IOT Based Electricity Theft Detection System

B.Sc. (Engineering) Project

A project paper submitted to the Department of Information and Communication Engineering, Pabna University of Science and Technology in partial fulfillments of the requirements for the degree of Bachelor of Science in Engineering in Information and Communication Engineering.

Submitted By

Sayma Sadia

B.Sc. (Engineering) Examination 2018
Roll No.: 190630
Reg. No.: 1065355
Session: 2019-2019

Project Supervisor

Sohag Sarker

Associate Professor
Department of Information & Communication Engineering
Pabna University of Science & Technology
Pabna, Bangladesh.

Department of Information & Communication Engineering Pabna University of Science & Technology Pabna-6600, Bangladesh

ACKNOWLEDGEMENT

First and foremost, I want to thank Allah, the Almighty, for his favor and mercy in helping me finish my assignment and study.

I would especially like to express my gratitude and respect to my honorable supervisor **Sohag Sarker, Associate Professor, Department of Information and Communication Engineering (ICE), Pabna University of Science and Technology (PUST),** for providing me with the chance to work under his guidance, continuous oversight, as well as constructive suggestions, advice, and support throughout the entire course of the work. I'm speechless with gratitude for all of his support and assistance. I would also like to express my gratitude and appreciation to all of my dear teachers in the department of Information and communication engineering for their diligent assistance and helpful suggestions.

Last but not least, I want to thank everyone who has supported me and inspired me to work on the project. I must also express my gratitude to my parents and friends for all of their support and assistance with this effort. It would have been incredibly challenging to finish this assignment without their assistance.

Sayma Sadia

Roll: 190630

Information and Communication Engineering (ICE)

Pabna University of Science and Technology (PUST)

"Allah is Almighty"

Department of Information and Communication Engineering

Pabna University of Science and Technology, Bangladesh

DECLARATION

*I hereby certify that the work which is being presented in the project entitled "**IOT Based Electricity Theft Detection System**" in partial fulfillment of the requirement for the award of degree of Bachelor of Science in Information and Communication Engineering, submitted in Information and Communication Engineering Department of Pabna University of Science and Technology, Pabna-6600,Bangladesh, is an authentic record of my own work carried out under the supervision of Sohag Sarker and refer other researcher's work which are duly listed in the reference section.*

This matter presented in this project has not been submitted for the award of any other degree of this or any other university.

Sayma Sadia

Roll not: 190630

CERTIFICATE

TITLE: IOT Based Electricity Theft Detection System

The Project titled Submitted by **Sayma Sadia, Roll No: 190630, Session:2018-19** has been accepted as satisfactory in partial fulfillment of the requirement for the degree of B.Sc. Engineering in **Information and Communication Engineering (ICE)**.

SUPERVISOR:

Signature: ----------

Name: Sohag Sarker

Assistant Professor

Department of Information and Communication Engineering

Pabna University of Science and Technology.

Date: ----------

TABLE OF CONTENTS

CHAPTER NO.	CHAPTER TITLE	Page No.
Acknowledgement……..		i
Declaration…… …..		ii
Certificate…….		iii
List of Figures……..		vi
List of Table...……..		vii
Abstract…….....		viii
CHAPTER 1	**INTRODUCTION**	**1-5**
1.1 Overview…….……		1
1.2 Literature Review…….		2
1.3 Proposed Model……		3
1.4 Summary……...……		5
CHAPTER 2	**METHODOLOGY**	**6-13**
2.1 Introduction……..……		6
2.2 Experimental Setup…….		6
2.2.1 Arduino Uno……		6
2.2.2 Current Sensor ……...……..		7
2.2.3 Nodemcu ESP8266……..……...…….		8
2.2.4 GSM SIM808 Module...……..…….		9
2.2.5 Software Setup ……...…….....		10
2.3 Hardware Analogy …….....		11
2.4 Workflow……..…….....		13
CHAPTER 3	**RESULT ANALYSIS**	**14-16**
3.1 Introduction…….…….		14
3.2 Theft Detection…….		14

CHAPTER 4 CONCLUSION 17

4.1 Introduction……. 17

4.2 Conclusion…..……. 17

References…… **18**
Appendix…… **19-25**

LIST OF FIGURES

1.1 IOT Architecture……. 1

1.2 Power Transmission Process …….. 2

1.3 Block Diagram of Proposed Model ……...……. 4

2.1 Arduino Uno ……..…….. 7

2.2 Current Sensor ……..…….. 8

2.3 Node MCU ……..…… 9

2.4 Arduino Logo AND Blynk Logo…… 9

2.5 GSM SIM808 Module ……..…… 9

2.6 Blynk Configuration Topology …….. 10

2.7 Hardware Connection Setup ……..…… 12

2.8 Flowchart for Line Tampering using IOT...…….. 13

3.1 Prototype of the system ……. 15

3.2 Screenshot of code's output in seral monitor……. 15

3.3 The screenshot of SMS sent with location detail …….. 16

3.4 Screenshot of Blynk app's output……. 16

List of Tables

Table 1. List of Hardware and Software Deployed 6

ABSTRACT

Internet of Things (IoT) is making next transformation within the world of web. It provides intelligent amenities to the society. Bangladesh is also not lagging behind to make use of IoT technology and because of this more cities are becoming smart in the country. Even though facing many challenges like garbage management, electricity and water supply. Electricity board in the township has many issues to provide the service at the expected level. One of the major issues is related to electricity losses which are of two types, technical and non-technical losses. Technical losses happen due to properties of materials utilized in transmission and dispersion system. Non-technical losses are electricity theft which includes tampering meters, unpaid bills, electric line tampering. Majority of the meter tampering issues have been resolved by taking smart meters into the picture but the line tampering issue still persists. The steps to solve line tampering problems include placing smart meters by removing lines which is exorbitant and time consuming. Thus, the paper provides unadorned and efficient way to solve the problem by IoT to detect the amount of electricity theft. When lines are connected in parallel, the electricity received is less than provided. Theft location is reported to the admin via SMS using SIM808 module. These things are monitored and managed by admin from remote place on the application to save the investigation time, energy, cost in a most efficient way possible. The results obtained are the comparisons between current v/s time with and without tampering. Also, the cost recurred when tampering is avoided.

Chapter 1

Introduction

1.1: Overview

The Internet of Things (IoT) is alluded as the Internet of Everything (IoE), comprising all the web-enabled gadgets that collect, send and act on information they secure from their encompassing situations utilizing inserted sensors, processors and communication equipment [1].

The IoT architecture consists of 4 stages [2] as shown in Fig. 1. The 1st stage includes sensing or collecting data from the devices through sensors which are processed by the boards. Devices may be home appliances; sensors may be temperature sensors and boards may include microcontroller boards. Data from the 1st stage is in the analog form. In the 2nd stage, IoT Gateways are responsible for conversion of data from analog to digital. The output of this conversion is routed to the 3rd stage which includes network/wireless services. The signal towers, WIFIs, LANs etc. are the services of this stage which are for further processing of the data. Once the data is processed & transformed, it needs to be stored, either locally or on the cloud. So, the 4th stage is the Backend Systems which may be data centers or cloud.

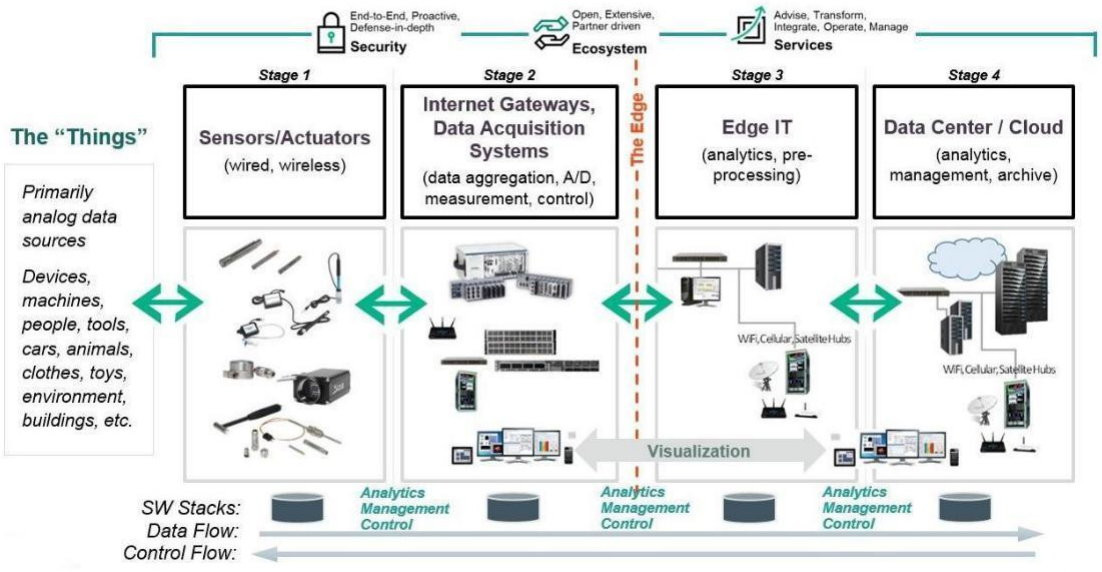


Figure1.1: IOT Architecture

1.2: Literature review

IoT is making part of buzz all over the world. Bangladesh is taking part by starting programs like Smart Bangladesh. As focusing on cities is vital for Bangladesh to develop, there is also a need to focus on challenges confronted by towns. Smart town concept got to be planned with focus on understanding grass root issues confronted by villagers[3]. The issues confronted by these villagers go unnoticed as the innovation arrangements are planned with cities within the setting.

one of the major issues faced by the towns is of electricity losses. They are of type technical and non-technical losses as. The electricity theft falls under non-technical losses. Line and meter tampering are major ways of electricity theft [1]. The meter tampering issues are almost solved taking smart meters in to the picture but the line tampering issue still exists. Fig. 2 shows the power transmission from generating stations to the consumer.

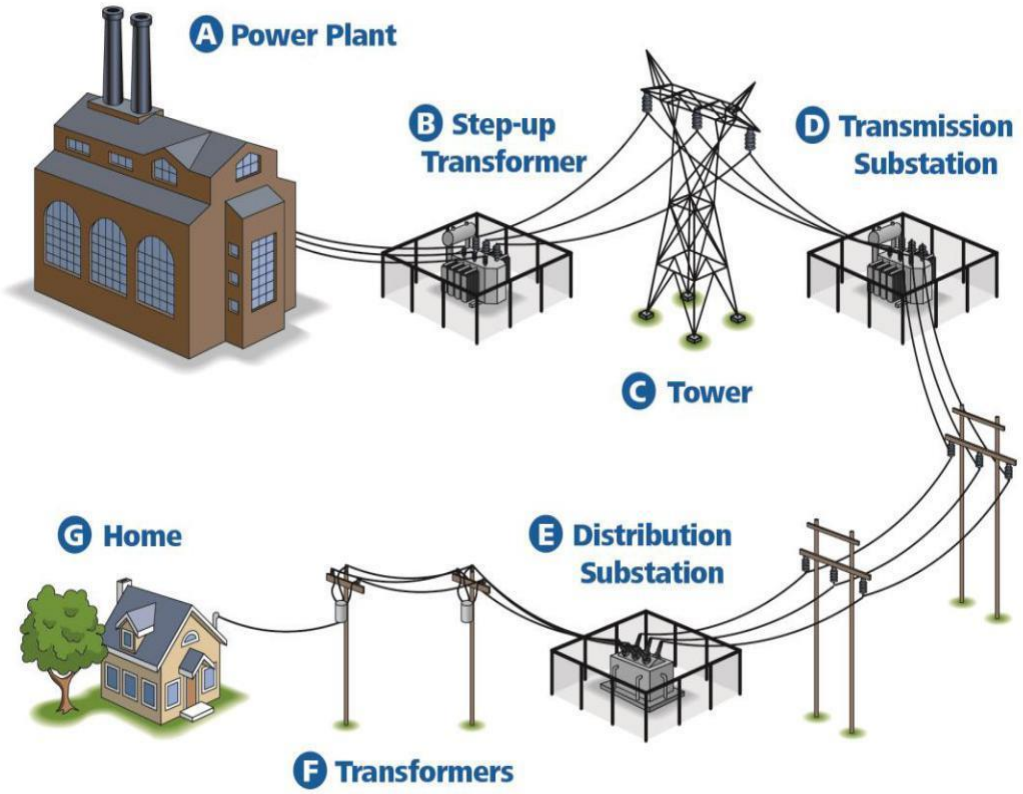


Figure 1.2: Power Transmission Process

Direct tapping from power line is very common to both high voltage and low voltage side causing huge loss of revenue since it can go for a long time undetected [3]. For the case of line tampering, it incorporates altering the terminal seal, breaking control wires and interfacing outside taps to decrease current going into the meter through shorting control wires [4]. To solve the issue of line tampering, the way being followed is replacing lines by smart meter which is costly and time consuming.

To avoid these issues, this paper focuses on saving the time of the officials with the energy being transmitted. It gives the amount of electricity theft with the location to the admin through SMS. The automatic power cut for that particular line is also provisioned so that no further theft should happen. These things can be monitored and managed by admin from the remote place saving investigation time, energy and the resources.

1.3: Proposed Model

Electricity theft is a major problem for electricity distribution companies, resulting in significant financial losses. It is estimated that electricity theft costs the global economy billions of dollars each year. In addition to the financial losses, electricity theft can also pose serious safety hazards.Traditional methods of detecting electricity theft are often labor-intensive and inaccurate. These methods typically involve manually inspecting meters and connections for signs of tampering. However, these methods are often difficult to scale and can be easily bypassed by thieves[4].

The proposed IoT-based electricity theft detection system utilizes smart meters, sensors, and cloud computing to detect and prevent electricity theft. The system is designed to be cost-effective, scalable, and accurate.

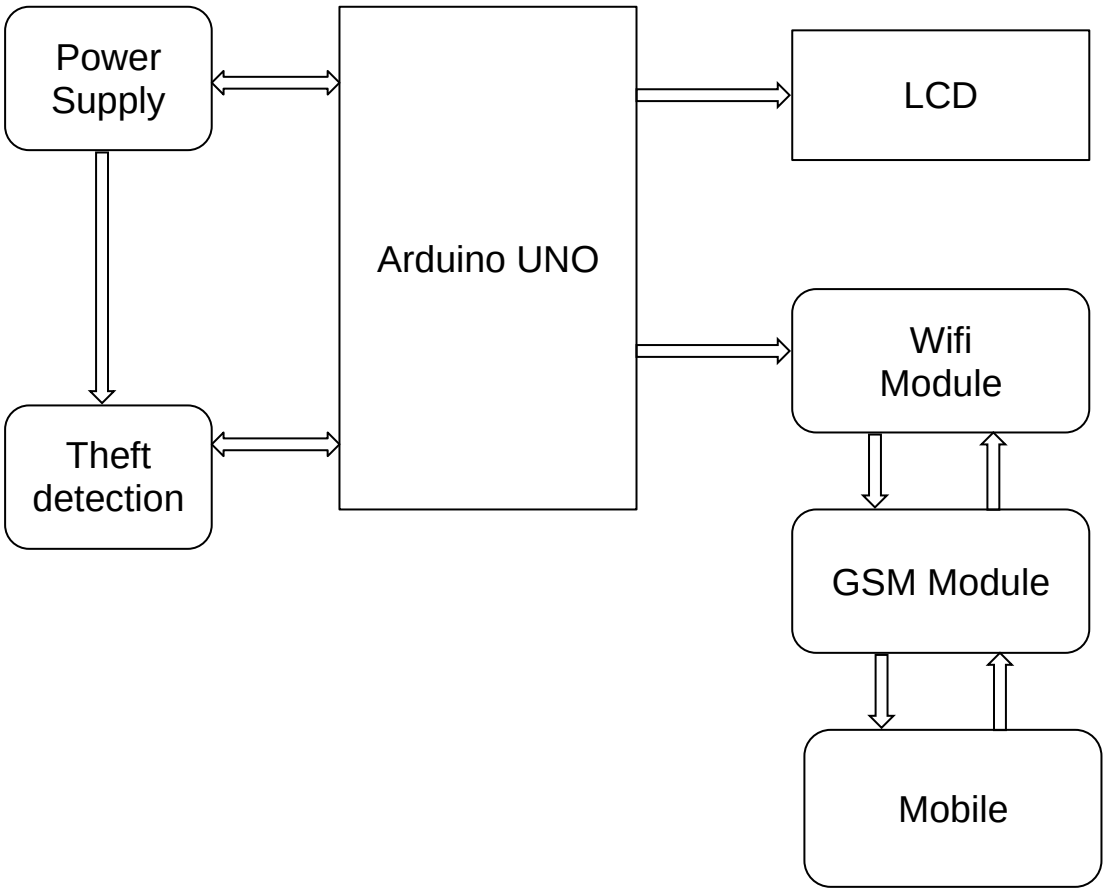


Figure 1.3 :Block Diagram of Proposed Model

The current sensor is placed in such a manner that detects the current both on the regional transformer and the consumer side. One of the Wi-Fi modules is used for sending the current reading of the consumer end to thingspeak from where the data is received by the other Wi-Fi module on the regional transformer end. Here, this Arduino on the transformer end is already taking the current reading and it compares this reading with the reading received from thingspeak [5]. If both the readings turn out to be same then no action is taken but if the readings come out to be different then it means that there is a theft in between which is drawing the surplus current of the transformer side. So, in case of theft the approximate location coordinates of the transformer end are fetched using geolocation API service. These coordinates are then sent to thingspeak where they are plot as “latitude” and “longitude” [5]. These coordinates are then sent to a mobile where they are displayed on the Google maps.

1.4: Summary

This project paper is organized in the manner with chapter 2 gives brief explanation about the work done i.e. methodology. Chapter 3 examines the result and chapter 4 concludes the article.

Chapter 2

Methodology

2.1: Introduction

This chapter gives brief explanation on the description of software and hardware, detailed connections setup, workflow.

2.2: Experimental setup

Electric lines are the main devices to be focused on. So, the Table I give the description about hardware and software used.

