UNIVERSITY of RWANDA

ACEIoT

Website: www.aceiot.ur.ac.rw

Mail: aceiot@ur.ac.rw

College of Science and Technology

AFRICAN CENTER OF EXCELLENCE IN INTERNET OF THINGS

Research Thesis Title:

GIS-BASED ELECTRICITY FRAUD DETECTION SYSTEM USING IOT:CASE STUDY:

RWANDA ENERGY GROUP(REG)

A dissertation submitted in partial fulfilment of the requirements for the award of masters of science degree in internet of things: wireless intelligent sensor network

Submitted By:

BIZIMANA Zephanie (Ref. No: 217291740)

December,2022

UNIVERSITY of RWANDA

ACEIoT

Website: www.aceiot.ur.ac.rw

Mail: aceiot@ur.ac.rw

College of Science and Technology

AFRICAN CENTER OF EXCELLENCE IN INTERNET OF THINGS

Research Thesis Title:

GIS-BASED ELECTRICITY FRAUD DETECTION SYSTEM USING IOT:CASE STUDY: RWANDA ENERGY GROUP(REG)

A dissertation submitted in partial fulfilment of the requirements for the award of masters of science degree in internet of things: wireless intelligent sensor network

Submitted By:

BIZIMANA Zephanie (Ref. No: 217291740)

SUPERVISORS: Dr. Emmanuel MASABO

Dr. Omololu Akin-Ojo

December,2022

Declaration

I **BIZIMANA Zephanie**, Master student from African Center of Excellence in Internet of Things, at University of Rwanda. I declare that this research thesis is my own original work, and it has never been presented before anywhere in the world.

Zephanie BIZIMANA

Ref: 217291740

Signed: ………………………….

Date: ……/……/……

Bonafide certificate

This is to certify that this submitted Research Thesis work report is a record of the original work done by **BIZIMANA Zephanie** (**Ref. Nu: 217291740**), MSc. IoT-WISENET Student at the African Center of Excellence in Internet of Things/ College of Science and Technology/ University of Rwanda, the Academic year 2020-2022.

This work has been submitted under the supervision of **Dr. Emmanuel MASABO** and **Dr. OMOLOLU AKIN-OJO.**

Main Supervisor: **Dr. Emmanuel MASABO** Co-Supervisor: **Dr. OMOLOLU AKIN-OJO**

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

Signature Signature:

The Head of master’s and Training

Dr. James RWIGEMA

Date: ……………………….

Signature…………………

Acknowledgments

I would like to raise up the name of the Almighty God, who gave me the grace to accomplish this work. I would like to express my deepest appreciation to my supervisors **Dr. MASABO Emmanuel** and **Dr. Omololu AKIN-OJO** for their endless support and guidance given to me during this journey to make this thesis successful. I’m deeply indebted to my friend Roger MIZERO for the help with the accommodation provided to me. I would also like to extend my deepest gratitude to my wife, my son, and my daughter for the way they treated me during my studies. I’m extremely grateful to my parents and parents-in-law, the completion of my thesis would not have been possible without their support and nurturing of them. I wish to thank the African Center of Excellence in the Internet of Things, College of Science and Technology, University of Rwanda. I also wish to thank my family members who have done great sacrifices by providing me with all the necessary means to have a good education.

I thank my classmates, especially those who were together in groups in all academic activities for their direct and indirect contribution to the achievement of my objectives. Lastly, my appreciation goes to the lecturers on the Internet of Things for the good job done during the 2 years of our courses. My acknowledgment goes to everyone who supported me in my everyday life to reach this accomplishment.

May the Almighty God bless you all!

Abstract

Adequate electricity is a main challenge in low income (developing) countries. Reducing technical and non-technical losses of electricity is, thus, important. This research aims at detecting the non-technical losses that are caused by electricity users who bypass the electricity meter and get electricity for free (theft), thus, lowering the financial income of the electricity utility companies. Beyond the detection of this fraud, this work will help identify the defaulters and proposes a new approach of apprehending these fraudulent customers by introducing a system that compares the input and the output currents. If there is a mismatch in these quantities, the system activates a counter to start reading the amount of electricity stolen, reports the duration of theft, and communicates directly with the branch manager of the utility company. The address and location of the fraudster as well as the historical data of electricity usage will be displayed (kept) and stored in a cloud and allow only authorized officials of the electricity board to keep track of all the frauds, areas of fraud, and the routes to reach the areas where the frauds are committed.

Keywords: Geographic Information System (GIS), Electricity fraud, internet of things (IoT),Thingspeak.

List of tables

List of Figures

LIST OF ACRONYMS/ABBREVIATION

AC	Alternative current
REG	Rwanda Energy Group
SG	Smart Grid
W	Week
RURA	Rwanda Utility Regulatory Authority
RQ	Research Question
RO	Research Objective
ML	Machine Learning
CT	Current Transformer
LCD	Liquid Crystal Display
DC	Direct current
PT	Potentiometer
SMS	Short Message Service
TL	Technical Loss
NTL	Non-Technical Loss
GIS	Geographical Information System
IOT	Internet of Things
i.e	I mean
ACEIOT	African Center of Excellence in Internet of Things
EBO	Electricity Board Officials
GSM	Global System for Mobile Communication

TVS	transient-voltage-suppression
MQTT	Message Queuing Telemetry Transport
REST	Representational State Transfer

Contents

Chapter 1: Introduction

1.1.Background introduction

In most countries worldwide, especially in Rwanda where there is currently insufficient power for citizens, the losses in electric power distribution networks are a common reality for electric utilities. These losses can be classified as technical or non-technical losses, the technical losses are the electrical energy dissipated between the energy supply and the delivery points of the consumer while a non-technical loss is the difference between the total losses and the technical losses, i.e. all other losses associated to the electric power distribution, such as energy frauds, metering errors, errors in the billing process, etc. This type of loss is directly related to the distributor's commercial management[1].and this leads to lower financial income for the providers.

One of the methods used to decrease electricity fraud is to do regular inspections which is tiresome and requires a budget to be allocated to this activity. Sometimes the fraudsters may be warned by one of the staff about this activity and disconnect, such that when the inspectors reach the field, they do not find any theft action, yet they carry out this illegal act. The fraudsters may even connect every evening and disconnect in the morning. According to ref.[2], the authors said that with global energy consumption on the rise, energy conservation is key to avoid unnecessary wastage. One way through which today's energy problems can be remitted through the elimination of energy fraud in households.

Electricity theft (fraud) has engendered big losses over the world. The tendency of its preservation constantly evolves even as smart technologies such as smart meters are deployed, although smart meters come under some ambushes, they provide sufficient data that are probed by clever strategies for effective observation and notice of compromised situation. Different techniques are being used but satisfactory results are yet to be obtained for real time detection of this electrical fraud with smart meters in ref.[3]. In ref.[2], the author says that with global energy consumption on the increase, energy conservation is the main point to avoid unnecessary wastage. One avenue through which today's energy problems can be addressed is through the reduction of energy usage in households.

1.2. Problem statement

In low-income countries like Rwanda where there is currently insufficient electricity for the citizens, the losses in electric power dispensation webworks are a common reality for the electric utility's losses can be classified as technical or non-technical losses, the technical loss is equivalent to the electrical energy immoderate between the energy supply and the delivery points of the citizen. On the other hand, a non-technical loss is the divergence between the total losses and the technical losses, i.e. all other losses associated with the electric power distribution, such as energy frauds, metering errors, errors in the billing process, etc. This loss type is directly connected to the provider's commercial management as mentioned in ref.[1] and this leads to lower financial income for the providers. Currently the total loss of Rwanda national Grid is equivalent to **19.1%** including both technical and non-technical loss while the commercial loss incurred due to electricity fraud is **6.5%** equivalent to **1.9 billion** Rwandan francs according to the authors in [4][5].

Some cases of electricity fraud involves meter tempering and bypass which is detected by inspection of technicians whereby the utility company selects some citizens' meters to check on a field visit randomly, this is tiresome and expensive in terms of financial resources as said in [6].

1.3.Research questions

RQ1. How do you inspect the customer's electricity usage?

RQ2. What are components of smart meter fraud detection system?

RQ3.what are the features of the smart meter to be designed?

RQ4. How do you get notified by smart meter about electricity fraud?

RQ5. Using smart meter, how do you measure the amount of energy stolen?

1.4.Aim and objectives

The aim of this research project is to design a cost effective and efficient power fraud detection system using internet of things (IoT). This system allows the energy utility managers to detect and monitor power usage at the household level in real-time and helps to reduce power theft activities. To achieve this goal the project will focus on the following specific objectives:

1.4.1. General objective

The general objective of the research study is to design an autonomous system to report electricity fraud, area of fraud in real time and to store data in the cloud.

1.4.2. Specific objectives

To achieve our general objective, specific objectives that must be achieved are as follows:

1. To assess and study the system requirements
2. To Design smart cash power detection system
3. To test and validate the system functionalities.
4. To monitor electricity usage of each household.

1.5. Features of the system will be like this:

- To calculate (compute) and display the amount of stolen electricity.
- To show the period (time) of electricity theft.
- To notify the energy utility manager.
- To indicate the location of the fraudsters.

Chapter 2: Literature review/ Research gap

2.1. Introduction

This chapter discusses related works and finds the limitations and suggests the contributions to adding them for efficient electricity fraud monitoring and detection. In this part, a review of the background of this research is discussed. Related works are presented. Similarities and dissimilar features with previous conferences, journals and articles are also highlighted. Some of the parameters, tools, technologies that are ignored by some previous researchers are highlighted and our scientific research is presented.

2.2. Review of related works

This research focuses on integrating technology usage in electricity monitoring, different authors tackled this area where they proposed different solutions and perspectives. As technology advances the customers are also wise and use different methods. Ref.[7] highlights that there are two methods of power theft, power theft is generally done by bypass or hook. So, to investigate power theft, a system is proposed in which the household distribution of current is done indirectly from the electric pole to an intermediate distributor box and then to the individual houses. The reference also says that current is calculated recurrently in the distribution box and is posted to the server database of each house using a GSM/GPRS module. The system uses GSM/GPRS to track and report the fraud detected.

The other author in ref.[8] mentions that the existing system for digging out the power theft is not a coherent one. The facility theft happening is detected while taking the energy meter readings by computing the difference between the facility received within the transformer of the source t and the destination. No measure is taken to forestall it. In ref.[9] , the authors describe a novel Convolutional Neural Network -Random Forest model introduced to investigate electricity stolen. According to authors, in Ref.[10], the information of stolen electricity is given to the Electricity Board Officials by using GSM and IoT technology, this system interfaces with the Arduino, the sensors interconnected with the Arduino to predict the current and voltage. This restrains electrical theft to its maximum. In Ref.[11], the authors stated various types of electrical power theft, including tapping a line or bypassing the energy meter. According to a study [11], 80% of worldwide theft occurs in private houses and 20% on commercial and industrial premises, If they try to investigate the fraud manually, it is not possible due to the large amount of data. So, here they applied machine learning algorithms to detect the theft. Fraud was detected by checking for abnormalities in the user's electricity consumption patterns. From user fundamental data, it is an easy task to analyze user behavior. They enacted a supervised ML-based theft detection model that identifies whether a fraudulent usage pattern has occurred in the SG (smart grid) meter. In ref.[12], the authors highlight that electricity fraud is through usually bypassing the energy meter but in this research, they specified the fraud by raising the load also and this method is cheap. In ref.[13], the authors stated that to recognize and monitor electricity theft an intelligent system was introduced. It consisted of two current transformers that are used to measure the actual load current, and the other is to measure the turning back or neutral current. Those two current signals are fed to a microcontroller. The microcontroller judges these two current signals. Depending on the comparison made by the microcontroller it concludes whether power theft through bypassing the energy meter or not and a message will be sent to notify the authorized power vendor using GSM Hence the power vendor can easily identify the customer who is illegally consuming the power for that energy meter. Moreover, when there is an occurrence of theft a relay will disconnect the load from the supply.

