

1809810

by David Thomas

Submission date: 24-Apr-2022 09:34PM (UTC+0100)

Submission ID: 177059011

File name: 16526_David_Thomas_1809810_179584_1530465563.pdf (827.57K)

Word count: 6398

Character count: 41633

75-80

Course: BSc (Hons) Electrical and Electronic Engineering
Module: SGEE6005 Electronic Design
Assignment: Micro-controllers and the Internet of Things
Name: David Mathew Thomas
University number: 1809810
Date submitted: 24-04-2022
Word count: 3291 -5

- ① CITATION LIST IS OF GOOD LENGTH, CITATIONS ARE HARVARD.
- ② RESEARCH IS EXTENSIVE AND COVERS ALL THE CRITERIA.
- ③ IT WOULD HAVE BEEN BENEFICIAL TO CONTEXTUALISE WITH A SPECIFIC EXAMPLE. AS IS, THE REPORT IS A BIT DESCRIPTIVE. A CONTEXT WOULD ALLOW CRITICAL ANALYSIS AND DEBATE.
- ④ THE WEATHER STATION WAS SUCCESSFULLY IMPLEMENTED.
- ⑤ EXCESSIVE USE OF LARGE TABLES OF TEXT CIRCUMVENTS THE WORD COUNT. AVOID THIS NEXT YEAR.

Contents

1. Executive Summary	5
2. Research Introduction	6
3. Research	7
4. Research Summary.....	23
5. Methodology, Testing & Results for Arduino IOT	24
6. Conclusions & Recommendations.....	28
7. References.....	29
8. Bibliography	31
9. Appendix.....	32

Table of Figures

Figure 1 - Pictorial representation of IoT.....	7
Figure 2 - Pictorial representation of IoT Enabling Technology	8
Figure 3 - IoT Architecture.....	12
Figure 4 - IoT Technology Classification.....	12
Figure 5 - Device-to-Device Model	13
Figure 6 - Device-to-Cloud Model	14
Figure 7 - Device-to-Gateway Model.....	15
Figure 8 - Back-End Data Sharing Model	15
Figure 9 - Drivers for IoT	16
Figure 10 - IoT Opportunities.....	17
Figure 11 - Examples of Challenges Facing IoT.....	18
Figure 12 - IoT Security/Privacy Threats	19
Figure 13 - Possible IoT Security Solutions	20
Figure 14 - AirTag® Communication Model	21
Figure 15 - Personal Weather Station.....	25
Figure 16 - Weather Station Carrier Results	26
Figure 17 - Weather Station Dashboard	27
Figure 18 - Weather Station Data Trend.....	27
Figure 19 - Arduino 1010 Board.....	32
Figure 20 - Arduino Weather Station Sketch Code.....	35
Figure 21 - Weather Station Dashboard Design	36

Table of Tables

Table 1 - Some IoT Enabling Technologies & Protocols.....	9
Table 2 - Key IoT Characteristics.....	10
Table 3 - IoT Enabling Technology & Functional Blocks	12
Table 4 - Examples of Published Security/Privacy Breaches Involving IoT	21
Table 5 - IoT Arduino Kit	24

1. Executive Summary

The project aim was to provide an understanding of the concept Internet of Things (IoT) and a practical demonstration of its use. The first part of the project involved research into IoT, and its relationship with Industry 4.0.

Industry 4.0 and Machine-to-Machine (M2M) aims to revolutionize industry operation and growth, focussing on efficiency, automation, connectivity and 'real-time' data. These however form part of a bigger picture, being a subset of the phenomenon IoT. IoT is an emerging global concept that aims to connect everyday objects to the internet, with the vision of transforming and facilitating our current way of life, personalizing interaction of users with devices/'things'. The projected concept of has brought excitement to several industries; with the potential for integration into homes, factories, environment and trade & economy to name but a few. In fact, with an increasing number of innovative solutions presented to a variety of businesses and industries, the global projection is that by 2025 there will be over 100 billion devices connected, worth over 10 trillion dollars (Internet Society, 2015).

Although IoT brings with it several transformational benefits, revolving around its powerful ability to analyse vast amounts of data, there are several challenges currently facing IoT that must firstly be addressed before it can be fully embraced, and its true potential realized. Concerns over the level of security and privacy for consumer data remain paramount, with increasing reports of breaches being publicised, the pressure for security specialists to overcome cyber-criminals is ever increasing.

In 2015, the Internet Society published guidance to IoT: The Internet of Things: An Overview, summarising the current position, including advances and challenges facing it. It surmised that there were four key concepts: IoT definitions, Enabling Technologies, Connectivity Models and Transformational Potential, that formed the foundations of IoT (Internet Society, 2015). The research explored these concepts, the literature, and considered the opportunities and challenges facing implementation of IoT, providing a clear understanding on how IoT has developed alongside technological advances, helping to create smart environments not only as part of Industry 4.0 but as part of everyday life.

The second part of the project involved the design and practical execution of an IoT enabled Arduino Weather Monitoring System used to visualize and control projects. Using the Arduino kit, a sensor module was built and the Arduino IoT cloud configured to enable recording and monitoring of the sensor data, involving both single and multiple parameters. The system was successfully tested, demonstrating IoT technology, the principle of Device-to-Cloud communication, and its capabilities, supporting the research undertaken.

2. Research Introduction

Industry 4.0 is the next stage/revolution of industry, focussing on digitalization of technology, automation, connectivity and 'real-time' data. An essential element of this concept is M2M, communication or interaction between two machines, or interconnection between the machines and the internet. The latter however, forms part of a bigger revolution, Industry 4.0 and M2M being a subset of the concept, Internet of Things (IoT) (Epicor, 2022). To embrace Industry 4.0 and optimize opportunities, industries must first understand IoT, including its driving forces and threats.

IoT, an emerging model connecting devices or 'things' to the internet, has revolutionised communication, interactions and day-to-day activities from home smart systems to industry maintenance and smart cities, promoting intelligence and efficiency (Gupta, 2021). Although coined back in 1999 as part of a presentation by Kevin Ashton to revolutionise tracking of consumer supply chains using Radio Frequency Identification (RFID), IoT is not a new concept, initial principles dating back to the 1980's (Hamza, 2021). Since then, IoT has been adopted by many businesses and industries under the guise of M2M & Industry 4.0, to create a modular, smarter, more efficient (and cost-effective) environment, where machines are effectively autonomous (GSMA, 2014). Increasing attention has been placed on extending the advantage to the wider population, IoT being incorporated into the home and workplace, with nearly 50 billion devices currently existence (Hamza, 2021).

3. Research Body

IoT has attracted a number of definitions over the years, with the idea that almost all physical ‘things’ can essentially be a computer and connect to the internet (fleisch, 2010), whether that be a combination of people-to-people, people-to-machines/things or machines/things-to-machine/things (S Patel, 2016); a global infrastructure, where devices can essentially be connected at anytime, anywhere, to anything/anyone using any service or network path. It is a revolution of the virtual and physical world, enabling a network, or integration, of various existing and evolving items incorporated with sensors or processes, connected to the internet, using a variety of protocols to share information, be interoperable and make intelligent context-based decisions. Unlike the traditional internet model, IoT involves connection of devices not typically/traditionally seen as ‘computers’ (Hadzialic, 2018)

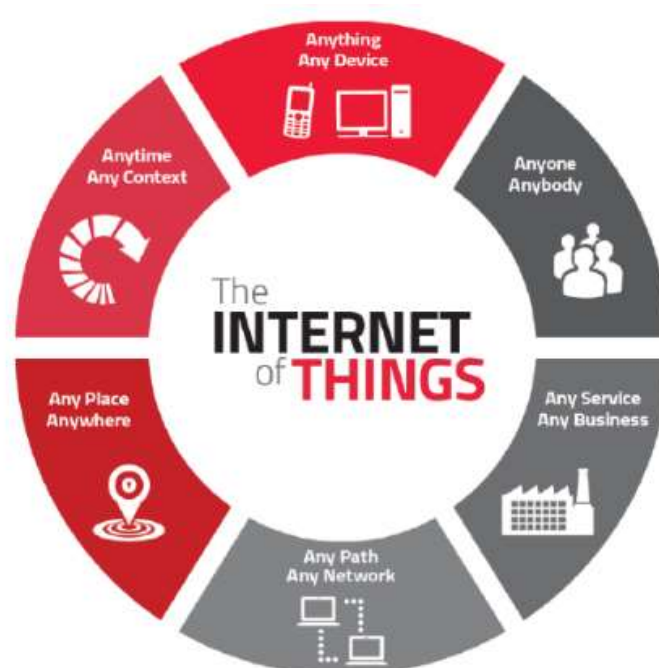


Figure 1 - Pictorial representation of IoT

(S Patel, 2016)

Increasing prominence and relevance is very much a result of recent progress in the development of enabling technologies, helping industry to achieve digital transformation, including development of IPv6; rise of cloud capabilities, essential for the increasing amount of data handled from assets (machines, production/resource, supply chain); and miniaturization of technology, enabling advanced communication technology to be

integrated into small devices and promote further development of sensors (Internet Society, 2015). However, IoT cannot be considered as an individual organisation, requiring integration of both software and hardware, with a variety of subsystems and technology; device sensors, networking/communication infrastructure, tools for data retrieval, analysis & storage to name a few. Development of these enabling technologies is key to IoT success, allowing devices/things to be connected anytime, anywhere and function in an ever-changing environment (Hadzialic, 2018).