Table 1. List of Hardware and Software Deployed

Hardware (H)/Software (S)	Description
(H) Current sensor (ACS712) of 20A	To sense/measure the current, voltage, etc. in the lines.
(H) Arduino Uno	To process the data i.e. for conversion of data from analog to digital.
(H) SIM808	To find the location of the theft and to inform the admin via SMS.
(H) NodeMCU	To monitor and access the data.
(S) Arduino IDE	To program the code in C/C++
(S) Blynk App (online)	Application for admin to monitor, access the information related to the theft from remote place.

2.2.1: Arduino Uno

Arduino is an open-supply platform used for constructing electronics tasks. Arduino includes each a physical programmable circuit board (often called a microcontroller) and a piece of software program, or IDE (integrated improvement environment) that runs to your laptop, used to put in writing and add computer code to the physical board. The Arduino platform has grown to be quite famous with people simply beginning out with electronics, and for true cause. in contrast to most previous programmable circuit boards, the Arduino does no longer want a separate piece of hardware (known as a programmer) which will load new code onto the board – you can honestly use a USB cable. additionally, the Arduino IDE makes use of a simplified version of C++, making it less complicated to discover ways to use software program [7].

Figure 2.1: Arduino Uno

The Arduino programming is a simplified version of C/C++. in case you understand C, programming the Arduino can be familiar. if you do not now recognize C, no need to worry as just a few commands are hard to carry out beneficial functions. An important characteristic of the Arduino is that you may create a control software at the host computer, download it to the Arduino and it will run automatically. get rid of the USB cable connection to the computer, and this system will nevertheless run from the pinnacle on every occasion you push the reset button.do away with the battery and put the Arduino board in a closet for 6 months. While you reconnect the battery, the final program you stored will run. which means you connect the board to the host computer to expand and debug your application, but once this is completed, you do not need the laptop to run the program[8]. Subsequently, Arduino offers a well known shape component that breaks out the capabilities of the micro-controller into a greater handy package.

2.2.2: Current Sensor

The Allegro ACS712 offers comparatively cheap and particular solutions for AC or DC modern-day sensing in commercial, commercial, and communications structures. The device bundle lets in for clean implementation by using the purchaser. typical programs encompass motor control, load detection and control, switched mode electricity components, and over modern-day fault safety. The tool isn't meant for automobile packages. For the car grade model, see acs712[6].

Figure 2.2: Current Sensor

The device includes a particular, low-offset, linear corridor sensor circuit with a copper conduction direction positioned near the floor of the die. carried out present day flowing through this copper conduction route generates a magnetic discipline which is sensed by the included corridor IC and transformed right into a proportional voltage. device accuracy is optimized through the close proximity of the magnetic sign to the corridor transducer[8]. A particular, proportional voltage is provided with the aid of the low-offset, chopper stabilized Bi CMOS corridor IC, that is programmed for accuracy after packaging.

2.2.3: Nodemcu ESP8266

NodeMCU is an open-source Lua primarily based firmware and development board specially targeted for IoT primarily based programs. It includes firmware that runs at the ESP8266 wireless SoC from Espressif systems, and hardware that is primarily based at the ESP-12 module.The Nodemcu ESP8266 development board comes with the ESP-12E module containing ESP8266 chip having Tensilica Xtensa 32-bit LX106 RISC microprocessor. This microprocessor helps RTOS and operates at 80MHz to 160 MHz adjustable clock frequency. NodeMCU has 128 KB RAM and 4MB of Flash memory to save records and packages. Its high processing strength with in-constructed wi-fi / Bluetooth and Deep Sleep operating capabilities make it perfect for IoT projects.NodeMCU can be powered by the use of Micro USB jack and VIN pin (outside deliver Pin)[8]. It supports UART, SPI, and I2C interface.

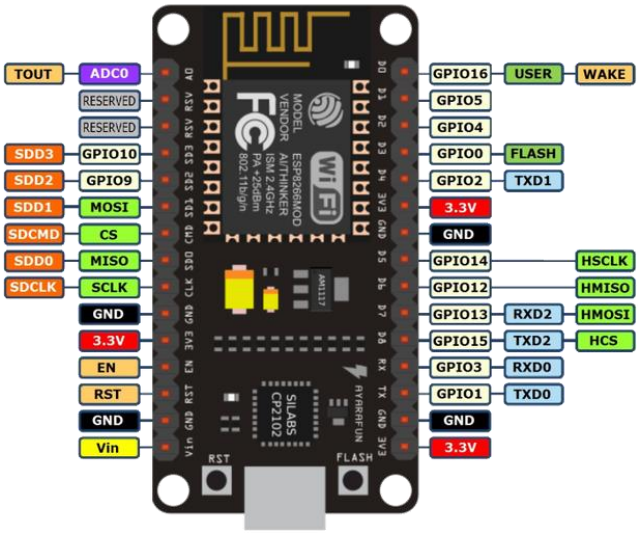


Figure 2.3: Node MCU

2.2.4: GSM SIM808 Module

SIM808 module is a complete Quad-Band GSM/GPRS module which combines GPS technology for satellite navigation. GSM Modem is built with dual band GSM engine-SIM 808. As mentioned in the above sensing circuit there is power theft then it will send message to Arduino as per our program and it will send message to GSM through. Also if mobile received SMS from authorized mobile phone[8].

Figure 2.4: GSM SIM808 Module

2.2.5: Software Setup

Figure 2.5: Arduino Logo AND Blynk Logo

An application called Arduino, an open-source hardware and software company, project and user community which designs and manufactures single-board microcontrollers for building digital devices is used to boot the program to the ESP32S module in this paper[6]. Also Blynk platform is the unified and easiest way that provide powerful web dashboard with drag and drop UI editor to manage devices, users and data and also provides Blynk IOT mobile application which provides user friendly addable widget.

