MIDLANDS STATE UNIVERSITY

FACULTY OF SCIENCE AND TECHNOLOGY

DEPARTMENT OF COMPUTER SCIENCE

Reg. Number:	R153509R
Name:	Nyasha Marambire
Level:	4.2
M.O.E:	Conventional
Module Name:	Dissertation
Module Code:	HCS 401
Title:	Data Center Watchdog
Year:	2019

ABSTRACT

The past decade has been characterised by many firms migrating to clouding services which are powered by data centers. This led to a vast growth rate in the number of data centers in the world and as a result data centers became the most energy consuming facilities. Researches conducted by different scholars reflected that these energy consumptions can be reduced by using free cooling in data centers and raising the data center operating temperatures but however both methods result in an increased rate or probability of occurrence of hotspots. It therefore follows that a mechanism to quickly detect hotspots and reduce their impact was required to be put in place and this research focused on development of an Arduino based data center watchdog system written in C and C++ that could continuously monitor the rack inlet temperature and humidity levels as well as protect the equipment in the affected racks. The watchdog was successfully developed and it was recommended that before deploying it the technicians should first do CFD calculations in order to account for temperature variations as well as installing DHT22 in every rack in order for all rack temperature and relative humidity values to be accounted for. In the future it is recommended that the system be interlinked with cooling system in order to allow it to automatically calibrate the cooling system variables.

DECLARATION

I, **Nyasha Marambire,** hereby declare that I am the sole author of this dissertation. I authorize the **Midlands State University** to lend this dissertation to other institutions or individuals for the purpose of scholarly research.

Signature: ……………………………………………. Date: ………………………………..

APPROVAL

This dissertation, entitled **“Data Center Watchdog”** by **Nyasha Marambire** meets the regulations governing the award of the degree of **BSc Honours Computer Science** of the **Midlands State University,** and is approved for its contribution to knowledge and literary presentation.

Supervisor’s Signature: ……………………………. Date: ……………………

ACKNOWLEDGEMENTS

First and foremost I would like to thank God for the gift of life and for giving me the strength to pull through up to the end of this research. Secondly I would like to thank my supervisor Ms B. Mugoniwa for the excellent supervision and guidance throughout the research. I would also like to thank my family for the unending support and encouragement. I also want to thank my friends Sharon, Phiniel, Courage, Shaun, Tanaka and Martin for the support and playing a pivotal role in helping to procure resources required for making the research a success.

DEDICATION

To my dear mother Mrs F Marambire, my brother Mr D. Marambire and my sister Mrs T. Dzimbanhete, to whom without, this research would have been a failure, since it is their unending love and support throughout during the course of my tertiary education that drove me to succeed.

TABLE OF CONTENTS

LIST OF ACRONYMS

IDE – Integrated Development Environment

GSM – Global System for Mobile Communications

IaaS – Infrastructure as a Service

CFD – Computational Fluid Dynamics

ESD – Electrostatic Damage

MW - Mega Watt

LIST OF FIGURES

LIST OF TABLES

LIST OF APPENDICES

CHAPTER 1: INTRODUCTION

1.1 INTRODUCTION

This chapter focuses on giving the reader an insight of the background of the research, a clear definition of the problem that was at hand, the aim and objectives of the research as well as the data gathering methods and instruments that were used during the course of the research. This chapter also takes into account the budget and project time plan of the research and also gives a justification for continuing with the research. This chapter also serves to give the reader detail on how a data center watchdog was a stepping stone towards addressing the problem as well as promoting green sustainable IT.

1.2 BACKGROUND OF RESEARCH

Over the past decade notable changes in computing can be observed as many enterprises migrated from client-server architectures to distributed computing. This resulted in many innovative business models with cloud computing being in the midst of most of them. Fehling etal (2014), state that is due to the ability of cloud computing to enable firms to shift capital expenditures of procuring IT equipment to operational expenses of receiving IaaS which can be increased or decreased flexibly depending on the current requirements. Due to the advancements in cloud computing, enterprises as well as individuals are able to receive computing services such as storage and processing on ad hoc as-per-needed basis from the cloud at cheaper costs. Apart from enabling users to get computing power at lower costs the rise and widespread adoption of clouding was a monumental movement in green computing since cloud service providers have more energy efficient equipment due to strict server policies. For example according to Larrson (2012), Facebook changes its servers after every three years for new modern alternative equipment.

As a result of the widespread adoption of cloud computing, there were also notable changes in the growth rate of data centers which serve as the backbone of the cloud and these data centers consume large amounts of energy with most of the energy being consumed by cooling systems. This led to researches that resulted in the emerging of various air management and containment strategies with the commonly used strategy being the Hot Aisle containment. Hwaiyu and Geng (2014), states that the hot aisle containment strategy was primarily developed to compartmetise the hot air and it provided significant energy saving benefits in comparison with other strategies which allowed exhaust air from one server to flow into the inlet of an adjacent server. Up to date most data center technicians use the hot aisle containment in conjunction with a number of recommended practices such as blanking panels to ensure proper cooling and support the realisation of green IT.

Further researches were undertaken and they reflected that more energy could be saved through raising the operating temperature levels or switching to floating operating temperatures in the data center facility. Basing on the second law of thermodynamics, Geng (2012), stated that heat could not spontaneously flow from one colder region to a hotter one hence work is required to be done implying that the colder the data center the more work that will need to be done to move the air hence the server fans will do more work in drawing the air thereby resulting in high energy consumptions than in warmer data centers. Practical evidence was provided by Brown (2016) in a white paper titled “The Unexpected Impact of Raising Data Center Temperatures” where they ran tests on three data centers in different locations to confirm whether raising a data center’s operating temperature would result in energy savings whilst guaranteeing optimum performance and they found out that switching to floating operating temperatures resulted in energy savings as high as 13%. Geng (2012), continued to support the idea that running a data centers at warmer temperature saves energy by stating that if the temperature levels are warmer, the energy consuming compressor cooling equipment and chillers will run at reduced capacity and leave the cooling load to the economizer which was developed to save energy in cooling systems.

Apart from raising temperature set points or switching to floating operating temperature levels, another breakthrough made by researchers on energy savings in a data center was the rise of free cooling. Larsson (2012), defines free cooling as an energy saving cooling method which utilises naturally cold water from lakes or rivers to cool data center equipment. An example of a free cooling system is See Cooling and according to Larsson (2012), after deploying the one of the See Cooling systems at the Royal Institute of Technology in Stockholm, a PUE of 1.12 was observed. Larrson (2012), also states that the resultant energy savings from a 1MW processing capacity data center can be as high as 2300MWh annually if free cooling is deployed in that datacenter.

However raising data center operating temperatures or switching to floating temperatures or resorting to free cooling is associated with an increase in the occurrence of hotspots which makes the adoption of the greener cooling methods become a problem. This is backed by Dai etal (2013), who state that when free air cooling is used, due to seasonal climatic changes, the operating temperatures might rise and exacerbate already existing minor hotspots. A hot spot/cold spot is a spot in a server cabinet with unfavorable tightly focused temperature levels. Hotspots are dangerous to servers as it leads to unreliability of equipment as well as leads to equipment failure.

So as to avoid the complications of data center hotspots, technicians prefer to run at cooler and safer temperatures thereby making the data center to have a higher PUE and leave a larger carbon footprint. Mehdi (2014), states that the addressing of hotspots is possible through the application of CFDs but however due to the inability of the method to quickly detect hotspots before the affected equipment is damaged, the common approach that is used by most data center personnel is throwing more cooling at the entire environment which is not cost effective and also results in energy consumption and lowers a data center PUE score.

Therefore so as to re-assure the data center technicians and promote sustainable Information Technology or green IT there was need to implement vigilant data center watchdogs in the racks that do not only keep watch for hotspots in real time and alert data center technicians but rather an agent with the fore-mentioned capabilities as well as capable of shutting down the affected server so as to protect it.

1.3 PROBLEM DEFINITION

The proposed data center watchdog was an agent based system which targeted at addressing the issue of quick detection of data center hotspots and relaying the issue to the technicians as well as protecting the equipment affected by the hotspot. Mackworth and Poole (2010), defined an agent as something that acts in an environment which is the rack in the case of the data center watchdog.

The problem scope that was to be addressed was based on the fact that temperature levels at the inlet of a server should lie in between a set range and any readings that falls above or below that range is either a hotspot or a coldspot respectively.

As such, the problem defined seemed feasibly addressable by the development of a data center watchdog which when fully operational could result in data center technicians raising their facility operating temperatures drastically causing a reduction in cooling system related energy usage thereby promoting green IT due to reliability of the watchdog to quickly detect hotspots and handle them in an effective novel way.

The catering for each problem stated above was done through DHT22 shields for measuring temperature and humidity and a GSM module for alerting the data center technicians via SMS platform and relay modules for shutting down the affected equipment to protect it. Status LEDs were be put in place to draw the attention of the data center technicians

1.4 AIM

Berddtsson etal (2007), defined the aim as a short clear unambiguous statement that describes the overall goal of the research.

The aim of the research was to develop a vigilant data center watchdog that is capable of quickly detecting hotspots, alerting technicians of the issue and protect equipment from damage.

1.5 OBJECTIVES

Ahmed (2016) stated that every research should have a set of clear well defined objectives that should be met for the project to be deemed a success and if any of the objectives is not met the research will be deemed a failure.

The objectives of the research were to develop a data center watchdog that:-

- ❖ Monitors temperature and humidity levels at the server inlet in real time.
- ❖ Alerts data center technicians as soon as temperature levels rises above specified ranges set by the data center technicians through SMS platform.(i.e. if a hotspot is detected or if extreme temperatures are detected.)
- ❖ Shuts down the affected server as a protection measure if extreme temperatures are detected after a waiting period set by the data center technicians.

1.6 METHODS AND INSTRUMENTS

This section refers to the methodologies that were used during the research to obtain knowledge about the research topic as well as knowledge to help with tailoring the data center watchdog as well as the tools that were used to build the system.

1.6.1 DATA COLLECTION TOOLS

The tools used during the course of the research are:-

- ❖ Academic Papers.
- ❖ The internet.

- Textbooks.
- Newspapers.

1.6.2 INSTRUMENTS USED IN SYSTEM CREATION

The following instruments were used to create the watchdog:-

- Codeblocks – It is the platform that was used to develop the watchdog’s class libraries.
- Arduino IDE – It is the platform that was used to write the program on to the Arduino micro controller board as well as other parts of the code.
- C++ - It is a programing language that facilitates object oriented programming that is used to write compiled applications which can be executed quickly by a computer system and for that reason, it was used to develop the data center watchdog’s code libraries.

1.7 BUDGET

Table 1.1 Budget for Components required.

Quantity	**Description**	**Item Price (RTGS)**	**Item Supply**
1	UNO R3 (Arduino)	$45.00	Netro Electronics Zimbabwe
1	DHT 22	$21.00	Netro Electronics Zimbabwe
1	GSM Module	$5.00	Netro Electronics Zimbabwe
1	Breadboard	$ 7.50	Netro Electronics Zimbabwe
1	Breadboard jumper wires	$7.50	Netro Electronics Zimbabwe
1	Relay Module	$ 6.00	Netro Electronics Zimbabwe
3	LEDs	$3.00	Netro Electronics Zimbabwe
	Total:	**$95.00**	

1.6 RESEARCH TIME PLAN

Berddtsson etal (2007), stated the purpose of a time plan as a tool to give the researcher a clear understanding of the relationship between project activities and the time needed for each activity.

Phase	Week					
	1	2	3	4	5	6
Introduction	■					
Literature Review		■	■			
Theoretical Analysis			■	■		
Design					■	
Conclusion						■
Documentation	■	■	■	■	■	■

Figure 1.1: Research Time Plan

1.9 JUSTIFICATION

The problem identified seemed addressable through the development of a data center watchdog. The watchdog would act just like a domestic dog that watches over our homes, barks to alert us when intruders are within premises and if we do not show any response it bites the intruder so as to safeguard the home. With context to the data center, the data center watchdog if fully implemented would monitor the data center environment on a 24 hour 7 days a week basis and alert the data center technicians about any abnormalities.

The data center watchdog system was successfully developed and it quickly detected hotspots in the data center as well as gave the technicians ample time to resolve the malfunctions. This instilled some degree of confidence in the technicians to raise their data center operating temperatures and switch to free cooling due to reliability of the autonomous sharp-eyed monitoring capabilities of the watchdog therefore results in energy savings were expected.

Apart from that, the watchdog system was an agent based system that shut down the equipment affected by the hotspot as a protective measure to protect the equipment on behalf of the technicians thereby placing the facilities in a position where they stood to cut risks of incurring heavy costs of replacing equipment damaged by extreme temperature levels. Besides that, through shutting down the racks, the watchdog did not only protect the equipment but also increased its fault tolerance significantly causing an increment in the data center's performance.

1.10 CONCLUSION

The conclusion can be defined as a chronological end of any discussion and serves to reflect the final arguments. This chapter highlighted the activities that were undertook so as to complete the research and deliver the required watchdog. It also clearly outlined what a data center is, its importance, and the benefits of raising the operating temperature in a data center along with the associated risks as well as how the implementation of the watch dog curbed the risks. The next chapter will be literature review which assessed whether if hotspot are really a threat to data centers.

CHAPTER 2: LITERATURE REVIEW

2.1 INTRODUCTION

Dawson (2009) defined literature review as a written representation of the critical conceptual and evaluations of materials found relating to the research being undertaken. Zobel (2015) suggested that research literature helps understand the current debates, theories and discoveries and can help identify new lines of questioning or investigations and should provide alternative perspectives on the author's work. According to Hart (2018), the purpose of a literature review is to provide the researcher with a body of knowledge which he or she can relate to his or her own findings and it also helps in the identification of what has been done and what is required to be done. In this chapter the author undertook an investigation to identify the existing works that have been made so as to aid data center technicians to detect hotspots in the data center. These existing works were compared against the proposed data center watchdog so as to assess its importance and the competitive advantages that data center technicians stand to benefit from using the watchdog. Also foreknowledge prior to the development of the data center watchdog was acquired from the investigations carried out during this chapter. It also gave a picture of how the data center watchdog is a stepping stone towards achieving Green IT.

2.2 DATA CENTER HOTSPOTS AND THEIR IMPACT IN DATA CENTERS

Data center hotspots are one of the most feared threats because they can silently creep up without drawing the technicians' attention until their impact becomes serious. A hotspot/coldspot is a spot in a server cabinet with unfavorable tightly focused temperature levels. Data center hotspots can go unrecognized until the equipment in the affected spot begins to get damaged, there are increases in system outages as well as massive energy wastages.