Figure 2 - Pictorial representation of IoT Enabling Technology

(S Patel, 2016)

Enabling Technology/Protocol	
RFID & NFC (Near-field communication)	Used to identify & track IoT devices. Allows short-distance information exchange using radio signals. Simple & low energy Can be active or passive RFID tags
Low-energy Bluetooth (BLE)	Supports low power, prolonged use Uses standard technology
IPv6 Low-energy Wireless (6LoWPAN)	Overcomes the power consuming wireless technology and enables extended life of the device Interconnect sensors and monitor industrial environment IPv6 (128bit) preferential choice for IoT over IPv4 (32-bit)
Radio Protocols	Low-rate private network Low power with high throughput which ↑smaller local device networks at lower cost e.g. ZigBee, Z-Wave & Thread Data rate (250KB/s) lower than BLE (270KB/s)
LTE-A	↑coverage, ↓latency & ↑throughput compared to standard LTE Useful in vehicle communication due to high range
Wi-Fi Direct	No access point needed or network element with no loss of speed or throughput
Cloud Computing	Offers unlimited storage & powerful processing

Table 1 - Some IoT Enabling Technologies & Protocols

(April, 2016) (Harbi Y, 2019) (Gupta, 2021)

Enabling technology must have the functionality to build intelligence into the physical devices/things, enabling them to:

- obtain background information
- process the information

whilst containing the technology to provide effective privacy and security. (S Patel, 2016)

To add to the complexity, as IoT expands there is an increasing heterogenous mix of technology involved in communication which require adaptation (Hadzialic, 2018), forming one of the many challenges facing IoT. Some key characteristics of IoT are summarised below:

Essential IoT Characteristic	Explanation
Interconnectivity	Principle that any object or 'thing' can be inter-connected using the IoT infrastructure
Things-Related Services (TRS)	Current constraints such as protection for privacy and consistent semantics between the physical and virtual things limit IoT's capabilities for TRS, however technology can change to address this
Heterogeneity	As many devices used in IoT operate on a variety of hardware and network, multiple heterogeneous (diverse) devices and service platforms must be able to interact (interoperability)
Dynamic changes	Device number, state (connection vs disconnection, 'awake' vs 'asleep') and context (location/speed) can actively shift
Enormous scale	Exponential increase in devices communicating compared to that currently connected
Safety	Data management and safety must be built into the design to protect privacy and health. Data transition across networks must be secured (e.g. endpoints) and this must be scalable and act across all 'layers'
Connectivity	Networks must be accessible (i.e. devices can get on) and compatible (i.e. data can be consumed and produced)

Table 2 - Key IoT Characteristics

(S Patel, 2016)

Enabling technologies are viewed or described in several ways in the literature. They can be seen as functional blocks formed of a four-layer domain (the architecture of IoT) (Hadzialic, 2018), each functional block aiding various aspects of the system e.g. sensor interaction, input/output, management of storage, communication. It is much more complex than previously depicted in M2M communication (Zymbler, 2019).

Layer / Domain	Enabling Technology & Functionality	Additional Requirements
Perception / Sensor / Object (lowest layer)	Hardware platform; embedded object; mechanical/electrical part Sensor integrated into object to provide physical/virtual connection & allow collection/processing of information Able to measure physical property & possibly store limited quantity of measurements. Can be converted into signal for interpretation by an instrument.	May need connection to sensor gateway e.g., LAN (Wi-Fi/Ethernet), PAN (ZigBee/BT) May connect via WAN, WSNs (lower power/data rate connections improving battery life)
Network / Gateway	Communication protocols; network interface; adaption mechanism Reliable high performing network infrastructure needed to transport data gathered from previous layer. Hardware/software & technology/protocols allow communication between objects, and objects and global interface. Seamless connectivity, data transfer Public/private - able to meet various needs e.g. bandwidth & security (fig. below = examples of gateways and networks)	Need to serve increasing range of IoT applications with higher performance demands e.g., speed and context
Middleware / Management	Cloud platform; data processing mechanism; data storage Information processing. Process modelling: uses rule engines (supporting decision logic/interaction & automation for response) to filter/route to post-processing organisations/offer immediate response e.g. health Analytics: extraction of information, separating relevant from raw data. Data management: manage flow, access, integration & control of information. Filtering: anonymise, integrate & synchronise data → only that essential. Security: essential across all layers → prevent hacking/compromise from unauthorised access	In-memory analytical tools: RAM to cache data volume & hastens decision-making process Streaming-analytical tools: decisions on real-time data → immediate response
Application	IoT application architecture; software, APIs Details 'Smart' endpoint e.g. home, health, industry, trade etc. Visualisation, system & deviation monitoring, data & service management.	

Table 3 - IoT Enabling Technology & Functional Blocks

(S Patel, 2016) (Hadzialic, 2018)

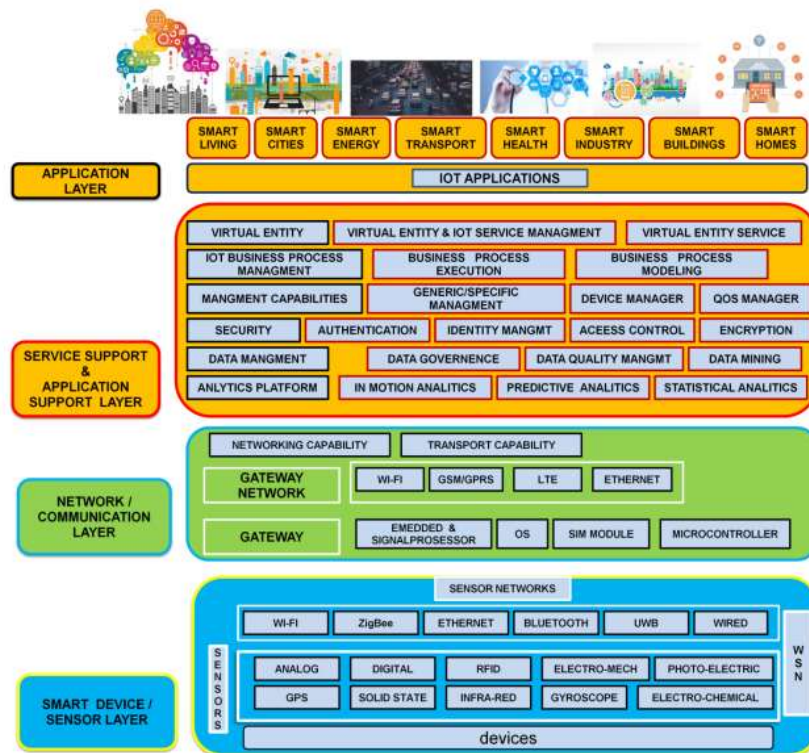


Figure 3 - IoT Architecture

(S Patel, 2016)

In addition to functional blocks, IoT technology involved can also be classified, falling under one of three groups:

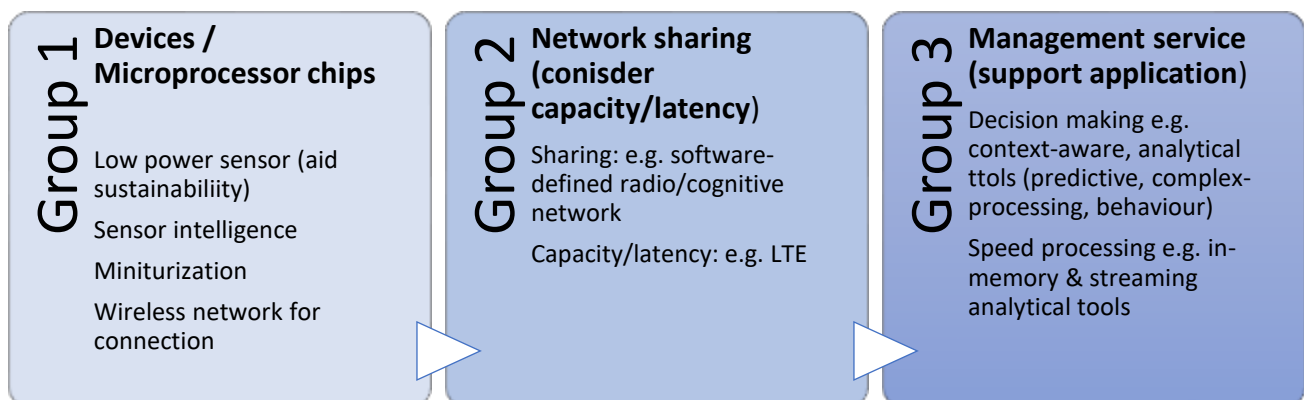


Figure 4 - IoT Technology Classification

(S Patel, 2016)

The downside of IoT incorporating such a raft of technologies is embedding the various domains into IP architecture requires advances in several technologies. When considering that involved; sensor and identification technology, hardware and software, algorithms for interpretation and analysis, cloud platforms for data storage, energy and power requirements, and security needs to name a few, the complexity of successfully integrating these systems can be understood.

Similarly, handling of such large amounts of data has limited IoT expansion. Significant developments in cloud platforms have provided an efficient solution, enabling a notable drive, able to support the vast amount of technology operating on the platform, along with data handling, monitoring, analysis and storage (Internet Society, 2015). Software-defined and secure-sensor networking e.g. Tinysec and Zigbee are two examples frequently used to provide the level of data privacy, protection and authorisation of IoT systems; a significant challenge of IoT (see below) (Zymbler, 2019).

Despite its complexity, ultimately the very backbone of IoT revolves around connection of devices/sensors to the internet. However, the variety of technology, brings the need for a number of communication, or connectivity models used (April, 2016). With this in mind, in 2015, the International Architecture Board outlined four of the most common models used to connect smart IoT objects/things to the internet, namely; Device-to-Device, Device-to-Cloud, Device-to-Gateway, and Back-End Data Sharing (Internet Society, 2015).

Device-to-Device is most frequently seen in ‘smart-homes’ e.g. lights, thermostats, where there is transfer of small amounts of data/information at a low-data rate. It refers to direct connection of two or more devices/things, communicating with one another over a network, most commonly using Bluetooth, ZigBee or T-wave protocols (April, 2016).



