drug delivery* [1].

A study by Doryab et al. (2014) investigated the possibility of using smart phones to monitor patients diagnosed with Major Depressive Disorder (MDD). The study aimed to determine whether behavioural changes of patients could be used to predict the onset of

MDD. The behavioural changes would be determined from the analysis of data captured by the patient's smart phone [11].

The application captured a variety of sensor data including; noise amplitude, location, light intensity and movement. The behavioural patterns of the patient were tracked by monitoring movement, application usage, call logs and text message logs [11].

While the sample group from the study was too small to make any conclusive findings, the innovative use of the sensor data and personal information available on a smart phone for medical purposes provide insight into the future use of IoT in healthcare.

4.3.2 Smart Cities

The field of urban dynamics uses computer simulation to predict the effects of new social policies in order to refine them before implementation [12].

> *Urban dynamics theory views the city as a complex social and economic system formed by the interactions of individual efforts to achieve personal goals [12]*

Gathering social and demographic data is extremely expensive and time consuming. With the advent and massive adoption of social media it is possible to analyse a huge amount of publically available geotagged-data.

Geotagged social-data can be used to determine the sentiments of a population group around aspects such as poverty, crime, or reaction to a specific event. This provides local governments and policy makers with a "real time" geotagged view on the status and mood of a population group or area [10].

An additional application of geotagged social-data is that it provides insights into the way a population group moves within a city. This allows city planners to better understand the needs of future transport networks [10].

5 Standards

The Internet already has communication protocols such as Internet Protocol (IP) and Transmission Control Protocol (TCP) for the transport of data packets from one thing to another, however communication between heterogeneous things is still problematic due to the number of proprietary standards and protocols being used [4].

A universal application-layer protocol is required that will allow smart devices, sensors, hubs, gateways and cloud servers to communicate regardless of the specific hardware or software platforms used to implement them. Such a protocol should be *lightweight, standard, loosely coupled, flexible and simple* [4].

A family of protocols that meet these needs already exist and are the basis of the World Wide Web. Uniform Resource Identifiers (URI) are used to uniquely identify any resource or device on the Internet [13] and functionality can be accessed via various standards such as REST based interfaces or the WS-* standards. Additionally data can be provided in many standard formats such as XML and JSON [4]. It seems that the WWW and its standards and protocols may provide a solution to the interconnectivity and integration challenges posed.

6 Challenges and Barriers

The number of challenges facing the widespread adoption of IoT are extensive and much work is required to address problems with security, cryptography, trusted architectures, data mining, privacy and standards adoption [5].

6.1 Moore's Law and IoT

Research has found that the Internet and the processing power of cloud-based solutions has continued to grow in accordance with Moore's Law [2]. A significant problem however is that the rate at which new things are being connected to the internet and the volume of data they will be capturing will rapidly exceed the capabilities of even the best distributed systems [2].

Distributed computing solutions of the future will require new processor architectures as well as new networks with increased bandwidth and lower latencies. This will need to be done while addressing the challenges of security, performance, energy requirements and the cost of equipment [1].

6.2 Security

Security has and always will be challenge to any device connected to the Internet. Some existing problems such as Denial of Service attacks and eavesdropping will continue to be a problem and will also apply to IoT. Emergent problems caused by the extremely distributed nature of the things that make up IoT include concepts such as node capture, where attackers gain access to the physical infrastructure of the IoT system, the risk of the physical theft of the sensors and devices, and finally the malicious destruction of infrastructure [5].

One example of the consequences of attackers gaining access to the physical infrastructure in IoT is that they can convert unsecured things into bots that are used to perform a variety of malicious activities such as Distributed Denial of Services attacks or steal confidential information.

6.3 Privacy

The data being collected by many IoT solutions go beyond what they need to perform their function. Consumers are also increasingly less aware of what personal data is being collected, when it is collected and how it will be used [5].

The invasion of privacy is not only happening in an anonymous manner. The increasing number of applications and solutions that allow parents to monitor their children are creating societal tensions that are not yet fully understood and recent studies have shown *that the use of IoT in the household could prove especially disruptive* [5].