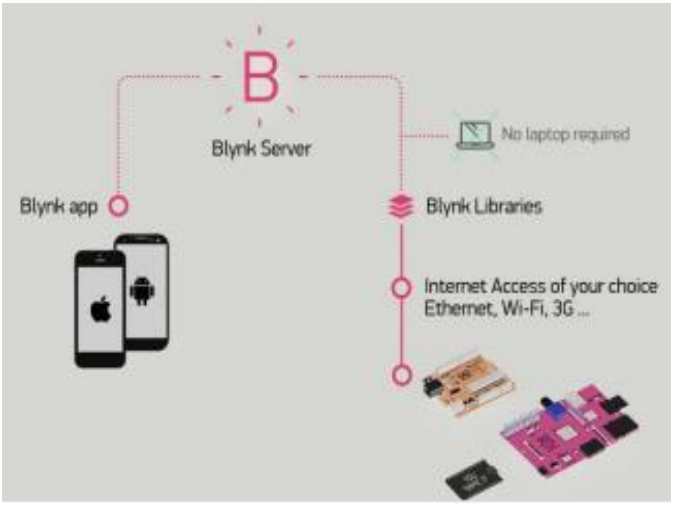


Figure 2.6: Blynk Configuration Topology

Blynk Library is created by Blynk corporation which provides a digital dashboard where we could build a graphic interface for the paper by simply dragging and dropping available widgets[7]. We can use Blynk's platform quickly which can support both Arduino and NodeMcu over Wi-Fi, Ethernet, or an ESP8266 chip. This library can download from open-source forum and can be manually added from Arduino library manager. While adding manually the esp32 chip must be selected[6].

However, as we see the Cloud Blynk server has imposed limitations which are due to the topology of the server: depending on your geographical location, the server may be in a different continent, which makes communications between the app, the devices, and the server slow due to the amount of time it takes packets to travel across the Internet.

2.3: Hardware Analogy

Insert a 4G sim card with internet and SMS options enabled in the SIM808. Connect GPS and GSM antenna. Now, connect the GND(Power/Analog In) of Uno to SIM808 GND, (Digital In) Tx(8) of Uno to Rx of SIM808, Rx(7) of Uno to Tx of SIM808, GNDs of ACS712 to GND(Power/Analog In) of Uno, OUT of a ACS712 to A0(Analog In) of Uno, OUT of another ACS712 to A1(Analog In) of Uno, VCCs of ACS712 to 5v(Power/Analog In) of Uno. While using the SIM808, the GPS antenna should be kept in an open place to get accurate location. All these connections between Uno, current sensor, SIM808 are done through jumper wires.

Now, connect 1 end of one ACS712 to 1 end of the bulb and other end of ACS712 to 1 end of the switch, the other end of the bulb to the left out end of the plug, connect the other end of the switch to the one end of another ACS712 and connect the other end of it to the plug. Take another bulb and connect it with wires having open ends before the switch. These connections between bulb and the current sensor are made through copper wires. Now connect Uno and Pi3 through USB cable. Insert the bulb and ACS712 connected plug to the socket to power up. Then power up SIM808 by connecting to an adapter. Fig. 3 gives the detailed connections in a pictorial representation.

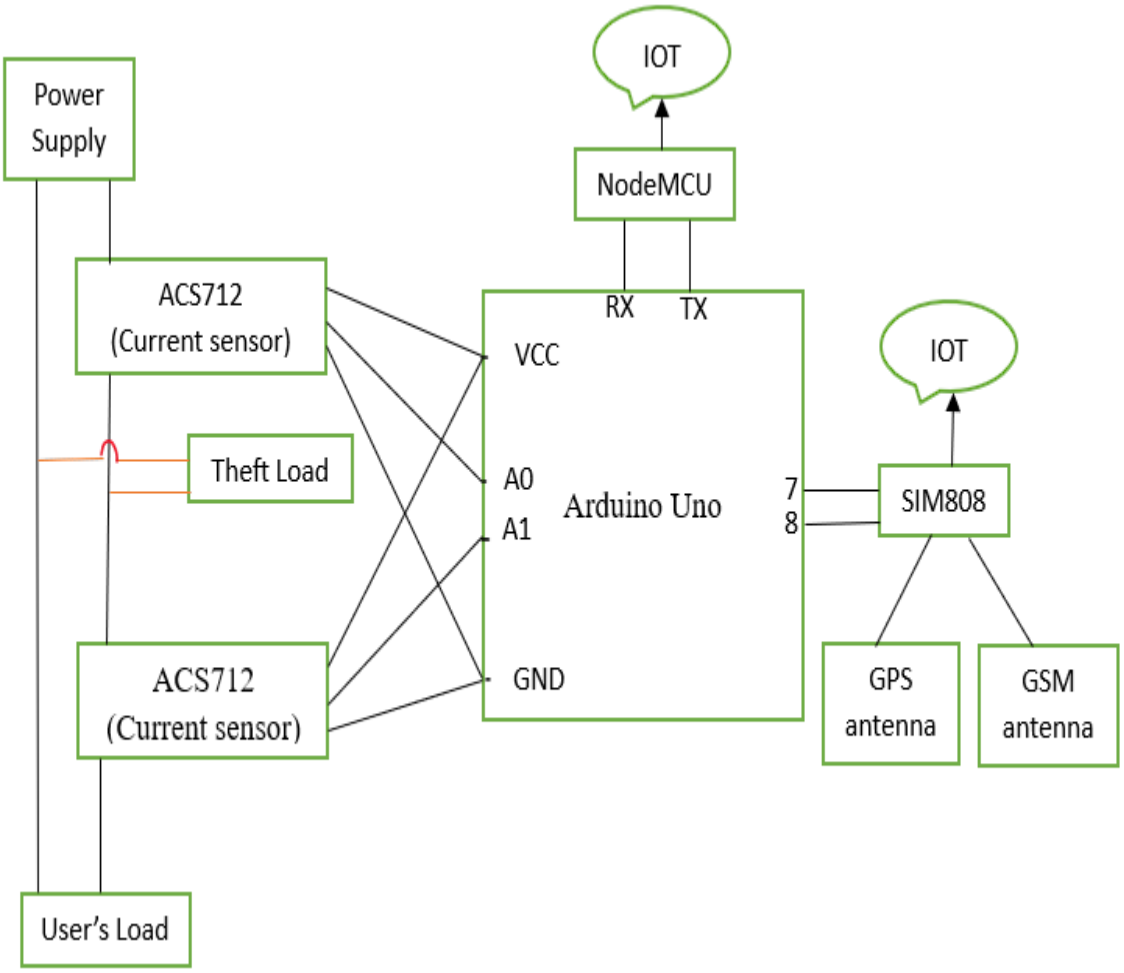


Figure 2.7: Hardware Connection Setup

This analogy will use a simple circuit to represent the electrical system, and a microcontroller to represent the central server. The sensor data will be represented by voltage signals, and the alerts will be represented by LED lights.