According to Mehdi (2014), one of the primary causes of hotspot is an insufficient volume of conditioned airflow at the server inlet and the addressing of hotspot is possible through the application of CFDs. Mehdi (2014), also states that an investigation carried out at Uptime Institute exposed that vertical hotspots occur because the internal fans within the computing equipment at the bottom of the cabinet would have consumed all the supply coming from the nearby perforated tiles and with no cool air remaining, the computing equipment at the upper racks of the cabinet ends up pulling hot exhaust air of the adjacent equipment.

Hwaiyu and Geng (2014), also suggested that free cooling has a down side of causing temperature and moisture content swings during the year as seasons change. Dai etal (2013), supported this by stating that in order to guard against corrosion related failure, relative humidity levels should be kept in between 40 to 60% basing on ASHRAE guidelines and using a method such as free cooling would be a challenge due to the uncontrollable temperature and humidity levels of the cooling body (for example temperature levels in a lake) being used to provide the cooling effect on the air which will be supplied to the data center. Due to the seasonal fluctuations in the outside world climatic conditions, it could be concluded that incorporating greener cooling methods results in increased hotspot occurrences hence a mechanism to quickly identify hotspots, alert the technicians of the occurrence of a hotspot so as to allow them calibrate their cooling system variables to match the cooling requirements and avoid the impact of hotspots is needed.

2.3 RELATED WORK DEVELOPED TO ADDRESS HOT SPOT DETECTION

Zobel (2015) defined related work as work that has been undertaken by other researchers and has been published by a reputable body or organisation. Dawson (2009) also defined related research as work, publications and research related to the given topic.

2.3.1 DATA CENTER TEMPERATURE-INDICATING BLANKING PANELS

The easiest and cost effective way to detect data center hot spots through the use of temperature-indicating blanking panels. A typical temperature indicating blanking panel is made up of a heat sensitive multi-colored strip that facilitates temperature monitoring through providing a visual indication of inlet air temperatures. An example of temperature-indicating blanking panels is Upsite’s HotLok ® Blanking Panels which are snap-in blanking panels which make use of colour codes to represent cabinet inlet temperature ranges. These blank panels are designed to fit in 1U and 2U openings and also have an added benefit of their capability to control airflow so as to ensure effective and optimised cooling.

However the blanking panels lack convenience in the sense that they require the technicians to manually check the blanking panels consistently and would not be useful in the absence of a technicians. Apart from that, a typical data center will consist of several racks which makes checking the blanking panels a tiresome process. Also the blanking panels lack the ability to offer real time alerts as well as the capability to protect the exposed equipment.

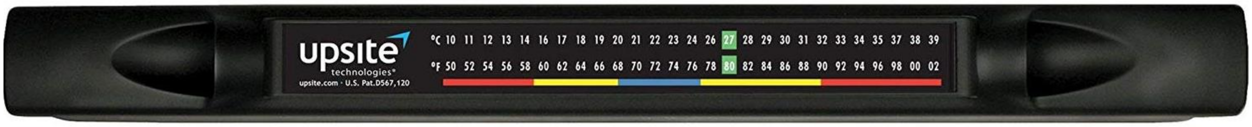

upsite
technologies®
upsite.com · U.S. Pat.D567,120
°C 10 11 12 13 14 16 17 18 19 20 21 22 23 24 26 27 28 29 30 31 32 33 34 35 37 38 39
°F 50 52 54 56 58 60 62 64 66 68 70 72 74 76 78 80 82 84 86 88 90 92 94 96 98 00 02

Figure 2. 1: HotLok temperature indicating blanking Panel

Advantages

- ✓ Provide visual representation of inlet temperature ranges.
- ✓ Does not consume any power.
- ✓ Readily available.

Disadvantages

- × Does not provide real time alerts
- × Not capable of protecting the exposed equipment
- × Needs consistent checking of strips which is tiresome
- × Requires too much human input

2.5 GAPS IDENTIFIED

The currently existing works required the technicians to regularly check the temperature indicating blanking panels and lacked the ability to notify the data center technicians of any irregularities. Also the blanking panels do not prevent the equipment from damage if no technician is around on premises to physically shutdown the affected server in order to protect it from electrostatic damages or short circuiting due to the abnormal temperature and humidity levels.

A data center watchdog could fill in the gap through its capabilities of monitoring inlet temperatures in real time, issuing out real-time SMS alerts of hotspots detected and its ability to protect the exposed equipment through physically shutting it down.

2.6 DATA CENTER HOT SPOT DETECTION USING DATA CENTRE WATCHDOGS

Hwaiyu and Geng (2014), defined monitoring temperature levels at each rack as an efficient method of identifying air management problems. The proposed data center watchdog system would facilitate hotspot detection through vigilantly monitoring the rack input air temperature and humidity levels in real time then alerting the technicians via SMS if the relative humidity and temperature levels fell below or above a specified range. As an added capability if the temperature and humidity levels rose above the extreme temperature ranges set, the data center watchdog would shut down the server exposed to the extreme temperatures levels so as to avoid further damages to the equipment thereby saving the organisation from incurring any further costs. Also the data center watchdog was set to be an autonomous agent and will therefore require little human intervention during its operation.

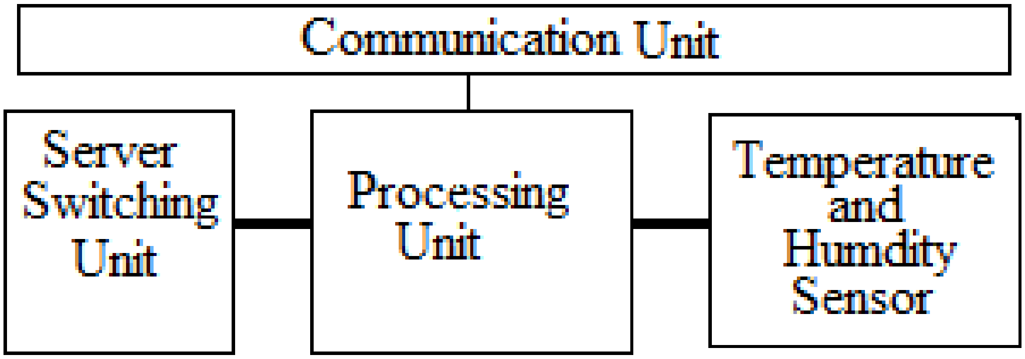


Figure 2. 2: Proposed Data Centre Watchdog Conceptual Representation

Advantages

- ✓ Ability to continuously monitor temperature and relative humidity levels in real time on a 24/7 basis.
- ✓ Able to quickly detect hotspots.
- ✓ Able to issue real time alerts in form of SMSes.

- ✓ Able to protect equipment from further damage through shutting down the exposed equipment.
- ✓ Little human intervention required.
- ✓ Idea is still new hence will offer competitive advantage

Drawbacks.

- × It make use of some open source libraries hence an expert might be able to exploit.
- × Idea still new hence might it is prone to errors

2.6 FOREKNOWLEDGE

The implementation of the data centre watchdog required less foreknowledge on working with the Arduino microprocessor board. Arduino based projects and libraries are usually open sourced hence knowledge to give the developers know how of how certain hardware components function and examples were readily available on the internet. The development of the data centre watchdog was sorely based on the Arduino microprocessor board and hardware shields due to their ability to allow quick and easy simulation. Apart from that, the data centre watchdog's firmware was to be written in C and C++, therefore a good background in the two languages was a necessity as well as a good background in electronics as there was interlinking of the various components that would make up the system.

2.7 CONCLUSION

This chapter gave a review of what hotspots are, how they affect data center equipment as well as how hotspots are a major drawback towards achieving green IT. Also this chapter outlined how the data center watchdog was an ideal solution for quick hotspot detection and protection of equipment from hotspots. The next chapter focused on giving a theoretical information of the components that make up watchdog.

CHAPTER 3: THEORETICAL INFORMATION

3.1 INTRODUCTION

This chapter focused on discussing the components that were to be used in the development of the data center watchdog. The discussion seeked to expose the components' underlying workings so as to give the reader a better understanding of how the components function. The components that were used in the project comprised of an arduino UNO R3, a DHT sensor, a relay Module, a GSM module, a breadboard and jumper cables.

3.2 COMPONENTS TO BE USED

The following sections are aimed at giving the reader an overview of the components that were used in the construction of the data center watchdog and an insight of their internal workings. The components used comprised of a microcontroller board, a DHT sensor, GSM module and relay shield.

3.2.1 ARDUINO UNO R3 BOARD

The Arduino Uno is an ATmega328P microcontroller based microcontroller board. Geddes (2014), defined the Arduino UNO as a small computer that can be programmed using C language via the Arduino IDE to connect and to control various physical objects. Singh etal (2014), also described the Arduino as a low cost, user friendly open source platform that has an onboard microcontroller. It comprises of 14 digital pins which can work as either inputs of outputs. Of the 14 digital pins 6 pins support pulse width modulation. Besides digital pins, the UNO R3 board also has 6 analog inputs. Apart from the pins, on the board you will also find a DC power supply jack, a Universal Serial Bus Port, an ICSP header and others components such as resistors, quartz crystal, as well as push button for reset and capacitors required to support the AT328P microchip.

3.2.1.2 HOW IT WORKS

To use the Arduino you simply write the program you want to run on the Arduino board using the Arduino IDE and upload it to the board using the USB Port then simply connect it to a power supply adapter or power it through the USB port and it will start running the program.

3.2.1.3 TECHNICAL SPECIFICATIONS

Table 3. 1: Arduino UNO R3 Technical Specifications

Microcontroller	ATmega328P
Power Ratings	5V/7-9V 2mA
DC Current	20 mA (per I/O)
DC Current	50 mA (for 3.3V)
Flash Memory	32 Kbytes (0.5 Kbytes used by bootloader)
SRAM	2 Kbytes
EEPROM	1 Kbytes
Clock Speed	1600 Hz
Dimensions	53.4x68.6 mm

3.2.1.3 PINOUT

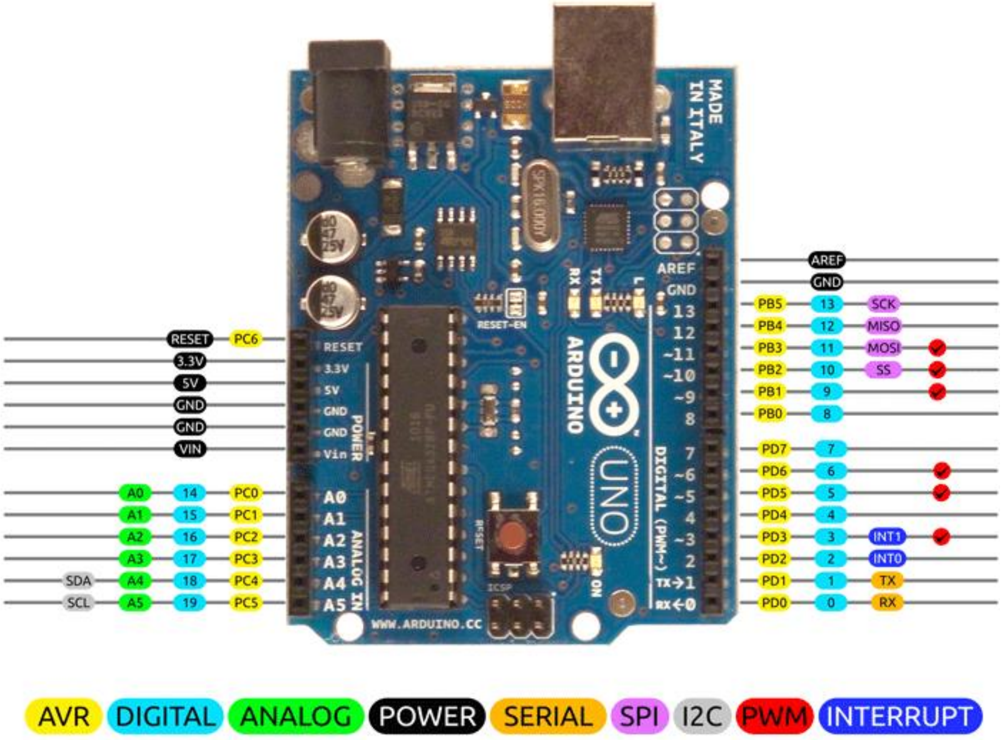


Figure 3. 1: Arduino UNO R3 Pinout Diagram

3.2.2 DHT 22 MODULE

The data center watchdog's input about the current relative humidity levels in its environment is fed in by a DHT22 sensor. According to Bosu and Choudhuri (2012), a sensor can be defined as an electronic device that senses some external stimuli for example heat or moisture. The DHT22 is a low-cost digital sensor that can reliably measure humidity and temperature levels whilst maintaining stability. However it has a limitation that it can only query temperature and humidity readings once in 2 seconds. Transmission of the temperature and humidity readings is fairly easy using any microcontroller.

3.2.2.2 PRINCIPLE OF OPERATION

The DHT 22 sensor is made up of three parts, a thermistor which is responsible for temperature measurement, a capacitive humidity sensor which is used to take the humidity measurements and a basic chip that performs the conversion of the analog measurements into digital readings. The chip is also responsible for serial transmitting the digital reading to a microcontroller for example in this instance the Arduino Uno R3.

Humidity Sensing Component

For measuring humidity the DHT 22 makes use of a capacitive humidity sensor. This capacitive sensor is made up of two electrodes with separated by a moisture holding substrate.

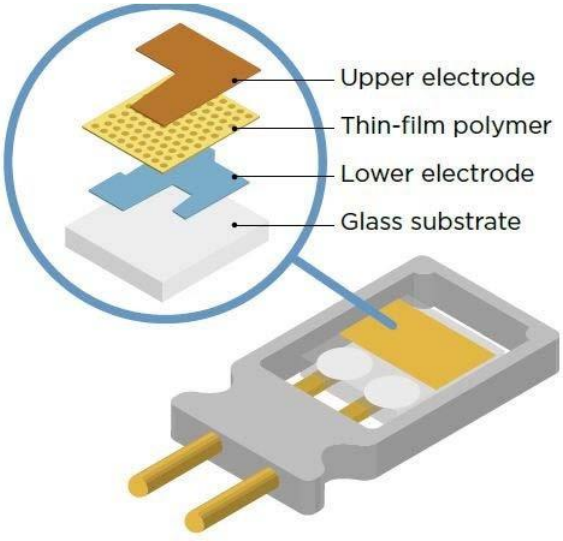


Figure 3. 2: Diagram of a typical Capacitive Humidity Sensor

During operation if humidity levels change, the conductivity of the substrate also changes. This implies that the resistance between the two electrodes also change. The change in the resistance is measured, by the IC then converted into a digital signal to prepare it for use by the microcontroller.

