

1809799

by Thomas Grennan

Submission date: 17-Apr-2022 10:55AM (UTC+0100)

Submission ID: 176431176

File name: 11301_Thomas_Grennan_1809799_179584_595651283.pdf (2.18M)

Word count: 6390

Character count: 42761

Course: BSc (Hons) Electrical and Electronic Engineering

Module: SGEE6005 Electronic Design

Assignment: Micro-controllers and the Internet of Things

Name: Thomas Grennan

University number: 1809799

Date submitted: 17/04/2022

Word count: 3285 words ✓

85-90

- ① Excellent research from a wide range of generally authoritative sources. Citations were appropriate and correctly formatted using Harvard convention.
- ② A critical analysis of the IoT was clearly carried out. You made good reference to the automotive industry which contextualised the arguments.
- ③ The weather station was carried out and you got the Opla kit to work satisfactorily.
- ④ Conclusions and recommendations were a little short, you could have lost some research in favour of the conclusions. Although the research did contain elements of analysis in itself.
- ⑤ Be careful of text talker and the word count.

Contents

Table of Figures	3
Table of Tables	3
1. Executive Summary.....	4
2. Research.....	6
2.1 Key Concepts.....	6
2.1.1 IoT Definitions	6
2.1.2 Enabling Technologies.....	6
2.1.3 Connectivity Models	7
2.1.4 Transformational Potential.....	7
2.2 The origins and drivers of the Internet of Things	9
2.3 IoT Communication Models.....	11
2.3.1 Device to Device.....	11
2.3.2 Device to Cloud	12
2.3.3 Device to Gateway	13
2.3.4 Back-end Data sharing	14
2.4 The security and privacy challenges faced by IoT.....	15
3. IoT enabled weather monitoring system.....	19
3.1.1 Weather Monitoring System Implementation	19
3.1.2 Weather Monitoring System Testing.....	23
4. Overall Conclusions and Recommendations	25
5. Citation List	27
6. Appendix	30
6.1.1 Arduino Code	30
6.1.2 Testing results on Arduino iPad App.....	36

Table of Figures

Figure 1 – IoT Transformational Potential (Digital, 2015).....	7
Figure 2 – Smart Factory (McLaughlin, 2021)	8
Figure 3 - Device-to-Device Model (NarayanaKar, 2017)	11
Figure 4 – Device-to-Cloud utilising CloudRail	12
Figure 5 – Device-to-Gateway model (Software, 2020).....	13
Figure 6 – Back-end Data Sharing Model (Qayyum, 2017).....	14
Figure 7 – Control System Security (Rambus, 2019).....	15
Figure 8 – Arduino 1010 board and MKR Carrier.....	19
Figure 9 – Personal Weather Station: Variable Declaration	20
Figure 10 – Personal Weather Station: Sketch Code	21
Figure 11 – Personal Weather Station: Dashboard Design Section 1	22
Figure 12 - Personal Weather Station: Dashboard Design Section 2.....	22
Figure 13 - Personal Weather Station: Carrier Test Results.....	23
Figure 14 - Personal Weather Station: Dashboard Under Test.....	23
Figure 15 - Personal Weather Station: Trends Under Test	24
Figure 16 - Personal Weather Station: Dashboard Under Test on Mobile App.....	36
Figure 17 - Personal Weather Station: Weather Report Displayed on Mobile App	37
Figure 18 - Personal Weather Station: Trends Under Test on Mobile App	38

Table of Tables

Table 1 – Benefits of Remote Connectivity by eWon	10
Table 2 – IoT aimed Cyber-attacks.....	16
Table 3 – Security measures for IoT Cyber-attacks (Rambus, 2019).....	18

1. Executive Summary

The basis of this report investigates the “Internet of Things (IoT)”, primarily its influence on the Industrial Automation sector focused on Programmable Logic Controllers (PLCs) and the connectivity tools implemented to remotely support these systems through industrial gateways. Initially the key IoT concepts were researched, these were broken down into IoT definitions, enabling technologies, connectivity models and the transformational potential of the Internet of Things, this section outlines the key concepts and connectivity aspects of the Internet of Things.

The origins and drivers were researched in detail, providing a background on the grounds that the IoT was built upon, from the first connected devices in 1832 to the present-day implementation of the IoT in everyday life. There are various companies and concepts that are driving the IoT, therefore research into drivers was narrowed down to focus on automated machine builders and machine end-users. Research into this area saw that HMS Networks are paving the way for IoT development in this sector through their “Anybus” device which offers connection between machines and devices on different protocols maximising the flexibility of machine builders and fully enabling the IoT in machines. Their “eWon” device was also found to be a key driver, offering remote connectivity to control systems across the world through secure virtual-private networks (VPN). Further research saw the exploration into the IoT’s communication models developed by the Internet Architecture Board (IAB) with reference to how machine builders implement these models within control systems. The four models researched are Device-to-Device, Device-to-Cloud, Device-to-gateway and Back-end data sharing, it was found that both Device-to-device and Device-to-Gateway are both widely used in industrial control systems giving flexibility during design, commissioning and support stages.

Research into the security and privacy challenges faced by the IoT was focused on the control systems that drive production in a wide range of industries, these systems are primarily controlled by PLCs and SCADA. It was found that security is one of the inhibiting factors restricting manufacturers from adopting full IoT connectivity. It found that the technology from blue-chip manufacturers that is paving the way for IoT integration also have their own security and privacy discrepancies that deter end-users from implementing them into their systems.

The vulnerability of machine builders and end-users was investigated. Further research focused on the cyber-attacks common to these systems and the preventative measures that companies can take to prevent these attacks.

Utilising Arduino’s Opla IoT kit, a weather monitoring system was implemented and tested. This system is enabled for both Bluetooth and Wi-Fi connectivity. The premise of this system was to create

a device that stores data in the cloud, whilst displaying it on a user interface known as the dashboard in real time. Software design was implemented through a text-based language to control data on 5 different variables. This was proven highly successful, demonstrating the potential of IoT enabled devices in conjunction with the Cloud.

It was concluded that the IoT will hugely benefit society, with the expected economic impact to reach 11% of the global economy by 2025. However, realistically the IoT is still in its early inception where manufacturers need to prepare their production and network infrastructures to cope with the IoT's requirements.

An excellent executive summary

2. Research

2.1 Key Concepts

2.1.1 IoT Definitions

The Internet of Things (IoT) is defined as the network of physical objects, or “things” such as computing devices, mechanical and digital machines, objects or people with unique identifiers (UIDs) that are integrated with software, sensors and various technologies with the purpose of connecting with devices and systems over the internet, enabling data to be generated, exchanged and utilised without requirements of human-to-human or human-to-computer interaction. Devices vary from household items such as fridges, to complex industrial control systems (Gillis, 2022).

2.1.2 Enabling Technologies

The idea of IoT has existed for a long time, recent technological advances made the implementation of it more pragmatic. Technological advances include connectivity breakthroughs, a vast host of network protocols enables ease of connecting sensing devices to other systems like the “Cloud” for efficient data transfer. Development and availability of cloud computing platforms such as Microsoft’s ‘Azure’ and Google’s ‘Cloud’ enables consumers and businesses alike to access infrastructures required to scale up processes, with limited management (Oracle, 2018). Technological advancements in industrial automation have allowed smart-sensor manufacturers such as ifm to produce reliable, power efficient and affordable IoT enabled sensors through protocols like IO-Link (IO-Link, 2022).

Advances in machine learning and analytics, in-conjunction with access to large amounts of cloud-based data enables businesses to gain insight into systems and processes. The emergence of these technologies pushes IoT’s concept limits, with data produced by IoT feeding these technological advancements (Oracle, 2018).

Developments in Artificial Intelligence (AI) systems provide connections between natural-language processing (NLP) and IoT devices like Alexa and Siri. Introducing IoT enabled devices to the general public with true uses in home environments (Oracle, 2018).

Very good arguments covering both industrial and domestic possibilities.

2.1.3 Connectivity Models

IoT's implementation has seen the development of various communication models, each offering their own characteristics for use in various applications. The Internet Architecture Board (IAB) have defined these as Device-to-Device, Device-to-Cloud, Device-to-Gateway, and Back-End Data-Sharing. Each model demonstrates extensive flexibility available for integrating IoT devices, providing solutions for end-users. These models are explained in section 2.3.

2.1.4 Transformational Potential

James Manikya et al from McKinsey Global Institute analysed more than 150 IoT use cases to acquire a broader view of potential benefits and challenges IoT poses on the global economy. These use cases include manufacturers who utilise IoT enabled sensors to optimise machinery productivity and downtime, to health and wellness devices such as 'Fitbit'. The bottom-up analysis undertaken estimated that IoT has a total economic impact of £3 trillion to £8.5 trillion by 2025, with top-end values accounting for 11% of the global economy, with increases of consumer surplus potentially increasing this (2015).

Figure 1 displays nine settings where value is expected to accrue as a result of IoT, with factories seeing the largest transformational potential.

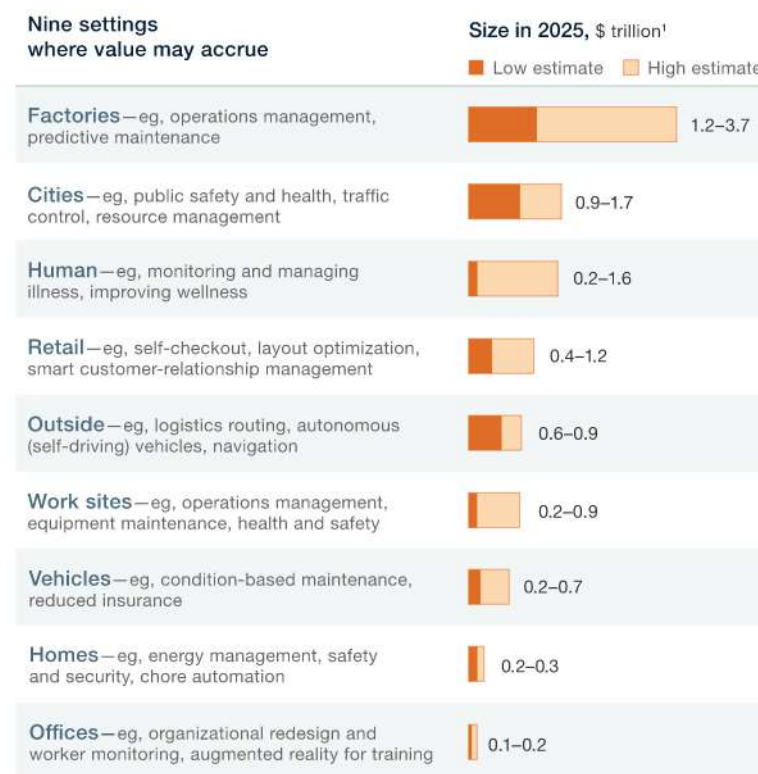


Figure 1 – IoT Transformational Potential (Digital, 2015) Total \$4 trillion–\$11 trillion

IoT has potential of revolutionising factories worldwide, making them “Intelligent Factories”. Factories will be highly digitized, data will be continuously collected, stored and shared through interconnected systems between machines, networks and production systems in manufacturing plants. Data will be utilised by self-optimized devices that will actively improve manufacturing processes, address issues and respond to demands. The transformational potential will be driven by Artificial Intelligence (AI), Cloud Computing and the Industrial Internet of Things (IIoT) in turn making manufacturing processes comprehensive. The capabilities of people and manufacturing devices will be enhanced, optimizing efficiency and productivity, thus creating agile and iterative production processes. Continuous improvement of manufacturing productivity will minimise costs, waste and downtime, the identification of areas where production capacities are underused enables opportunities for growth without the requirement of additional resources or funds (Tulip, 2021) .