Figure 5 - Device-to-Device Model

(Internet Society, 2015)

The downside is the need for device specific data models, leading to development challenges and the need to use devices employing the same protocols. This however, brings reliable communication (Internet Society, 2015). Sustainability of batteries is also an issue; however this is being addressed with the development of BLE standards which enables single batteries to operate for prolonged periods due the low power usage. Smart watches utilise this communication model as there is often no need to share the data with multiple users. The main advantage of device-to-device model is one-to-one or short-range connection, meaning devices are less open to security concerns, as security is simplified (April, 2016).

Comparatively, Device-to-Cloud connected devices suffer from significant security issues, allowing easy access for hackers to sensitive information. In this model data exchange and message traffic are controlled by an application service provider, with devices connected directly to an internet-cloud service allowing remote access to the device for the application (April, 2016).

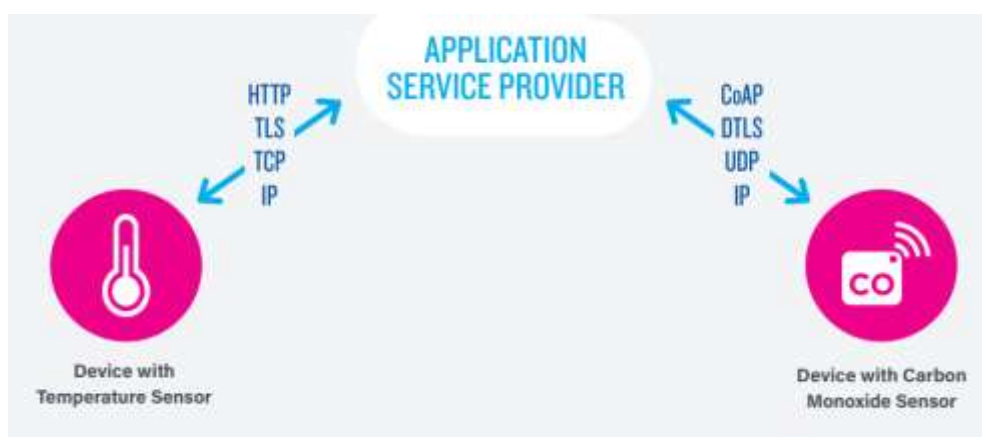


Figure 6 - Device-to-Cloud Model

(Internet Society, 2015)

These models predominantly use Ethernet or Wi-Fi connections, though cellular can be used. Such a model is used by ‘smart-tags’ and some Nest® labs (analyse home energy consumption), having the benefits of being able to remotely send software updates to the device, and allowing access when the user is away as the model uses wide-area or remote monitoring (April, 2016). Unlike Device-to-Device connectivity, this model is plagued with interoperability issues, users often committed to single vendor’s device and cloud service. However, as with Device-to-Device this offers reliability (Internet Society, 2015).

To address interoperability and possibly security issues seen above, Device-to-Gateway communication can be used, allowing communication between devices using differing standards, and increased security measures. In comparison to Device-to-Cloud, connection to the cloud service is via an intermediary device e.g. smartphone, using application software that pairs with the device and also communicates to the cloud service (April, 2016).

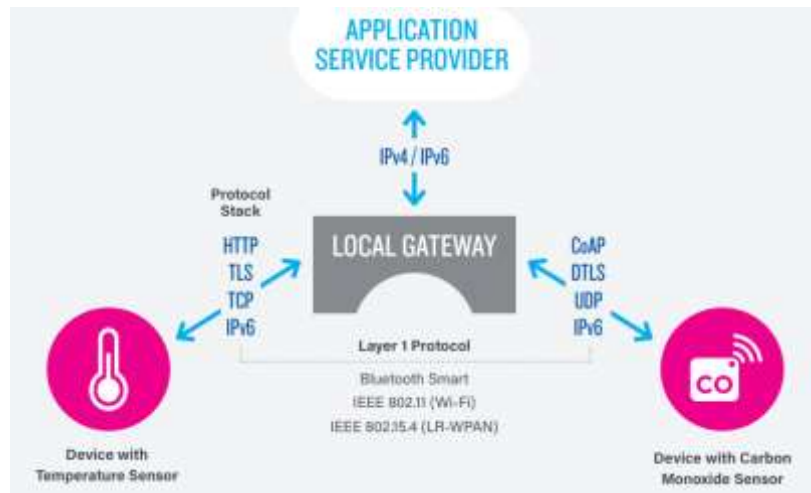


Figure 7 - Device-to-Gateway Model

(Internet Society, 2015)

Unlike Device-to-Device, it is possible to provide functions such as translation of data protocols, seen with fitness trackers and home automation where a ‘Smart-hub’ acts as a local gateway able to communicate between different protocols such as Zig-Bee and Z-Wave. It is useful therefore for integration of legacy systems and new smart devices which otherwise would not be interoperable e.g. bridging the gap between Industry (IoT) 4.0 & legacy systems/machines. However, this model attracts additional costs (Internet Society, 2015).

The final model, Back-End-Data-Sharing, is an extension to Device-to-Cloud, allowing access of the device and sensor data to third parties (authorised only) (April, 2016).

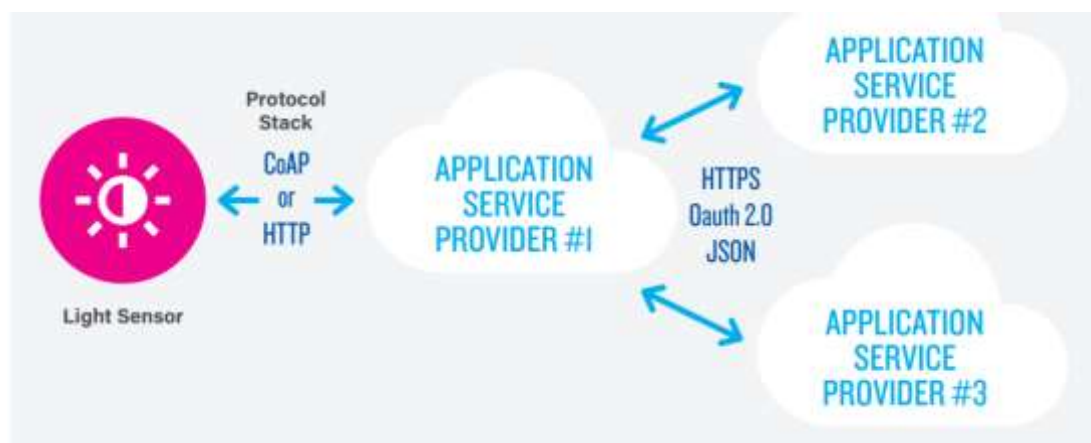


Figure 8 - Back-End Data Sharing Model

(Internet Society, 2015)

The third party can, in conjunction with other data from various devices, access exported and analysed device data from the cloud service, which can be combined and further analysed by another service e.g. MapMyFitness application (April, 2016).

As it can be seen with the evolving technology, IoT is creating a world where everything is connected, allowing integration of several differing standards and technologies which incorporate a variety of sensors, connections, storage and other capabilities. Although there are many challenges at present, IoT is still envisaged as the next big innovation. However, as the development of IoT continues and the transformational potential realised, the implications for humans and industry need to be considered e.g. security, health, environmental impact, energy usage and safety. The days where engagement with such technology was more of an active role (Internet Society, 2015) e.g. downloading/generating content, have progressed, and as the required architectures and enabling technologies are met, more services and applications will be able to utilise the technology, leading to a population of passive engagement, devices/machines sending/receiving data without human intervention or knowledge (Hadzialic, 2018).

Although still in its embryonic stage, there is a significant drive to promote and progress IoT, evident by the significant increase in press coverage. As technology develops, so do opportunities which are increasingly vast and diverse; IoT beginning to integrate into almost all areas of the everyday, signifying a notable transformation in the way life operates. Rapid development in technologies have added significant drive for unlocking IoT potential, progression of Web3.0 offering seamless connectivity, the number of IoT device types and contexts rising (Hadzialic, 2018). Several established drivers which have taken IoT to a new level are shown below:

