Available Online at www.ijcsmc.com/journal

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 7.056

IJCSMC, Vol. 11, Issue. 12, December 2022, pg.53 – 60

An IOT Based Data Loss Prevention Regulatory System in the Zimbabwean Telecommunications Sector

Chikumbirike Kudzai Carlos[1]; Eng. Mainford Mutandavari[2]; Crispen Mafirabadza[3]
Department of Information Technology
Harare Institute of Technology University
kudcarlo@gmail.com
mmutanda.vari@gmail.com
Harare Institute of Technology, P.O Box BE277, Belvedere Harare, Zimbabwe

DOI: https://doi.org/10.47760/ijcsmc.2022.v11i12.005

ABSTRACT: ***The regulation of server room controls that prevent data loss in Zimbabwe is mostly physical. Data loss can be caused by human and non-human factors. Non-human factors are mainly fires, rodents and rats, earthquakes, and tremors, low or high extreme humidity and floods, as well as high unregulated temperatures. These are the main commonly prevalent non-human attributes causing data loss in Zimbabwe. In order to regulate server room standards with a bias towards data protection. Inspections are random and physical. This means that physical travelling is required to each and every site in order to provide assurance that every data center is compliant with the server room regulations. This study therefore sought to design and develop an experimental set-up to understand how emerging technologies such as Internet Of Things can be used to remotely regulate and obtain simultaneous result from multiple data centers in real time. The developed system was designed using circuits and sensors that were mounted together on a Node MCU and the software developed using Arduino. Further studies may include automated regulatory action when an anomaly is observed.***

KEYWORDS- IOT based data loss prevention regulatory system.

I. INTRODUCTION

In with globally accepted regulations and standards such as the GDPR, [1] fundamentals of data protection include lawfulness, fairness and transparency, data minimisation, purpose limitation accuracy, minimal data retention and availability these fundamentals are only relevant and useful when the actual data is available.[13] The Zimbabwean Cybersecurity and Data protection Act [2] also further defines data subject rights as right to consent of processing, right to refuse automated processing, right to data portability, right to be forgotten among others. But unless data is available all these principles and rights will not be enforceable. Data therefore should be available and it is the duty of the regulator or Data Protection Authority (DPA) to ensure that practices by omission or commission that lead to data loss should be discouraged and not go without a reprimand or fines. Non-human threats to data availability especially in the server room are basically five. 1. Excessive heat- High temperatures above the standard recommended server room temperatures will cause tiny

components within the server room to over heat and malfunction. Servers run all day long even in moments when humans are asleep. This means that the temperatures must be conducive for continuous operation. A good range of temperatures in the server in between 20 to 22 degrees Celsius.[3] 2. Tremors and earth quakes- In Zimbabwe, tremors and Earthquakes are not uncommon when these become intense they may damage servers leading to data loss. 3. Humidity: Humidity below the recommended values may cause static electricity within the server room while moisture and flooding from leaking taps and excess rains may also damage the servers. An optimal humidity level for a server room is between 40-55.[4] 4. Fire: Fire and flames destroy servers and cause data loss. 5. Rodents and rats: these bite the cables and the servers causing data unavailability.

II. METHODS AND MATERIAL

In this section, hardware, software and sensors used in the development of an IoT based data loss prevention regulatory system is presented. The project aims at providing a solution that provides a framework for the regulator to detect breaches of server room standards and rules that may potentially lead to data loss, in line with the Zimbabwean Data Protection Act. The proposed system will regulate and recommend detective, preventive and corrective controls to all threats that may compromise data security within the telecommunications sector in Zimbabwe. This project alerts the regulator remotely through the use of IoT, about breach of data centre standards that have a potential of threatening the security and or existence of data residing in data centres and servers. . In this project Node MCU controller was used to link between the sensors and internet and uses data from sensors to regulate the behaviour of controlling elements. This system will flag threats to data such as excessive heat, floods, rodents and any other creeping creatures that may bite off cables leading to server and data loss. The use of technology has grown in the past years and consequently data mobility has also increased in the past few years. [13]. The designed system is elastic and scalable. Table 1.1 provides detailed description of the tools used in their broad categories: hardware, software, and sensors used.