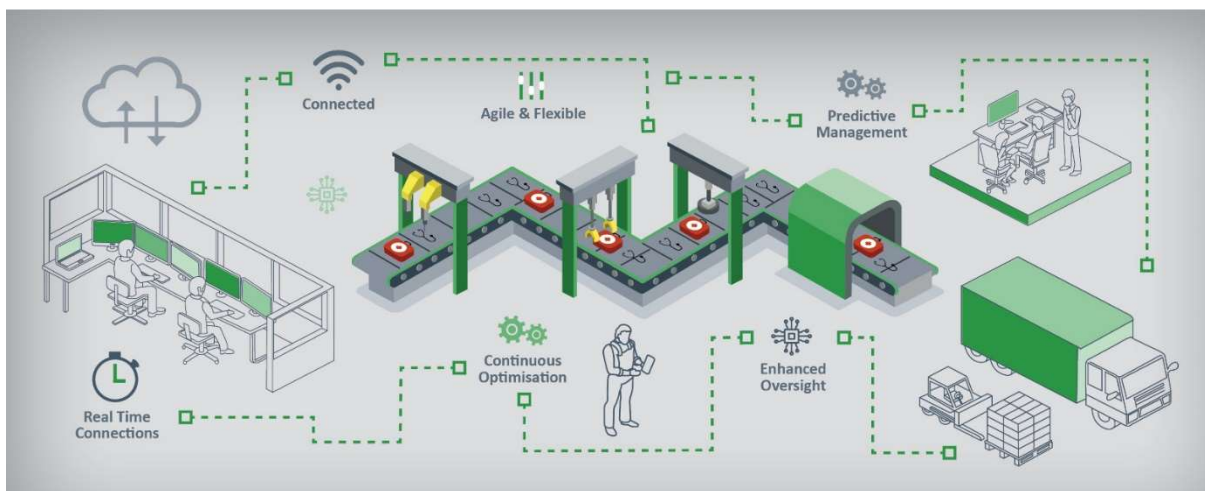


Figure 2 – Smart Factory (McLaughlin, 2021)

A good clear diagram

2.2 The origins and drivers of the Internet of Things

The term “Internet of Things” was conceived by Kevin Ashton in 1999 during a presentation at Procter & Gamble on Radio Frequency Identification (RFID), revolutionising communication in industrial automation. During this time, the internet became the newest trend, leading to Ashton’s presentation being titled “The Internet of Things” (Lueth, 2014). However, the idea of device connectivity has existed for far longer. The first ‘connected device’ dates back to 1832 where the first electromagnetic telegraph was implemented, enabling direct communication between machines by electrical signals and the idea of connecting devices was further explored in the 1970s labelled the “Embedded Internet” (Scammells, 2020).

2008 saw the first international conference on IoT in Switzerland where technologies such as RFID, Sensor Networks and Short-Range Wireless Communications were discussed, driving IoT for industrial machinery (Zencke, 2008). By this time many manufacturing plants found multiple systems with “Machine-to-Machine” communication, however, this was not achieved by the IoT technology but by hardwired IO. Further development saw the “Decade of IoT” in the 2010s, this decade saw the industrial automation sector benefit from the implementation of IoT, the development of IO-Link enabled bi-directional communication between fieldbuses and sensors allowing data to be gathered that was not previously fathomable.

Mohamed Kande stated there are six technological trends that are driving IoT’s development in the industrial automation sector. Lower costs of PLC CPU memory and storage enabled possibilities of storing big data collections and analytics, enabling data to be monitored and analysed for process improvements, also allowing manufacturers to invest in PLC controlled equipment. Furthermore, cloud-based repositories permit unlimited storage of data with encrypted security. Lower data costs enable machine builders to invest into IoT enabled cloud-based applications such as Siemens Edge, where machines equipped with smart sensors can be monitored in real time through a CAD model, benefiting machine builders with the ability to remotely diagnose machines and digitally change components to trial improvements without labour and component costs. The proliferation of IoT enabled sensors at low prices gives manufacturers the realization of information that could be collected on machines, smart sensors allow data on processes, services and events to be cyclically monitored, reducing downtime providing fault diagnosis. Falling costs of megabytes has increased the money available for investments into IoT enabled processing systems and “Cloud” based storage technologies offer flexible repositories for secure data storage. One of the largest driving forces for machine builders is remote connectivity, enabling engineers to provide support to machines worldwide without the disruption of travelling and the costs incurred (2016).

An excellent analysis of its origins and drivers.

Technological developments from HMS Networks revolutionised the industrial automation sector, driving IoT in collaboration with automated control systems for Industry 4.0. HMS Networks' "eWon" remote connectivity device has revolutionized both machine builders and end-users, providing effective and sustainable remote access to all major PLC brands with successful worldwide connectivity and security as standard through secure VPN connections, enabling proactive remote monitoring of machines through quick status overviews and information based on PLC data that is visualised through local or cloud-based dashboards at any time through a multitude of devices. The eWon allowed machine builders to support end-users during COVID-19 where travel bans were imposed, ensuring that vital machines producing food and medicine were fully operational (eWon, 2022). Table 1 displays the benefits of eWon for both machine builders and users.

Benefits of eWon in Industrial Automation	
Benefits for Machine Builders	Benefits for Machine Users
Optimises the productivity for service engineers, reducing travel time	Speed up issue resolutions
Easily involve experts for remote assistance	Improve first time fix rate
Support a larger number of customers	Reduce the impact of emergencies
Lower travel costs	Maximize machine uptime
Easy update of PLC programs and project versions	Control who has access to machine
Reduce the CO2 footprint of your value-chain	Modernize the existing machine fleet

Table 1 – Benefits of Remote Connectivity by eWon (eWon, 2022)

2.3 IoT Communication Models

The Internet Architecture Board (IAB) released a guide to IoT networking in 2015. This document outlined four common communication models utilised by “Smart Objects”; Device-to-Device, Device-to-Cloud, Device-to-Gateway and Back-end data sharing. These models highlight the flexibility in the way that IoT devices connect and aggrandizes value to end users (Futures, 2016). Both Device-to-Cloud and Device-to-Gateway are widely used in industrial automation.

2.3.1 Device to Device

Rose et al states that direct connection of two or more devices is represented by the Device-to-Device model. Devices directly connect and communicate with one another, without requirement of intermediate application servers. Communication is possible through various IP networks or the Internet. Devices also use protocols such as Bluetooth and Z-Wave to establish direct communication (2015).

This model is utilised between devices within close proximity, allowing communications to share data even during network absences, improving data rates and total load reduction of base stations, which handle communications (NarayanaKar, 2017).

Further advantages include increased network efficiency, efficient traffic load management and ability to locally broadcast emergency and warning messages. However, complex algorithms are needed to handle devices efficiently without interference, and due to it being a proximity-based protocol the distance between devices is limited due to power constraints (Rajiv, 2018).

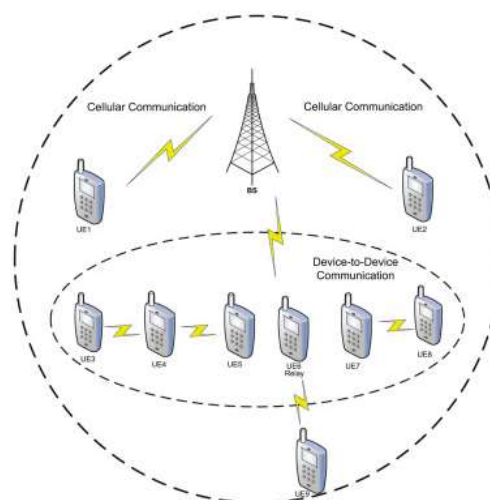


Figure 3 - Device-to-Device Model (NarayanaKar, 2017)

2.3.2 Device to Cloud

The Device-to-Cloud communication model sees devices directly connected to an Internet cloud service, enabling message and data control. These messages are an envelope of telemetry or alert data which is sent and stored in the IoT hub. Device-to-cloud utilises existing architectures such as hardwired Ethernet and Wi-Fi connections to establish connection between the device and IP network. Data can be separated, analysed, stored and sent back to devices (Parenzan, 2019).

Device-to-cloud is widely implemented in automated systems in order to record and store process data for analysis. The development of CloudRail enabled machinery data on processes and sensors to be pre-processed locally and sent to any cloud, utilising industry standards such as OPC-UA to connect modern equipment and old equipment retrofitted with secondary sensors to data repositories. Vastly reducing development time of large-scale projects, IoT deployments are scalable and simple enabling easy management of thousands of devices with industry grade security providing an end-to-end encrypted connection between the gateway and cloud all through device-to-cloud communications (aws, 2021).

