

A platform for Internet-connected wireless sensor networks

Stuart Whitehead

8th January 2016

Abstract

Acknowledgements

Contents

Abstract	ii
Acknowledgements	iii
Contents	iv
List of Figures	vi
List of Tables	vii
1 Introduction	1
2 Background	2
2.1 Opportunities	3
2.2 Challenges	4
2.3 Use Cases	6
2.4 Existing Platforms	7
2.4.1 Hosting	7
2.4.2 Source Availability Model	8
2.4.3 Connectivity	8
2.4.4 Bidirectional Communication	10
2.4.5 Application Triggers	12
2.5 Sensor Hardware	12
2.5.1 Processor Architecture	12
2.5.2 Memory	13
2.5.3 Input/Output	14
2.5.4 Connectivity	14
2.6 Case Study: UK Smart Meters	15
2.6.1 Overview	15
2.6.2 Governance	17
2.6.3 Implementation	18
2.7 Conclusions	19
3 Specification	20
3.1 Functional Requirements	20
3.1.1 Framework	20
3.1.2 Demonstration Application	22
3.2 Non-functional Requirements	24

3.2.1	Constraints	24
3.2.2	Performance Requirements	25
3.2.3	Security Requirements	25
3.2.4	Software Quality Attributes	25
3.2.5	Legal, Social, Ethical and Professional Issues	26
4	Design	27
5	Implementation	28
6	Results and Evaluation	29
7	Future Work	30
8	Conclusions	31
	Bibliography	32

List of Figures

2.1	The boundary between IoT and other trends in computing	3
-----	------------------------------------------------------------------	---

List of Tables

2.1	A summary of the current state of the Internet of Things	7
2.2	Characteristics of existing IoT platforms	12
2.3	Summary of hardware boards	16

Chapter 1

Introduction

Chapter 2

Background

The term ‘Internet of Things’ captures the essence of the vision well; the vision of a world where everyday, physical objects are gateways to web-based services. These so-called ‘smart objects’ comprise of sensors to perceive their environment or context, as well as a notion of interconnectivity with other objects or services. Connected objects or services may react to collected data to trigger actions, and these actions may be digital or physical. The Internet of Things could be summarised as data collection, aggregation and reaction in the physical domain.

The boundaries between IoT and other trends help to define its place in computing. For instance the research area of Wireless Sensor Networks (WSN) carries similarities in hardware requirements and challenges. In particular, WSN also comprise of connected sensors and actuators (Mottola and Picco, 2011). WSNs differ from IoT because of the scope of connectivity—they are limited to specific applications and area coverage, such as a production line or a single building. In comparison, IoT applications have a global scope which encourages co-operation between devices, networks and services. Wireless Sensor Networks can, however, form one aspect of an IoT application.

The research area of ‘Wearables’ also overlaps with IoT. Wearables are smart devices designed to be worn or embedded within the body. They combine sensors with some form of connectivity, typically integrating with a smartphone (Wei, 2014). Consumer Wearables products are already on the shelves, such as Fitbit—a wrist-worn personal health tracker. The Fitbit wristband connects to a smartphone with Bluetooth Low Energy (BLE) and this smartphone then provides global connectivity through its wireless connection. Users can sign-in to a web-based dashboard which will collate and organise personal data. In this scenario, Wearables are collecting, aggregating and reacting to data in the physical domain. Wearables could therefore be described as a subset of IoT (as shown by Figure 2.1) because they are an application in a specific domain.

IoT can also take advantage of research conducted for the ‘Big Data’ trend. Over the past three decades, scalable and distributed data management have been a focus for the database research community (Agrawal et al., 2011). This research originally focused on traditional enterprise applications, but it has expanded to include the Cloud Computing paradigm across two classes of systems: update-heavy applications and ad-hoc analytics & decision support. IoT is expected to generate large volumes of data and so by leveraging Big Data analytical processes, valuable information can be deduced. For example, Fitbit’s web-based dashboard could use Big Data analytics to analyse personal health statistics and to find data trends.

IoT also goes some way to realise the Ubiquitous Computing concept. Ubiquitous Computing (also known as pervasive computing) envisages a world where users are surrounded by connected technology—technology in our homes, workplaces and recreational activities. In his seminal

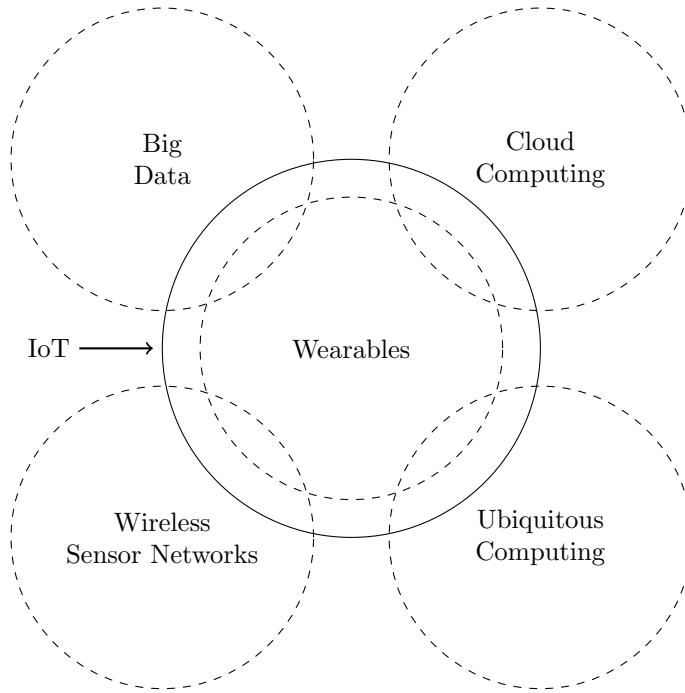


Figure 2.1: The boundary between IoT and other trends in computing

article, Weiser (1999) notes that “specialized elements of hardware and software, connected by wires, radio waves and infrared, will be so ubiquitous that no one will notice their presence”. Lyytinen and Yoo (2002) take this further and suggest that we will not only be surrounded by technology, but it will be embedded in our social and physical interactions. Research areas such as this not only contribute to the IoT concept but also benefit from its research endeavours.

2.1 Opportunities

Why should we develop IoT solutions? Would our society actually benefit from them? These are the questions posed by stakeholders of all backgrounds. Pilot projects as well as industrial and academic research have shown that there are wide-reaching opportunities to be grasped. Until recently, these opportunities were achievable only in theory or laboratory scenarios, but due to performance improvements and cost reductions in the supporting technology, IoT is very much a reality.

Mattern and Floerkemeier (2010) describe a number of opportunities created by the evolving technical capabilities of IoT systems. Since much of the value of IoT is derived from the communication of data, the technologies supporting inter-device communication and cooperation are particularly important. Wireless Personal Area Network (WPAN) technologies such as Wi-Fi, Bluetooth, ZigBee and 6LoWPAN give objects the ability to network with Internet resources or each other. These WPAN technologies also provide device addressability mechanisms which allow objects to be uniquely identified from anywhere in the world, through extensions to protocols like MAC Addressing or IPv6. With this level of global interconnectivity, novel services and products become possible.

Another main characteristic of IoT is the ability to interact with the physical domain. Digital applications will interact with the physical world in two ways: through the monitoring and sensing of physical properties and through the actuation of the physical world in reaction to data. There are a massive variety of sensors available, even to hobby markets, and can measure any imaginable physical property. The reduced cost and improved support by hardware manufacturers will allow measurements to be collected at a scale and precision not previously possible.

Since IoT microcontrollers are becoming more powerful, there are opportunities for embedded information processing. Embedded information processing refers to end devices performing some form of data processing or storage before transmitting their data; for example, an end device might analyse its own data and only transmit if a specific threshold is met, rather than relying on Cloud Computing-based processing. This is an active area of research called edge computing (or fog computing) and allows for novel methods of data processing and is another method to optimise bandwidth and power consumption.

Along with these technical capabilities are big-picture societal and economic opportunities. The European Union is a strong example of an economy which can benefit from IoT uptake. The governmental body of the EU, The European Commission, recognises the potential opportunity: “One major next step in this development [of the Internet] is to progressively evolve from a network of interconnected computers to a network of interconnected objects, from books to cars, from electrical appliances to food, and thus create an ‘Internet of things’.” In 2009 the Commission published an action plan for embracing the Internet of Things.

The action plan (The European Commission, 2009) describes how IoT will improve citizen well-being both now and into the future. In the present, citizens will benefit from specific IoT initiatives—for instance, Internet-connected health monitoring systems could alleviate pressure on medical services for the ageing society. Other applications such as connected cars or smart waste management are expected to reduce the EU’s carbon footprint and therefore protect resources for future generations.