Temperature measuring component

The DHT 22 sensor makes use of a NTC thermistor sensor for the purpose of temperature measurement. A thermistor is a type of a variable resistor that changes resistivity as a result of a change in temperature surrounding it. These sensors are constructed through sintering semi conductive materials, for example ceramic or polymers so as to cause huge changes in a resistance in response to small temperature changes. When temperature changes, there will be a change in resistance and the IC will read the value of the resistance and convert it into a digital value then transmit it.

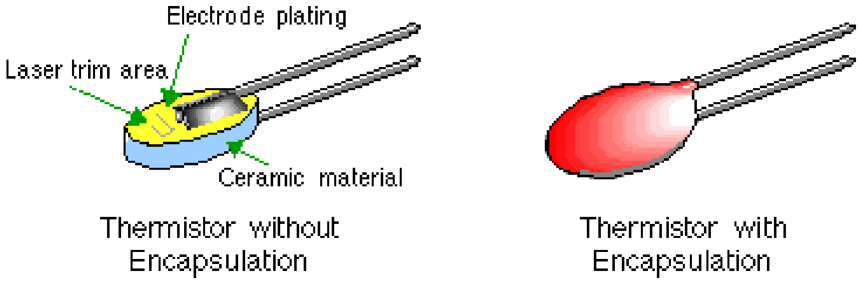

Electrode plating
Laser trim area
Ceramic material
Thermistor without Encapsulation
Thermistor with Encapsulation

Figure 3. 3: Illustration of a Thermistor

3.2.2.3 TECHNICAL SPECIFICATIONS

Table 3. 2: DHT22 Technical Specifications

Operating Voltage	3.5v to 5.5v
Max Current	2.5mA
Protocol	a serial transmission
Measuring Range	• Temperature (-40°C to 80°C) • Humidity (0% to 100%)
Precision	±0.5°C and ±1%
Sampling Rate	0.5 Hz once every two seconds
Dimensions	27 x 59 x 13.5mm

Pins	3 or 4

3.2.2.4 PINOUT

To get started with the module you simply have to connect the VCC to the first Pin from the left, the data cable from the Arduino board to the second pin from the left and lastly the ground cable to the pin on the extreme right.

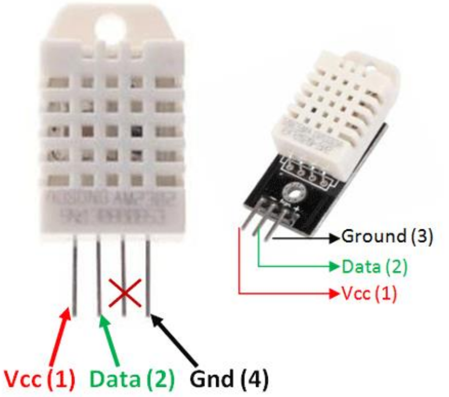


Figure 3. 4: DHT 22 Pinout Diagram

3.2.3 GSM MODULE

The SIM800L is a scaled down, quad band frequency cellular module that supports transmission of data packets through GPRS, sending and receiving SMSes or placing and receiving voice calls via GSM transmission. It has a relatively low cost and is capable of supporting long range connectivity

3.2.3.2 HOW IT WORKS

When connected to a power supply the module will boot up, then search for a cellular network to connect to and login automatically. The onboard LED acts as a status display to represent its connectivity state i.e. if there is no network coverage the LED will blink once every second and once every three seconds when its logged on to a network.

3.2.3.3 TECHNICAL SPECIFICATIONS

Table 3. 3 SIM800L Technical Specifications

Operating voltage	3.8V - 4.2V
Power consumptions	• sleep mode < 2.0mA • idle mode < 7.0mA • GSM transmission (avg): 350 mA • GSM transmission (peek): 2000mA
Supported frequencies	Quad Band (850 / 950 / 1800 /1900 MHz)
Interfaces	• UART (max. 2.8V) • AT commands
Antenna connector	IPX
SIM socket	microSIM
Dimensions	25 x 23 mm

3.2.3.3 PINOUT

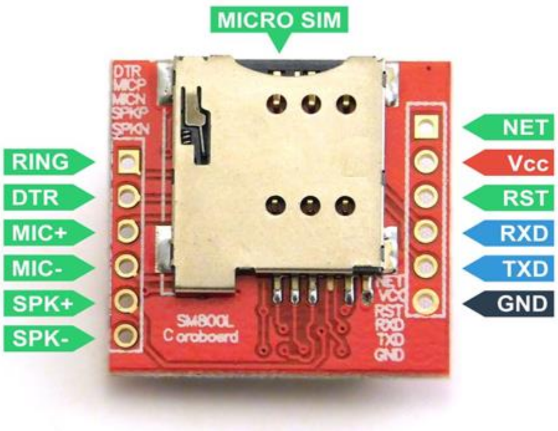


Figure 3. 5: SIM800L Pinout Diagram

3.2.4 ELECTRONIC RELAY MODULE

A relay is a switch that utilizes the principle of magnets and electro magnets to control circuits. A Relay is operated electronically by charging and discharging it. Padmanabhan K, (2006), differentiates relays from basic switches saying that basic switches require a mechanical force which is usually applied by a human to close or open a circuit whereas a relay utilizes magnetic forces to open or close circuits. The electromagnet requires a low voltage to drive it. We can control high voltage electronic devices using relays.

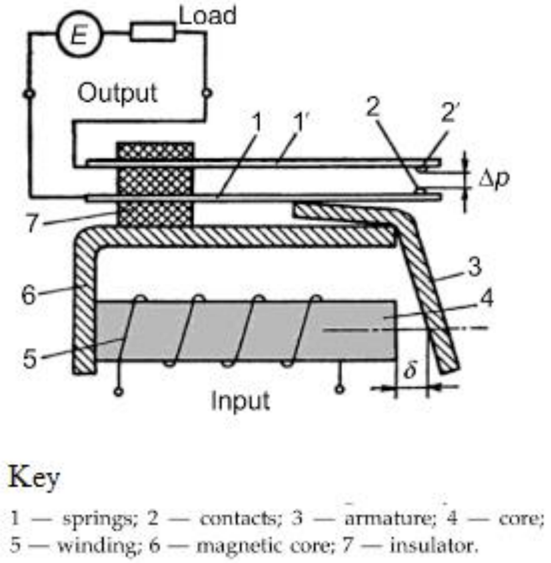

E
Load
Output
1
1′
2
2′
Δp
7
3
6
4
5
δ
Input
Key
1 — springs; 2 — contacts; 3 — armature; 4 — core;
5 — winding; 6 — magnetic core; 7 — insulator.

Figure 3. 6: Illustration of a simple Relay

3.2.4.2 PRINCIPLE OF OPERATION

Padmanabhan K, (2006) states that a relay is made up current carrying electromagnetic coil that is wound on a soft core magnet and when a voltage is applied to the coil, the coil exerts a magnetic force that moves the soft core magnet which in turn causes a mechanical force that will close the contacts together thereby closing or opening the circuit it is controlling depending on the configuration used. For example if you supply 5 volts from a microcontroller to the electromagnet, it will pull a contact to close or open a high voltage circuit depending on the way it is connected.

3.2.4.3 ARDUINO RELAY

Bosu and Choudhuri (2017), define an Arduino relay as a shield used to interface the microcontrollers which are DC powered for example AC powered devices using an arduino Uno. Hwaiyu and Geddes (2014), define a shield as an accessory that is readily available to add that functionality would require a certain circuit to be designed and eliminates the developers' overhead of having to design the circuit from ground up.

Bosu and Choudhuri (2017) state that the live wire of the power supply is connected to the COM Pin, then the live wire to the appliance is connected to the NO pin and the control signal pin is connected to an Arduino digital pin whilst the ground and VCC pins are connected to the Arduino GND and 5V pin respectively.

Arduino Relay modules are a solution for giving Arduino microcontrollers the capability of controlling high power circuits since the Microcontroller is unable to control them directly using digital input and output pins, due to the presence of high current and voltage in the circuit than the digital pins cannot sustain them. Relay shields are commonly available as 1, 2, 4 and 8 channel relays. Each relay has 2 pole changeover contacts namely the Normally Open (NO) and the normally closed (NC).It also has an LED that serves the purpose of indicating the on or off state the relay. It is driven by 5 volts.

Table 3. 4: Technical Specifications

Interfaces	Digital IO
Operating Voltage	5 V
Operating Current	35 mA

3.2.4.4 PINOUT

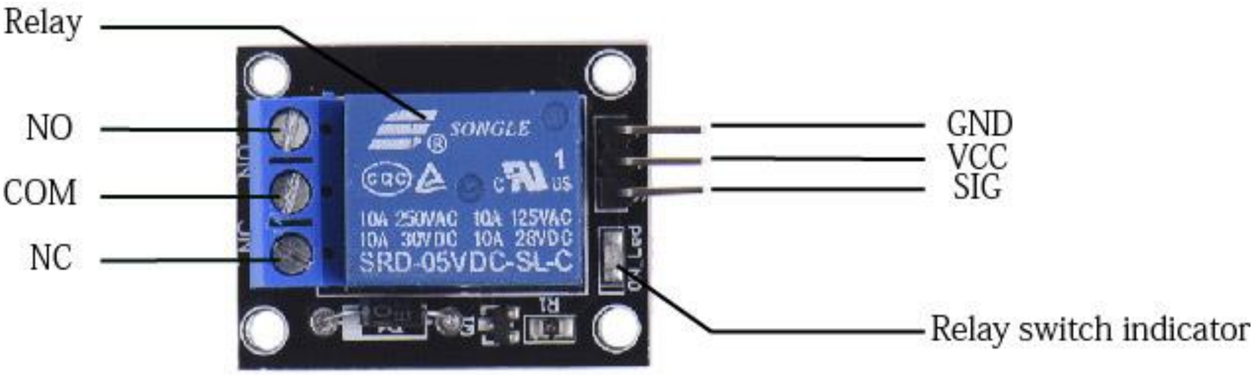


Figure 3. 7: Arduino Single Channel Relay module Pinout Diagram

3.2.5 BREADBOARD

This is a basic prototyping tool that provides a cheap and reusable connection base that is easy to connect. It is also known as a plug board due to its functionality that allows a circuit designer to simply plug in and connect components without the need to first solder them. For this project the developer used a 830 pin bread board.

Table 3. 5: Breadboard Technical Specifications

Number of Holes	830
Dimensions	165.1x54.6x8.5mm

Figure 3. 8: Breadboard

3.2.7 JUMPER CABLES

Jumper cables are simply copper wires that are coated with plastic for insulation and then soldered to a connector or tip to allow them to facilitate an easy way to connect components. They are widely used when making connections between a breadboard and another component as well as for connecting one component to the other. There are mainly three types of jumper cables which are male to male, male to female and female to female jumper cables. They also come in various colours and length sizes with the most common ones being 20cm long jumper cables and they are the ones that are going to be used in developing the data center watchdog.

Table 3. 6: Jumper Cable Technical Specifications

Type	Length
Male to female	20cm
Male to Male	20cm

Figure 3. 9: Jumper Cables

3.3 SCHEMATIC DIAGRAM OF THE DATA CENTER WATCHDOG

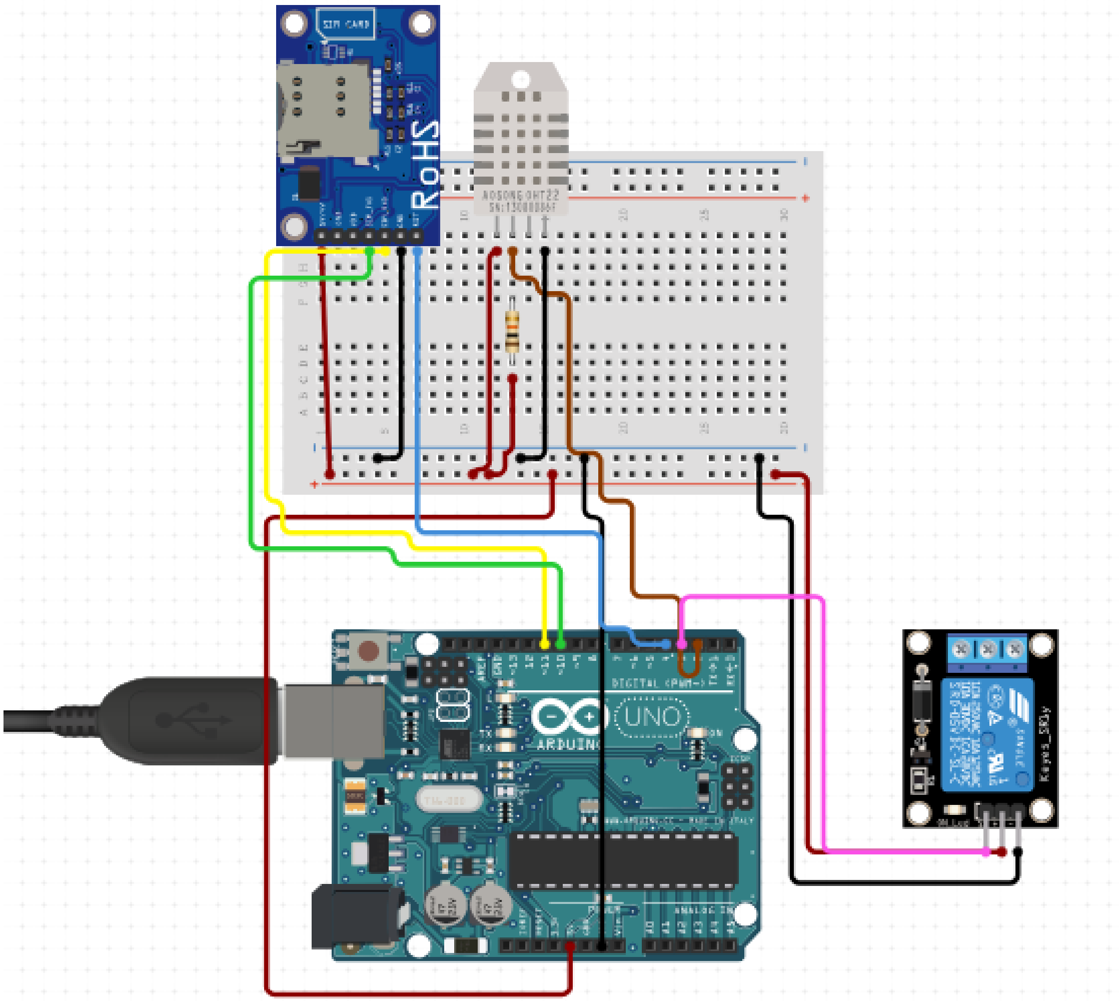


Figure 3. 10: Schematic Diagram of the Data Center Watchdog system

3.3 EXPLANATION OF WORKING OF THE DATA CENTER WATCHDOG

The data center watchdog is first configured and after configuration it would be in active state and ready for deployment. During configuration, the technicians will set the acceptable temperature and relative humidity ranges, the tolerated extreme temperature and relative humidity range, as well as the window period that the data center watchdog is allowed wait before shutting down the server.