2.3. Summary of weaknesses identification and our scientific contribution

Based on related work, electricity fraud detection systems have been created using different technologies as cited in the literature review above. However, weaknesses have been identified and, through this research, a scientific and technological contribution is made to reinforce the culture of accountability and consumption in a perfect way.

2.3.1. Weakness identified

After reviewing the literature above and analyzing them, gaps have been identified. Details are provided in the table below.

Table 2.1: Gaps identified.

S/N	Authors	Topic	Contribution/ Achievements	Gaps identified
1	**k. Kumaran et al.**	**Power Theft Detection and Alert System using IOT**	Information of theft detection is provided to the EB officials by using GSM and Internet of Things technology	- Stolen electricity is not computed. - the address of fraudster not identified. - duration of theft is not shown.
2	**Shuan Li et al.**	**Electricity Theft Detection in Power Grids with Deep** **Learning and Random Forests**	A novel CNN-RF model is presented to detect electricity theft. In this model, the CNN is similar to an automatic feature extractor in investigating smart meter data and the RF is the output classifier. Hybrid model is used to detect electricity theft.	Investigating how the granularity and duration of smart meter data might affect this privacy. Notification of theft missing. - Compute the stolen electricity.

3	**Nitin K Mucheli et al.**	**Smart Power Theft Detection System**	The main objective of this connection is to measure the total current entering the electric meter. So, a fixed connection is made at the inlet terminal of the electric meter in such a manner that tampering of this connection is made void with the help of laser sensors and microcontroller.	- Compute the stolen electricity. - Duration of fraud.

Table 2. 1:Gaps identified

After reading different papers, journals and articles, the common gaps identified in the table above illustrates that the power stolen is not computed and when the energy utility catch the fraudsters by different means they estimate the amount of electricity stolen and this leads to a loss of financial income by electricity provider. Tracing the location of fraudsters is another gap identified; the duration of fraud is also not shown.

2.3.1. Scientific contribution

Our research works on the designing of a prototype for electricity fraud detection system that tracks the amount of stolen electricity, the location of fraud and the duration of the fraud. To address the limitations/challenges identified in all the previous works read and consulted, our research target is to design the electricity fraud detection system that autonomously monitors electricity fraud. A GSM based power theft control system is developed. We used Proteus software to analyze and estimate what the hardware will look like. Mainly this system consists of a microcontroller, energy meter, current transformers, LDR, relay, LCD, and GSM module.

This system is installed in the meter, if the customer tries to open the meter, the device will activate the alarm and send the message to the authorities to have updates on what is happening.

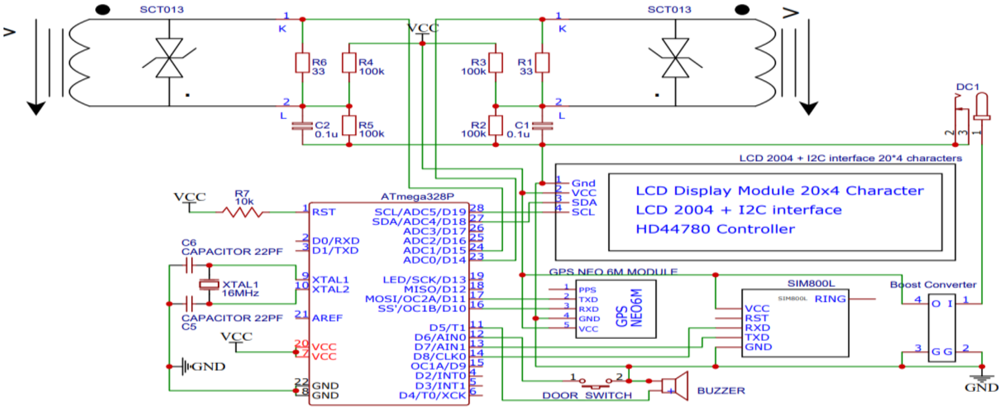


Figure 2. 1: Circuit diagram of the system **Source: Own drawing**

***Table 2. 2*: Component list used in the circuit diagram given in figure 1**

Components	Specifications
SCT 013	Current sensor SCT 013 30 Amps
R1 33, R6 33	Resistors of 33kΩ
R2 100K, R3 100K, R4 100K	Resistors of 100kΩ
R6 10k, R7 10K	Resistors of 10kΩ
C1, C2, C3, C4, C5, C6	Capacitors of different capacity
ATmega 328P	Microcontroller ATmega 328P
LCD	Liquid Crystal Display of 16 X2
Buzzer	Piezo electric buzzer
DC1	Power adaptor 12V
SIM 800L	GSM module of 800L
GPS NEO6M	GPS module

CHAPTER 3: METHODOLOGY AND THE PROPOSED RESEARCH PLAN

3.1. Research approach and design of the system

This part describes the overview of the research approaches and the steps involved in system development from the step of gathering the ideas to the final step of prototype and getting result.

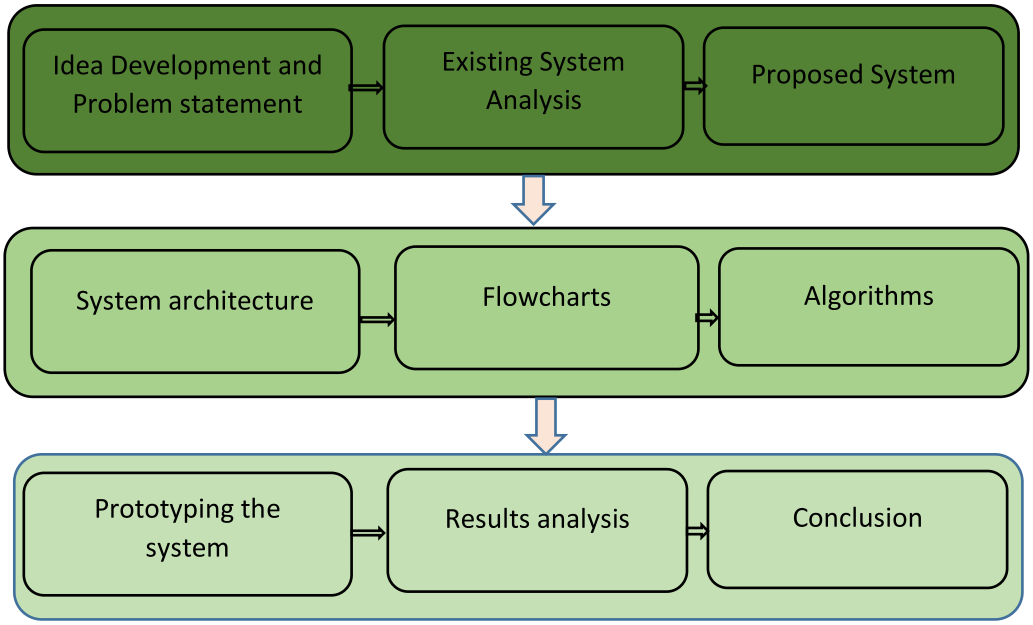


Figure 3. 1: Research Approach

The idea development and problem statement for this research departed from reading and analyzing related works to identify the problem they were solving, what the solved and the drawbacks of their works. This research comes as a mitigating tool to the problems that the existing research presented.

3.1.1. Proposed system design

This research avails a solution to the energy utility providers with the prototype, it will be possible and cheap to monitor and control the household electricity usage and detect the non-technical loss which was raising at high speed and avail the energy utility staffs to not do inspection which consumes fuels and costing them.

Data from the sensors are transmitted wirelessly using Wi-Fi than any other communication protocol is encompassed in the microcontroller (Node MCU) used and the ThingSpeak API is used as a cloud platform.