The Commission’s action plan also describes economic opportunities. IoT has the potential to provide many new income streams to businesses as well as finding other money through efficiency savings. First of all IoT opens up new markets which were previously not feasible nor even considered. These markets may include consumer products or novel service solutions in areas such as home security and monitoring. For organisations with complex supply chains or processes, IoT could help to maximise resources and stock control through large-scale automation and efficient information exchange.

2.2 Challenges

It is apparent that IoT is still an evolving area of research with numerous challenges to be addressed. In order for IoT to become a mainstream paradigm, the technologies and ecosystem surrounding them must converge and become more mature. Mattern and Floerkemeier (2010) state that IoT is not the result of a single novel technology but rather several complementary technical developments, so invariably, the challenges span many technical disciplines.

A good user experience must be offered by these technologies to encourage adoption. Mattern and Floerkemeier (2010) state that devices “need to establish connections spontaneously, and organize and configure themselves to suit their particular environment” which they coin ‘Arrive and Operate’. The process of connecting a laptop to a home Wi-Fi router is representative of the current experience a user might have. They will turn on the Wireless Network Interface Card via a mouse and a Graphical User Interface and select their wireless network before inputting a password with a keyboard. This experience is far from ideal for constrained devices with a

simplistic user interface, or no interface at all. The challenge here is to develop technology which allows consumers to use smart objects with little or no configuration.

Device discovery and interoperability is required to build an open and extensible Internet of Things. Since the world of things is diverse, each type of device is likely to have different capabilities. Mineraud and Tarkoma (2015) state that the heterogeneity of existing platforms is considerable (numerous hardware, technologies, requirements and objectives) and as a result, IoT would benefit from a generic architecture which provides IoT developers with a common toolkit. Research efforts have gone some way to address these challenges, such as the IoT ‘meta-hub’ offered by Mineraud and Tarkoma, which provides a feed of available features for a given service.

IoT infrastructures must be scalable to handle the large number of connections and volume of data. By all estimates, IoT will have a much larger scope and footprint when compared to the existing Internet of computers. The European Commission puts this figure at 50–70 billion devices (on average, 10 per human). Mattern and Floerkemeier (2010) also note that things will be cooperating mainly within a local environment. This means that IoT devices, software and infrastructure must work equally efficiently in both small- and large-scale environments. This complexity is also reflected with the verocity and variety of data being generated; a challenge currently being addressed with research around Big Data.

Fault tolerance, power supply and efficient wireless communication are challenges facing hardware manufacturers. There are a number of possible operating environments for IoT devices, such as office spaces, homes, public spaces and remote areas, so smart objects might depend on a self-sufficient power source. The industry is therefore challenged to produce long-lasting batteries. As well as improving power supply solutions, the industry should maximise power efficiency in other areas such as existing wireless communication technologies which consume too much overhead and power.

Technical challenges will continue to be addressed through academic and industrial research, however IoT will not achieve widespread uptake without social acceptance. This is the risk that the industry is carefully attempting to balance; the social acceptance of IoT products is imperative to their success but consumers and markets could be less accepting if industries try too much too soon. The European Commission’s action plan describes practical challenges which need to be addressed.

Many aspects of digital technology is governed by public bodies and the Commission believes that IoT should not be any different. They note that technology will advance due to a normal cycle of innovation and that “simply leaving the development of IoT to the private section is not a sensible option in view of the deep societal changes that IoT will bring about.” The main areas which may need to be governed are identification, information security and ethical & legal accountability. In terms of device identification, Mattern and Floerkemeier (2010) and (The European Commission, 2009) suggest that some form public registry (similar to those governed by the Institute of Electrical and Electronics Engineers) will be necessary. In terms of legal accountability, users may be reluctant to use IoT services unless there are safeguards in place. Without effective governance of these areas, IoT may suffer from stifled innovation; a mistrust with data and jeopardised system integrity.

Standardisation is a technical consideration but also impacts on the economic potential of IoT. The purpose of a standard is to give different entities and stakeholders a common language to design, build or communicate. The widespread adoption of a standard gives businesses of all sizes the opportunity to develop interoperable solutions. In being interoperable, standards-based solutions will be suitable for a wider market and in turn, this will encourage innovation and improve international competitiveness. If IoT is to maximise economic impact and to benefit from widespread adoption, there must be accepted practices or formal standards in place.

The greatest challenges to social acceptance are security and data privacy, particularly in

the EU where the protection of privacy and personal data are two fundamental rights. The challenge with this, in respect to IoT, is that new methods of collecting and using data will be invented. Does current legislation and safeguards protect the interest of EU citizens adequately? Who will own the data—the user whom it is about or the organisation that captured it? The Commission suggests that in response to this challenge, IoT components should be designed from their inception with a privacy- and security-by-design mindset.

2.3 Use Cases

Use-cases are a helpful mechanism for demonstrating the IoT concept. It is a difficult concept to explain because there are many cooperating components and ideas and for this reason, research papers exemplify their arguments with practical examples. Although IoT applications could be developed for virtually any industry there are domains where its application is more obvious. Table 2.1 presents six such domains for IoT, together with opportunities, challenges and related areas of research.

‘Smart Cities’ is a vision which convincingly demonstrates many benefits of IoT. The Department for Business Innovation & Skills (2013) describes the main issues facing local authorities which includes: piecemeal urban infrastructure, climate change targets, the changing nature of the high street and elderly social care. The economic downturn has also reduced budgets assigned to local authorities by as much as 30% between 2010 and 2013 making cost efficiencies another issue. By developing or retrofitting urban infrastructure with IoT connectivity, local authorities can monitor services in much finer detail. For instance, Bigbelly Solar is a smart waste and recycling system. The Internet-connected waste bins allow local authorities to monitor their status and to schedule collections when they are full. Bonomi et al. (2012) also describe a system of smart, connected traffic lights which can control the traffic flow through a whole city, reducing congestion and improving safety.

IoT in the utilities sector is one use-case which has started to become realised. The British Government is requiring energy companies to install smart meters for their customers and expect most to have a smart meter installed by 2020 (The Department of Energy & Climate Change, 2013). Smart meters monitor domestic energy usage on a per-site basis and can give real-time information about how much electricity is being used, expressed in pounds and pence. For individual households this has the benefit of enabling homeowners to save money and to reduce emissions. At a national level, smart meters are a step towards reducing energy consumption and meeting climate change goals. This use case is particularly interesting and well documented, so section 2.6 investigates the smart meter concept further. Additionally, smart thermostats like Nest also allow households to minimise their gas consumption and to reduce heating bills. This is achieved through usage optimisation based on occupancy patterns.

Logistics is one area which demonstrates the efficiency savings that an IoT application can make. The European Commission (2007) states that “Freight Transport Logistics focuses on the planning, organisation, management, control and execution of freight transport operations in the supply chain” and notes that it is one of the drivers of European competitiveness. To remain competitive, this industry must continue to improve and streamline infrastructure, fleet management and goods tracking. IoT could be used to share content-related data and location information for regulatory or commercial purposes. This is achieved through the use of inexpensive RFID tags (which store specific information about the item) and GPS sensors (which can identify precise locations). This would reduce time spent by workers manually recording goods and it will reduce errors at interchange points. The Commission has coined this the ‘Internet for Cargo’.

Overlapping Research	Opportunities		Challenges		Example Use Cases
	Economic & Societal	Technical	Economic & Societal	Technical	
Cloud Computing	Citizen Well-Being	Communication & Cooperation	Governance	‘Arrive and Operate’	Smart Cities
Big Data	Economic Prosperity	Addressability	Standardisation	Interoperability	Waste Management
Ubiquitous Computing	Ageing Society	Identification	Security	Discovery	Smart Traffic Lights
Wireless Sensor Networks	New Markets	Sensing	Data Privacy	Software Complexity	Utilities
Wearables	Business Optimisation	Actuation	Trust	Scalability	Smart Meters
Edge Computing		Localisation		Data Management	Logistics
		Embedded Information Processing		Fault Tolerance	
		User Interfaces		Power Supply	
				Wireless Communication	

Table 2.1: A summary of the current state of the Internet of Things

2.4 Existing Platforms

There are a number of IoT platforms both in service and under active development; in fact, Amazon announced their own platform, Amazon IoT, when writing this very comparison (Amazon Web Services, Inc., 2015). The aim of an IoT platform and the tools which it provides does differ from vendor to vendor, however common characteristics are beginning to emerge. We propose to compare platform offerings across five dimensions: hosting model, source availability model, connectivity, bidirectional communication support and trigger support.

