INTERNET OF THINGS

Everything about IoT and the loopholes

17001172

Contents

1. Introduction

This project goes through the Internet of Things, what it is and why it means so much in today's society. Internet of Things also known as IoT is around us everywhere, without realising but it has mass power to control ultimately anything with the use of new technologies to begin the process. It will go through what IoT is, the implementation process, history, how it's used and will focus solely on the issues it brings.

2. About IoT

IoT was coined from the Internet of Things, whereby plays a large role in the computing and technology field and was a paradigm shift known to be at the bases of nearly absolutely everything from sensors to the astonishing cloud. It is an eco-system of ever-increasing complexity which will essentially humanize every object in our life. It has the potential to turn real-life objects into virtual technical objects suggesting the reason behind its name of 'internet' and 'things'. It is important to quickly distinguish and understand these two variables individually before investigating looking at them as a whole.

The internet is defined by Slevin, (2007) as a 'global networks of interconnected computer systems, which creates the possibility of storage, retrieval, circulation and processing of information and communication across time and space', which also opened up the possibilities for new innovates. The internet is used by billions of individuals daily and has been around since the evolution of 1983, however, it wasn't until 1990 when Tim Berners-Lee established the World Wide Web. The internet uses the protocol TCP/IP to provide users all over the world. This mass network of networks has been successful since its growth so successful that the University of Oxford investigated how many users use the internet which resulted in over 7 billion individuals. Things, in this case, refer to any object which is noticed by the average person or any inanimate material object. Things conclude all electronic objects and subsequently, those which do not go into the category of for example gadgets.

These two words then make the phrase, Internet of Things, to which varies in definitions by different academics and scholars, some of which are, "it is the network of physical objects - devices, vehicles, buildings embedded with electronics, software, sensors, and network connectivity- that enables these objects to collect and exchange data" (Villena, 2016). It was also defined as, "the networked interconnection of everyday objects, which are often equipped with ubiquitous intelligence, IoT has the power to increase the ubiquity of the internet by integrating every object for interaction via embedded systems" (Wang et al, 2012). In addition to these, the Internet of Things creates a network in a global state allowing there to be communication between objects and people, for example, human to human, human to things and subsequently things to things. IoT opens up the possibility where anything and everything can be connected not just electronic devices, in a sophisticated way. For an object to fall under the category of IoT they are wired and linked to wireless or wired networks, doing so by using the internet IP, to which the objects are equipped with ubiquitous intelligence.

2.2 Before the implementation

Before implementation can begin of IoT, a process known as standardization components is undergone. It simply encounters the different hurdles of IoT before the implementation, from this there are 4 main aspects.

- *Platform*: this focuses on the design aspect of IoT devices, whether the developer focuses on a user interface or user experience. Analytics uses this step to ensure that during the implementation that the mass of data streams from all products in an extremely secure way.

- *Connectivity*: this looks at both day and night aspects, and whether when the end product is to be used for. The business perspective is used massively here when connectivity uses the Industrial Internet of Things are used, here machine to machine communications control the field.

- *Business model*: known as the motivation for the IoT, discussed as the motivation for starting, investing and operating any business without this step creates another hole, this step is used to ensure before the creation begins all requirements are considered.

- *Killer applications*: this set ensures that there are 3 vital functions are required, to have the 'killer application' which in other terms means well established. These include the controlling of things, collection of the data and the analysis which will be used.

2.3 Implementation

It has already been stated that for an object to become an Internet of Things, it is embedded with electronics and different components which will open up the collection and exchange of data. The process is not as simple as the objects must be equipped with ubiquitous intelligence to make them 'smart'. These components are shown in figure one.

Figure 1- components of IoT, Villena, (2016).

The first component of IoT is sensors, to which a journal produced by Lee and Sharma, (access date 05/02/2020) whereby defines and explains them as 'an electronic device that produces electrical, optical or digital data derived from a physical condition or event'. The sensors are used to gather and produce data that is transformed by another device, known as the output device, which is further used in decision making carried out by an advanced infrastructure or by a human. There are many different types of sensors particularly used to make an object IoT the two main

ones being active and passive, depending on many factors; the purpose of the object, whether it's for determining the temperature, the motion or bio. Other factors include accuracy if the object must be accurate to the smallest form a more precise sensor would be considered, reliability, range, and level of intelligence such as the dealing of noise and interference are other main factors when choosing the most appropriate type of sensor. The benefits of using sensors in the internet of things are due to their intelligence, the small and compact size makes it easy to fit into any object and the price of sensors is relevantly cheap. However, they require a high level of power and security.