After deployment the data center watchdog continuously monitor the temperature and relative humidity levels. If the temperature or relative humidity levels detected are out of the range set during configuration, within the set tolerable extreme temperature or relative humidity range, the data center watchdog will alert the technicians of a possible hotspot or coldspot and it will continue monitoring. If the temperatures continue to rise above, or fall below the tolerable range, the data center watchdog will notify the data center technician of the event and that it will shut down the equipment in the rack which it is deployed and will shut down the equipment. Power will be restored to the unit after temperatures are back in the normal temperature range and if the technician presses the reset button.

The DHT 22 module is responsible for collecting the temperature and humidity readings which are processed by the Arduino UNO. The SMSes is sent out using a GSM module and the relay will be responsible for cutting out power to the rack affected by the extreme temperatures.

3.4 THE DATA CENTER WATCHDOG SOFTWARE DESIGN

The data center watchdog is an Arduino based agent system that assists data center technicians with quick detection of hotspots and protection of equipment from the identified hotspots. The data center watchdog makes use of two libraries namely the DHT Library and the GSM library which are both open source and readily available on the internet. The rest of the firmware of the watchdog which gives it logic was coded using C programming language in the Arduino IDE. The syntax of C can be seen through the use of statements such as the #include statement which is used to import the specified library from the Arduino packages. The watchdog is an artificially intelligent agent system with no memory so as to make it a cheap and viable solution.

3.5 THE DATA CENTER WATCHDOG SYSTEM FLOW CHART

According to Davis and Yen (2019), “A system flowchart as a concrete, physical model that documents in an easily visualized, graphical form, the system discrete physical components (its programs, procedures, files, report, screen, etc.).”

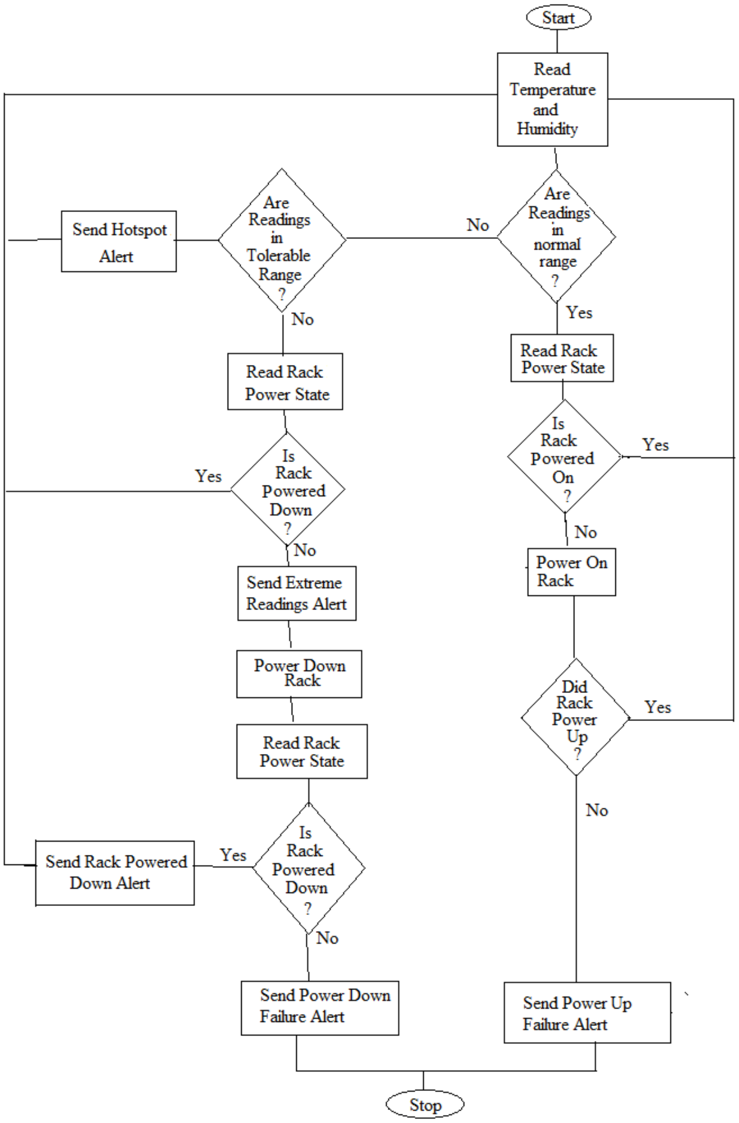


Figure 3. 11: Data Center Watchdog Flow Chart

3.6 CONCLUSION

This chapter outlined the theoretical information about the components that were used so as to give the reader comprehensive knowledge of the overview, principles of operation as well as the pinouts of the components. It also gave an illustration of the logic of the data center watchdog graphically through a flowchart. The following chapter was aimed at building the actual prototype of the data center watchdog, running simulated tests and implementing the data center watchdog.

CHAPTER 4: SIMULATION AND IMPLEMENTATION

4.1 INTRODUCTION

The previous chapters focused on extensively reviewing the data center watchdog's structure as well as exposing the functions and principles of operation of the various components which make up its build. This chapter focused on bringing the data center watchdog to life, running simulations to verify its functionality against its objectives as well as its implementation.

4.2 INTERFACING COMPONENT

Interfacing components refers to the process of physically connecting the various shields that make up the data center watchdog as well as executing a test code or sketch to validate the connections.

4.2.1 INTERFACING THE DHT 22 SENSOR MODULE

The DHT 22 Sensor used in the development of the data center watchdog is a 3 pin DHT 22 sensor which has an on board pull up resistor for current regulation. It uses UART to communicate via serial with the Arduino Uno. The Pin at the extreme left is the VCC Pin and the one next to it is the data pin and the pin at the extreme right is ground pin.

WIRING

Table 4. 1: Pin Connections

DHT22 Pins (starting from the left)	Arduino Pins
Pin 1-VSS Pin	5V power supply line on the breadboard.
Pin 3 – Data Pin	DI/O Pin 7
Pin 2 – GND Pin	GND Pin

CONNECTION SCHEMATIC

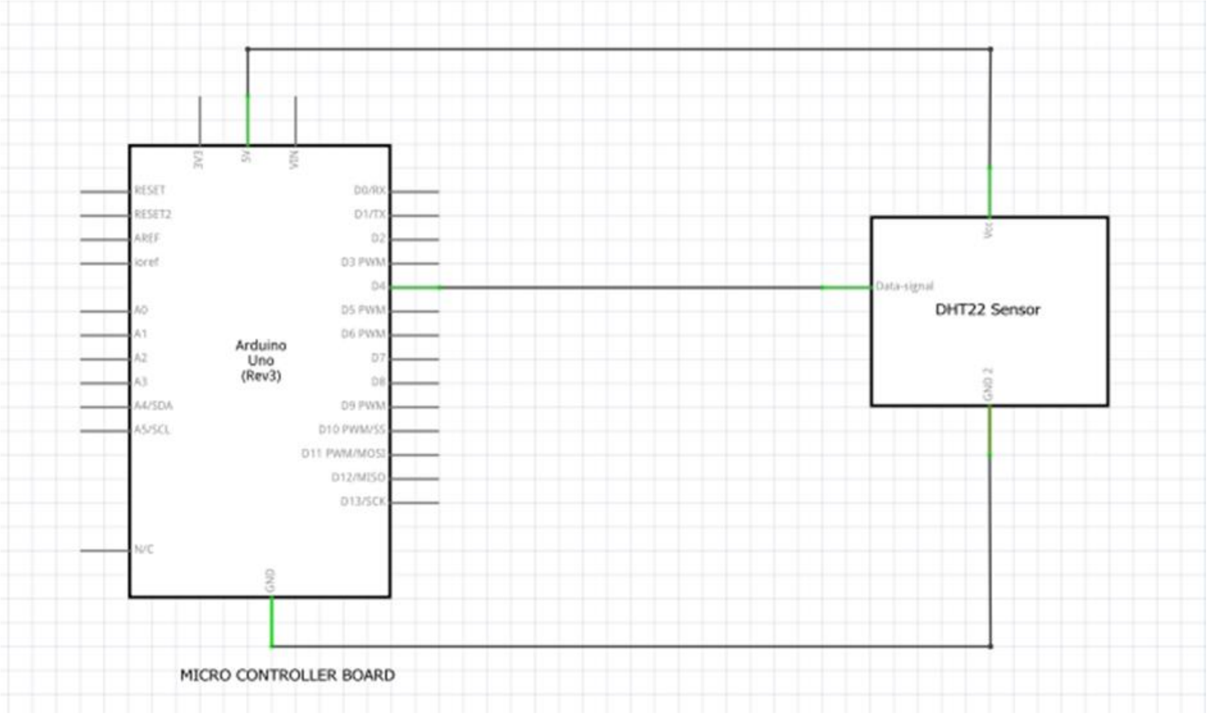
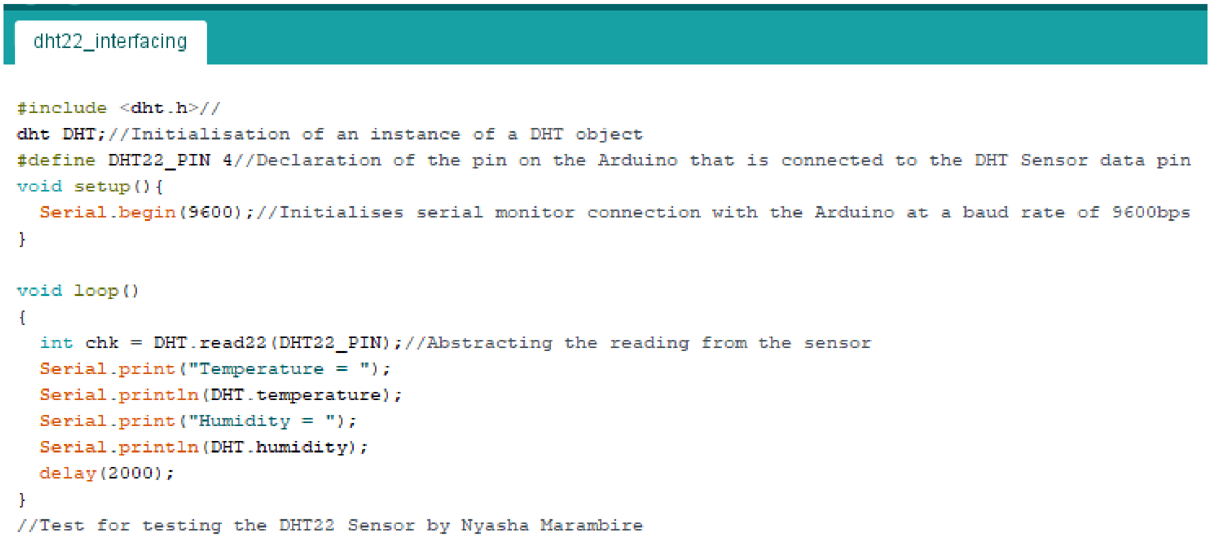


Figure 4. 1 Arduino and DHT22 Interfacing Schematic Diagram

TEST CODE

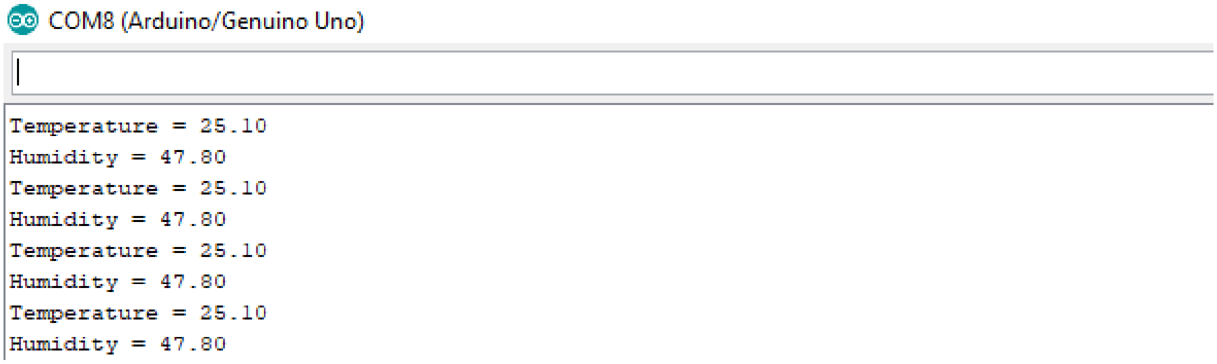


```
#include <dht.h>//
dht DHT;//Initialisation of an instance of a DHT object
#define DHT22_PIN 4//Declaration of the pin on the Arduino that is connected to the DHT Sensor data pin
void setup(){
  Serial.begin(9600);//Initialises serial monitor connection with the Arduino at a baud rate of 9600bps
}

void loop()
{
  int chk = DHT.read22(DHT22_PIN);//Abstracting the reading from the sensor
  Serial.print("Temperature = ");
  Serial.println(DHT.temperature);
  Serial.print("Humidity = ");
  Serial.println(DHT.humidity);
  delay(2000);
}
//Test for testing the DHT22 Sensor by Nyasha Marambire
```

Figure 4. 2: DHT22 interfacing test code

OUTPUT OF THE DHT22 MODULE INTERFACING



```
Temperature = 25.10
Humidity = 47.80
Temperature = 25.10
Humidity = 47.80
Temperature = 25.10
Humidity = 47.80
Temperature = 25.10
Humidity = 47.80
```

Figure 4. 3 Output illustrating a successful DHT22 interfacing

4.2.2 INTERFACING THE SIM800L MODULE

The SIM800L is a GSM Module that has at its heart a SIM800L GSM cellular chip manufactured by SimCom. The first revision had an operating voltage in the range from 3.4V to 4.4V but the latest revision has tolerance of 5V which makes it ideal to power it from the Arduino. In the construction of the Watchdog the latest revision of the SIM800L was used. It was interfaced with the Arduino using the RXD, TXD, VCC and GND were the only.