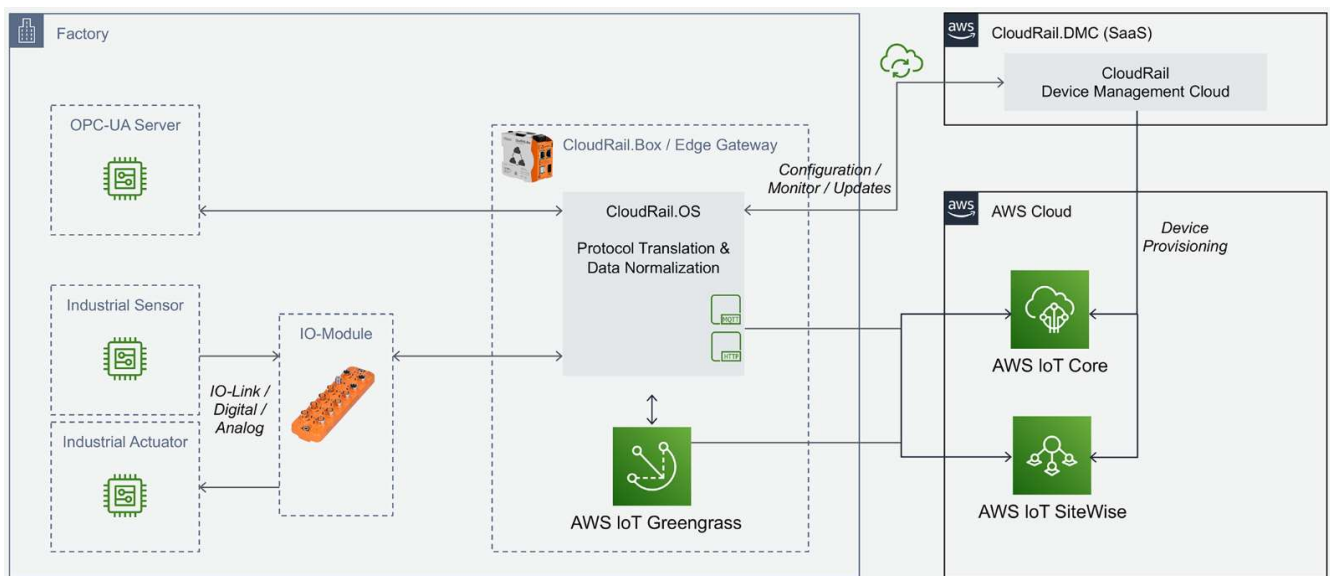


Figure 4 – Device-to-Cloud utilising CloudRail

2.3.3 Device to Gateway

The Device-to-Gateway model utilises an intermediate gateway, this model often involves application software operating on a local gateway device like a network switch or a mobile phone acting as an intermediary between a Cloud service and IoT device. The gateway is a hardware device, which houses application software to perform essential tasks (Software, 2020).

HMS Networks has built upon the Device-to-Gateway model with the Anybus Gateway selector as a solution to communication issues between devices that operate on different protocols in automated systems. Anybus provides protocol translation and security enabling PLCs, Robots and field equipment from any OEM to seamlessly communicate through a gateway. Anybus also allows non-networked devices to communicate through any protocol, converting information into serial data that can be processed by a PLC (HMS, 2021).

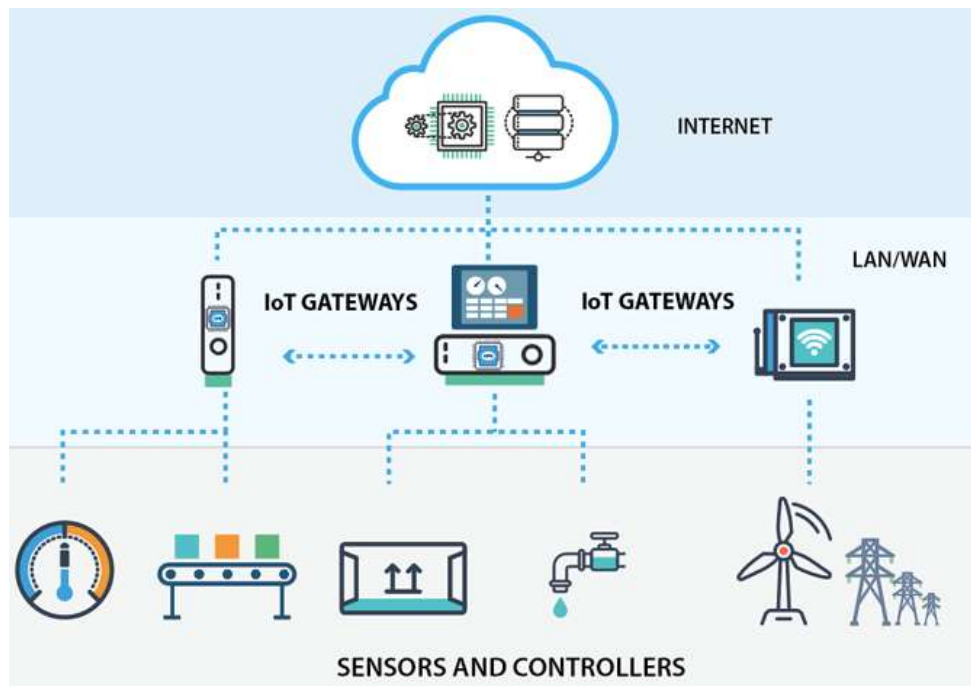


Figure 5 – Device-to-Gateway model (Software, 2020)

2.3.4 Back-end Data sharing

The back-end data-sharing model is the communication architecture that harbours the ability for users to export and analyse smart object data from multiple cloud services in combination with data from other sources. This model supports end-users' requirements for allowing third-party access to gathered data. Iqra Zain et al states that this model is built upon the single device-to-cloud model where IoT devices only uploaded data to a single application layer, back-end architectures allow for aggregation and analysis of data streams (2016).

Multiple "Application Service Providers" are implemented through protocols like Json and HTTPS. Manufacturing plants utilise this to consolidate information on all internet-enabled devices and sensors on site, in turn collecting information on productivity and downtime. This model requires extensive design, initial costs and commissioning time to be properly implemented (Sendler, 2016).

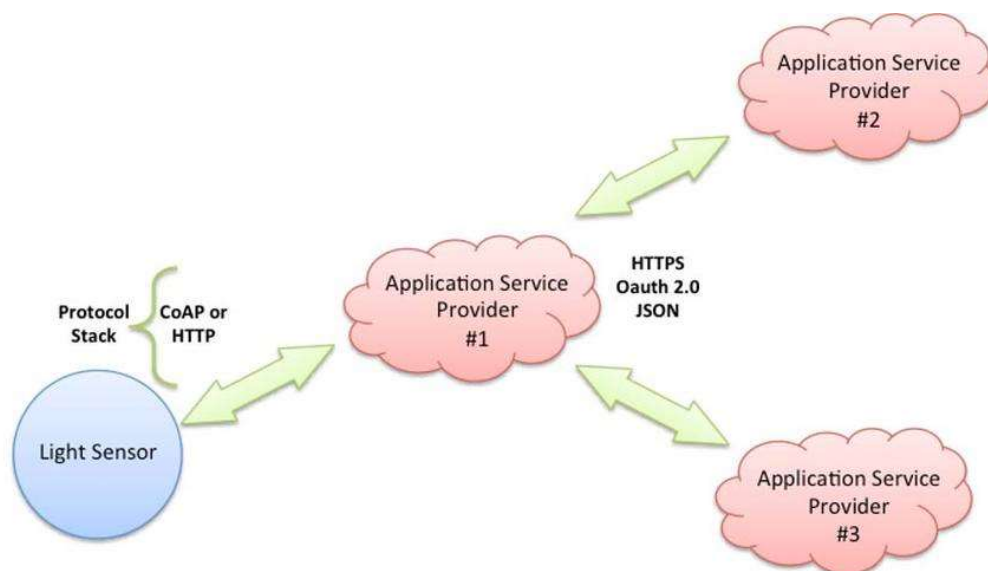


Figure 6 – Back-end Data Sharing Model (Qayyum, 2017)

A very good approach of connectivity models and how they relate to the automotive industry

2.4 The security and privacy challenges faced by IoT

The Internet of Things has vastly improved service and productivity of control systems across industries ranging from health care to manufacturing. These systems include Programmable Logic Controllers (PLCs), Supervisory Control and Data Acquisition (SCADA) systems and Human Machine Interfaces (HMI). However, with anything connected to the internet, IoT devices are targeted by cyber-attacks. Implementation of IP-based devices with increased complexity comes with growing risks aimed at infrastructure as seen in figure 7 (Rambus, 2019).

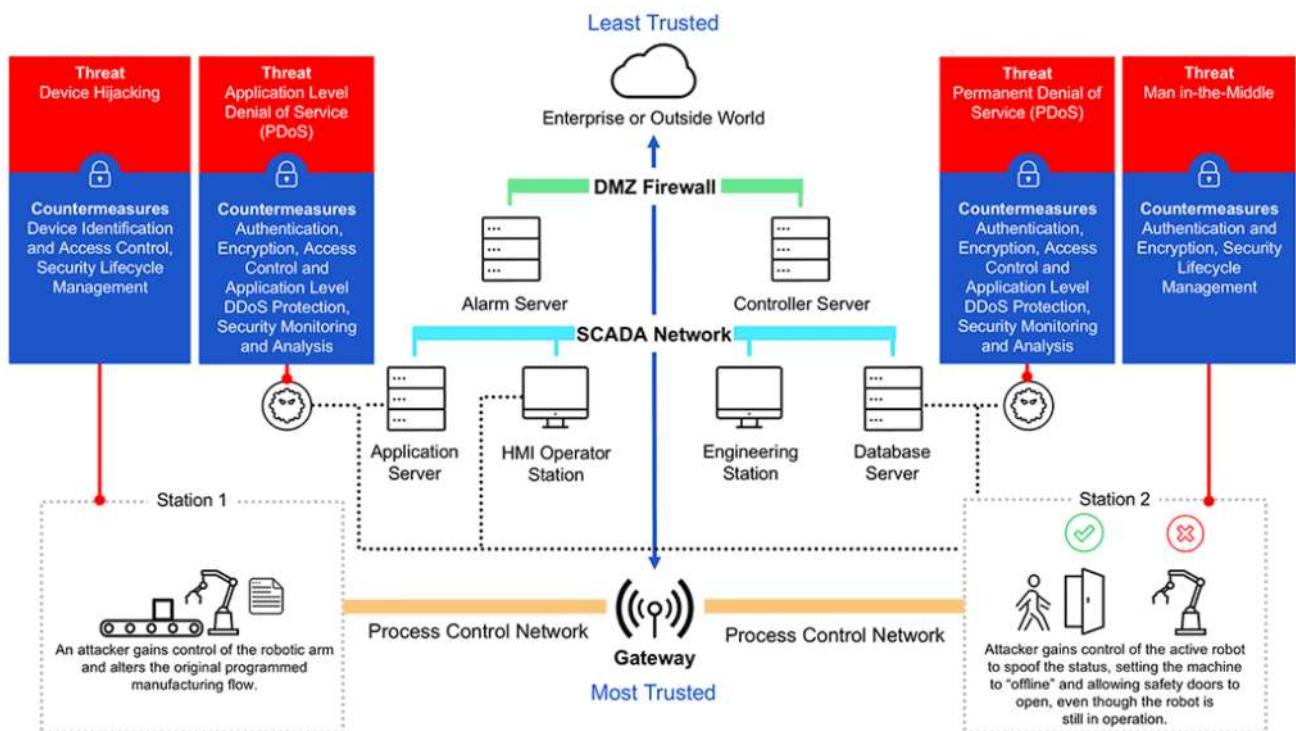


Figure 7 – Control System Security (Rambus, 2019)

Security is one of the biggest inhibiting factors to the adoption of IoT. Threats of cyber-attacks make manufacturers hesitant to open their processes up to potential disruption and losses of critical business because of internet strikes. As a result of COVID-19, IT security companies rapidly implemented ad hoc solutions for remote access at uncertain times, resulting in poor remote cybersecurity policies in organizations, this combined with unsecure networks could be disastrous for IoT enabled systems (Graham, 2021). *Excellent point*

Table 2 outlines three common IoT aimed cyber-attacks.

