DAYANANDA SAGAR COLLEGE OF ENGINEERING

(An Autonomous Institute affiliated to VTU, Belagavi - 590018)
Accredited by National Assessment & Accreditation Council (NAAC) with 'A' grade
Shavige Malleshwara Hills, Kumaraswamy Layout
Bengaluru-560078

Mini Project Report on

POWER THEFT DETECTION AND MONITORING SYSTEM WITH TWO-WAY DATA RECORDING IN REAL-TIME

Submitted in partial fulfillment for the award of degree of

Bachelor of Engineering
in
Electrical and Electronics Engineering

Submitted by

NAVNEET RAJ	**1DS21EE062**
NIKHILESH SINGH	**1DS21EE063**
RAHUL KUMAR	**1DS21EE076**
RASHISH BHARGHAV	**1DS21EE081**

Under the Guidance of
Dr. Sujit Kumar
Assistant Professor,
Dept. of E&E Engg.
DSCE, Bengaluru

VISVESVARAYA TECHNOLOGICAL UNIVERSITY
JNANASANGAMA, BELAGAVI-590018
2023-24

DAYANANDA SAGAR COLLEGE OF ENGINEERING

(An Autonomous Institute affiliated to VTU, Belagavi – 590018, Approved by AICTE & ISO 9001:2015 Certified)
Accredited by National Assessment & Accreditation Council (NAAC) with 'A' grade
Shavige Malleshwara Hills, Kumaraswamy Layout
Bengaluru-560078
2023-2024

DEPARTMENT OF ELECTRICAL & ELECTRONICS ENGINEERING

CERTIFICATE

Certified that the mini project report entitled **"Power theft detection and monitoring system with two-way data recording in real-time"** carried out by **NAVNEET RAJ** bearing **USN: 1DS21EE062, NIKHILESH SINGH** bearing **USN: 1DS21EE063, RAHUL KUMAR** bearing USN: **1DS21EE076, RASHSISH BHARGHAV** bearing USN: **1DS21EE081** are bonafide students of **DAYANANDA SAGAR COLLEGE OF ENGINEERING**, an autonomous institution affiliated to VTU, Belagavi in partial fulfillment for the award of Degree of **Bachelor of Engineering in Electrical and Electronics Engineering** during the year **2023-2024**. It is certified that all corrections/suggestions indicated for Internal Assessment have been incorporated in the report deposited in the departmental library. The mini project report has been approved as it satisfies the academic requirements in respect of work prescribed for the said Degree.

Signature of the Guide	Signature of the HOD	Signature of the Principal
Dr. Sujit Kumar	Dr. M. Premkumar	Dr. B G Prasad
Assistant Professor	Professor & HOD	Principal
Dept. of E&E Engg.	Dept. of E&E Engg.	DSCE, Bengaluru
DSCE, Bengaluru	DSCE, Bengaluru	

Name of the Examiners	Signature with date
1.	....
2.	....

DAYANANDA SAGAR COLLEGE OF ENGINEERING

(An Autonomous Institute affiliated to VTU, Belagavi – 590018, Approved by AICTE & ISO 9001:2015 Certified)
Accredited by NBA, National Assessment & Accreditation Council (NAAC) with 'A' grade
Shavige Malleshwara Hills, Kumaraswamy Layout
Bengaluru-560078
2023-2024

DEPARTMENT OF ELECTRICAL & ELECTRONICS ENGINEERING

DECLARATION

We, **Navneet Raj (1DS21EE062), Nikhilesh Singh (1DS21EE063), Rahul Kumar (1DS21EE076) and Rashish Bharghav (1DS21EE081)**, respectively, hereby declare that the mini project work entitled **"Power Theft Detection And Monitoring System With Two-Way Data Recording In Real-Time"** has been independently done by us under the guidance of **Dr. Sujit Kumar, Assistant Professor, EEE department** and submitted in partial fulfillment of the requirement for the award of the degree of Bachelor of Engineering in Electrical & Electronics Engineering, at Dayananda Sagar College of Engineering, an autonomous institution affiliated to VTU, Belagavi during the academic year 2023-2024.

We further declare that we have not submitted this report either in part or in full to any other university for the award of any degree.

NAVNEET RAJ	**1DS21EE062**
NIKHILESH SINGH	**1DS21EE063**
RAHUL KUMAR	**1DS21EE076**
RASHISH BHARGHAV	**1DS21EE081**

PLACE:

DATE:

ABSTRACT

India, one of the fastest-growing economies, faces significant challenges in its power sector due to widespread electricity theft. Despite being the third-largest producer and second-largest consumer of electricity globally, with an installed capacity of 395.07 GW as of January 2022, India loses about 34% of its generated electricity to technical and commercial factors, impacting revenue collection and sector stability.

Electricity theft, defined under Section 135(1) of the Electricity Act 2003, includes unauthorized connections, meter tampering, and fraudulent billing practices. These issues are pervasive across rural and urban areas, leading to substantial financial losses.

The Union Power Ministry's key measures to combat this include the adoption of smart meters. These devices offer precise billing, remote control of consumption, and detection of unusual power demands. Smart meters are being deployed in states like New Delhi, Maharashtra, Andhra Pradesh, Puducherry, and Karnataka to enhance efficiency and reduce theft.

A proposed solution is a real-time power theft monitoring and detection system using smart meters. Equipped with sensors, these meters enable continuous two-way communication for accurate power measurement from distribution transformers to consumer houses. This system focuses on monitoring the distribution network, ensuring accurate power measurement and reducing theft.

Implementing smart metering systems, along with public awareness campaigns and stringent monitoring, is crucial for mitigating electricity theft in India. These measures will ensure reliable and equitable electricity distribution, supporting the nation’s economic growth and development.

AKNOWLEDGEMENT

The satisfaction and euphoria that accompany the successful completion of any task would be incomplete without the mention of people who made it possible and under whose constant guidance and encouragement the task was completed. We express our sincere regards to the **Management of Dayananda Sagar College of Engineering, Bengaluru.**

We express our sincere regards and thanks to **Dr. B G Prasad, Principal, Dayananda Sagar College of Engineering, Bengaluru.** His incessant encouragement guidance and valuable support have been immense help in realizing this mini project.

We express our sincere regards and thanks to **Dr. Premkumar M, Professor & HOD, Department of Electrical and Electronics Engineering, Dayananda Sagar College of Engineering, Bengaluru.** His incessant encouragement guidance and valuable technical support have been immense help in realizing this mini project. His guidance gave us the environment to enhance our knowledge, skills and to reach the pinnacle with sheer determination, dedicated and hard work.

We would like to express profound gratitude to our guide **Dr. Sujit Kumar, Assistant professor, Department of Electrical and Electronics Engineering, Dayananda Sagar College of Engineering, Bengaluru** who has encouraged us throughout the mini project. His moral support enabled us to complete our work successfully.

We express our sincere thanks to Mini project Coordinator **Dr. Suchana Mishra**, **Assistant Professor, Department of Electrical and Electronics Engineering** for her continues support and guidance. We thank all teaching and non-teaching staff of Electrical and Electronics Engineering department for their kind and constant support throughout the academic Journey.

NAVNEET RAJ	**1DS21EE062**
NIKHILESH SINGH	**1DS21EE063**
RAHUL KUMAR	**1DS21EE076**
RASHISH BHARGHAV	**1DS21EE081**

TABLE OF CONTENTS

LIST OF FIGURES

DAYANANDA SAGAR COLLEGE OF ENGINEERING

(An Autonomous Institute affiliated to Visvesvaraya Technological University (VTU), Approved by AICTE and UGC, Accredited by NAAC with an "A" grade)

DEPARTMENT OF ELECTRICAL & ELECTRONICS ENGINEERING

(Accredited by NBA Tier-1: 2022-2025)

Mini Project Course Outcomes and Mapping

Course Outcomes: The Students would be able to

CO1	**Identify a topic related to present day challenges.**
CO2	**Analyze technical aspects of the chosen project with a systematic approach to find a feasible solution for the chosen work.**
CO3	**Use/ implement modern Engineering tools/ technologies to get optimized results**
CO4	**Demonstrate an ability to work in teams.**
CO5	**Develop presentation ,communication and report writing skills**

CO'S\PO'S\PSO	**CO-PO Mapping**														
	PO 1	**PO 2**	**PO 3**	**PO 4**	**PO5**	**PO6**	**PO7**	**PO8**	**PO9**	**PO10**	**PO11**	**PO12**	PSO1	PSO2	PSO3
CO1	3	2	1	1	2	2	2	2	1	2	3	1	1	2	3
CO2	3	3	2		2	3	3	2	1	1	2	2	1	2	1
CO3				1	2										
CO4			2			1	3		3	3	3	1	2	3	1
CO5			2	2	3	2	3	2	3	1					

CHAPTER 1 – INTRODUCTION

India is one of the fastest growing economies and the changing time has completely changed the dynamics of human life at par. Ever since the inception of electricity it has served mankind significantly and thus became the fourth pillar of life apart from food clothing and shelter. India is the third largest producer and second largest consumer of electricity worldwide with an installed capacity of 395.07 GW as of January 2022.2 Still Indian Power Sector is facing a serious issue of lean revenue collection against the energy supplied and one of the major reasons behind the revenue losses is electricity theft.

On an average in India about 34% of the generated electricity is lost due to losses, both technical and commercial. Electricity theft may seem like a petty offence at rural level but it is rampant at urban level and when looked at national level the impact of this offence magnifies and the financial loss it brings is beyond imagination[1].

