BINDURA UNIVERSITY OF SCIENCE EDUCATION

HBScIT NETWORKING ENGINEERING RESEARCH PROJECT

DATACENTER SURVEILLANCE SYSTEM

REG NUMBER: B1953765

NAME: PANASHE WILLIAM KASEKE

PROGRAMME: HBScIT

LEVEL: 4 SEMESTER 2

COURSE CODE: IT414

COURSE NARRATION: RESEARCH PROJECT

ABSTRACT

Recently the has been a massive change in the technological world, enterprises have been migrating from traditional way of acquiring ICT infrastructure to clouding services which are powered by datacenters. This resulted in a significant increase in the number of datacenters around the world and they have become the most energy consuming facilities. Different scholars conducted researches and highlighted that these energy consumptions can be reduced by using free cooling in datacenters and raising the datacenter operating temperatures. These methods have however resulted in increased rate of occurrence of hotspots in datacenters, giving birth to the agent need for a mechanism to quickly detect hotspot and reduce their impact to be put in place. This research focuses on the development of an Arduino based datacenter surveillance system written in C and C++ that monitors the temperature and humidity levels as well as protecting the equipment. The system was successfully developed and it is recommended that before deploying it technicians must first do CFD calculations in order to account for temperature variation as well as installing DHT11 in every rack.

DECLARATION

I, PANASHE WILLIAM KASEKE, REG NUMBER B1953765, hereby declare that I am the sole author of this dissertation. I authorize the BINDURA UNIVERSITY OF SCIENCE EDUCATION to lend this dissertation to other institutions or individuals for the purpose of scholarly research.

Signature: ……. Date: …….

APPROVAL

This dissertation, entitled "DATA CENTER SURVEILLANCE SYSTEM" by PANASHE WILLIAM KASEKE meets the regulations governing the award of the HBScIT at BINDURA UNIVERSITY OF SCIENCE EDUCATION, and is approved for its contribution to knowledge and literary presentation.

Supervisor's Signature: ……. Date: ……..

ACKNOWLEDGEMENTS

I would like to extend my gratitude and sincere thanks AMAI na BABA Kaseke for thier constant motivation and support during the course of my work. I truly appreciate and value their esteemed guidance and encouragement for the past 4 years. I also want to thank Mr. Matombo, Mr. Musariwa and Mr Magomelo for their supervision, I really appreciate all the time and efforts they put with the bid of helping me to come up with a quality research. Furth

Contents

LIST OF FIGURES

1 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 is at hand, the aim and objectives of the research as well as the data gathering methods and instruments that will be used during the course of the research. This chapter also gives a justification for continuing with the research. This chapter also serves to give the reader detail on how a data center surveillance system was a stepping stone towards addressing the problem as well as promoting green sustainable IT.

1.2 BACKGROUND OF RESEARCH

Over the past years notable changes have been observed in the computing world as many enterprises moved from client-server architectures to distributed computing. As a result, innovative business models were formulated with cloud computing being one of the innovations. (Fehling et al., 2014), state that 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. Computing services such as storage and processing on ad hoc as be need basis can now be easily accessed at a cheaper cost due to advancement in cloud computing. 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.

Commented [pk1]: citation

The widespread adoption of clod computing resulted in notable changes in the growth rate of data centers. These data centers serve as the backbone of the cloud and they consume huge amount of energy with most of the energy being consumed by cooling systems. This led to researches that give rise to the emerging of countless 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. To date many data center technicians, use hot aisle containment with many recommended practices which include blanking panels to ensure proper cooling and support realization of green IT.

Further researches reflected that more energy could be saved through raising the operating temperature levels or switching to floating operating temperature in data center facilities. 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 energy saving methods above, another breakthrough was made by researchers on energy saving in data center which was to rise free cooling. (Larsson, 2012), defines free cooling as an energy saving cooling method which utilizes 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.

Raising data center operating temperature, switching to floating temperatures or resorting to utilizes free cooling is however associated the increased occurrence of hotspots. This makes the adoption of greener cooling methods became a problem. This is backed by (Dai et al., 2013), who state that when free air cooling is used, due to seasonal climatic changes, the operating 3 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.

To duck the worries of data center hotspots, technicians prefer to run at cooler and safer temperatures thus making data centers to have a higher Power Usage Effectiveness (PUE) and leave a large carbon footprint. (Mehdi, 2014), states that the addressing of hotspots is possible through the application of Computational Fluid Dynamics (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, as a way to soothe the data center technicians and to promote sustainable information technology there was need to implement a vigilant datacenter surveillance system in the racks that do not only keep watch for hotspots in real time and alerts datacenter technicians but with the capabilities to shut-down the affected server so as to protect it.

1.3 PROBLEM DEFINITION

The proposed data center surveillance system is an agent-based system which is aimed at addressing the issue of real time detection of data center hotspots and reporting the issue to technicians as well protecting the equipment affected by hotspots and coldspots. (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 surveillance system.

The scope of the problem to be addressed is based on the fact that inlet temperature in data center racks should lie between a certain range and any readings that falls above or below that is referred to as a hotspot or coldspot respectively.