IoT aimed Cyber-attacks	
Attack	Description
Device hijacking	The attacker hijacks and effectively assumes control of a device. These attacks are quite difficult to detect because the attacker does not change the basic functionality of the device. Moreover, it only takes one device to potentially re-infect others, for example, smart meters connected to a grid. In an IIoT scenario, a hijacker could assume control of a smart meter and use the compromised device to launch ransomware attacks against Energy Management Systems (EMSs) or illegally siphon unmetered power lines.
Distributed Denial-of Service (DDoS)	A denial-of-service attack (DoS attack) attempts to render a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet. In the case of a distributed denial-of-service attack (DDoS), incoming traffic flooding a target originates from multiple sources, making it difficult to stop the cyber offensive by simply blocking a single source. DoS and DDoS attacks can negatively affect a wide range of IIoT applications, causing serious disruptions for utility services and manufacturing facilities.
Permanent Denial of-Service (PDoS)	Permanent denial-of-service attacks (PDoS), also known as phlashing, is an attack that damages the device so badly that it requires replacement or reinstallation of hardware. BrickerBot, coded to exploit hard-coded passwords in IoT devices and cause permanent denial of service, is one such example of malware that could be used to disable critical equipment on a factory floor, in a wastewater treatment plant, or in an electrical substation.

Table 2 – IoT aimed Cyber-attacks

A large percentage of the manufacturing sector consists of automated machine builders; these companies design and manufacture special purpose machinery and robotic systems. In this sector, Machine-to-Machine (M2M) communications are vulnerable, with the potential of PLC and DCS software being stolen or maliciously modified. One of the most overlooked security threats is the network architecture between PLCs and PCs. Many companies have extensive controller networks, CyberX reported that out of 850 industrial networks 16% have weak wireless access points, as many PLCs are out of the way of employees many manufacturers adapt network architectures to enable remote access through gateways such as HMS' eWon (CyberX, 2019).

This solution is convenient but has security issues. The Cybersecurity & Infrastructure Security Agency (CISA) reported that eWon's "Flexy" and "Cosy" models have security vulnerabilities. Low-skill ~~level~~ hackers were able to inject scripts into the Cross-origin Resource Sharing (CORS) to abuse these vulnerabilities, enabling hackers to obtain confidential information through sniffing (CISA, 2020). Further issues where eWon devices did not trigger the discarding of browser session data in response

to log-off actions, this allowed remote hackers to obtain access into control systems by leveraging unattended workstations with no authentication requirements. As a result, a customer of EBS Automation denied the use of eWon devices in their control system due to the privacy challenges that eWon has become associated with. The customer did not want sensitive process information potentially extracted from the machine, along with the possibilities of an unwanted profile of data being available. Instead opting for a highly-encrypted VPN tunnel fully-controlled by the end-user, ultimately making remote support difficult, increasing downtime and negatively impacting production.

A good specific example.

These privacy issues are not just worries for end-users, but for the machine builders too. If hackers have the ability to remotely hack into control systems this means they can extract and modify PLC code. Siemens' S7-1200 & S7-1500 PLCs have been victim to exploitation by malicious hackers remotely enabling access into protected memory and undetected and unrestricted code execution. Remote hackers with access to TCP port 102 have the ability to write arbitrary data and code to the PLCs protected memory whilst reading sensitive data, potentially dangerously modifying the machines sequence, posing risk to manufacturers and humans (Lakshmanan, 2021).

Pepperl+Fuchs Control IO-Link Master gateways are widely used in automated systems; these gateways have flaws, which have been exploited allowing hackers to gain root access to devices. Cross-site request forgery (CSRF) and Reflected cross site scripting (XSS) attacks have affected systems due to outdated versions of third-party components that Control gateway utilises. XSS attacks were commonly implemented permitting hackers to execute device commands with root privileges and implement consistent backdoors (Kovacs, 2021). This outlines security issues due to irregular updates and patches. Devices such as the Control Master are secure at release, however, hackers find security bugs and issues over time, making the IoT device exposed to Botnet attacks such as "Satori" which is a worm that spreads without human interaction from device-to-device by targeting known vulnerabilities in gateways (Thales, 2022).

As IoT is a relatively new technology, there are skill gaps resulting in poor IoT device management. The combination of devices connected traditionally and legacy systems with substandard security results in disruption of reputation, operations and compromised data and security breaches (Peerbits, 2022). Therefore, cyber-attacks originating from industrial control systems integrated with IoT can be disastrous for both the end-user's facility and for the machine builder's reputation and image. The number of cyber-attacks causing disruption to operations is increasing dramatically. As a result, many customers restrict the use of IoT enabled equipment due to the lack of knowledge of security and maintenance resources.

Excellent critical analysis of the security issues with good examples to illustrate the argument.

However, IoT infrastructure can be secured by a set of comprehensive security solutions that pose no hindrance on reliability, service and operation. Secure communication through end-to-end encryption protects the transition of data between a device and the cloud. Encryption ensures that only those who access a decryption key can access transmitted data. Smart actuators implement this in SCADA systems protecting its usage data from digital eavesdropping. Table 3 displays further security measures (Rambus, 2019).

IoT Cyber Attack Security Measures	
Security Measure	Description
Firmware integrity and secure boot	Secure boot utilizes cryptographic code signing techniques, ensuring that a device only executes code generated by the device OEM or another trusted party. Use of secure boot technology prevents hackers from replacing firmware with malicious instruction sets, thereby preventing attacks. Unfortunately, not all IIoT chipsets are equipped with secure boot capabilities. In such a scenario, it is important to ensure that IIoT devices can only communicate with authorized services to avoid the risk of replacing firmware with malicious instruction sets.
Security monitoring and analysis	Security monitoring captures data on the overall state of an industrial system, including endpoint devices and connectivity traffic. Data is then analysed to detect possible security violations or potential system threats. Once detected, a broad range of actions formulated in the context of an overall system security policy should be executed, such as revoking device credentials or quarantining an IoT device based on anomalous behaviour. This automatic monitor-analyse-act cycle may execute in real time or at a later date to identify usage patterns and detect potential attack scenarios. It is critical to ensure that endpoints devices are secured from possible tampering and data manipulation, which could result in the incorrect reporting of events.
Mutual authentication	Every time a smart actuator in the manufacturing floor connects to the network it should be authenticated prior to receiving or transmitting data. This ensures that the data originates from a legitimate device and not a fraudulent source. Secure, mutual authentication—where two entities (device and service) must prove their identity to each other—helps protect against malicious attacks. Cryptographic algorithms involving symmetric keys or asymmetric keys can be utilized for two-way authentication. For example, the Secure Hash Algorithm (SHA-x) along with hash-based message authenticated code (HMAC) can be used for symmetric keys and Elliptic Curve Digital Signature Algorithm (ECDSA) for asymmetric keys.

Table 1 – Security measures for IoT Cyber-attacks (Rambus, 2019)

Avoid large tables as it may be seen as an attempt to circumvent the word count.

3. IoT enabled weather monitoring system

Utilising Arduino's OPLA IoT kit, an IoT connected "Weather Monitoring System" is constructed, programmed and tested. Main control is enabled through the "MKR WIFI 1010 Board". The board is Bluetooth and Wi-Fi enabled, implemented with a Cortex-M0 32-bit processor and ATECC508 crypto chip for data security and protection.

The 1010 board is coupled with the "MKR IoT Carrier" through pins on the board. The carrier is integrated with three sensors; temperature & humidity, pressure and light. The carrier also provides a colour display and five capacitive touch buttons to navigate between screens.

3.1.1 Weather Monitoring System Implementation

The Arduino board and carrier assembly is seen in figure 8.

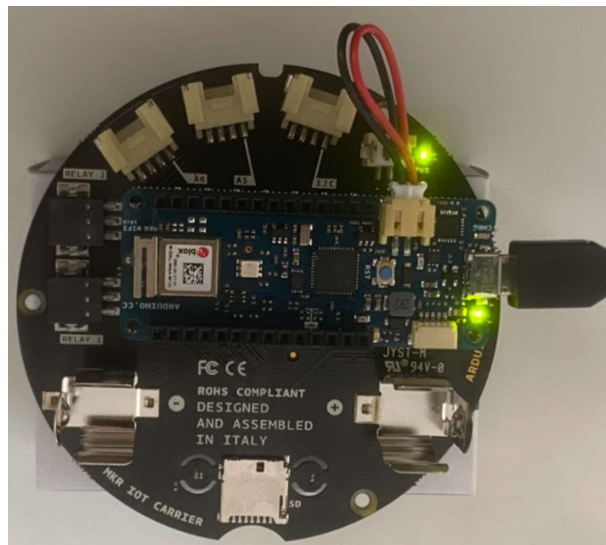


Figure 8 – Arduino 1010 board and MKR Carrier

The "1010 Board" was connected via USB to the Arduino "IoT Cloud" webpage. The Weather Station template was imported onto the board, configuring it to become "IoT ready" by establishing communications with the Arduino Cloud. All network parameters were configured.

After configuration, the “Things” menu is entered, in ‘set-up’ the device and network configuration are accessed. Figure 9 shows five variables for humidity, light, pressure, temperature and weather report declared by the template with data types. The variables permissions and update requests are edited to refresh every 120 seconds.

The screenshot displays the 'Tom Grennans Personal Weather Station' interface. At the top, there's a header with the station name and a 'Thing ID: a6e6dd2a-7a84-432f-9c5c-2b201fd09349'. Below the header are two tabs: 'Setup' and 'Sketch'. The 'Setup' tab is active, showing a 'Variables' section with an 'ADD' button. The 'Variables' section contains a table with five entries:

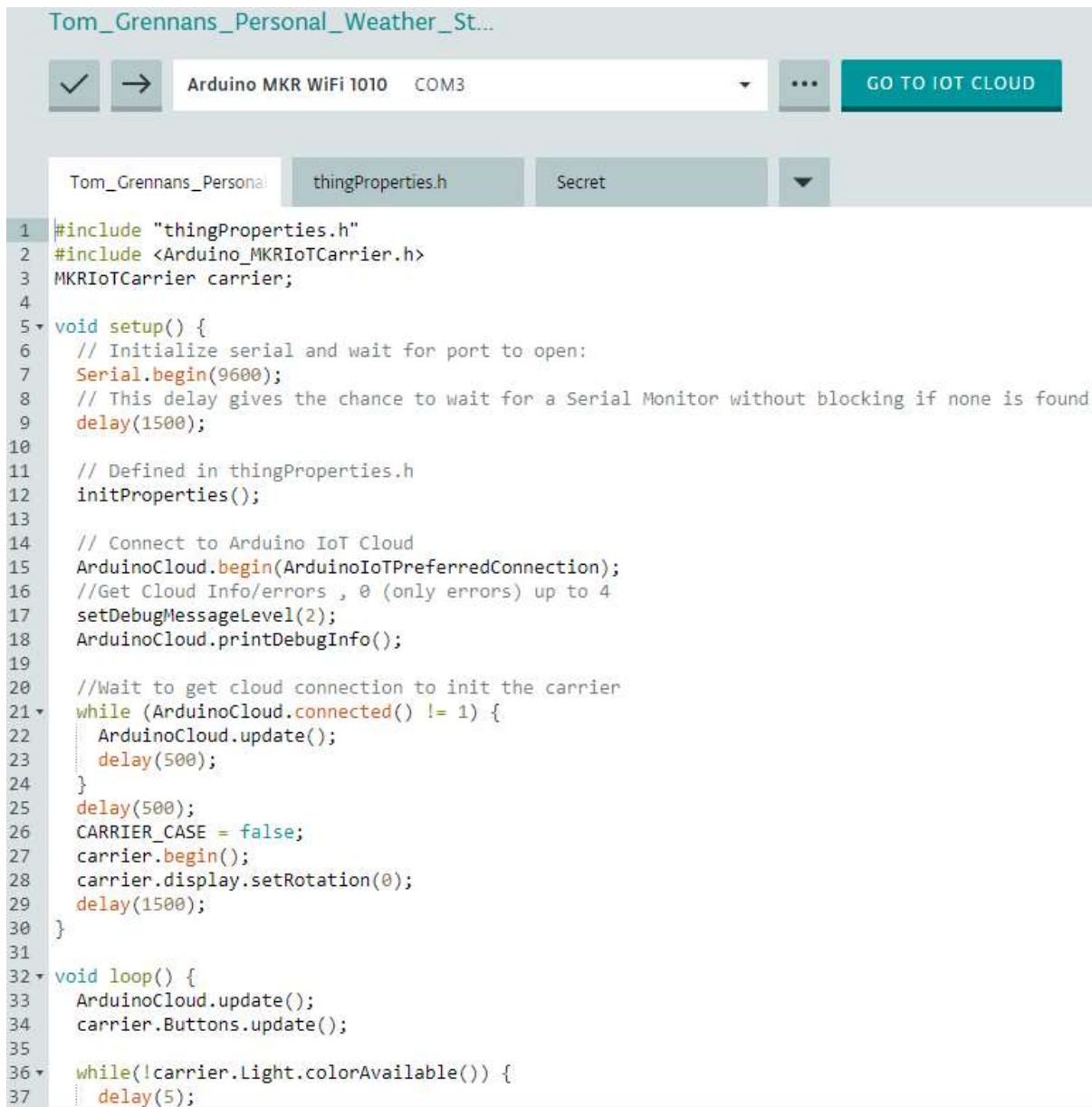
Name ↓	Last Value	Last Update
☐ humidity float humidity;	46.501	19 Mar 2022 13:08:25
☐ light int light;	38	19 Mar 2022 13:08:25
☐ pressure float pressure;	103.003	19 Mar 2022 13:08:25
☐ temperature float temperature;	23.395	19 Mar 2022 13:08:25
☐ weather_report String weather_report;	Weather is n...	19 Mar 2022 13:07:15

To the right of the variables table are two sections: 'Device' and 'Network'. The 'Device' section shows the device name 'lanto', its ID 'da527e41-371a-4c19-8e12-...', type 'Arduino MKR WiFi 1010', and status 'Online'. It includes 'Change' and 'Detach' buttons. The 'Network' section shows the Wi-Fi name 'BT-N7A2...' and a masked password, with a 'Change' button.

Figure 9 – Personal Weather Station: Variable Declaration

Figure 9 shows the “things” menu’s “Sketch” tab. Here the system code is imported and developed. The first lines of code show the inclusion of the “thing properties” and the carrier board. The code consists of two main sections, “Void setup” where the setup code is implemented only once at the start of the sequence for single tasks like connecting to the serial monitor and to the cloud. “Void loop” is the code that constantly runs in loops as long as the board is connected, data of variables is controlled as well as commands to the serial monitor. Modifications were made to the sketch to improve the monitor display.

The full program is seen in appendix 6.1.1.



```
1 #include "thingProperties.h"
2 #include <Arduino_MKRIoTCarrier.h>
3 MKRIoTCarrier carrier;
4
5 void setup() {
6     // Initialize serial and wait for port to open:
7     Serial.begin(9600);
8     // This delay gives the chance to wait for a Serial Monitor without blocking if none is found
9     delay(1500);
10
11     // Defined in thingProperties.h
12     initProperties();
13
14     // Connect to Arduino IoT Cloud
15     ArduinoCloud.begin(ArduinoIoTPreferredConnection);
16     //Get Cloud Info/errors , 0 (only errors) up to 4
17     setDebugMessageLevel(2);
18     ArduinoCloud.printDebugInfo();
19
20     //Wait to get cloud connection to init the carrier
21     while (ArduinoCloud.connected() != 1) {
22         ArduinoCloud.update();
23         delay(500);
24     }
25     delay(500);
26     CARRIER_CASE = false;
27     carrier.begin();
28     carrier.display.setRotation(0);
29     delay(1500);
30 }
31
32 void loop() {
33     ArduinoCloud.update();
34     carrier.Buttons.update();
35
36     while(!carrier.Light.colorAvailable()) {
37         delay(5);
```

Figure 10 – Personal Weather Station: Sketch Code

The final design implementation is the “Dashboard”, this is the IoT cloud interface that displays the variables data in real time. Figure 11 displays the first section of the dashboard, this displays real data on current temperature, humidity, pressure and light, along with a weather report which is determined by “if” and “elseif” statements dependent on the condition of variables. The variables are mapped to the necessary widgets.

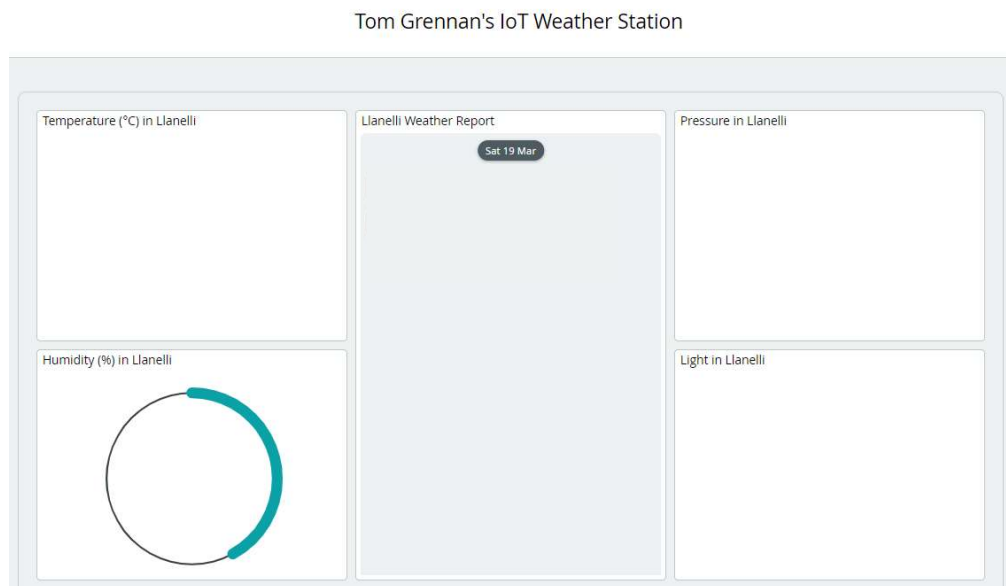


Figure 11 – Personal Weather Station: Dashboard Design Section 1

Figure 12 displays data trend dashboard design for weather and humidity. Trends can be viewed from current live data to data from the past 15 days that is stored in Arduino’s cloud.

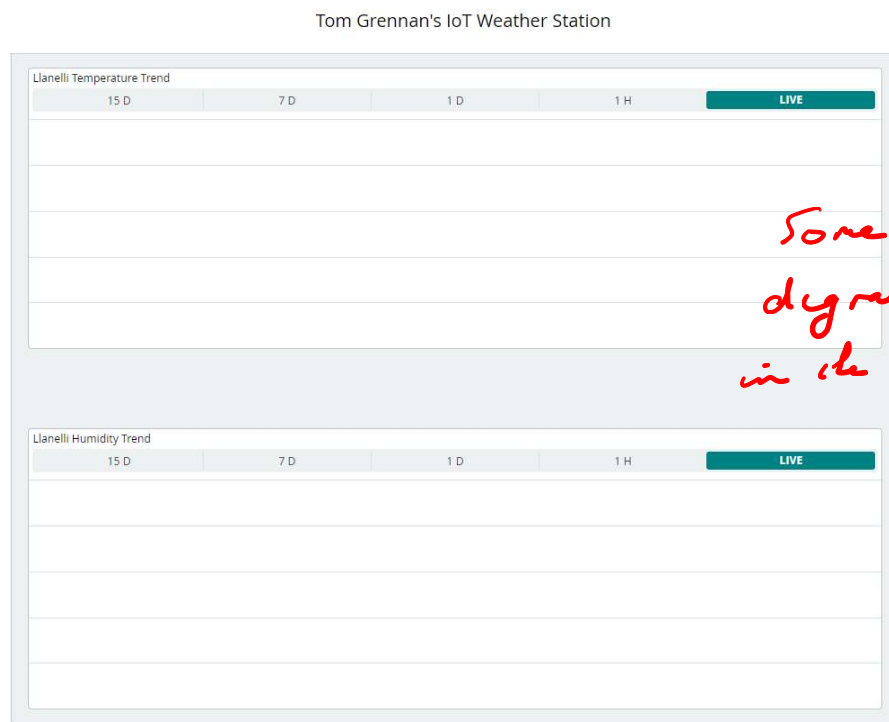


Figure 12 - Personal Weather Station: Dashboard Design Section 2

3.1.2 Weather Monitoring System Testing

The final code and dashboards were compiled and uploaded onto the board. Figure 13 shows the values of temperature, humidity, light intensity and pressure that the carrier has measured and displayed.



Figure 13 - Personal Weather Station: Carrier Test Results

Figure 14 shows the current data displayed on the dashboard. The values displayed are highly accurate when compared to the carrier readings in figure 13. Small discrepancies are due to the author manually taking readings of the carrier which refreshes quickly, making it difficult to get both readings simultaneously.

Tom Grennan's IoT Weather Station

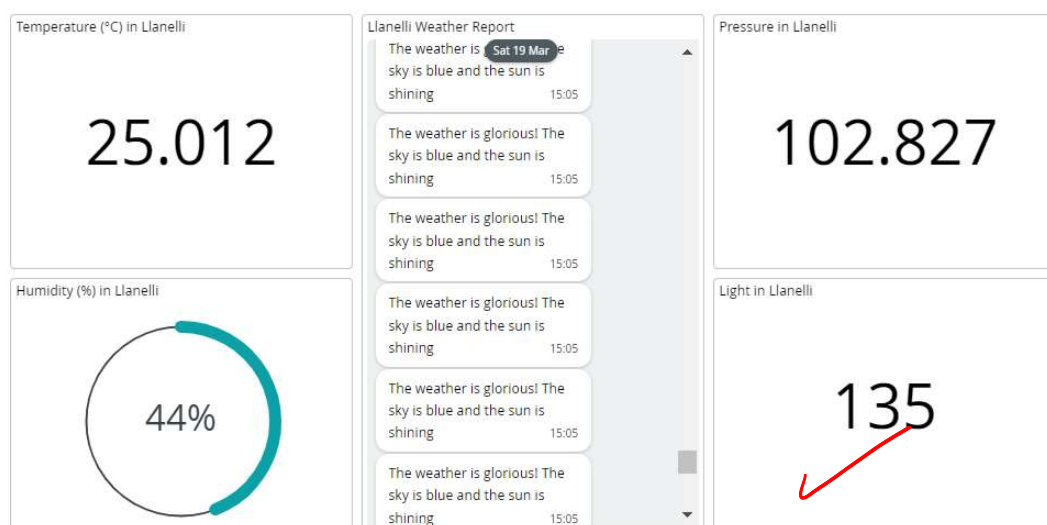


Figure 14 - Personal Weather Station: Dashboard Under Test

Figure 15 displays temperature and humidity trends in intervals over an hour period, successfully displaying the weather stations integration with the Arduino cloud to store and display previously recorded data.

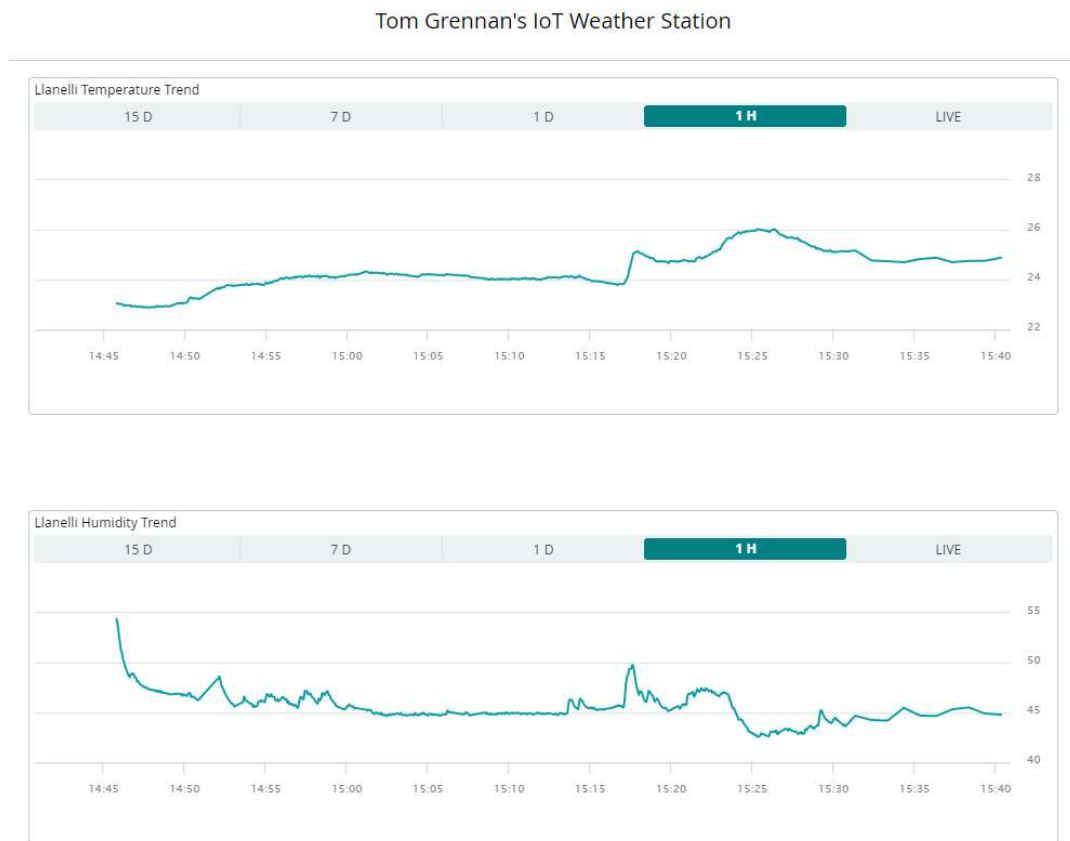


Figure 15 - Personal Weather Station: Trends Under Test

Images in appendix 6.1.2 displays the cloud dashboards flexibility, showing the ability of the OPLA IoT device to display the same data as the desktop dashboard to a mobile dashboard in real time. In turn proving that with the login details, anyone can access the information as the Internet of Things intends.

4. Overall Conclusions and Recommendations

The research undertaken demonstrated benefits that IoT already has on society. The collaboration of key global companies to drive enabling technologies such as sensor and cloud-based developments has proven pinnacle in further development. Research into transformational potential proved the worldwide influence the IoT has. Every area of human life will see improvements from factories, cities and apartments, further developments will increase the economic impact to 11% of the global economy, with the largest impact being on factories.

It was found that IoT drivers such as HMS' remote connectivity and gateway modules are heavily influencing machine builders to adopt IoT communication models into their systems. The benefits of implementing these devices in conjunction with Device-to-Cloud, Device-to-Device and Device-to-Gateway are paramount for both system integrators and end users alike, reducing overheads, increasing productivity and limiting downtime with a reduced carbon footprint.

However, the research illustrated how the IoT is still in its inception, and whilst major companies have plans on its development it's true transformational potential is still unknown, the multitude of developmental forces driving the concept has the potential to steer it any direction. From the research, it is clear that digital infrastructure needs vast improvements to be able to support the goal of the IoT. The security infrastructure of end-users requires improvements to meet requirements of smart factories, including up-skilling of employees. Smart factories require secure network infrastructures, IoT enabled controllers, analytical software integrated with information systems and the implementation of cloud computing and artificial intelligence, these requirements come with costs that many manufacturers will not be able to justify due to design, implementation, commissioning and integration times, not to mention millions of legacy systems that will require complete overhauls function with IoT devices.

Companies that are already up-to-date will need to adapt to fast-changing advances that are common with the IoT, these advancements are essential for the functionality and security of systems.

The Opla IoT kit was appropriate in demonstrating the potential and power of IoT connected devices integrated with smart sensors and the cloud. Simplicity of the set-up, software language and dashboard design prove that the implementation of smart systems is not only achievable by engineers, but by the general public. It demonstrated that the integration of basic hardware with cloud-based functionality can be used to obtain, display and store data seamlessly and accessed over a multitude of devices worldwide. The flexibility of these microcontrollers proves that the potential IoT based applications are limitless at low-costs.

In conclusion, a world with full device connectivity through the IoT will positively benefit millions of lives. Manufacturing plants will see increased productivity through full connectivity, processes will see improvements from the data and analytics collected and developments such as “Machine Learning” will be the driving force for both machine builders and end-users where artificial intelligence is implemented to enable systems to learn from data to identify patterns and make key decisions with no human interaction. IoT will help humans live and work smarter, gaining control over their lives through data obtained from smart devices through the analysis of behaviours and activities. However, it is paramount that security systems can keep these systems locked down, this will be possible through the upskilling of employees and harsher security infrastructures.

5. Citation List

- al, I. Z. e., 2016. Internet of Things. *Internet of Things* , 4(3), pp. 1088-1092.
- al, K. R. e., 2015. *The Internet of Things: An Overview*, Geneva: Internet Society.
- aws, 2021. *CloudRail Solutions on AWS*. [Online]
Available at: <https://aws.amazon.com/iot/solutions/cloudrail/>
[Accessed 03 31 2022].
- CISA, 2020. *ICS Advisory (ICSA-20-254-03)*. [Online]
Available at: <https://www.cisa.gov/uscert/ics/advisories/icsa-20-254-03#:~:text=An%20attacker%20with%20local%20access,been%20assigned%20to%20this%20vulnerability.>
[Accessed 31 03 2022].
- CyberX, 2019. *Providing Secure Remote Access For Industrial Networks*. [Online]
Available at: https://cyberx-labs.com/wp-content/uploads/2018/12/CYBX_CyberArk_122018.pdf
[Accessed 31 03 2022].
- Digital, M., 2015. *Unlocking the potential of the Internet of Things*. [Online]
Available at: [https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world#:~:text=Our%20bottom%20Dup%20analysis%20for,the%20world%20economy%20\(exhibit\).](https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world#:~:text=Our%20bottom%20Dup%20analysis%20for,the%20world%20economy%20(exhibit).)
[Accessed 13 03 2022].
- esds, 2019. *How would Smart IoT shape our lives in the future?*. [Online]
Available at: <https://www.esds.co.in/blog/smart-iot-shape-lives-future/>
[Accessed 13 03 2022].
- eWon, 2022. *Industrial remote connectivity solutions*. [Online]
Available at: <https://www.ewon.biz/home>
[Accessed 18 03 2022].
- Futures, C., 2016. *The Four Internet of Things Connectivity Models Explained*. [Online]
Available at: <https://www.channelfutures.com/best-practices/the-four-internet-of-things-connectivity-models-explained#:~:text=This%20outlined%20four%20common%20communication,Back%2DEnd%20Data%2DSharing.>
[Accessed 2022 03 2022].
- Gillis, A. S., 2022. *What is the internet of things (IoT)?*. [Online]
Available at: <https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT>
[Accessed 13 03 2022].
- Graham, K., 2021. *Common Vulnerabilities with Remote Access*. [Online]
Available at: <https://www.bitsight.com/blog/common-vulnerabilities-associated-with-remote-access>
[Accessed 31 03 2022].
- Hajda, J., 2021. *Security Challenges in Industry 4.0 PLC Systems*, Basel: MDPI.
- HMS, 2021. <https://www.anybus.com/>. [Online]
Available at: <https://www.anybus.com/>
[Accessed 31 03 2022].