The analysis of social media data can also be used to determine personal and sensitive information about an individual. One study found that the sexuality of a person could be inferred from the publically reported sexuality of their immediate social circle [10]. American Express has been found to reduce credit card limits due to an individual being socially connected to specific activities, events or places that are associated with poor repayment of debt [10].

7 Conclusion

The Internet of Things (IoT) is first major change to the infrastructure of the Internet. Billions of things will be connected to the Internet and that will gather data about everything. The Internet will truly become a fully interconnected-network of all networks. This merging of the physical and digital worlds and will change the way we interact with technology and will affect nearly every aspect of our lives.

Section two of this paper provided a detailed description of what the Internet of Things is and what makes it different from traditional remote “command and control” type systems. The evolution of the internet and its expansion into every aspect of our lives was explored and the way data is acquired, processed and analysed locally and remotely was discussed.

Section three of this paper provided an overview of Big Data and the analytics behind it. The relationship between the Internet of Things and Big Data was explained and the difference between Big Data and normal data solutions was discussed.

Section four of this paper looked at some of the real world applications of the Internet of Things and the author proposed that most use cases can be broken down into either automation focused or people focused solutions. The differences between these two categories were expanded upon.

Section five of this paper looked at the problem posed by a lack of common standards and proposed that the existing standards used by the World Wide Web may provide a potential solution to the problem.

Section seven looked the technological, security and privacy challenges facing the adoption of IoT and provided examples of various risks posed and the potential for abuse of personal information.

8 References

[1] Freescale Semiconductor, Inc., “Freescale,” July 2014. [Online]. Available: http://www.freescale.com/files/32bit/doc/white_paper/INTOTHNGSWP.pdf. [Accessed 15 May 2015].

[2] D. Evans, “Cisco Consulting Thought Leadership,” April 2011. [Online]. Available: http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf. [Accessed 15 May 2015].

[3] D. E. O'Leary, “‘Big Data’, the ‘Internet of Things’ and the ‘Internet of Signs’,” *Intelligent Systems in Accounting, Finance and Management,* vol. 20, no. 1, pp. 53-65, 26 March 2013.

[4] A. Gilchrist, A Concise Guide to the Internet of Things for Executives, RG Consulting, 2015.

[5] E. Alsaadi and A. Tubaishat, “Internet of Things: Features, Challenges, and Vulnerabilities,” *International Journal of Advanced Computer Science and Information Technology,* vol. 4, no. 1, pp. 1-13, 2015.

[6] P. Zikopoulos and et al., Harness the Power of Big Data, New York: McGraw-Hill, 2013.

[7] A. Venkatraman, “Growth in cloud and IoT lend momentum to European managed datacentres,” Computer Weekly, [Online]. Available: http://www.computerweekly.com/news/2240224750/Growth-in-cloud-and-IoT-lend-momentum-to-European-managed-datacentres. [Accessed 19 May 2015].

[8] P. Crosman, “Content Router Delivers 10 Million Trade Messages Per Second,” WallStreet and Technology, 15 April 2008. [Online]. Available: http://www.wallstreetandtech.com/trading-technology/content-router-delivers-10-million-trade-messages-per-second/d/d-id/1259428. [Accessed 19 May 2015].

[9] A. K. Dey, “Understanding and Using Context,” Georgia Institute of Technology, Atlanta, 2001.

[10] D. Tasse and J. Hong, “Using Social Media Data to Understand Cities,” Carnegie Mellon University, 2014.

[11] A. Doryab, J. K. Min, J. Wiese and J. Zimmerman, “Detection of behavior change in people with depression,” Carnegie Mellon University, 2014.

[12] L. E. Alfeld , “UNESCO - Encyclopedia of Life Support Systems,” [Online]. Available: http://www.eolss.net/sample-chapters/c15/e6-63-01-01.pdf. [Accessed 18 May 2015].

[13] M. Rouse, “URI (Uniform Resource Identifier),” TechTarget, September 2005. [Online]. Available: http://searchsoa.techtarget.com/definition/URI. [Accessed 20 May 2015].