Table1: List of the required hardware, software, and dataset for the experiment

Software	**Purpose**	**Source from which it was obtained**
Proteus	Design and simulation of system circuitry	Open Source Application Software
Node Red	Developing the web interface for remote logging to the virtualised cloud environment	Open Source Application Software
Arduino	Programming the API to perform the map reduce function	Open source application software
Linux	Operating system supported by the application	Open source application software
Windows 10+	Operating System supported by the application	Microsoft
Hardware		
Laptop – HP EliteBook	Accessing the platform	HP
Sensors used		
DHT11 Sensor	A sensor that detects humidity levels in the server room that are out of range. This sensor also measures temperatures out of range within the server room.[8]	
Flame Sensor	A sensor that detects presence of the properties of flames that may destroy servers and data [9]	
PIR Sensor	Passive Infrared Sensor for the detection of rodents mice and rats that might destroy servers and data[10]	
Vibration Sensor	This sensor detects vibrations that may signify existence of tremors and earthquakes.[11]	

III. RESULTS

The section provides experimental results of the IOT based Data loss prevention regulatory system in the Zimbabwean Telecommunications sector. The purpose of this research was to provide a regulatory framework that helps regulators make necessary interventions to prevent data loss and security breaches in line with the new Data Protection Act. A recap of the objectives of this system may help inform the structure followed in this section. The system developed had the following objectives:

- To detect data centre regulatory breaches
- To develop a regulatory technology that informs the regulator when ISP's and MNO's breach server regulations.
- To provide a regulatory response to potential data breaches.
- To provide a framework that propels data loss awareness in Zimbabwe, bridging the digital divide.

As highlighted in the above research objectives the main purpose of this study was to design and develop an IOT based Data loss prevention regulatory system as the main engine behind the regulation of data protection processes in the data centres.

A. Design of the IoT based Data loss prevention regulatory system

The system is entirely based on the IoT technology. This structure allows server room conditions to be observed even without physically visiting the server room. Sensors are interfaced to the NODEMCU and operate at 5Volts. This NODEMCU has the functionality and capacity to generate its own Wi-Fi. A program developed using Arduino gives functionality to the Wi-Fi, access control and coordinates readings from the sensors in order to provide regulatory response.

By making it IoT based it serves huge resources on the part of the regulator because one does not have to physically visit data centres for inspections. Unless there is a real control breach to react to.

B. Overview of the system design architecture

HARDWARE DESIGN OVERVIEW

There are two main circuits; power supply circuit and the main circuit i.e. NODEMCU circuit.

Power Supply Block Diagram

Figure__ below is the block diagram of the power circuit.

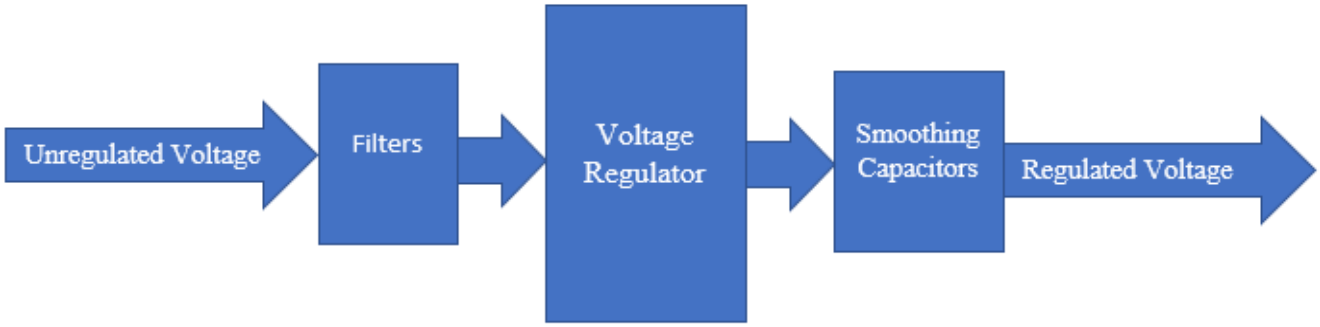


Figure 1. Power Supply Block Diagram

Circuit Design

The NodeMCU ESP8266 Wi-Fi module because it has a self-contained [5]SOC with integrated TCO/IP protocol stack that can give my controller to my Wi-Fi. It also has a powerful on-board processing and storage

capability that allows it to be integrated with sensors and other application specific devices. Figures below shows some of the circuits designed for this system.