1.1 - Meaning of Electricity Theft

Electricity theft is a criminal practice of stealing electric power. Section 135(1) of the Electricity Act 2003 defines 'Theft of Electricity' which says a person is guilty of electricity theft if he dishonestly makes use of electricity in the following ways. Taps or makes any connection with overhead, underwater lines or cables. Tampers meters or uses current reversing transformer, or any device which interferes with accurate registration of electric current. Damage or destroy electric meter, equipment or wire so as to interfere with proper metering of electricity. Use of electricity for the purpose other than for which the usage of electricity was authorized. Irregularity in paying the bill by bribing the billing authority and record the meter at a lower number than what it is shown in real life.[1]

Further the Electricity theft can be categorized in different kinds as per the electrical equipment used to carry out this offence and they are:

Billing irregularity and Unpaid Bills.

Meter Tampering: This one meter can be used in different ways to carry out the electricity theft. Tampering of meters and preventing the mechanical disc from moving by sealing it. Next is to bypass the meter illegally by connecting it to the fuse which prevents the movement of rotating disc and the consumption of energy is not recorded. The other method includes opening of meter without damaging its seal and reversing the dials. Electronic meters can also be tampered by a sudden electrostatic discharge which causes latent or permanent damages.[2]

Wires and Cables: Illegal tapping of bare wires or underground cables is another way of electricity theft. Even at times the circuit wire is disconnected or broken from the circuit terminal block and a triple breaker is inserted in the circuit to carry of theft.[3]

1.2 - Issues and Challenges for curbing Electricity Theft

Electricity is the strongest pillar of all-round growth and development of any economy as it facilitates everything from domestic uses to education, from commercial uses to industrialization, from charging gadgets to charging electrical vehicle, to even connecting the world via internet. Nothing in left untouched by electricity and still availability of electricity is a dream for many till today. Electricity theft is a major reason for huge electricity losses in the county and it is backed by few other issue and challenges which makes it even worse. Government of India is providing free electricity to households of BPL (below poverty line) under the Deen Dayal Upadhyaya Gram Jyoti Yojana (DDUGJY) scheme but the BPL households are not willing to take this free electricity connections in fear of high amounted bills, this further highlights the other issue of unawareness among the people about electricity schemes[1]. Quality, reliability and timing of electricity supply are also considered as important reasons for not taking up electricity connections. Bigger states like Uttar Pradesh has a prevalent practice of ‘katia Connection’ which is nothing but direct theft of electricity and this issues has to monitored seriously by the discom staff of the respective state[3]. Furthermore some of the major challenges faced are invalid meter reading due to installation of meter at inaccessible places, absence in quality checks, errors in recording the electricity consumption, data tampering all these magnifies the non-technical losses to greater extent[1].

1.3 - Measures by Government to curb Electricity Theft

The Union Power Ministry came up with suggestions for the States that the power distribution companies should raise awareness among public about curbing electricity theft and irregularities and focus on quality, quantity, reliability and supply of electricity. The Ministry has also suggested 100 percent metering at all levels to facilitate energy audit and rationalization of cost of connection at rural level and improve energy efficiency and interventions which are made to reduce the AT&C (aggregate technical and commercial) losses.

Government of India has introduced smart meters as they are becoming extremely relevant in power saving and giving the exact bill. It can remotely control the electricity consumption and maximize the energy efficiency and load balancing. They are highly cost- effective and are capable of having one way communication. These smart meters are good for distribution companies which will help them detect unusual and heavy power demand. It’s very useful in areas where the ratio of electricity theft is high and manually detecting it is difficult. The electricity service providers can further discontinue the services to domestic and commercial users which don’t pay bills.

1.4 - PROPOSED SYSTEM

Figure 1.2 presents a block diagram of a proposed real-time power theft monitoring and detection system. As stated, each smart meter consists of a current sensor, voltage sensor, Arduino ATMega328P microcontroller, and a GSM module. This system is designed to work in a combination of two-by-two continuous communication systems using feedback lines for accurate power measurement results. The main smart meter from the distribution transformer (main observer meter) communicates with the distribution pole grid 1 smart meter (observer meter) to measure power distributed from the distribution transformer against the power received by pole grid 1. The same applies with pole grid 1 to pole grid/node 2. The smart meter for distribution pole grid 1 (observer meter) communicates with the distribution pole grid/node 2 smart meter (observer meter). This includes the distributor pole node smart meter connected to the supply of each consumer house also communicates with the consumer house smart meter to measure power distributed from the pole node against the power received by each consumer house.

The proposed smart metering system is mainly designed to focus on the distribution network system starting from the distribution transformer (delta-star step-down transformer) receiving a Medium Voltage (MV) 11 kV three-wire supply system from the substation. It then stepped down to Low Voltage (LV) 400 V three-phase four-wire system (with 230 V single-phase). From the distribution transformer to each distribution pole grid, the proposed smart metering system can calculate the power distributed in three-phase or single-phase. With the simulated and implemented prototype design system, a single-phase (230 V) smart metering system is designed for system-accurate functionality testing. Therefore, a single-phase smart metering system is used from distribution pole grid number one to distribution pole grid number two, including two single-phase smart meters in consumer houses

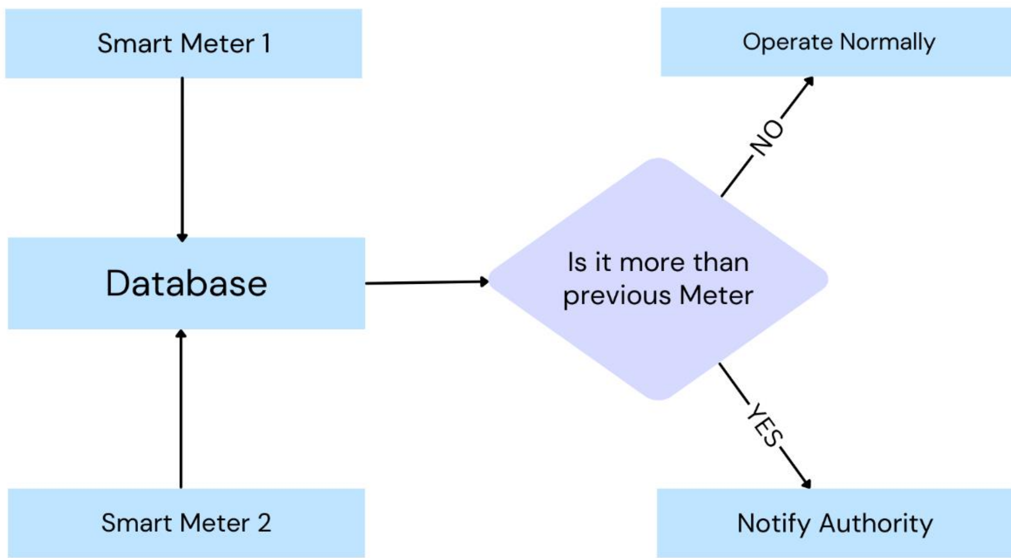


Fig 1.1 Proposed system working

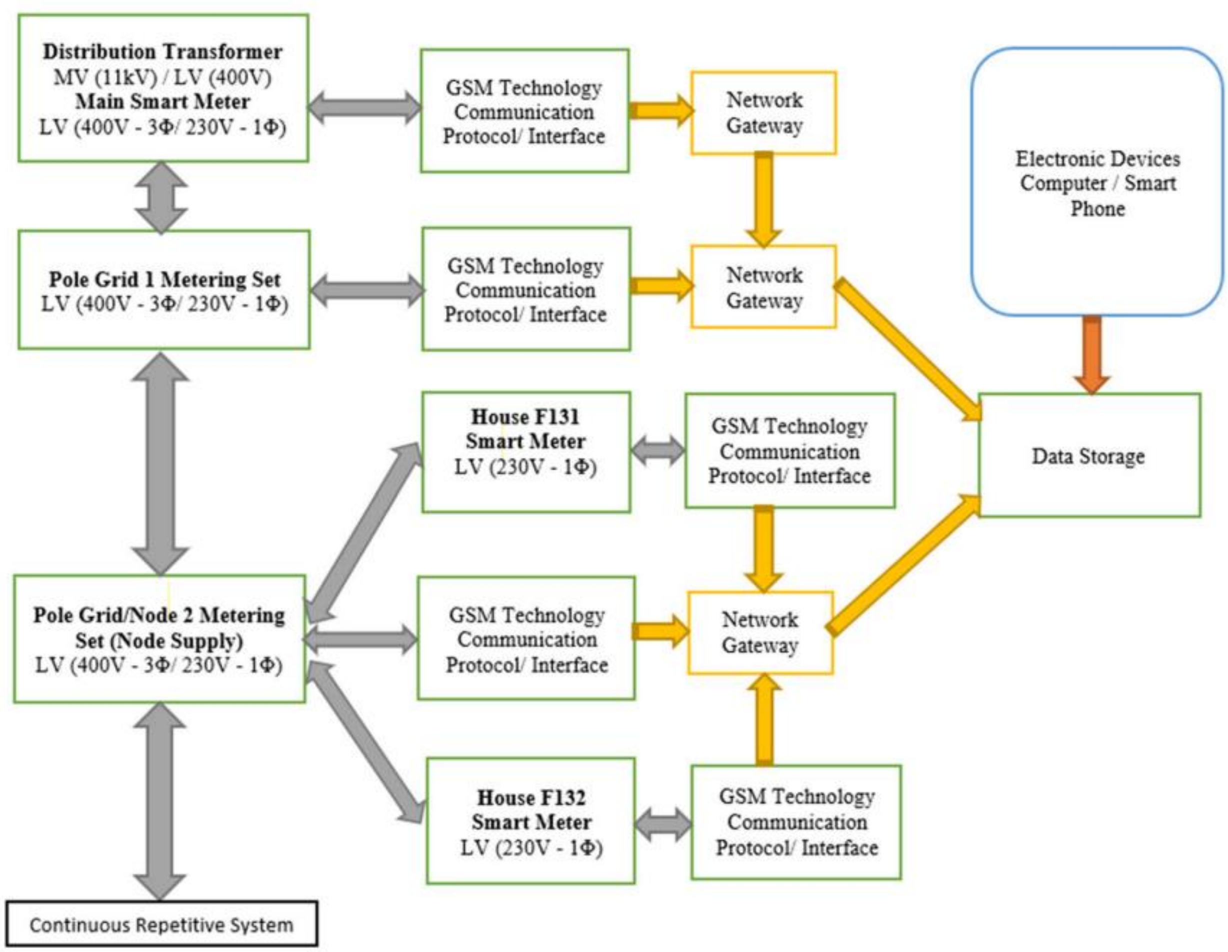


Fig 1.2 Data flow through various sensors

There should also be a three-phase supply be used from the distribution transformer to the distribution pole grids,

