

COMP1715 Scholarly and Academic Practice

Academic Paper

The Internet of Things in a Wider Urban Context

University of Greenwich

Usman Basharat

000874782

Word Count: 2486

# ABSTRACT

Technology has changed the world drastically. Hence, why Internet of Things is the future of technology. In this report, it explores how Internet of Things is going to run in the near future. This paper discusses the legal, ethical, logical, social, environmental and professional issues about this topic.

## INTERNET OF THINGS

### IS IT GOING TO ALL CHANGE?

Internet of Things (IoT) is a physical object that contains an internet-based system that can be controlled remotely. International Data Corporation is a telecommunication organisation that does an analysis on technology globally. They help make decisions to enhance technology. According to the Senior Vice-President of Research of IDC Vernon Turner, he feels, "The Internet of Things will give IT managers a lot to think about. Enterprises will have to address every IT discipline to effectively balance the deluge of data from devices that are connected to the corporate network." IDC predicts that Internet of Things can be introduced by 2020 and they feel that it could be a huge asset towards any organisation (Hudges, 2014).

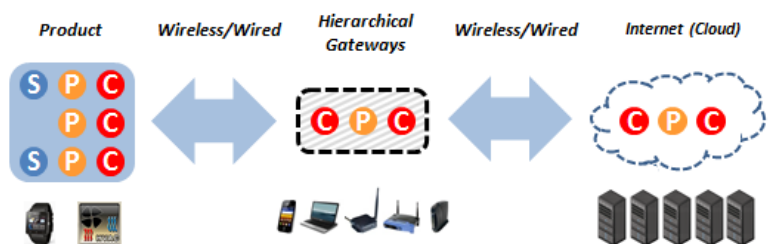
It seems ridiculous, but one example could be by reducing your heating temperature when you need before you enter your own home. However, having physical objects that are controlled remotely in a place of residence can have security issues. On the other hand, Internet of Things can revolutionise the perspective of the healthcare system, home facilities, transportation and retail stores (Abigail, 2015). Many different features can come into play in the next five years. Technology is rapidly increasing much of its developing innovation would enhance everything by making daily routines easier for consumers. By 2020, it is estimated that 50 billion objects connected to the internet (Strickland, 2015). The daily lifestyle routine will improve drastically.

### HOW IT WILL WORK?

Each category of the IoT will run differently. For example, sensors will be different depending on what is needed. For example, once the temperature sensor is activated this could be the presence of the person; it connects to the internet wirelessly and automatically predicts what the user requires. Imagine you walk into your own room, with your latest mobile phone; a sensor will detect the current date through your phone. Once this is complete, it will check the current weather allowing the temperature of the room to be either cooler or warm. This will be linked to any other devices, e.g. mobile phone to get the current day and weather, for the temperature being cooler, or warmer. Therefore, it would change according to the status. It predicts by using specific algorithms that will be made so precise that it predicts what

any person needs. Having different types of sensors would enable different type of products, or services, to work differently. Referring to Figure 1.1, it summaries it all by the product being connected to a sensor.

Figure 1.1 – A rough idea of how Internet of Things work



Referring to Figure 1.2, this shows only how many sensors are connected within one room. There will be over trillions of sensors in our smart world. As shown, each sensor should be able to detect and pick up information based on what the sensor will be about. The sensor is triggered functions by allowing it to collect data. This data is collected and stored within a cloud-based service.

Cloud computing is also involve and large groups of servers are grouped together to allow others for a use of service. Clouds can be classified as public, private or hybrid. Internet of Things will be looking to use Cloud storage to store data.