InetServicesCloud, 2016. *The Four Internet of Things Connectivity Models Explained*. [Online]
Available at: <http://www.inetservicescloud.com/the-four-internet-of-things-connectivity-models-explained/#:~:text=In%20the%20Device%2Dto%2DGateway,device%20and%20a%20cloud%20service>
e.

[Accessed 13 03 2022].

IO-Link, 2022. *IO-Link*. [Online]

Available at: <https://io-link.com/en/index.php>

[Accessed 13 3 2022].

Kande, M., 2016. *The Six driving forces of the Internet of Things*. [Online]

Available at: <https://www.pwc.com/gx/en/technology/pdf/six-forces-driving-iot.pdf>

[Accessed 18 03 2022].

Kovacs, E., 2021. *Vulnerabilities Can Allow Hackers to Create Backdoors in Control Industrial Gateways*. [Online]

Available at: <https://www.securityweek.com/vulnerabilities-can-allow-hackers-create-backdoors-control-industrial-gateways>

[Accessed 31 03 2022].

Kraeling, M., 2019. *Software Engineering for Embedded Systems*. 2nd ed. London: Elsevier.

Lakshmanan, R., 2021. *A New Bug in Siemens PLCs Could Let Hackers Run Malicious Code Remotely*. [Online]

Available at: <https://thehackernews.com/2021/05/a-new-bug-in-siemens-plcs-could-let.html>

[Accessed 31 03 2022].

Lueth, K. L., 2014. *Why the Internet of Things is called Internet of Things: Definition, history, disambiguation*. [Online]

Available at: <https://iot-analytics.com/internet-of-things-definition/>

[Accessed 18 03 2021].

McLaughlin, S., 2021. *The Essential Steps in Your Smart Factory Evolution*. [Online]

Available at: <https://slcontrols.com/the-essential-steps-in-your-smart-factory-evolution/>

[Accessed 31 03 2022].

NarayanaKar, U., 2017. *An overview of device-to-device communication in cellular networks*. 1st ed. Bhubaneswar: KIIT University.

Networks, H., 2021. *Anybus*. [Online]

Available at: <https://www.anybus.com/home>

[Accessed 18 03 2022].

Oracle, 2018. *What is IoT?*. [Online]

Available at: [https://www.oracle.com/internet-of-things/what-is-iot/#:~:text=The%20Internet%20of%20Things%20\(IoT\)%20describes%20the%20network%20of%20physical, and%20systems%20over%20the%20internet](https://www.oracle.com/internet-of-things/what-is-iot/#:~:text=The%20Internet%20of%20Things%20(IoT)%20describes%20the%20network%20of%20physical, and%20systems%20over%20the%20internet).

[Accessed 13 03 2022].

Parenzan, M., 2019. *Introduction to Azure IoT Hub*. [Online]

Available at: <https://cloudacademy.com/course/introduction-to-azure-iot-hub/device-to-cloud-1/#:~:text=A%20device%2Dto%2Dcloud%20message, and%20sending%20data%20from%20devices>.

[Accessed 13 03 2022].

- Peerbits, 2022. *17 Biggest security challenges for IoT*. [Online]
Available at: <https://www.peerbits.com/blog/biggest-iot-security-challenges.html>
[Accessed 31 03 2021].
- Qayyum, M., 2017. *Back-End Data sharing model*. [Online]
Available at: https://www.researchgate.net/figure/Back-End-Data-sharing-model_fig4_316735737
[Accessed 13 03 2022].
- Rajiv, 2018. *How does device to device communication work*. [Online]
Available at: <https://www.rfpage.com/how-does-device-to-device-communication-works/>
[Accessed 13 03 2022].
- Rambus, 2019. *Industrial IoT: Threats and Countermeasures*. [Online]
Available at: <https://www.rambus.com/iot/industrial-iot/>
[Accessed 14 03 2022].
- Scammells, J., 2020. *History of the Internet of Things (IoT)*. [Online]
Available at: <https://www.itonlinelearning.com/blog-history-iot/#:~:text=The%20world's%20first%20IoT%20device%20was%20invented%20in%20the%20early,machine%20was%20out%20of%20Coke.>
[Accessed 18 03 2022].
- Sendler, U., 2016. *The Internet of Things*. 1st ed. Berlin: Springer Verlag.
- Software, O. A., 2020. *What is an IoT Gateway?*. [Online]
Available at: <https://openautomationsoftware.com/open-automation-systems-blog/what-is-an-iot-gateway/>
[Accessed 13 03 2022].
- Thales, 2022. *IOT SECURITY ISSUES IN 2022: A BUSINESS PERSPECTIVE*. [Online]
Available at: <https://www.thalesgroup.com/en/markets/digital-identity-and-security/iot/magazine/internet-threats>
[Accessed 31 03 2022].
- Tulip, 2021. *What Is A Smart Factory? (And What It Means For You)*. [Online]
Available at: <https://tulip.co/glossary/what-is-a-smart-factory-and-what-it-means-for-you/>
[Accessed 31 03 2022].
- Zencke, D. P., 2008. *Internet of Things 2008*. [Online]
Available at: <https://iot-conference.org/iot2008/>
[Accessed 18 03 2022].

6. Appendix

6.1.1 Arduino Code

```
/*
```

Sketch generated by the Arduino IoT Cloud Thing "Untitled"

<https://create.arduino.cc/cloud/things/151ec4be-5c5f-47b2-9225-e383f05732e5>

Arduino IoT Cloud Variables description

The following variables are automatically generated and updated when changes are made to the Thing

```
String weather_report;
```

```
float humidity;
```

```
float pressure;
```

```
float temperature;
```

```
int light;
```

Variables which are marked as READ/WRITE in the Cloud Thing will also have functions which are called when their values are changed from the Dashboard.

These functions are generated with the Thing and added at the end of this sketch.

```
*/
```

```
#include "thingProperties.h"
```

```
#include <Arduino_MKRIoTCarrier.h>
```

```
MKRIoTCarrier carrier;
```

```
int modeSelect = 0;
```

```
int previousMode = 0;
```

```
int refreshCount = 0;
```

```
void setup() {
```

```

// Initialize serial and wait for port to open:
Serial.begin(9600);

//while (!Serial);

// Defined in thingProperties.h
initProperties();

// Connect to Arduino IoT Cloud
ArduinoCloud.begin(ArduinoIoTPreferredConnection);

//Get Cloud Info/errors , 0 (only errors) up to 4
setDebugMessageLevel(2);
ArduinoCloud.printDebugInfo();

//Wait to get cloud connection to init the carrier
while (ArduinoCloud.connected() != 1) {
  ArduinoCloud.update();
  delay(500);
}
delay(500);
CARRIER_CASE = true;
carrier.begin();
carrier.display.setRotation(0);
carrier.display.fillScreen(ST77XX_BLACK);
carrier.display.setTextColor(ST77XX_WHITE);
carrier.display.setTextSize(3);

carrier.display.setCursor(60, 80);
carrier.display.print("Weather");
carrier.display.setCursor(60, 120);
carrier.display.print("Station");
delay(2000);

```

```

carrier.display.fillScreen(ST77XX_BLACK);
carrier.display.setTextColor(ST77XX_WHITE);
carrier.display.setTextSize(2);

carrier.display.setCursor(70, 80);
carrier.display.print("Connected");
carrier.display.setCursor(50, 110);
carrier.display.print("To IoT Cloud");
delay(2000);
}

void loop() {
  ArduinoCloud.update();
  carrier.Buttons.update();

  while(!carrier.Light.colorAvailable()) {
    delay(5);
  }
  int none;
  carrier.Light.readColor(none, none, none, light);

  temperature = carrier.Env.readTemperature();
  humidity = carrier.Env.readHumidity();
  pressure = carrier.Pressure.readPressure();

  if(carrier.Button0.onTouchDown()) {
    modeSelect = 0;
  }
  else if(carrier.Button1.onTouchDown()) {
    modeSelect = 1;
  }
}

```

```

else if(carrier.Button2.onTouchDown()) {
    modeSelect = 2;
}
else if(carrier.Button3.onTouchDown()) {
    modeSelect = 3;
}
else if(carrier.Button4.onTouchDown()) {
    modeSelect = 4;
}

if(modeSelect != previousMode) {
    updateDisplay();
    previousMode = modeSelect;
    refreshCount = 0;
}
else if (refreshCount >= 50) {
    updateDisplay();
    refreshCount = 0;
}

if (humidity >= 60 && temperature >= 15) {
    weather_report = "It is very humid outside";
}
else if (temperature >= 25 && light >= 700) {
    weather_report = "Hot and sunny outside";
}
else if (light <= 100) {
    weather_report = "It is dark outside";
}
else if (temperature >= 15 && light >= 700) {
    weather_report = "Warm and sunny outside";
}

```

```

}

else if (temperature <= 16 && light >= 700) {
    weather_report = "A little cold, but sunny outside";
}

else if (humidity >= 90 && temperature <= 15) {
    weather_report = "It is wet and rainy outside";
}

refreshCount++;
}

```

```

void updateDisplay () {
    if (modeSelect == 0) {
        carrier.display.fillScreen(ST77XX_RED);
        carrier.display.setTextColor(ST77XX_WHITE);
        carrier.display.setTextSize(4);

        carrier.display.setCursor(70, 50);
        carrier.display.print("Temp:");
        carrier.display.setCursor(40, 110);
        carrier.display.print(temperature);
        carrier.display.print(" C");
    }

    else if (modeSelect == 1) {
        carrier.display.fillScreen(ST77XX_BLUE);
        carrier.display.setTextColor(ST77XX_WHITE);
        carrier.display.setTextSize(4);

        carrier.display.setCursor(70, 50);
        carrier.display.print("Humi:");
        carrier.display.setCursor(40, 110);
        carrier.display.print(humidity);
    }
}