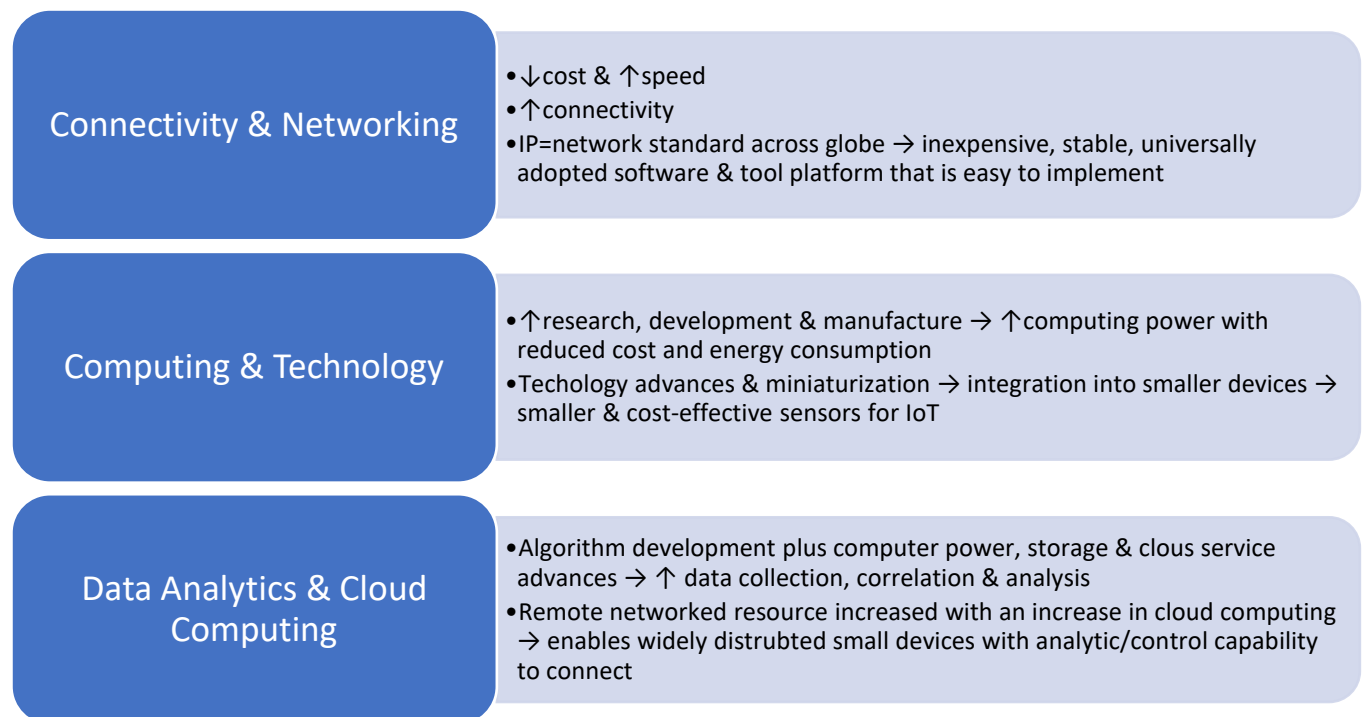


Figure 9 - Drivers for IoT
(Internet Society, 2015)

Smart environments are key to industry 4.0 revolution, the value of IoT for ‘smart-factories’ seen in management of supply chains, predictive maintenance (self-monitoring/diagnosing), and tracking of assets, with cost/efficiency savings, transparency and energy-efficiency a few of the predicted benefits (Epicor, 2022). Similar environments are also evolving in homes, transport, healthcare, retail, energy and the environment. However, with any of these there remains concerns over environmental impact and sustainability (Hamza, 2021). Below details examples of current and potential applications/benefits of IoT:

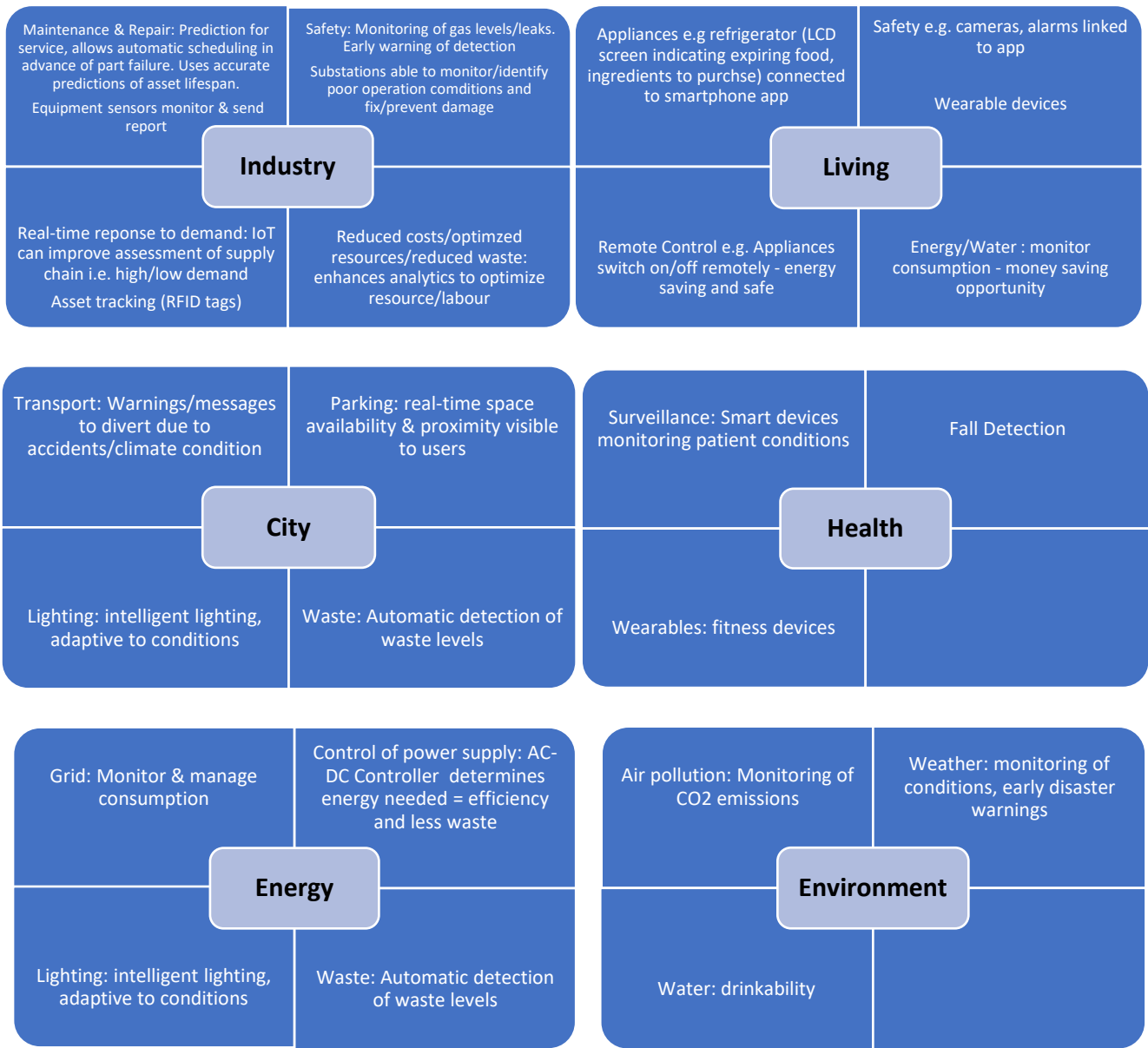


Figure 10 - IoT Opportunities
(Kadry, 2021) (Zymbler, 2019) (Hamza, 2021)

The decision tree around integration and connectivity to the internet for IoT devices is complex. As newer industry technology is developed to address needs of lower energy consumption, size and cost, there comes the caveat that there is a lack of maturity/evolution resulting in a compromise of security and privacy (Afzal et al, 2021). These challenges raise concerns as use grows. There needs to therefore be an attitude of continuous improvement to meet these challenges, some of which are highlighted below:

Security & Privacy	•See below
Cost vs Useability	•Component costs need to reduce in order enable global expansion
Interoperability	•Ability for different devices/systems to swap information •Integration requires communication between the physical & virtual world. •Interoperability = ≥ 2 systems/components able to exchange data & utilise information •Heterogenicity of devices and communication technologies, and interoperability between various layers remains a challenge for global expansion; Proprietary vs User Choice; Clock-ins vs limiting •Consideration of technical, syntactical, semantic and organizational interoperability. Issues with fragmentation of standards & variation of technology •Stabilization is key
Data Management & Traffic Load	•Handling of the data volume & processes involved are critical •$\uparrow$ number of devices $\rightarrow \uparrow$ traffic •Cloud technology needed to meet these requirements
Energy Issues / Environment	•Communication process involves significant energy consumption. •In order to be accepted and sustainable, energy consumption must be minimised •+ve impact = opportunity to develop systems to increase environmental sustainability
Legal /Regulatory Rights	•Data protection

Figure 11 - Examples of Challenges Facing IoT

(Internet Society, 2015) (S Patel, 2016) (Hadzialic, 2018)

However, with the internet known for security and cyber-attack threats, data/information gathered and held as part of IoT is vulnerable and at risk from hackers. Security and privacy arguably present the most significant challenge to expansion (Afzal et al, 2021). Although intended to facilitate everyday life, IoT can result in significant risk to its quality, privacy and security if introduced and used inappropriately e.g. interception of a baby monitor compromising privacy. With IoT utilising many enabling technologies as described in table 1, it follows that each

security flaw can be inherited. Creating a secure path for communication is a key challenge, traditional complex mechanisms impractical for increasingly smaller IoT devices (Harbi Y, 2019). As a result, there has been a focus on security and privacy research, recommendations for a standard framework able meet global needs of all users, furthermore, stating any organization using IoT must ensure that various protective measures are in place such as authentication, access control, protection from attacks etc. (Zymbler, 2019). Testing and protection mechanisms are essential to successful implementation (Afzal et al, 2021). Further research identified issues with systems using IP, identifying IoT can involve third parties and security protocols, and that architecture must be scalable as the scale of IoT applications varies. The complex architecture of IoT opens up a number of other potential security issues; end-to-end security protocols needing to also cover gateway translations, and security for all layers needing to be addressed (Zymbler, 2019), focusing efforts on a single layer only likely to open up vulnerabilities in the rest of the system. Encryption is required at any level of data transfer (Harbi Y, 2019).