The next component networks, this particular implementation is used in line with sensors to transmit the data produced by the sensors, its key to remember that networks alone have many components, routers, LAN, WAN and many more which are connected through established technologies like Bluetooth, Wi-Fi, Ethernets. Networks open the pathway for IPv6 development, Xas concept, small prices of data usage whilst consuming large data rates. The challenges networks face in the role of IoT is again, security, the coverage, power and enormous growth in the number of connected devices, Villena, (2016) estimates through a study over 50 billion devices will be connected to a network globally.

The component which comes next comes under the name of standards, which can mean many things, but in this case, it is a term coined to hold the handling, processing and storing of data which has been obtained through the use of component number one. To put these into further sectioned standards there is the use of technology standards: network protocols such as Wi-Fi, communication protocols, Http and data aggregation standards. Regulatory standards tend to less likely be used apart from in cases where the government sees fit, it is administrated by massive agencies such as HIPAA. Likewise, with each component there have been many encounters individuals faced when discovering the correct standard, many highlighted by Banafa, (2016) who states that the standard for handling unstructured data is considered, typically using SQL database language. Security and privacy issues are mentioned as a big sector to this, where there is a requirement to consider the need for retention, use, and security of data, and finally, the skills needed for these newer aggregation tools, whereby are used for the overall process of systems, including the execution and maintaining.

Intelligent analysis is used as the fourth stage, just like any other analysis in any field it uses the data collected from something (in this term the sensor) and is analyzed, typically through intelligent and cognitive technologies. Using cognitive technologies allows the analysis of data to be carried out in a sophisticated and visual form as well as predictive and prescriptive analytics. The cognitive technologies are adapted to be used within this process are '

- Computer vision: which looks at the visuals, and the computers' capability to identify and look in-depth at objects, scenes, and activities within images produced by the sensor
- NLP (natural language processing): similarly works the same way as computer vision however it focuses on text rather than the graphical side, it

extracts meanings or particular words that may relate to something from a piece of text.
- Speech recognition is used and uses the human's voice.

There has been researching carried out to prove that this step is becoming more used through the process of making something 'IoT', these include the growth in the software particularly cloud sourcing and open source software, which is known typically as the cloud developing the pathway for new algorithms and improvements. A typical place for this data to be analysed in the cloud.

Again, the challenges faced within this particular component is the inaccuracy of analysis which may occur because of the different flaws which it perceives, this inaccuracy may cause false positives or false negatives. The analysis of unstructured data can cause a major problem, as it proves to be a lot more difficult than analyzing structured data that legacy systems are best known for and unfortunately IoT devices are less known for.

The final process is intelligent actions, these are known as machine to machine, machine to human, human to human all with the advancement of user interface and user experience. They are widely used due to the small price of machines, machine functionality, and learning tools. Again, the challenges which follow the intelligent actions are the slow adoption of technologies, security, privacy, their actions in unpredictable situations followed by human behaviors.

2.4 How it's used

As mentioned IoT can be used to change any object into something of the internet, subsequently meaning turning any object into anything mechanical, electrical or a thing within an electrical system such as a building. Using the process of hardware to collect send and act on data as discussed above it results in communication between devices to make them smart and subsequently, easier for humans as there is no requirement for a human to human or human to computer interaction. To make it easier to understand, the collection of data could be sensors, antenna or microcontroller, which is then passed into an IoT hub or gateway and uses smartphones, human-machines, or other systems to analyze and further take control.

2.5 Why IoT is important

IoT has been known to change the lives of individuals for the better, helping life and work smarter whilst ensuring they have complete and utter control. It changes something from a basic form to a smart form. It has become essential to individuals and businesses through daily activities. Particularly with businesses it provides a real-time look into their systems focusing on every aspect, such as performance of the system, the GUI, the functioning and maintenance of machines and logistic operations. IoT allows the following:

- Monitors the general business process, which can include stock checks for shops
- Improves customer experience
- makes more revenue

- ensures there are fewer problems

IoT is extremely important in any field, however, it has been essentially important for agriculture, infrastructure and home industries which all in end increases the digital transformation. Doing so can ease the job of the individual at focus, for example for farmers the use of sensors can determine how much food is left for the animals or the temperature of a chicken farm, all very crucial and can be sometimes hard or an inconvenience for farmers. These are all determined by the use of sensors that monitors the changes and uses the cloud to process the data and further display on different devices such as a smartphone. The generating, collection and processing of acquired information allows these decisions to be made.

