Internet of Things (IoT)

Intelligent and Digital Manufacturing

Derek Badman

Patrick Maynard

Linda George

Noor Pola

2024

Contents

Executive Summary 2

1. Introduction 2

2. What is Internet of Things (IoT) 2

3. Experiment 2

3.1. Premise 2

3.2. Breakdown 2

3.2.1. Physical Setup 2

3.2.2. Flashing and Verification 4

3.2.3. Troubleshooting 4

3.3. Outcome 5

4. Our Findings/Experience 6

5. Applications in the industry 8

6. Security Concerns and Implementation 8

7. Next Steps for IoT 9

7.1 Security and Regulation 9

7.2 Trends in Technology 9

7.3 Market Growth 9

8. Conclusion 10

References 11

Appendix 13

1. Arduino MKRWfFi1010V2.0 Schematic 13

2. Raw Experiment Data 14

3. Arduino Boilerplate Code 16

4. GitHub Repository 19

# Executive Summary

# Introduction

The Internet of Things (IoT) is a revolutionary concept that is changing the way we interact with technology and our surroundings. At its heart, the Internet of Things (IoT) is a network of networked devices embedded with sensors, software, and other technologies that allow them to gather and share data with one another as well as with central systems or users over the internet.

The Internet of Things (IoT) covers a wide range of devices, from domestic appliances, wearable gadgets, and smart thermostats to industrial machinery, cars, and infrastructure components such as smart cities and smart grids.

One of the primary advantages of IoT is its capacity to deliver real-time insights and allow data-driven decision-making across a variety of sectors. For example, in healthcare, IoT devices may remotely monitor patients' vital signs and inform clinicians to any irregularities, resulting in early intervention and better patient outcomes. In agriculture, IoT sensors may collect data on soil moisture levels, meteorological conditions, and crop health, allowing farmers to improve irrigation and crop management strategies to increase yields and sustainability.

However, the proliferation of IoT devices raises questions about privacy, security, and data management. With billions of networked devices transmitting and receiving data, strong security measures are required to protect sensitive information from unwanted access or modification. As IoT evolves and becomes increasingly interwoven into our everyday lives and industries, it has the potential to drive innovation, increase efficiency, and improve quality of life. From smart homes that change lighting and temperature depending on tenant preferences to smart factories that improve production processes and decrease downtime, IoT's potential uses are limitless, offering a future in which almost everything is linked and intelligent.

# Objectives

The objective of this report is to explore the internet of Things as used in todays industry. We will attempt to do this by conducting a small-scale experiment to show the basic functionality of an IoT device and then expand upon that with a look at how it is rolled out on a larger scale.

# What is Internet of Things (IoT)

The Internet of Things (IoT) encompasses a vast ecosystem of interconnected devices, ranging from household appliances and wearable gadgets to industrial machinery and infrastructure components. By leveraging sensors and connectivity capabilities, these devices can gather real-time data about their environment and operational status. This data can then be analyzed to derive insights, optimize performance, and facilitate proactive decision-making. Moreover, IoT systems often incorporate machine learning and artificial intelligence algorithms to continually improve their functionality and adapt to changing conditions. As a result, IoT technology has the potential to revolutionize numerous industries, including healthcare, agriculture, transportation, and manufacturing, by enabling unprecedented levels of automation, efficiency, and innovation.

Furthermore, the proliferation of IoT devices has led to the emergence of interconnected ecosystems known as smart environments. These environments integrate various IoT-enabled devices, such as smart homes, smart cities, and smart factories, to create interconnected networks that enhance overall functionality and user experience. In a smart home, for instance, IoT devices like smart thermostats, lighting systems, and security cameras can communicate with each other to create personalized and energy-efficient living spaces. These devices can learn user preferences over time, adjusting temperature settings, lighting levels, and security protocols accordingly. Similarly, in smart cities, IoT sensors embedded in infrastructure components can monitor traffic flow, detect environmental pollution levels, manage waste disposal systems, and optimize public transportation routes in real-time. This data-driven approach to urban management not only improves efficiency but also promotes sustainability and enhances the overall quality of life for residents. Additionally, in smart factories, IoT technology enables the implementation of predictive maintenance strategies, where equipment sensors detect potential failures before they occur, minimizing downtime and optimizing production processes. Through these applications and more, IoT is revolutionizing various sectors, ushering in an era of unprecedented connectivity, efficiency, and innovation.