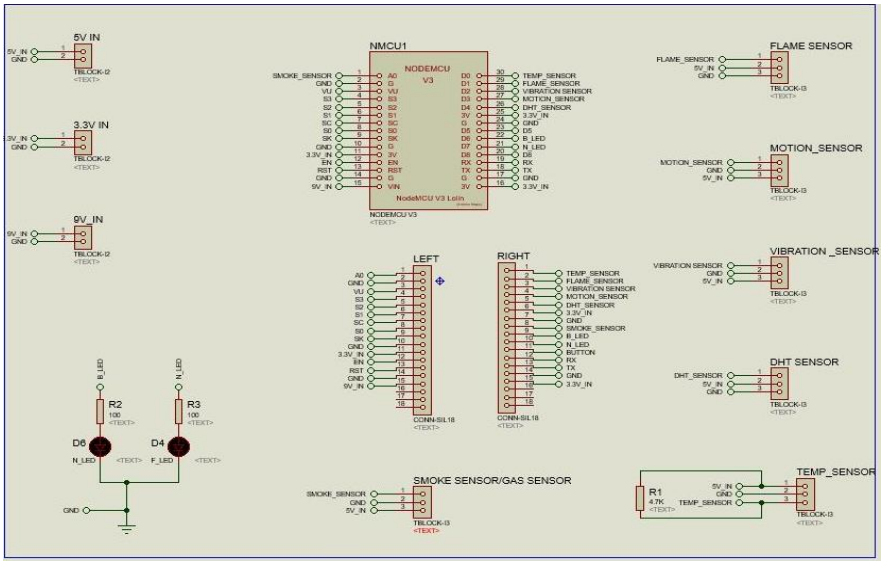


Figure 2. NODEMCU Circuit

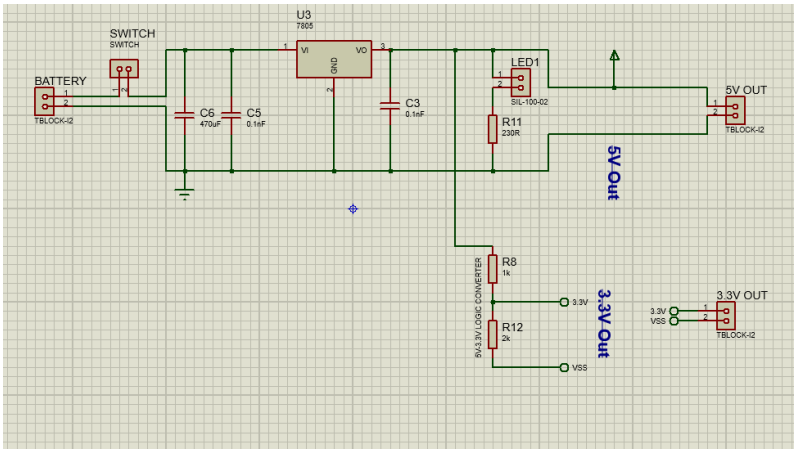


Figure 3 Power Supply Circuit

PCB Design

PCB was designed using proteus 8.9. which is easy to debug simulate and save files [6]. Both the virtual lay out and the schematic design view are documented below. Proteus uses ARES design suit to develop PCB layouts.