Figure 1.2 shows how many sensors will there be in one room

## The Internet of Things

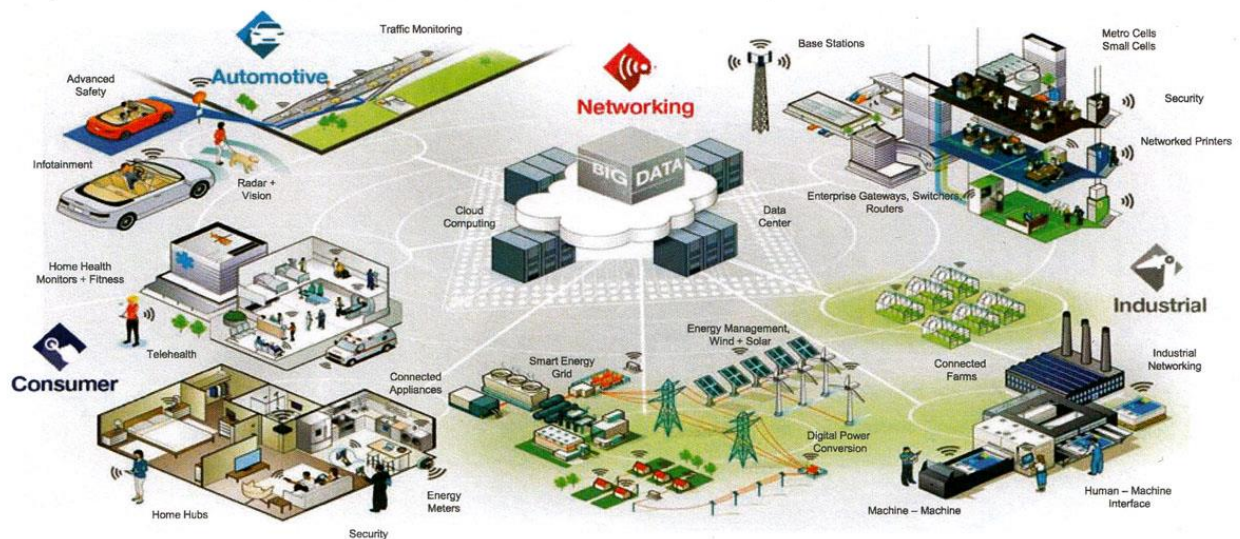


Figure 1.3 – A smart city

- I. HOME
- II. HEALTHCARE
- III. TRANSPORTATION
- IV. STORES

As shown on Figure 1.3, it clearly is evidence on how roughly our smart city would look like. Homes are going to be very much different. The difference is that sensors would detect the

weather to enable the home becoming more hot or cold by using the weather status on your phone. Therefore, if we come back from work cold, the sensors would pick that up from our phones as soon as we reach home, and put the heaters on. This is enabled by all devices to be connected with each other.

According to (Follett, J 2014), a beta test was carried out in a store. A beta test was set up in a store to test the sensors. The storeowners began to analyse the data during the test. As expected, the sensors were up and running. Once the store got busy, the results left the owners of the store to rearrange the middle floor. However, the problem was that the customers started to notice the sensors. This left them alarmed by avoiding the store because they thought something else might happen. To avoid this, sensors need to be small but be able to do its job. By using several of sensors such as camera sensors, activity sensors, it could benefit stores in many ways.

### **GOOGLE SAMSUNG APPLE**

Big businesses, such as Google and Samsung, have already started to take advantage of Internet of Things. All three companies have invested hugely already to start up with Internet of Things. According to (Rogers B, 2015), Apple was first with the most influence towards Internet of Things. Google have already purchased Nest for \$3.2 billion for home appliances whilst Samsung have touched upon Smart Home appliances too. Many companies want to take advantage of Internet of Things as it gains a reaping reward. As you can see Figure 1.4, this is one of Nest's products, as Google's latest purchase, called Nest Thermostat.



*Figure 1.4 shows the Thermostat from Nest*

### WHAT DO YOU EXPECT?

4G is the current generation of telecommunication. As we all know, many data is expected to be transferred and the data to be handled. As expected, 5G is the next major generation to improve the current one. This runs at a rate of 1TB per second. Internet Protocol is a unique numbers to identify each computer. As the population and technology keeps on growing, it enables more computers to be released and run. The current internet protocol version is IPv4. IPv4 is the current version of the internet Protocol. *IPv4* is a 32-bit and they are running out of IPs. IPv4 is worth  $2^{32} = 4,294,967,296$  addresses. An example of IPv4 is 156.15.259.3. As we, all want Internet to be fast, the population keeps growing; therefore, more IPs are needed. Therefore, *IPv6* is going to be released in 2020 and this is going to be 128 bits.