# Experiment

## Premise

To get a better working understanding of the Internet of Things concept we felt it best to set up an IoT project from start to finish on a small scale. We found a project that would monitor the temperature and humidity of an area using a small, embedded board and a multi-function sensor. Then using the data gathered from the device populate a web-based dashboard provided by Arduino Cloud [https://app.arduino.cc/].

## Breakdown

## 3.2.1. Physical Setup

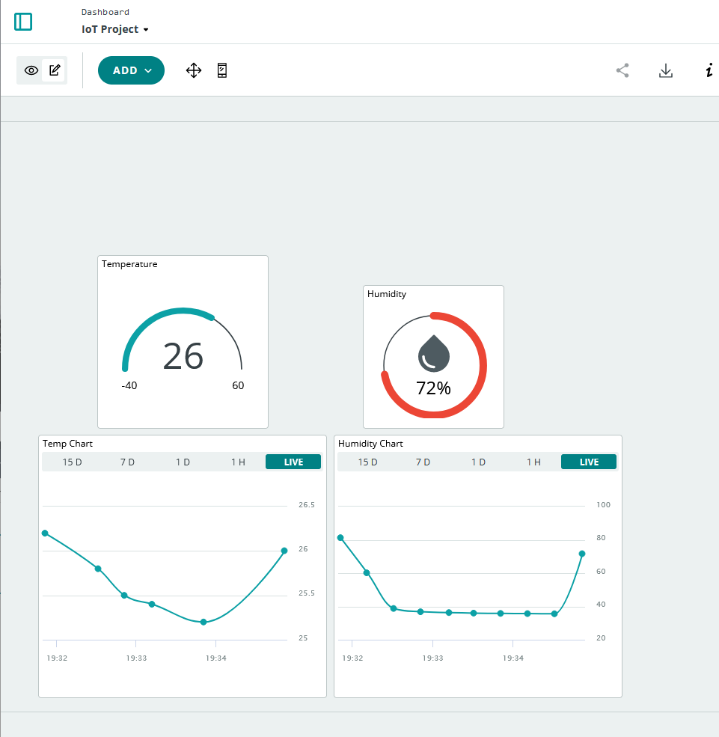
We began with setting up and wiring our breadboard with our Arduino MKR 1010 Wi-Fi board and a DHT multi-function sensor (Fig. 1). After the board, now named Zaria, had come online it came time to flash it with the boilerplate code and wi-fi credentials to enable it to communicate via wireless on its own.

A close-up of a machine

Description automatically generated

Fig 1: MRK Board and DHT Sensor Setup

## 3.2.2. Flashing and Verification

A screenshot of a computer

Description automatically generatedOnce Zaria was online uploading the code was the next step (Fig. 2). Using the Arduino Cloud (<https://app.arduino.cc>) we flashed the code and set up a dashboard to monitor the output of the sensor (Fig. 3).

Fig 2: Code Upload

Fig 3: Live Dashboard

## 3.2.3. Troubleshooting

After getting out initial feedback from our sensor we noticed that it was reading incredibly high. After re-wiring and re-flashing, the conclusion was that the sensor itself was intermittent. After replacing our DHT11(Fig. 4) with a DHT22 (Fig. 5) sensor the project was back on track.

A close up of a device

Description automatically generated

Fig 5: DHT 22 Sensor

Fig 4: DHT 11 Sensor

## Outcome

The final product of our small scale IoT experiment was a fully functional temperature and humidity monitor for a home server room. Thanks to Arduino Cloud we were able to make a multi-platform IoT dashboard (Fig. 6 and Fig. 7) using minimal hardware.

# A screenshot of a device Description automatically generatedOur Findings/Experience

Fig 7: Desktop Dashboard

Fig 6: Android Dashboard

The most notable lesson learned from this experiment has been, the more companies make IoT devices modular and accessible the more everyday users can innovate with them. With just a few simple boards and a web browser, we were able to set up a basic IoT monitoring system. After the system had run for a few days, we were easily able to export some data from it to present (Fig. 8). If we wanted to take it further, the boilerplate code could be updated to send the data directly to our database and polled from there for any number of custom tasks. The IoT possibilities are endless. This small-scale experiment is a single use example of what we would see in a factory monitoring system. But instead of one board and one sensor, we would see hundreds or thousands of sensors fed back to a controller and used to populate several dashboards and end-user tools (Fig. 7).