Many types of security threats to IoT devices exist including attacks on/with nodes, sinkholes, wormholes, codes, sleep modes, RFIDs and malicious software, ultimately with one of three aims (Harbi Y, 2019):

- Providing access to sensitive/private data
- Taking control of communication
- Causing damage to the device & impact service accessibility



Figure 12 - IoT Security/Privacy Threats

(Afzal et al, 2021) (Kadry, 2021)

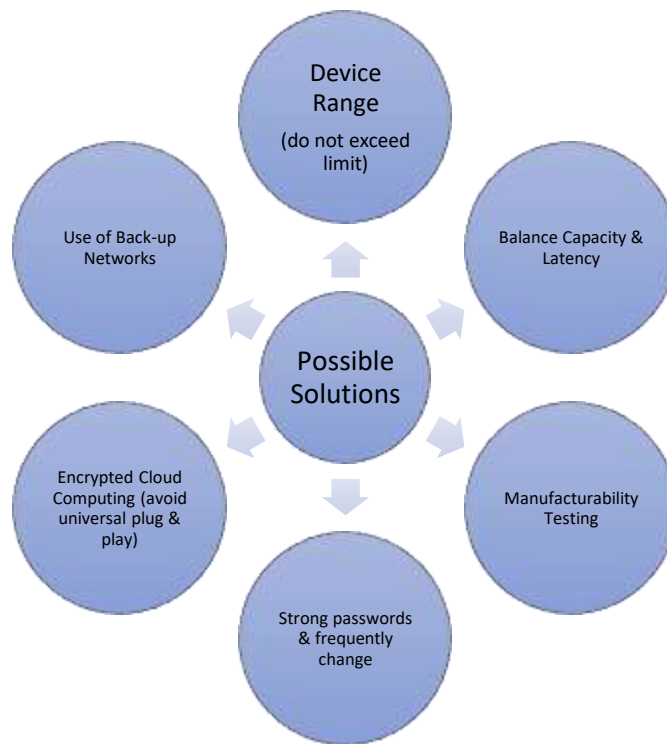


Figure 13 - Possible IoT Security Solutions

(Afzal et al, 2021)

Vulnerability of IoT devices can be due to several reasons. Firstly, private data is rarely protected and often sent unencrypted meaning it is open to interception. Secondly with the increasing market, there is notable pressure on manufacturers to make the device available, resulting in critically insecure software; security development and testing is rushed. Insecure software often deploys unencrypted updates which again can be intercepted and corrupted. Many devices do not force users to employ ‘strong’ passwords i.e. have inadequate authorisation protection, leaving access open to attack. This is further of concern where users share passwords across devices. Finally, security holes can often be found in devices where user interface is inadequately coded (Afzal et al, 2021). There are many examples of IoT devices that have, as a result of poorly designed security and privacy protection, been attacked. Benefits of incorporation of IoT in healthcare has been previously described, however consequences of these devices lacking security are significant. Reports of smart medical devices such as insulin pumps, and implantable defibrillators employing out-of-date software and a lack of data encryption has led to a breach of patient confidentiality and more importantly put patients’ health at risk e.g. St Jude’s medical implantable cardiac device (see below) (Larson, 2017). This vulnerability, formally reported by the FDA, was of such concern that subsequently they published official guidance ‘Postmarket Management of Cybersecurity in Medical Devices’ (FDA, 2016). A more recent contentious IoT device is the AirTag®, marketed as a device to solve the widespread problem of loss of possessions. The device operates on a Device-to-Cloud platform (Raymone, 2022).

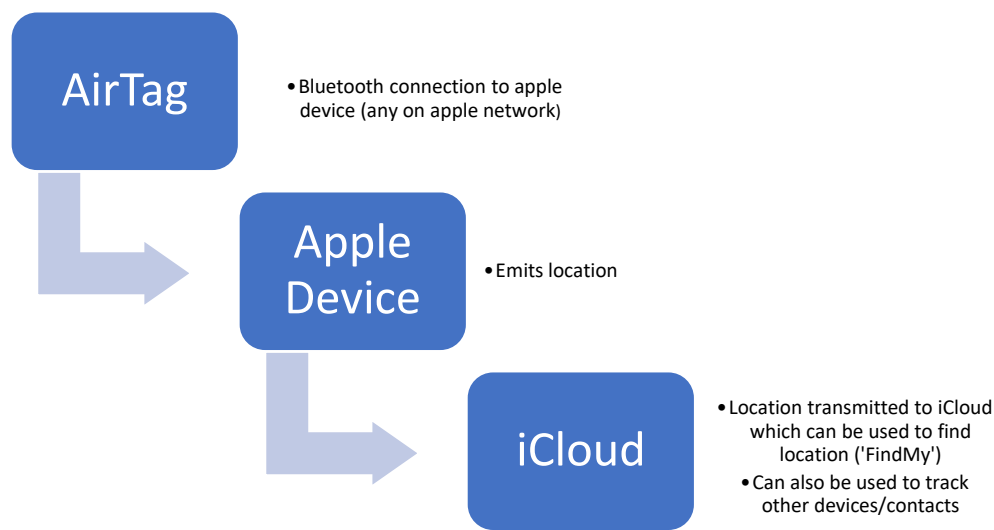


Figure 14 - AirTag® Communication Model

(Raymone, 2022)

This model is known for security concerns (see above), and in fact was identified by security experts as a possible physical Trojan horse, hackers able to access and manipulate the device when in lost-mode (Kerbs, 2021). Not only this, but there are serious privacy issues, as it can easily be used as a tracking device, a particular concern given the extent of the Apple network (Bandara, 2021).

Below lists examples of security/privacy breaches reported with IoT:

Device	Details
Internet Service Provider 'Mirai Bonet attack'	Largest known attack on Dyn → widespread loss of internet service Following infection with Mirai malware it can search for vulnerability in other IoT devices, log in and further infect
St Judes Medical Implantable Cardiac Device	Vulnerability = transmitter responsible for reading data and remotely sharing to medical team. Control achieved by hacking transmitter. Control could enable battery depletion or administration of shocks, altering of packing i.e. serious risk to health.
TrendNet Security Cameras	Software fault that allowed access to any individual that had the IP address of the camera Login details of users were clear and readable on the internet & and when stored on the mobile application. Breached basic security measures of preventing hacking by securing IP addresses and encrypting/password protecting user logins

Table 4 - Examples of Published Security/Privacy Breaches Involving IoT

(Larson, 2017) (Dunlap, 2020)

With the number of devices and data handled rising, and the size of IoT technology decreasing, new effective solutions and standardized protocols for security and privacy are needed. In addition, there should be a drive towards autonomous detection and recovery (Harbi Y, 2019).

4. Research Summary

IoT is the key to Industry 4.0, M2M and creation of 'smart-factories'; the Industrial IoT. It is however much more than simply smart manufacturing, offering resource improvement, cost-reduction, better product control, real-time problem identification/response to issues in production/supply-chain. Although there is significant drive for development and progression to achieve global utilization, ultimately it is still in its infancy, with several challenges facing it. As IoT at its core is communication of technology, interoperability is one key challenge, requiring integration of differing standards, which are currently fragmented and diverse. Despite the drive to standardize, correlating framework incorporating defined standards is still lacking. However, advances in enabling technology such as component miniaturization, IP networking, Web3.0 and cloud platforms/services have enabled significant advances to be made. Key requirements of the architecture are a scalable, interoperable, open and modular design to meet the heterogeneous challenge facing IoT.

Ultimately IoT is progressing at an exponential rate, press coverage increasing due the wide potential for use and incorporation. A focus must however be placed on the security and privacy issues facing it, as despite its potential, technology is not yet fully developed and importantly not secure. With vulnerability of access, and large amounts of data available, these need to be addressed as a priority and are critical to development.

Development of enabling technologies continue to advance and promote a more cost-effective, global option. As new devices and opportunities and applications develop, further research challenges will continue to promote a continuously improving concept.

5. Methodology, Testing & Results for Arduino IOT

An IoT enabled Weather Monitoring Station using Arduino OPLA kit was designed, built and tested.

Arduino OPLA Kit Hardware	Key features
MKR IoT Carrier	OLED colour display 5 capacitive touch buttons for screen navigation On-board sensors: Temperature, humidity, pressure, light 24V relays
MKR WiFi 1010 Board	Control system Bluetooth & WiFi enabled ATECC508 crypto-chip: security of data transfer

Table 5 - IoT Arduino Kit

(Arduino, 2022)

Once the board and carrier were assembled, (see appendix 8), a USB cable was used to connect the ‘1010’ board to the Arduino IoT Cloud web page. Following import of the weather station template, the Arduino Cloud was created to configure the board as ‘IoT ready’, configuration of the device and network accessed through the ‘things’ menu. Shown in the image below are the five declared template variables (and associated data types); temperature, humidity, light, pressure and weather report, their permissions and updates adjusted to allow a two-minute refresh cycle.