2.4.1 Hosting

The hosting model offered by an organisation defines which stakeholder is responsible for maintaining the IoT application and its hardware infrastructure; either the platform provider or the customer. This is a notable differentiator between platforms and can be indicative of the platform vendor’s business objectives. There are generally two variations in hosting models: Platform as a Service (PaaS) or self-hosting.

Platform as a Service

A Platform as a Service (PaaS) is a Cloud Computing concept. It is an abstraction of the complete application technology stack including both hardware and software. An organisation providing a PaaS would be responsible for the management and maintenance of the hardware such as servers, RAID backing storage and networking appliances like routers or switches. Depending on the software on offer, the vendor would also be responsible for managing and maintaining the server operating system as well as any supporting software packages and applications. Customers are typically provided access to this abstraction through a control panel or an Application Program Interface (API).

Carriots is an example of a centralised PaaS and their website describes various benefits to a customer (Carriots, 2015). Primarily the customer does not need to allocate resources for infrastructure maintenance since this is managed by them, with the result being more time for the customer to focus on business needs. There is also less investment required on behalf of the customer—PaaS resources can be provisioned when and if they are needed, rather than

purchasing hardware upfront. Another benefit is the extra layer of support—system scalability, stability and fault tolerance are the responsibility of Carriots.

Self-hosted

An alternative to a PaaS is the self-hosted option. As the name implies, this option makes customers responsible for the maintenance and management the application infrastructure (although software updates may still be provided by the platform vendor). There are technical and legal arguments to support such a business decision.

The main technical aspect is that of control. With the self-hosted option, the system architecture can be optimised for specific use-cases, such as the global location of servers to reduce application latencies (the time taken for network transmissions between devices and servers). This also gives customers direct access to the core software and makes it easier to modify it for their own purposes (if the licence or software allows for that).

Self-hosting may also be necessary for legal compliance, especially in the realm of data protection. Depending on the country of operation, it may be necessary to retain data within country boundaries and this may not be enforceable with a PaaS. In October 2015 the Court of Justice of the European Union ruled that the Safe Harbour agreement between the EU and United States is invalid (Case C-362/14). This case found that the United State’s data protection legislation was not adequate and means that any organisation sharing data under this agreement is now acting unlawfully. This problem could be avoided, or at least remedied more quickly, if data is managed from within the European Union. One example of a self-hosted platform is Nitrogen.io.

2.4.2 Source Availability Model

The Source Availability Model chosen by a platform developer defines the level of accessibility for their source code. This model comes in two forms—open or closed source—and can be further refined by a software license framework.

The source code of Open Source Software (OSS) is made publicly available. This could be served as a standard file download or, as is becoming common practice, on a code sharing service such as Github or Bitbucket. OSS will typically be provided under the conditions defined in a license, such as the GPL, MIT or Apache license frameworks. These vary on points like distribution, modification and notification of copyright (Github, Inc., 2015).

Closed Source Software is proprietary source code not made publicly available, although it may be necessary to distribute compiled binaries. This just means that the organisation does not wish to make source code available for modification or knowledge sharing.

In conjunction with the hosting model, the source availability is indicative of business objectives. Organisations wishing to commercialise their platform as a product offering will use a Closed Source model to protect their intellectual property. Conversely those organisations where knowledge sharing is an aim, or where the platform is a mechanism to sell other products or services (such as Sparkfun and their electronic hardware) may use an Open Source model.

2.4.3 Connectivity

The IoT concept *is* interconnectivity and communication, making device and application connectivity a very important topic. The platforms investigated support a range of connectivity protocols and concepts. These range from widely-accepted HTTP-based APIs to more niche protocols like CoAP and MQTT.

HTTP

The Hypertext Transfer Protocol (HTTP) underpins the internet. It benefits from widespread support and most notably, is used by web browsers to interface with web servers. RFC 2616 (Fielding et al., 1999) defines the specification for HTTP version 1.1 and notes:

It is a generic, stateless, protocol which can be used for many tasks beyond its use for hypertext, such as name servers and distributed object management systems, through the extension of its request methods, error codes and headers.

As hinted at by this RFC 2616 quote, three important features of HTTP are: request methods, error codes and headers. To generalise the HTTP lifecycle, a user agent will send a request to an origin server, the server will process the request and will return a response. The request will use an HTTP *verb* to define the action to take, such as `GET` or `POST`, and will include headers to specify other parameters. The response has an associated status code, such as `200 OK` or `404 Not Found`.

Most of the platforms investigated here support HTTP requests through a Representational State Transfer (REST) API. Fielding (2000) states that the REST architectural style emphasises scalability, independence of components, minimises latency and maximises security. These characteristics are achieved by applying constraints to the application, such as stateless communication, a uniform component interface and a layered approach to infrastructure technologies. REST methods are based on the HTTP verbs like `GET`, `POST`, `PUT` and `DELETE`. For IoT application developers, a REST API provides a scalable, uniform and robust interface between devices and the Internet.

Software engineers working on specifications for the Internet have foreseen the Internet of Things, even if it was taken in jest. RFC 2324 (Masinter, 1998) is an April Fool’s joke and defines the Hyper Text Coffee Pot Control Protocol version 1.0 (HTCPCP/1.0). It specifies methods by which an Internet-connected coffee pot can be controlled, and even adds a new error code: “Any attempt to brew coffee with a teapot should result in the error code ‘418 I’m a teapot’. The resulting entity body MAY be short and stout.”

WebSockets

The WebSocket Protocol is an independent TCP-based protocol that enables two-way communication. It uses an HTTP request as part of the handshaking process, which is treated as a connection upgrade request. RFC 6455 (Fette and Melnikov, 2011) states “The goal of this technology is to provide a mechanism for browser-based applications that need two-way communication with servers that does not rely on opening multiple HTTP connections (e.g., using `XMLHttpRequest` or `<iframe>`s and long polling).” This technology plays a vital role in enabling bidirectional communication between web browsers and servers, as will be covered in section 2.4.4.

WebSockets use standard HTTP ports for communication by default (port 80 and 443 for unencrypted and encrypted connections respectively). This has the added benefit of being compatible with common network and firewall configurations.

MQTT

MQ Telemetry Transport (MQTT) is a simple and lightweight messaging protocol. It is based on a publish/subscribe model and is specifically designed for constrained devices and low-bandwidth, high-latency or unreliable networks. In general, MQTT is used in conjunction with a message

broker. Clients subscribe to topics on this broker which will then forward any relevant messages. Clients are then free to do whatever they please with these messages (Banks and Gupta, 2014).

MQTT uses TCP/IP to transmit messages and operates on ports 1883 and 8883 for unsecured and secured uses respectively. Since these ports are not common, firewalls will typically block access. For this reason, MQTT can be tunnelled using WebSockets (and means this can be used in the browser, too).

CoAP

Constrained Application Protocol (CoAP) is another protocol designed with the Internet of Things in mind. Shelby et al. (2014) describe CoAP as “a specialised web transfer protocol for use with constrained nodes and constrained networks.” Some headline features align with principles used with HTTP, such as utilisation of the REST model. RFC 7252 defines the proposed specification for CoAP. It specifically notes some main features:

- Web protocol fulfilling M2M requirements in constrained environments
- UDP [RFC0768] binding with optional reliability supporting unicast and multicast requests
- Asynchronous message exchanges
- Low header overhead and parsing complexity
- URI and Content-type support
- Simple proxy and caching capabilities

CoAP is likened to HTTP throughout the specification however there are some notable differences. HTTP uses the TCP/IP transport protocol whereas CoAP uses UDP, a protocol with significantly less overhead. UDP is not a request/response protocol so to provide a request/response interaction model, CoAP must deal with this through a logic layer.

UDP

One of the researched platforms also offers the User Datagram Protocol (UDP) as a connectivity option. RFC 768 (Postel, 1980) notes “this protocol provides a procedure for application programs to send messages to other programs with a minimum of protocol mechanism.” To achieve ‘a minimum of protocol mechanism’, UDP does not establish a connection with the receiving device, so unlike TCP/IP it is connectionless. The protocol also specifies no mechanism for error correction so if a packet is lost in transit, it is lost forever.

Since data can be lost, this protocol should only be used in applications which can tolerate data loss. To give a real-world example, a battery-powered hygrometer sensor may be collecting data about the environmental humidity. If UDP was used as the connectivity protocol, it would allow this sensor to wake up, transmit its reading and then fall back to sleep without being concerned about the packet’s progress. If a packet was lost, it would not have business or safety impacts.