A hand holding a tablet with a graph on it

Description automatically generated

Fig. 7

A person holding a clipboard

Description automatically generated

Fig 8: Data Export

# Applications in the industry

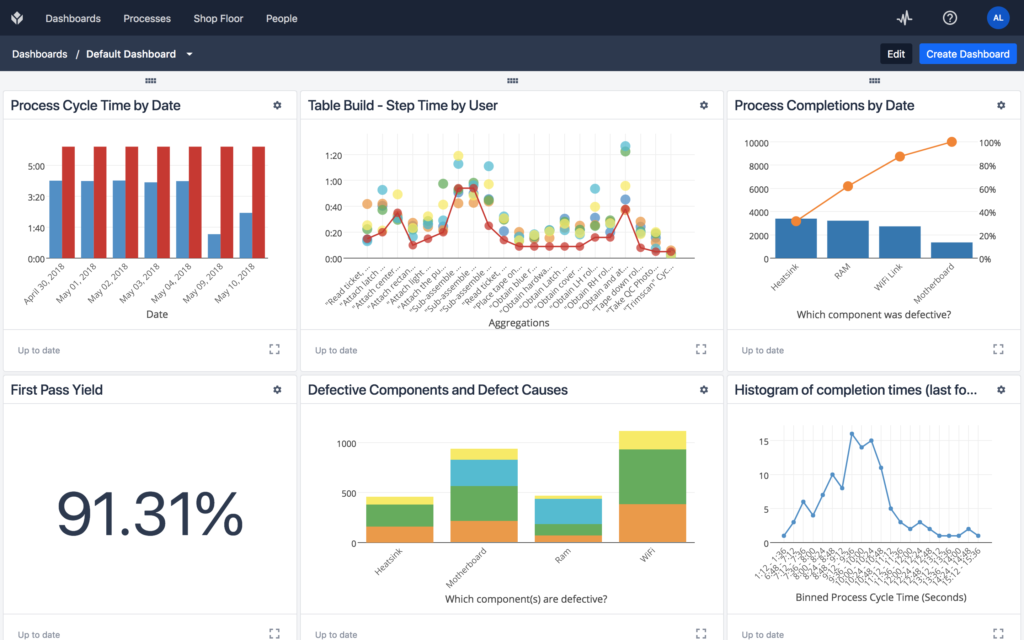
As technology continues to advance, more companies are shifting to using IoT for better operations, process optimization and exceptional delivery to customers. It has been used in a variety of industries, such as:

* Transportation, by offering a method to track shipments in real-time, optimize routing, vehicle maintenance status, driver status and more. This allows for greater supply chain visibility, delivery accuracy and efficient operations to meet customer demands and satisfaction.
* Healthcare, by offering remote patient monitoring, asset and inventory management, as well as medical equipment maintenance status. This allows better patient care, efficient resource utilization and ultimately provides more enhanced operational efficiency.
* Agriculture, by offering methods for precision farming, soil conditions monitoring, livestock tracking, and the capability of optimizing irrigation systems. This allows farmers to make more informed decisions when increasing crop yield, resource consumption reductions, and beneficial sustainable farming practices.
* Retail, by offering inventory management, supply chain optimization, targeted marketing, and efficient store solutions. This allows retailers to assure customer satisfaction, create better modes of operation and increase sales through proper marketing.
* Manufacturing, by offering methods to monitor production, inventory tracking, and optimize asset performance. This allows manufacturers to improve operational efficiency, track and reduce downtime, and assure product quality.