Referring to (Goldman Sachs, 2014), it is predicted that 28 billion devices can be connected to the internet. Comparing that number to the current population, 7.3 billion. All of these figures link as 28 billion devices will be used; IP addresses will be more than ever as more devices can be made; lastly, is the population will be around 8 billion.

Referring to Figure 1.5, it demonstrates the timeline of what to expect from the technology to come. This picture was released from 2014, therefore it predicts what to expect from then. However, you can see that Internet of Things is highlighted to be reached within 5 to 10 years. Many more advanced technologies is shown below too.

A case study shows that it leads a breakthrough figure of numbers by saving 55 million kWh of electricity. However, leading to the cost of the whole project, it will cost this \$7.1 trillion by 2020, (Sulleyman A, 2014). A question could be raised whether deprived countries and areas would be supported with these emerging technologies. However, those potential countries that become rich can invest in this huge project enabling their country to be cost effective. Would this enable people to migrate more?

Countries and people with a financial crisis cannot benefit with the technologies expected. This shows that the cost of the project leads to how it will take and how big the project is leading to changing the way we all live. How would people afford these devices?



Figure 1.5 Expecting what technology to get from more than 10 years. Year predicted at 2014.

# CHALLENGES WE FACE

Evidently, it is clear that technology makes human lifestyle easier to live. On the other hand, some of the technology might not appeal well of the elderly and disability. This is not professional. Some people, who are blind or deaf, are not even able to live the entertainment. Is this right? A blind person can obviously hear what is going on and touch on braille to read, but not watching what is going on does not fulfil the full potential.

Toddlers have clear issues with modern day technology that it has come to a stage of addiction. Referring to (Ward V, 2013), experts have given a strict warning that usage of iPads and iPhones can produce damaging long-term effects. "Children have access to the internet almost from birth now", this demonstrates that the mass increase in technology could cause serious illnesses, or injuries. Some of those include eyesight problems, neck injuries, back pain, addiction and causing some teenagers to become angrier. How long do we use the internet? On average, users spend every day on the internet. If Internet of Things were to invent such amazing ideas, it would enable users to constantly use the internet.

The future of technology is enhancing and this would attract more toddlers and young-aged teenagers to become addicted of using the Internet. Even more, this would attract adults too. (Woollaston, V 2014) On average, from 7:51am, many of us pick up our phones 1,500 times each week. Becoming addicted to the internet enables users to prolong their sociable activities to a later stage. Furthermore, most teenagers use social networking sites enabling them to go through an emotional trauma. Emotional disasters could lead to risk of teenagers being suicidal.

The culture of each person that they go with is different. Consider the following scenario: if any person were to buy an Indian takeaway only for one day, the person would receive emails based on the action and behaviour of the person. It only predicts what the user may want depending on what they need. It may predict something wrong. For example, if it is all new and I came back from work late, it would assume that I need some relaxing music to relax. However, the change there is that I want something of my taste. Some IoT sensors need to get use to each person being different and adapting to the cultural or atmospheric needs.

## SECURITY

Security may be at a huge risk even when Internet of Things emerge. An annual report is given out and every year huge amount of employees are employed to tackle security breaches. An unauthorised outsider attacked 55% of large businesses in the last year, (Gov.uk, 2014).

The USA Government has invested security in over \$13 billion in 2010. Security is a big issue. A case study shows that a malevolent attack on 700,000 devices were hacked by using refrigerators to get access to these devices, (Eric Bleeker, 2015).