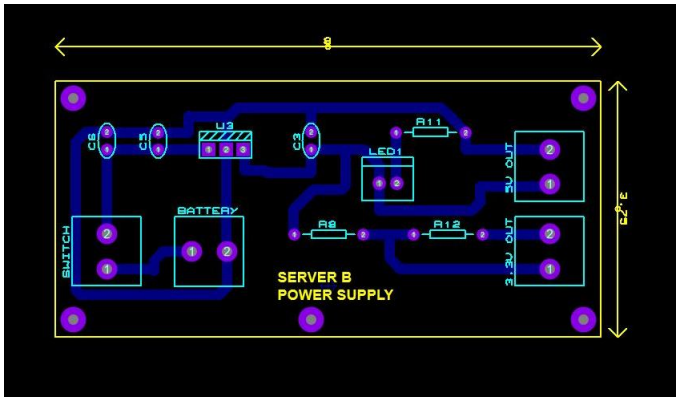


Figure 4. Power Supply PCB Circuit

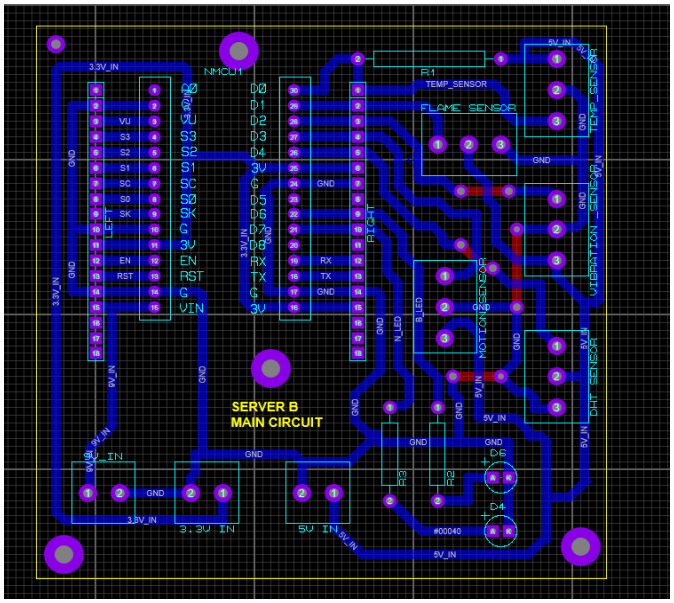


Figure 5. NODEMCU PCB Circuit

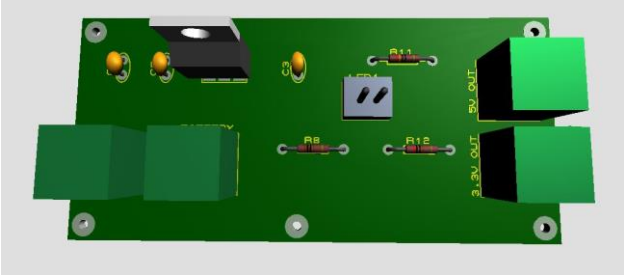
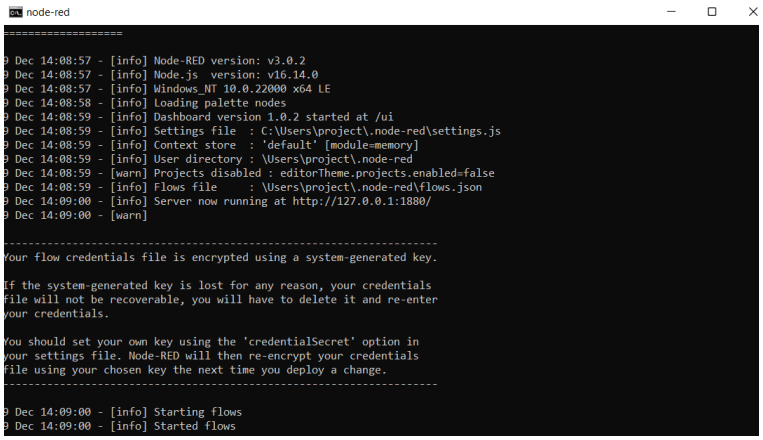


Figure 6. Power Supply 3D visual

The above diagrams show the 3D visuals of the created circuits both for the power supply and the NODEMCU showing how it will look on the actual circuit board.

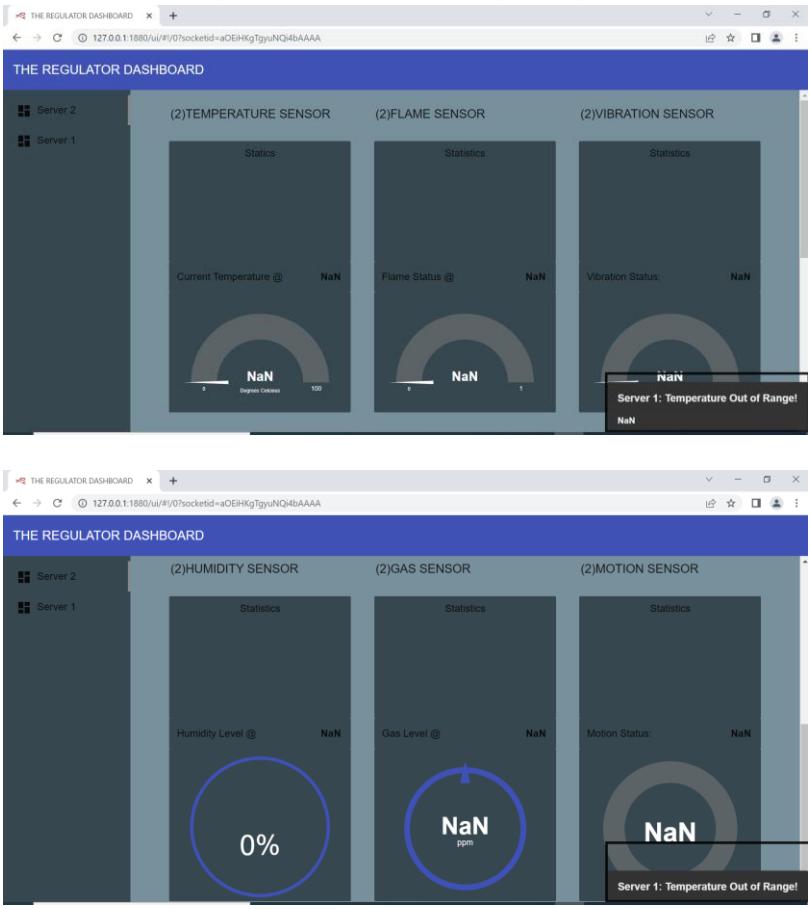
C. Application program and the user interface

Using Arduino the sensors will dump their readings into a secure file. Node Red, a web interface platform, will allow users to view the readings[7]. Node red will also validate the readings so that they become useful to the regulator. Upon running the interface as shown below details of flow credentials will be displayed:



The IP address that is used to access the NODE RED Interface http://127.0.0.1:1880/ backend and http://127.0.0.1:1880/ui for the user interface the dashboard will pop up as shown in table 2.

Table 2 Log on form to the Integrating API



Source: System Interface

D. Interpretation of Results

Each result will be displayed on the screen in an easy to interpret format. When conditions pose the risk of adverse effects on the servers and data the result comes out in red. With text that explain to the regulator the condition the risk and the action that the regulator ought to take in the prevailing circumstances. Risks and regulatory responses are displayed on the dashboard as follows:

Smoke

Red signifies smoke detection.

Risk: Smoke may signify presence of fire or spark within the server room which will destroy servers and data.

Action: Schedule a compliance inspection to verify presence of fire detection and suppresant system.

Tremours and Earthquakes

Red signifies tremour detection.

Risk: Tremours and earthquakes destroy servers and data.

Action: Schedule a compliance inspection to verify backup restoration or fail over to disaster recovery site.

Fires

Red signifies fire detection.

Risk: Fire will destroy servers and data.

Action: Schedule a compliance visit to verify that fire detection and suppresant system is present and effective.

Rodents and Mice

Red signifies unusual movement detected.

Risk: Rats and rodents bite cables and gear. This destroys servers and data.

Action: Schedule a compliance inspection to verify rodent repellants are installed.

Extreme Humidity
Red signifies unacceptable humidity.
Risk: Low humidity causes static electricity. High moisture conflicts with current cables. This destroys servers and data.
Action: Schedule a compliance inspection to verify that servers are on raised floors and HVAC.

High Temperatures
Red signifies high temperatures.
Risk: Overheating damages gear. This destroys servers and data.
Action: Schedule a HVAC compliance inspection.