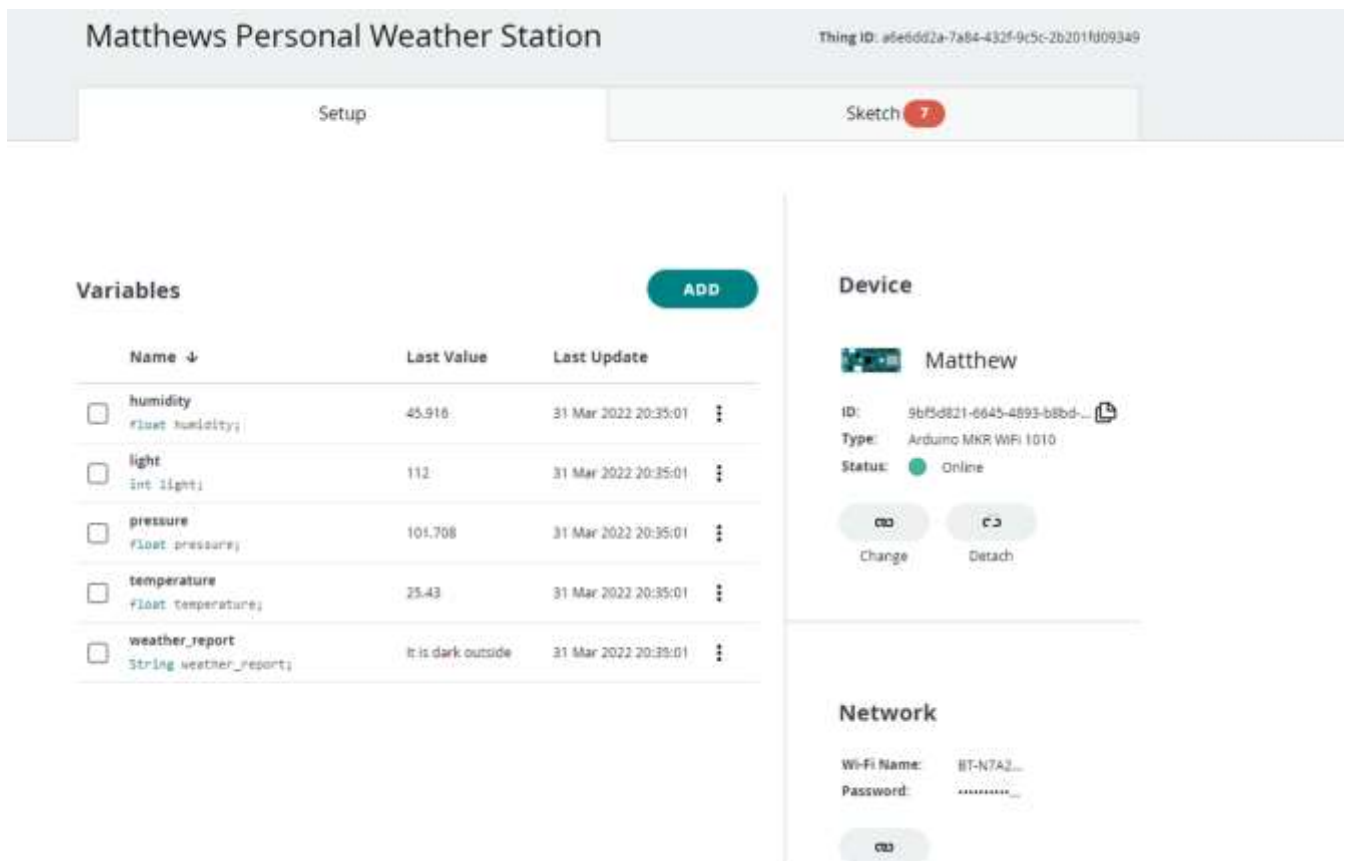


Figure 15 - Personal Weather Station

The generated system code, shown in appendix 8, was imported with the weather station template above. Using the sketch tab, further development of the code was made for display enhancements. Within the code, is the inclusion of ‘thing properties’ and carrier board. ‘Void setup’ and ‘Void Loop’ form the main sections of the code, in which there is control of variable data and serial monitor directions:

- Void setup: single implementation when the sequence begins; permitted for single functions e.g. connection of the serial monitor or cloud.
- Void loop: in continual ‘loop’ while there is connection of the board.

‘Dashboard’ design and execution follows (see appendix 8 for design and data trends); enabling visualisation of the variable data using the IoT Cloud interface. Real-time data can be viewed for each variable, which are also given individual widgets. The dashboard can also display up to fifteen days worth of cloud stored data for weather and humidity, enabling trending. A weather report can be generated, depending on variable condition, using ‘if’/‘elseif’ clauses.

Upload to the 1010 board of the finalised code and dashboard was completed, the image below showing proof of concept; visualisation of real-time variable data measured by carrier sensors.



Figure 16 - Weather Station Carrier Results

Illustrated below is the real-time dashboard data and trend graph. Minor discrepancies in real-time values compared to that displayed by the carrier can be attributed to the timing of operator manual reads and the frequency with which the carrier data values change/refresh. The trended data displaying stored data from earlier readings (over a 60min interval period), proves the IoT communication model, showing integration with the IoT Cloud.

The IoT device also has the ability to display the recorded data, real-time, on either the computer or mobile dashboard, providing IoT anywhere, anytime access, providing correct login credentials are used.

Matthew's IoT Weather Station

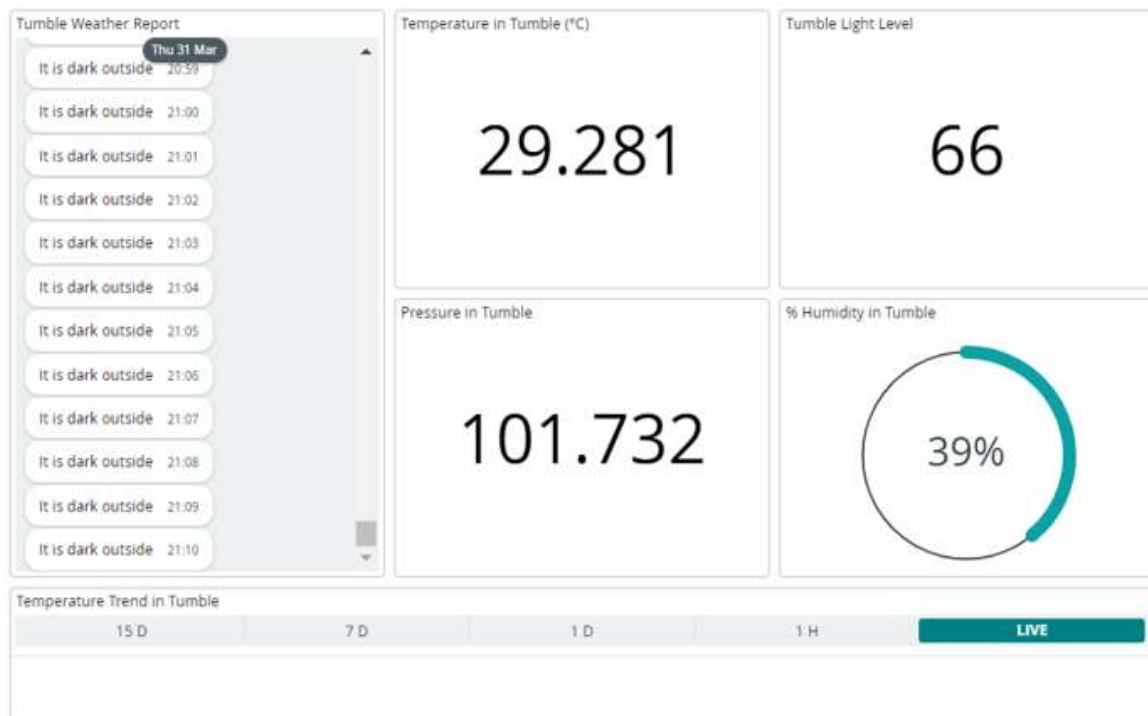


Figure 17 - Weather Station Dashboard



Figure 18 - Weather Station Data Trend

6. Conclusions & Recommendations

IoT has existed in various guises for several decades, however as advances in enabling technology has increased the number, and evolution of smaller sensors, the drive to create smart environments to facilitate and revolutionise everyday living gains momentum.

Research into IoT provided a degree of insight and knowledge on the topic, which could then be used to inform and guide part two of the project. As well as covering the four key concepts; IoT definitions, Enabling Technologies, Connectivity Models and Transformational Potential, key opportunities and challenges facing its implementation were also established.

Part two, using the Arduino Weather Monitoring System, successfully demonstrated the core principle of IoT, ability to connect sensors/devices to the internet, to generate, collate, analyse and store data on environmental conditions, namely humidity, light, pressure and temperature.

Using the Device-to-Cloud communication model, the data from the newly constructed sensor module was successfully uploaded to the configured Arduino Cloud, the Arduino Dashboard enabling visualisation and control of the system anywhere at anytime, demonstrating another IoT principle frequently reported in the research. Although IoT is depicted as available to ‘anyone’, access was restricted with unique log-ins, providing a necessary level of security to the system and data, a topic that challenges IoT expansion. Although not demonstrated in the project, with Device-to-Cloud communication known for security issues, Arduino also incorporates a crypto-chip for secure data transfer.

Though a success, the Arduino Weather Monitoring System functioning as designed, there were issues during project execution which required the support of colleagues, as the device failed to pair i.e. communicate with the computer software. This demonstrated how key seamless connectivity and ubiquitous networking is to the operation and implementation of IoT, without this the technology is of no use.

Should further work be permitted, it is possible to further extend the Arduino project through incorporation of a LoRa gateway which would offer the opportunity to explore a different IoT communication model; the Device-to-Gateway (Bagur J, 2022).

7. References

- Afzal et al, 2021. www.ijser.org. [Online]
Available at: <https://www.ijser.org/researchpaper/Internet-of-Things-IoT-Security-Issues-Challenges-and-Solutions.pdf>
[Accessed 17 03 2022].
- April, C., 2016. www.channelfutures.com. [Online]
Available at: <https://www.channelfutures.com/best-practices/the-four-internet-of-things-connectivity-models-explained>
[Accessed 19 03 2022].
- Arduino, 2022. www.arduino.com. [Online]
Available at: <https://opla.arduino.cc/>
[Accessed 12 03 2022].
- Bagur J, C. T., 2022. www.docs.arduino.. [Online]
Available at: <https://docs.arduino.cc/learn/communication/lorawan-101>
[Accessed 15 04 2022].
- Bandara, A., 2021. www.bit.com.au. [Online]
Available at: <https://www.bit.com.au/guide/the-dangers-of-apple-airtags-and-how-to-ensure-you-are-not-being-tracked-565860>
[Accessed 27 03 2022].
- Dunlap, T., 2020. www.iotforall.com. [Online]
Available at: <https://www.iotforall.com/5-worst-iot-hacking-vulnerabilities>
[Accessed 17 03 2022].
- Epicor, 2022. www.epicor.com/. [Online]
Available at: <https://www.epicor.com/en/blog/learn/what-is-industry-4-0/>
[Accessed 01 04 2022].
- FDA, 2016. www.fda.gov. [Online]
Available at: <https://www.fda.gov/regulatory-information/search-fda-guidance-documents/postmarket-management-cybersecurity-medical-devices>
[Accessed 19 03 2022].
- fleisch, E., 2010. www.researchgate.net. [Online]
Available at:
https://www.researchgate.net/publication/46016701_What_is_the_Internet_of_Things_An_Economic_Perspective
[Accessed 15 03 2022].
- GSMA, 2014. [Online]
Available at: [cl_iot_wp_07_14.pdf \(gsma.com\)](#)
[Accessed 14 03 2022].
- Gupta, S. K. & G., 2021. www.sciencedirect.com. [Online]
Available at: <https://www.sciencedirect.com/science/article/pii/S2214785321051221?via%3Dihub>
[Accessed 22 03 2022].