3.1.1. BLOCK DIAGRAM FOR THE PROPOSED SOLUTION

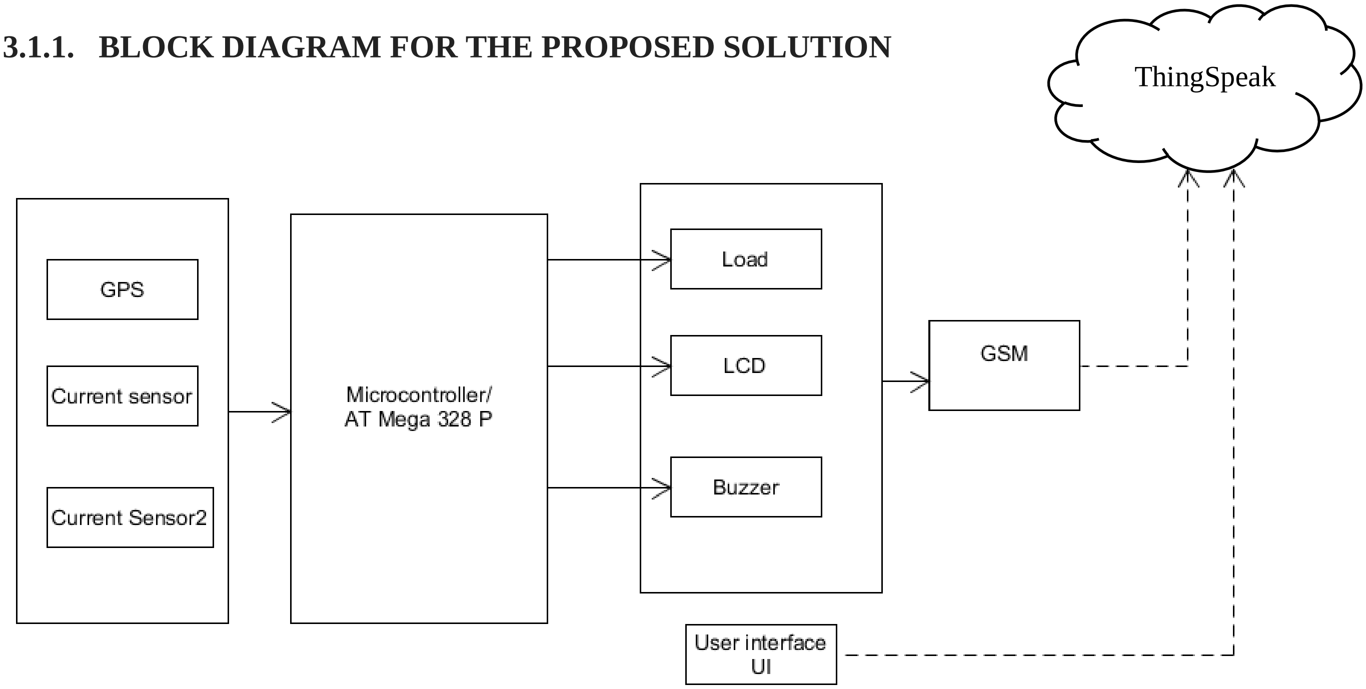


Figure 3. 2 : Proposed system block diagram

3.1.2. Flowchart

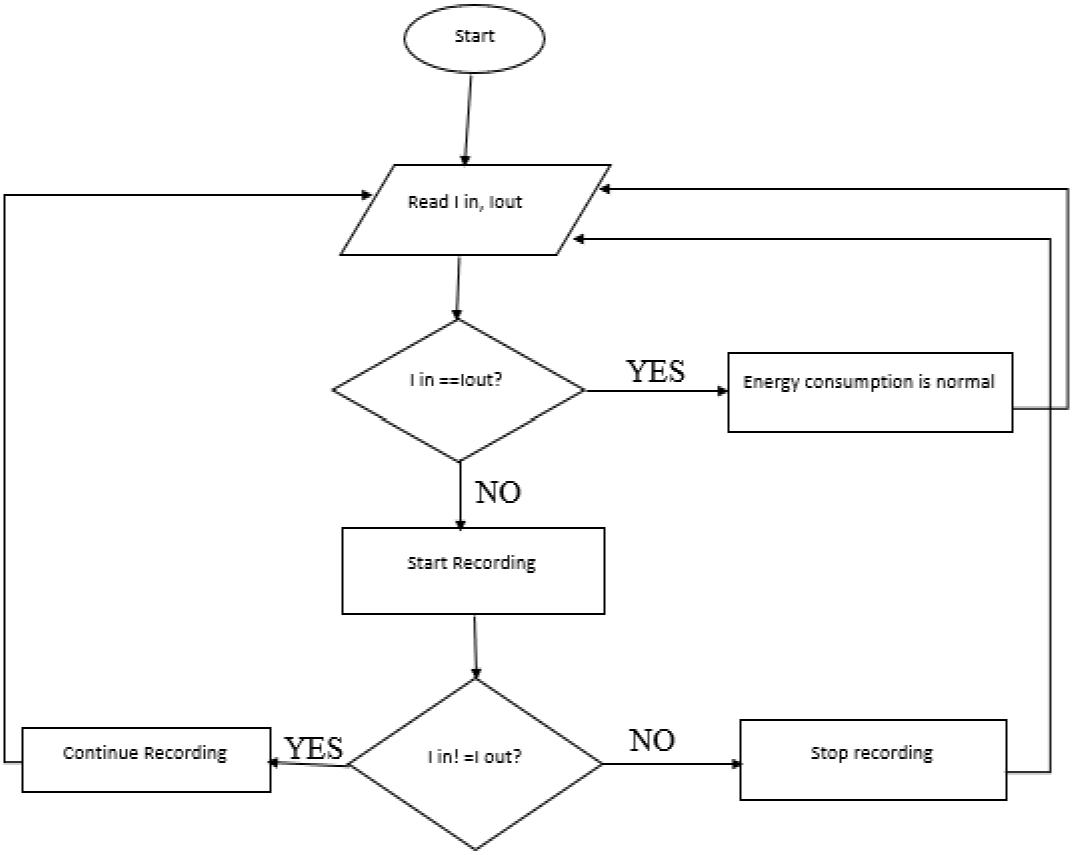


Figure 3. 3: Flowchart of the proposed solution Source: Own drawing

It shows how the current will be measured. Normally the current should be the same from the pole to the input of the meter. If the difference occurs this is the sign that the customer is stealing the electricity.

In the proposed methodology each specific objective is explained in detail and how it will be achieved as it is going to be done below:

3.1.4.1 RO 1. To assess and study the system requirements, we assess what is required to have a successful system that is computing the electricity stolen using different electronic devices that are made intelligent to detect the change in input and output current.

3.1.4.2. RO 2. To design smart power detection system, smart power detection system is designed using different electronic components and the calculated data are sent to the cloud using GSM with sim card inside. The exact value of the electricity stolen is recognized and this leads to accountability instead of estimating the amount of electricity used by the fraudsters.

3.1.4.3. RO 3. To test and validate the system functionalities, this objective aims at testing and validating the system functionalities through different tests done.

3.1.4.1. RO 4. To monitor electricity usage of each household, GSM will be used to send the notification(message) to the energy utility manager to see what is happening to the customer's power delivery and take further measures accordingly**.**

If fraud is detected, the system will send the address(coordinates) of the fraudster using GPS to the energy utility manager. Thus, there is a need to map every cash power at each household level.

3.2.Tools and Components

The objectives above will be achieved by using the components listed here:

3.2.1. Microcontroller (AT Mega 328P)

A microcontroller is a computer on a single integrated circuit that has the RAM, some form of Read Only Memory (ROM), and Input/Output ports. It has a great impact in our daily life which cannot be ignored. Microcontrollers are dedicated to performing a single and specific job and single applications. Microcontrollers are also used in devices that are used in specific purpose jobs like microwaves, single driven devices[14][15][16].

Figure 3. 4: Microcontrollers[14][15][16].

3.2.2. Printed Circuit Board (PCB)

Printed circuit board is the most common method of putting up together modern electronic circuits. Made concession of the sandwich of one or many covering layers and one or more copper layer which contain the signal traces and the powers and grounds, the design of the layout of printed circuit boards may be as demanding as the design of the electrical circuit. Components are mounted on the top layer in holes which extend through all layers and are referred to as through holes components but most recently, with the near universal adoption of surface mount components, they are commonly found components mounted on both top and bottom layers[17][18].

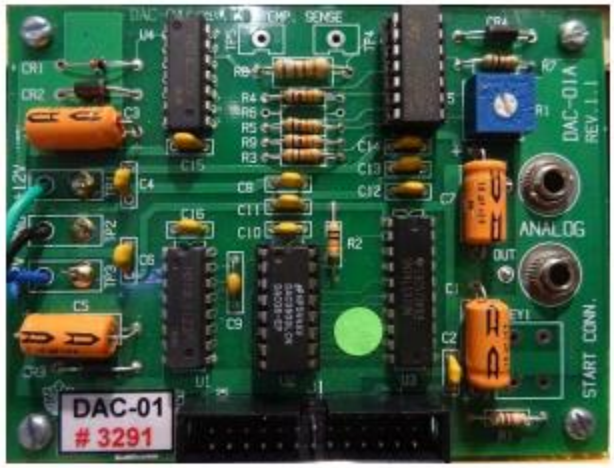


Figure 3. 5: Example of Printed Circuit Board (PCB) with different components mounted[19].

3.2.3. Buzzer

Piezo buzzers are electronic devices that produce a sound when triggered. It has two pins one anode and another is cathode.it has the ability to provide alarm when the set condition is met [20].

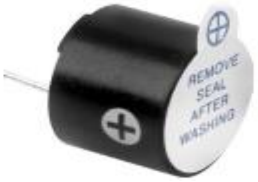


Figure 3. 6: Buzzer[21].

3.2.4. Current sensor (current transformer sensor, potential transformer sensor)

A current sensor is a device that detects and converts current to an easily measurable output voltage, which is proportional to the current through the measured path. There are a wide variety of sensors, and each sensor is suitable for a specific current range and environmental condition. Some of the features are: The split core, with 0.333V for output, built-in with sampling resistance and a leading wire of 1 m [22].

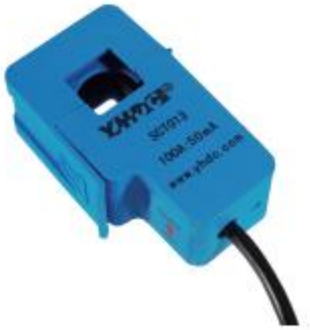


Figure 3. 7: Current sensor SCT013[22].

3.2.5. LCD 16x4 screen

LCD (Liquid Crystal Display) is a type of flat panel that is used to display the output data. This device has the capability of changing colors according to the user of the device[23].

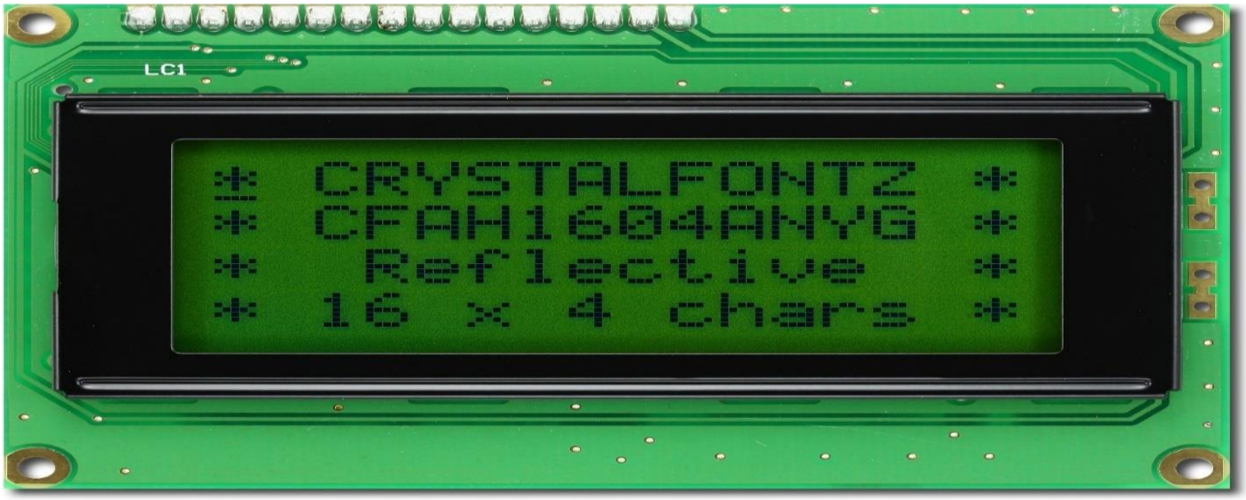


Figure 3. 8: 16x4 LCD

3.2.6. GSM Module

GSM (Global System for Mobile communication) is a is an electronic device used to transmit data either voice or SMS, the one used is SIM 800L[24][25].

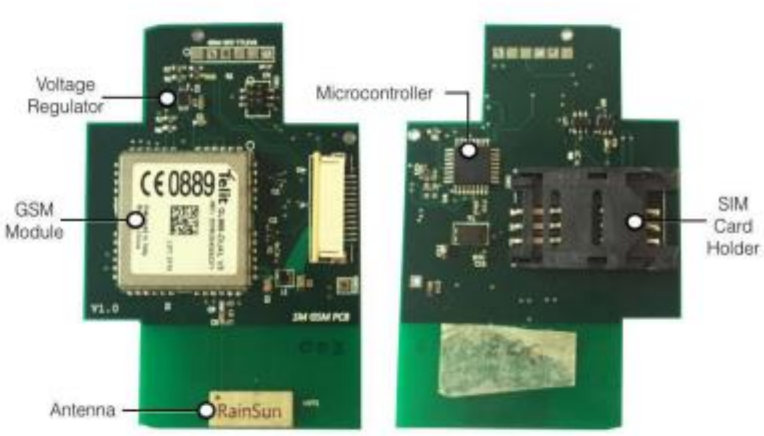


Figure 3. 9: GSM Module[24]

3.2.7. Resistor

A resistor is an electronic/electrical component used to limit the flow of a current. Resistor may be passive or active component[26].

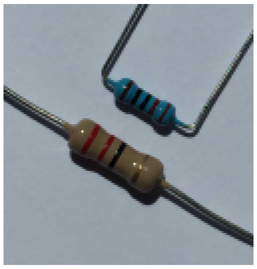


Figure 3. 10: Resistor[26] **Two axial lead resistor[26]**

3.2.8. Thingspeak

Thingspeak is used to store data on the cloud so that it is viewed wherever you are in real time to view what is happening at each household.

3.2.9. GPS module

GPS receiver uses a constellation of satellites and ground stations to calculate accurate location wherever it is located. These GPS satellites transmit information signal over radio frequency (1.1 to 1.5 GHz) to the receiver [23].

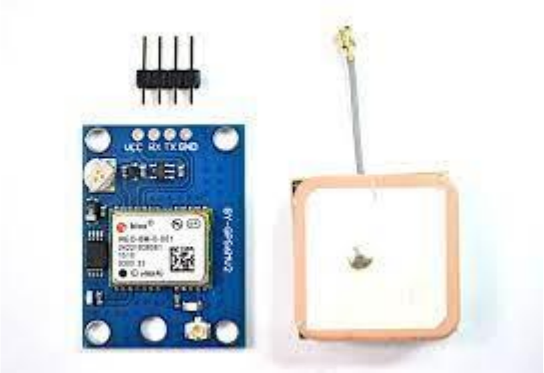


Figure 3. 11: GPS module [23].

3.2.10. Crystal Oscillator

A crystal oscillator is an electronic oscillator circuit that is used for the mechanical resonance of the vibration crystal of piezoelectric material. It creates an electrical signal with a given frequency, the frequency commonly used to keep track of time in digital integrated circuit to provide a stable clock signal and used to stabilize the frequency for radio transmitters and receivers[27].