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

The catering for each problem stated above, DHT11 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 will be used. Status LEDs were to be put in place to draw the attention of the data center technicians.

1.4 AIM

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

The aim of the research is to develop a vigilant data center surveillance system 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 are to:

- To investigate on how temperature and humidity levels at the server inlet be monitored in real time.
- To inspect on how data center technicians be alerted as soon as temperature levels rises above specified ranges set by the data center technicians through SMS platform. (i.e., if a hotspot or coldspot is detected.)
- To explore on how can data center equipment be protected from extreme temperatures when they are detected after waiting for a period set by data center technicians.

1.6 RESEARCH QUESTIONS

A research question is a specific inquiry which the research seeks to provide a response to. It resides at the core of systematic investigation and it helps you to clearly define a path for the research process. The data center surveillance system is motivated by the following questions:

- How can temperature and humidity levels be monitored in datacenters?
- How can data center technicians be notified of changes in temperature on racks in real time?
- How can datacenter equipment be protected from extreme temperature?

1.7 METHODS AND INSTRUMENTS

Methods and instruments refer to the methodologies that were used during the research period to obtain knowledge about the research.

1.7.1 DATA COLLECTION TOOLS

Tools that I used during the period of this research were:

- The internet
- Academic papers
- Textbook
- Newspapers

1.7.2 INSTRUMENT USED IN SYSTEM CREATION

When creating the data center surveillance system, I used the following instruments

- Arduino IDE- – It is the platform that will be 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 will used to develop the data center data center surveillance system's code libraries.

- Code blocks – It is the platform that will be used to develop the data center surveillance system's class libraries.

1.8 JUSTIFICATION

The problem highlighted above seemed addressable through the development of a data center surveillance system. The system would work like a domestic dog which watches over our homes, barks to alert us when there are intruders and if we don't show any response it bites the intruder to safeguard the premise. Applying the above example to data center, when fully implemented the data center surveillance system would monitor the data center on a 24/7 basis and alert data center technicians about the abnormalities, if data center technicians does not respond within specified period shutdown the affected server so as to safeguard them.

The data center surveillance system development was a success and it quickly detected hotspots in the data center as well as giving the data center technicians time to resolve the faults. This instilled some degree of self-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 surveillance system therefore results in energy savings were expected. Apart from that, the data center surveillance 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 suffering heavy costs of replacing equipment damaged by extreme temperature levels. Besides that, through shutting down the racks, the system did not only protect the equipment but also increased its fault tolerance significantly causing an increment in the data center's performance.

1.9 CONCLUSION

The conclusion can be defined as a sequential end of any discussion and serves to echo the final arguments. This chapter painted the activities that were undertook so as to complete the research and deliver the required system. It also clearly drew what a data center is, its importance, and the paybacks of raising the operating temperature in a data center along with

the allied risks as well as how the application of the system curbed the risks. The next chapter will be literature review which assessed whether if hotspots are really a threat to data center

2 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 I undertook an investigation to identify the prevailing 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 surveillance system so as to evaluate its importance and the competitive advantages that data center technicians stand to benefit from using the system. Also, foresight prior to the development of the data center surveillance system was acquired from the researches carried out during this chapter. It also gave a picture of how the data center surveillance system is a stepping stone towards achieving Green IT.

2.2 DATA CENTER HOTSPOTS AND THEIR IMPACT IN DATA CENTERS

Hotspots are one of the most dangerous threats to data centers because the can silently creep up without drawing the technicians' attention until their impact becomes serious. Hotspots or coldspot are cabinets with unfavorable temperatures level in data centers. If data center hotspots go unnoticed, they can damage equipment installed in the affected areas.

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 et al., 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 being used to provide the cooling effect on the air which will be supplied to the data center. Due to the seasonal variations in the outside world climatic conditions, it could be concluded that integrating greener cooling methods results in increased hotspot occurrences hence a mechanism to quickly detect 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 organization. (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 hotspots 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 optimized cooling.

However, the blanking panels lack convenience in the logic that they need the technicians to physically 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

2.4 GAPS IDENTIFIED

In the data centers the currently existing works require technicians to regularly check the temperatures indicated by blanking panels. This system lacks the ability to notify data center technicians of any irregularities. This system also lacks the ability to prevent data center equipment from any damage if no technician is not around on the premise to physical shutdown the equipment to protect it from electrostatic circuiting due to abnormal temperature or humidity levels. A data center surveillance system 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.

2.5 DATA CENTER HOT SPOT DETECTION USING DATA CENTRE SERVIELLANCE SYSTEM

(Hwaiyu and Geng, 2014), defined monitoring temperature levels at each rack as an efficient method of identifying air management problems. The proposed data center surveillance system would facilitate hotspot and coldspot 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 surveillance system would shut down the server exposed to the extreme temperatures levels so as to avoid damages to the equipment thereby saving the organization from suffering any further costs. Also, the data center surveillance is set to be a self-directed agent and will therefore require little human intervention during its operation.

2.5.1 ADVANTAGES

- Capable of monitoring temperature and humidity levels in real time.
- Can quickly detect hotspots or coldspot
- Issue real time alerts to data center technicians
- Little human intervention is required.
- Protects the equipment through shutting down the exposed equipment.

2.5.2 DISADVANTAGES

- Idea still new hence might be prone to errors

2.6 FOREKNOWLEDGE

The implementation of the data center surveillance system 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 center surveillance system 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 center surveillance'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 surveillance system 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 surveillance system.

3 CHAPTER 3: THEORETICAL INFORMATION

3.1 INTRODUCTION

In this chapter, I will focus on discussing the components that I will use in the development of the data center surveillance system. In this discussion seek to expose the components' underlying workings so as to give the reader a better understanding of how the components function.

3.2 COMPONENTS TO BE USED

In this research I will use different components to construct data center surveillance system. The components I will use comprises of a microcontroller board, a DHT senser, 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 et al ,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 or 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.

3.2.1.1 HOW IT WORKS

Uno R3 works by simply writing the program you want to run in it using the ardiuno IDE and upload it to the board using the USB Port. Once the program has been uploaded, power on the Arduino an it starts to run the program.

3.2.1.2 TECHNICAL SPECIFICATION

Micro controller	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
Clock Speed	1600 Hz

Figure 3-1:ardiuno R3 techinical specification

3.2.2 DHT11 MODULE

The data center surviellance's input about the current relative humidity levels in its environment is fed in by a DHT11 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 DHT11 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.

3.2.2.1 PRINCIPLE OF OPERATION

The DHT11 is made up of three parts which are; a thermistor which is in-charge for the measurement of temperature, a capacitive humidity sensor which is responsible for humidity measurement and a chip which is responsible for the conversion of analog measurement into digital readings.

3.2.2.1.1 HUMIDITY SENSING COMPONENT

Capacitive humidity sensor is used by the DHT11 to measure humidity. It is made up of two electrodes which are separated by a moisture holding substrate. 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.

3.2.2.1.2 TEMPERATURE MEASURING COMPONENT

The DHT 11 sensor makes use of a NTC thermistor sensor for 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 built 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.

3.2.2.2 TECHNICAL SPECIFICATIONS

Operating Voltage	3.5v to 5.5v
Protocol	a serial transmission
Measuring Range	i. Temperature (0°C to 50°C) ii. Humidity (0% to 100%)
Precision	±0.5°C and ±1%
Sampling Rate	0.5 Hz once every two seconds

Figure 3-2:DHT11 technical specification

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 SMSs or placing and receiving voice calls via GSM transmission. It has a relatively low cost and is capable of supporting long range connectivity

3.2.3.1 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 it’s logged on to a network.

3.2.3.2 TECHNICAL SPECIFICATIONS

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

Figure 3-3: SIM800L Technical Specifications

3.2.4 ELECTRONIC RELAY MODULE

A relay module is a switch that uses the principle of magnets and electro magnets to regulator circuits. A Relay is operated electronically by charging and discharging it. (Padmanabhan, 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 19 forces to open or close circuits. The electromagnet needs a low voltage to energy it. High voltage electronic device can be controlled using relay modules.

3.2.4.1 PRINCIPLE OF OPERATION

(Padmanabhan, 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.

3.2.5 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.

3.2.5.1 TECHNICAL SPECIFICATIONS

Interfaces	Digital IO
Operating Voltage	5 V
Operating Current	35 mA

Figure 3-4:relay Technical Specifications

3.2.6 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 research I will use a 830 pin bread board.

3.2.7 JUMPER CABLES

Jumper cables are copper wires that are covered with plastic for insulation and then joined to a connector or tip to allow them to facilitate an easy way to connect components. They are commonly 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 colors 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 surveillance system.

3.3 SCHEMATIC DIAGRAM OF THE DATA CENTER SURVEILLANCE SYSTEM

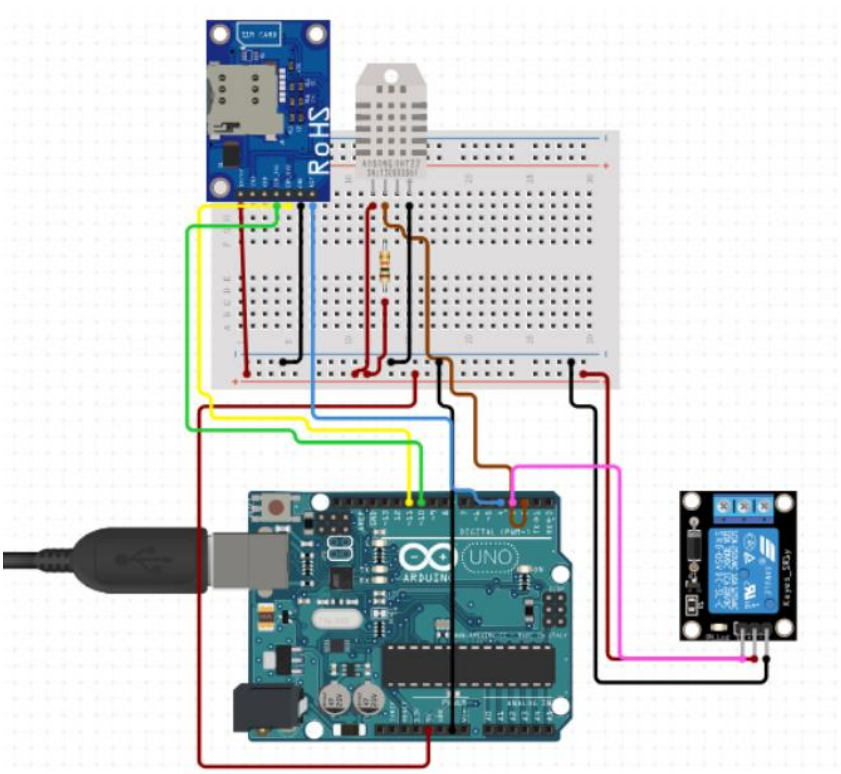


Figure 3-5: Schematic Diagram of the Data Center Surveillance system

3.4 EXPLANATION OF WORKING OF THE DATA CENTER SURVEILLANCE SYSTEM

The data center surveillance system is first configured and after configuration it will be in active mode and ready for deployment. During configuration, the technicians will set the tolerable temperature and relative humidity ranges. The tolerated extreme temperature and relative humidity range, as well as the window period that the data center surveillance system is allowed wait before shutting down the server are also set. After deployment the data center surveillance unceasingly 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 surveillance system 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 surveillance system 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 DHT11 module is responsible for collecting the temperature and humidity readings which are processed by the Arduino UNO. The SMSs 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.

3.5 THE DATA CENTER SURVEILLANCE SYSTEM SOFTWARE DESIGN

The data center surveillance system 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 surveillance system 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 surveillance system 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 surveillance system is an artificially intelligent agent system with no memory so as to make it a cheap and viable solution.

3.6 THE DATA CENTER SURVEILLANCE SYSTEM SMSs 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.)."

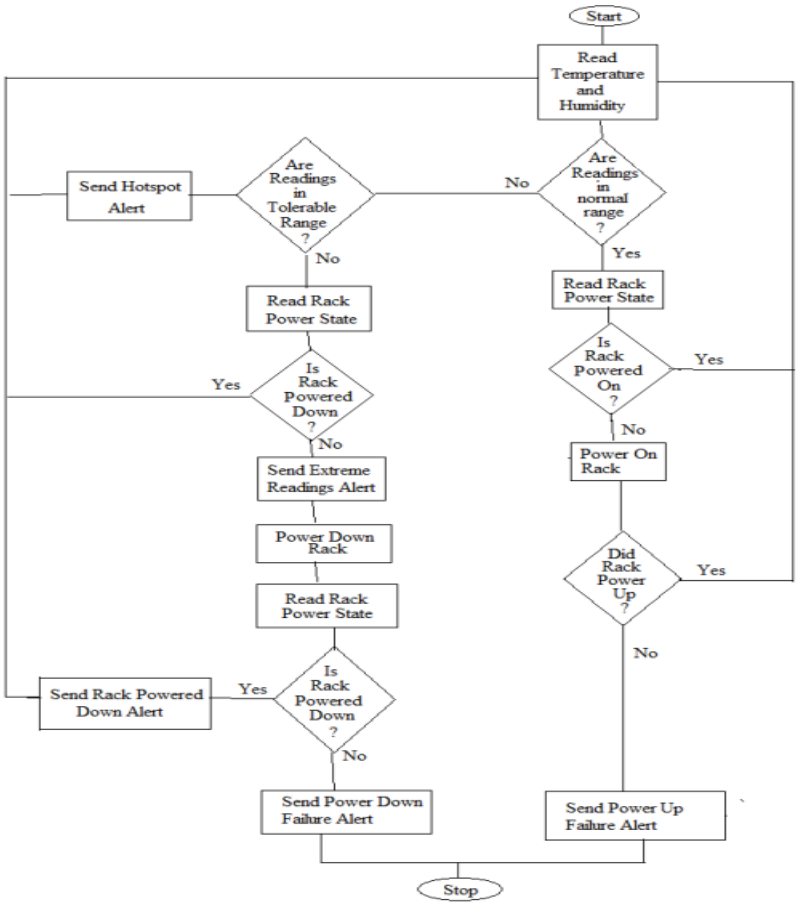


Figure 3-6: Data Center Surveillance flowchart

3.7 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 surveillance system graphically 25 through a flowchart. The following chapter was aimed at building the actual prototype of the data center surveillance system, running simulated tests and implementing the data center surveillance system

4 CHAPTER 4: SIMULATION AND IMPLEMENTATION

4.1 INTRODUCTION

The preceding chapters focused on widely reviewing the data center surveillance system's structure as well as revealing the functions and principles of operation of the various components which make up its build. In this chapter, I will focus on bringing the data center surveillance system to life, running simulations to verify its functionality against its objectives as well as its implementation.

4.2 INTERFACING COMPONENTS

This refers to the process of physically connecting the various shields that makeup the surveillance system as well as executing the test code.

4.2.1 INTERFACING THE DHT11 SENSOR MODULE

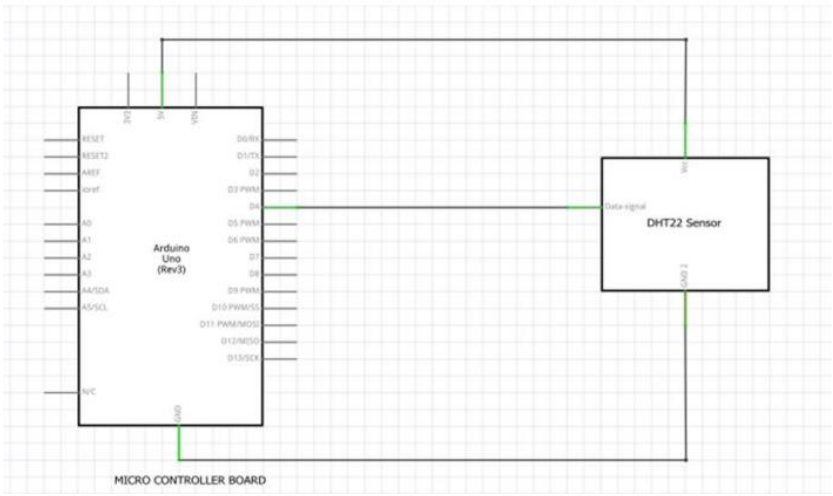
The DHT11 Sensor I will use in the development of the data center surveillance system is a 3 pin DHT11 sensor which have an on board pull up resistor for current regulation. It uses UART to communicate via serial with the Arduino Uno. The Pin at the extreme left is the VCC Pin and the one next to it is the data pin and the pin at the extreme right is ground pin.

4.2.1.1 WIRING

DHT11 PINS (STARTING FROM THE LEFT)	ARDIUNO PINS
Pin 1- VSS pin	5V power supply line on the breadboard
Pin 2- GND pin	GND pin
Pin 3- Data pin	D I/O pin 7

Table 4-1:DHT11 pin connection

4.2.1.2 CONNECTION SCHEMATIC



4.2.1.3 TEST CODE

Figure 4-1: DHT11 test code

4.2.1.4 OUTPUT OF THE DHT11 MODULE INTERFACING

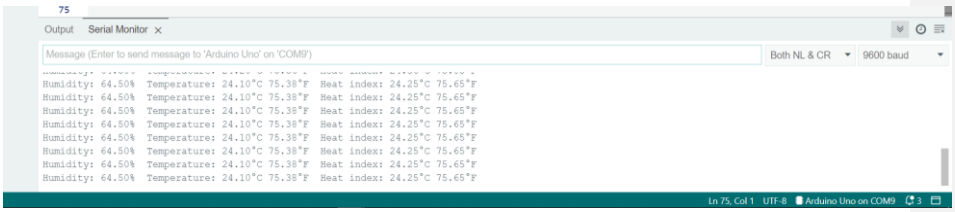


Figure 4-2: DHT11 test results

4.2.2 INTERFACING THE SIM800L MODULE

The SIM800L is a GSM Module that has a 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. I will use the latest SIM800L in the construction of the data center surveillance system. It will be connected with the Arduino using the RXD, TXD, VCC and GND.

4.2.2.1 WIRING

SIM800L pin	Arduino
Vcc	5V pin
RXD	D I/O pin 2
TXD	D I/O pin 3
GND	GND pin

Table 4-2:GSM module pin connections

4.2.2.2 CONNECTION SCHEMATIC

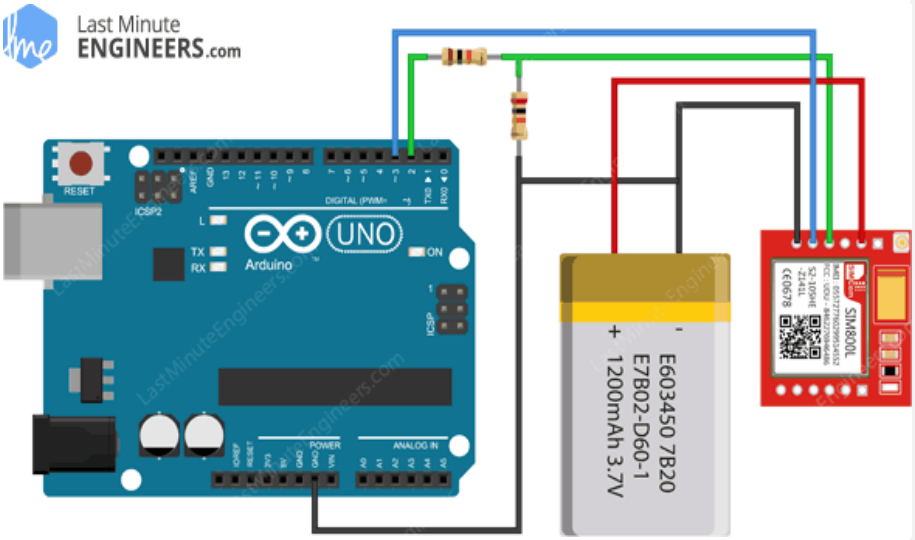


Figure 4-3:GSM800l module schematic diagram

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. I will interface the relay with the Arduino using 3 pins namely the VSS, GND and the control signal.

4.2.3.1 WIRING

Relay pins	Arduino pins
VSS pin	5V pin
GND pin	GND pin
Control signal pin	D I/O pin 5

Table 4-3: RELAY module pin connections

4.2.3.2 CONNECTION SCHEMATIC

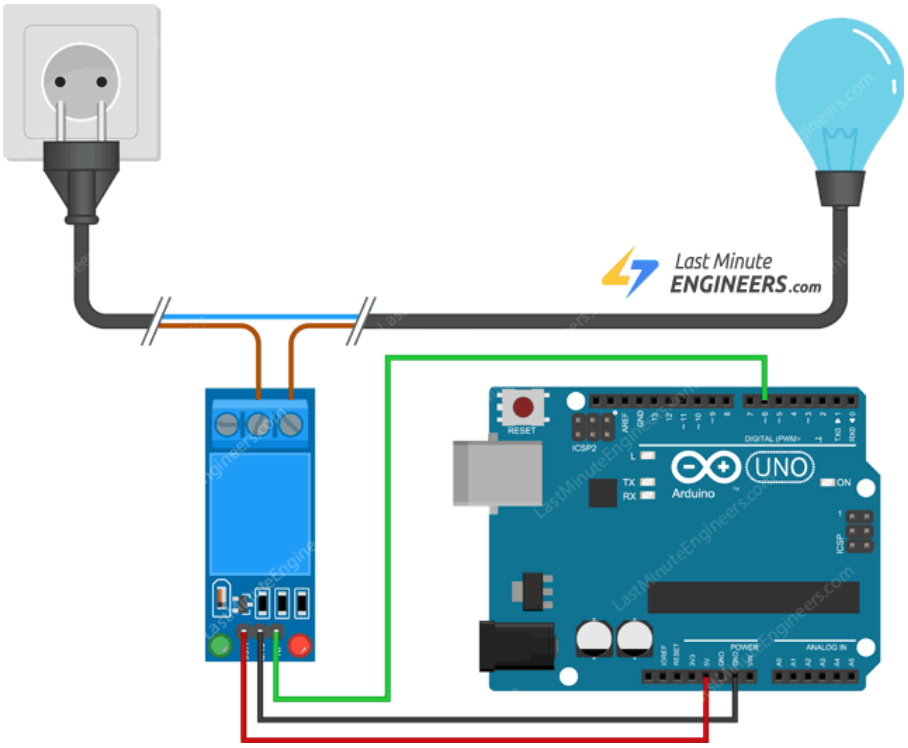


Figure 4-4:relay module schematic diagram

4.2.3.3 TEST CODE

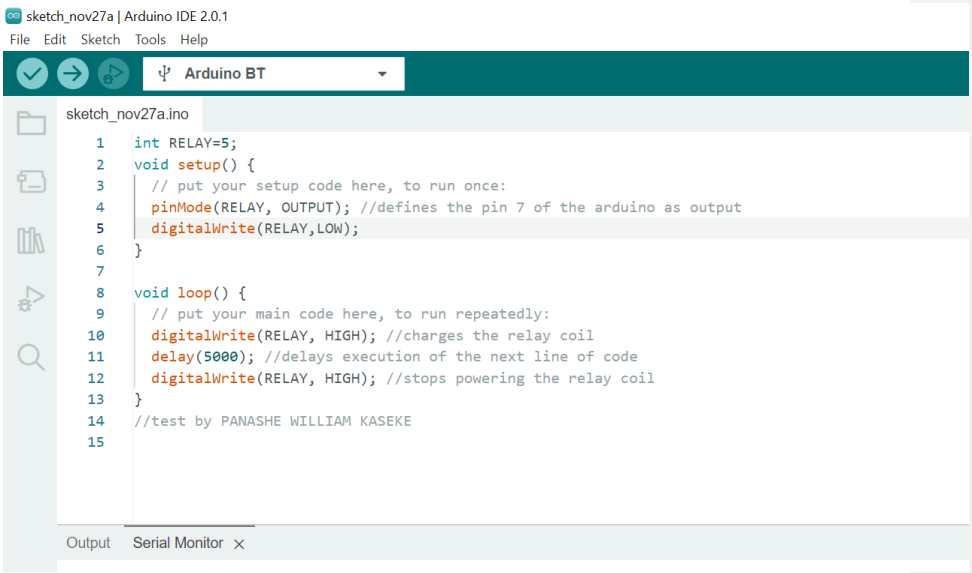


Figure 4-5:test code for relay module interfacing

4.3 SECURITY DESIGN

In this section, I will focus on security trials that can be put in place to protect the system from intruders.

4.3.1 PHYSICAL SECURITY

Normally every data center is equipped with CCTV cameras to record events of people entering the data center and all the actions that they took while inside. This system will be used to ensure the security of the data center surveillance system.

4.3.2 NETWORK SECURITY

The data center surveillance system is 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 surveillance system by physically visiting where the data center surveillance system is stationed.

4.3.3 OPERATIONAL SECURITY

The data center surveillance system operates with minimum human interaction with the technicians. The data center surveillance system is 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 surveillance system to alert him or her using the same number otherwise the surveillance system 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 power it up.

4.4 WORKING OF THE DATA CENTER SURVEILLANCE SYSTEM to

The data center surveillance system is activated by powering it with a 9V 2A power supply. Once active, the data center surveillance system will unceasingly fetch current temperature readings from the DHT11 sensor. Basing on these readings and the tolerated temperature levels set by the technicians during configuration, the data center surveillance system 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 surveillance system is said to be in normal operation if the readings of the temperatures fall within the set normal threshold. The surveillance system will continuously monitor the rack temperatures. Also, the relay will be turned on.

4.4.2 HOTSPOT DETECTED MODE

If the rack temperature rises directly above the set normal temperature range but falls within the set tolerated extreme temperatures, the surveillance system Also, will change into the hotspot detected mode. Once in this mode the surveillance system 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 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 surveillance system 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 surveillance system will notify the technicians that the temperature has restored to normal and system will let the rack return to 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 surveillance system will alert 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 surveillance system will power off the rack. The data center surveillance system will continue monitoring the rack temperature and will again notify the technicians when the temperature levels fall into the normal range but however it does not require the technician to press the reset button for the system to power up the rack, it will automatically power up the rack when temperaters lowers to normal ranges.

4.4.4 SYSTEM FAILURE MODE

The data center surveillance system will be made up of several components and during its operating, if one component of the data center fails, the surveillance system 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 is 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.

TYPE OF DATA	DHT11 READING	EXPECTED ACTION	ACTION EXECUTED
Normal	22 to 25	Works properly	Works properly
Extreme	25.1	i. Send Hotspot detected SMS Alert	Hotspot detected SMS Alert was sent
Abnormal	27	i. Send Out of Range temperatures detected SMS Alert ii. Power down Rack.	Send out of Range temperatures detected SMS Alert was sent. And Rack was powered down.

Table 4-4: operating test

4.6 IMPLEMENTATION AND RESULT

This 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, DHT11 sensor for temperature readings input and a Relay to power on or off the rack. The end result for the surveillance system is a system that takes in inlet air temperatures from its real time environment and sends alerts. In the actual setup of

the surveillance system, in every rack of the cabinets, there is supposed to be a DHT11 sensor to take temperature readings, 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 realization of green sustainable IT.

4.7 PRACTICAL SET-UP AND RESULT

The practical setup joins all of the different components of the system which make up the complete data center surveillance system realization. In the rack, there is a DHT11 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 surveillance system and status LEDs for indicating the current rack status.

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 surveillance system.

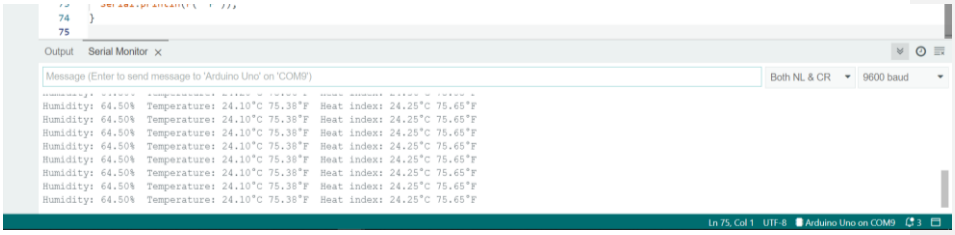


Figure 4-6: serial output of data center surveillance system monitoring temperature in real time

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: The diagram below shows SMS alerting Data center technicians of hotspot from the data center surveillance system.

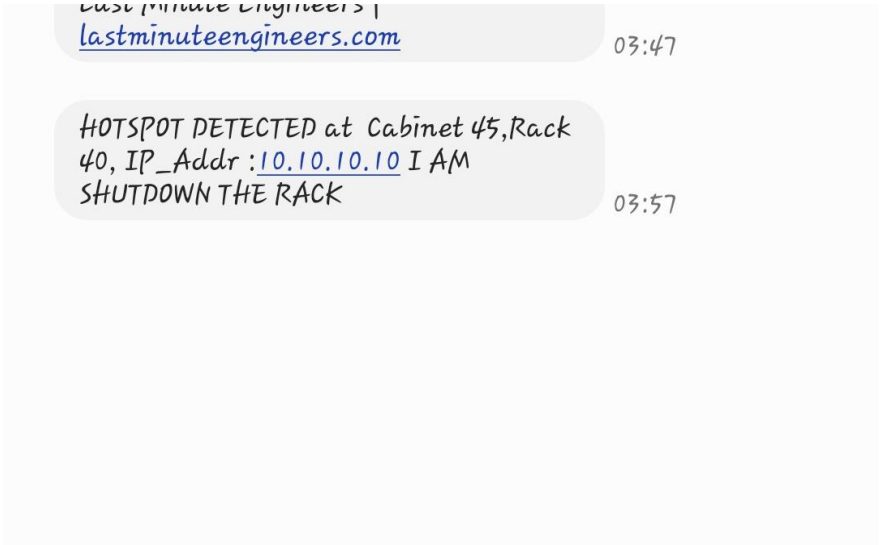


Figure 4-7: SMS send by the system

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

Results: The diagram below shows SMS alerting Data center technicians of extreme temperature and relay module transition from normal temperature to extreme temperature.

Figure 4-8:relay module ectivated by hotspot

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 surveillance system from the wiring stage as wells as providing illustrations of results from a successful interfacing. It also focused on running the data center surveillance system in a simulated environment so as to assess its performance and also to confirm whether the data center surveillance system meets its requirements. The next chapter will focus on giving recommendations of what can be added to the system in its next revision.

5 CHAPTER 5: CONCUSION AND RECOMMENDATIONS

5.1 INTRODUCTION

In the previous chapters, I introduced the data center surveillance system, exposing how it works and running tests and simulations as well as testing the system against its objectives. In this chapter I will focus on conducting a discussion on the data center surveillance system, 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 surveillance system prototype was successfully made using a minimal number of modules. With the application of these surveillance systems 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 surveillance system 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 Surveillance system are:

i. the DHT11 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 surveillance system goes down.
iii. The data center surveillance system real-life will require the technician's intervention to properly shutdown the rack equipment for example the surveillance system 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 surveillance system 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 surveillance system far, 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 DHT11 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 surveillance system should funds suffice, the surveillance system 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 surveillance system.

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 surveillance system was successfully developed and met all its objectives hence the research can be deemed as a success. The data center surveillance 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.

6 REFERENCES

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

SYSTEM CODE

```
#include <Wire.h>
#include <SoftwareSerial.h>
#include <Adafruit_Sensor.h>
#include <DHT.h>
#define DHTPIN 7
#define DHTTYPE DHT11   // DHT 11
DHT HT(DHTPIN, DHTTYPE);

#include <SoftwareSerial.h>
//Create software serial object to communicate with SIM800L
SoftwareSerial mySerial(3, 2); //SIM800L Tx & Rx is connected to Arduino #3 & #2

#define relayPin6 6
int sensePin = 2;
int humidity;
//float tempC
float tempF;
const int setTime = 50; //takes a measurement every 50ms
const int waitT = 5000; //Delay time in ms
String AlertMsg="", Rack_Details=" Cabinet 45,Rack 40, IP_Addr :10.10.10.10";


void setup() {
  // put your setup code here, to run once:
 Serial.begin(9600);
 Serial.println(F("DATA CENTER SURVEILLANCE SYSTEM, BY PANASHE WILLIAM KASEKE"));
 HT.begin();

  digitalWrite(relayPin6, OUTPUT);
  pinMode(relayPin6, OUTPUT);
  delay(setTime);

 //Begin serial communication with Arduino and Arduino IDE (Serial Monitor)
  Serial.begin(9600);

  //Begin serial communication with Arduino and SIM800L
  mySerial.begin(9600);

  Serial.println("Initializing...");
  delay(1000);
```

```
  mySerial.println("AT"); //Once the handshake test is successful, it will back
to OK
  updateSerial();

  mySerial.println("AT+CMGF=1"); // Configuring TEXT mode
  updateSerial();
  mySerial.println("AT+CMGS=\"+263785557541\"");
  updateSerial();
  mySerial.print("HOTSPOT DETECTED at "+ Rack_Details + " I AM SHUTTING-DOWN THE
RACK" ); //text content
  updateSerial();
  mySerial.write(26);

}

void loop() {
  // put your main code here, to run repeatedly:
delay(2000);
  float h = HT.readHumidity();
  float t = HT.readTemperature();
  float f = HT.readTemperature(true);
  if (isnan(h) || isnan(t) || isnan(f)) {
    Serial.println(F("Failed to read from DHT sensor!"));    //code by PANASHE
WILLIAM KASEKE
  return;
  }

  float hif = HT.computeHeatIndex(f, h);
  float hic = HT.computeHeatIndex(t, h, false);
  Serial.print(F("Humidity: "));
  Serial.print(h);
  Serial.print(F("%  Temperature: "));
  Serial.print(t);
  Serial.print(F("°C "));
  Serial.print(f);
 Serial.print(F("°F  Heat index: "));
  Serial.print(hic);
  Serial.print(F("°C "));
 Serial.print(hif);
  Serial.println(F("°F"));

  if (t <= 26.00) {
    digitalWrite(relayPin6, HIGH); //If the room temp is below nothing happened
    }
```

```
  else if ((t >= 27.01) && (t <= 40.00)) {
    digitalWrite(relayPin6, LOW); //If the room temp is betweem 75°F and 80°F the
YELLOW LED will be on.
    updateSerial();
  }

  else if (t >= 40.00){
  digitalWrite(relayPin6, LOW); //If the room temp is below 75°F the GREEN LED
will be on.
  updateSerial();

  }
  else Serial.print("error 44");



  delay(waitT); //Screen prints a reading every 5,000ms!1000ms = 1 second.
}
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
  }
}
```