- Hadzialic, A. C. & M., 2018. www.researchgate.net. [Online]
Available at: https://www.researchgate.net/publication/326539025_Internet_of_Things_IoT_A_Review_of_Enabling_Technologies_Challenges_and_Open_Research_Issues
[Accessed 21 03 2022].
- Hamza, M., 2021. www.smarthometrends.net/. [Online]
Available at: <https://smarthometrends.net/2021/06/28/a-beginners-guide-to-the-internet-of-things-iot-2021/>
[Accessed 30 03 2022].
- Harbi Y, A. Z. H. S. B. A. R. A., 2019. www.link.springer.com. [Online]
Available at: <https://link.springer.com/article/10.1007/s11277-019-06405-y?noAccess=true>
[Accessed 22 03 2022].
- Internet Society, 2015. www.internetsociety.org. [Online]
Available at: [ISOC-IoT-Overview-20151221-en.pdf](https://www.internetsociety.org/publications/ISOC-IoT-Overview-20151221-en.pdf) ([internetsociety.org](http://www.internetsociety.org))
[Accessed 14 04 2022].
- Kadry, L. R. & S., 2021. www.researchgate.net. [Online]
Available at: https://www.researchgate.net/publication/351554927_Internet_of_things_IoT
[Accessed 14 03 2022].
- Kerbs, 2021. krebsonsecurity.com. [Online]
Available at: <https://krebsonsecurity.com/2021/09/apple-airtag-bug-enables-good-samaritan-attack/>
[Accessed 14 03 2022].
- Larson, S., 2017. www.money.cnn.com. [Online]
Available at: <https://money.cnn.com/2017/01/09/technology/fda-st-jude-cardiac-hack/index.html>
[Accessed 06 03 2022].
- Raymone, A., 2022. www.cnet.com. [Online]
Available at: <https://www.cnet.com/news/privacy/apple-airtags-how-to-protect-yourself-from-being-tracked/>
[Accessed 30 03 2022].
- S Patel, C. S., 2016. www.researchgate.net. [Online]
Available at: https://www.researchgate.net/publication/330425585_Internet_of_Things-IOT_Definition_Characteristics_Architecture_Enabling_Technologies_Application_Future_Challenges
[Accessed 21 03 2022].
- Zymbler, S. K. & P. T. & M., 2019. www.journalofbigdata.springeropen.com. [Online]
Available at: <https://journalofbigdata.springeropen.com/articles/10.1186/s40537-019-0268-2>
[Accessed 16 03 2022].

8. Bibliography

Integrating M2M Communications across Industries | TE Connectivity (2022)

Internet of Things (IoT) Tutorial (tutorialspoint.com) (2022)

9. Appendix

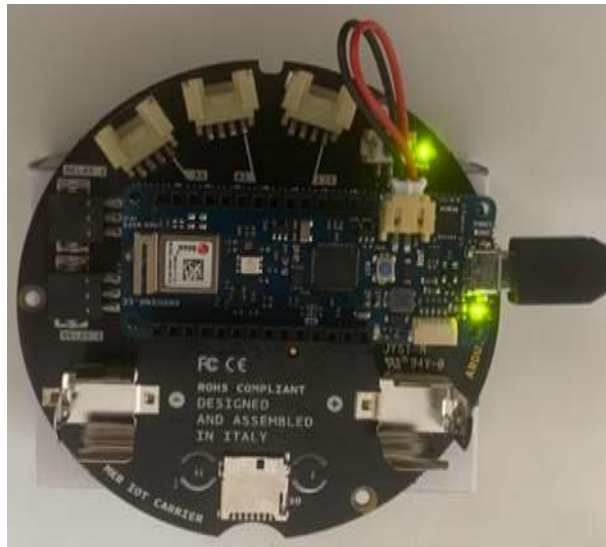


Figure 19 - Arduino 1010 Board

```
1  /*
2   Sketch generated by the Arduino IoT Cloud Thing "Untitled"
3   https://create.arduino.cc/cloud/things/151ec4be-5c5f-47b2-9225-e383f05732e5
4
5   Arduino IoT Cloud Variables description
6
7   The following variables are automatically generated and updated when changes are made to the Thing
8
9   String weather_report;
10  float humidity;
11  float pressure;
12  float temperature;
13  int light;
14
15  Variables which are marked as READ/WRITE in the Cloud Thing will also have functions
16  which are called when their values are changed from the Dashboard.
17  These functions are generated with the Thing and added at the end of this sketch.
18  */
19
20  #include "thingProperties.h"
21  #include <Arduino_MKRIoTCarrier.h>
22  MKRIoTCarrier carrier;
23
24  int modeSelect = 0;
25  int previousMode = 0;
26  int refreshCount = 0;
27
28  void setup() {
29    // Initialize serial and wait for port to open:
30    Serial.begin(9600);
31    //while (!Serial);
32
33    // Defined in thingProperties.h
34    initProperties();
35
36    // Connect to Arduino IoT Cloud
37    ArduinoCloud.begin(ArduinoIoTPreferredConnection);
```

```

38 //Get Cloud Info/errors , 0 (only errors) up to 4
39 setDebugMessageLevel(2);
40 ArduinoCloud.printDebugInfo();
41
42 //Wait to get cloud connection to init the carrier
43 while (ArduinoCloud.connected() != 1) {
44     ArduinoCloud.update();
45     delay(500);
46 }
47 delay(500);
48 CARRIER_CASE = true;
49 carrier.begin();
50 carrier.display.setRotation(0);
51 carrier.display.fillScreen(ST77XX_BLACK);
52 carrier.display.setTextColor(ST77XX_WHITE);
53 carrier.display.setTextSize(3);
54
55 carrier.display.setCursor(60, 80);
56 carrier.display.print("Weather");
57 carrier.display.setCursor(60, 120);
58 carrier.display.print("Station");
59 delay(2000);
60 carrier.display.fillScreen(ST77XX_BLACK);
61 carrier.display.setTextColor(ST77XX_WHITE);
62 carrier.display.setTextSize(2);
63
64 carrier.display.setCursor(70, 80);
65 carrier.display.print("Connected");
66 carrier.display.setCursor(50, 110);
67 carrier.display.print("To IoT Cloud");
68 delay(2000);
69 }
70
71 void loop() {
72     ArduinoCloud.update();
73     carrier.Buttons.update();
74 }

```

```

38 //Get Cloud Info/errors , 0 (only errors) up to 4
39 setDebugMessageLevel(2);
40 ArduinoCloud.printDebugInfo();
41
42 //Wait to get cloud connection to init the carrier
43 while (ArduinoCloud.connected() != 1) {
44     ArduinoCloud.update();
45     delay(500);
46 }
47 delay(500);
48 CARRIER_CASE = true;
49 carrier.begin();
50 carrier.display.setRotation(0);
51 carrier.display.fillScreen(ST77XX_BLACK);
52 carrier.display.setTextColor(ST77XX_WHITE);
53 carrier.display.setTextSize(3);
54
55 carrier.display.setCursor(60, 80);
56 carrier.display.print("Weather");
57 carrier.display.setCursor(60, 120);
58 carrier.display.print("Station");
59 delay(2000);
60 carrier.display.fillScreen(ST77XX_BLACK);
61 carrier.display.setTextColor(ST77XX_WHITE);
62 carrier.display.setTextSize(2);
63
64 carrier.display.setCursor(70, 80);
65 carrier.display.print("Connected");
66 carrier.display.setCursor(50, 110);
67 carrier.display.print("To IoT Cloud");
68 delay(2000);
69 }
70
71 void loop() {
72     ArduinoCloud.update();
73     carrier.Buttons.update();
74 }

```

```

75 • while(!carrier.Light.colorAvailable()) {
76     delay(5);
77 }
78 int none;
79 carrier.Light.readColor(none, none, none, light);
80
81 temperature = carrier.Env.readTemperature();
82 humidity = carrier.Env.readHumidity();
83 pressure = carrier.Pressure.readPressure();
84
85 • if(carrier.Button0.onTouchDown()) {
86     modeSelect = 0;
87 }
88 • else if(carrier.Button1.onTouchDown()) {
89     modeSelect = 1;
90 }
91 • else if(carrier.Button2.onTouchDown()) {
92     modeSelect = 2;
93 }
94 • else if(carrier.Button3.onTouchDown()) {
95     modeSelect = 3;
96 }
97 • else if(carrier.Button4.onTouchDown()) {
98     modeSelect = 4;
99 }
100
101 • if(modeSelect != previousMode) {
102     updateDisplay();
103     previousMode = modeSelect;
104     refreshCount = 0;
105 }
106 • else if (refreshCount >= 50) {
107     updateDisplay();
108     refreshCount = 0;
109 }
110
111 • if (humidity >= 60 && temperature >= 15) {
112     weather_report = "It is very humid outside";
113 }
114 • else if (temperature >= 25 && light >= 700) {
115     weather_report = "Hot and sunny outside";
116 }
117 • else if (light <= 100) {
118     weather_report = "It is dark outside";
119 }
120 • else if (temperature >= 15 && light >= 700) {
121     weather_report = "Warm and sunny outside";
122 }
123 • else if (temperature <= 16 && light >= 700) {
124     weather_report = "A little cold, but sunny outside";
125 }
126 • else if (humidity >= 90 && temperature <= 15) {
127     weather_report = "It is wet and rainy outside";
128 }
129     refreshCount++;
130 }
131
132 • void updateDisplay () {
133     if (modeSelect == 0) {
134         carrier.display.fillScreen(ST77XX_RED);
135         carrier.display.setTextColor(ST77XX_WHITE);
136         carrier.display.setTextSize(4);
137
138         carrier.display.setCursor(70, 50);
139         carrier.display.print("Temp:");
140         carrier.display.setCursor(40, 110);
141         carrier.display.print(temperature);
142         carrier.display.print(" C");
143     }
144 • else if (modeSelect == 1) {
145         carrier.display.fillScreen(ST77XX_BLUE);
146         carrier.display.setTextColor(ST77XX_WHITE);
147         carrier.display.setTextSize(4);
148