Figure 3. 12: crystal oscillator[27]

3.2.11. Arduino Uno

Arduino Uno is a device that is used to upload data on a microcontroller because it is the one that accommodates the Arduino code[21][28].

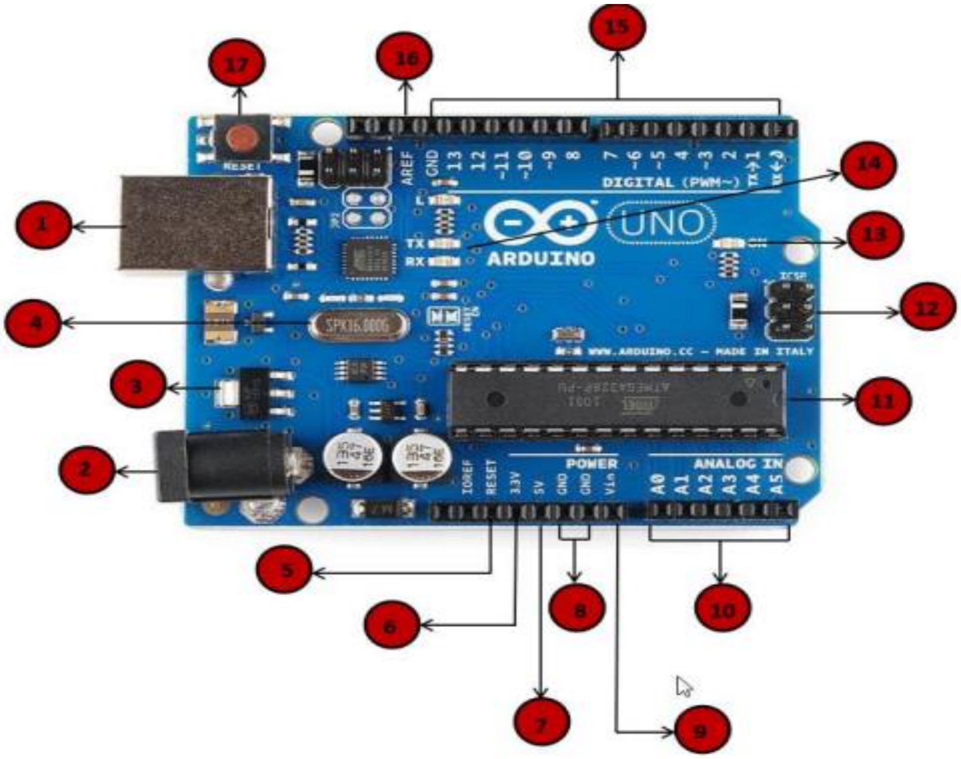


Figure 3. 13: Arduino Uno[28].

3.2.12. Push Button

A push button switch is a mechanical device used to control an electrical circuit in which the operator manually presses a button to actuate an internal switching mechanism and designed so that its contacts are opened and closed by depressing and releasing a pushbutton on the Switch in the direction of its axis[29].

Figure 3. 14: Push Button Switch[29].

3.3. Research tools and technique

Research methods are the methods used to conduct research into a desired subject to further understand it.[30].

3.3.1. Interview

The interview represents a social interaction between two persons, the psychological process requiring both individuals mutually respond though the social research purpose of the interview call for a varied response from the two parties concerned where this method highlights different advantages that are in this research technique[31].

3.3.2. Documentation

This technique will be used to review and read the reports related to the electricity theft compiled by REG to have experience on this topic.

3.3.3. Schedule

Schedule is the name usually applied to a set of questions, which are asked and filled by an interviewer in a face-to-face situation with another. It is best suited to the study of a single item thoroughly[31].

3.4. Scientific research approach

In this research, we used qualitative research including observation of the existing meters and document consultancy by reviewing journal papers. The goal is to investigate the existing meter and interrogate its benefits and backwards to find the way of improving it by applying technology.

Kirchhoff's law

By using the second law of Kirchhoff of current says that the amount of electricity in is equal(equivalent) to the number of electricity to get out[32].

Here, $\mathbf{I_1=I_2+I_{3+}I4}$ and this implies that $\mathbf{I_1-I_2-I_3-I_4=0}$

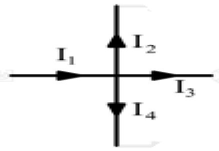


Figure 3. 15: Second law of Kirchhoff electricity[32].

By applying this law, we detect that the amount of electricity flowing in the wire must not change regardless of different hazards that may present like noise caused by the type of cable.

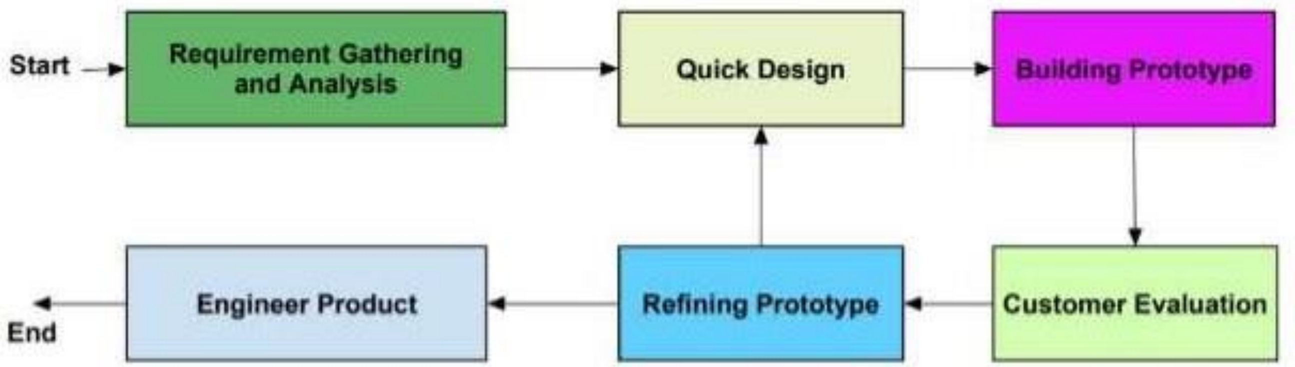
This second Kirchhoff's law states that the amount of electricity entering must be equal to the amount of electricity going out.

The energy consumed is calculated in kilowatt-hour (Kwh), the formulae Energy=**V*I*time.**

3.5. System development

In the context of research methodology, software development life cycle is a prototyping model with a system development method (SDM) in which a prototype is constructed, examined, and then reworked as the necessary until an acceptable prototype is finally achieved from which the full system or product can now be developed[33].

The following figure illustrates the steps involved in the system development method used



(Prototype model)

Figure 3. 16: System development model adapted from[33].

3.6.Cloud platform selection

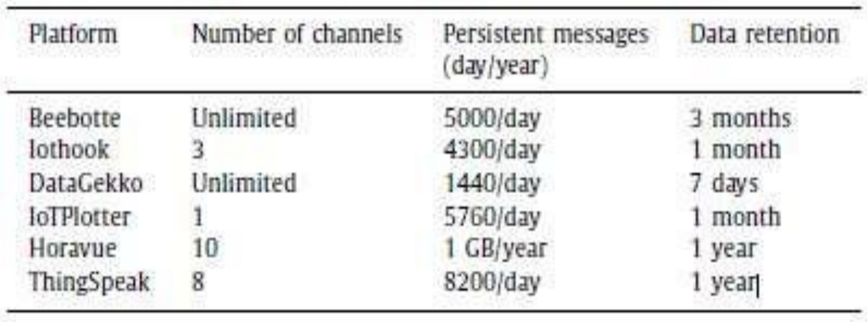
Cloud computing is a platform for storing and accessing data and programs over the internet instead of your physical computer. The cloud is also not about having dedicated to network attached storage hardware or server in residence, it's as a service such that with all the various data stored on the computers in a cloud, data mining and analysis are necessary to access that information in an intelligent manner[34]. Thingspeak is an open-source Internet of Things application and API to keep, to store and retrieve data from things using the HTTP and MQTT protocol over the internet. Thingspeak is an IoT analytics platform service that allows to aggregate, visualize, and analyze data streams in the cloud[34].

Within table 2 below, six platforms are compared by examining their number of channels, tenacity days of the messages per year, and data retention. These platforms need a personal usage license freely delivered but with some restrictions[34]. Beebotte is a cloud platform that conveys key building blocks to accelerate the development of the Internet of Things and real-time connected applications. Beebotte allows the transformation of any physical object or software application into a channel of digital resources. Beebotte is a cloud platform that offers infrastructure and connectivity with the help of REST, WebSockets, and MQTT [34].

Data Gekko is a fully managed enterprise-grade metrics as a service solution, Data Gekko can devour data over MQTT with millisecond precision of data points with full resolution, this is an IoT Telemetry platform ready for the next generation of internet-connected devices that speeds up with you from hobby plans to enterprise systems[34].

IoT Plotter and Horavue are also good cloud platforms, but ThingSpeak conquers them in terms of receiving many messages a day per year.

Table 3.1: Comparison between IoT platforms[33]**.**



Platform	Number of channels	Persistent messages (day/year)	Data retention
Beebotte	Unlimited	5000/day	3 months
Iothook	3	4300/day	1 month
DataGekko	Unlimited	1440/day	7 days
IoTPlotter	1	5760/day	1 month
Horavue	10	1 GB/year	1 year
ThingSpeak	8	8200/day	1 year

Figure 3. 17: Comparison between IoT platforms[33]

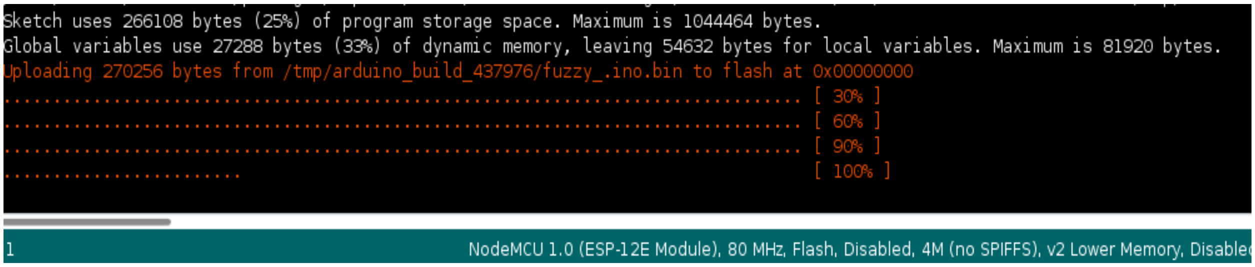
For our project, the ThingSpeak API is chosen because it has three channels where each channel can store 8 variables and we must store data about electricity stolen, location of fraudster and real- time with an additional feature of best store and visualize data.

3.7.Integrated Development Environment (IDE) Selection

The Arduino Integrated Development Environment (IDE) is a cross-platform application (for Windows, macOS, Linux) that is written in functions from C and C++.

Arduino is a prototype platform (open source) based on easy-to-use hardware and software. It consists of a circuit board, which can be programmed, and ready-made software called Arduino IDE (Integrated Development Environment) which is used to write and upload the computer code to the physical board[28].

It is used to write and upload codes to Arduino compatible controllers, but also, with the help of third-party cores, other vendor development boards. In this research, Arduino 1.8 version is used.



```
Sketch uses 266108 bytes (25%) of program storage space. Maximum is 1044464 bytes.
Global variables use 27288 bytes (33%) of dynamic memory, leaving 54632 bytes for local variables. Maximum is 81920 bytes.
Uploading 270256 bytes from /tmp/arduino_build_437976/fuzzy_.ino.bin to flash at 0x00000000
................................................................................ [ 30% ]
................................................................................ [ 60% ]
................................................................................ [ 90% ]
........................                                                         [ 100% ]

1                                        NodeMCU 1.0 (ESP-12E Module), 80 MHz, Flash, Disabled, 4M (no SPIFFS), v2 Lower Memory, Disablec
```

Figure 3. 18: On-device performance specifications   Source: Arduino application

CHAPTER 4. RESULT ANALYSIS AND INTERPRETATION

4.1.Introduction

This chapter focuses on the obtained results with the different interfaces. Its main parts are the results of the whole system and the description of the electric meter bypassed in different attempts.