WIRING

Table 4. 2: Pin Connections

SIM800L PIN	ARDUINO
VCC	5V Pin
RXD	DI/O Pin 2
TXD	DI/O Pin 3
GND	GND Pin

CONNECTION SCHEMATIC

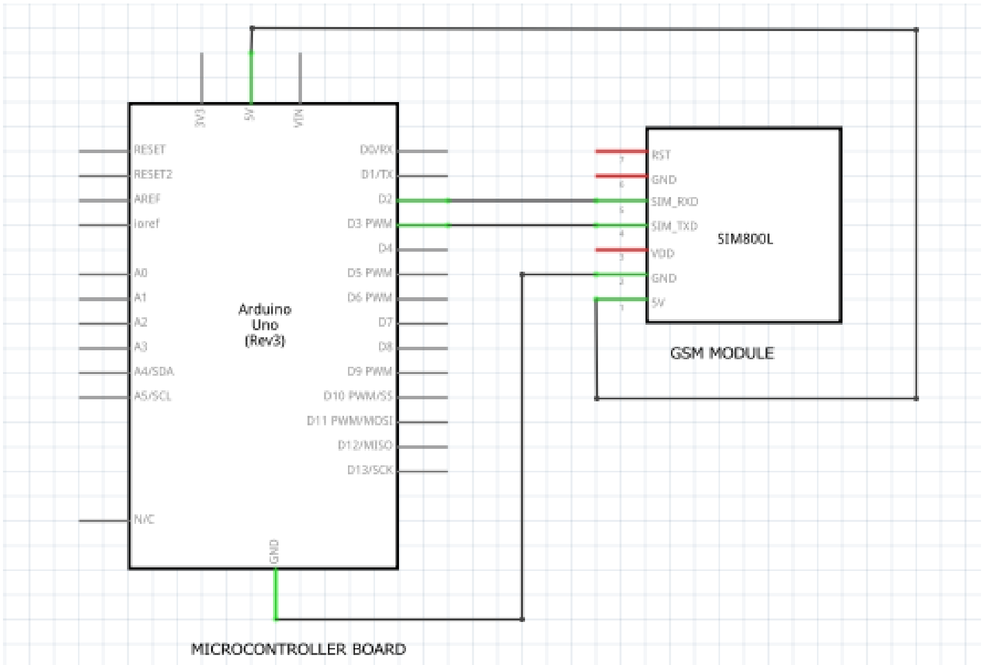
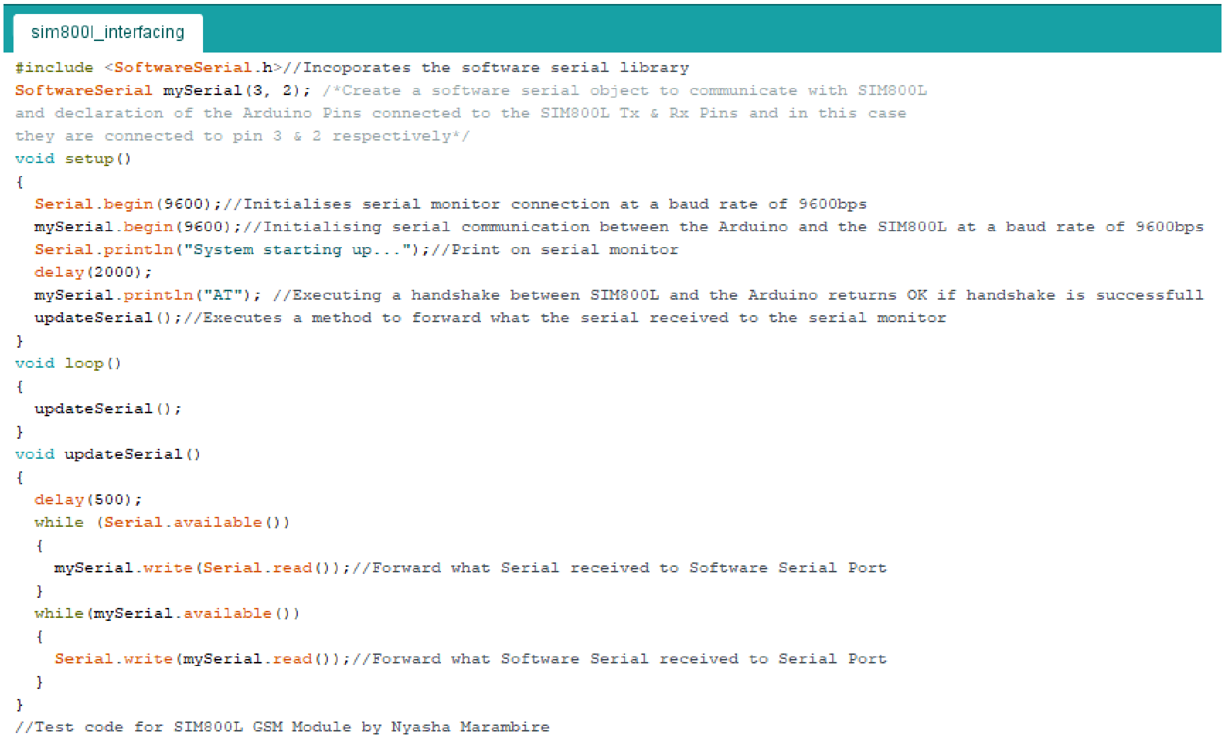


Figure 4. 4 : Connection Schematic of interfacing the SIM800L

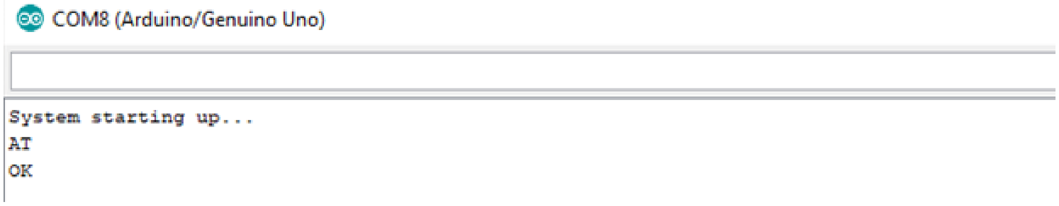
TEST CODE



```
#include <SoftwareSerial.h>//Incoporates the software serial library
SoftwareSerial mySerial(3, 2); /*Create a software serial object to communicate with SIM800L
and declaration of the Arduino Pins connected to the SIM800L Tx & Rx Pins and in this case
they are connected to pin 3 & 2 respectively*/
void setup()
{
  Serial.begin(9600);//Initialises serial monitor connection at a baud rate of 9600bps
  mySerial.begin(9600);//Initialising serial communication between the Arduino and the SIM800L at a baud rate of 9600bps
  Serial.println("System starting up...");//Print on serial monitor
  delay(2000);
  mySerial.println("AT"); //Executing a handshake between SIM800L and the Arduino returns OK if handshake is successfull
  updateSerial();//Executes a method to forward what the serial received to the serial monitor
}
void loop()
{
  updateSerial();
}
void updateSerial()
{
  delay(500);
  while (Serial.available())
  {
    mySerial.write(Serial.read());//Forward what Serial received to Software Serial Port
  }
  while(mySerial.available())
  {
    Serial.write(mySerial.read());//Forward what Software Serial received to Serial Port
  }
}
//Test code for SIM800L GSM Module by Nyasha Marambire
```

Figure 4. 5: Test Code for SIM800L Module Interfacing

OUTPUT OF THE SIM800L INTERFACING



```
System starting up...
AT
OK
```

Figure 4. 6: Showing a successful handshake

4.2.3 INTERFACING THE RELAY MODULE

The Arduino relay allows the Arduino to control high power circuits through charging and discharging the relay coil using an Arduino DI/O Pin. The developer interfaced the relay with the Arduino using 3 pins namely the VSS, GND and the control signal.

WIRING

Table 4. 3: PIN Connections

RELAY PINS	ARDUINO PINS
VSS Pin	5V Pin
GND Pin	GND Pin
Control Signal Pin	DI/O Pin 5

CONNECTION SCHEMATIC

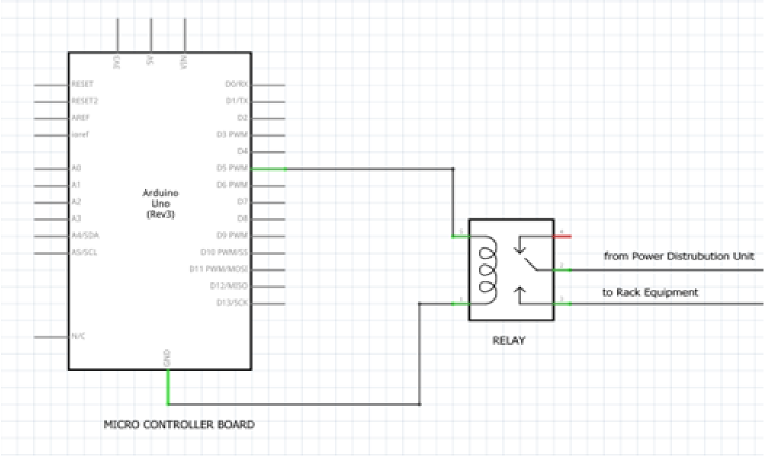
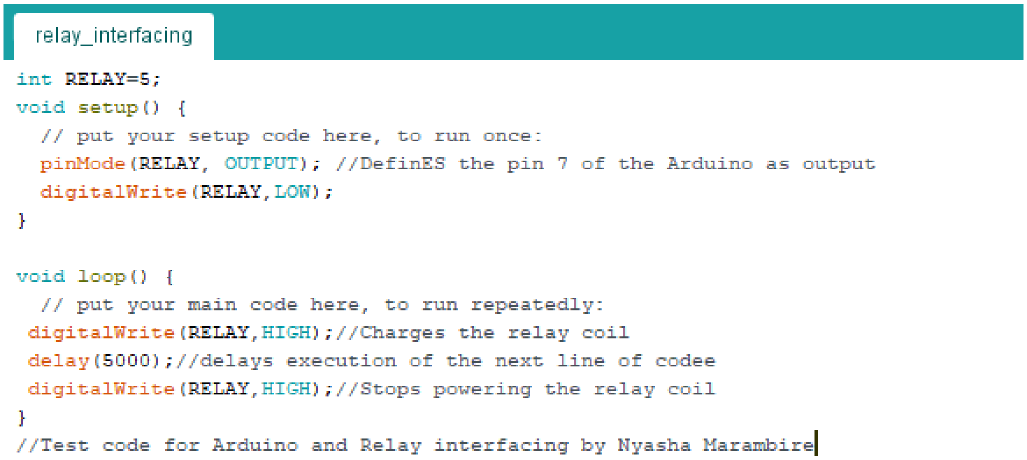


Figure 4. 7: Connection Schematic of interfacing the Relay Module

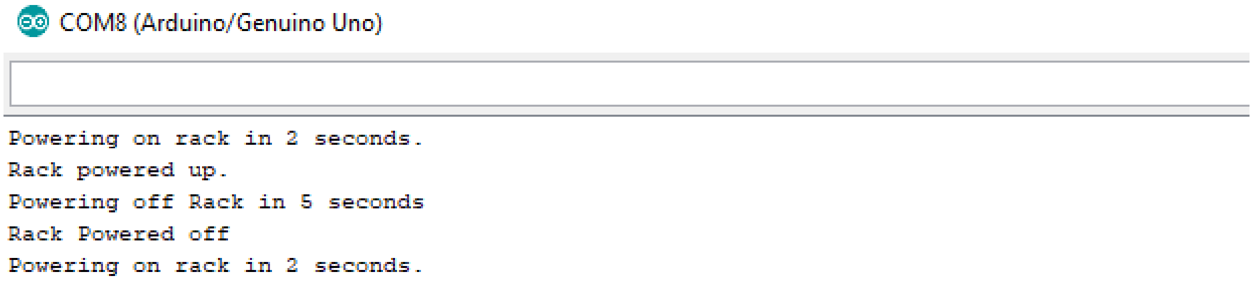


```
int RELAY=5;
void setup() {
  // put your setup code here, to run once:
  pinMode(RELAY, OUTPUT); //DefinES the pin 7 of the Arduino as output
  digitalWrite(RELAY,LOW);
}

void loop() {
  // put your main code here, to run repeatedly:
 digitalWrite(RELAY,HIGH);//Charges the relay coil
 delay(5000);//delays execution of the next line of codee
 digitalWrite(RELAY,HIGH);//Stops powering the relay coil
}
//Test code for Arduino and Relay interfacing by Nyasha Marambire
```

Figure 4. 8: Test Code for Relay Module Interfacing

OUTPUT OF THE RELAY INTERFACING



```
Powering on rack in 2 seconds.
Rack powered up.
Powering off Rack in 5 seconds
Rack Powered off
Powering on rack in 2 seconds.
```

Figure 4. 9: Sample Output of controlling the Relay

4.2.8 INTERFACING THE STATUS LEDS

Inorder to provide a visual aid of the current state of the rack, the faulty rack the data center watchdog has status LEDs of the following colours, green, amber and red to show the various states the watchdog will be in. Each LED has 2 pins and the longer pin is the anode and the shorter pin is the cathode and also the side of has a flat edge. When interfacing the LEDs the developer connected to the cathode to the ground and the D/IO pins to the anode of the LEDs through 220 Ohm resistors.