the authority would install the three-phase smart metering system in both distribution pole grids. In the distribution pole grid number one three-phase smart metering system, the current transformer (CT) would measure current flow from each of the three lines (L1, L2, and L3) and combine all three currents to get a total current. It will then calibrate it with the voltage transformer (VT) reading in all three lines to determine the three-phase power distributed from distribution pole grid one to distribution pole grid two. The distribution pole grid number two three-phase smart metering system supplying three consumer houses from each of the three lines (L1, L2, and L3) would measure the current reading of line 1 supplying consumer house 1. These include the current reading of line 2 supplying consumer house 2 and the current reading in line 3 supplying consumer house 3. Then those readings would be determined separately by the distribution pole grid number two smart metering system to capture the power supplied to each consumer house. It will also combine the three power distributed readings to determine the total three-phase power consumption from the distribution pole grid number two.

CHAPTER 2 – LITERATURE SURVEY

2.1 - Electricity Theft in India: An Analysis

(Year: 2023 |Conference Paper | Publisher: International Journal For Research and Analysis)

India, despite being one of the fastest-growing economies globally, struggles with a significant portion of its population living at a subsistence level. Electricity, which has become a fundamental pillar of modern life alongside food, clothing, and shelter, plays a critical role in economic development. As of January 2022, India stands as the third-largest producer and second-largest consumer of electricity worldwide, with an installed capacity of 395.07 GW. However, the Indian power sector grapples with a major challenge: significant revenue losses due to electricity theft.[1]

Electricity Theft and Its Impact

Electricity theft, a criminal activity that involves the unauthorized use or tampering of electric power, is a significant issue in India. Section 135(1) of the Electricity Act 2003 defines this crime as any dishonest act of using electricity without authorization, which includes illegal connections, meter tampering, or damaging electrical equipment to avoid proper metering. This theft can be categorized into various forms, such as billing irregularities, meter tampering, and illegal connections using wires and cables.

On average, India loses about 34% of generated electricity through both technical and commercial losses. While it may appear as a minor issue at the rural level, the scale of electricity theft in urban areas exacerbates the problem, leading to substantial financial losses nationwide.

Challenges in Addressing Electricity Theft

Addressing electricity theft in India involves several complex challenges. Despite government initiatives like the Deen Dayal Upadhyaya Gram Jyoti Yojana (DDUGJY), which offers free electricity connections to households below the poverty line (BPL), many eligible households avoid these connections due to fears of high bills and a lack of awareness about the scheme. Furthermore, issues such as the quality, reliability, and timing of electricity supply deter people from accepting these connections.

States like Uttar Pradesh face specific issues like the ‘katia connection,’ a direct theft method that requires stringent monitoring by distribution companies. Additional challenges include invalid meter readings due to inaccessible installation sites, poor quality control, and data tampering, which exacerbate non-technical losses.

2.2 - Smart Power Theft Detection System

(Year: 2019 | Conference Paper | Publisher: IEEE)

Power theft is normally done by two methods that is bypassing or hooking. So to detect it, a system (current measuring and comparing) 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 current is measured periodically in the distributor box and is posted to the server database for each house using GSM/GPRS module. Similarly, for each house electric meter is designed which can measure the value of the current and post the same to the server database periodically using GSM/GPRS module. At the time of the installation of the electric meter the details of the users are stored in the database through a user friendly mobile application including the address, latitude, longitude using mobile GPS and the photograph of the user's house/area. Upon successful comparison between the current values from distributor box and electric meter in the server if we get a marginal difference between the currents then the theft is detected. Finally, the details of the user are shared with the authorized mobile application including the address and photograph of the area. The latitude and longitude are also used to show the area of theft in Google maps. And hence the required steps are taken. The same process is used for hooking but on the individual electric poles.[2]

CHAPTER 3 – METHODOLOGY

This project mainly aims at detecting electricity theft directly from the transmission lines and meters being tampered by altering the wheel or using any shunt elements.

3.1 HARDWARE COMPONENTS

Sl. No	Component	Specifications
1	ESP32 Wroom DA Module	WiFi Modules (802.11) SMD Module, ESP32-D0WDQ6, 32Mbits SPI flash, UART Mode. Powerful, Generic Wi-Fi and BT and BLE MCU Module. SMD MODULE, ESP32-D0WDQ6, 32MBIT.
2	ACS712 5A Current sensor	5V, Up to 5A Current sensor, sensitivity = 185mV/A
3	230/12 V Step down transformer	220/12V, 100mA
4	16x2 LCD	16x2, I2C
5	I2C Communication module	
6	Incandescent bulbs	220V, 40W

3.2 SOFTWARE COMPONENTS

Sl. No	Component
1	Google Firebase Realtime database
2	ThingSpeak IOT platform
3	Arduino IDE
4	Kodular

3.2 HARDWARE DESCRIPTION

1. ESP32 Wroom 32 The ESP32 is a powerful microcontroller developed by Espressif Systems, featuring a dual-core Tensilica LX6 CPU with clock speeds up to 240 MHz. It integrates Wi-Fi (802.11 b/g/n) and Bluetooth 4.2 (classic and BLE) connectivity, making it ideal for IoT applications. With 520 KB SRAM, it supports a wide range of peripherals including GPIO, ADC, DAC, UART, SPI, I2C, and I2S. The ESP32 also includes hardware encryption support (AES, SHA-2, RSA), an integrated Hall sensor, and capacitive touch sensors. Its low-power modes and deep sleep capabilities enable energy-efficient designs. The chip operates at a voltage range of 2.2 to 3.6V, with a typical operating current of around 80mA.

Fig 3.1 ESP32 Wroom 32 Dev Board

2. ACS712 5A Current sensor The ACS712 5A current sensor is a precise Hall-effect-based linear sensor developed by Allegro MicroSystems. It can measure both AC and DC currents up to ±5A, with an output sensitivity of 185 mV/A. The sensor operates on a supply voltage of 5V and provides an analog voltage output that is directly proportional to the sensed current. It features a nearly zero magnetic hysteresis and a bandwidth of 80 kHz, making it suitable for high-frequency applications. The ACS712 includes internal electrostatic discharge (ESD) protection and is housed in a compact SOIC8 package, making it ideal for integration into various electronic projects and current monitoring systems.

Fig 3.2 ACS712 5A current sensor

3. 12 – 0 – 12 Step down Transformer A 12-0-12 volt step-down transformer is an electrical device used to convert high voltage AC mains (typically 220V or 120V) to a lower voltage of 12V AC with a center tap. The primary winding is connected to the mains supply, while the secondary winding provides two 12V outputs with a central ground (0V), facilitating dual voltage output or full-wave rectification. These transformers typically have an iron core to maximize magnetic flux and efficiency. They are commonly used in power supplies, audio amplifiers, and other electronic circuits requiring stable, lower voltage AC power. The transformer's power rating is crucial, usually specified in VA (volt-amps), dictating the maximum load it can handle.

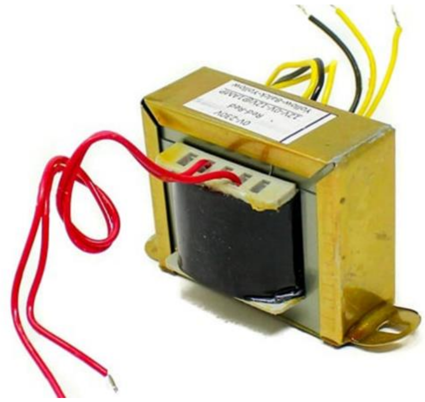


Fig 3.3 220/12 Step down transformer

4. 16x2 LCD Display A 16x2 LCD is a compact alphanumeric display module that can show 32 characters arranged in two lines of 16 characters each. It typically uses the Hitachi HD44780 controller or its equivalent, which interfaces with microcontrollers via a parallel or I2C interface. The display operates on a 5V supply and features an adjustable backlight and contrast control. Each character is composed of a 5x8 pixel matrix, allowing for clear text representation. Commonly used in embedded systems, this LCD supports custom character creation, making it versatile for various applications like digital meters, clocks, and user interfaces. The module includes 16 pins for easy connection and integration into electronic projects.