2.4.4 Bidirectional Communication

One main opportunity of IoT, as described in Section ??, is to drive actuators in response to data. There are three aspects which define whether unidirectional or bidirectional communication is possible: the connectivity protocol, the software application and the network environment. To

illustrate the following points, a hypothetical scenario will be used, where one server and one actuator are connected together through the internet. In this case, unidirectional communication means that only the actuator can initiate network requests whereas bidirectional communication allows either the server or actuator to initiate.

If the actuator is publicly addressable with a dedicated IP address, bidirectional communication is trivial to implement. Supposing that the HTTP protocol is being used for communication, both the actuator and server can initiate requests to each other by using the appropriate IP address. The server may send an HTTP request instructing the actuator to do something. In real-world scenarios, there are three factors which make bidirectional communication like this difficult: firewalls, Network Address Translation and IPv6 uptake.

Firewalls are common-place both in businesses and at home. They are a network security tool and can be either a dedicated hardware unit or software built into other devices, such as a domestic router. Their purpose is to screen both in and outbound connections which may have a malicious or compromising effect on the network integrity. The side effect which this has on IoT systems is that non-common protocols may be blocked, such as MQTT (since it uses ports 1883 and 8883). While devices behind a firewall may be publicly addressable, they may not be reachable, depending on the IoT application.

While obtaining a public IP address for each IoT device is a worthy aim, it is not achievable in many situations due to Network Address Translation. Network Address Translation (NAT) is a tool used to delay the depletion of IPv4 addresses and is very common with domestic internet connections. RFC 2663 (Srisuresh and Holdrege, 1999) states “NAT devices are used to connect an isolated address realm with private unregistered addresses to an external realm with globally unique registered addresses.” In essence, this allows a number of privately addressed devices to communicate through one public address. In terms of IoT, this means that any devices connected behind NAT will not be publicly addressable—the server can not directly send a request to the actuator.

Internet Protocol version 6 (IPv6) will solve the issue of IP address depletion. It will offer over 340 undecillion possible addresses, compared to just under 4 billion available from IPv4, and will allow every connected device to have its own IP address for the foreseeable future (The European Commission, 2008). With regards to the Internet of Things, this is still not achievable. IPv6 is still not supported by many internet service providers (ISPs) and networks, including that of Robert Gordon University. For the Internet of Things, this means that universally supported IPv6 is still a while off.

There are some useable techniques to overcome these three issues and to enable (or mimic) bidirectional communication. The first of these solutions is HTTP polling. With standard polling, the actuator would periodically ask the server for updates. If this period was 1 second, the communication may feel like it was real-time and bidirectional. This is however wasteful because not every request will result in an update. A more efficient form of polling is called long polling. The actuator will send a request to the server, but if there are no updates yet, the server will not respond. When the server does have a message to send to the actuator, it will respond and then end the request. This is better, but implementations suffer from the added complexity of managing connections.

A final and more effective solution is to implement communication using WebSockets. As previously described, the WebSocket protocol allows for bidirectional, full duplex communication and it can solve every challenge already addressed. WebSockets use the same communication ports as HTTP (port 80 and 443) by default, meaning that firewalls will allow them. Networks that support web browsing will support WebSockets. Also, the WebSocket connection can be initiated by the client and still allow bidirectional communication. In this case, the actuator can open a WebSocket connection to the server and overcome any Network Address Translation in

Service	Hosting	Source	Connectivity	Bidirectional	Triggers
Amazon IoT	PaaS	Closed	MQTT, HTTP	Yes	Yes
Bug Labs Dweet	PaaS	Closed	HTTP	Yes (app)	No
Carriots	PaaS	Closed	HTTP, MQTT	No	Yes
Sparkfun	PaaS or self-hosted	Open	HTTP	No	No
Exosite	PaaS	Closed	CoAP, HTTP, UDP	No	Yes
Google Brillo	PaaS	Closed	Unknown	Unknown	Unknown
Digi	PaaS	Closed	HTTP	Yes	Yes
IFTTT	PaaS	Closed	HTTP	No	Yes
Newaer	PaaS	Closed	HTTP	No	Yes
Nimbits	Self-hosted	Open	HTTP	No	Yes
nitrogen.io	Self-hosted	Open	MQTT, HTTP	Yes	Yes
ThingSpeak	PaaS or self-hosted	Open	HTTP	No	Yes

Table 2.2: Characteristics of existing IoT platforms

place because it does not require a public IP address.

2.4.5 Application Triggers

An application-level feature common across investigated platforms is event triggers or rules. Where supported, platforms can trigger actions based on the data received from sensors and third-party APIs. Combining examples already mentioned, a hygrometer may send data to an IoT application. An application trigger could be configured to turn on a dehumidifier actuator if the humidity passes a certain threshold. If bidirectional communication is supported, this trigger would react in real-time. Triggers could also be configured to interact with other third-party software APIs.

2.5 Sensor Hardware

The Internet of Things is a multidisciplinary area of research and is just as dependant on advancements in electrical and electronics engineering as it is computer science. Since the hardware driving IoT sensor nodes is intertwined with the upper layers of software, it would be appropriate to investigate the current state of this area too. Rather than research the intricacies of how these pieces of hardware work, this paper will investigate existing end device hardware with regards to their implementation in IoT applications, particularly technical capability and energy efficiency.

With a similar method to Section 2.4, various makes and models of hardware boards were analysed to find comparable characteristics. The manufacturers chosen—Arduino, Raspberry Pi, Intel and Samsung—represent a cross-section of the field. These manufacturers aim their products at different markets, from the DIY ‘maker’ market of the Arduino to the professional, consumer electronics market of Samsung. This section will compare and contrast hardware models produced by these manufacturers across a range of key areas: processor architecture, memory, input/output options and wireless connectivity. Table 2.3 summarises each model and their specifications.

2.5.1 Processor Architecture

Just like any other computer system, the processor is the heart of the hardware board. It is responsible for running the operating system, orchestrating the various system components and for running the user application. The type and specification of the processor defines what can be

processed and how quickly, which is ultimately reflected in the responsiveness and capability of the IoT device. Processor throughput is not the only consideration when scoping an IoT device however—energy consumption is also an important factor. The specification of the processor can be categorised into smaller areas: processor type, instruction set, number of bits, clock speed and the number of cores.

There are two broad types of processor systems, namely microcontrollers and microprocessors. A microcontroller (also known as an embedded controller) is a complete computer in one chip. A single microcontroller chip will typically combine a central processing unit (CPU), small amounts of program memory and Random Access Memory (RAM) and input/output lines (Ibrahim, 2011). In comparison, a microprocessor requires other system components to function, such as external memory, input/output lines and a clock circuit. In this regard, microprocessor hardware cannot be upgraded because it is integrated whereas a microprocessor system can, but they are cheaper to manufacture.

Processor architecture can also vary between makes and models. (Ibrahim, 2011) notes that processors can be classified by the number of bits they process, with 8 bits being the most popular for microcontrollers. Processors with a greater number of bits are more powerful but are also more expensive. The instruction set used also effects the performance of the processor; Reduced Instruction Set Computer (RISC) instructions take only one CPU cycle to complete whereas Complex Instruction Set Computer (CISC) instructions can take multiple cycles.

Clock speed and the number of cores are two final factors of a processor's performance. The clock speed describes how many cycles the CPU executes in one second and is regulated by a crystal timer or internal digital clock oscillator (DCO) A greater clock frequency means more instructions which can be processed in a time period, and the more powerful the processor. Microcontrollers typically have clock speeds in the tens of Megahertz whereas microprocessors might run at hundreds of Megahertz or a number of Gigahertz. However due to physical limitations of hardware components, there is a practical limit in possible clock speed. In this case more cores are added to the processor allowing it to evaluate multiple instructions concurrently. With regard to power consumption, Mikhaylov and Tervonen (2010) state that clock speed is one factor affecting the lifetime of a battery powered device so the CPU should be carefully considered for its application.

2.5.2 Memory

In any computer system, different types of memory are used to store program instructions and the temporary data associated with them. While these types of memory can be split into more discrete categories, there are generally two types of memory: non-volatile and volatile. Non-volatile memory, such as Read-Only Memory (ROM) or Programmable Read-Only Memory (PROM), is used to store program instructions and fixed user data. Non-volatile memory is used to store this kind of data because it is not lost when power is disconnected. In comparison, volatile memory loses its contents when power is removed and so it is used for temporary or intermediate data.

Memory characteristics also contribute to the capabilities and performance of the hardware system. Primarily, the available memory size defines how much data can be stored. The Arduino boards researched have 32KB of program memory available compared to the Gigabytes available on some Samsung Artik boards. This constrains the number of program instructions which can be stored and means the software running on the Samsung Artiks could be much more complex. Memory word length also has implications. The word length is the number of bits which a single unit in memory can store, and is commonly found to be 8, 16, 32 or 64 bits. Larger word lengths can store larger pieces of instructions or data, such as larger numbers.