WIRING

Table 4. 4: Pin Connections

LED COLOUR	ANODE	CATHODE
Green	DI/O Pin 10	GND Pin
Amber	DI/O Pin 11	GND Pin
Red	DI/O Pin 12	GND Pin
Blue	DI/O Pin 13	GND Pin

CONNECTION SCHEMATIC

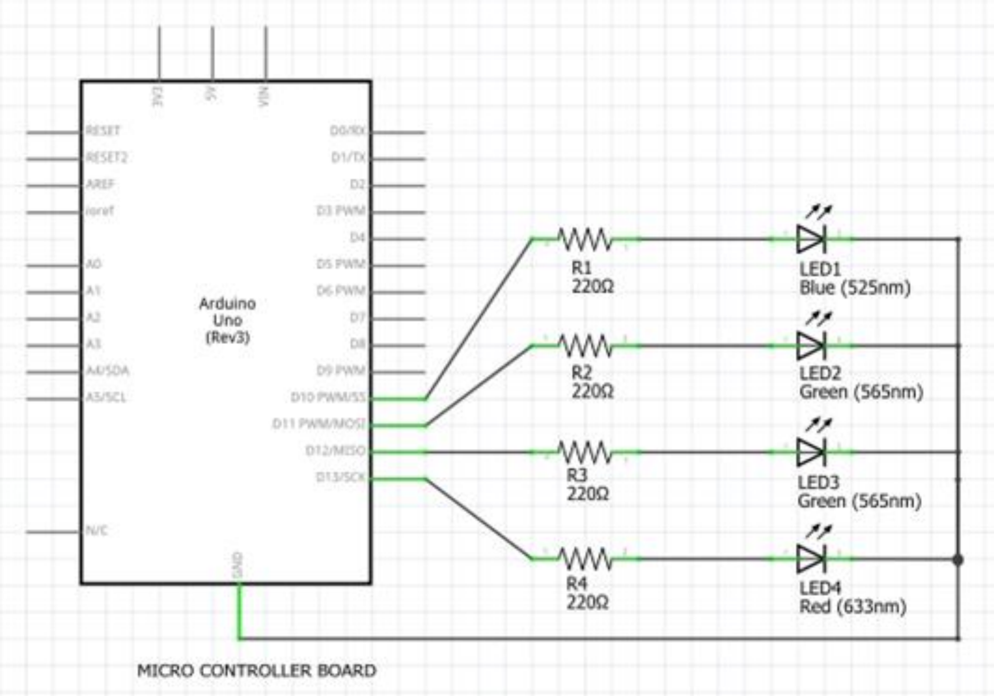
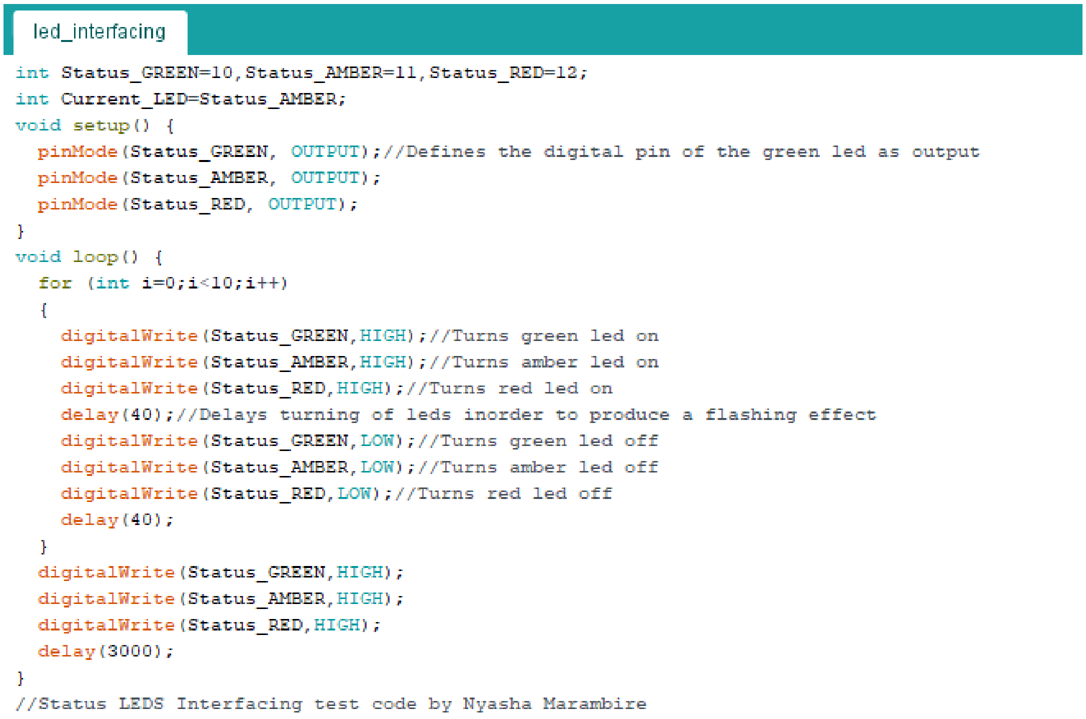


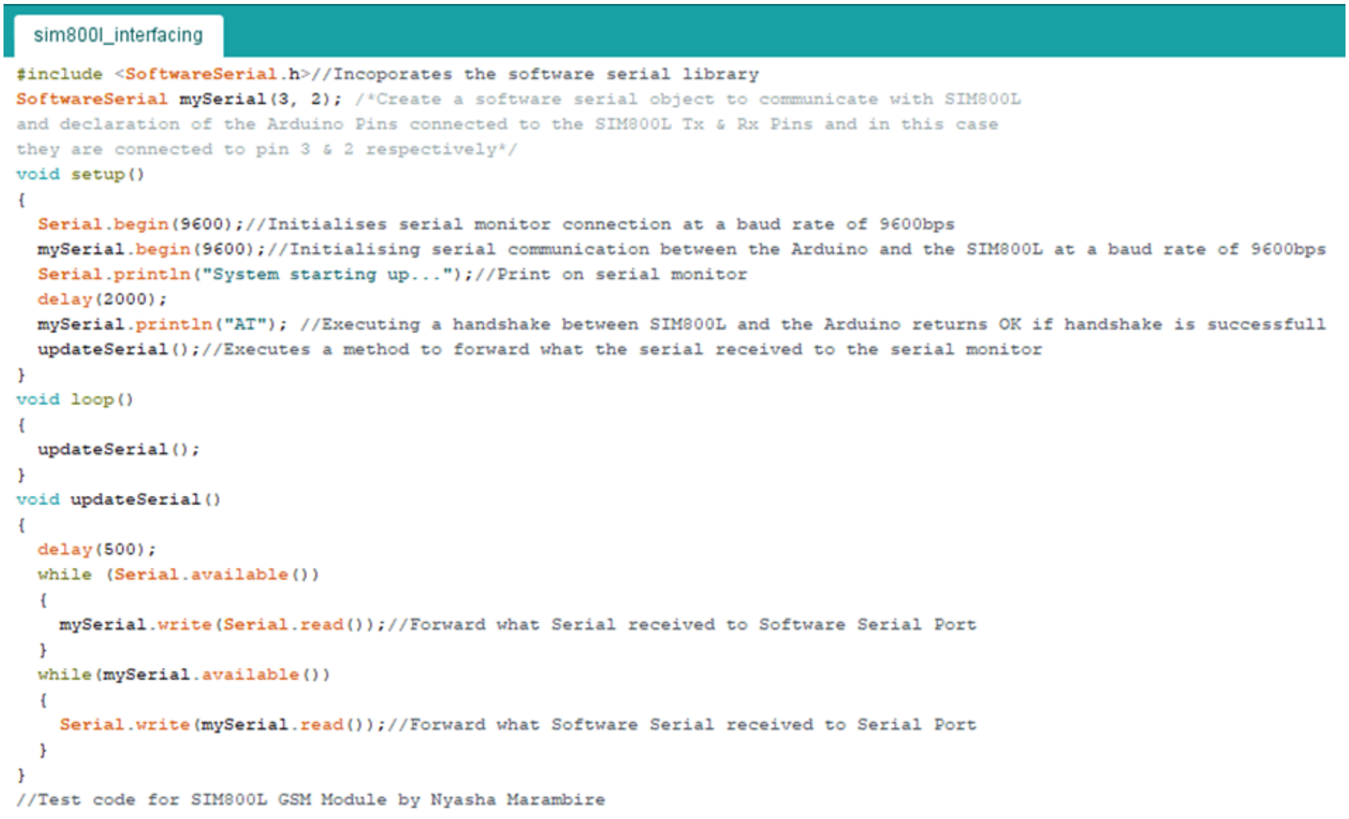
Figure 4. 10: Circuit Diagram of Status LEDs



```
int Status_GREEN=10,Status_AMBER=11,Status_RED=12;
int Current_LED=Status_AMBER;
void setup() {
  pinMode(Status_GREEN, OUTPUT);//Defines the digital pin of the green led as output
  pinMode(Status_AMBER, OUTPUT);
  pinMode(Status_RED, OUTPUT);
}
void loop() {
  for (int i=0;i<10;i++)
  {
    digitalWrite(Status_GREEN,HIGH);//Turns green led on
    digitalWrite(Status_AMBER,HIGH);//Turns amber led on
    digitalWrite(Status_RED,HIGH);//Turns red led on
    delay(40);//Delays turning of leds inorder to produce a flashing effect
    digitalWrite(Status_GREEN,LOW);//Turns green led off
    digitalWrite(Status_AMBER,LOW);//Turns amber led off
    digitalWrite(Status_RED,LOW);//Turns red led off
    delay(40);
  }
  digitalWrite(Status_GREEN,HIGH);
  digitalWrite(Status_AMBER,HIGH);
  digitalWrite(Status_RED,HIGH);
  delay(3000);
}
//Status LEDS Interfacing test code by Nyasha Marambire
```

Figure 4. 11: Test Code for Status LEDs Interfacing

SAMPLE OUTPUT



```
#include <SoftwareSerial.h>//Incoporates the software serial library
SoftwareSerial mySerial(3, 2); /*Create a software serial object to communicate with SIM800L
and declaration of the Arduino Pins connected to the SIM800L Tx & Rx Pins and in this case
they are connected to pin 3 & 2 respectively*/
void setup()
{
  Serial.begin(9600);//Initialises serial monitor connection at a baud rate of 9600bps
  mySerial.begin(9600);//Initialising serial communication between the Arduino and the SIM800L at a baud rate of 9600bps
  Serial.println("System starting up...");//Print on serial monitor
  delay(2000);
  mySerial.println("AT"); //Executing a handshake between SIM800L and the Arduino returns OK if handshake is successfull
  updateSerial();//Executes a method to forward what the serial received to the serial monitor
}
void loop()
{
  updateSerial();
}
void updateSerial()
{
  delay(500);
  while (Serial.available())
  {
    mySerial.write(Serial.read());//Forward what Serial received to Software Serial Port
  }
  while(mySerial.available())
  {
    Serial.write(mySerial.read());//Forward what Software Serial received to Serial Port
  }
}
//Test code for SIM800L GSM Module by Nyasha Marambire
```

Figure 4. 12: Test Code for Status LEDs Interfacing

4.3 SECURITY DESIGN

This refers to security measures that have been put in place to protect the system from intruders.

4.3.1 PHYSICALSECURITY

A practical data center setup includes a CCTV cameras to record events such as people entering the Computer and the actions they take. This security system will be responsible for ensuring the physical security of the data center watchdog.

4.3.2 NETWORK SECURITY

The data center watchdog was designed in such a way that it will only send the alerts to the data center technician with the phone number saved and the technician can only respond to the watchdog using the same number otherwise the watchdog will reject any response from any other number.

4.3.3 OPERATIONAL SECURITY

The data center watchdog operates with minimum human interaction with the technicians. The data center watchdog was designed in such a way that it will only send the alerts to the data center technician with the phone number saved and the technician can only remind the watchdog to alert him or her using the same number otherwise the watchdog will reject any response from any other number. For critical events such as powering up the rack, the data center technician will be required to manually interact with the data center technician.

4.4 WORKING OF THE DATA CENTER WATCDOG SYSTEM

The data center watchdog is activated by powering it with a 9V 2A power supply. Once active, the data center watchdog will continuously fetch current temperature readings from the DHT 22 sensor. Basing on these readings and the tolerated temperature levels set by the technicians during configuration, the data center watchdog will then decide an operating mode and can be in one of the 4 modes described below.

4.4.1 NORMAL OPERATION MODE

The data center watchdog is said to be in normal operation if the readings of the temperatures fall within the set normal threshold. The data center watchdog will visually show it in this state through flashing a green status LED. The watchdog will continuously monitor the rack temperatures. Also the relay will be turned on.

4.4.2 HOTSPOT DETECTED MODE

If the rack temperature rises above the normal temperature range but falls within the tolerated extreme temperatures, the watchdog system will change into the hotspot detected mode. Once in this mode the watchdog will send a hotspot detected SMS Alert which will include the physical cabinet and rack address as well as the IP Address of the server. In conjunction with the alert sent the data center watchdog will visually display this mode through flashing the Amber LED. In this mode the relay will still be charged hence the equipment in the rack will still be powered on and has become a hotspot the data center watchdog will send an alert to the technician. In this mode the system will continue to monitor the rack temperatures and if the rack temperature levels fall back into the normal mode the data center watchdog will notify the technicians that the temperature has restored to normal and will require the technician to acknowledge the system to return to the normal operating mode.

4.4.3 OUT OF EXTREME TEMPERATURE RANGE MODE

If temperature levels in the rack continue to rise and go above a certain threshold set by the technicians, the data center watchdog will alert of the technicians of the event via SMS as well as notify the technicians that it will shut down the rack after a certain time period that would have been set during configuration and after that time period the watchdog will power off the rack. The watchdog will also flash the red status LED. The data center watchdog will continue monitoring the rack temperature and will again notify the technicians when the temperature levels fall into the normal range but however it will require the technician to press the reset button on the watchdog so as to power up the rack.

4.4.4 SYSTEM FAILURE MODE

The data center watchdog will be made up of several components and during its operating, if one component of the data center fails, the watchdog will send an SMS and indicate the malfunction visually through flashing all the status LEDs.

4.5 SIMULATIONS AND TESTS

Chemuturi and Cagley (2010), define systems testing environment consists of the target configurations in which the developed product is expected to function in real life. During the simulations the normal rack temperature range was set to between 20 to 25 degrees Celsius and the threshold temperature was set at 27 degrees Celsius. The shutdown delay was set to 10 seconds.

Table 4. 5: Operating Test

Type of Data	DHT 22 Reading	Expected Action(s)	Action(s) Executed
Normal	22.00	- Flash Green Status LED	- Green status LED was flashed.
Normal	24.00	- Flash Green Status LED	- Green status LED was flashed.
Normal	25.00	- Flash Green Status LED	- Green status LED was flashed.
Extreme	25.01	- Send Hotspot detected SMS Alert - flash the Amber status LED	- Hotspot detected SMS Alert was sent and the Amber status LED started flashing.

Abnormal	27.00	- Send Out of Range temperatures detected SMS Alert - Flash the Red status LED. - Power down Rack.	- Send out of Range temperatures detected SMS Alert was sent. - The Red status LED was flashed. - Rack was powered down.

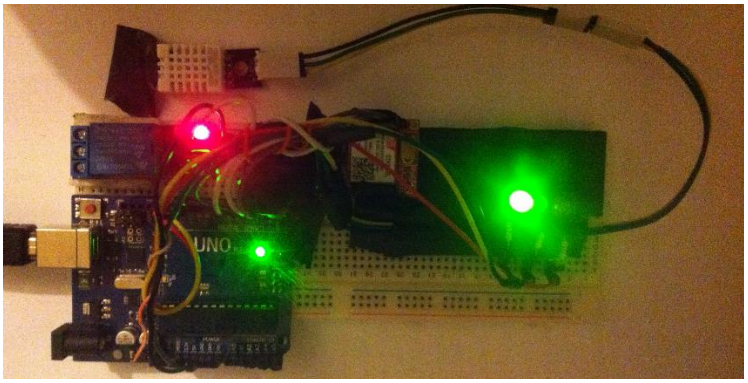


Figure 4. 13: Data Center Watchdog under normal operating mode.

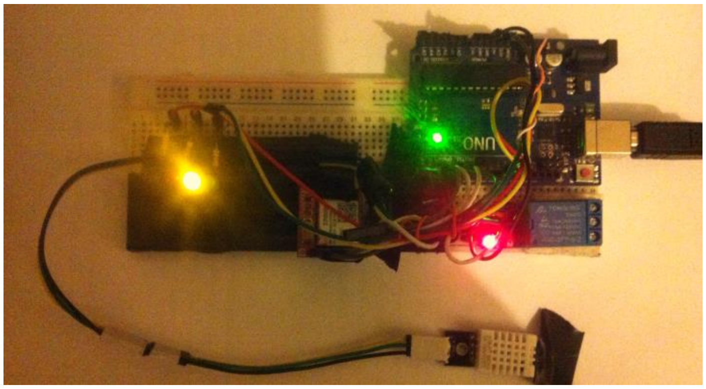
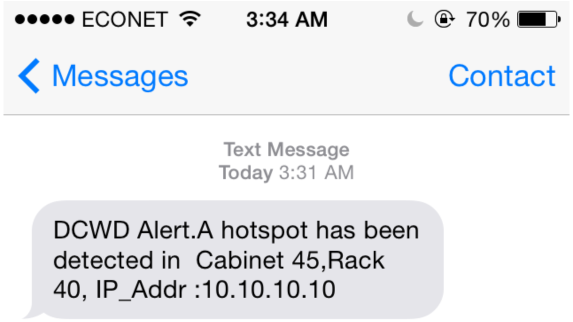


Figure 4. 14: Data Center Watchdog under detected hotspot operating mode.



DCWD Alert.A hotspot has been detected in Cabinet 45,Rack 40, IP_Addr :10.10.10.10

Figure 4. 15: Screenshot of a hotspot SMS alert sent by the Data Center Watchdog.

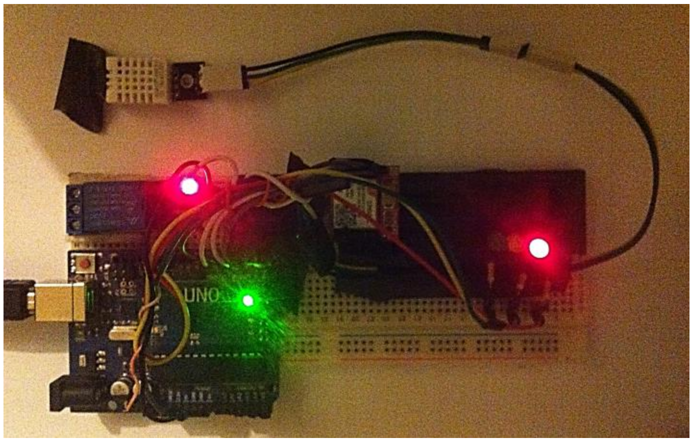
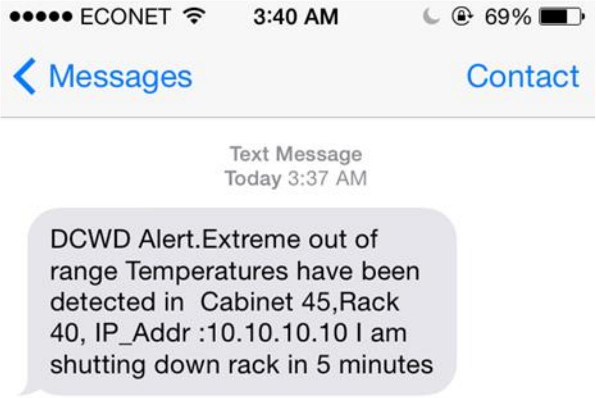


Figure 4. 16: Data Center Watchdog under extreme operating mode.



DCWD Alert.Extreme out of range Temperatures have been detected in Cabinet 45,Rack 40, IP_Addr :10.10.10.10 I am shutting down rack in 5 minutes

Figure 4. 17: Extreme Temperature levels detected SMS Alert sent by the Data Center Watchdog.

Table 4. 6: Self Diagnostics Test

Malfunctioning	Expected Action(s)	Action(s) Executed
DHT 22 Sensor was disconnected.	- Flash all Status LEDs - Send DHT Malfunction SMS Alert	- All Status LEDs were flashed - DHT Malfunction SMS Alert was sent.
Failed to connect to network	- Flash all Status LEDs	- All Status LEDs were flashed.
Failed to send power On or Off Signal	- Send SMS Alert - Flash the all status LEDs.	- Send SMS Alert was sent. - The all status LEDs were flashed.

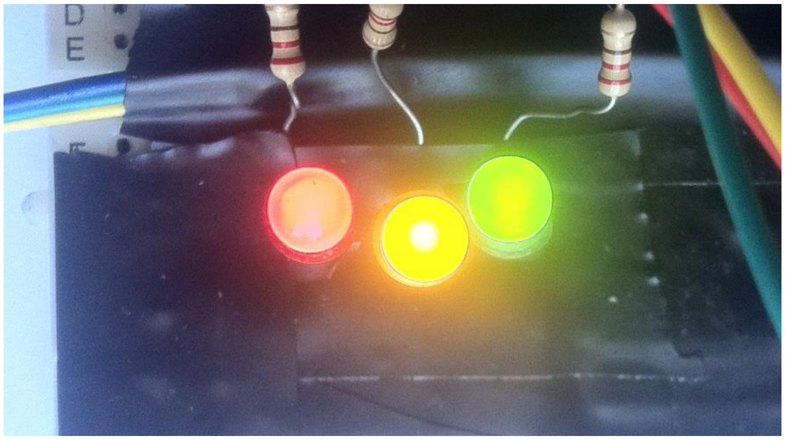
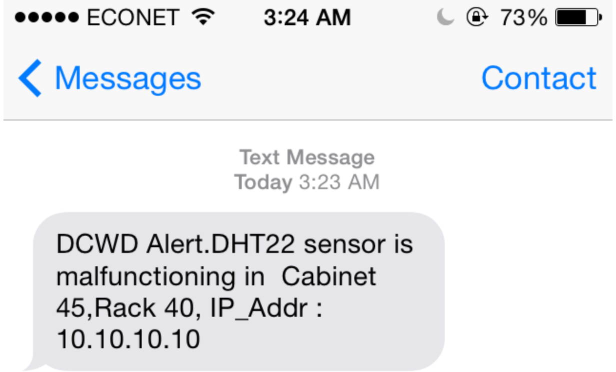


Figure 4. 18: Data Center Watchdog Malfunction Status LEDS



DCWD Alert.DHT22 sensor is malfunctioning in Cabinet 45,Rack 40, IP_Addr : 10.10.10.10

Figure 4. 19: DHT22 malfunction SMS Alert sent by the Data Center Watchdog.

4.6 IMPLEMENTATION AND RESULT

The systems implementation is based on a microprocessor as the central point of the components, a GSM for sending SMS alerts and the LEDs to provide a visual output of the system's status to the user, DHT 22 sensor for temperature readings input and a Relay to power on or off the rack. The end result for the watchdog is a collective is a system that takes in inlet air temperatures from its real time environment and sends alerts, flashes status LEDs and power on or off the rack basing on the range the temperature readings fall under. In the actual setup of the watchdog, in every rack of the cabinets, there is supposed to be a DHT22 sensor to take temperature readings, status LEDs to give a visual of the current status of each rack and a relay to control the power of each rack. The overall expected result with a perfectly implemented system is a general decrease in the number of equipment damage due to hotspots and also an increased level of confidence to increase data center operating temperatures which in turn promotes the realisation of green sustainable IT.

4.7 PRACTICAL SET-UP AND RESULT

The practical setup incorporates all of the different components of the system which make up the complete data center watchdog system. In the rack, there is a DHT22 sensor that is for taking readings of the current rack temperatures once system is activated. It has a GSM Module, a SIM800L model in particular for rolling SMS alerts basing on the current operating mode of the watchdog and status LEDs for indicating the current rack status.

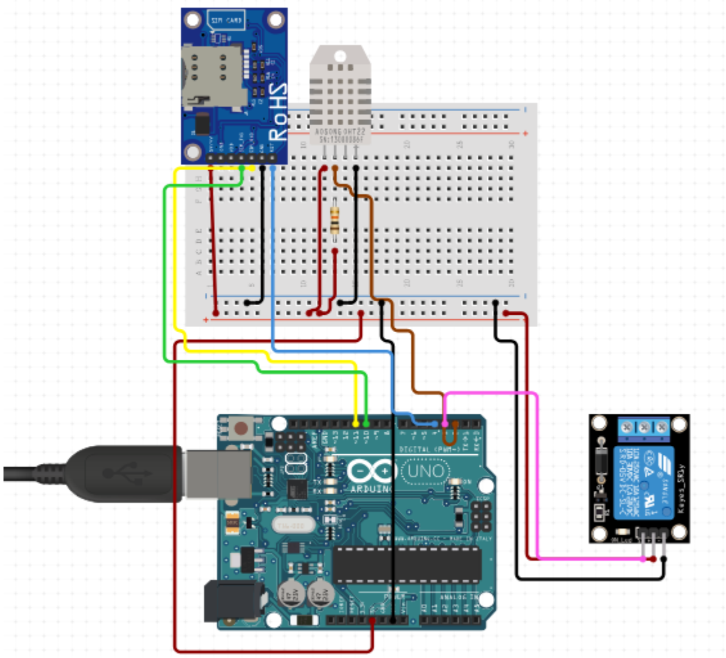


Figure 4. 20: Schematic View Data Center Watchdog System

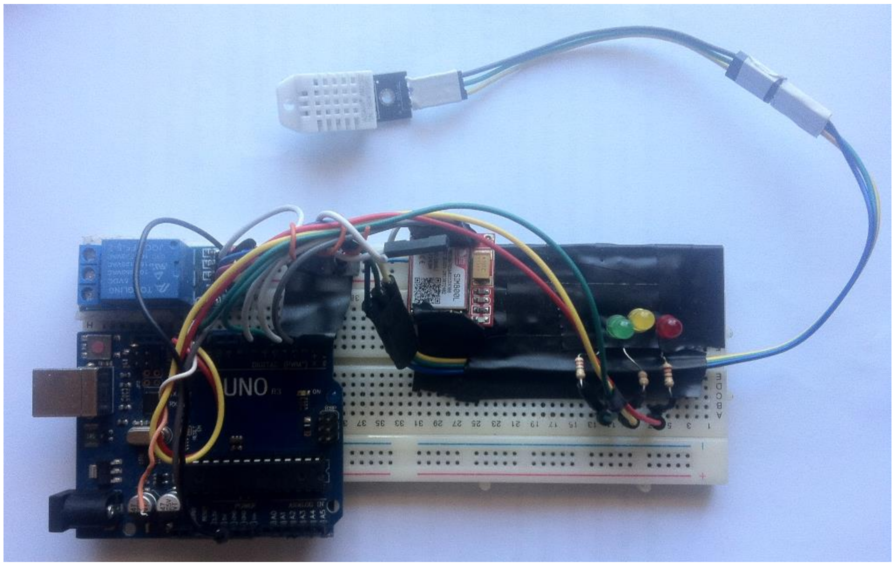


Figure 4. 21: Actual Data Center Watchdog System.

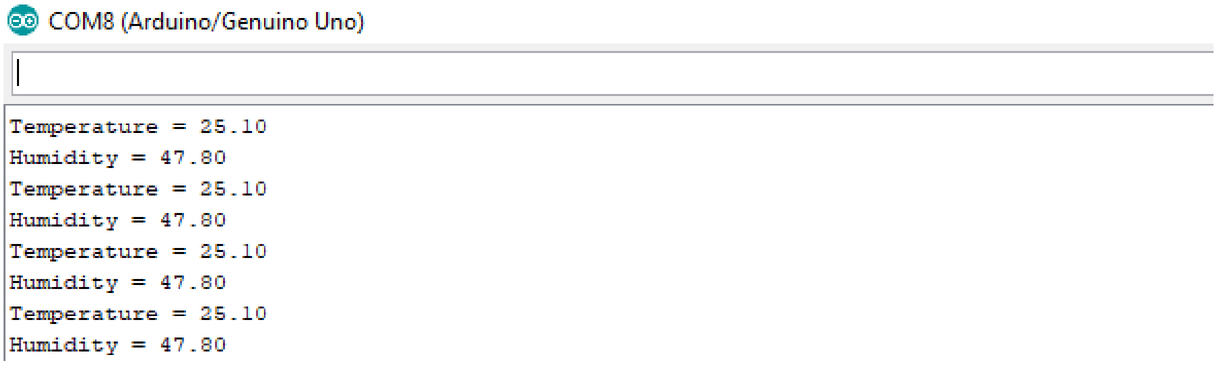
4.8 SYSTEM VS OBJECTIVES

Objective: Monitors temperature and humidity levels at the server inlet in real time.

Result: The diagram below shows serial output from the data center watchdog.

Objective: Alerts data center technicians as soon as temperature levels rise above specified ranges set by the data center technicians through SMS platform.(i.e. if a hotspot is detected or if extreme temperatures are detected.)

Result:

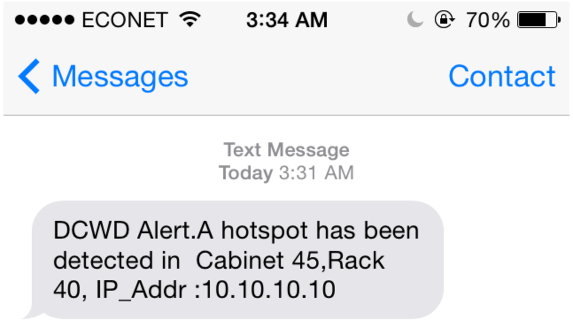


COM8 (Arduino/Genuino Uno)

```
Temperature = 25.10
Humidity = 47.80
Temperature = 25.10
Humidity = 47.80
Temperature = 25.10
Humidity = 47.80
Temperature = 25.10
Humidity = 47.80
```

Figure 4. 22: Serial output of the watchdog illustrating continuous monitoring.

SMS sent when Hotspot is detected

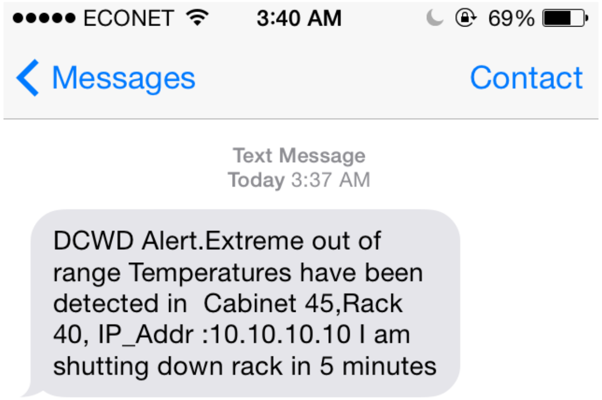


Text Message
Today 3:31 AM

DCWD Alert.A hotspot has been detected in Cabinet 45,Rack 40, IP_Addr :10.10.10.10

Figure 4. 23: Hotspot detected SMS.

SMS sent when extreme temperatures are detected.



Text Message
Today 3:37 AM

DCWD Alert.Extreme out of range Temperatures have been detected in Cabinet 45,Rack 40, IP_Addr :10.10.10.10 I am shutting down rack in 5 minutes

Figure 4. 24: Extreme Temperature levels detected SMS Alert sent by the Data Center Watchdog.

Objective: Shutdown the affected servers as a protection measure if harmful conditions remain present for the tolerated time set by the data center technicians.

Result:

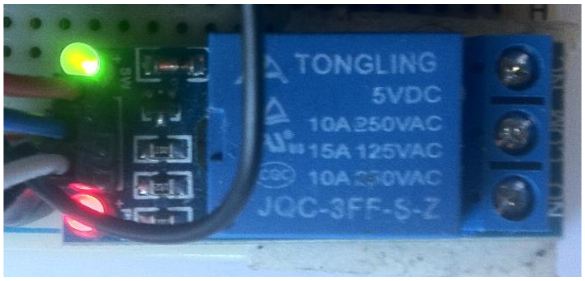


Figure 4. 25: Diagram showing relay state before extreme temperatures were detected.

Please note that if the green light is on it showing that the relay is in its on state.

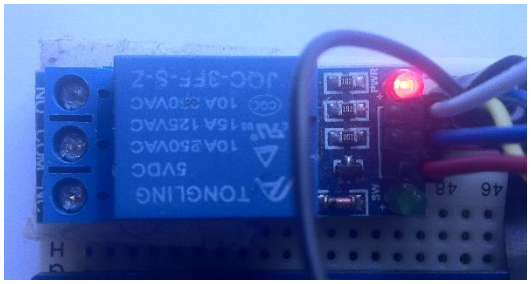


Figure 4. 26: Diagram showing relay state after extreme temperatures were detected.

Please note that if the green light is off it showing that the relay is in its off state.

4.9 CONCLUSION

This chapter paid attention on giving the reader an insight of the interfacing of the various components that make up the data center watchdog from the wiring stage as wells as providing illustrations of results from a successful interfacing. It also focused on running the data center watchdog in a simulated environment so as to assess its performance and also to confirm whether the data center watchdog meets its requirements. The next chapter will focus on giving recommendations of what can be added to the system in its next revision.

CHAPTER 5: CONCUSION AND RECOMMENDATIONS

5.1 INTRODUCTION

The previous chapters served the purpose of introducing the data center watchdog, exposing how it works and running tests and simulations as well as testing the system against its objectives. This chapter focused on conducting a discussion on the data center watchdog, stating its limitation giving recommendations as well as the future scope of the system. This chapter also serves to conclude the research

5.2 DISCUSSION

The Data center watchdog prototype was successfully tailored using a minimal number of modules. With the application of these watchdogs in data centers, there is a reasonable degree of expectation that there will be a significant decline in equipment damage and expenditures incurred due to hotspots as well as an increased degree of confidence in technicians and enterprises to raise their data center operating temperatures and switch to free cooling methods. Although there are not yet any real life application results at the moment, the watchdog is undoubtedly capable of performing its primary objectives which are quickly measuring temperature in real time, able to notify the technicians as well as able to shut down the equipment in the rack so as to protect it when temperature levels set in the hazardous temperature range are detected therefore the research can be concluded as a success.

5.3 LIMITATIONS

The Limitations of the Data Center Watchdog are that:

(i) The DHT22 can only be query once every second therefore there is a lag time in temperature measurement.

(ii) If the SIM800L GSM module is faulty, communication between the technician and watchdog goes down.

(iii) The data center watchdog system will require the technician’s intervention to properly shutdown the rack equipment for example the watchdog will simply cut the physical server’s power supply instead of first shutting down virtual machines and then shutting down the hypervisor and lastly cutting down the power to the physical server.

5.4 RECOMMENDATIONS

The data center watchdog being the first of its kind has its own limitations but however leaves more than enough room for improvement during the course of its operation and so far the recommendations available are:-

(i) It is most important that before implementation of the data center watchdog system the data center technicians should first undertake Computational Fluid Dynamics calculation in order to account for temperature variations between racks.

(ii) Unlike in this case where there was only one DHT22 temperature sensor and a relay, the complete system should incorporate a sensor and a relay as well as status LEDs in every rack.

5.5 FUTURE SCOPE

In the near future during the lifetime of the data center watchdog should funds suffice, the watchdog should be:

(i) Revised to incorporate a graphical web interface and storage for showing a summary of hotspots occurrence so as to allow the technicians to keep an up to date historical records.

(ii) Interlinked with cooling systems so as to implement dynamic cooling controlled by the data center watchdog.

(iii) Integrated with systems that have an effect of inlet rack temperature such as door and window locking systems so as to allow the system

5.6 CONCLUSION

The data center watchdog was successfully developed and met all its objectives hence the research can be deemed as a success. The data center watchdog system in overall if fully implemented can lead to a decline in damages caused by hotspots and be a major game changer in green sustainable IT through its reliability to vigilantly keep an eye on the inlet temperature levels in the racks as well as protecting equipment from damage. This marks the end of the research.

REFERENCE LIST

Ahmed, A. (2016), Software Project Management: A Process-Driven Approach, CRC Press, Boca Raton.

Berddtsson, Hansson and Lundel (2007), Thesis Projects: A Guide for Students in Computer Science and Information Systems 2nd ed, Springer, London.

Bosu, K. Choudhuri, R. (2017) Learn Arduino Prototyping in 10 days, Publishing Ltd, Birmingham.

Brown (2016) white paper titled “The Unexpected Impact of Raising Data Center Temperatures

Chemuturi, M, Cagley, T.M. (2010), Mastering Software Project Management: Best Practices, Tools and Techniques, J. Ross Publishing, Lauderdale.

Dai, J. Ohadi, M.M. Das, D. Petch, M.G. (2013), Optimum Cooling of Data Centers: Application of Risk Assessment and Mitigation Techniques, Springer Science & Business Media, New York

Dawson, C. (2009) Projects in Computing and Information Systems A students guide 2nd ed, Pearson Education Ltd, Essex.

Fehling, C. Leymann, F. Retter, R. Schupeck, W. Arbitter, P. (2014) Cloud Computing Patterns: Fundamentals to Design, Build, and Manage Cloud Applications, Springer Science & Business Media,London.

Geddes, M. (2014) Arduino Project handbook, Sketch Publishing, Dumfries.

Hart, C. (2018), Doing a Literature Review: Releasing the Research Imagination 2nd ed, SAGE, London.

Hwaiyu, X. Geng. X. (2014) Data Center Handbook John Wiley & Sons.

Larrson, M. R. (2012), The Business of Global Energy Transformation: Saving Billions through Sustainable Models, Springer, Hampshire.

Mehdi, K. (2014) Encyclopedia of Information Science and Technology, Third Edition IGI Glob

Poole, D.L. Alan K. Mackworth, A.K. (2010), Artificial Intelligence: Foundations of Computational Agents, Cambridge University Press, Cambridge.

Rountree, D. Castrillo, I. (2013), The Basics of Cloud Computing: Understanding the Fundamentals of Cloud Computing in Theory and Practice, Newnes

Singh R, Gehlot A, Singh B, Choudhury S, (2018), Arduino meets MATLAB: Interfacing, Programs and Simulink, Bentham Science Publishers, Sharjah.

Zobel. J, (2015), Writing for Computer Science 3rd ed, Springer, London.

APPENDICES

Appendix 1: Code

```
#include <SoftwareSerial.h>
#include <dht.h>
dht DHT;
//Create software serial object to communicate with SIM800L
SoftwareSerial mySerial(3, 2); //SIM800L Tx & Rx is connected to Arduino #3 & #2
#define DHT22_PIN 4
int Power_Detect=6, Power_Live=5, Status_GREEN=10, Status_AMBER=11, Status_RED=12, Status_SYSTEM=13;//PINS
String AlertMsg="", Rack_Details=" Cabinet 45,Rack 40, IP_Addr :10.10.10.10";
int HotspotAlert=0,Shutdown_Alert=0,ExtremeTempsAlert=0, StabilisedTempsAlert=0;//ALERTS
int Rack_Status=1, Unstable=0,Current_LED,Current_LED2;//ADDITIONAL VARS
int Shutdown_Delay=500;//DELAYS
int Temp_Range[]={28,29};//Temperature Limits for Hotspot and Extreme Temperatures in degrees C
float Temperature;

void setup() {
  initialisePins();
  status_BOOT();
  digitalWrite(Power_Live,LOW);
  Serial.begin(9600);//Begin serial communication with Arduino and Arduino IDE (Serial Monitor)
  mySerial.begin(9600);//Begin serial communication with Arduino and SIM800L
  Serial.println("DATA CENTER WATCHDOG v1.001 initialising...");
  Serial.println("Tailored by Nyasha Marambire (2019)");
  delay(1000);
  AlertMsg=mySerial.println("AT"); //Once the handshake test is successful, it will back to OK

  updateSerial();

  int chk = DHT.read22(DHT22_PIN);

  Serial.print("Temperature = ");

  Serial.println(DHT.temperature);

  Serial.print("Relative Humidity = ");

  Serial.print(DHT.humidity);

  Serial.println("%");

  if((DHT.temperature)==-999.00){status_BOOT();Serial.println("DHT22 sensor malfunction in "+ Rack_Details + ".Sending Alert...");AlertMsg="DHT22 sensor malffunction in "+ Rack_Details;sendAlert();}

  else{Current_LED=Status_GREEN;Serial.println("DCWD active."+ Rack_Details + ".Sending Notification...");AlertMsg="DCWD active. Sent by "+ Rack_Details;sendAlert();}

}


void loop() {

  // put your main code here, to run repeatedly:

  status_FLASH();

  monitorRack();

}

void sendAlert(){

  mySerial.println("AT+CMGF=1"); // Configuring TEXT mode

  updateSerial();

  mySerial.println("AT+CMGS=\"+263718599607\"");//change ZZ with country code and xxxxxxxxxxx with phone number to sms

}
```

Appendix 2: User Manual

Powering Up the Data Center Watchdog

Connect the data center watchdog to the Power Supply

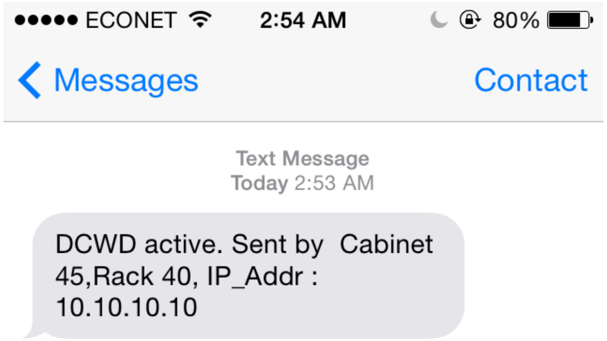
The data center watchdog will flash all the three status light whilst in its booting sequence

Booting

After successfully booting the data center watchdog will start flashing the green status LED. (if not please see troubleshooting).

Active State

Also after a successful boot the data center watchdog will send a SMS notification stating that it is active. An illustration of the message is shown below.

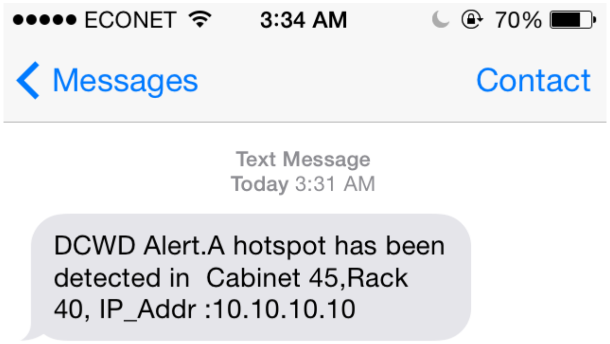


DCWD active. Sent by Cabinet 45,Rack 40, IP_Addr : 10.10.10.10

The watchdog will continue monitoring the server inlet air temperatures and flash the green status LED.

Hotspot Detected

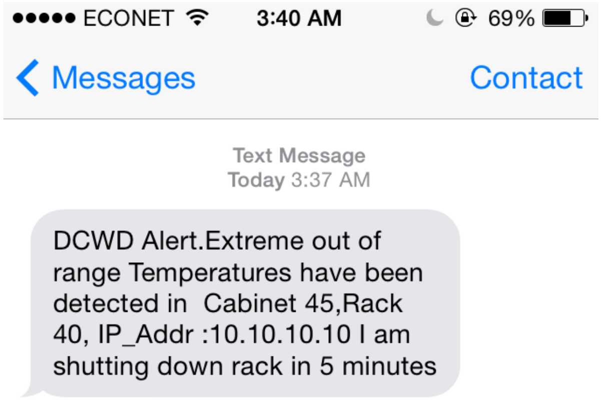
If a hotspot is detected the data center watchdog will start flashing the amber light and send a SMS like the one shown below.



DCWD Alert.A hotspot has been detected in Cabinet 45,Rack 40, IP_Addr :10.10.10.10

Extreme out of range temperature levels detected

If extreme out of range temperature levels have been detected is detected the data center watchdog will start flashing the amber light and send a SMS like the one shown below.



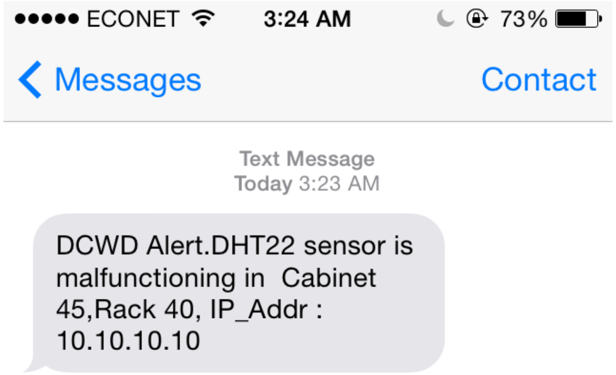
DCWD Alert.Extreme out of range Temperatures have been detected in Cabinet 45,Rack 40, IP_Addr :10.10.10.10 I am shutting down rack in 5 minutes

TROUBLESHOOTING

My Data Center watchdog keeps flashing all the status LEDs. What is wrong?

Remove the data center watchdog and connect it to your PC and open your serial monitor. The problem will be out put on the serial monitor. For example below is an illustration of a DHT sensor malfunction error.

Also the data center watchdog will send a malfunction alert.



Text Message
Today 3:23 AM

DCWD Alert.DHT22 sensor is malfunctioning in Cabinet 45,Rack 40, IP_Addr : 10.10.10.10