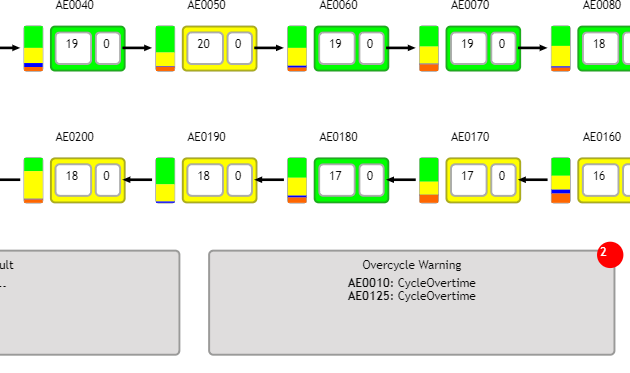
Several industries have turned to IIoT technologies to enable data-driver decision-making, operate more efficiently, improve asset utilization, and drive innovation. One industry in particular has put great importance on the use of IIoT technologies: manufacturing. With the new, advanced capabilities, automotive manufacturing companies have noticed great improvements in supply chain management, vehicle connectivity, operational efficiency, and customer satisfaction. Several automotive companies have opted to utilizing IIoT for a number of reasons.

* Supply Chain Management: IIoT technologies are utilized to enhance visibility and transparency in the automotive supply chain. It has allowed the tracking of inventory and assets to optimize obsolescence issues, reduce lead times, and minimize any disruptions that may impact production.
* Predictive Maintenance: Predictive maintenance of production equipment can be enforced through IIoT technologies. This can be done by collecting and analyzing real-time data from production smart-devices (any device using an IP address), which are located within the production line. By monitoring device status and performance, automotive companies are able to detect and avoid potential issues, which reduces the risk of downtime, optimizes maintenance scheduling, as well as extend components’ lifecycle.
* Smart Manufacturing: By using IIoT technologies, automotive companies are able to optimize production processes, monitor equipment performance, and ensure high-quality manufacturing, resulting in what can be considering a smart factory. This can be done by using IIoT to monitor production lines in real-time, predict machine maintenance scheduling, and improve productivity through streamline operations.
* Customer Experience: The customer’s experience and satisfaction can be enhanced with the use of IIoT by enabling personalized services, offering vehicle monitoring and predictive maintenance notifications, as well as seamless connectivity features. Through these innovative solutions, automotive companies are able to meet customers’ preferences and expectations.

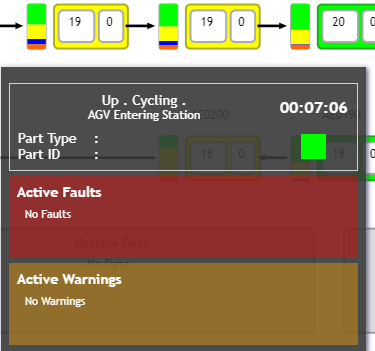
The use of IIoT technologies and solutions have greatly impacted the automotive industry. Companies are reporting enhanced connectivity, data-driver insights, production times, product development, cost-savings and customer experiences. An example of a company that utilizes the use of IIoT technologies is Ford Motor Company. Majority of Ford plants have implemented the use of IIoT monitoring on their production lines, with plans to adopt this innovative solution at all remaining plants that are currently not utilizing it. Ford’s use of IIoT technologies are mainly used to monitor production lines. Through IIoT, the plants are able to monitor the line’s Performance KPI (Key Performance Indicator), Machine State, Cycle Time, Alerts, Rate of Climb and Events. Similar IIoT monitoring dashboards are widely used in other automotive companies, as shown in the image below.



The dashboard, that displays data collected by IIoT technology can create tables and graphs to outline the cycle times by date and/or shift, the operator’s personal cycle time per station to allow management to evaluate their employees’ performance, the shift’s defects and their causes and more. IIoT also allows the plant to analyze and eliminate any faults/issues that may hinder production.



The image above shows the layout of the line with added features that allow the user to dictate what type of information they want displayed. In this case, the top priority is to assure cycle times are being met. If a fault occurs, the option to investigate the reason behind this over-cycling issue.



A feature that is commonly used through IIoT is the data collection of the machines’ status. As shown in the image above, the user is able to see the machine is currently cycling, what task it’s currently performing, as well as the fault and warning status. This allows the plant to assure a smooth operation and an efficient method to troubleshoot any stations that are experiencing problems. The use of IIoT has greatly improved cycle times, production, and quality.