2.6 IoT at home

The convergence of technologies will ensure that life is much easier which would improve, whereby improves many aspects of life at home and work. Simply by the connectivity of household items through Wi-Fi to the internet.

Plugs

These are plugs developed to fit into a regular socket, when an object is connected to the plug it is then able to be controlled through the users' smartphone or tablet. The objects that tend to be used for these plugs are lights, heaters, fans or even kettles! An individual can even boil the kettle without being home.

Doorbells

This has proved to become extremely popular, with many more organizations producing their video doorbell product. It allows the homeowner to see who is at their door without having to move, again through their smartphone. It is also a means of keeping the house secure, as it allows videos to be seen from hours go, currently and can have a conversation with the individual at the door if the homeowner is not home.

Thermostat

Having a smart thermostat allows individuals to control their heating from anywhere in the world, if homeowners are on holidays particularly during the winter and are not arriving in till late or coming home late from work they can have the heating on before they get in. It has also been seen as a smart move as many individuals forget to turn the heating off before leaving the house, it is a money-saving product.

Home security system

This uses sensors, cameras, smoke detectors, and heat detectors to ensure that individuals within their home are safe, sending data to the cloud to be analyzed will determine whether an alarm should be activated. If for example, the camera senses someone outside the house the user will get a notification on their phone and will be given the chance to view who the individual is or more over what they are doing. If temperatures are rising or if the detectors detect smoke or heat increasing it can signal the individual first to notify them of these increasing changes before it reaches the alarming levels.

Lights and light switches

Having a system set in place which allows brightening or dimming to your preference is extremely suitable for homeowners, and particularly elderly who may be fragile and have no energy to get up to turn on or off the lights.

These IoT legacy systems are required to manage real lifetime events, such as the time a car enters or leaves a carpark which can automatically process whether a car has outstayed their time on the ticket using their registration number as well. Gartner, (2013) states by this year, 2020, the internet of things installed base will grow to at least 26 billion.

2.6 Standards, Protocols and Technologies

There have been many different ways discovered to make these day to day objects fall under the category of 'internet of things', this small section will go through the different standards it upholds and frameworks to be followed for it to be grouped within. One which was mentioned earlier as connecting to the internet IP. The following standards, protocols, and technologies are just many ways which enable the process to happen:

Internet protocol (IP)

Mentioned earlier the Internet protocol used today is version 6, however, either 4 or 6 can be used in the creation of IoT devices, it is the principal communications protocol that enables relaying datagrams across networks. The difference between 4 and 6 is simply the difference in the IP address, by which each one typically defines the address differently. Going into more detail each version has different classes by which the developer will decide on the most appropriate class; A, B, C, D, E. Whilst version 4 can still be used it is typically more seen for version 6 to be used, the reason for being is it has availability to over 85,000 trillion addresses and has sufficient support for the 21st century IP addresses.

IPv6

It is used on low power wireless personal area networks and is known to be an 'open' standard and defined by the internet engineering task force, it provides any low power radio the ability and opportunity to communicate to the internet, including the IP 804.15.4, Bluetooth with low energy and a z wave protocol which allows smart devices to connect.

ZigBee

Tends to be the standard used within bigger industrial settings and environments, focused on the Institute of Electrical and Electronics Engineers (IEEE) whereby the language of Dotdot is further used to ensure that smart objects communicate through a secure and versatile network.

one machine to machine

This particular framework uses a machine to machine structure in terms of a layer that is embedded within the object's properties or software to enable connectivity. It uses the global standard as part of the framework which overturns a reusable standard, creating the opportunity for numerous internet of things applications to interconnect.

Data distribution service (DDS)

This type of standard is used to provide real-time events, such as the time a car entered a carpark it is more frequently used for machine to machine communication due to its high satisfactory performance levels.