2.4: Workflow

The setup function includes and initialing the variables for current, Latitude, Longitude, Time GPS and admin's phone number. Then, initializing SIM808 for powering it up, configuring it through set of AT commands like AT+CMGF=1 and AT+CGNSPWR=1. Then, set the baud rate to 9600 bits per second to process the received data quickly. The loop function is for running the part of the code n number of times. Initially current transferred or produced through the line is calculated by both the current sensors. Now, another wire with bulb of 60W is connected in parallel with the main line having bulb of 60W, which increases the current from 0.24amps to 0.47amps and its difference is calculated. If the "current1" (calculated by supply side current sensor) is greater than "current2" (calculated by user end current sensor), then through the AT commands like AT+CGNSINF = location (latitude and longitude) is sent to the given AT+CMGS = number via SMS. This whole part is about detecting the theft.

Now, the data is received by the admin where he can view the location on the map and manage the data which will be stored continuously either on the local server or on the cloud with graphical representation of the data. The application is built by using the Blynk App. Fig. 6 gives the process flow of the work carried out. Now, the data can be extracted for the data analytics purpose. Thus, the work provides accessing data from remote place for the admin to save time, energy, resources, cost, etc.

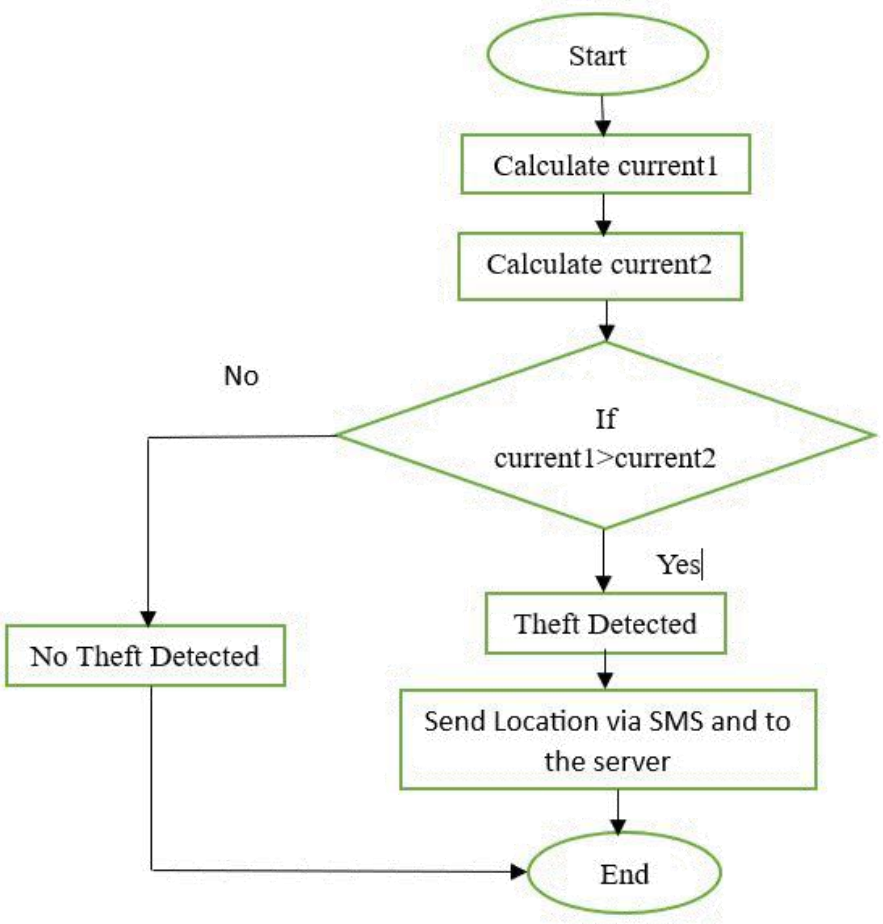


Figure 2.8: Flowchart for Line Tampering using IOT

Chapter 3

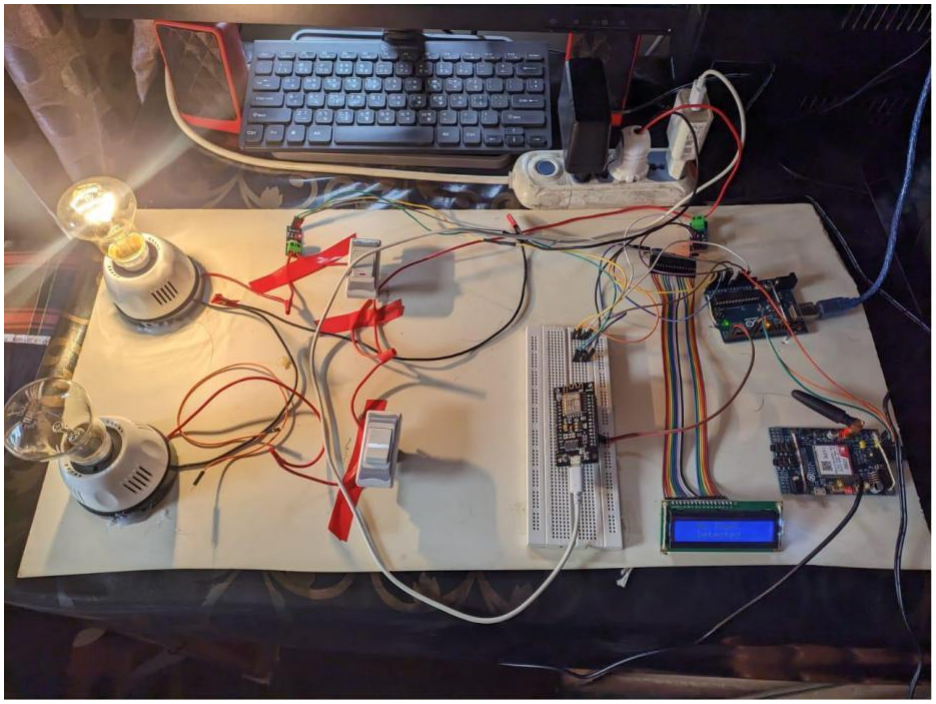
Result Analysis

3.1: Introduction

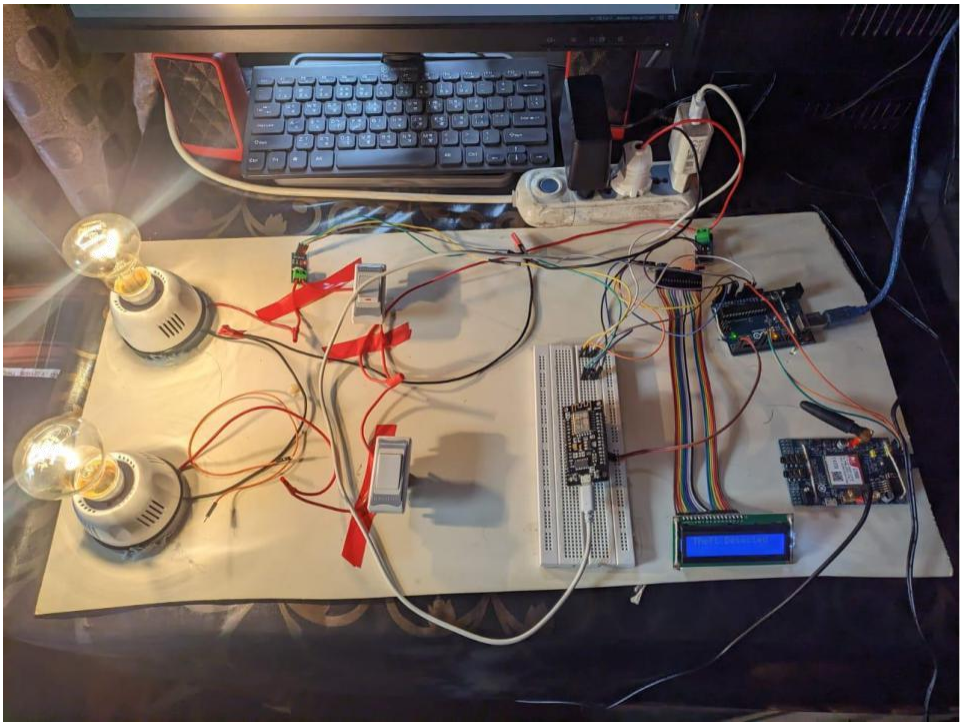
This chapter gives brief explanation about the outcome of the work done in different parts.

3.2: Theft Detection

The current is measured in amperes. Initially both the current values were equal around 0.24amps to 0.26amps so no theft detected. But, as soon as the new line is connected in parallel with the main line, “current1” becomes greater than “current2” which detects theft. After theft is detected geographical location (latitude and longitude) is sent to the admin's phone number via SMS where he can manage it remotely on the mobile application. Fig. 5 shows screenshot of code’s output in seral monitor. Fig.6 shows the screenshot of SMS sent with location details and Fig.7 shows the screenshot of Blynk app’s output. And also, in fig. 8 shows the prototype of the system (a) In case of no theft (b) in case of theft.



(a)



(b)

Figure 3.1: Prototype of the system (a) in case of no theft occurrence(b) in case of theft occurrence

```
Theft Detected
Time:20230711021024.000
Latitude:24.016097
Longitude:89.234400
Theft Detected
Time:20230711021024.000
Latitude:24.016097
Longitude:89.234400
Theft Detected
Time:20230711021024.000
Latitude:24.016097
Longitude:89.234400
```

Figure 3.2: Screenshot of code's output in seral monitor

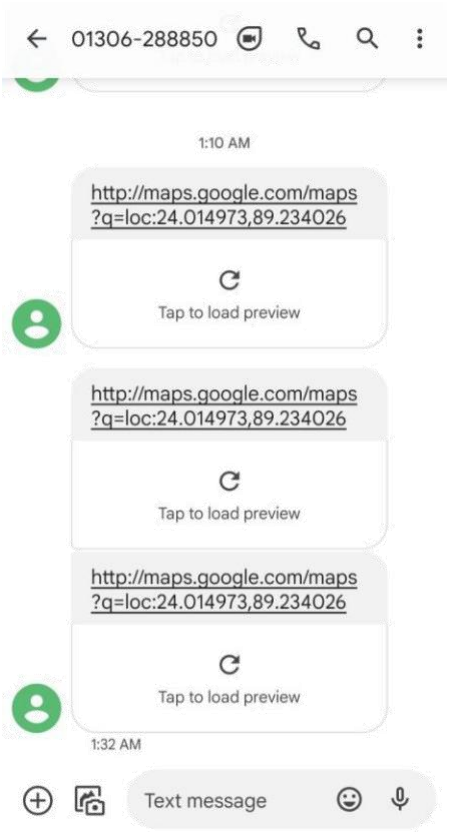


Figure 3.3: the screenshot of SMS sent with location detail

Figure 3.4: screenshot of Blynk app's output.

Chapter 4

CONCLUSION

4.1: introduction

This chapter states the brief explanation of the issue considered, work carried out, results obtained and comparison of the work with similar works done.

4.2: Conclusion

The work has been successfully carried out in the way that it gives solution for line tampering. Other author's work is mainly focused on the meter tampering. The work included IoT devices and software for the connection. There are several issues we faced regarding this project. This project can provide region wise GPS location to the admin. Although NedeMCU is an easy-to-use cheap microcontroller which open-source firmware, it requires strong WIFI signal to upload data. Again, the SIM808 module works great when the signal is adequate. Its reliability becomes less in low signal condition and in that case the GSM feature does not work. The GPS antenna needs to be under open sky for proper calculation of location.

In future, the meters are to be placed at the generation station and receiving end to check whether the electricity produced and received is same or not at all the respective places. The location tracker and cameras are to be placed in all the important places where exact location can be tracked. Batter GSM and GPS antenna would increase the reliability. Theft area prediction is to be made based on the records to prevent theft before it happens. As well as automatic power cut feature in case of theft occurred can be added for prevent further electricity theft.

References

[1] M. a. E. V. S. Singh, "Minimizing electricity theft by internet of things," *International Journal of Advanced Research in Computer and Communication Engineering,* 2015.