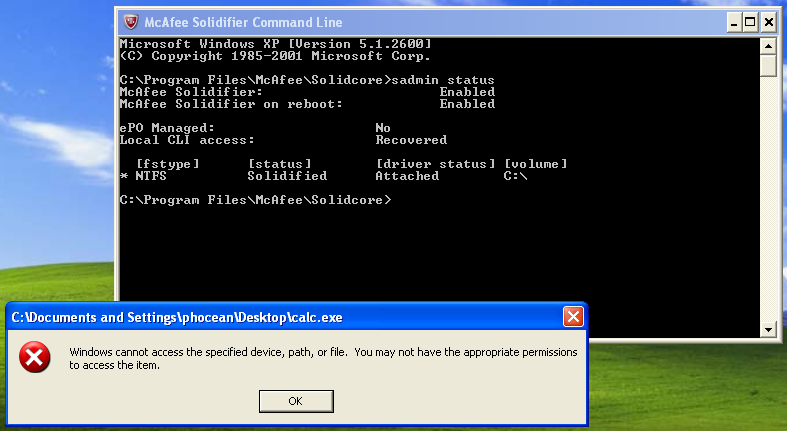
# Security Concerns and implementation

Due to the fact that IIoT uses internet to process data, it also carries risks of being compromised and releasing confidential and classified information. Therefore, security measures must be implemented to avoid any risks associated with connecting industrial devices and systems to the internet. Some commonly used security measures include:

* Access Control: Using strong authentication methods to enforce strict access control. This will restrict unauthorized access to the IIoT system being used.
* Device Authentication: Allow only specific devices trusted devices to connect to the network. The verification of these devices can be done using certificates, security keys, and/or device authentication protocols to eliminate the risk of compromising critical systems and data.
* Network Segmentation: Isolate critical systems from external threats by implementing network segmentation. This can be done by dividing the network into separate segments and controlling the flow of traffic between them. By doing so, the company can eliminate the risk of a security breach and prevent attackers within the network.
* Data Encryption: Implement strict access control policies to restrict unauthorized access to devices, systems and data. To do so, the company can use protocols such as TLS (Transport Layer Security) to securely communicate between IIoT devices, gateways and servers.
* Monitoring: Using real-time monitoring of IIoT network traffic, device behavior and security events to detect abnormal activities that can be views as potential security threats. Using security information and event management tools will help analyze logs, generate alerts/reports and resolve security breaches.

There are many methods to avoid the possibility of data breach; however, the implementation of one or several is critical when using IIoT to protect industrial assets and eliminate the cybersecurity risks associated with the interconnections within the industry. These security methods are necessary to protect the company’s integrity, classified and confidential data and to avoid any disruptions to production that would result in a lose in profit.

There are several softwares that are used when implementing security measures. A commonly used software is McAfee’s Solidcore. This security solution is designed to protect by only allowing trusted applications to run and prevent any unauthorized changes to a system’s files and configurations.



# Next Steps for IoT

Within the next five to ten years, the Internet of Things is expected to undergo rapid growth to support an increased user interface. To succeed in developing a technology that will continue to make societal impacts and leave a lasting footprint in technological history. Internet of Things will need to focus on the following areas of development:

## 7.1 Security and Regulation

As internet crime increasingly continues to rise (125% in 2021 compared to 2020), cybersecurity and the regulation of the same is an important focus for the developers of Internet of Things technology.

Internet of Things developers are expected to incorporate practical cybersecurity measures such as encryption, certificate-based authentication, and security standardization across platforms.

Developers of the Internet of Things will be challenged by ensuring the technology and security measures conform to privacy legislation across global jurisdictions. In Canada, developers must ensure they comply with the federal Personal Information Protection and Electronic Documents Act.

## 7.2 Trends in Technology

A large focus of developers of the Internet of Things throughout the development of the technology will be to keep up with ever-changing trends and societal progression. As society evolves, technology is expected to become ever more integrated into the consumer’s daily life.

Internet of Things is expected to expand to a futuristic society that incorporates technology such as smart cities, wearables, and transportation. As such, developers are expected to focus much of their attention on ensuring the Internet of Things technology is advanced in a way that can support such a change in global societies.

## 7.3 Market Growth

It is important for developers of Internet of Things technology to be aware of the differing market needs and industries of the many users of the technology. For example, the needs and wants of a user of wearable technology will differ greatly from a user of medical technology.

Developers will have to implement practical approaches and apply revolutionary as well as precedent techniques to ensure that different industries are accommodated. This will ensure a smooth transition to Internet of Things technology.