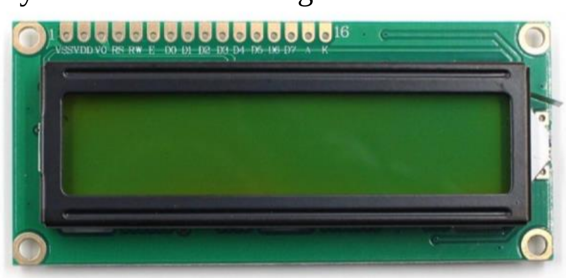


Fig 3.4 16x2 LCD

5. I2C Communication module An I2C module is an essential component for enabling communication between microcontrollers and various peripherals over the I2C (Inter-Integrated Circuit) bus, which uses two bidirectional lines: SDA (Serial Data) and SCL (Serial Clock). Operating at standard data transfer rates of 100 kbps (Standard Mode), 400 kbps (Fast Mode), and up to 3.4 Mbps (High-Speed Mode), it ensures efficient communication. The module supports multiple devices on the same bus, addressing up to 128 unique slave devices with 7-bit or 10-bit addresses. Voltage levels are typically 3.3V or 5V, ensuring compatibility with most microcontrollers and peripherals. The I2C module also includes pull-up resistors to maintain line stability and data integrity. Applications range from connecting sensors and real-time clocks to displays and memory devices, making it indispensable for embedded systems and IoT projects. Additionally, it supports multi-master configurations, where multiple controllers can manage the bus, and clock stretching, where slower devices can hold the clock line low to manage data flow.

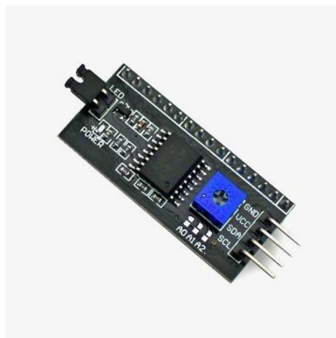


Fig 3.4 I2C Module

6. Incandescent bulbs Incandescent bulbs produce light by heating a tungsten filament until it glows. They operate on standard AC or DC voltage and emit a warm, continuous spectrum of light. They are inexpensive and widely used, they have been used as loads in this project.

Fig 3.5 40W Incandescent Lamp

SOFTWARE DESCRIPTION

1. Google Firebase realtime database Google Firebase's Realtime Database is a cloud-hosted NoSQL database that enables real-time data synchronization across clients. Structured as a JSON tree, it allows developers to store and retrieve data effortlessly. Changes to the data are instantly reflected across all connected clients, making it ideal for collaborative applications, chat apps, and live data feeds. The Realtime Database offers robust offline capabilities, automatically syncing data once the connection is restored. It supports security through Firebase Authentication and database rules, ensuring data access control. Additionally, it provides automatic scaling, handling large numbers of concurrent users efficiently. Integration with Firebase's ecosystem, including Analytics, Cloud Functions, and Storage, enhances its versatility for building comprehensive, real-time applications.

2. ThingSpeak ThingSpeak is an IoT analytics platform and API service that allows users to collect, visualize, and analyze live data streams from various IoT devices. It supports real-time data collection via HTTP, MQTT, or directly from supported hardware such as Arduino and Raspberry Pi. Users can store and retrieve data in channels, visualize it with integrated MATLAB analytics, and perform actions based on the data using triggers. ThingSpeak provides features like data aggregation, processing, and cloud storage, making it suitable for applications in smart agriculture, environmental monitoring, and industrial automation. Its open-source nature and integration with MATLAB enable advanced data analysis and predictive modeling, enhancing the capabilities of IoT solutions.

3. Arduino IDE

The Arduino project gives the Arduino incorporated development surroundings (IDE), that's throughout-platform utility written inside the programming language Java. It originated as a hierarchy of operation menus. It consists of a code editor with capabilities which includes text reducing and pasting, looking and changing textual content, automated indenting, brace matching, and syntax highlighting, and provides easy one-click on mechanisms to collect and add programs to an Arduino board. It also carries a message location, a text console, a toolbar with buttons for not unusual functions. An application written with the IDE for Arduino is called a ketch. Sketches are stored on the development pc as textual content documents with the record extension into. Arduino software program (IDE) pre-1.0 saved sketches with the extension. The Arduino IDE helps the languages C and C++the use of unique regulations of code structuring. user-written code most effectively requires simple functions.

4. Kodular

Kodular is a user-friendly, visual programming platform designed to simplify the creation of Android applications for users with varying levels of coding expertise. It offers a drag-and-drop interface where developers can design app layouts and implement functionality by assembling blocks of code rather than writing text-based code. The platform provides a wide range of components and tools, including buttons, text fields, databases, web services, sensors, and multimedia elements, allowing users to build complex applications quickly and efficiently. Kodular’s intuitive environment supports real-time app testing and debugging, streamlining the development process from concept to deployment. It features a comprehensive set of pre-built components for integrating functionalities like user authentication, in-app purchases, and push notifications. Kodular is particularly popular in educational settings for teaching programming concepts, as well as among hobbyists and entrepreneurs for rapid app prototyping and development. By lowering the barrier to entry for app development, Kodular enables users of all skill levels to create and publish their own Android applications on the Google Play Store or other platforms.

3.3 CIRCUIT DESCRIPTION

3.3.1 Simulation Circuit Diagram

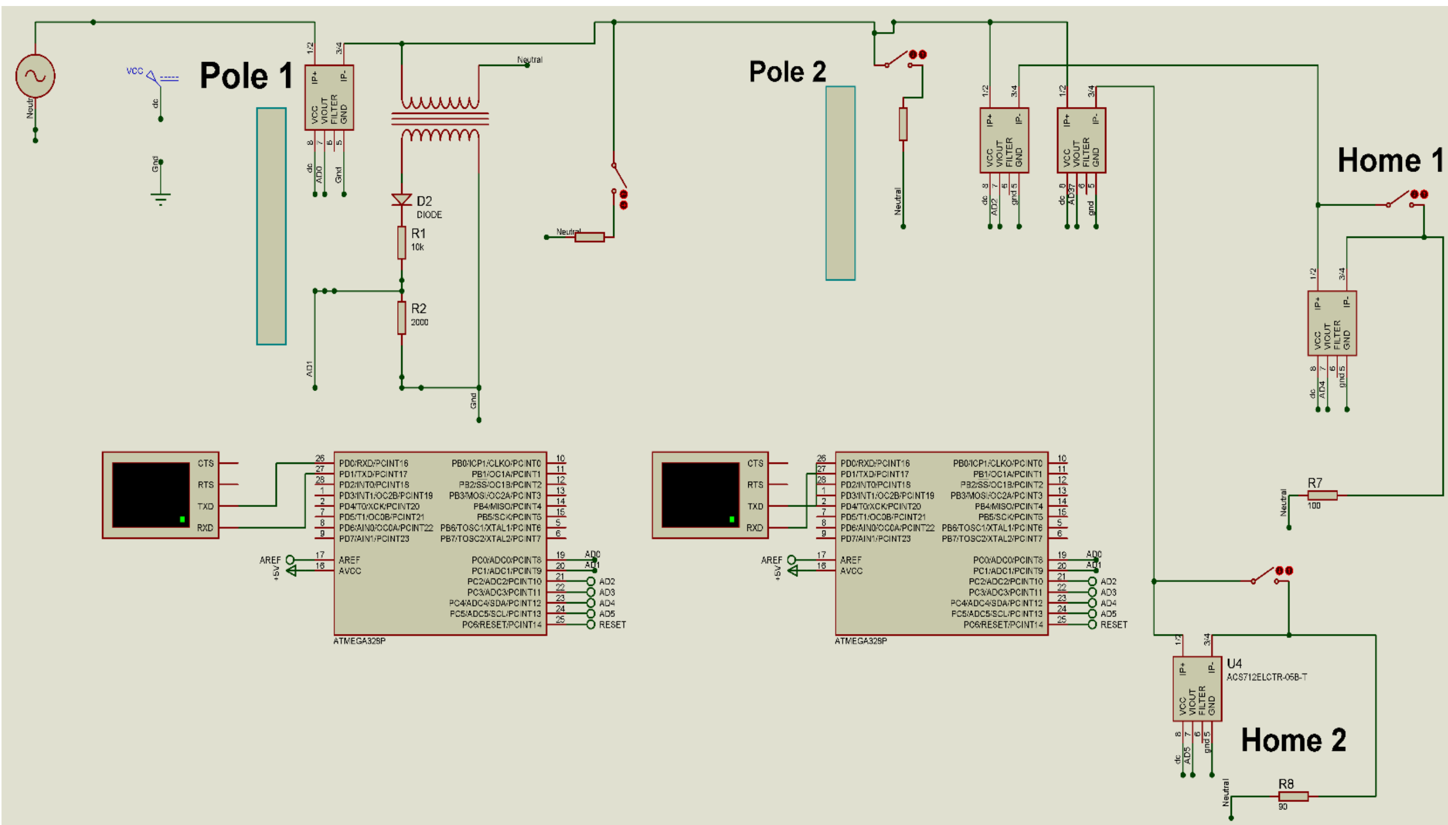


Fig 3.6 Circuit Diagram for 2 pole 2 home system

The mains supply coming in at the first electricity pole is passed through a current sensor and the values are recorded. This is then multiplied with the measured voltage to find the power. One the next pole the current is measured again, if there are is a major difference between the power measured at both the terminals then there must be an illegal connection hooked up to the line.

From the second pole there two domestic loads named “home 1” and “home 2” connected, these loads can have their meters tampered, to detect the same we have added two meters each first measure the power being sent to the homes. At the respective homes there are smart meters installed which will read the power draw and send it to the backend database where the power from the pole meters and the home meters are compared and when there is a major difference there is meter tampering.