2.5.3 Input/Output

The Input/Output (I/O) lines of a hardware board are the interface between sensors or actuators and the processor (or beyond). Without this physical connectivity, developers would not be able to capture information about the physical world, stopping the IoT concept in its tracks. This aspect of hardware boards is therefore important to the flexibility and future potential of IoT applications. To ensure compatibility between hardware platforms and external hardware like sensors, various industry standards have been developed.

Before any I/O standards are discussed though, it is first important to establish the importance of the operating voltage for an individual electronics circuit. The hardware boards analysed operate at various logic voltages; for instance most Arduino boards run at 5V whereas the native voltage of the Intel Edison is 1.8V. The standard logic voltage also effects I/O operation. Digital sensors may have their own, incompatible standard logic voltage—a microcontroller running at 5V would damage a sensor running at 3.3V. If directly interfacing between processors and sensors, a logic level shifter might have to be implemented so careful planning is required. Logic voltage is another aspect which affects the lifetime of a battery-powered node (Mikhaylov and Tervonen, 2010).

General Purpose Input Output (GPIO) pins are a blank canvas for engineers and developers. They are digital I/O pins with no default use and as their name suggests, can be configured as input or output. Since they are digital, GPIO pins can only read or write with 2 discrete values, logic high (1) or logic low (0), and these values usually respect the standard system voltage. Depending on the device, a number of GPIO pins might support Pulse Width Modulation (PWM). PWM is a technique for emulating analogue levels by pulsing the digital value at differing frequencies. Using a light bulb as an example, PWM could emulate the effect of dimming the light, like what could be achieved with an analogue potentiometer.

While GPIO pins allow for basic I/O operations, there is a need for communicating with more complex data. There are various available standards for interfacing between low-level electronics components. The datasheets for the selected model note some common standards, namely: Serial Peripheral Interface (SPI), Universal Asynchronous Receiver/Transmitter (UART), Inter-Integrated Circuit (I²C) and Integrated Interchip Sound (I²S). There are a variety of uses for these standards so this paper will go no further than noting that they exist.

2.5.4 Connectivity

Interconnectivity is yet one more important aspect to hardware designed for the Internet of Things. Since IoT devices are becoming increasingly mobile and wire-free, connectivity is being discussed almost exclusively in regards to wireless communication protocols and standards. As was discussed in Section ??, some IoT-specific wireless standards have already been established. Many of these technologies are supported by the various hardware platforms investigated, validating their purpose. The standards supported by these hardware platforms are IEEE 802.11 (Wi-Fi), Bluetooth and IEEE 802.15.4 (Low-Rate Wireless Personal Area Network).

Wi-Fi is a technology which has become synonymous with wireless connectivity and the Internet. The IEEE 802.11 standard states that the purpose of Wi-Fi is “to provide wireless connectivity for fixed, portable, and moving stations within a local area” where a local area could refer to a home, classroom or office space. Wi-Fi benefits from wide utilisation in all areas and industries so wireless coverage is likely to be in place already. Aust et al. (2012) state that the radio frequencies used by Wi-Fi (2.4GHz and 5GHz bands) are becoming crowded and are increasingly resulting in radio interference. This is being addressed in a new standard, IEEE 802.11ah, which makes use of the 900MHz frequency band. The two main potential advantages of this standard are greater range and less power consumption, which is beneficial to IoT devices.

Even with this standard, however, end devices are impeded by the large overhead of upper layer protocols used in conjunction with Wi-Fi.

The Bluetooth standard has been repurposed as an effective wireless communication protocol for IoT devices. Prior to the introduction of Bluetooth 4.0 in 2010, it was primarily used in multimedia applications such as streaming stereo audio (Chang, 2014). With the introduction of Bluetooth 4.0 came new features, namely Bluetooth Low Energy (BLE), which consumes such a small amount of power that a sensor can run from a coin battery for months or years. For an average usage scenario, BLE could be expected to achieve a practical maximum range of 77 meters (Labs, 2015) which makes it ideal for use-cases such as body sensors and intelligent transport systems.

One final wireless connectivity standard supported by the investigated hardware is IEEE 802.15.4 Low-Rate Wireless Personal Area Networks (WPAN). The standard states that it “provides for ultra low complexity, ultra low cost, ultra low power consumption, and low data rate wireless connectivity among inexpensive devices” and covers the physical layer (PHY) and Medium Access Control (MAC) sublayer specifications. This IEEE standard has manifested into various competing technologies, in particular ZigBee and 6LoWPAN. ZigBee is a set of layers built on top of 802.15.4 and adds three important features: routing, ad-hoc network creation and self-healing mesh (Faludi, 2010). In comparison, 6LoWPAN is an adaptive layer defined in RFC 4944 and allows IPv6 packets to be transmitted using the short addresses in 802.15.4 (Hui and Culler, 2008). The average range for ZigBee and 6LoWPAN is 291 and 191 meters respectively (Labs, 2015).

2.6 Case Study: UK Smart Meters

2.6.1 Overview

The smart meter project by the British government serves as an ideal case study to exemplify an Internet of Things application. In Section 2.3, this paper described some stand-out use cases, which were collated from various sources. Upon researching the smart meter concept further, this massive governmental project—currently being developed for the United Kingdom utilities sector—was discovered. As more research on this project was carried out, it became clear that it represents a significant commentary in regard to the IoT concept.

In comparison to other potential case studies, the smart meter project is important for many reasons. First of all, the transparent and objective nature of public projects does prevent an operational bias. It would be possible to evaluate case studies provided by commercial organisations; for instance, Digi provide case studies across a number of industries. This however introduces the risk of bias—it is in the business’s interest to make a sale. In order to satisfy stakeholders, it is also necessary for the public project to unambiguously document discussions, actions and expectations. Furthermore, the scale, purpose and complexity of this project truly puts the Internet of Things concept to the test.

Before analysing the technical details of this project, it is first important to understand the purpose of smart meters. The project was announced by the Department of Energy and Climate Change (Decc) in 2009. It ambitiously aims to replace the electricity and gas meters for all residents of the United Kingdom with so-called ‘Smart Meters’ by 2020, giving a projected time frame of 10 years (The Telegraph, 2009). For consumers, these systems comprise of two main components: the electricity/gas meter and the in-home display. The display will wirelessly connect to the meter and will provide a near real-time indication for the resources being consumed, expressed in pounds and pence (The Department of Energy and Climate Change, 2009). Utility

Board		Processor			Memory		Input/Output			Voltage	Connectivity
Make	Model	Bits	Cores	Speed	App	RAM	Analogue	Digital	PWM		
Arduino	Uno	8	1	16MHz	32KB	2KB	6	14	6	5V	-
	Yún	8	1	16MHz	32KB	2.5KB	12	20	7	5V	Ethernet Wi-Fi
	Pro Mini	8	1	8MHz/16MHz	32KB	2KB	6	14	6	3.3V/5V	-
Raspberry Pi	2	32	4	900MHz	SD Card	1GB	0	40	0	5V	Ethernet
	A+	32	1	700MHz	SD Card	256MB	0	40	0	5V	-
	Zero	32	1	1GHz	SD Card	512MB	0	40	0	5V	-
Intel	Edison	64	2	500MHz	4GB	1GB	6	20	4	1.8V/3.3V	Wi-Fi a/b/g/n Bluetooth 4.0
Samsung	Artik 1	32	1	240MHz	4MB	1MB	2	0	0	Unknown	Bluetooth 4.0
	Artik 5	32	2	1GHz	4GB	512MB	2	47	2	1.8V/2.4V	Wi-Fi a/b/g/n Bluetooth 4.0 ZigBee/802.15.4
	Artik 10	32	4+4	1.3GHz/1GHz	16GB	2GB	6	51	2	1.8V/2.4V	Wi-Fi a/b/g/n Bluetooth 4.0 ZigBee/802.15.4

Table 2.3: Summary of hardware boards

companies will also be provided with remote access to the meter, primarily allowing them take readings.

With an estimated cost of £10.9 billion (The Department of Energy and Climate Change, 2014a), the project must deliver benefits to consumers, suppliers and the government. One of the main drivers for meters are the potential financial savings. For the consumer, they are more aware of their own energy usage which allows them to reduce their spending. Into the future, this could become automated with Smart Appliances which wait for cheap energy. For the supplier, large savings will be made through the automation of meter readings and billing. Operational maintenance will also become streamlined as smart meters can immediately identify faults. For the government, efficiency savings will reduce the national environmental impact and will help the United Kingdom meet climate change targets (Thomas and Jenkins, 2012). The total projected savings from the combination of these points is £17.1 billion, resulting in a net benefit to the British economy of at least £6 billion (The Department of Energy and Climate Change, 2014a).

2.6.2 Governance

Effective governance and organisation is imperative for the success of the smart meter roll-out in the United Kingdom. Governance was discussed, in board terms, as part of Section ?? and found three main areas which may require governing: device addressability, information security and ethical & legal accountability. Similar issues face the British government. The Department for Energy and Climate Change have been responsible for managing the smart meter programme since April 2012 and delegates governing roles to various actors in the project. Some of the main actors include the Office of Gas and Electricity Markets (Ofgem), the purpose-built Data and Communications Company (DCC) as well as various subcontractors and licensees. These bodies govern the smart meter project roll-out across many areas, including two which are of special interest to this paper: consumer protection and technical implementation.

Widespread social acceptance is one of the main challenges facing IoT products and services; consumer protection offered by Decc and its subcontractors goes some way to earn this public trust. First and foremost, the energy data generated by smart meters is useful to consumers, suppliers and the government. In response to the privacy issues which this creates, the Decc has developed the Data Access and Privacy Framework (DAPF). The Department of Energy and Climate Change (2015) notes that this governing framework serves three main purposes:

- Protect consumers' interests, including by addressing concerns that consumers may have about privacy;
- Enable proportionate access to data by authorised parties to ensure that benefits can be delivered; and
- Promote competition and innovation in the developing energy services market.

The DAPF is expected to be finalised by 2018. The Decc also addresses specific consumer concerns with governance and legislation. For instance, there are restrictions in regards to the supplier-led installation as detailed by the Smart Meter Installation Code of Practice, including: prohibition of sales during installation visits and the mandatory provision of energy advice.

Governance also extends to the technical standards and specifications used for the smart meter project. One important challenge facing this project is hardware and software interoperability between the large number of parties. The Smart Metering Equipment Technical Specifications (SMETS) document was drawn up in 2012 and represents the technical standards to be followed

by suppliers and systems developers for the in-home products. The responsibility of Wide Area Network communication has been delegated to the Data and Communications Company (DCC). This organisation specifies its own standards for connecting to the WAN, which go as far as XML schema for inter-system communication.

2.6.3 Implementation

From the perspective of this paper, the technical implementation is the most interesting aspect of the smart meter project. There is a huge level of complexity and interconnectivity covered by SMETS and DCC specifications. The completed system will be a distributed and connected platform for smart meters in the United Kingdom and can be split into three constituent components: energy consumers, wide-area connectivity and service users. The implementation is summarised in Figure x.x.

Before discussing the implementation of specific technologies it is first worthwhile to understand the high-level system architecture. The energy consumers for the smart meter project are homes and small businesses. As was previously noted, there are three product types which each premises will have: smart meters (gas and electric), in-house displays and communication hubs. The communication hubs have two responsibilities, namely to provide premises-wide wireless connectivity—dubbed the Smart Meter Home Area Network (SM HAN)—and to connect each SM HAN to the nationwide Wide Area Network (WAN) provided by the Data and Communications Company. Service users are the utility companies like British Gas or Scottish and Southern Energy (SSE) as well as authorised third-parties such as online energy comparison websites. Authorised service users will gain bidirectional connectivity with their customer’s smart meters through the DCC WAN.

The SMETS and Communications Hub Technical Specification (CHTS) documents complement one another to unambiguously define the functional requirements for smart meters and the home area networks. Since the communication hub will provide wireless connectivity across a single premises, its functional requirements are indicative of how this network will operate. The Department of Energy and Climate Change (2014b) state that the HAN interface of the communications hub will use ZigBee over the 2.4GHz frequency band. The CHTS also notes the minimum capacity of the SM HAN: four Electricity Smart Metering Equipment (ESME), one Gas Smart metering Equipment (GSME), one Gas Proxy Function (GPF), seven Type 1 devices and three Type 2 devices. Type 1 devices are those which can issue any command to ESME or GSME meters whereas Type 2 devices can only issue read requests (The Energy & Utilities Alliance, 2014).

Individual metering devices have their own functional requirements which will inform their hardware implementation. The high-level expectations of a ESME or GSME device are: a clock, a data store, meter containing one measure element, a HAN interface, a load switch, a Random Number Generator and a user interface (The Department of Energy and Climate Change, 2014c). It is also important to note that ESME or GSME devices must be capable of storing 13 months of readings taken at 30-minute intervals, even after power loss. Thomas and Jenkins (2012) compared the UK requirements against an existing smart meter, the Elster REX2. This meter has an 8-bit Texas Instrument SoC with a clock speed of 32MHz, 4KB of RAM, 256KB of application memory along with 21 GPIO lines and up to 8 analogue inputs. These specifications would place the required hardware in the realm of the Arduinos researched in 2.5 however the authors argue that the UK devices would need to be more powerful and with greater memory due to the data storage and potential computational requirements.

The final piece to the smart meter project is the Wide Area Network managed by the Data and Communications Company. The DCC is responsible for secure communication, access control

and scheduled data retrieval for this project. Since the installation environments will differ from premises to premises, various connectivity methods are being employed, such as cellular, broadband and 802.15.4 mesh radio. This is, in essence, the platform supporting the whole project. The DCC will maintain a web-based service where service users can issue HTTP requests with XML document payloads to achieve tasks. The possible functions are defined in the DCC User Interface Specifications (DUIS).

2.7 Conclusions

Chapter 3

Specification

To obtain a complete and practical understanding of IoT, the software implementation accompanying this paper will comprise of two distinct components: a generic IoT application framework and a demonstration application. Mineraud and Tarkoma (2015) suggest that developers would benefit from a generic architecture which provides a common set of tools, and that is the aim of the framework component. The second component has two main purposes. First of all, it will build on top of this framework with the aim of validating design decisions. The second purpose is to demonstrate the opportunities present in IoT. This chapter will define the requirements for both of these components.

To help reference these two software components throughout the remainder of this paper, they have been given product names. Haar is a cold sea fog which forms on the east coast of Scotland and is a fitting metaphor for IoT being all around us. It is also a nod towards the Fog Computing paradigm, and towards Robert Gordon University's location in Aberdeen. The generic framework will be called the Haar Engine and the demonstration application will be named Haar.

3.1 Functional Requirements

3.1.1 Framework

The target users of the Haar Engine are designers and developers of IoT services and applications. The general aim of a framework is to encapsulate design decisions into a logical and elegant toolkit. The Haar Engine aims to perform the same task by encapsulating the knowledge which has been collated in Chapter 2. The following subsection specifies the main requirements.

User and Device Management

Users and devices are two overlapping components of an IoT framework. Nitrogen.io is an existing IoT platform and refers to users and devices as *principals* of the system. The documentation states that principals are a unit of authentication and authorisation. Since users and devices of the Haar Engine share a number of overlapping requirements, this project will adopt the same terminology. The following requirements have been derived from analysis of existing platforms and the requirements of use cases.

1. The framework shall model users

- (a) A user shall be identified by a unique username
 - (b) A user shall have an associated profile including: full name, email address
 - (c) Users shall be assigned a privilege level: standard or administrator
2. The framework shall authenticate genuine users only
3. The framework shall model connected IoT devices
 - (a) A device shall be identified by a unique identification number
 - (b) A device shall be designated as either an input (sensor) or output (actuator)
4. The framework shall authenticate genuine devices only
5. The framework shall authorise and facilitate the management of devices
 - (a) A device will have one owner
 - (b) Access to device data and configuration options shall be restricted to the device owner by default
 - (c) The device owner shall be able to make device data public
 - (d) A device owner shall be able to grant access permission to specified users

Device Connectivity

A main aspect of the IoT concept is the interconnection of devices. The Haar Engine is responsible for managing the connectivity between devices and itself. The issue surrounding bidirectional communication was described in Section 2.4.4, which should be addressed by this framework.

1. The framework shall establish a connection with end devices
 - (a) Devices shall be addressable and identifiable whilst the connection is open
 - (b) The connection shall remain open under normal operating conditions
 - (c) Under error conditions, the connection shall be reestablished
2. The connection shall be bidirectional
 - (a) Input devices shall be able to transmit data packets to the framework
 - (b) The framework shall be able to transmit data packages to output devices
 - (c) The connection shall be tolerant of network obstacles such as firewalls and Network Address Translation

Data Storage

IoT applications will collect a large volume of data. The data collected by these applications will vary in structure and type, so the Haar Engine must be tolerant of this. The developers potentially using this framework will have specific domain knowledge and so should be empowered to tailor the system for their needs.

1. The framework shall store data received by devices
2. The framework shall provide an interface for using different database types
 - (a) The framework shall provide a default 'out of the box' database connector
 - (b) Application developers shall be able to create their own database connectors

Data Access API

The Haar Engine must be able to provide access to stored data. Primarily this access will be for use in its own application, however 3rd-party access would enable interoperability between external services and applications.

1. The framework shall provide structured access to stored data
 - (a) Access shall be granted to authenticated and authorised users only
2. Application developers shall be able to modify data access
 - (a) Application developers shall be able to add custom data searches
 - (b) Application developers shall be able to add custom data filters

Real-Time Event API

The ability to react to data in real-time enables novel use cases. As with the Data Access API, the primary purpose is to satisfy the needs of a specific application. However, 3rd-party access to this API would allow for further real-time integrations.

1. The framework shall provide a real-time event API
 - (a) Client applications shall be able to listen for device events
 - (b) The real-time API shall leverage bidirectional connectivity with devices
2. The API shall provide real-time access to data received from devices
3. The real-time API shall enable developers to create application rules and triggers

3.1.2 Demonstration Application

Haar is the second software component for this project. The aim of Haar is to validate the Haar Engine in practice, as well as to demonstrate the opportunities present in the IoT concept. This will be achieved through the implementation of an arbitrary web-based application which sufficiently covers key features.

Devices

The IoT concept enables the interconnection of devices so this is a logic requirement to begin with. Haar should comprise of at least two separate local device networks to demonstrate global interactivity. These local networks should themselves comprise of a number of devices with enough variety to validate Haar Engine use cases.

1. The application shall comprise of two local area device networks
2. Devices of these networks shall be capable of establishing a connection between themselves and the web application
3. The device networks shall comprise of two sensor devices
 - (a) The device network shall contain a sensor device which measures a single data point, such as temperature

- (b) The device network shall contain a sensor device which measures more complex data, such as a vector of wind direction and speed
- 4. The device networks shall comprise of a single actuator device
 - (a) The actuator device shall be flexible enough to represent a variety of data types

Dashboard

The web-based dashboard will be the main interface between a user and their devices.

1. The dashboard shall be accessible on the World Wide Web
2. The dashboard shall authenticate users with a username and password
3. The dashboard shall list profile details
4. The user shall be able to manage their devices
 - (a) The dashboard shall list devices owned by the user
 - (b) The user shall be able to add a new device
 - (c) The dashboard shall show whether devices are connected or not
 - (d) The user shall be able to transfer ownership of the device
 - (e) The user shall be able to grant access permissions to other users
5. The dashboard shall enable users manage application rules
 - (a) The dashboard shall list existing rules
 - (b) The user shall be able to create new rules
 - (c) An actuator device shall be able to react to sensed data
 - (d) User devices shall be able to integrate with 3rd-party services [See 3rd-Party Integration overleaf]
6. The dashboard shall display data for a given device [see Data Visualisation below]
7. The dashboard shall be able to trigger actuators with virtual controls

Data Visualisation

There is an opportunity to develop a rich user interface for the dashboard. Since so much of IoT relies on data, it would be appropriate to develop example data visualisation tools for it.

1. A section of the dashboard shall be dedicated to data visualisation
2. A generic visualisation tool shall plot temporal data as a graph
 - (a) The date range shall be configurable
 - (b) Multiple data sources shall be comparable on one graph interface
 - (c) The graph shall leverage the real-time event API to update when new data is received
3. Specialised visualisation tools shall reflect specific device types. For example, a virtual thermometer would visualise a temperature
 - (a) Specialised visualisation tools shall leverage the real-time event API to update when new data is received

3rd-Party Integration

Interoperability between IoT services is described as a challenge in Section 2.2. Haar should therefore demonstrate an ability to integrate with third-party services.

1. The application shall provide pre-defined 3rd-party integrations
2. The integrations shall be listed as 3rd-party rules
3. One integration shall demonstrate reaction to a 3rd-party event
4. One integration shall trigger a 3rd-party service in response to new data

3.2 Non-functional Requirements

In addition to the features required for Haar and the Haar Engine, there are a number of additional considerations. Since both of these software components are destined for use in the same system, this section will detail their non-function requirements collectively.

3.2.1 Constraints

Network Environment

The potential operating environments in which IoT devices could be implemented vary from domestic household appliances to heavy industrial applications. These networks will all have different configurations, capabilities and customisability. In order to reduce deployment issues, the software components must operate in a common network scenario. A typical home network will be used as a baseline, where only common firewall ports will be allowed.

Public IP Address

IPv6 is the successor to IPv4 and will allow every connected device to have a unique, globally addressable IP address. While this is the direction the industry is heading in, many businesses and Internet Service Providers are not prepared its adoption. Network Address Translation (NAT) is still commonly deployed and prevents devices on these networks from being publically addressable. It should therefore be assumed that end devices will not have a public IP address.

Initial Setup

In a domestic situation, consumers would be expected to connect products to their internet connection by themselves. This is an important user experience to get right. While this project acknowledges the importance of this, it will not be considered a requirement for Haar so more effort can be afforded to developing a robust application.

Sensor Nodes

To demonstrate the various framework use cases, the application should connect a variety of sensor types. To ensure this project remains achievable, sensor nodes will be limited to those whose data can be represented by a single data interchange format like XML or JSON. Binary data such as images or audio will not be considered for this project.

3.2.2 Performance Requirements

Since this project is a research endeavor, it neither requires nor promises any performance benchmarks. In saying that, the implemented product should meet general performance expectations, especially in regards to any web-based user interfaces.

3.2.3 Security Requirements

This particular software product will not store sensitive personal details, nor will it need to satisfy criteria for professional accreditation. However security is an important topic in IoT and so real-world security measures should be implemented. In particular, any device or application connectivity should be implemented over encrypted connections to prevent potential network sniffing. Also any live demonstration versions of this software should be hosted on up-to-date hosting services to prevent any bug exploitations.

3.2.4 Software Quality Attributes

Extensibility

The application domain of an IoT project could be in virtually any industry. It is important that this software product is extensible, meaning that the core functionality can be extended to cover specific use-cases.

Portability

The server infrastructure supporting a generic platform such as this could vary between organisations and use-cases. For instance it may be beneficial to use a Platform as a Service such as Heroku or conversely a range of dedicated servers may be in use. This project should be platform agnostic.

Scalability

It is difficult to predict the exact number of sensor nodes and the data which they will produce. The software components should be scalable, either horizontally and/or vertically.

Testability

It is important that core system functions execute as designed. This project should therefore be testable through assertions where possible and appropriate.

Robustness

With many devices relying on a system for data and connectivity, system stability is an important focus. The framework should strive to be as fault tolerant as possible, however this is the sum of many parts. Reliable hardware infrastructure and high quality tested code all play a part.

Reusability

Of course a main feature of a generic framework is the ability to be reused. Two different organisations with different use-cases should both be able to use the framework without issue.

Chapter 4

Design

Chapter 5

Implementation

Chapter 6

Results and Evaluation

Chapter 7

Future Work

Chapter 8

Conclusions

Bibliography

- Divyakant Agrawal, Sudipto Das, and Amr El Abbadi. Big data and cloud computing: Current state and future opportunities. In *Proceedings of the 14th International Conference on Extending Database Technology*, EDBT/ICDT '11, pages 530–533, New York, NY, USA, 2011. ACM. ISBN 978-1-4503-0528-0. doi: 10.1145/1951365.1951432. URL <http://doi.acm.org/10.1145/1951365.1951432>.
- Amazon Web Services, Inc. Announcing aws iot, now in beta. Seattle, WA: Amazon Web Services [Online], Oct 2015. URL <https://aws.amazon.com/about-aws/whats-new/2015/10/announcing-aws-iot-now-in-beta/>. [Accessed 10 October 2015].
- S. Aust, R.V. Prasad, and I.G.M.M. Niemegeers. Ieee 802.11ah: Advantages in standards and further challenges for sub 1 ghz wi-fi. In *Communications (ICC), 2012 IEEE International Conference on*, pages 6885–6889, June 2012. doi: 10.1109/ICC.2012.6364903.
- Andrew Banks and Rahul Gupta. Mqtt version 3.1.1. OASIS Standard, Oct 2014. URL <http://docs.oasis-open.org/mqtt/mqtt/v3.1.1/os/mqtt-v3.1.1-os.pdf>.
- Flavio Bonomi, Rodolfo Milito, Jiang Zhu, and Sateesh Addepalli. Fog computing and its role in the internet of things. In *Proceedings of the First Edition of the MCC Workshop on Mobile Cloud Computing*, MCC '12, pages 13–16, New York, NY, USA, 2012. ACM. ISBN 978-1-4503-1519-7. doi: 10.1145/2342509.2342513. URL <http://doi.acm.org/10.1145/2342509.2342513>.
- Carriots. What is carriots. Madrid: Carriots [Online], November 2015. URL <https://www.carriots.com/what-is-carriots>. [Accessed 12 November 2015].
- Case C-362/14. Maximillian Schrems v Data Protection Commissioner. OJ C351, Oct 2015. URL <http://curia.europa.eu/juris/document/document.jsf?text=&docid=172254&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=199525>.
- Kuor-Hsin Chang. Bluetooth: a viable solution for iot? [industry perspectives]. *Wireless Communications, IEEE*, 21(6):6–7, December 2014. ISSN 1536-1284. doi: 10.1109/MWC.2014.7000963.
- Robert Faludi. *Building Wireless Sensor Networks: With ZigBee, XBee, Arduino, and Processing*. O'Reilly Media, Inc., 1st edition, 2010. ISBN 0596807732, 9780596807733.
- I. Fette and A. Melnikov. The WebSocket Protocol. RFC 6455 (Proposed Standard), December 2011. URL <http://www.ietf.org/rfc/rfc6455.txt>.