These figures may have doubled by now. This shows that the government cares about the security of data. However, if the current stage is at that point, more security issues can be evolved. As mentioned above, 28 billion devices are at a stage of vulnerability. Even though the top priority is security of the whole project, it seems even more likely that the exposure of privacy can be exposed easily. If security is at risk at this point, how is security going to be maintained at 2020? If a rough figure of \$13 billion is currently spent on only security and the number of device usage is 10 times bigger; the number of money

spent could increase by 10 times too. How much more do you think money would be spent on to maintain and secure over 28 billion devices around the world?

One more thing we have to remember is that the current technology is expanding. Therefore, people are gaining access to more information on the internet than ever. Of course, when the new data is arrived, mistakes are made within it. If someone does something for them not too, they can get in trouble.

Furthermore, if hackers get access to one user's details, the hacker can access to all of the information of the users. Therefore, he can bribe the user to do things they do not want to do. Things are already in place, and without thinking, it shows that security threats are a bigger concern. This will get more complicated and hard to maintain. More legislations are needed to be in place in order for security to be secure. Use CCTV as an example. It is as if someone is watching you, wherever you go, whatever you do, when you do it; but you do not know whom it is. Some acts that can be put in place is not only knowing that there is a potential threat, but acting upon this threat. Investing more in security, because this can be done by putting more people in each city to check thoroughly of any big potential. Making sure people know what they are letting themselves into buy using these devices. Making sure devices are secured with the right security and level of protection.

#### *DATA PROTECTION ACT*

Vast amounts of data is processed as millions, or even trillions, of data being transferred. Top priorities should be held with security and privacy. This act was introduced in the 1990s for any organisation that deals with information that transfers data, which needs to be lawfully processed. This law was set as this is vital information was to prevent any data being exposed. For example if a user's information were to be hacked and expose, it would embarrass their privacy. A life insurance company had insurance on the user's information and it reveals news that he or she did not want to reveal; it would enable the life insurance not to insure on the person's life.

Security is at a top of the list for customers and companies. Therefore, when accessing any IoT element, or device, a solution could be the only way they can access it is by using the owner's fingerprints.

Everyone knows that keeping a strong password prevents emails being hacked easily. However, by raising this, it would enable users not to keep an easy password that someone can guess.

## **CONCLUSION**

Big companies have already started to take advantage of the future technology and investments are ongoing. I feel that, as exciting as it sounds, security and privacy is more the issue. Furthermore, vast amount of money is spent on this project. Only a few countries can take advantage. On the other hand, more people would be aware of security. Security should be the top priority as every department of technologies is enhancing.