3.3.2 Voltage divider circuit

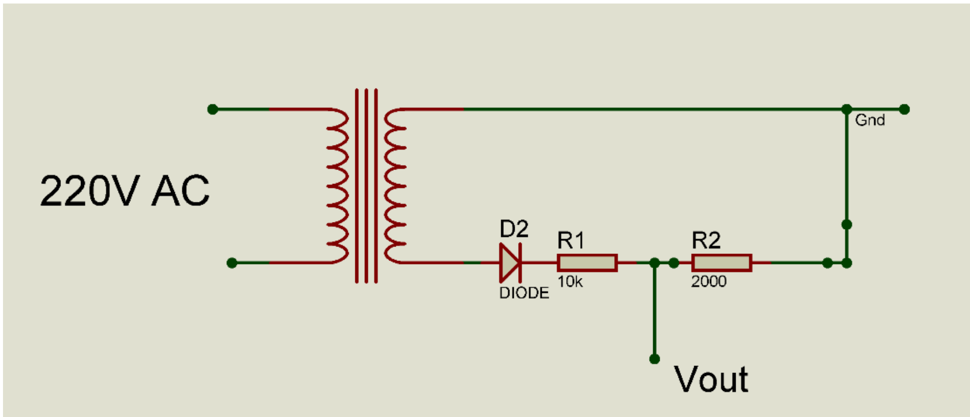


Fig 3.7 Voltage divider circuit

The voltage divider circuit is designed to step down and convert the 220V AC supply from the mains to a lower level which can be read by a microcontroller, an esp32 in this case.

The circuit consists of a resistive divider having 2 resistances of 10k and 2.2k along with a diode allowing only the positive halves to flow through.

Max allowed ADC voltage of esp32 = 3.3V

Transformer steps it down to 12V (RMS), which means the peaks are at 17V. This 17V must be reduced further to less than 3.3 V to do this the resistive divider is used.

$$\text{Vout} = 12 * \frac{2.2k}{10k+2.2K}\text{V}$$

This gives us a peak of about 2.1V which can be read by the esp32.

The 12Bit ADC On the esp32 will read the value and produce a digital output of about 2600, which is mapped as 2.1Volts in code.

Code for voltage reading:

```
 for(int i = 0;i<400;i++){        //sampling for a few cycles of input
   val = analogRead(32);
   if(val>0){
     if(val>m){
       m = val;                   //Finding peak value
     }
   }
```

```
  }
  m = m/3.3 * 4095;
  float voltage = map(m,0,3.3,0,230);
```

3.3.3 Calibrating the Current sensor:

The sensor produces a voltage proportion to the current flowing through it, 0A produces 2.5 volts and anything above or below 0A is mapped as 185mV/A.

The ADC channel on the esp32 is 12bit, with a maximum of 3.3V,

$$\mathrm{V} = \frac{Vin}{4095} * 3.3$$

The current I can be obtained by dividing the voltage by the minimum step value of the adc.

$$\mathrm{I} = \frac{V - 2.5}{185}\mathrm{A}$$

Code for current reading:

```
  m = 0;
  for(int i = 0;i<400;i++){    //sampling for a few cycles
    val = analogRead(32);
    if(val>0){
      if(val>m){
        m = val; //Finding peak value
      }
    }
  }
  m = m/4095 * 3.3;
  m = m - 2.5;
  float current = m/185;
```

3.3.4 Power Calculations

The average power of a circuit can be given as the product of The rms Voltage, rms current and the power factor of the load. In this project for simplicity we have assumed the power factor to be unity which is the case for most domestic loads.

Code for calculating power:

```
  power[0] = voltage*currents[0];
```

```
  power[1] = voltage*currents[1];
  unit[0] = unit[0] + power[0]/3600000;
  unit[1] = unit[1] + power[1]/3600000;
```

This piece of the code is updating the power values from two different sensors stored in an array.

3.3.5 Updating the LCDs

The LCDs are used to show the power flowing at the individual homes and the total units being consumed at the homes. The I2C module drives the LCD by receiving data from an ESP32 microcontroller over the I2C communication protocol. The ESP32 sends commands and data to the LCD using only two wires: SDA (Serial Data) and SCL (Serial Clock), significantly reducing the number of pins needed compared to parallel communication and conserving valuable GPIO pins. The ESP32 initializes the I2C communication by specifying the LCD's I2C address and setting the data rate. Commands, such as clearing the display or setting the cursor position, and data bytes representing characters are sent in standard I2C packets. The I2C module receives these packets, interprets the commands, and processes the data to update the display. It converts the serial I2C data into parallel signals that the LCD can understand, ensuring proper timing and control. This efficient communication method allows the ESP32 to handle multiple peripherals on the same I2C bus, facilitating real-time display updates with minimal wiring complexity.

Code for driving lcd

```
#include <Wire.h>
#include <LiquidCrystal_I2C.h>
LiquidCrystal_I2C lcd(0x27, 16, 2);
void setup() {
  // Initialize the LCD
  lcd.init();
  // Turn on the backlight
  lcd.backlight();
}
Void loop(){
  String one = String(voltage) + " V" + String(currents[0]) + "A";
  String two = String(power[1]) + " W" + String(unit[1]) + " KWHr";
  lcd.clear();
  lcd.setCursor(0,0);
  lcd.print(one);
```

```
  lcd.setCursor(0,1);
  lcd.print(two);
}
```

This code is updating the lcd with the voltage, current, and power values.

3.3.6 The Backend database using google firebase

We have used Google's firebase Realtime database to store all the values being read by all the sensors and make it available to any apps requiring it, providing they have access. Its safe and secured with the admin having the option to give or take data access from clients. The data is stored in json format using three different keys named "voltages", "power" and "units".


```
{
  "power": {
    "home1": 32.69842,
    "home2": 4.19211,
    "pole1": 20,
    "pole2": 1.04803,
    "pole21": -7.75539,
    "pole22": 8.80342
  },
  "units": {
    "home1": 0,
    "home2": 0,
    "pole1": 0,
    "pole2": 0,
    "pole21": 0,
    "pole22": 0
  },
  "voltage": {
    "voltage1": 225,
    "voltage2": 225
  }
}
```


This is the json from a particular instance, the values are updated every 5 seconds.

Code to initialize and update firebase:

```
#include <WiFi.h>
#include <FirebaseESP32.h>
#define WIFI_SSID "your_SSID"
#define WIFI_PASSWORD "your_PASSWORD"
#define FIREBASE_HOST "your-project-id.firebaseio.com"
```

```
#define FIREBASE_AUTH  "your-database-secret"
FirebaseData firebaseData;
void setup() {
  Serial.begin(115200);
  WiFi.begin(WIFI_SSID, WIFI_PASSWORD);
  while (WiFi.status() != WL_CONNECTED) {
    delay(1000);
    Serial.println("Connecting to WiFi...");
  }
  Firebase.begin(FIREBASE_HOST, FIREBASE_AUTH);
  Firebase.reconnectWiFi(true);

  if (Firebase.setInt(firebaseData, "/test/int", 123)) {
    Serial.println("Data sent successfully");
  } else {
    Serial.println("Failed to send data");
    Serial.println(firebaseData.errorReason());
  }
}
```

3.3.7 ThingSpeak IOT for graphical view.

We have used ThingSpeak as the second database primarily to keep a track of the power draw and show it in a graphical way. ThingSpeak graphs are set to public view making it viewable from the app by embedding links to the respective graphs.

Code to update ThingSpeak:

```
#include <WiFi.h>
#include <HTTPClient.h>
#define WIFI_SSID "your_SSID"
#define WIFI_PASSWORD "your_PASSWORD"
#define THINGSPEAK_API_KEY  "your_API_KEY"
#define THINGSPEAK_SERVER  "http://api.thingspeak.com"
void setup() {
  Serial.begin(115200);
  WiFi.begin(WIFI_SSID, WIFI_PASSWORD);
  while (WiFi.status() != WL_CONNECTED) {
    delay(1000);
    Serial.println("Connecting to WiFi...");
```

```
  }
  Serial.println("Connected to WiFi");
}
void loop() {
  if (WiFi.status() == WL_CONNECTED) {
    HTTPClient http;
    String url = THINGSPEAK_SERVER + "/update?api_key=" + THINGSPEAK_API_KEY + "&field1=25.5";
    http.begin(url);
    int httpCode = http.GET();
    if (httpCode > 0) {
      Serial.println("Data sent successfully");
    } else {
      Serial.println("Error sending data");
    }
    http.end();
  }
  delay(20000); // Upload interval (e.g., 20 seconds)
}
```

3.3.8 App to monitor everything

The app is made to monitor the power flow through the line, it uses the Kodular framework and firebase to be connected with the microcontrollers.