IV. DISCUSSION

Results from the IoT Data loss prevention system in Zimbabwe significantly makes regulatory work more effective, efficient and continuous. By reading data that pertains to environmental threats to data, the system validates the readings against standards and best practices and provides the regulator with action plan. Servers run all day long and all year round, even in moments when human beings have retired for rest. The proposed system works all round the clock doing what human beings would have been doing in regulation. Regulators spend a lot of resources in compliance inspections. When they travel to all the server rooms in the country to perform routine inspections and sometimes on a sample basis. The chances of missing a non-compliant server room in the sample is a non-zero. With an automated system accuracy is improved. When a regulator then visits a server room it will be for issuing fines or initiating corrective action rather than just checking in case something is wrong. The above enhances accuracy, wider sample coverage, and continuous monitoring thereby reducing costs and time invested in physical inspections. The monitoring box unit with sensors does not need salary, leave days or maintenance funds this renders this system an automated tool that needs no human resources demands. The data sets from the sensors are straightforward, Motion detection, tremors, flame and fire is purely binary while temperature and humidity are analogue and continuous. All data is validated to see if it is below or above the acceptable ranges and a user-friendly dashboard interprets the results for the regulator.

V. CONCLUSION

The Zimbabwe data protection Act can only make sense if data is available. Non-human threats to the availability of data are fire, tremors, floods, rodents and unfavourable temperature and humidity conditions. If these are regulated a firm premise for the enforcement of the data protection act will be enabled. The IoT data loss prevention system targets threats to data availability that are common in Zimbabwe and other developing countries. It is capable of monitoring environmental server conditions in real time and on a non-sample basis. If all corrective action is implemented when server room standards are reached, the standard of data servers in the country and sector will be greatly improved. The major limitation that is key is the reliability of the system on electric power availability. In this environment where power outages are frequent. Alternatives such as battery power may for a limited time provide a solution. Internet of Things is an emerging technology that allows many devices to be interconnected and this has provided many advantages in this world of regulatory collaboration.[12] Proper maintenance of the equipment however remains key. So that sensors will not be affected by dust moisture that may impair readings and functionality. It also imperative that the box kit be connected to power via a UPS (Uninterrupted Power Supply) system to avoid damages due to power surges.

VI. Recommendations

In line with the objectives and broad expectation in the regulator sector the following recommendations represents opportunities for future work as well as areas of improvement to this system:

- MSD explores the use of Hadoop MapReduce software in a cloud-based environment to manage its data, in order to reap the optimization and predictive power of the tool while introducing cloud-based approach to extraction, accessing, manipulation and transmission of the data.
- Further research might be necessary to explore a similar technology that run on natural sources of power such as solar or wind.
- Web based display interface is only relevant when a regulator has an active internet connection. However, some regulators may not have a reliable consistent internet connection and in such a situation an email based solution may be more preferable. Where an email is sent to a data protection officer or regulator if a breach occurs.

REFERENCES

[1]. EU commission, GDPR, https://gdpr-info.eu/ 2018.
[2]. Zimbabwean Parliament, https://media.zimlii.org/files/legislation/akn-zw-act-2021-5-eng-2022-03-11.pdf , 2021.
[3]. Server room temperature, https://www.theseverngroup.com/category/cooling-solutions/, April 5, 2017.
[4]. By Doug N, Recommended Server Room Temperature and Humidity, https://www.poweradmin.com/blog/recommended-server-room-temperature-and-humidity/, February 11, 2021.
[5]. Insight Into ESP8266 Node-MCU Features & Using It With Arduino IDE, https://lastminuteengineers.com/esp8266-nodemcu-arduino-tutorial/, 2022.
[6]. Bo Su; Li Wang "Application of Proteus virtual system modelling (VSM) in teaching of microcontroller", https://en.wikipedia.org/wiki/Proteus_Design_Suite, 2010.
[7]. Arduino book, https://www.academia.edu/36930186/ARDUINO_BOOK_pdf, 2022.
[8]. DHT22 temperature and humidity sensor, https://create.arduino.cc/projecthub/MisterBotBreak/how-to-use-temperature-and-humidity-dht-sensors-9e5975, February3 2019.
[9]. Flame sensor working principle, https://www.elprocus.com/flame-sensor-working-and-its-applications/, 2022.
[10]. PIR sensor working principle, https://quickandeasylighting.com/what-is-a-pir-sensor/, 2021.
[11]. Vibration sensor, https://www.wellpcb.com/Vibration-Sensors.html, 2022.
[12]. Gillis, A. S. (n.d.). What is the internet of things (IoT)? Retrieved from tech gadget: https://www.techtarget.com/iotagenda/definition/Internet-of-Things-IoT.