Amazon web services (AWS)

This is described as a computing platform for IoT developed and produced by Amazon, it interconnects the AWS cloud to ensure easy communication and security.

Google's brillo

Similar to amazon it is a platform created for quick process of implementation of IoT, with the use of brillo and android os as the main structure to the framework. It is particularly used for those which require limited or very small amounts of power, whilst using Weave as the communication protocol served between the object and cloud.

Arm Mbed

This framework is essentially used for the development of microcontrollers of IoT devices, which has been known to serve as a connected, secure environment.

Electronic product code (EPC)

This is a 64 or 98-bit code which is typically recorded on an RFID tag and is used for the development within barcode systems, the data stored in the code refers to properties such as type of EPC, the serial number of the product, its specifications, and manufacturer.

Barcode

This is another way of encoding data about a product, however, it can make use of numbers and letters with different sized black bars with different spaces in between.

Wi-Fi

This networking technology allows devices and other compatible technologies to communicate over a wireless signal, for high-speed communication it uses Wireless Local Area Networks. WLANs are typically used within cafes, offices, big organization buildings, and airports.

3. History of IoT

After distinguishing what the internet of things is, it is hard to imagine a world without smart technology or even the cloud as storage. The discussion of the subject has

been around since the 1970s however, it only was properly established in 1999 by an intellectual named Kevin Ashton who then, worked at Procter and Gamble. A company based in America whose mission is to distribute packaged goods across the world. The term internet of things was formed during his presentation to the senior management where he established the success of the RFID (radio frequency identification) a new technology then could create. During this presentation, he empathized that if devices or objects were 'tagged' as such computers and other future devices could have control over these objects. The first application which used the internet was in the 1980s, however, imperfect the coke machine used the web and different programs which would determine if there was a cold drink or not. However, it wasn't until 2010 that IoT began its road to success.

This year showed a lot of improvements in the use of the technology, with the government of China making a prompt stating that the IoT would be a major priority in their 5-year plan. Google had already tackled the internet of things with introducing their new street view service, which stored data of individual's Wi-Fi networks

With the increased talk of IoT, it was the year 2013's feature during LeWeb, known to be the biggest internet conference and show within Europe, helping those people with a passion of technology to deepen their understanding of new technologies and what the technology is. It was at this point the phenomenon of IoT was the center of attention, featuring in newspapers and tech magazines such as Forbes. During this year the IoT developed into more than technologists thought with the use of wireless communications and microelectromechanical systems to embedded systems, (Foote, 2016). This field had opened up an endless list of interconnectivity to devices, the creativity of IoT devices has and will be developed throughout many years to come, however, since its evolution there has also been an endless list of potential security and privacy problems.

4. IoT loopholes – Security and Privacy

The use and more importantly the development of IoT has been proven by many scholars and intellectuals that the main downfall and urgent concern of this internet of things are the security and privacy it lacks. The first problem is the privacy of customers or individuals in shops, centers, entertainment centers, transport centers, hotels, anywhere really.

Without awareness these individuals are captured and recorded through the use of sensors and cameras and have information collected and stored without any consent, however, this is allowed as part of security measures within buildings and has many signs which can be seen as 'CCTV'. The data stored from these different devices can be exploited through privacy and security issues much easier than first thought.

The communication infrastructure enabled from IoT is flawed, whereby results in a mass loss of privacy for the users, the flaws can happen through all the different connections and layers within the various spheres, or simply through the different technologies used to relay data.

4.1 Wireless sensor networks (WSN)

One of the most commonly used devices to obtain data whether it's indoors, outdoors or anywhere in the use of sensors by which brings various levels of security issues and therefore attacks, these are displayed in figure 2.

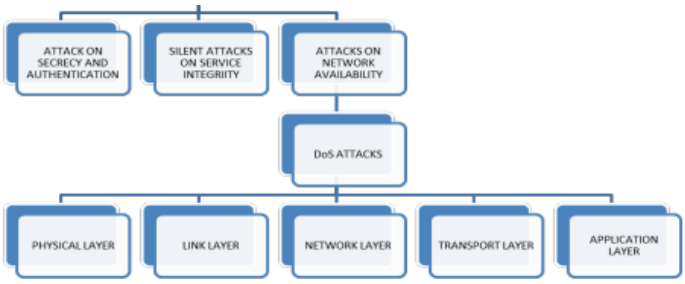

Figure 2- hierarchical diagram of security in WSN, (Sanyal et al 2015)

There tend to be 3 different attacks in this particular network, these are as followed:

- Attacks on authentication
- Silent attacks on service integrity
- Attacks on the network as a whole

It is also important to know that any denial of service within this network falls under this section, as a security method is used to prevent access of data to genuine end-users through mysterious third parties. Which can occur through the different layers a network clenches?