```

```

112     weather_report = "It is very humid outside";
113 }
114 else if (temperature >= 25 && light >= 700) {
115     weather_report = "Hot and sunny outside";
116 }
117 else if (light <= 100) {
118     weather_report = "It is dark outside";
119 }
120 else if (temperature >= 15 && light >= 700) {
121     weather_report = "Warm and sunny outside";
122 }
123 else if (temperature <= 16 && light >= 700) {
124     weather_report = "A little cold, but sunny outside";
125 }
126 else if (humidity >= 90 && temperature <= 15) {
127     weather_report = "It is wet and rainy outside";
128 }
129 refreshCount++;
130 }
131
132 void updateDisplay () {
133     if (modeSelect == 0) {
134         carrier.display.fillScreen(ST77XX_RED);
135         carrier.display.setTextColor(ST77XX_WHITE);
136         carrier.display.setTextSize(4);
137
138         carrier.display.setCursor(70, 50);
139         carrier.display.print("Temp:");
140         carrier.display.setCursor(40, 110);
141         carrier.display.print(temperature);
142         carrier.display.print(" C");
143     }
144     else if (modeSelect == 1) {
145         carrier.display.fillScreen(ST77XX_BLUE);
146         carrier.display.setTextColor(ST77XX_WHITE);
147         carrier.display.setTextSize(4);
148
149         carrier.display.setCursor(70, 50);
150         carrier.display.print("Humi:");
151         carrier.display.setCursor(40, 110);
152         carrier.display.print(humidity);
153         carrier.display.print(" %");
154     }
155     else if (modeSelect == 2) {
156         carrier.display.fillScreen(ST77XX_GREEN);
157         carrier.display.setTextColor(ST77XX_BLACK);
158         carrier.display.setTextSize(4);
159
160         carrier.display.setCursor(60, 60);
161         carrier.display.print("Light:");
162         carrier.display.setCursor(80, 120);
163         carrier.display.print(light);
164     }
165     else if (modeSelect == 3) {
166         carrier.display.fillScreen(ST77XX_CYAN);
167         carrier.display.setTextColor(ST77XX_BLACK);
168         carrier.display.setTextSize(4);
169
170         carrier.display.setCursor(60, 60);
171         carrier.display.print("Press:");
172         carrier.display.setCursor(20, 110);
173         carrier.display.print(pressure);
174         carrier.display.print(" Pa");
175     }
176     else {
177         carrier.display.fillScreen(ST77XX_BLACK);
178     }
179 }
180
181
182
183
184

```

Figure 20 - Arduino Weather Station Sketch Code

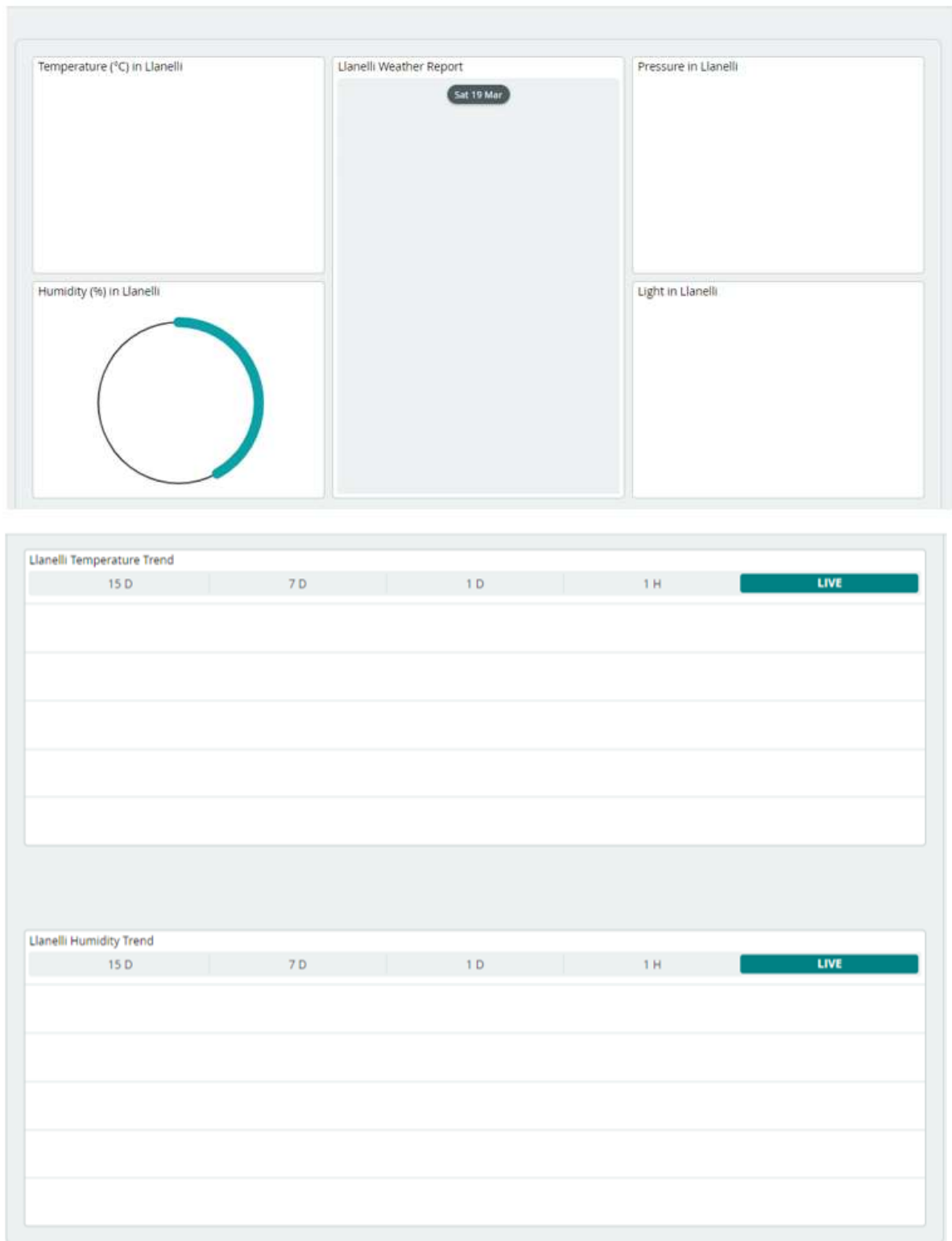


Figure 21 - Weather Station Dashboard Design

FINAL GRADE

GENERAL COMMENTS

Instructor

77 /100

PAGE 1

PAGE 2

PAGE 3

PAGE 4

PAGE 5

PAGE 6

PAGE 7

PAGE 8

PAGE 9

PAGE 10

PAGE 11

PAGE 12

PAGE 13

PAGE 14

PAGE 15

PAGE 16

PAGE 17

PAGE 18

PAGE 19

PAGE 20

PAGE 21

PAGE 22

PAGE 23

PAGE 24

PAGE 25

PAGE 26

PAGE 27

PAGE 28

PAGE 29

PAGE 30

PAGE 31

PAGE 32

PAGE 33

PAGE 34

PAGE 35

PAGE 36

GRADING FORM: CSG-RUBIC

DAVID THOMAS

0

RESEARCH-INFORMED LITERATURE



There was evidence of extensive further reading and research from credible and reliable sources. Your interpretation and understanding of the additional research was very good and demonstrated a deep underlying appreciation of the subject. Your references were consistently applied and appropriate to the task and your reference list was of an appropriate length for this assignment.

16/20

KNOWLEDGE AND UNDERSTANDING



The knowledge and understanding of the subject demonstrated by this assignment was generally excellent. There were very few gaps in your knowledge of the basic principles and your understanding of the higher level concepts was demonstrated to a high degree. You have demonstrated a highly competent critical understanding of the main concepts and expanded your knowledge well beyond that contained in the course notes.

24/30

ANALYSIS



Your analysis of the task was excellent, both in class and as shown in this assignment. You have demonstrated highly competent analytical skills and your approach to the task was highly logical. You carried out a detailed evaluation of the results

22/30

and included an excellent conclusion relating your practical results to accepted theory. You have demonstrated a capacity for independent thought and your interpretation of the quantitative and qualitative data was excellent with sound judgements based on wholly valid arguments.

PRACTICAL APPLICATION AND DEP.



Your application of practical skills for this task was generally excellent. You used both the basic and advanced features of the resources appropriately when conducting both experiments and you used appropriate advanced options for testing and evaluating the circuit performance. You managed to evaluate circuit performance and achieved this by rarely asking for assistance thus demonstrating some advanced problem solving skills.

10/10

SKILLS FOR PROFESSIONAL PRAC.



Your written report was very well presented in terms of content and layout and was mostly structured in a coherent way, however you should endeavour to use the available word count more effectively in future. You need to be much more selective with where you put diagrams and graphs, only put those essential for the explanation in the report, the rest can be referred to in the appendix. There was a lot of text heavy tables which could be construed as an attempt to circumvent the word count.

5/10