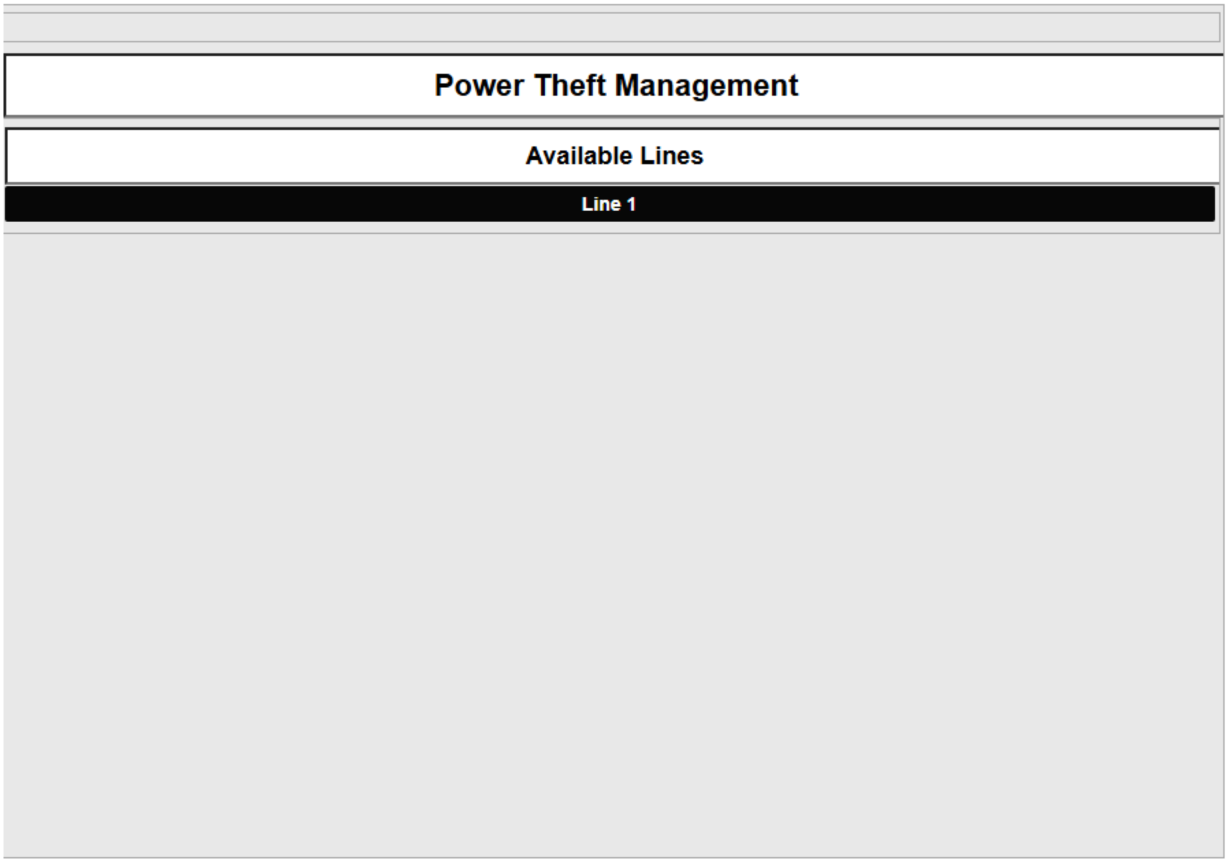


Fig 3.8 App starting screen

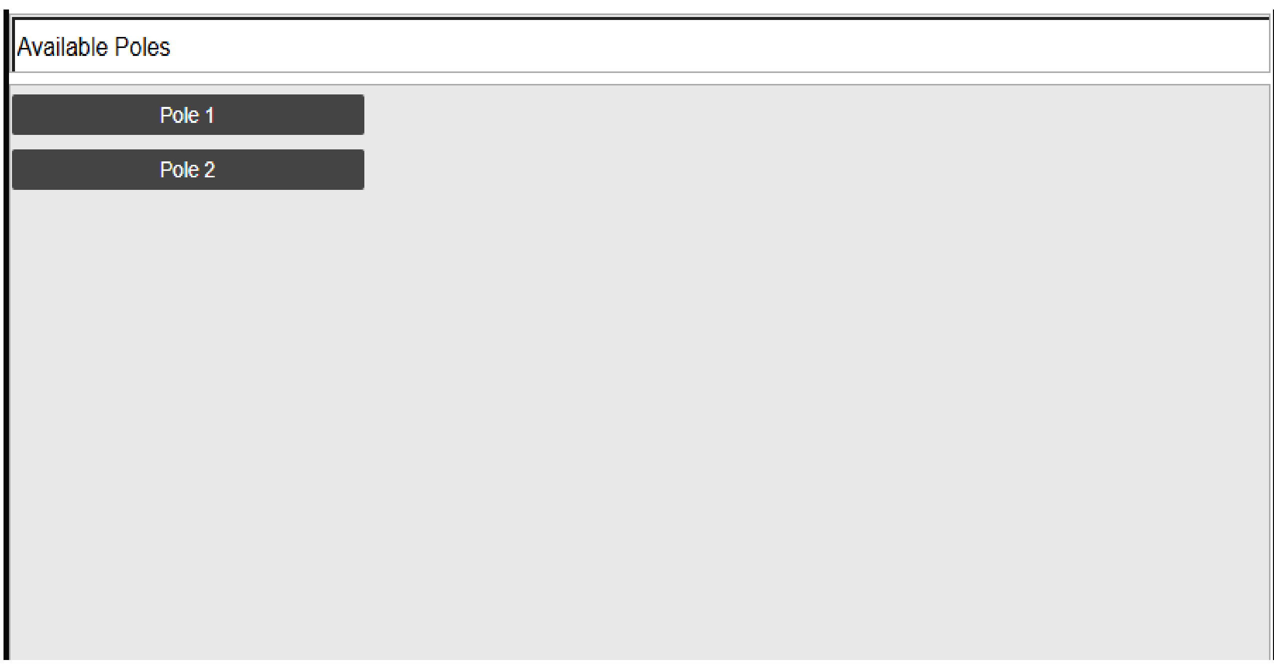


Fig 3.9 App Distribution Line selection screen

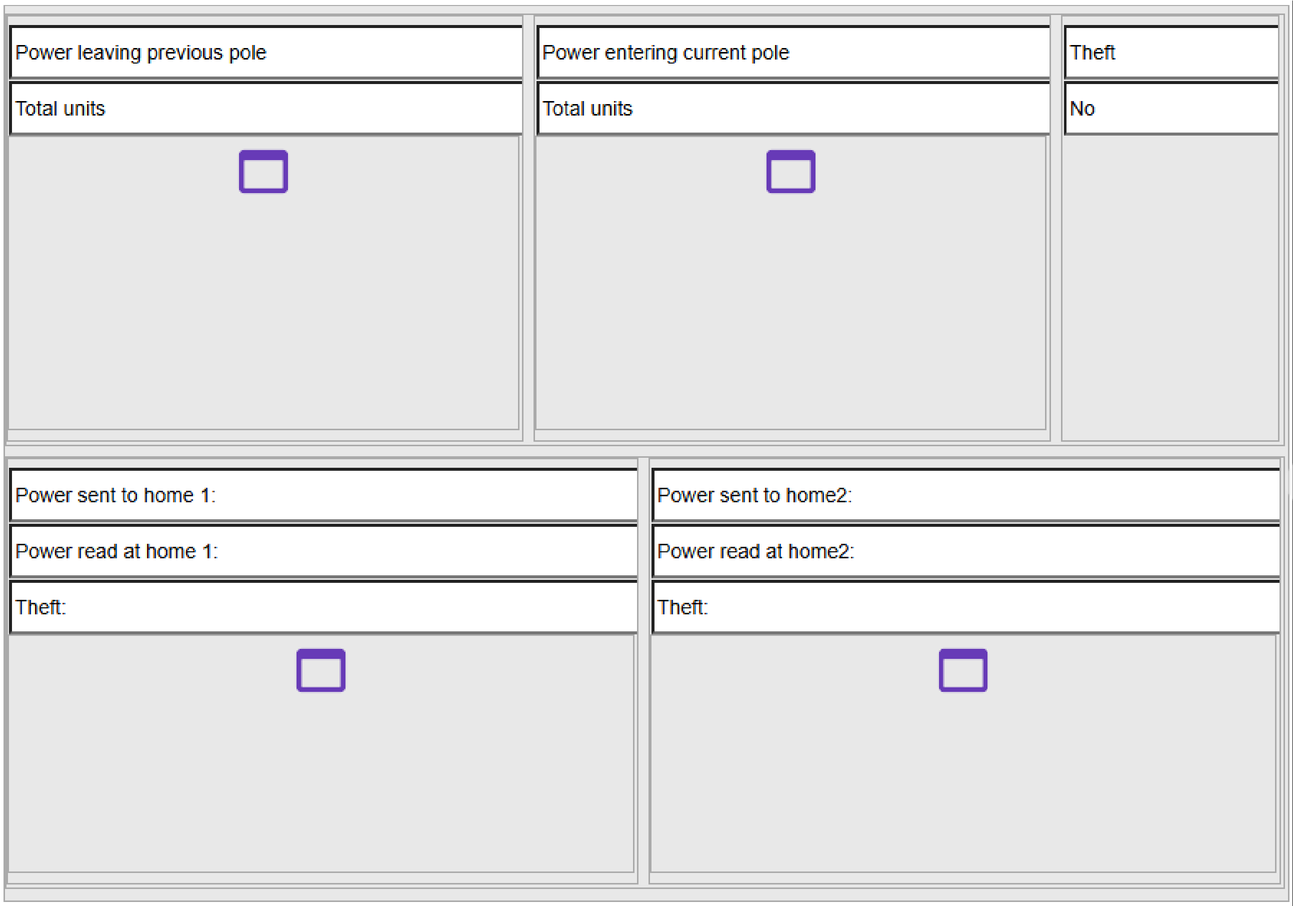


Fig 3.10 Power flow and theft monitoring screen

CHAPTER 4 – RESULTS

4.1 HARDWARE CIRCUIT

It is seen in fig 4.1 the complete built distribution system with 2 poles, 2 homes each having their own smart meters which will be communicating with the firebase backend. The incoming power goes through pole 1 where it is measured. An illegal connection is made between pole 1 and 2 which can be switched on and off with a switch. The power received by pole 2 is measured again and if there is a measured difference between pole 1 and 2 then a power theft is detected.

Next the power goes from pole 2 to homes 1 and 2, these are domestic loads each having their own meters which can be tampered by connecting a shunt across the meter current terminals, by the flick of a switch.

If the power being read at pole 2 is not the same as the pole being read by either of the homes that means power theft is occurring and message is shown.