# REFERENCES

- Cha, B. (2015). A Beginner's Guide to Understanding the Internet of Things. [Online] Re/code. Available at: <http://recode.net/2015/01/15/a-beginners-guide-to-understanding-the-internet-of-things/> [Accessed 30 Oct. 2015].
- DaCosta, F. (2013). Rethinking the Internet of Things. [New York, N.Y.]: ApressOpen.
- Eric Bleeker, C. (2015). *Your Credit Card Number Was Hacked by a Refrigerator -- The Motley Fool*. [Online] The Motley Fool. Available at: <http://www.fool.com/investing/general/2014/06/07/your-credit-card-was-hacked-by-a-refrigerator.aspx> [Accessed 12 Dec. 2015].
- Follett, J. (2014) *Designing for emerging technologies*.
- Goldman Sachs, (2015). *The Internet of Things: Making sense of the next mega-trend*. [Online] Available at: <http://www.goldmansachs.com/our-thinking/outlook/internet-of-things/iot-report.pdf> [Accessed 12 Nov. 2015].
- Gubbi, Jayavardhana, (2013). "Internet of Things (IoT): A vision, architectural elements, and future directions." *Future Generation Computer Systems* 29.7 [Accessed 29 Oct. 2015]
- Gov.uk, (2014). Information security breaches survey 2014 - Publications - GOV.UK. [online] Available at: <https://www.gov.uk/government/publications/information-security-breaches-survey-2014> [Accessed 12 Dec. 2015].
- Niewolny, D. (2013). How the Internet of Things Is Revolutionizing Healthcare. 1st ed. [eBook] Available at: [http://cache.freescale.com/files/corporate/doc/white\\_paper/IOTREVHEALCARWP.pdf](http://cache.freescale.com/files/corporate/doc/white_paper/IOTREVHEALCARWP.pdf) [Accessed 30 Oct. 2015].
- Roberto, I.Belda, (2014). Internet of Things: Advantages May Far Outweigh Its Drawbacks. Available at: <http://guardianlv.com/2014/01/internet-of-things-advantages-may-far-outweigh-its-drawbacks/> [Accessed on 16 Oct 2015]
- Rogers, B. (2015) Forbes Welcome, *Forbes.com*, [online] Available at: <http://www.forbes.com/sites/brucerogers/2014/07/08/apple-and-google-dominate-internet-of-things-influence-with-home-automation-efforts/> (Accessed 26 November 2015).
- Sulleyman, A. (2014). *IDC predicts an IoT riot: Internet of Things market to be worth £4 trillion by 2020 | IProPortal.com*. [Online] IProPortal. Available at: <http://www.itproportal.com/2014/06/06/internet-of-things-to-be-worth-trillions-consumers-and-businesses-thirsty-for-a-taste/> [Accessed 10 Nov. 2015].
- Understanding the Internet of Things (IoT). (2014). first ed. [eBook] Available at: [http://www.gsma.com/connectedliving/wp-content/uploads/2014/08/cl\\_iot\\_wp\\_07\\_14.pdf](http://www.gsma.com/connectedliving/wp-content/uploads/2014/08/cl_iot_wp_07_14.pdf) [Accessed 2 Nov. 2015].



VJ Nair, L. (2015). Security aspect of internet of things. [Online] MSys. Available at: <http://msys technologies.com/blog/2015/05/21/the-security-aspect-of-the-internet-of-things/> [Accessed 30 Oct. 2015].

Woollaston, V. (2014) Average user now picks up their phone more than 1,500 times a day, *Mail Online*, [online] Available at: <http://www.dailymail.co.uk/sciencetech/article-2783677/How-YOU-look-phone-The-average-user-picks-device-1-500-times-day.html> (Accessed 8 December 2015).

Ward, V. (2013). *Toddlers becoming so addicted to iPads they require therapy*. [Online] Telegraph.co.uk. Available at: <http://www.telegraph.co.uk/technology/10008707/Toddlers-becoming-so-addicted-to-iPads-they-require-therapy.html> [Accessed 4 Nov. 2015].

Zanella, A., Bui, N., Castellani, A., Vangelista, L. and Zorzi, M. (2014). Internet of Things for Smart Cities. *IEEE Internet of Things Journal*, 1(1), pp.22-32.

## IMAGES

- **FIGURE 1.1**

Surepass, (2015) *Sensors overview*, [Image] Available at: <http://surepass.org/wp/wp-content/uploads/2014/03/SurePass Internet of Things IoT Security Solution.png> (Accessed 11 December 2015).

- **FIGURE 1.2**

*Internet of Things, home sensors*, (2015). [Image] Available at: <http://blog.nxp.com/wp-content/uploads/2013/12/Livingroomautomation.jpg> (Accessed 4 December 2015).

- **FIGURE 1.3**

Regmedia, (2015) *Internet of Things Overview*, [Image] Available at: <http://regmedia.co.uk/2014/05/06/freescale internet of things overview 1.jpg> (Accessed 11 December 2015).

- **FIGURE 1.4**

Energycircle, (2015) *Nest Thermostat*, [Image] Available at: [http://www.energycircle.com/sites/default/files/images/catalog/nest\\_thermostat.jpg](http://www.energycircle.com/sites/default/files/images/catalog/nest_thermostat.jpg) (Accessed 10 December 2015).

- **FIGURE 1.5**

Hype Cycle, (2014). *Hype Cycle for Emerging Technology*. [Image] Available at: <http://cdn.geekwire.com/wp-content/uploads/2014/08/hypecycle444.jpg> [Accessed 5 Nov. 2015].