```

```

    carrier.display.print(" %");
}
else if (modeSelect == 2) {
    carrier.display.fillScreen(ST77XX_GREEN);
    carrier.display.setTextColor(ST77XX_BLACK);
    carrier.display.setTextSize(4);

    carrier.display.setCursor(60, 60);
    carrier.display.print("Light:");
    carrier.display.setCursor(80, 120);
    carrier.display.print(light);
}
else if (modeSelect == 3) {
    carrier.display.fillScreen(ST77XX_CYAN);
    carrier.display.setTextColor(ST77XX_BLACK);
    carrier.display.setTextSize(4);

    carrier.display.setCursor(60, 60);
    carrier.display.print("Press:");
    carrier.display.setCursor(20, 110);
    carrier.display.print(pressure);
    carrier.display.print(" Pa");
}
else {
    carrier.display.fillScreen(ST77XX_BLACK);
}
}

```

6.1.2 Testing results on Arduino iPad App

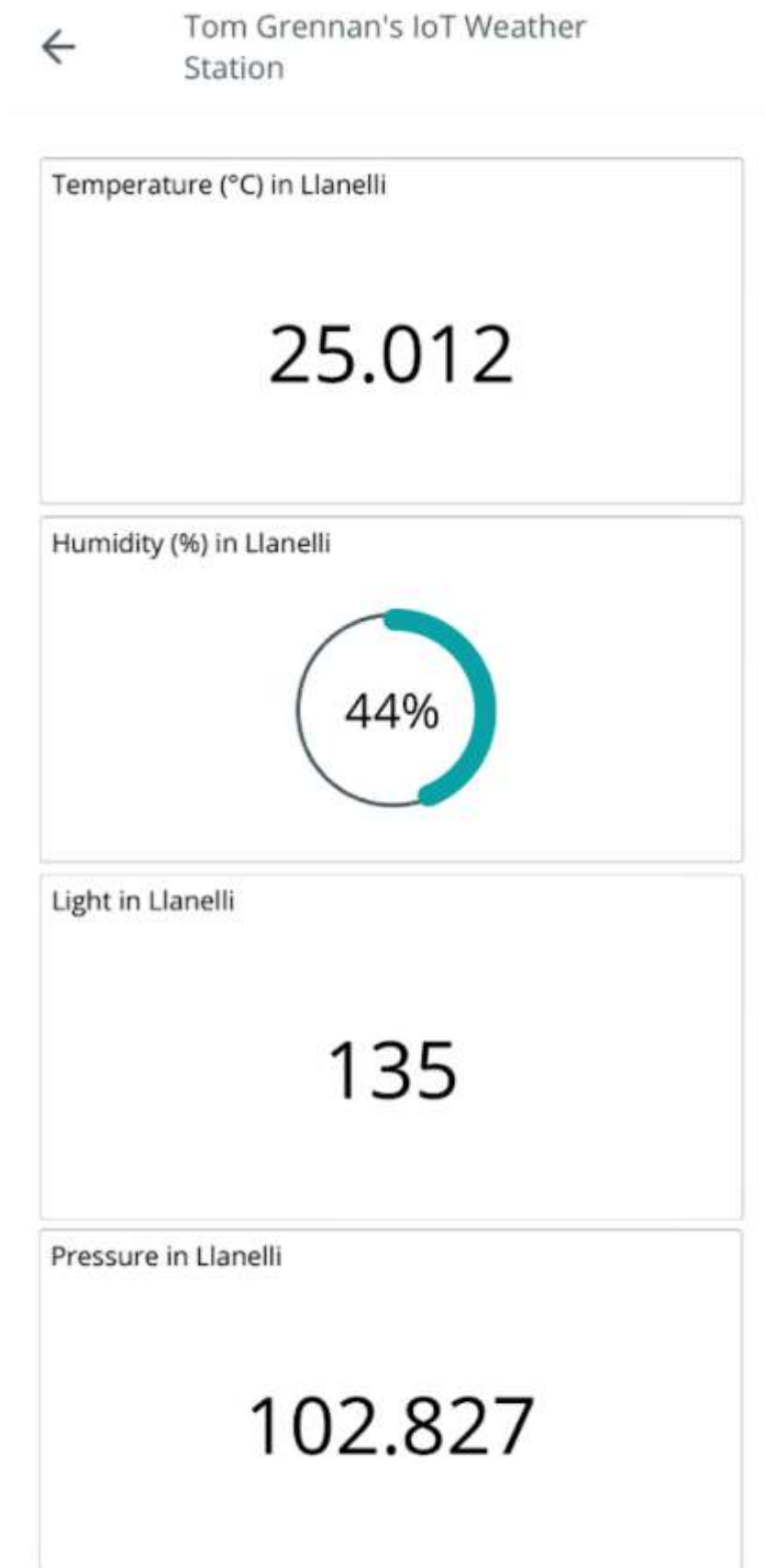


Figure 16 - Personal Weather Station: Dashboard Under Test on Mobile App

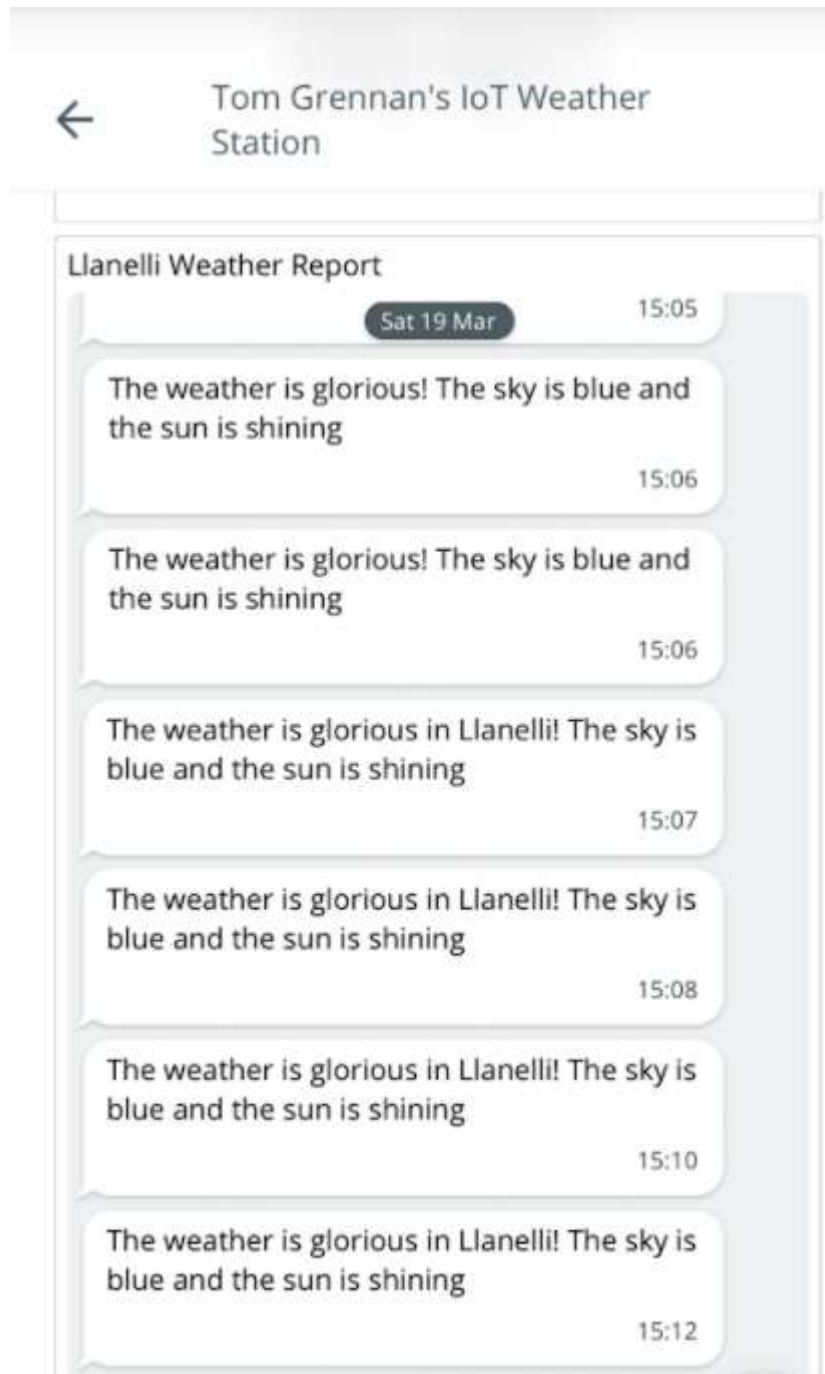


Figure 17 - Personal Weather Station: Weather Report Displayed on Mobile App



Figure 18 - Personal Weather Station: Trends Under Test on Mobile App

FINAL GRADE

GENERAL COMMENTS

Instructor

90/100

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

PAGE 37

PAGE 38

GRADING FORM: CSG-RUBIC

THOMAS GRENNAN

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.

18/20**KNOWLEDGE AND UNDERSTANDING**

The knowledge and understanding of the subject demonstrated by this assignment was exceptional. There were no gaps in your knowledge of the basic principles and the higher level concepts were extremely well explained. You contextualised the report and have demonstrated an exceptionally detailed knowledge and critical understanding of the main concepts and expanded your knowledge beyond that contained in the course notes.

27/30**ANALYSIS**



Your analysis of the task was outstanding, 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 and included an excellent conclusion connecting ideas and providing logical and persuasive arguments. You have demonstrated a considerable capacity for independent thought and the ability to see beyond the question and your interpretation of the quantitative and qualitative data was exceptional with sound judgements based on wholly valid arguments.

26/30

PRACTICAL APPLICATION AND DEP.



Your application of practical skills for this task was generally exceptional. You used both the basic and advanced features of the resources appropriately when designing the dashboard and you used appropriate advanced options for testing and evaluating the performance. You managed to design an effective dashboard that functioned well within the specification and achieved this by rarely asking for assistance thus demonstrating some advanced problem solving skills.

10/10

SKILLS FOR PROFESSIONAL PRAC.



In this assignment you have demonstrated skills in working individually and also collaboratively. Your written report was written in a professional and confident style, however you still need to be more efficient with your word count. The report was very well presented, with excellent diagrams in

9/10

appropriate places, good sentence/paragraph structure and clear calculations.