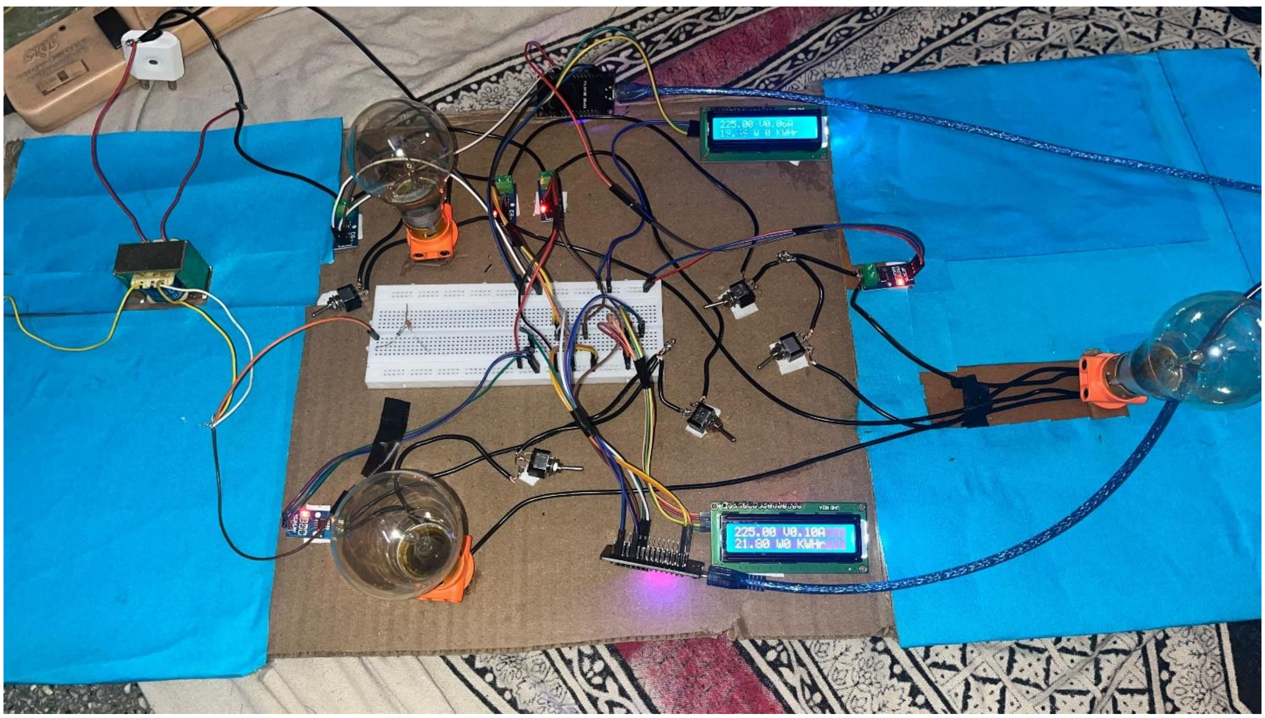


Fig 4.1 Hardware circuit

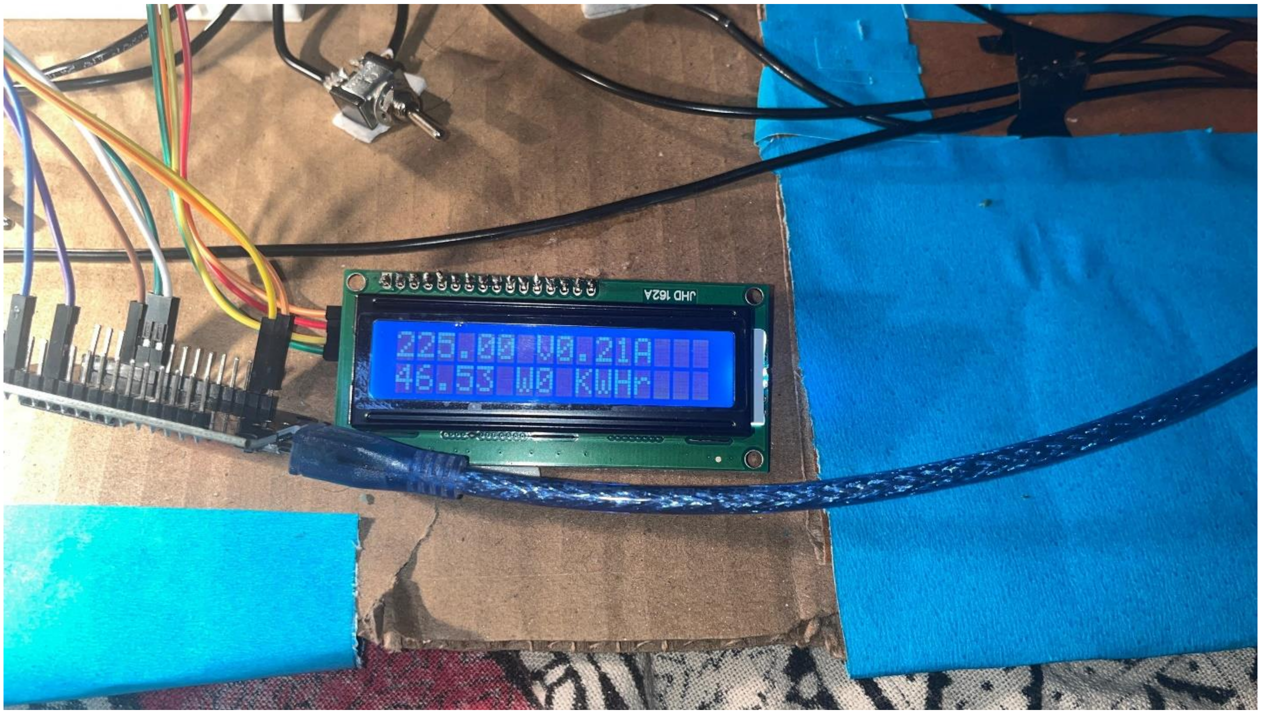
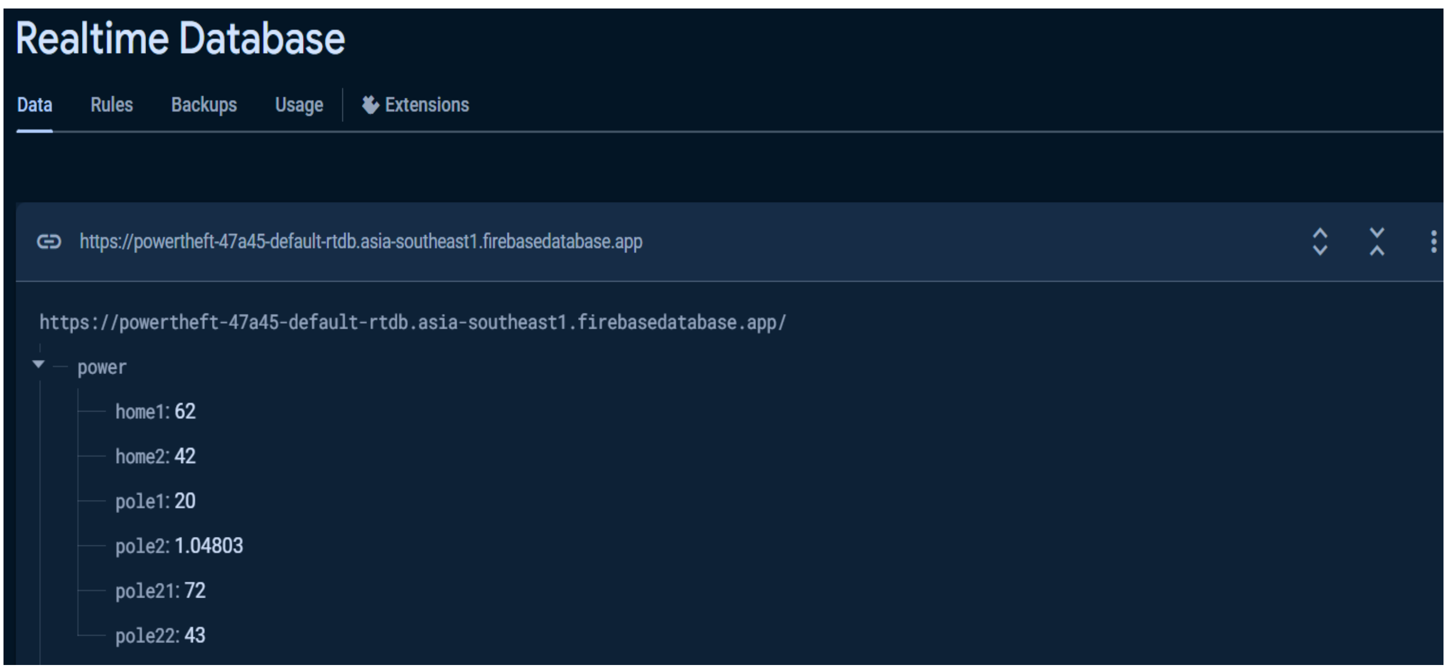