[2] J. R. Pimentel, "An effective and easy to use IoT architecture.," *Factory Communication Systems (WFCS),* 2014.

[3] S. S. S. R. Depuru, "Measures and setbacks for controlling electricity theft," *North American Power Symposium (NAPS),* 2010.

[4] M. a. H. V. P. Tariq, "Real time electricity theft detection in microgrids through wireless sensor networks," *SENSORS, 2016 IEEE.* ,2016.

[5] F. T. Zohora Saima, M. N. Islam Rimon, T. I. Talukder, J. Ali, Z. Hossain and N. Sadia, "IoT and GSM Based Smart Grid Controlling and Monitoring System," *2022 International Conference for Advancement in Technology (ICONAT)*, Goa, India, 2022,

[6] Prabu, S. "Blynk 2.0 based Smart Electricity Monitoring Meter."2014.

[7] Pawar, Vijaya R., Janhavi J. Jadhav, Jayasmita Saha, and Shreya S. Jadhav. "Arduino Uno Based Automatic Power Theft Detection."2016.

[8] Mohite, Nilesh, Rinkuraj Ranaware, and Prakash Kakade. "GSM based electricity theft detection." *International Journal of Scientific Engineering and Applied Science* 2 (2016).

[9] https://sist.sathyabama.ac.in/sist_naac/documents/1.3.4/b.e-eee-batchno-21.pdf

Appendix:

Programing Code of Arduino uno for theft detection:

```
#include <SoftwareSerial.h>

SoftwareSerial sim808(7,8);

char phone_no[] = "01868391381";

String data[5];

#define DEBUG true

String state,timegps,latitude,longitude;

#include "ACS712.h"

#include <Wire.h>

#include <LiquidCrystal_I2C.h>

ACS712 sensor1(ACS712_20A, A0);

ACS712 sensor2(ACS712_20A, A1);

LiquidCrystal_I2C lcd(0x3F, 16, 2);

void setup() {

 Serial.begin(9600);

 sim808.begin(9600);

 delay(50);

 sim808.print("AT+CSMP=17,167,0,0"); // set this parameter if empty SMS
received delay(100);

 sim808.print("AT+CMGF=1\r");

 delay(400);

 sendData("AT+CGNSPWR=1",1000,DEBUG);

 delay(50);

 sendData("AT+CGNSSEQ=RMC",1000,DEBUG);

 delay(150);
```

```
 sensor1.calibrate();
  sensor2.calibrate();
  lcd.begin();
}
void loop() {
  float current1 = sensor1.getCurrentAC();
  float current2 = sensor2.getCurrentAC();
  // Check if current is below a certain threshold, set it to
  zero if (current1 < 0.15) {
            current1 = 0;
  }
  if (current2 < 0.08) {
    current2 = 0;
  }
  if (current1 > 0.20)
  {
    if(current1 > 0.4)
    {
      if(current1>0.5)
      {
        current1=0.50;
      }
      else
      {
        current1=0.40;
      }
    }
    else
    {
      current1 = 0.24;
```

```
  }
}
if (current2 > 0.20)
{
 if(current2 > 0.4)
 {
  if(current2>0.5)
  {
   current2=0.50;
  }
  else
  {
   current2=0.40;
  }
 }
 else
 {
  current2 = 0.24;
 }
}

if(current1>current2)
{
 Serial.println(" Theft Detected");
 lcd.clear();
 lcd.print("Theft Detected");
 delay(1000);
 sendTabData("AT+CGNSINF",1000,DEBUG);
 Serial.println(" Time:"+timegps);
 delay(3000);
```

```
  Serial.println(" Latitude:"+latitude);
  delay(5000);
  Serial.println(" Longitude:"+longitude);
  sim808.print("AT+CMGS=\"");
  sim808.print(phone_no);
  sim808.println("\"");
  delay(300);
  sim808.print("http://maps.google.com/maps?q=loc:");
  sim808.print(latitude);
  sim808.print(",");
  sim808.print (longitude);
  delay(200);
  sim808.println((char)26);
  delay(200);
  sim808.println();
 delay(20000);
 sim808.flush();
  delay(1000);
}
else
{
  Serial.println(" No Theft");
  lcd.clear();
  lcd.print("   No Theft");
  lcd.setCursor(3,1);
  lcd.print("Detected");
  delay(2000);
}
```

```
  delay(5000);
}

void sendTabData(String command , const int timeout , boolean debug){
  sim808.println(command);
  long int time = millis();
  int i = 0;
  while((time+timeout) > millis()){
    while(sim808.available()){
      char c = sim808.read();
      if (c != ',') {
        data[i] +=c;
        delay(100);
      }
       els
       e
       {
       i+
       +;
      }
      if (i == 5) {
        delay(100);
        goto exitL;
      }
    }
  }exitL:
  if (debug) {
    state = data[1];
    timegps = data[2];
    latitude = data[3];
    longitude =data[4];
```

```
  }

}

String sendData (String command , const int timeout ,boolean
  debug){ String response = "";

  sim808.println(command);

  long int time = millis();

  int i = 0;

  while ( (time+timeout ) > millis()){

    while (sim808.available()){

      char c = sim808.read();

      response +=c;

    }

  }
  if (debug) {

     Serial.print(response);

     }
     return response;

}
```

Programing code for NodeMCU for theft detection:

```
#define BLYNK_PRINT Serial

#include <ESP8266WiFi.h>

#include <BlynkSimpleEsp8266.h>

#define VIRTUAL_PIN V3 // Replace V1 with the desired virtual pin number


char auth[] = "h-76q0c6wR8YAmxhIx6qQ2OPDBSqqne6"; // Replace with your
Blynk auth token

void setup() {

  Serial.begin(9600);

  Blynk.begin(auth, "JAHED", "95K8f790");  // Replace with your WiFi credentials

}

void loop() {

   char buffer[300]="";
```

```
 if(Serial.available()>0){
   char data=Serial.read();
   Serial.readBytesUntil('\n',buffer,20);
   Serial.println(buffer);
   String message = buffer; // Message to be sent to
   Blynk Blynk.run();
   Blynk.virtualWrite(VIRTUAL_PIN, message); // Send data to Blynk app
 }
}
```