Attacks within the physical layer

This is discussed by Sanyal, et al (2015) who declares each layer and the physical layer is known for the 'selection and generation of the carrier frequency, modulation, and demodulation, encryption, and decryption, transmission, and reception of data'. Many security attacks can occur through this layer, regarded as jamming and node tampering. The jamming attack is simply the occupation of the communication through the nodes which blocks communication with each device. The node tampering is simply the tampering of the node which will results in the leaking of sensitive information, drawing on the privacy issues.

Arracks within the link layer

This layer is known to detect data and time frames, data streams and provides error control to ensure readability is upheld. The attacks within are Collision; this occurs whenever two nodes provide data within the same frequency and on the same channel, causing a collision as the identification can be unidentified at the receiving end. Battery exhaustion is the next attack that can potentially occur whenever there are multiple requests known as the traffic it can cause disruption and causes the battery to work harder and much faster to respond to the number of requests which are occurring over the network.

Attacks within the network layer

Within the wireless sensor networks, the routing function is considered the main purpose to which attacks are made. Spoofing attacks, hello flood is an attack where there a potentially dangerous level of traffic within the network; which results in numerous messages being outputted. These messages can a type of malware which the end-user responds to obliviously and the attacker is in. The wormhole is another attack which creates a relocation of the data from its previous original position within the system, the relocation is carried out through tunneling of data. The other attacks are selective following, homing, Sybil and acknowledgment flooding.

Attacks within the transport layer

This layer holds much power as it is known for the reliability of the transmission of data and helps to evade potential congestion of high trafficking, however, it has susceptible attacks known as flooding and de-synchronization. Flooding is the typical congestion of high levels of traffic through the networks whilst the other attack is invalid messages created by attackers known to request retransmission of data that is carried out.

Attacks on the application layer

This is one of the superior layers by which is responsible for the management of traffic, as discovered is the main security issue that can cause the previously mentioned attacks. Not only does it manage the traffic it is the provider of translation of data and whereby helps in query assembling.

4.2 Radio Frequency Identification (RFID)

Another very popular technology that is used for the exchange of information without any manual input, as it popularly used it is also prone to vicious attacks.

Unauthorized tag disabling

This is an attack on the authenticity, which changes an RFID tag to malfunction and further behave in a way it was not programmed for, this is carried out under the scan of a tag reader. It can be done remotely which allows an attacker to attack from a distance.

Unauthorized tag cloning

This is an attack on integrity, the identification data in which each tag has been manipulated by the tag by rogue readers, which then is replicated using false security measures.

Replay attacks

This is an attack on the vulnerability, where the attackers use a response made by the tag to impersonate it, in this case, the communication between the tag and reader is interrupted, recorded and replayed at any later time which fakes the availability.

Other security issues within this technology and other technologies used are;

- Tracking

- Spoofing
- Viruses
- Killing the tag approach
- Eavesdropping
- Power analysis
- Denial of service

All of the attacks discussed above bring on many of the privacy issues which are today meant to be considered to protect the information of individuals, which can be obtained through any physical or logical entity another word for an object, the exposure of such information can be carried out by any object which upholds a unique identifier. This unique identifier is used for communication over the internet, it allows IoT to carry out.

Privacy within IoT is important as it abides firstly, by all laws and regulations set out by the government and organizations to keep users safe, such as The Data Protection Act (2018). Another very important reason which individuals must consider privacy before designing and implementing an IoT device is to minimize the threat a system may portray, without privacy there is simply no trust. Likewise in day to day life, if there was no privacy with health records and the NHS the general public would not have any trust to explain their problems with a certain practitioner.

As this internet of things generates a vast amount of data they uphold a greater risk of data confidentiality, data integrity data authentication, flexibility, secure locational and robustness. Examples of data collected in an IoT such way can be through the use of website cookies, social networking sites such as Facebook before signing up requires individuals to accept to the terms and conditions which in small print allows them to sell your information to other companies for a large revenue, details such as liked pages and hobbies. However, in a Cisco Consumer Privacy Report, (2019) it was discovered that 45% of all respondents did not trust or allow companies of such to use the data they collected, however, unless agreeing to terms and conditions they do not have much choice.

5. Flaws of devices in the real world

To put these attacks into perspective, there have been real-world examples of security properties within these devices and objects have been exploited, increasing the concern of security and privacy within IoT devices.

The first case study was discussed in Verizon’s Data Breach Report in 2017, where an unidentified university had its network flooded with numerous requests of the DNS (domain name service) for a restaurant. The attack took place by a hacker outside the university’s organization and had no involvement with the university, to carry out the hack it used over 5,000 IoT devices which are found within, for example, a lighting system. The type of attack fitted under the category of ‘brute force attack’ whereby the use of weak passwords created by any member within the uni was used to deploy causing the network to crash.

As discussed earlier, CCTV and security systems through the use of cameras is a very important and successful IoT device in today’s society, capturing every second

and storing each second allows the end-user to potentially go back and watch the cameras from a particular time. However, a hacker can easily interpret this data if there are unknown network infrastructures. A camera company named NeoCoolCam faced problems with security when they realized that any network using their cameras could be hacked from outside of the system. The reason for this was established by Bitdefender, who studied this security and gained an understanding that attacks occurred through the easily accessible manipulation of the login screen which allows the hacker to gain access to the thousands upon thousands of cameras by NeoCoolCam which are in use. This is a main privacy and security issue as the hackers have access to data and footage of individuals which breaches the Data Protection Act and can cause trust issues between businesses and their customers/members.

Another very real example with IoT flaws is the lack of password management, control, and encryption, which The Mirai Botnet takes full benefit of. The Mirai Botnet is a piece of malicious programming that searches the internet for IoT devices that are vulnerable. By which the use of passwords and usernames are still set as their default making it easier to obtain the network and take control of devices within the network, Mirai has a list of default credentials giving them easy unauthorized access.

A very scary scenario where security flaws have been highlighted was the hacking of a Jeep Cherokee 4 x 4, where IoT security researchers name Charlie Miller and Chris Valasek under safe circumstances could hack the jeep through their entertainment system. It occurred through their experiment where they discovered they could change the temperature, song and other more serious features such as steering and braking system without even being in the car. This is extremely dangerous and caused the need for more research to be done within this field.

6. Prevention measures for future attacks

There has been a mass amount of research carried out in the field of the Internet of Things, with loopholes as such proven to be very detrimental, with precautions put in place during development will result in a more trustworthy IoT environment. To ensure future exploitation of security with IoT devices does not continue or are limited to protect privacy the government has set a Code of Practice out for all parties involved in the development and manufacturing of objects. The aim of the guideline is ‘to ensure that products are secure by design and to make it easier for people to stay secure in a digital world’. It sets out what they believe is 13 ways to promote good practice in IoT security, these 13 guidelines have been established by major corporations who worked in line with the government to ensure thorough first-hand research was carried out. These corporations fall under the names of the Department for Digital Culture, Media and Sport (DCMS) who work in conjunction with the National Cyber Security Centre.

Adoption of sound security measures is put in place, as are cryptographic and stenographic measures during the exchange process and the use of more efficient and secure methods of communication will ensure that the IoT infrastructure is robust and secure. As would the use of IoT security analytics, there is a need for this as it can reduce the vulnerabilities the IoT security has. The analytics takes into

consideration the correlating and analyzing of data which can help prevent potential threats.

The use of public key infrastructure will effectively encrypt data and information collected, doing so both asymmetrically and symmetrically. The Public Key Infrastructure is another set of policies by which software or hardware used during the implementation and designing of IoT devices is required to be followed for digital certificates. These certificates as such are used in the verifying of devices that are connected and used as a communication, it keeps the privacy element upheld a type of PKI is the cryptographic key which the hacker would not comprehend if there were potential attacks.

There should be the security of the actual network, as devices connect to the internet or IoT network should be secured effectively to prevent any future attacks. To do so successfully there is a need for employing endpoint security features, these include anti-malware, antivirus, firewalls which all can protect devices effectively. As can ensuring authentication is legitimate, this can be carried out using digital certificates, two-factor authentication, and even biometrics. Doing these security measures will ensure IoT devices are secured against exploitation.

7. The future of IoT

As technology evolves, so will the Internet of Things, as the growth is rapid individuals so depend on the internet and the devices which use the internet to communicate, so the future of the internet of things can be predicted to move quicker than ever before.

It has been predicted by the International Data Corporation that by the year 2025 internet of things will have developed so rapidly the components such as sensors are expected to generate 79.4 zettabytes of data. From this year until 2025 the growth rate is set to be 28.7% and anticipated to be over 78 billion devices connected in the IoT world.

With the growth of IoT, it has also been hypothesized that it will grow artificial intelligence which essentially aids computers to learn without the programming process. These computers have been adapted to focus on data received from a device and further use this data to understand the meaning for example if it was a consumer's preference. The use of AI ensures that human input is put to a minimum and therefore so is human effort. Mehavarunan, (2019) highlights that 'An I is considered the key propellant to the growth of the IoT revolution'.

5G is very much in the close future with some companies already using the technology and has been discussed that IoT applications from 2020 to 2030 will move from 4g to 5g technology whereby up to a million devices can be handled in 5g technology within one cell.

And to ensure that the security is upheld, even when devices become smarter so should security to limit cybercrimes. Within homes communication of IoT devices is done through the use of the router, therefore more advanced firewalls, encryption,

and configuration will be developed to ensure that users are protected from each entry point.

8. Conclusion

In conclusion, just like many scholars mentioned throughout the use of IoT in today's world has much success, to help ease life at home and work for all individuals, however, without awareness IoT has raised many security issues. An ongoing topic with many different intellectuals as it was mentioned a lot more research is needed in this field. As the infrastructure has required further development needed to ensure the protection of all end-users is upheld and attackers do not find new entrances. Furthermore, the technologies used to implement the internet of things must have extreme security measures set in place to ensure maximum security.

9. References

Anon, (2017). [online] Available at: https://www.bitdefender.com/box/blog/smart-home/neo-coolcams-not-cool-buffer-overflow/ [Accessed 18 Feb. 2020].

Banafa, A., 2016. IoT standardization and implementation challenges. IEEE Internet of Things Newsletter, pp.1-10.

Borgohain, T., Kumar, U. and Sanyal, S., 2015. Survey of security and privacy issues of the internet of things. arXiv preprint arXiv:1501.02211.

Byun, J., Kim, S., Sa, J., Kim, S., Shin, Y.T. and Kim, J.B., 2016. Smart city implementation models based on IoT technology. Advanced Science and Technology Letters, 129(41), pp.209-212.

Consumer Privacy Survey The growing imperative of getting data privacy right. (2019). [ebook] Available at: https://www.cisco.com/c/dam/en/us/products/collateral/security/cybersecurity-series-2019-cps.pdf [Accessed 18 Feb. 2020].

Foote, K. (2016). A Brief History of the Internet of Things - DATAVERSITY. [online] DATAVERSITY. Available at: https://www.dataversity.net/brief-history-internet-things/# [Accessed 18 Feb. 2020].

Journal, T. (2013). Gartner Says the Internet of Things Installed Base Will Grow to 26 Billion Units By 2020. [online] Quotidien Finance Digitale, open finance, blockchain. Available at: https://www.finyear.com/Gartner-Says-the-Internet-of-Things-Installed-Base-Will-Grow-to-26-Billion-Units-By-2020_a27901.html [Accessed 12 Feb. 2020].

Max Roser, Hannah Ritchie and Esteban Ortiz-Ospina (2020) - "Internet". Published online at OurWorldInData.org. Retrieved from: 'https://ourworldindata.org/internet' [Online Resource]

Mehavarunan (2019). The Future of IoT: 4 Predictions about the Internet of Things. [online] Thriveglobal.com. Available at: https://thriveglobal.com/stories/the-future-of-iot-4-predictions-about-the-internet-of-things/ [Accessed 18 Feb. 2020].

Slevin, J., 2007. Internet. The Blackwell encyclopedia of sociology.

Xia, F., Yang, L.T., Wang, L. and Vinel, A., 2012. Internet of things. International journal of communication systems, 25(9), p.1101.