- R. Fielding, J. Gettys, J. Mogul, H. Frystyk, L. Masinter, P. Leach, and T. Berners-Lee. Hypertext Transfer Protocol – HTTP/1.1. RFC 2616 (Draft Standard), June 1999. URL <http://www.ietf.org/rfc/rfc2616.txt>. Obsoleted by RFCs 7230, 7231, 7232, 7233, 7234, 7235, updated by RFCs 2817, 5785, 6266, 6585.
- Roy Thomas Fielding. Architectural styles and the design of network-based software architectures. Irvine, CA: University of California, 2000. URL https://www.ics.uci.edu/~fielding/pubs/dissertation/rest_arch_style.htm.
- Github, Inc. Choose a license. San Francisco, CA: Github, Oct 2015. URL <http://choosealicense.com/>. [Accessed 14 October 2015].
- Jonathan W. Hui and David E. Culler. Ip is dead, long live ip for wireless sensor networks. In *Proceedings of the 6th ACM Conference on Embedded Network Sensor Systems*, SenSys '08, pages 15–28, New York, NY, USA, 2008. ACM. ISBN 978-1-59593-990-6. doi: 10.1145/1460412.1460415. URL <http://doi.acm.org/10.1145/1460412.1460415>.
- Dogan Ibrahim. Advanced pic microcontroller projects in c. Oxford: Newnes, 2011. URL <http://www.mylibrary.com?ID=127324>. [Accessed 1 December 2015].
- Link Labs. M2m & iot technologies explained. Annapolis, MD: Link Labs, 2015.
- Kalle Lyytinen and Youngjin Yoo. Introduction. *Commun. ACM*, 45(12):62–65, December 2002. ISSN 0001-0782. doi: 10.1145/585597.585616. URL <http://doi.acm.org/10.1145/585597.585616>.
- L. Masinter. Hyper Text Coffee Pot Control Protocol (HTCPCP/1.0). RFC 2324 (Informational), April 1998. URL <http://www.ietf.org/rfc/rfc2324.txt>. Updated by RFC 7168.
- Friedemann Mattern and Christian Floerkemeier. From active data management to event-based systems and more. chapter From the Internet of Computers to the Internet of Things, pages 242–259. Springer-Verlag, Berlin, Heidelberg, 2010. ISBN 3-642-17225-3, 978-3-642-17225-0.
- K. Mikhaylov and J. Tervonen. Optimization of microcontroller hardware parameters for wireless sensor network node power consumption and lifetime improvement. In *Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), 2010 International Congress on*, pages 1150–1156, Oct 2010. doi: 10.1109/ICUMT.2010.5676525.
- Julien Mineraud and Sasu Tarkoma. Toward interoperability for the internet of things with meta-hubs. Technical Report arXiv:1511.08063v1, University of Helsinki, Helsinki, Finland, nov 2015. URL <http://arxiv.org/pdf/1511.08063v1.pdf>.
- Luca Mottola and Gian Pietro Picco. Programming wireless sensor networks: Fundamental concepts and state of the art. *ACM Comput. Surv.*, 43(3):19:1–19:51, April 2011. ISSN 0360-0300. doi: 10.1145/1922649.1922656. URL <http://doi.acm.org/10.1145/1922649.1922656>.
- J. Postel. User Datagram Protocol. RFC 768 (INTERNET STANDARD), August 1980. URL <http://www.ietf.org/rfc/rfc768.txt>.
- Z. Shelby, K. Hartke, and C. Bormann. The Constrained Application Protocol (CoAP). RFC 7252 (Proposed Standard), June 2014. URL <http://www.ietf.org/rfc/rfc7252.txt>.
- P. Srisuresh and M. Holdrege. IP Network Address Translator (NAT) Terminology and Considerations. RFC 2663 (Informational), August 1999. URL <http://www.ietf.org/rfc/rfc2663.txt>.

- The Department for Business Innovation & Skills. Smart cities background paper. *London: Department for Business Innovation & Skills Publications*, Oct 2013. URL https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/246019/bis-13-1209-smart-cities-background-paper-digital.pdf.
- The Department of Energy & Climate Change. Smart meters: a guide. *London: Department of Energy & Climate Change*, Oct 2013. URL <https://www.gov.uk/guidance/smart-meters-how-they-work>. [Accessed 29 November 2015].
- The Department of Energy and Climate Change. Smart meters: a guide. *London: Department of Energy and Climate Change [Online]*, Oct 2009. URL <https://www.gov.uk/guidance/smart-meters-how-they-work>.
- The Department of Energy and Climate Change. Third annual report on the roll-out of smart meters. *London: Department of Energy and Climate Change*, Dec 2014a.
- The Department of Energy and Climate Change. Communications hub technical specifications. *London: Department of Energy and Climate Change*, Nov 2014b.
- The Department of Energy and Climate Change. Smart metering equipment technical specifications. *London: Department of Energy and Climate Change*, Nov 2014c.
- The Department of Energy and Climate Change. Consultation on the timing of the review of the data access and privacy framework. *London: Department of Energy and Climate Change [Online]*, Mar 2015. URL <https://www.gov.uk/government/consultations/consultation-on-the-timing-of-the-review-of-the-data-access-and-privacy-framework>.
- The Energy & Utilities Alliance. Smart metering device assurance scheme operator services. *Kenilworth: Energy & Utilities Alliance [Online]*, Sep 2014. URL [http://www.eua.org.uk/sites/default/files/SMDA%20Scheme%20Operator%20RFP%20v1.2%20\(Final\).pdf](http://www.eua.org.uk/sites/default/files/SMDA%20Scheme%20Operator%20RFP%20v1.2%20(Final).pdf).
- The European Commission. Freight transport logistics action plan. *Luxembourg: Publications Office of the European Union, COM/2007/0607*, Oct 2007. URL <http://www.ipex.eu/IPEXL-WEB/dossier/dossier.do?code=COM&year=2007&number=0607>.
- The European Commission. Action plan for the deployment of internet protocol version 6 (ipv6) in europe. *Luxembourg: Publications Office of the European Union, COM/2008/0313*, May 2008. URL <http://www.ipex.eu/IPEXL-WEB/dossier/document/COM20080313FIN.do>.
- The European Commission. Internet of things — an action plan for europe. *Luxembourg: Publications Office of the European Union, COM/2009/0278*, June 2009. URL <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52009DC0278>.
- The Telegraph. Energy suppliers to install smart meters in all households by 2020. Dec 2009. URL <http://www.telegraph.co.uk/news/earth/energy/6708822/Energy-suppliers-to-install-smart-meters-in-all-households-by-2020.html>. [Accessed 5 December 2015].
- Lee Thomas and Prof. Nick Jenkins. Smart metering for the uk. *HubNet [Online]*, Jun 2012. URL http://www.hubnet.org.uk/position_papers.
- J. Wei. How wearables intersect with the cloud and the internet of things : Considerations for the developers of wearables. *Consumer Electronics Magazine, IEEE*, 3(3):53–56, July 2014. ISSN 2162-2248. doi: 10.1109/MCE.2014.2317895.

Mark Weiser. The computer for the 21st century. *SIGMOBILE Mob. Comput. Commun. Rev.*, 3(3):3–11, July 1999. ISSN 1559-1662. doi: 10.1145/329124.329126. URL <http://doi.acm.org/10.1145/329124.329126>.