Despite the many challenges that the developers of Internet of Things technology will face in the coming years, there is no doubt that the Internet of Things will have a significant impact on society as a whole.

# Summary and Conclusion

The Internet of Things is a rapidly growing platform that touches everything from everyday household items to industrial robots. One great example of this is the Arduino platform that lets anyone create IoT dashboards right from their laptop. With emerging user-friendly technologies IoT is becoming accessible to everyone.

Cyber security must evolve with the technology to keep everyone’s information private. As we grow this technology, we are sure to see more legislation focusing on its implementation. With security methods such as McAfee Solidcore, companies can ensure the integrity of their classified and confidential information while utilizing a simple means of storing and collecting a wide variety of data.

# References

Articles :

Bhattacharayya, R. et al. (2010). Low-cost, ubiquitous RFID-tag-antenna-based sensing. Proceedings of the IEEE. 98 (10). 1593-1600.

L. D. Xu, W. He and S. Li, "Internet of Things in Industries: A Survey," in IEEE Transactions on Industrial Informatics, vol. 10, no. 4, pp. 2233-2243, Nov. 2014, doi: 10.1109/TII.2014.2300753.

Li, S., Xu, L.D. & Zhao, S. The internet of things: a survey. Inf Syst Front 17, 243–259 (2015). https://doi.org/10.1007/s10796-014-9492-7

Madakam, S. , Ramaswamy, R. and Tripathi, S. (2015) Internet of Things (IoT): A Literature Review. Journal of Computer and Communications, 3, 164-173. doi: 10.4236/jcc.2015.35021.

LaFlamme, R., & LaFlamme, R. (2023, October 30). *What’s next for the Internet of Things* Auvik. https://www.auvik.com/franklyit/blog/future-of-it/

Imber, D. (2024, February 21). The Latest Cyber Crime Statistics (updated February 2024) AAG IT Support. *AAG IT Services*. https://aag-it.com/the-latest-cyber-crime-statistics#:~:text=Cyber%20Crime%20Overview,businesses%20and%20individuals%20in%2 2022.

Legislative Services Branch. (2019, June 21). *Consolidated federal laws of Canada, Personal Information Protection and Electronic Documents Act*. https://laws-lois.justice.gc.ca/eng/acts p-8.6FullText.html#:~:text=An%20Act%20to%20support%20and,the%20Statutory%20Instrums20Act%20and

Websites:

*Temperature Monitoring with Arduino IoT Cloud using DHT22*. (n.d.). projecthub.arduino.cc. https://projecthub.arduino.cc/attari/temperature-monitoring-with-arduino-iot-cloud-using-dht22-cd8e34