Fig 4.2 Smart meter reading power

4.2 FIREBASE INTERFACE



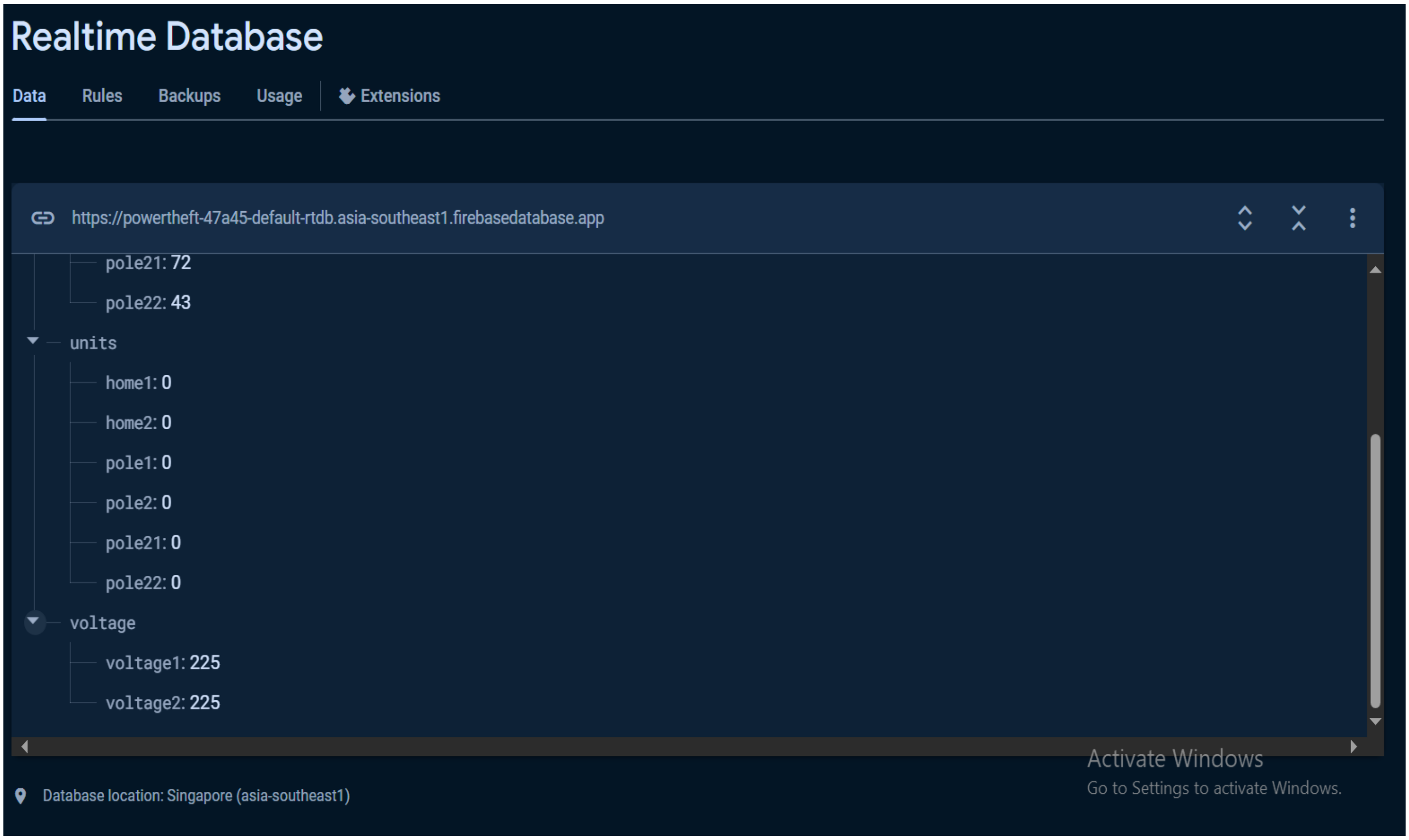


Fig 4.4 Firebase output

4.3 THINGSPEAK OUTPUT

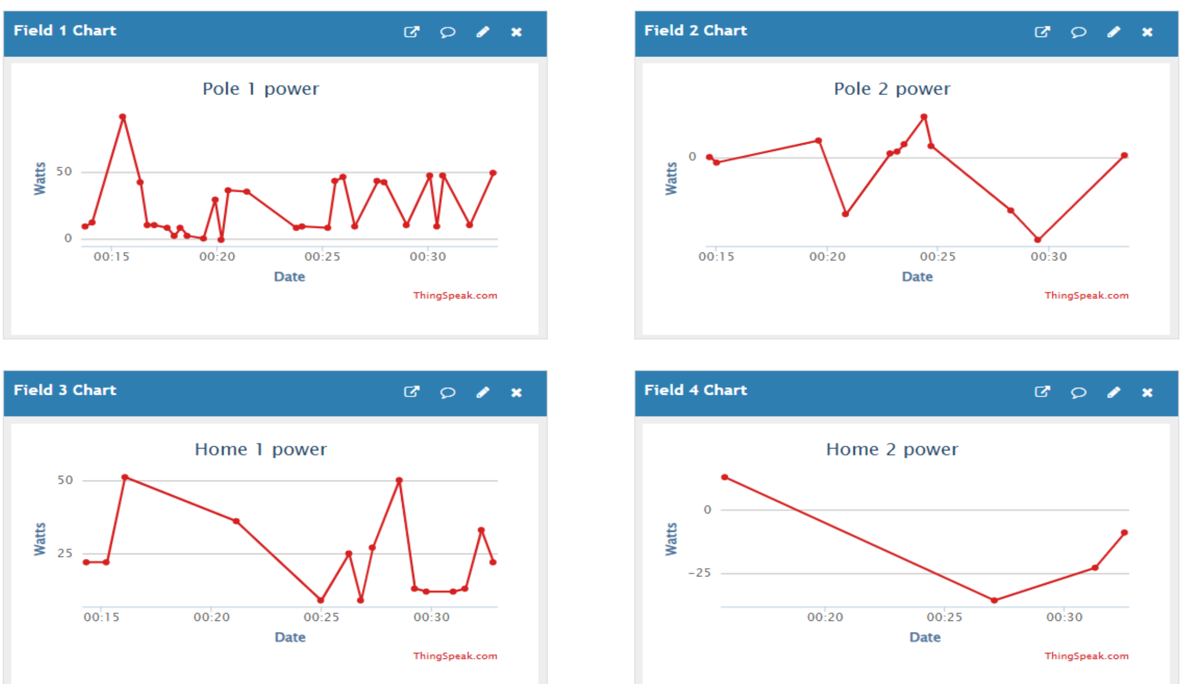
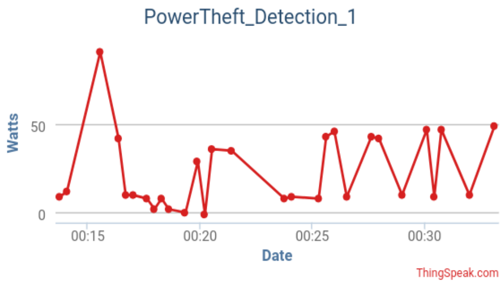


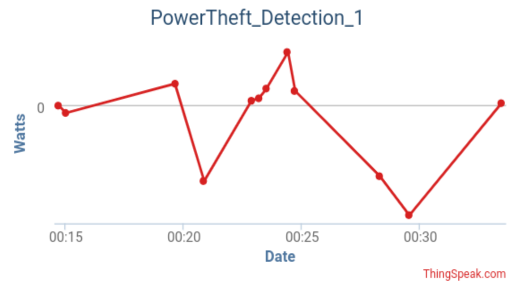
Fig 4.5 ThingSpeak graph view

4.4 MONITORING APP OUTPUT

Power leaving previous pole (Watts) : 20 | Power entering pole (Watts) : 1.04803 | Theft

Total units | Total units | NO

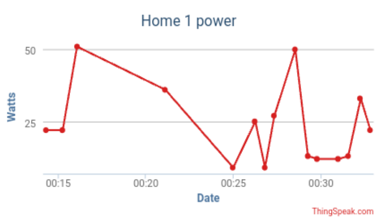




Power sent to home 1 (Watts) : 72 | Power sent to home 2 (Watts) : 43

Power read at home 1 (Watts) : 62 | Power read at home 2 (Watts) : 42

Theft: NO | Theft: NO



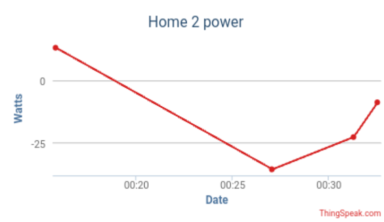
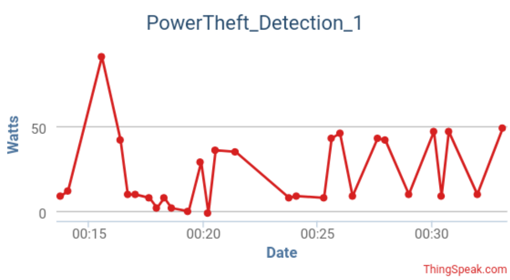
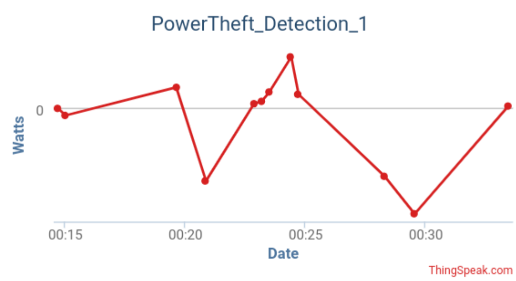


Fig 4.6 Monitoring app with no thefts occurring

Power leaving previous pole (Watts) : 20 | Power entering pole (Watts) : 1.04803 | Theft

Total units | Total units | NO

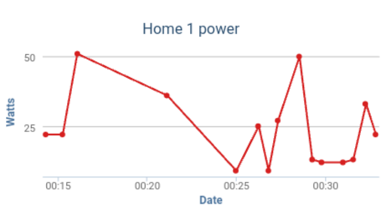




Power sent to home 1 (Watts) : 85 | Power sent to home 2 (Watts) : 43

Power read at home 1 (Watts) : 60 | Power read at home 2 (Watts) : 42

Theft: YES | