Internet of Things: Survey, Observations & Future Trends

Campbell Rehu
Manukau Institute of Technology
rehu26@manukaumail.com

Firas Al-Ali
Manukau Institute of Technology
firas.al-ali@manukau.ac.nz

ABSTRACT

Internet of Things (IoT) has recveived a surge of interest and innovation in recent years as a result of the rapid evolution of wireless communication, cloud computing, sensor technologies, networking and big data analytics. However, unique challenges must first be addressed in order to assure both businesses and consumers of the safety and viability of adopting this new technology. These challenges include; the lack of standards across the IoT ecosystem, the societal impact of IoT, striking a balance between constant monitoring to provide helpful insight and invasion of privacy, and the management of devices that are heterogeneous in type and location. These challenges are inter-related and, therefore, a full architectural system re-design would be required in order to create a future-proof solution. In this literature survey paper, different IoT implementations, architectures, infrastructures, devices, protocols, platforms, frameworks, languages, and challenges, are discussed. This paper concludes with a recommendation for future work.

Keywords: Internet of Things, IoT, Smart Devices, Sensors, Cloud Computing, Big Data Analytics, ADAS, Advanced Driver-Assisted System, Technology Convergence, Field Programmable Gate Array, FPGA, Arduino, Raspberry

1. INTRODUCTION: WHAT IS INTERNET OF THINGS?

Internet of Things (IoT), according to Sarangi & Sethi (2017), is not just a single technology; "rather, it is an agglomeration of various technologies that work together in tandem" (p. 1). IoT is any device embedded with electronics, sensors, software and network connectivity. This enables the devices to collect data about their surroundings. From this data, meaningful information is discerned and presented to the user allowing them to make more informed decisions. IoT is a global trend that is the product of both the advancements in technologies (such as wireless communication, networking, cloud computing, and big data analytics) and their inevitable "technology convergence".

1.1 Current State of IoT

IoT is still in a nascent stage. A key force behind early IoT applications was the "competitive rush to market" (Lindqvist & Neumann, 2017, p. 28). This brought to light issues that organisations hadn't fully considered beforehand such as security and privacy, device resource constraints, interoperability and implications of malfunctioning devices. Although there has been a consistent influx in certain industries such as home automation and in personal devices (Skerrett, 2017, para. 4), other industries have lagged behind. In some cases, such as in industrial automation, the cause of this could be due to long development cycles, organisational reluctance to adopt the new technologies or the lack of employees who are able to develop, deploy and maintain IoT solutions (Patel et al., 2017, para. 4). Vansen Bourne (2017) also identified security concerns, budget constraints, increased initial cost and unclear business benefits as factors that are stopping organisations from implementing more IoT solutions (p. 7).

This quality assured paper appeared at the 8th annual conference of Computing and Information Technology Research and Education New Zealand (CITRENZ2017) and the 30h Annual Conference of the National Advisory Committee on Computing Qualifications, Napier, New Zealand, October, 2-4, 2017. Executive Editor: Emre Erturk. Associate Editors: Kathryn MacCallum and David Skelton.

1.2 Where IoT Is Headed

As IoT matures and IoT standards bodies (such as the *IPSO Alliance*, *Allseen Alliance* and *Open Connectivity Foundation)* work to create a more cohesive and standardised IoT ecosystem, IoT adoption will continue to increase. Many technology forecasters predict the IoT market to grow significantly over the next five years with *Cisco* predicting it to reach almost $15 trillion by 2022 (Columbus, 2015, para. 3). This growth will spawn a number of side effects. These include; market saturation whereby consumers may only be able to purchase IoT-enabled devices as non-IoT devices are now being made redundant (Lindqvist & Neumann, 2017, p. 30), changes to the infrastructure in order to support the extra devices being connected to the Internet (Patel et al., 2017, p. 7), and also the development and adoption of low-power WAN (Wide Area Network) protocols.

2. IOT IMPLEMENTATIONS

In this section, we provide a brief overview of both the current IoT implementations and the potential future implementations. One particular industry; namely home automation has seen the largest increase in IoT development and innovation in recent years. However, many other industries are realising the potential for IoT applications and are bringing products to market. These include the industrial/manufacturing, automotive, healthcare and connected city industries. There is also an increase in the number of IoT platform or middleware solutions, which aim to provide end-to-end services for hardware makers to implement their solutions on. IoT platforms will be discussed in Section 5.2 in more detail.

2.1 Current IoT Implementations

IoT is being implemented currently in a number of devices such as smart wearables, smart thermostats, connected vehicles, home and bike locks, brain-sensing headbands, medical monitoring and smart fabrics. These devices, generally, are controlled via smartphone applications.

2.2 Potential Future IoT Implementations

In the future, IoT has the capability of being used in every area of society. Autonomous cars are already gaining significant momentum and the technology is set to have a huge impact on society in the future. Traffic and street lighting, parking management, water management, energy management, building and maintenance services, healthcare services and traffic management will all come together in order to create smarter and more efficient cities. IoT applications spanning large areas of land are currently on the horizon with a number of trials being conducted around the world. In such applications, the communication distance is so vast that new technologies must be explored in order to make it possible.

3. IOT ARCHITECTURE & INFRASTRUCTURE

In this section, we will discuss the design and layout of architectures that currently exist in the IoT world. We will also consider alternative architectures

3.1 Current Design & Layout

The design of IoT architecture uses parts similar to the existing Internet infrastructure but with the addition of layers that are relevant to IoT. As such, two architecture design models are currently in use. These are the *Three-layer* and *Five-layer* architectures.

3.1.1 IoT Three-Layer Architecture

The *Three-Layer Architecture* (as shown in Figure 1) features *Perception*, *Network* and *Application* layers.

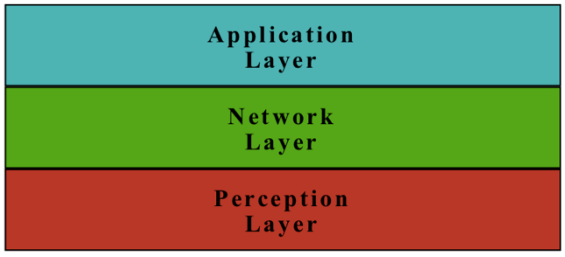

Figure 1: IoT Three-Layer Architecture

The *Perception* Layer contains the physical sensors and sensing devices and is responsible for "sensing and gathering information about the environment" (Sarangi & Sethi, 2017, p. 2). The *Network* Layer is responsible for the transportation and analysis of the data, which is received from the *Perception* Layer. Finally, the *Application* Layer is where the processed information from the *Network* Layer is presented as either meaningful information and/or as recommended action to the end-user. The *Three-Layer* Architecture is sufficient enough to capture the different functions in the IoT ecosystem. However, Sarangi & Sethi, (2017, p. 2) suggest that the this model can be refined further resulting in a *Five-Layer* architecture.

3.1.2 IoT Five-Layer Architecture

As shown in Figure 2, the Networking Layer has been split into two new layers: the *Transport* Layer and the *Processing* Layer. These two layers separate the functions of transporting the data from the *Perception* Layer and processing it.

The *Processing* Layer is also commonly referred to as the *Middleware* Layer. There is also the addition of a *Business* Layer which "manages the whole IoT system, including applications, business and profit models, and users' privacy" (Sarangi & Sethi, 2017, p. 3).

These two architectural models are reiterated by Bhuvaneswari (2017, p. 136), Manohar & Perumal (2017, 283), Mulligan (2017, p. 188) and Asim (2017, p. 996) who emphasise that IoT is working atop the existing Internet stack. They suggest that

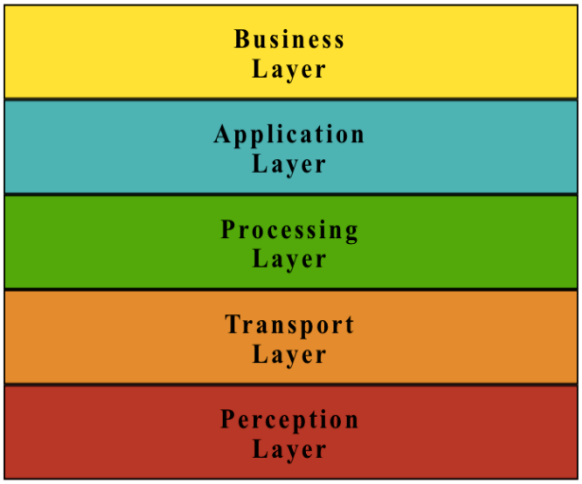

Figure 2: IoT Five-Layer Architecture

this is not optimal because IoT-specific issues (such as the inherent physical and resource constraints) must be considered. In Section 3.2, we will consider some alternative architectural patterns that may be more suited to IoT applications.

3.2 Alternative Design & Layout

A number of alternative architectural patterns have been emerging. These patterns use different techniques to enable IoT to work in a secure and resource-considered fashion. Examples of these patterns used are; Edge Computing, Social IoT and Field-Programmable Gate Arrays (FPGAs). These are explained below.

3.2.1 Edge Computing

Edge Computing refers to an architecture pattern whereby a part of the processing is conducted at the sensor level. This can aid in minimising the amount of data needing to be sent to the cloud via the network and, as a result, can lead to better security and privacy. As suggested by Satyanarayanan (2017), edge computing applications "could help address growing concerns over data privacy arising from IoT over-centralisation [where] a user should be able to delete or denature a subset of sensor data he or she deems sensitive" (p. 35-36). This would mean that devices could process and/or sanitise the raw data to include only the necessary information to be sent to the cloud, and remove any sensitive data as the user requires.

Edge computing also has the benefit of providing low latency service to applications that need fast response times. This is particularly important for autonomous cars and smart traffic lights in cities, which require a tight feedback loop between data input and output.

An additional benefit of the low latency and "closeness" of the processing capability to the edge device is that cloud outages can be masked. "As our dependence on the cloud grows, so does our vulnerability to cloud outages. Implicit in the convergence of mobile and cloud computing is the assumption that the cloud is easily accessible at all times" (Satyanarayanan, 2017, p. 36). This seems to be a user experience issue that is similar to the motivation behind using client-side frameworks in modern websites that mask delays due to server request processing.

An example of an edge computing platform is *AWS Greengrass* from Amazon. This platform allows device manufacturers to use *AWS* (Amazon Web Services) to create functions (called *Lambdas*) that are able to run on edge devices independent of the *AWS* cloud platform. This is a significant move and other organisations such as *Microsoft*, *Google*, *HP and IBM* have similar products on the market.

3.2.2 Social IoT

The overarching theme of Social IoT is that the connection of devices is modelled on a human-to-human social network. In this paradigm, the devices themselves are responsible for creating connections with other devices as required. This 'social networking' of devices is predicated on a number of factors. These factors include the requirement of service from other devices, whether those devices are trustworthy (based on past and current performance) and the reputation of the devices (Dong & Lin, 2017, p. 1-2).

3.2.3 Field-Programmable Gate Arrays (FPGA)

FPGAs provide reconfigurable hardware design through the writing of special computer code. This decreases the time between deployments and the cost of updating systems. FPGAs provide a serious amount of processing power because of its true parallelism, which would enable large IoT applications to run off of a single FPGA chip.

These paradigms do not have to exist independently, rather they can and should be used in tandem to create a more effective and efficient IoT architecture structure.

3.3 Current Hardware Components

In this section, we identify a few key hardware options that exist on the market. It has become increasingly accessible to build IoT applications, not only for large organisations but also for smaller groups and even individuals.

3.3.1 Sensors

There is a multitude of sensors that can be used within IoT applications. These include accelerometers (used to sense motion and acceleration), gyroscopes (to detect device orientation), magnetometers, light sensors, Global Positioning System (GPS) sensors, proximity sensors, humidity sensors, barometers (used to measure atmospheric pressure) and thermometers (Sarangi & Sethi, 2017, p. 5-8). In many cases, these sensors are embedded within modern smartphones thus making smartphones one of the most widely used IoT devices.

3.3.2 Entry-Level Development Devices

There is also an increasing number of products emerging on the market that provide both processing and communication functionality. Consumer-aimed development boards such as the Arduino and Raspberry Pi provide easy-to-use entry-points for individuals to develop and test their own IoT applications.

3.3.2.1 Arduino

Arduino is an open-source hardware and software platform that features a board that is able to collect data transmitted through a number of onboard General-Purpose Input/Output (GPIO) pins, process it using an on-board microcontroller and turn it into desired output.

Figure 4: Arduino Uno (Oomlout, 2013)

Through its *Arduino Integrated Development Environment (IDE)*, users are able to write code in the programming language *Wiring* (a C-based language that allows for low-level language capabilities) and run it on the board.

There are many different configurations of *Arduino* boards which can be customised to provide additional functionality with the use of *shields* such as Ethernet, Wi-Fi and USB Host shields. Also, since the hardware is open-sourced, there are a number of Arduino-based variants available which were made by third-parties such as the *SparkFun RedBoard.*

3.3.2.2 Raspberry Pi

Raspberry Pi is slightly different to the Arduino in that it is a pocket-sized computer that runs a flavour of the Linux operating system (the Arduino can only run the code that it is programmed to do by the user). The Raspberry Pi features a system-on-a-chip (SOC), built-in Wi-Fi, Bluetooth, an SD card slot for the operating system and program memory among many other features.

Figure 4: Raspberry Pi (Multicherry, 2015)

Most of the programs running on Raspberry Pi are written in Python. However, many languages have been ported to it including JavaScript, Java, C, C++, Erlang, and Scratch.

3.3.3 Other Development Devices

In April 2017, Intel released an IoT development board called the *Terasic DE10-Nano,* which features both a Hard Processor System (HPS) and a field-programmable gate array (FPGA) on the same chip. The inclusion of an FPGA in a relatively inexpensive development board is particularly exciting because of the FPGA capabilities described previously in Section 3.2.3.

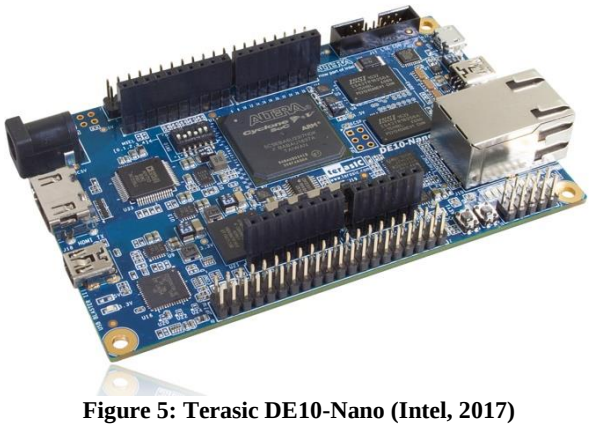

Figure 5: Terasic DE10-Nano (Intel, 2017)

Another device that was unveiled in 2017 was from semiconductor company, *Qorvo*, who introduced a System-on-Chip (SoC) called the *GP695 ZigBee/BLE Smart Home Communications Controller*. It incorporates compatibility with many of the communication protocols that are specifically aimed at IoT applications such as 802.15.4, Bluetooth Low

Energy and Thread. These protocols are discussed further in Section 4. The *GP695* is due to be released in Quarter 2 of 2017.

4. IOT PROTOCOLS

In this section we will discuss the protocols that are currently being used in the IoT ecosystem. There are many protocols to choose from and new protocols are introduced regularly. This occurs as various groups vie to create a single protocol in the hope that it will become the industry standard. As a result, the market is saturated with protocols that are not interoperable. All of these protocols use different optimisations to ensure that IoT devices with low power and processing capabilities are able to communicate completely and securely.

4.1 Transport

The Transport protocols are responsible for the "end to end control and retransmission" of data (Mulligan, 2017, p. 188). IoT devices use either *User Datagram Protocol (UDP)* or *Transmission Control Protocol (TCP)*.

TCP is one of the most common Transport protocols used on the Internet because it ensures data is sent to the correct destination, in the correct order. However, this requires additional power and processing overheads.

UDP, on the other hand, does not require the overheads that *TCP* does. This makes it more appealing for use in IoT devices where there are processing and power constraints. An interesting workaround for the issues of having a protocol like *UDP* is implementing the connection features in a different layer of the IoT architecture. For example, the *Constrained Application Protocol (CoAP)* is able to transmit confirmable messages that require confirmation of receipt and correct ordering.

4.2 Messaging

The Messaging protocols make up a part of the *Application Layer*. They define how the data is structured and the way in which the data is distributed in terms of single- or multi-device delivery (unicast vs. multicast). There are many IoT messaging protocols. The two most widely-used protocols are *Message Queuing Telemetry Transport (MQTT)* and *Constrained Application Protocol (CoAP)*.

The *MQTT* protocol allows devices to subscribe to other devices in order to receive any data that they transmit. The function of transmitting that data is outsourced to a *broker* device, which receives all incoming data and relays it onto all devices that are subscribed to that data source. *MQTT* is lightweight and has minimal overhead, which makes it particularly suited to IoT applications. However, it relies on an underlying *TCP* layer. This is not optimal for devices with low power and processing ability but there is an extension of *MQTT* called *MQTT/SN*, which features optimisations for constrained devices and is not concerned with the underlying network structure.

CoAP is a protocol based on *HyperText Transport Protocol (HTTP)* where it uses the same request names (GET, POST, PUT, DELETE) but has optimisations that *HTTP* doesn't. These optimisations include data compression, support for multicast messages, and confirmable messages. These all work to provide a secure and reliable messaging system specifically for constrained devices.

4.3 Addressing

The Addressing protocols are responsible for providing a reachable address for each IoT device. This is to ensure that data is sent to the correct devices. *Internet Protocol version 6 (IPv6)* was the second iteration of *IP* which increased the number of available addresses. However, the increased addressing space also increases the processing overhead. This means that certain IoT devices are unable to process IPv6 due to power and processing limitations. As a result, an optimised implementation of IPv6 for devices with limited processing and power capabilities was developed. This is called *IPv6 over Low Power Personal Area Networks* (*6LowPAN)*. It uses compression and fragmentation in order to provide the required information using less power and processing.

4.4 Routing

Routing protocols enable the best paths between origin and destination devices to be realised. The routing protocol used in most IoT applications is called *Routing over Low Power and Lossy Networks (RPL)*. *RPL* is used to determine the most optimal path for data to flow in order to "minimise latency or the expected number of packets that need to be sent" (Sarangi & Sethi, 2017, p. 12).

4.5 Data Transmission

There is a variety of ways for physically transmitting the information between devices. The predominant technologies used are *Radio Frequency IDentification (RFID), Bluetooth & Bluetooth Low-Energy (BLE), IEEE 802.11-based protocols (WiLAN), IEEE 802.15.4-based protocols and Low-Power Wide Area Network Protocols (LPWAN)*.

RFID is comprised of a tag chip with an antenna that is able to be read by an *RFID* reader. These devices use a low amount of power and passive *RFID* tags don't require any external power. This makes it useful for applications such as "supply chain management, access control, identity authentication and object tracking" (Sarangi & Sethi, 2017).

BLE is the "low power version of Bluetooth that was built for the Internet of Things" (Bluetooth SIG, 2017, para. 1). It features optimisations that allow resource constrained devices to communicate and remain online and available for extended periods of time. Additionally, the upcoming iteration of *Bluetooth version 5* features greater data throughput, increased transmission range and improved transmission speed. It also has the capability to form mesh networks, share multicast messages and communicate to devices that use other protocols such as *ZigBee* all because it is able to communicate using *IPv6*.

The majority of IoT devices use *802.11-based protocols* like *802.11a/b/g/n/ac* (commonly defined by the general *Wi-Fi Alliance* name of *Wi-Fi*). However, these protocols use a significant amount of power during transmission so, for devices that have power and processing constraints, a revision called *802.11ah* was defined in 2016. *802.11ah* uses less power because it utilises sub-1GHz frequency bands and lower transmission rates.

The *IEEE 802.15.4 protocols* define personal-area networks that use low power. The reach of these technologies is relatively small (between 10 and 100 metres) but it supports different types of network topologies including star and mesh patterns. *ZigBee* and *Thread* are two protocols that work on top of the *802.15.4 protocol*. They are both able to implement mesh network patterns. Mesh networks allow devices to act as routers, which means that physically-separate devices can still share data as long as they are connected through intermediary devices in the mesh network. This has applications in larger personal area networks and even, potentially, in large wide area networks since devices are not required to be within a specified range to communicate with each other.

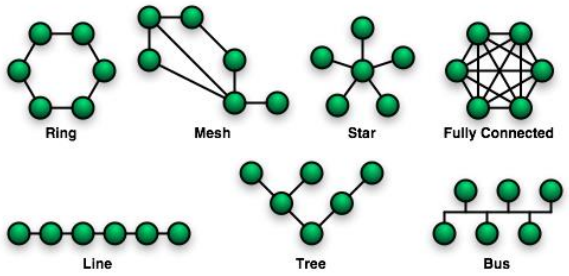

Figure 6: Various Network Topologies including Mesh & Star (Foobaz, 2006)

An upcoming release from the *ZigBee Alliance* is a communication protocol called *dotdot*. The protocol is *ZigBee*'s attempt to create a "universal language for IoT, making it possible for smart objects to work together on any network" (ZigBee Alliance, 2017, para. 1). Another universal communication protocol was introduced by Google in 2016 called *Weave* which allows device manufacturers to communicate directly with Google cloud services. *Weave* is capable of communicating over *Bluetooth*, *802.11-based protocols* and *802.15.4-based protocols*.

LPWAN protocols have a lower transmission rate because they use larger frequency bands. This allows data to be shared over thousands of kilometres using very low power and processing, thus making them ideal for long-range IoT devices. Examples of *LPWAN* protocols are *NarrowBand IoT (NB-IoT), LoRaWAN, SigFox, and Weightless*. These all share the features of using a small amount of power to transmit data over large distances securely. Recently, a large amount of interest in *LPWAN*s has been shown as applications in agriculture (crop and livestock condition monitoring), safety (citywide energy, water, pollution etc. monitoring systems) and productivity (supply chain tracking) are explored (Patel et al., 2017, para. 18).

5. IOT FRAMEWORKS & LANGUAGES

In this section, we outline the programming languages used in IoT. We also discuss the multi-layered frameworks that organisations (such as *Google*, *Microsoft* and *IBM*) provide to give developers use of various data services such as transmission, storage, security and analytics.

5.1 Programming Languages

IoT utilises existing programming languages that have a history of being useful and effective in controlling computers. A 2017 IoT developer survey conducted by Skerrett, (2017) revealed that "*Java* and *C* are the primary IoT programming languages, along with significant usage of *C++*, *Python* and *JavaScript*" (para. 7). The prevalence of the *C* and *C++* languages in IoT programming is not surprising given that they are low-level languages that are processor independent. *Java* is popular and has a large user-base. It also provides the latest security standards and a high level of encryption and authentication to ensure data security and privacy (Badami, 2017, para. 21). At a slightly higher level, Google released an IoT operating system called *Android Things* (codenamed *Brillo*) which is based on the Android operating system and runs on a variety of development boards and SoCs. The language used in *Android Things* development is *Java*. Finally, *JavaScript* and *Python* are both preferred languages of the web. As a result, well-managed web and networking libraries are available and make IoT communication and programming easier to implement with those languages.

5.2 IoT Platforms

The large amount of data that is collected by IoT devices must be properly processed, analysed and stored. However, many IoT hardware manufacturers don't have the infrastructure (servers, processors etc.) to do all of that processing. Large organisations (such as Microsoft, IBM, and Amazon) have recognised this need and provide their well-established services to hardware manufacturers. These services are encapsulated and named *IoT Platforms* and act as *Platforms-as-a-Service (PaaS)*. This enables device-makers to access the cloud and processing capabilities that such large organisations already have. Using these services significantly decreases cost and outsources one of the most difficult tasks in the IoT ecosystem. Examples of such IoT platforms are *Amazon AWS IoT*, *Microsoft Azure IoT Suite*, *IBM Watson IoT*, *Samsung ARTIK* and *ThingWorx*.

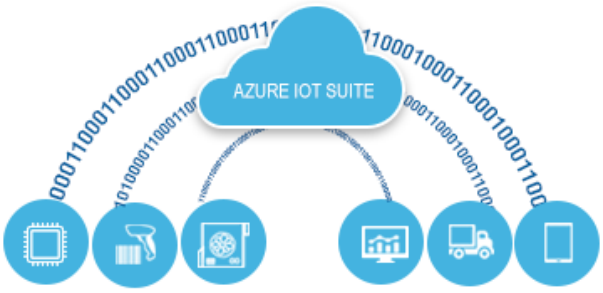

Figure 7: Microsoft Azure IoT Suite (Saviant Intelligent Solutions, 2016)

6. IOT IMPLEMENTATION IN NEW ZEALAND

In 2017, an IoT trial is being conducted called *Connecting Farms* which is an implementation of wide-area IoT in farms located in the Waikato region. The pilot uses a wide-area network of sensors that allow farmers to receive real-time information about what is going on in their farms. The sensors communicate using *NB-IoT* over SparkNZ's 4G network (MatthewC, 2017, para. 1). This trial is significant because it is the first major use of *LPWAN*s in New Zealand. Furthermore, farming is one of New Zealand's biggest export trades, hence successful applications could have widespread effect on the New Zealand economy.

7. IOT CHALLENGES

There are many challenges that must be addressed before IoT can live up to its future potential. Solving these challenges is of crucial importance considering the real-world reach and implications that IoT has outside of the traditional computing ecosystem.

7.1 Security

Security is one of the biggest concerns surrounding IoT. Businesses and consumers alike are cautious of adopting IoT because of the unknown security and privacy implications—as is often the case with unexplored terrain. These concerns are not groundless since cyberattacks have increased significantly since 2015 (PWC, 2017, "Connecting the Dots"). Only a few of these cyberattacks were conducted using IoT devices because they are not as pervasive as traditional computers. However, as more and more IoT devices are connected to the Internet, they will become more viable targets for hackers to exploit. One such example of a large scale attack that was caused by IoT device exploitation was the *distributed denial-of-service (DDOS)* attack on the domain name system company, *Dyn*. The attack involved a large number of outdated Internet-connected devices (such as security cameras, appliances and routers) being hacked and used to form a botnet which flooded the *Dyn* servers. This caused websites such as *Netflix*, *Amazon* and *Twitter* to become unavailable. It was later revealed that poor security (such as default administration credentials that were

left unchanged) made it possible for hackers to exploit the devices. This attack highlights the potential consumer disruption that can be caused by insufficient security measures. Extrapolating those findings to IoT reveals the implications of such an attack occurring in modern-day connected devices such as cars, medical equipment, and cities.

Figure 8: Dyn Domain Name System (Schuetz, 2016)

Causes for the lack of security stem from the "competitive rush to market with very few concerns for trustworthiness" (Lindqvist & Neumann, 2017, p. 28), and the fact that there is no "basic level defined for security and privacy of connected and smart devices" (Infineon Technologies et al., 2016, p. 1). Infineon Technologies et al., (2016) state that the solution to these security concerns is to develop a "policy framework for ensuring minimal security requirements for connected devices" and a "framework for interoperability testing" (p. 2-3). They also suggest that insurance companies could provide incentives for "implementation of security solutions", and governing bodies could enforce penalties for "vendors of security products and services that abuse established practices on certification and/or deliver counterfeit products" (p. 4). Schneier, (2016) affirms this stance saying that "government could impose minimum security standards on IoT manufacturers" and "liabilities on manufacturers" (para. 7).

Though IoT is an exciting platform for innovation, businesses and product manufacturers must be able to see the business value in implementing IoT solutions. In such situations, security and testing are not at the top of the list for product requirements. Schneier, (2016) states that, the software market demands that "products be fast and cheap and that security be a secondary consideration" (para. 12). Unfortunately, this deprioritizing of security has been transferred into the IoT industry. This is because "the market won't stand for the additional costs that security would require" (Schneier, 2016, para. 4) and "trusted solutions are more costly for suppliers". Furthermore, "buyers are reluctant to pay a premium for security and privacy" (Infineon Technologies et al., 2016, p. 1). This challenge is summarized by Wright, (2017), who states that "it's a technical problem, but it's closely tied to business interests. These days, the way companies tend to look at security is as a loss leader" (p. 17).

The security in these devices should be inherent and not compromise the reliability and availability of the service. Consumers are not likely to demand more secure systems. Furthermore, they may find frequent requests for security updates cumbersome. A secure IoT system that is unobtrusive to the user should be a priority within the industry (Lindqvist & Neumann, 2017, p. 29).

Device disposal presents a further security issue. Mulligan (2017) states that "no one thinks twice about throwing out a burned-out light bulb – what else would you do with it? But what if it is a 'smart bulb' that is connected to a home network? It therefore contains security information, perhaps encryption keys, that allows that bulb to talk to other devices on the network" (p. 195). This idea is similar to the concern surrounding disposal of computer hard drives—they must be completely wiped to ensure that the data is not recoverable by any third-parties. The disposal of IoT connected devices must be in a secure manner.

Until the IoT security issues are resolved, cyber attackers will continue to leverage the availability and connectivity of IoT devices for malicious purposes. As it stands, businesses have no incentive to fund more secure solutions and consumers will not think twice before purchasing a 'shiny and new' IoT device that brings them closer to a smarter and more connected future. This combination of nonchalance from both the producer and the consumer will perpetuate the current state of IoT security into the future. This sentiment is captured by Schneier, (2016) who says that "your security on the Internet depends on the security of millions of Internet-enabled devices, designed and sold by companies you've never heard of to consumers who don't care about your security" (para. 3).

7.2 IoT Device Management

Creating secure IoT solutions isn't limited to the network and software. Physical security of IoT devices and sensors is also an important consideration because the devices could be deployed in remote or inaccessible locations. Therefore, "the development of tamper-resistant and tamper-evident enclosures, remote surveillance, and Trusted Platform Module-based attestation are all important paths" (Satyanarayanan, 2017, p. 37).

Additionally, certain IoT devices may not require regular, in-person human interaction to operate properly which creates challenges around how humans will interact with the devices. Possible solutions include using secondary devices (smartphones or tablets) or using voice interaction (Lindqvist & Neumann, 2017, p. 28). Using secondary devices would be limiting because the consumer would need to already own a secondary device and rely on it for interaction with a separate device. This may, however, be mitigated by the decreasing cost of such devices. Using voice interaction, though convenient and accessible, may raise additional problems such as "linguistic ambiguities, and obvious privacy risks associated with ubiquitous devices that continuously record and process voice conversations, as well as interesting opportunities for replay or synthesised voice-command attacks" (Lindqvist & Neumann, 2017, p. 28).

There is also the issue of design of the devices and their method of management for the consumer. The design of user interfaces will need to be "seamlessly easy to use, intuitively self-evident, and friendly for those who are technologically impaired, as well as adequately configurable by everyone" (Lindqvist & Neumann, 2017, p. 29).

Managing IoT devices (especially those in remote locations) is not just about network management but rather the physical management and user experience considerations that must be made.

7.3 Resource-Constrained Devices

IoT devices that are remote in location may also face the problem of needing to work on low power for extended periods. Data communication can use a significant amount of power and if devices are equipped with additional functionality such as pre-processing storage or encryption, battery life will diminish quickly. *LPWAN* protocols such as *NB-IoT* aid in preserving battery life but more research and development must be undertaken to investigate alternate power source technologies. A potential power solution would be to use energy harvesting technologies and "although solar energy could provide an answer for many IoT applications, semiconductor companies should also investigate other sources such as wind, thermal energy, and kinetic energy" (Patel et al., 2017, para. 19).

7.4 Standards & Interoperability

Standards are the universally understood definitions of best practices which provide a way of levelling the field and allow for open interoperability between different vendors. However, there is a current lack of codification "as many companies have aligned with groups that have competing agendas and goals" (Dorsch, 2016, para. 2). This is illustrated by the many competing connection protocols that create an "acronym soup" (Govindachari & Sutaria, 2013, p. 1) of confusion.

Should universal standards not be adopted, a possible solution would be to use gateways and/or middleware to "act as a bridge between the things and the applications." (Sarangi & Sethi, 2017, p. 15). Using a gateway would, however, force consumers to purchase separate devices to allow their other devices to communicate with each other. This would propagate the problems associated with having another device to manage (software and firmware updates and user experience design) and would create a "single point of failure and a single point of attack" (Mulligan, 2017, p. 192). Middleware could be a beneficial solution, however, the level of abstraction required to produce such a generic middleware that captures the functionality of a large number of IoT devices could be problematic and create issues around coherence and readability.

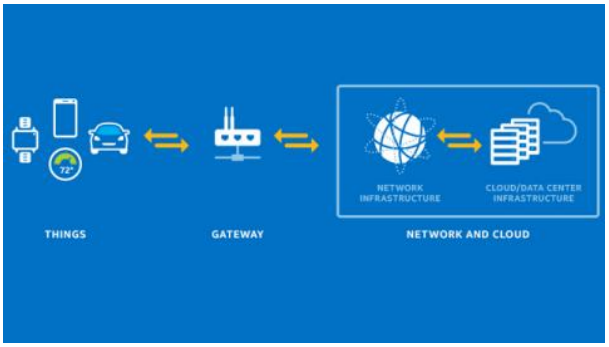

Figure 9: How IoT Gateways Work (Intel, 2016)

7.5 Societal & Ethical Implications

There are serious societal and ethical challenges around IoT that must be considered. IoT's real potential lies in its ability to be ubiquitous, pervasive and invisible. This requires communication between countless devices and creates a substantial amount of data about individuals and their activities. As a result, ethical challenges are presented. Consider; who is responsible for the devices if they malfunction and cause damage or harm, who will own the devices and the data that is collected, and what will the effect be on our personal privacy?

As discussed in Section 7.1, responsibility for device malfunction could be placed on manufacturers, if caused by poor security. However, what if the user was too complacent to update the device to a software version that fixed the security flaw? Should the user be held accountable? Alternatively, should the software developer be held responsible as their code was where the bug occurred that compromised the entire system? These situations are where standards could remove some ambiguity.

Lindqvist & Neumann, (2017) suggest that government regulation and testing is required for "electronic products that have the potential to hurt or kill people" in order to protect consumers (p. 29). This is reiterated by Schneier, (2016) who says that we need "increased regulation of what are now critical and life-threatening technologies" (para. 1). Schneier goes on to say, rather bleakly, that "a fatal IoT disaster will spur our government into action, and it's unlikely to be well-considered and thoughtful action" (para. 11). He is referring to the rushed and unconsidered creation of the Department of Homeland Security in reaction to the September 11 terrorist attacks.

The data that is collected by IoT devices is high in volume, velocity and variety. But who owns it? One would assume that the data would be owned by the person or people that it pertains to, but this may not be the case. Knight, (2017) states that "the entity that owns the IoT device also owns the data produced by that device" (para. 3). He suggests that "data title rights are similar to the rights afforded by a copyright [where] an entity that holds the title to data [also] holds the associated data ownership rights: [however] if the data set is copied and transmitted elsewhere, the author relinquishes the usage rights" (para. 7-10). There is no blanket approach to how this data is handled. For example, within agriculture, farmers "own the data produced by his or her sensors platforms"; and with regard to connected cars data that is "captured after a purchase is owned by the entity who bought the car" (Knight, 2017, para. 15, 18). Data ownership becomes more complicated when device leasing or subscription-based business models are used. An example of this would be a household that leases its smart meter from a power company (this scenario is complicated further if the power company leased the hardware and/or software from a third-party). Who owns the data in such situations is unclear. As time goes by, consumers may realise that they don't need to "own" devices. For example, owning a car may be viewed as a source of depreciating value because of the amount of time that a car is idle. This would lead the consumer to seek out subscription-based car services where they use the car as required and pay substantially less than if they bought the car outright.

In order to be effective, IoT devices need to be constantly collecting data affecting the privacy of individuals. Will society, collectively, need to sign a contract to agree to constant monitoring of activity when in smart cities? Will the benefits for individuals and businesses outweigh the loss of personal privacy? The answer to these questions is not clear and until larger scale implementations of smart cities, smart grids and connected homes are tested, we will not know the answer for sure. An example of the need for balance between individual privacy and business benefit comes from Patel et al., (2017). They recommend that IoT manufacturers apply "sophisticated algorithms to videos [and] audio captured" of individuals to analyse their consumer behavior (para. 15). This would provide a great amount of insight for businesses but the negative effect on consumer privacy is clear. Although, use of technologies such as *Lidar*, can provide abstract representations of people and objects in order to protect privacy, and could mitigate the tension between "individual privacy and the use of personal information to promote effectiveness, safety and security" (Berman & Cerf, 2017, p. 6).

7.6 IoT Architecture Redesign

The challenges discussed above are not isolated. Rather they are related, which, to resolve them, may require a complete system overhaul. With security and privacy as the starting point, we could rebuild the ecosystem from the ground up using the alternative architecture paradigms described in Section 3.2 such as edge computing, to decrease the amount of data being shared to the cloud and heighten security; paired with the flexibility of FPGA chips, to tighten the development lifecycle; and energy harvesting, to maximise battery life. Then we employ the use of the appropriate protocols as described in Section 4 such as the *LPWAN*s for devices that require infrequent data transmission or are in remote locations, or *BLE* or *ZigBee* for creating mesh networks of sensors that use little power. Finally, utilising an IoT *platform-as-a-service* such as Microsoft Azure IoT Suite for the data analytics, storage and

security services would complete a solution that has end-to-end security and privacy as the driving factors.

8. WHERE TO FROM HERE?

As IoT becomes more widespread, it should feature more in schools and higher education. This would bind the ease of programming to the real-world possibilities and would bring awareness to the implications of unconsidered coding practices. Edge computing could solve many issues in IoT because of the smaller data transmission footprint to the cloud and subsequent increase security. This would, however, require development of better device energy management, battery technologies and energy harvesting. As more industries adopt IoT technologies, the importance of awareness of the challenges and issues is critical to ensure that they are resolved first and not perpetuated into the future.

9. REFERENCES

Asim, M. (2017). A Survey on Application Layer Protocols for Internet of Things (IoT). *International Journal of Advanced Research in Computer Science*, *8*(3), 996–1000.

Badami, V. (2017, January 22). Top programming languages used in IoT. Retrieved June 7, 2017, from http://blog.hackerearth.com/programming-languages-in-iot

Berman, F., & Cerf, V. (2017). Social and Ethical Behavior in the Internet of Things. *Communications of the ACM*, *60*(2), 6–7.

Bhuvaneswari, A. (2017). A Survey on Internet of Things [IoT]. *International Journal of Advanced Research in Computer Science*, *8*(1), 134–140.

Bluetooth SIG. (2017). Bluetooth Low Energy. Retrieved June 19, 2017, from https://www.bluetooth.com/what-is-bluetooth-technology/how-it-works/le-p2p

Columbus, L. (2015, December 27). Roundup Of Internet of Things Forecasts and Market Estimates, 2015. Retrieved May 20, 2017, from https://www.forbes.com/sites/louiscolumbus/2015/12/27/roundup-of-internet-of-things-forecasts-and-market-estimates-2015/#7a1bd32e4b93

Dong, L., & Lin, Z. (2017). Clarifying Trust in Social Internet of Things. *IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING*. Retrieved from https://arxiv.org/pdf/1704.03554v1.pdf

Dorsch, J. (2016, October 10). Where Are The IoT Industry Standards? Retrieved May 27, 2017, from http://semiengineering.com/where-are-the-iot-industry-standards/

Foobaz. (2006). *NetworkTopologies*. Retrieved from https://commons.wikimedia.org/wiki/File:NetworkTopologies.png

Govindachari, R., & Sutaria, R. (2013). Making sense of interoperability: Protocols and Standardization initiatives in IOT. Presented at the 2nd International Workshop on Computing and Networking for Internet of Things (CoMNet-IoT) held in conjunction with 14th International Conference on Distributed Computing and Networking (ICDCN 2013). Retrieved from https://pdfs.semanticscholar.org/cc70/63734f97701e853a4fb8830f64f16f11df92.pdf

Hu, F. (Ed.). (2016). *Security & Privacy in IoT*. CRC Press.

Infineon Technologies, NXP Semiconductors, STMicroelectronics, & ENISA. (2016). *Common Position on Cybersecurity* (p. 5). Retrieved from https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/infineon-nxp-st-enisa-position-on-cybersecurity

Intel. (2016). *Transform Business with Intelligent Gateway Solutions for IoT*. Retrieved from https://www.intel.com/content/www/us/en/internet-of-things/gateway-solutions.html

Intel. (2017). *Terasic DE10-Nano Get Started Guide*. Retrieved from https://software.intel.com/en-us/terasic-de10-nano-get-started-guide

Knight, D. (2017, January 30). Who owns the data from the IoT? Retrieved June 24, 2017, from http://www.computerworld.com/article/3152837/internet-of-things/who-owns-the-data-from-the-iot.html

Lindqvist, U., & Neumann, P. G. (2017). Inside Risks: The Future of the Internet of Things. *Communications of the ACM*, *60*(2), 26–30.

Manohar, M., & Perumal, K. (2017). A Survey on Internet of Things: Case Studies, Applications and Future Directions. In M. Geetha & D. Acharjya (Eds.), *Internet of Things: Novel Advances and Envisioned Applications* (pp. 281–297). Springer International Publishing AG.

MatthewC. (2017, June 8). Demonstrating the Internet of Things (IoT) to Connecting Farms. Retrieved June 14, 2017, from http://nztechblog.net/2017/06/08/news-demonstrating-internet-things-iot-connecting-farms/

Mulligan, G. (2017). IPv6 For IoT and Gateway. In H. Geng (Ed.), *Internet of Things and Data Analytics Handbook* (First, pp. 187–196). John Wiley & Sons, Inc.

Multicherry. (2015). *Raspberry Pi 2 Model B v1.1 front angle new*. Retrieved from https://commons.wikimedia.org/wiki/File:Raspberry_Pi_2_Model_B_v1.1_front_angle_new.jpg

Oomlout. (2013). *Arduino_Uno_005*. Retrieved from https://commons.wikimedia.org/wiki/File:Arduino_Uno_005.jpg

Patel, M., Shangkuan, J., & Thomas, C. (2017, May). What's new with the Internet of Things? Retrieved May 28, 2017, from http://www.mckinsey.com/industries/semiconductors/our-insights/whats-new-with-the-internet-of-things

PWC. (2017). The Global State of Information Security Survey 2017. Retrieved June 23, 2017, from http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey.html

Sarangi, S., & Sethi, P. (2017). Internet of Things: Architectures, Protocols and Applications. *Journal of Electrical and Computer Engineering*, *2017*, 1–25.

Satyanarayanan, M. (2017). The Emergence of Edge Computing. *Computer*, *50*(1), 30–39.

Saviant Intelligent Solutions. (2016). *Microsoft Azure IoT Services*. Retrieved from http://www.saviantconsulting.com/azure-iot-suite.aspx

Schneier, B. (2016, November). Your WiFi-connected thermostat can take down the whole Internet. We need new regulations. Retrieved June 7, 2017, from https://www.washingtonpost.com/posteverything/wp/2016/11/03/your-wifi-connected-thermostat-can-take-down-the-whole-internet-we-need-new-regulations/?utm_term=.8ef0c1789631

Schuetz, M. (2016, October 21). Hacking vendetta seen in attack on Manchester's Dyn Inc. Retrieved June 24, 2017, from http://www.concordmonitor.com/Hackers-attack-Dyn-in-Manchester-5537170

Skerrett, I. (2017, April 19). IoT Developer Trends 2017 Edition. Retrieved May 19, 2017, from https://ianskerrett.wordpress.com/2017/04/19/iot-developer-trends-2017-edition/

Vansen Bourne. (2017). *IoT STRATEGY : INSIGHTS FROM EARLY IoT ADOPTERS*. HCL Technologies. Retrieved from https://www.hcltech.com/iot-survey

Wright, A. (2017). Mapping the Internet of Things. *Communications of the ACM*, *60*(1), 16–18.

ZigBee Alliance. (2017, January 3). The zigbee alliance to Unveil Universal Language for the IoT from CES 2017 – Making it Possible for Smart Objects to Work Together on Any Network. Retrieved June 20, 2017, from http://www.zigbee.org/the-zigbee-alliance-to-unveil-universal-language-for-the-iot-from-ces-2017-making-it-possible-for-smart-objects-to-work-together-on-any-network/