# Appendix

## Screenshot 2024-03-03 at 11.10.02 AM.pngScreenshot 2024-03-03 at 11.06.37 AM.png1. Arduino MKRWfFi1010V2.0 Schematic

## 2. Raw Experiment Data

| **Time** | **Humidity** | **Temperature** |
| --- | --- | --- |
| 2024-02-23T00:15:07.154216356Z | 870.5 | 640.2999877929690 |
| 2024-02-23T00:15:27.16232095Z | 870.5999755859380 | 640.2000122070310 |
| 2024-02-23T00:16:07.189374697Z | 870.7000122070310 | 640.0999755859380 |
| 2024-02-23T00:16:27.197187536Z | 870.5999755859380 | 640.2000122070310 |
| 2024-02-23T00:17:27.372441351Z | 870.5 | 640.0999755859380 |
| 2024-02-23T00:17:47.223373163Z | 870.7000122070310 | 640.2000122070310 |
| 2024-02-23T00:18:27.23820977Z | 870.5999755859380 | 640 |
| 2024-02-23T00:18:47.65518405Z | 870.7000122070310 | 640.0999755859380 |
| 2024-02-23T00:19:07.293200722Z | 870.5999755859380 | 640 |
| 2024-02-23T00:19:27.298825208Z | 870.7000122070310 | 640.0999755859380 |
| 2024-02-23T00:19:47.306921705Z | 870.5999755859380 | 640 |
| 2024-02-23T00:20:07.315180638Z | 870.7000122070310 | 640.0999755859380 |
| 2024-02-23T00:21:07.741060404Z | 871.0999755859380 | 640.5999755859380 |
| 2024-02-23T00:21:27.371427129Z | 845.5 | 640.5 |
| 2024-02-23T00:21:47.449481926Z | 0 | 0 |
| 2024-02-23T00:23:11.921398119Z | 0 | 0 |
| 2024-02-23T00:25:34.866884658Z | 0 | 0 |
| 2024-02-23T00:25:49.308228086Z | 819.7999877929690 | 666.2000122070310 |
| 2024-02-23T00:27:03.422177734Z | 819.7999877929690 | 665.7999877929690 |
| 2024-02-23T00:27:19.556141981Z | 33.29999923706060 | 665.7999877929690 |
| 2024-02-23T00:27:39.562747806Z | 33.5 | 25.5 |
| 2024-02-23T00:27:59.575034211Z | 34 | 25.399999618530300 |
| 2024-02-23T00:28:19.583631639Z | 33.5 | 25.5 |
| 2024-02-23T00:29:39.617700076Z | 33.599998474121100 | 25.399999618530300 |
| 2024-02-23T00:29:59.623955856Z | 33.70000076293950 | 25.299999237060500 |
| 2024-02-23T00:30:39.960013182Z | 33.79999923706060 | 25.200000762939500 |
| 2024-02-23T00:30:59.661877726Z | 33.900001525878900 | 25.100000381469700 |
| 2024-02-23T00:31:39.685076624Z | 34 | 25.200000762939500 |
| 2024-02-23T00:31:59.701111112Z | 86.5999984741211 | 25.100000381469700 |
| 2024-02-23T00:32:19.903859517Z | 81.30000305175780 | 26 |
| 2024-02-23T00:32:39.715065425Z | 60.20000076293950 | 26.200000762939500 |
| 2024-02-23T00:32:59.728030558Z | 38.79999923706060 | 25.799999237060500 |
| 2024-02-23T00:33:19.75402825Z | 36.79999923706060 | 25.5 |
| 2024-02-23T00:33:40.191138091Z | 36.29999923706060 | 25.399999618530300 |
| 2024-02-23T00:33:59.768802624Z | 36 | 25.200000762939500 |
| 2024-02-23T00:34:19.785873899Z | 35.79999923706060 | 26 |
| 2024-02-23T00:34:39.792169472Z | 35.70000076293950 | 27.799999237060500 |
| 2024-02-23T00:34:59.801103872Z | 35.599998474121100 | 25.799999237060500 |
| 2024-02-23T00:35:20.131639357Z | 71.80000305175780 | 25.700000762939500 |
| 2024-02-23T00:35:39.81817694Z | 95 | 25.5 |
| 2024-02-23T00:35:59.847205574Z | 58.5 | 25.299999237060500 |
| 2024-02-23T00:36:19.842703549Z | 39.5 | 25.200000762939500 |
| 2024-02-23T00:36:40.004774028Z | 37.099998474121100 | 25.100000381469700 |
| 2024-02-23T00:36:59.862867658Z | 36.400001525878900 | 25.200000762939500 |
| 2024-02-23T00:37:19.872705943Z | 36.099998474121100 | 25.100000381469700 |
| 2024-02-23T00:37:39.883085759Z | 36 | 25 |
| 2024-02-23T00:37:59.908612733Z | 35.79999923706060 | 25.100000381469700 |
| 2024-02-23T00:38:20.357643565Z | 35.599998474121100 | 24.899999618530300 |
| 2024-02-23T00:38:39.913532292Z | 35.5 | 25.200000762939500 |

## 3. Arduino Boilerplate Code

/\*

Sketch generated by the Arduino IoT Cloud Thing "MKR WiFi 1010 and DHT22"

https://create.arduino.cc/cloud/things/e75efe13-eb5e-432a-86d3-0bf1cd34aaac

Arduino IoT Cloud Variables description

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

CloudTemperatureSensor temperature;

CloudRelativeHumidity humidity;

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 <Adafruit\_Sensor.h>

#include <DHT.h>

#include <DHT\_U.h>

#define DHTPIN 7 // Digital pin connected to the DHT sensor

#define DHTTYPE DHT22 // Write DHT11 or DHT22 According to your Sensor

DHT\_Unified dht(DHTPIN, DHTTYPE);

uint32\_t delayMS;

unsigned long previousMillis = 0;

const long interval = 20000; //milliseconds total time for 20 Seconds

void setup() {

// Initialize serial and wait for port to open:

Serial.begin(9600);

// This delay gives the chance to wait for a Serial Monitor without blocking if none is found

delay(1500);

// Defined in thingProperties.h

initProperties();

// Connect to Arduino IoT Cloud

ArduinoCloud.begin(ArduinoIoTPreferredConnection);

/\*

The following function allows you to obtain more information

related to the state of network and IoT Cloud connection and errors

the higher number the more granular information you’ll get.

The default is 0 (only errors).

Maximum is 4

\*/

setDebugMessageLevel(2);

ArduinoCloud.printDebugInfo();

dht.begin(); //Init DHT

Serial.println(F("DHTxx Unified Sensor Example"));

// Print temperature sensor details.

sensor\_t sensor;

dht.temperature().getSensor(&sensor);

Serial.println(F("------------------------------------"));

Serial.println(F("Temperature Sensor"));

Serial.print (F("Sensor Type: ")); Serial.println(sensor.name);

Serial.print (F("Driver Ver: ")); Serial.println(sensor.version);

Serial.print (F("Unique ID: ")); Serial.println(sensor.sensor\_id);

Serial.print (F("Max Value: ")); Serial.print(sensor.max\_value); Serial.println(F("°C"));

Serial.print (F("Min Value: ")); Serial.print(sensor.min\_value); Serial.println(F("°C"));

Serial.print (F("Resolution: ")); Serial.print(sensor.resolution); Serial.println(F("°C"));

Serial.println(F("------------------------------------"));

// Print humidity sensor details.

dht.humidity().getSensor(&sensor);

Serial.println(F("Humidity Sensor"));

Serial.print (F("Sensor Type: ")); Serial.println(sensor.name);

Serial.print (F("Driver Ver: ")); Serial.println(sensor.version);

Serial.print (F("Unique ID: ")); Serial.println(sensor.sensor\_id);

Serial.print (F("Max Value: ")); Serial.print(sensor.max\_value); Serial.println(F("%"));

Serial.print (F("Min Value: ")); Serial.print(sensor.min\_value); Serial.println(F("%"));

Serial.print (F("Resolution: ")); Serial.print(sensor.resolution); Serial.println(F("%"));

Serial.println(F("------------------------------------"));

// Set delay between sensor readings based on sensor details.

delayMS = sensor.min\_delay / 1000;

STHAM();

}

void loop() {

ArduinoCloud.update();

// Your code here

unsigned long currentMillis = millis();

if (currentMillis - previousMillis >= interval) {

STHAM();

previousMillis = currentMillis;

}

}

void STHAM(){

// Get temperature event and print its value.

sensors\_event\_t event;

dht.temperature().getEvent(&event);

if (isnan(event.temperature)) {

Serial.println(F("Error reading temperature!"));

//Assign temperature value 0 to Cloud Variable

temperature=0;

}

else {

Serial.print(F("Temperature: "));

Serial.print(event.temperature);

Serial.println(F("°C"));

//Assign temperature value to Cloud Variable

temperature=event.temperature;

}

// Get humidity event and print its value.

dht.humidity().getEvent(&event);

if (isnan(event.relative\_humidity)) {

Serial.println(F("Error reading humidity!"));

//Assign humidity value 0 to Cloud Variable

humidity=0;

}

else {

Serial.print(F("Humidity: "));

Serial.print(event.relative\_humidity);

Serial.println(F("%"));

//Assign humidity value to Cloud Variable

humidity=event.relative\_humidity;

}

}

/\*

Since Temperature is READ\_WRITE variable, onTemperatureChange() is

executed every time a new value is received from IoT Cloud.

\*/

void onTemperatureChange() {

// Add your code here to act upon Temperature change

}

/\*

Since Humidity is READ\_WRITE variable, onHumidityChange() is

executed every time a new value is received from IoT Cloud.

\*/

void onHumidityChange() {

// Add your code here to act upon Humidity change

}

## 4. GitHub Repository

<https://github.com/PMcTwist/IoT_Project>

A screenshot of a computer

Description automatically generated