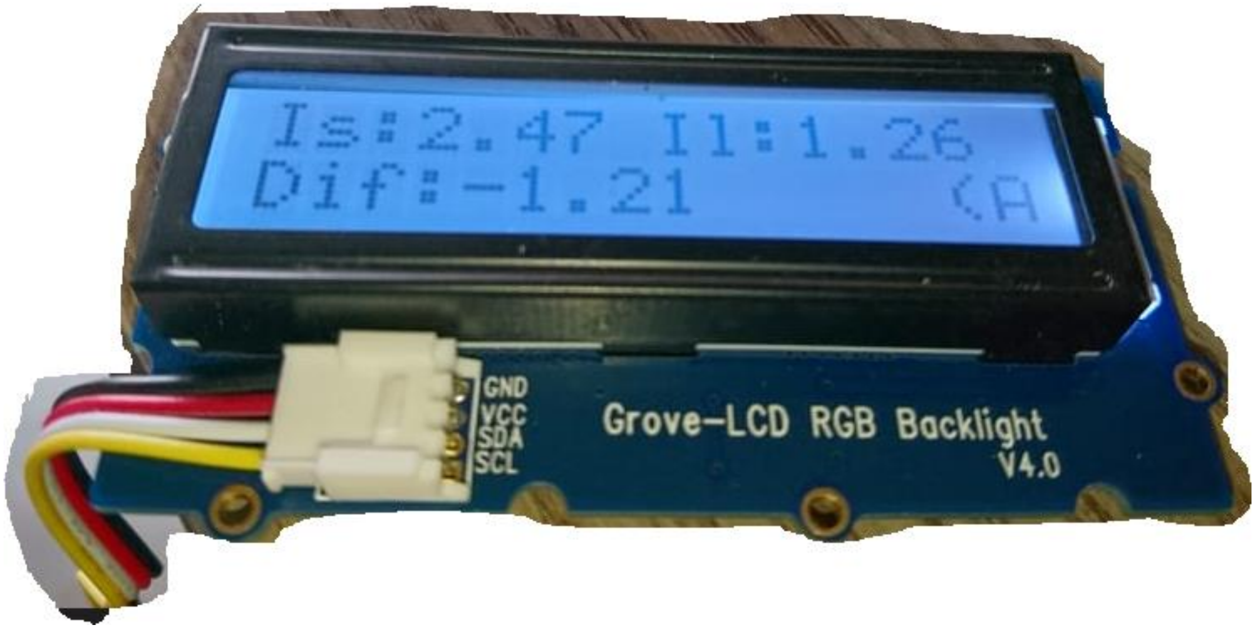


Figure 4. 1: LCD displaying difference in current

Here the device shows the difference between the input and the output current. Once this difference occurs the device automatically computes the electricity stolen, and the readings will be displayed on the cloud

In this chapter also, the core parameters are data of stolen electricity was captured and tested by current sensor and GPS nodes.

The data are locally processed by the microcontroller AT Mega 328P and are sent to the cloud via GSM to be analyzed, processed, and monitored on the dashboard in different ways.

4.2.Circuit diagram

The figure below illustrates the components gathered or combined to have the functioning system with the aim of providing our expected output.

These two sensors detect the current passing in it to compare whether the current received by the second sensor is equivalent to the one in sensor one, if there is a big difference the device activates automatically to start counting the amount of electricity stolen and sending readings to the cloud in real time.

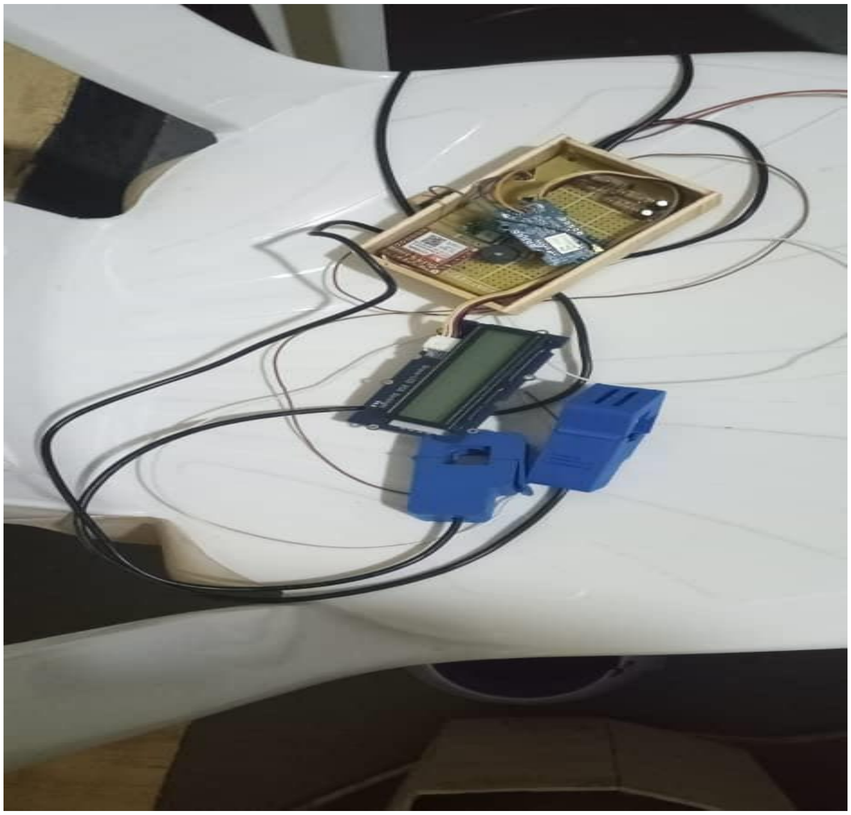


Figure 4. 2: Components **Source: This system**

4.3.Data on location (Address)

For location tracking, the GPS is used to indicate the place where fraud is taking place using coordinates of longitude and latitude.

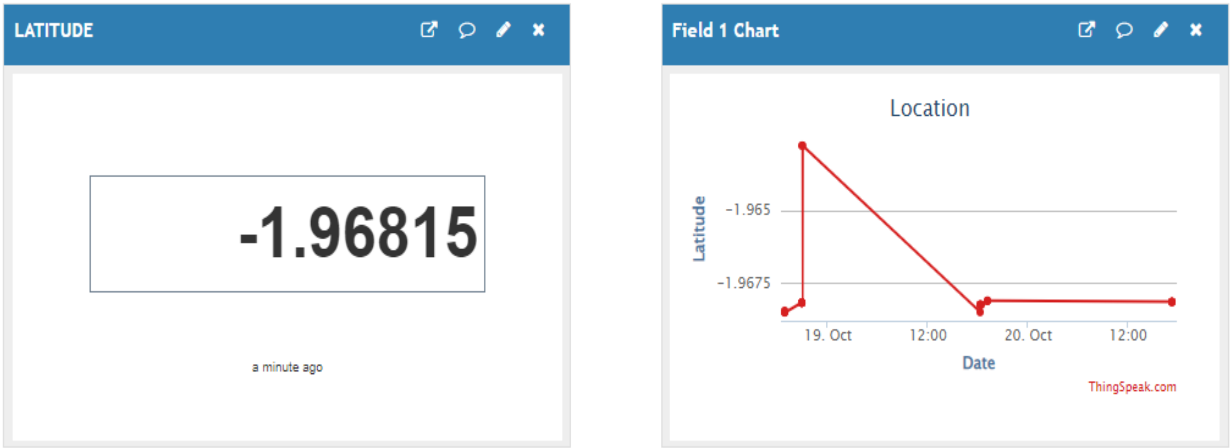


Figure 4. 3: Latitude of where the fraud was committed Source: Thingspeak API

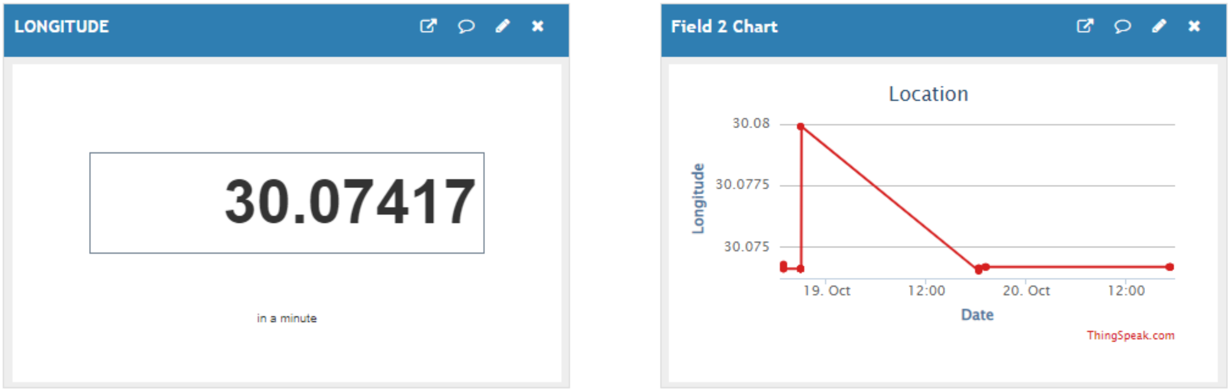


Figure 4. 4: Longitude source: Thingspeak API

This result from the above figure was generated to the ThingSpeak cloud platform when the electricity is being stolen by using hall-effect principal generate an electrical pulse with every revolution. That signal applied to the digital pin of microcontroller is processed and transmitted to the cloud every eight seconds as indicated in X-axis graph. This curve keeps increasing during the act of fraud during experiment testing.

4.4.Data on stolen electricity

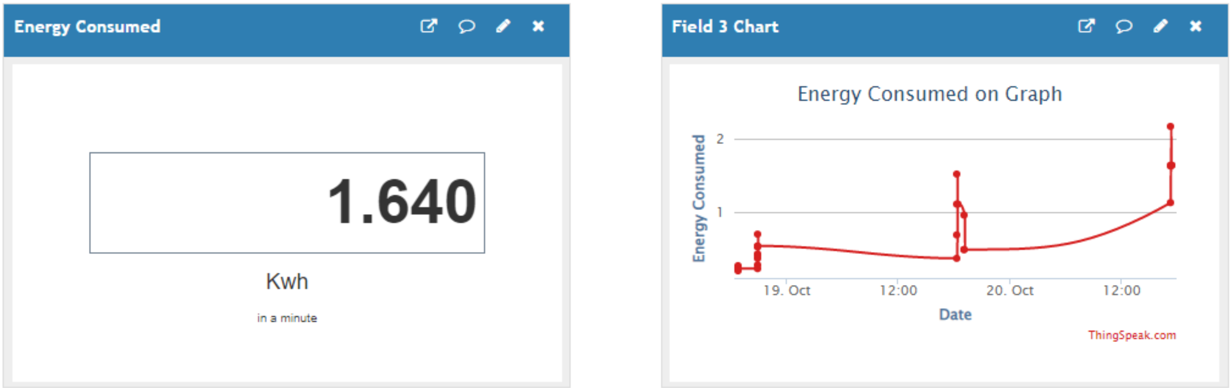


Figure 4. 5: Electricity stolen **source: Thingspeak API**

This figure shows the readings of the electricity stolen where this number is showing the last kilowatts-hour stolen in the last attempt, and the next figure illustrates the periods of theft and the amount of electricity stolen at each attempt.

As the graph is illustrating the starting hour of stealing the electricity and the end hour of stealing as well as the number of kilowatts-hours at each attempt.

4.5.Data of former location

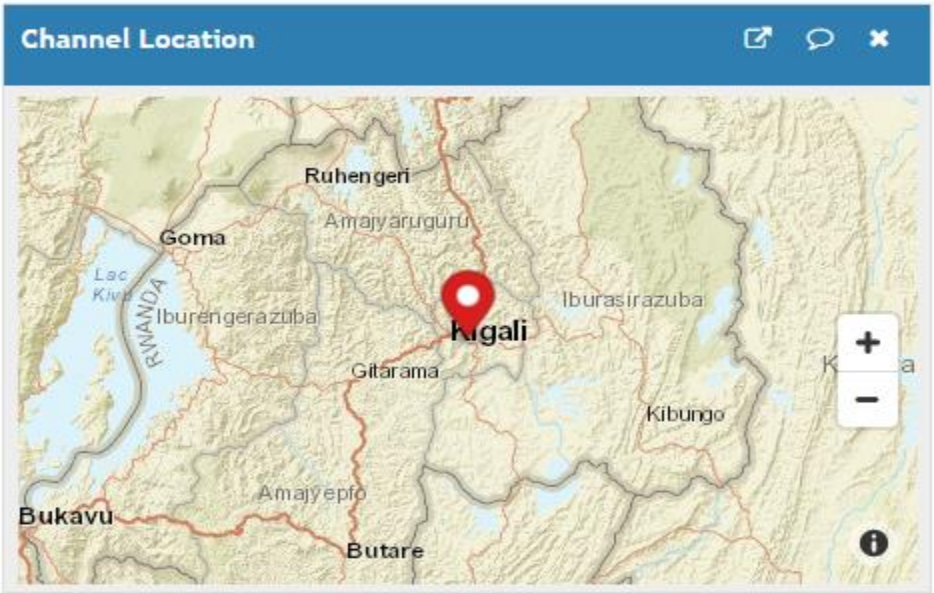
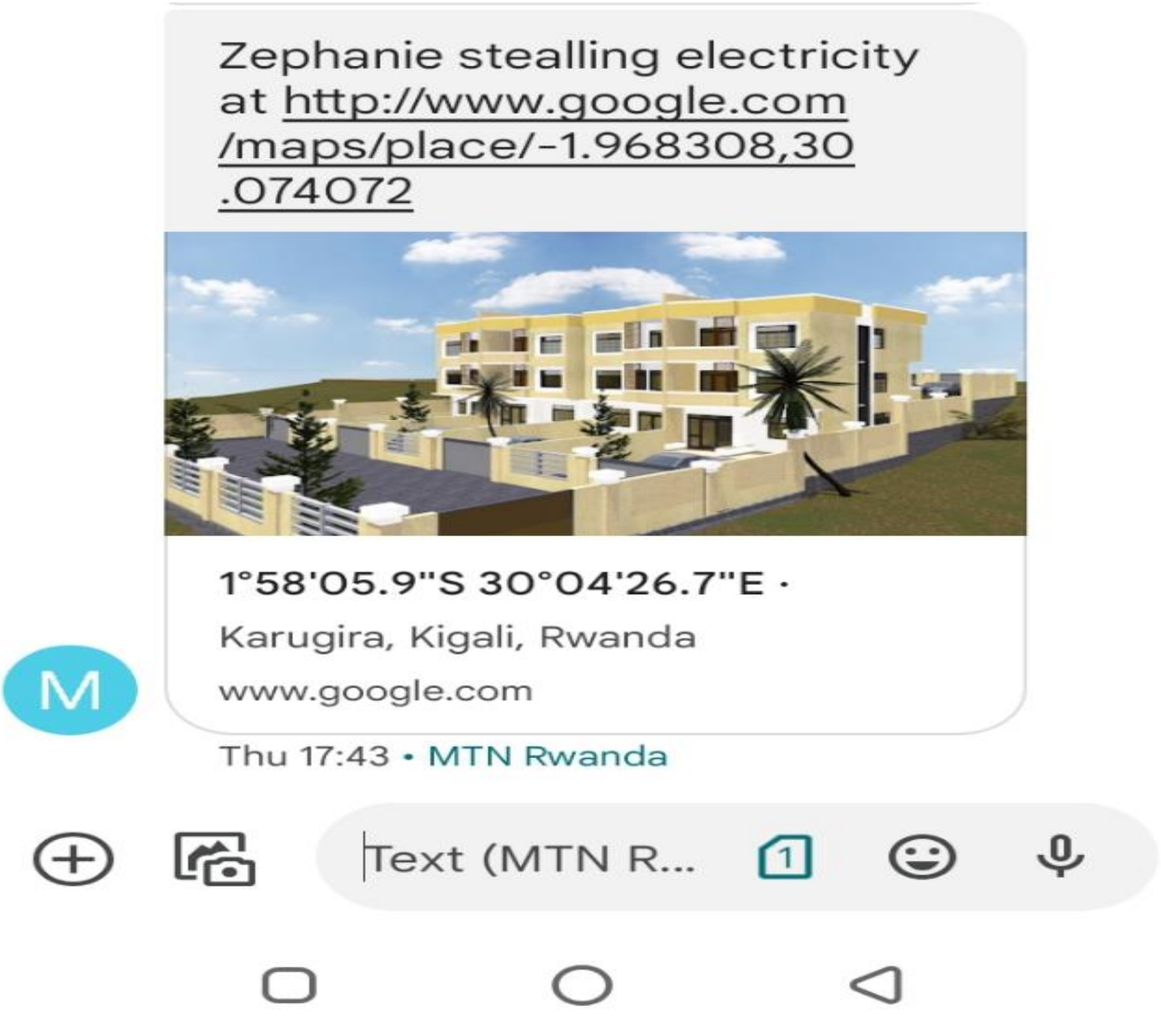


Figure 4. 6: Location of meter placement **source: Thingspeak**

This figure shows that the former location of meter was changed or not beacause this containg the location of where the meter has been installed, if the meter was misplaced the current location will be displayed in the SMS sent for the authorities to know where the fraud is being committed.

4.6.Data sent on the cell phone



Zephanie stealling electricity at http://www.google.com/maps/place/-1.968308,30.074072

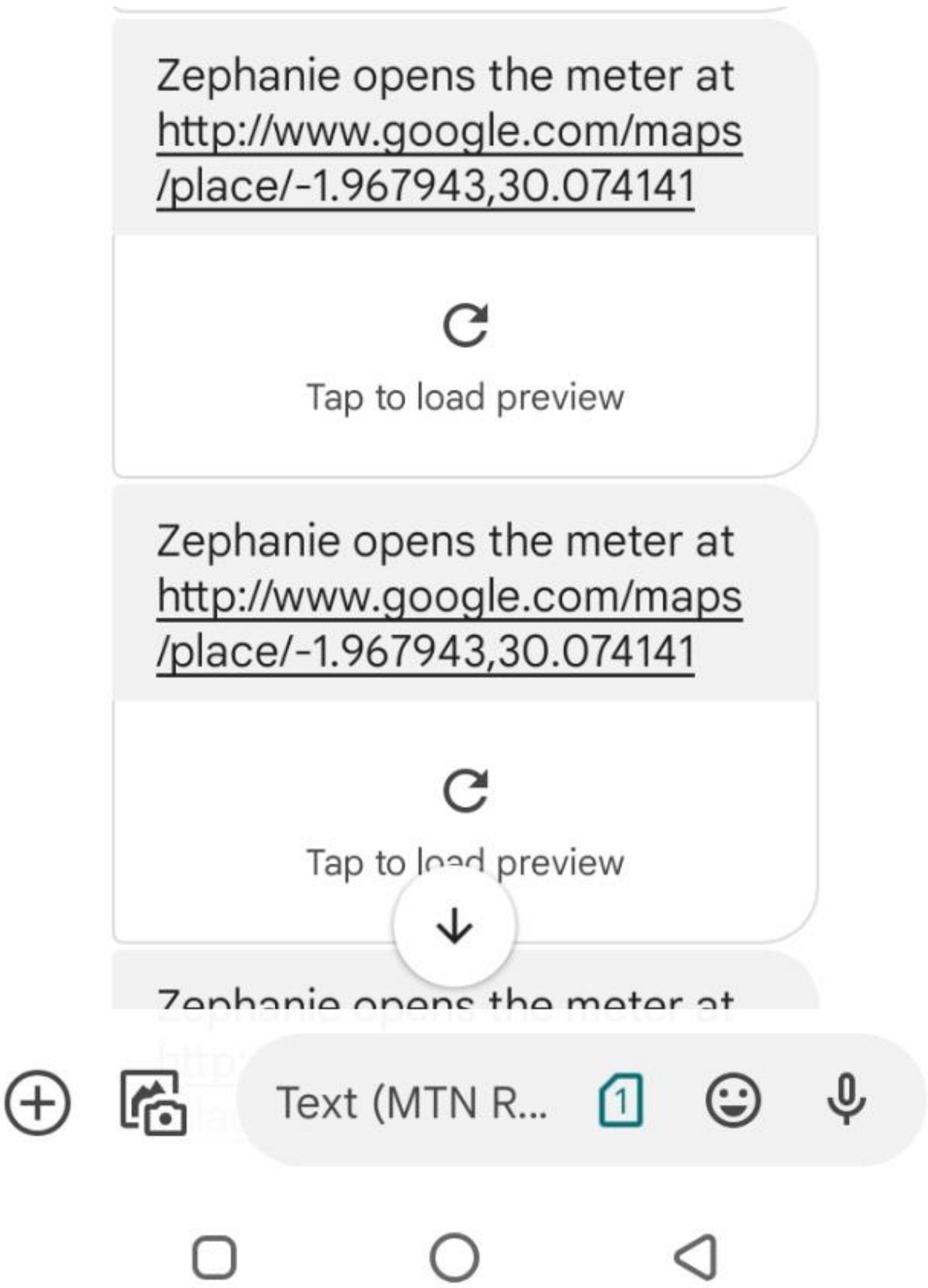
1°58'05.9"S 30°04'26.7"E ·
Karugira, Kigali, Rwanda
www.google.com

Thu 17:43 • MTN Rwanda

Figure 4. 7: SMS of Electricity fraud **Source: Message from GSM of System**

This is the message sent to the cell phone to warn the electricity manager that someone is stealing the electricity with the current location (address) where this fraudster is located.

4.7.Data on meter opening



Zephanie opens the meter at http://www.google.com/maps/place/-1.967943,30.074141

Zephanie opens the meter at http://www.google.com/maps/place/-1.967943,30.074141

Figure 4. 8: SMS of Meter opening **Source: SMS from system**

This is the message of when the meter box is opened, just to inform the electricity manager that someone opens the meter for further analysis and investigation.

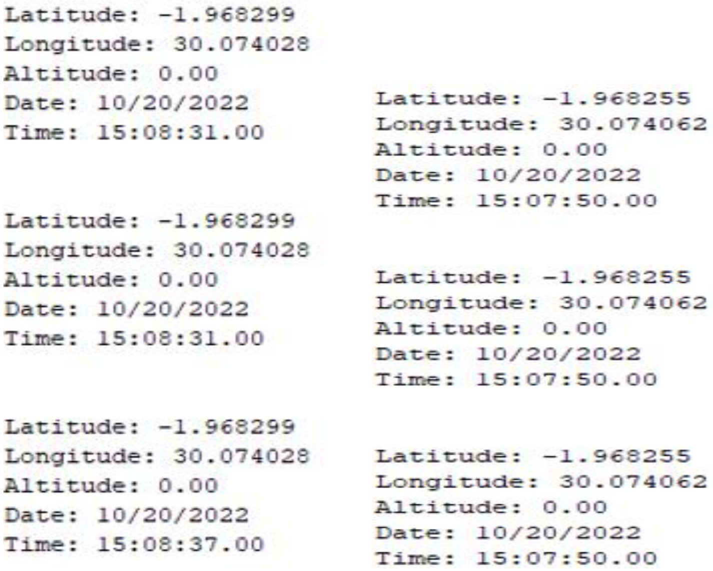
4.8. Prototype Efficiency

As a prototype, the **GIS BASED ELECTRICITY FRAUD DETECTION SYSTEM USING INTERNET OF THINGS** has been successfully implemented. All of the sensors and other equipment work as expected.

The sensors successfully detect and provide readings based on the surrounding conditions. Electricity fraud is effectively predicted based on readings. The system continuously detects and transmits data.

When the GSM is trying to send data to the cloud the readings in the system will stay stable until data are sent to the cloud, and this is done every eight seconds(8sec) to have data on real time for further processing and the message is sent to the energy utility manager at the time of sending data to the cloude platform

In addition, when the electric meter bos is opened the automatic message is sent showing the name of the fraudster ahd his/her address (location) using google map.



```
Latitude: -1.968299
Longitude: 30.074028
Altitude: 0.00
Date: 10/20/2022          Latitude: -1.968255
Time: 15:08:31.00         Longitude: 30.074062
                          Altitude: 0.00
                          Date: 10/20/2022
                          Time: 15:07:50.00
Latitude: -1.968299
Longitude: 30.074028
Altitude: 0.00            Latitude: -1.968255
Date: 10/20/2022          Longitude: 30.074062
Time: 15:08:31.00         Altitude: 0.00
                          Date: 10/20/2022
                          Time: 15:07:50.00

Latitude: -1.968299
Longitude: 30.074028      Latitude: -1.968255
Altitude: 0.00            Longitude: 30.074062
Date: 10/20/2022          Altitude: 0.00
Time: 15:08:37.00         Date: 10/20/2022
                          Time: 15:07:50.00
```

Figure 4. 9: **Location being updated   Source: Serial monitor**

Chapter 5: CONCLUSION AND RECOMMANDATION

5.1. conclusion

GIS BASED ELECTRICITY FRAUD DETECTION SYSTEM USING INTERNET OF THINGS collects data with sensors that contain current sensors and GPS used to collect data and send them to the cloud through Global system for mobile communication, Wi-Fi and Network protocal then stored in cloud. Those data are monitored in real time through mobile phone and ThingSpeak cloud platform application. This system solution respond to the research questions of detecting and monitoring described data and paramenters which were the main purpose of this study by controlling sensed data with Arduino C programming and process, analyse them by Arduino microcontroller AT Mega 328P microcontroller and ThingSpeak cloud to visualize and monitor data timely. Additionally researcher use GSM technology to send message notification to help electricity utility managers to control the electricity usage and plan audits on the fraudesters' location by saving money they should lose in the fraud.

The complete scope of this study was covered, and the results of many tests show that **GIS BASED ELECTRICITY FRAUD DETECTION SYSTEM USING IOT** can have a favorable impact on society and the electricity service provider, and the data generated by the system would contribute in further studies or in further researches.

This system increaseses the speed in national strategy transformtion one (NST1) strategies in energy sector where the budget allocated to this activity of inspection will be used in other activities that will accelerate the universal access to electricity.

Scale up electricity generation and improve quality, affordability, and reliability. Generation plans will be informed by medium and long-term projections and analysis of supply and demand. Long-term generation plans will include identification of least cost sources of energy generation with the objective of ensuring a cost-reflective and competitive tariff. A pro-active strategy will be developed to attract industries for economic growth and to ensure that they are supplied with available, reliable and 7 Years Government Programme: National Strategy for Transformation (NST1) 2017 – 2024 22 affordable electricity. Key sectors of focus to increase demand include mining, manufacturing, ICT, and commercial premises. The quality of electricity will be improved by continuing investments in network upgrading and strengthening as well as investing in loss reduction projects. Priority will be given to productive use connections such as industrial zones, market centers and other socio-economic facilities such as schools and health centers. This will be achieved through Universal access to basic infrastructure such as electricity[35]. Access to electricity will be scaled up to all from 34.4% (EICV5) to 100% by 2024 in collaboration with the private sector to reach off-grid areas and investments in grid expansion

5.2. RECOMMENDATION

The following recommandations are drawn after conducting this research thesis entitled "**GIS BASED ELECTRICITY FRAUD DETECTION SYSTEM USING IOT**":

- The local authorities and the community itself are requested to give information and teach the citizens to be accountable on electricity usage.
- The use of ICT skills on electricity utility managers in order to manipulate the system and monitor the electricity parameters on time from cloud platform.
- The traing of electricity ulitility managers is required to be familiar with this new system and technology to have the insights on the usage of technologies in accountabilities checking.
- Ministry of infrastructure though its agency REG is srequested to use this system as tool to prevent(avoid) electricity fraud by bypassing the meter.Future researchers are recommanded to enhanced the capability of designed solution by using biometric technologies such as fingerprints, iris, face recognition and voice regnition in meter oppening to avoid unwanted openings of unauthorised user. Satallite and GPS techonologies .

References

[1] B. C. Costa, B. L. A. Alberto, A. M. Portela, M. W, and E. O.Eler, “Fraud Detection in Electric Power Distribution Networks using an Ann-Based Knowledge-Discovery Process,” *Int. J. Artif. Intell. Appl.*, vol. 4, no. 6, pp. 17–23, 2013, doi: 10.5121/ijaia.2013.4602.

[2] A. A. Muktar, “WIRELESS POWER CONSUMPTION MONITORING SYSTEM BY UNIVERSITY OF LAGOS SUPERVISING LECTURER : SUBMITTED IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE AWARD OF A BSC (HONS) IN ELECTRICAL AND ELECTRONICS ENGINEERING UNIVERSITY OF LAGOS .,” 2015.

[3] A. O. Otuoze *et al.*, “Electricity theft detection framework based on universal prediction algorithm,” *Indones. J. Electr. Eng. Comput. Sci.*, vol. 15, no. 2, pp. 758–768, 2019, doi: 10.11591/ijeecs.v15.i2.pp758-768.

[4] E. Parliament *et al.*, “Press release Press release,” no. 20120523, pp. 32–33, 2011.

[5] N. S. Agency, “Annual Report Annual Report,” *Mares*, no. December, pp. 2–2, 2019, [Online]. Available: https://www.pvh.com/-/media/Files/pvh/investor-relations/PVH-Annual-Report-2020.pdf

[6] B. Coma-puig, J. Carmona, and R. Gavald, “Fraud Detection in Energy Consumption : A Supervised Approach”.

[7] N. K. Mucheli *et al.*, “Smart Power Theft Detection System,” in *Proceedings of 3rd International Conference on 2019 Devices for Integrated Circuit, DevIC 2019*, 2019, no. March, pp. 302–305. doi: 10.1109/DEVIC.2019.8783395.

[8] P. A. Sai, P. B. Teja, and C. Engineering, “Iot based power theft detection 1,” vol. 5, no. 3, pp. 249–253, 2020.

[9] S. Li, Y. Han, X. Yao, S. Yingchen, J. Wang, and Q. Zhao, “Electricity Theft Detection in Power Grids with Deep Learning and Random Forests,” vol. 2019, 2019.

[10] M. Education and E. Engineering, “Power Theft Detection and Alert System using IOT,”

vol. 12, no. 10, pp. 1135–1139, 2021.

[11] H. M. Dabir, A. S. Kadam, G. Hadge, and A. S. Rathore, "Efficient Electricity Theft Detection Using Machine Learning Algorithms," vol. 4, no. 12, pp. 1276–1282, 2019.

[12] R. Meenal, K. M. Kuruvilla, A. Denny, R. V. Jose, and R. Roy, "Power monitoring and theft detection system using IoT," *J. Phys. Conf. Ser.*, vol. 1362, no. 1, 2019, doi: 10.1088/1742-6596/1362/1/012027.

[13] S. Arivazhagan, "GSM and Arduino based power theft detection and protection," vol. 5, no. 4, pp. 581–588, 2019.

[14] A. Nayyar and V. Puri, "Raspberry Pi-A Small , Powerful , Cost Effective and Efficient Form Factor Computer : A Review," *Int. J. Adv. Res. Comput. Sci. Softw. Eng.*, vol. 5, no. 12, pp. 720–737, 2015.

[15] M. Alcaraz and A. Calbet, "M Sc Pl O E –," no. January 2003, 2014.

[16] A. Hussain, M. Hammad, K. Hafeez, and T. Zainab, "Programming a Microcontroller," *Int. J. Comput. Appl.*, vol. 155, no. 5, pp. 21–26, 2016, doi: 10.5120/ijca2016912310.

[17] Q. M. Hussein, "Counters Object :," no. August, 2020.

[18] H. Zumbahlen, "Printed Circuit-Board Design Issues," *Linear Circuit Des. Handb.*, pp. 821–895, 2008, doi: 10.1016/b978-0-7506-8703-4.00012-2.

[19] R. R., S. A., G. D., M. B., and A. S.Vaidya, "Quality Control of PCB using Image Processing," *Int. J. Comput. Appl.*, vol. 141, no. 5, pp. 28–32, 2016, doi: 10.5120/ijca2016909623.

[20] C. Devices, "Buzzer Basics - Technologies , Tones ," 2019, [Online]. Available: www.cuidevices.com%0ABuzzer

[21] P. N. Table, "Part Number Table," *Group*, pp. 1–2, 2012.

[22] "0.333V Split core current transformer," p. 333, 2015.

[23] J. A. Castellano, "c," no. October 2005, 2015, [Online]. Available: https://www.researchgate.net/profile/Joseph_Castellano/publication/282650374_The_Hist

ory_of_LCD_Development/links/5615874b08aec6224411bcf5/The-History-of-LCD-Development.pdf

[24] N. A. Abd Rahman *et al.*, “GSM module for wireless radiation monitoring system via SMS,” *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 298, no. 1, 2018, doi: 10.1088/1757-899X/298/1/012040.

[25] T. Gsm and G. Module, “GSM / GPRS Module,” *Group*, no. September, p. 32523301, 1800.

[26] T. Gamsjäger, “Electronic Engineering 2: Resistors, Elementary Resistor Circuits and the Resistor Paradox,” *Electron. Eng.*, no. August, 2017.

[27] T. Ormond, “Crystal Oscillators.,” *Edn*, vol. 30, no. 23, pp. 98–108, 110, 1985, doi: 10.1016/b978-0-7506-0937-1.50110-5.

[28] E. Sugawara and H. Nikaido, “Tutorialspoint,” *Forex Trade*, vol. 58, no. 12, pp. 7250–7257, 2020, [Online]. Available: www.tutorialspoint.com

[29] W. Is and P. Switch, “Technical Explanation for Pushbutton Switches,” pp. 1–4.

[30] S. Gounder, “Chapter 3 - Research methodology and research questions,” *Res. Methodol. Res. Method*, no. March 2012, pp. 84–193, 2012.

[31] O. Uusitalo, *Research methodology*, no. 9783319068282. 2014. doi: 10.1007/978-3-319-06829-9_3.

[32] “Practicum report basic physics ii ‘kirchoff law’ collection date: 16,” no. March, 2018.

[33] D. Mukanyiligira, N. Jean, and D. La Croix, “College of Science and Technology African Center of Excellence in Internet of Things Master of Science in Internet of Things - Embedded Computing Systems "A FUZZY INFERENCE MODEL FO...,” no. May, 2022.

[34] H. Ouldzira *et al.*, “A Survey on RF Energy Harvesting-RFEH- in WSNs To cite this version : HAL Id : hal-02296957 A Survey on RF Energy Harvesting-RFEH- in WSNs,” 2019.

[35] R. Government, “(ref NST1).(ref NST1).,” pp. 2017–2024, 2017.

Appendices:

Appendix A: Resources and Cost

List of components to be used in this research project are detailed below:

LIST OF COMPONENTS TO USE AND THEIR COST

S/N	Item	Item specification	Unit price	Quantity	Total Price
1	Microcontroller	AT Mega 328P	26$	1	26$
2	Current sensor	STC 103	50$	2	100 $
3	PCB	12*18 PCB	3$	1	3 $
4	Push Button	PUSHBUTTONROUND SWITCH	2$	2	4$
5	Buzzer	Voltage:3.5-5.5V	2$	2	4 $
6	LCD+I2C	RGB LCD 16x2	60$	1	60 $
7	Back boost converter	5v	30$	1	30$
8	Jumpers	Male to Male Male to female	0.1$	40	6 $
9	PCB board	Universal board	10$	1	10 $
10	Infrared (IR) sensor	Infrared sensor (transmissive and receiver)	5$	2	10 $
11	Arduino Uno	Arduino Uno	15$	1	15 $
12	Crystal oscillator	2W10 2A, BRIDGE RECTIFIER	5$	1	5 $
13	GSM	SIM800L	15$	1	15 $

14	Node MCU	LOLIN D1 MINI V3.1.0	25$	1	25$
15	Resistors, capacitors, transistors, and diodes	1kΩ,100 kΩ			7$
16	Sim card	MTN Sim Card	1$	1	1$
17	Socket	Electric Socket	2$	2	4$
18	GPS module	NEO-M8N GPS / GNSS MODULE WITH EEPROM	14$	1	14$
19	Electric wire	4 M of electric meter	1.5$	4	6$
	Total				350$

Table A. 1: list of components with its cost

Appendix B: Timetable for Completion or Research Work-Plan

RESEARCH IMPLEMENTATION WORK PLAN

S/N	Activity	April 2022			May 2022				June 2022					July 2022				August 2022					September 2022				October 2022					November 2022			
		W2	W3	W4	W1	W2	W3	W4	W1	W2	W3	W4	W5	W1	W2	W3	W4	W1	W2	W3	W4	W5	W1	W2	W3	W4	W1	W2	W3	W4	W5	W1	W2	W3	W4
1.	Research proposal and abstract submissions	🟩	🟩	🟩	🟩	🟩	🟩	🟩																											
2.	Working on literature review								🟩	🟩	🟩	🟩	🟩																						
3.	Research Methodology										🟩	🟩	🟩	🟩	🟩																				
4.	Data analysis and result interpretation and device construction															🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩												
5.	Working on conclusion, recommendation and device construction																							🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩				
6.	Thesis finalization & presentation																															🟩	🟩	🟩	

***Table A. 2:* Research implementation work plan**

Appendix C: Code:

```
#include <TinyGPS++.h>
#include <SoftwareSerial.h>

double longitude;
double latitude;
char buff[10];
int open1 = 6;
int buzzer = 5;
int lm = 10;
int RXPin = 11;
int TXPin = 10;
String mylong = "";
String mylati = "";

#include "EmonLib.h"
#include <Wire.h>
#include "rgb_lcd.h"
rgb_lcd lcd;
const int colorR = 240;
const int colorG = 240;
const int colorB = 240;

int GPSBaud = 9600;

TinyGPSPlus gps;

SoftwareSerial gpsSerial(RXPin, TXPin);
```

```
#define VOLT_CAL 224
#define CURRENT_CAL 308.18
EnergyMonitor emon1;
#define VOLT_CAL1 224
#define CURRENT_CAL1 308.18
EnergyMonitor emon11;
#include <SoftwareSerial.h>
SoftwareSerial SIM800(7, 8);

int trg = 0;
int ptemp = 0;
float Results = 0;
float last = 0.00;
float last1 = 0.00;


void setup()
{
  Serial.begin(9600);
  lcd.begin(16, 2);
  pinMode(open1, INPUT_PULLUP);
  pinMode(buzzer, OUTPUT);
  lcd.setRGB(colorR, colorG, colorB);
  emon1.voltage(3, VOLT_CAL, 1.7);  // Voltage: input pin, calibration, phase_shift
  emon1.current(0, CURRENT_CAL);       // Current: input pin, calibration.

  emon11.voltage(2, VOLT_CAL1, 1.7);  // Voltage: input pin, calibration, phase_shift
  emon11.current(1, CURRENT_CAL1);       // Current: input pin, calibration.
  lcd.print("  ENERGY METER  ");
  delay(1000);
  SIM800.begin(9600);
  //Serial.println("SIM800 ready...");
  SIM800.print("AT+CMGF=1\r");
  delay(100);
  SIM800.print("AT+CNMI=2,2,0,0,0\r");
  delay(100);
  gpsSerial.begin(GPSBaud);
}

void loop()
{
  int btn = digitalRead(6);
  Serial.print("Button: ");
  Serial.println(btn);

  if (btn == 1) {
    digitalWrite(buzzer, HIGH);
    sendSMS1();
  }
  else {
    digitalWrite(buzzer, LOW);
  }
  while (gpsSerial.available() > 0)
    if (gps.encode(gpsSerial.read()))
      displayInfo();

  // If 5000 milliseconds pass and there are no characters coming in
  // over the software serial port, show a "No GPS detected" error
  if (millis() > 5000 && gps.charsProcessed() < 10)
  {
    //Serial.println("No GPS detected");
    while (true);
  }
```

```
}
void sendSMS() {
  SIM800.println("AT+CMGF=1"); // Configuring TEXT mode
  updateSerial();
  SIM800.println("AT+CMGS=\"+250783052653\"");
  updateSerial();
  SIM800.print("Zephanie stealling electricity at http://www.google.com/maps/place/" + mylati +
"," + mylong); //text content
  updateSerial();
  SIM800.write(26);
}
void sendSMS1() {
  SIM800.println("AT+CMGF=1"); // Configuring TEXT mode
  updateSerial();
  SIM800.println("AT+CMGS=\"+250783052653\"");
  updateSerial();
  SIM800.print("Zephanie opens the meter at http://www.google.com/maps/place/" + mylati + ","
+ mylong); //text content
  updateSerial();
  SIM800.write(26);
}
void updateSerial() {
  delay(500);
  while (Serial.available())
  {
    SIM800.write(Serial.read());//Forward what Serial received to Software Serial Port
  }
  while (SIM800.available())
  {
    Serial.write(SIM800.read());//Forward what Software Serial received to Serial Port
  }
```

```
}

void displayInfo()
{
  if (gps.location.isValid())
  {

    latitude = gps.location.lat(), 6 ;

    longitude = gps.location.lng(), 6 ;
    // for latitude
    mylati = dtostrf(latitude, 3, 6, buff);
    mylong = dtostrf(longitude, 3, 6, buff);

    //Serial.print("Latitude: ");
    //Serial.println(gps.location.lat(), 6);
    //Serial.print("Longitude: ");
    //Serial.println(gps.location.lng(), 6);
    //Serial.print("Altitude: ");
    //Serial.println(gps.altitude.meters());
    emon1.calcVI(20, 2000);
    emon11.calcVI(20, 2000);

    float currentDraw            = ((emon1.Irms) - 1.85) / 100;
    float supplyVoltage   = emon1.Vrms;


    float currentDraw1            = ((emon11.Irms) - 1.85) / 100;
    float supplyVoltage1   = emon11.Vrms;
    Results = (currentDraw - currentDraw1) ;

    if (Results >= 0) {
      last = last + Results;
    }
    last1 = last + Results;
    if (currentDraw < 0) {
      currentDraw = 0;
    }
    if (currentDraw1 < 0) {
      currentDraw1 = 0;
    }
    if (Results < 0) {
      Results = 0;
    }
    //  //Serial.print("Current: ");
    //  //Serial.print(currentDraw);
    //  //Serial.print("          Current1: ");
    //  //Serial.println(currentDraw1);
    lcd.clear( );
    lcd.setCursor(0, 0);
    lcd.print("IP: ");
    lcd.print(currentDraw1);
    lcd.setCursor(8, 0);
    lcd.print("IM: ");
    lcd.print(currentDraw);
    lcd.setCursor(0, 1);
    lcd.print("Consu: ");
    lcd.setCursor(4, 1);
    lcd.print(last1); lcd.setCursor(11, 1); lcd.print("(Kwh)");

    //Serial.print("Watts: ");
    //Serial.println(currentDraw * 220);
    //Serial.println("\n\n");
```

```
  if (last1 >= 0.2) {
    sendSMS();
    delay(1000);
    pushData();
    trg = 1;
  }
  else if (last1 < 0.2) {
    trg = 0;
  }
  if (trg = 1) {
    if (trg != 0) {

      trg = 0;
    }
  }
}
else
{
  //Serial.println("Location: Not Available");
}
//Serial.print("Date: ");
if (gps.date.isValid())
{
  //Serial.print(gps.date.month());
  //Serial.print(" / ");
  //Serial.print(gps.date.day());
  //Serial.print(" / ");
  //Serial.println(gps.date.year());
}
else
{
   //    //Serial.println("Not Available");
  }

  //Serial.print("Time: ");
  if (gps.time.isValid())
  {
    if (gps.time.hour() < 10); //Serial.print(F("0"));
    //Serial.print(gps.time.hour());
    //Serial.print(": ");
    if (gps.time.minute() < 10); //Serial.print(F("0"));
    //Serial.print(gps.time.minute());
    //Serial.print(": ");
    if (gps.time.second() < 10); //Serial.print(F("0"));
    //Serial.print(gps.time.second());
    //Serial.print(".");
    if (gps.time.centisecond() < 10); //Serial.print(F("0"));
    //Serial.println(gps.time.centisecond());
  }
  else
  {
    //Serial.println("Not Available");
  }
  //Serial.println();
  //Serial.println();
  delay(1000);
}
void pushData() {
  SIM800.println("AT");
  delay(1000);
  updateSerial();
  SIM800.println("AT+CPIN?");
  delay(1000);
  updateSerial();
  SIM800.println("AT+CREG?");
  delay(1000);
  updateSerial();
  SIM800.println("AT+CGATT?");
  delay(1000);
  updateSerial();
  SIM800.println("AT+CIPSHUT");
  delay(1000);
  updateSerial();
  SIM800.println("AT+CIPSTATUS");
  delay(2000);
  updateSerial();
  SIM800.println("AT+CIPMUX=0");
  delay(2000);
  updateSerial();
  SIM800.println("AT+CSTT=\"internet.mtn\"");//start task and setting the APN,
  delay(1000);
  updateSerial();
  SIM800.println("AT+CIICR");//bring up wireless connection
  delay(3000);
  updateSerial();
  SIM800.println("AT+CIFSR");//get local IP adress
  delay(2000);
  updateSerial();
  SIM800.println("AT+CIPSPRT=0");
  delay(100);
  updateSerial();
    SIM800.println("AT+CIPSTART=\"TCP\",\"api.thingspeak.com\",\"80\"");//start up the connection
  delay(2000);
  updateSerial();
  SIM800.println("AT+CIPSEND");//begin send data to remote server
  delay(4000);
  updateSerial();
  //  String str = "GET
https://api.thingspeak.com/update?api_key=ZXT0E29XCRTXKBOY&field1=" +
String(analogRead(A1)) + "&field2=" + String(analogRead(A2));
  String str = "GET
https://api.thingspeak.com/update?api_key=ZXT0E29XCRTXKBOY&field1=" + String(mylati)
+ "&field2=" + String(mylong) + "&field3=" + String(last1);

  //Serial.println(str);
  SIM800.println(str);//begin send data to remote server
  delay(3000);
  updateSerial();
  SIM800.println((char)26);//sending
  delay(3000);//waitting for reply, important! the time is base on the condition of internet
  SIM800.println();
  updateSerial();

  SIM800.println("AT+CIPSHUT");//close the connection
  delay(100);
  updateSerial();
}
```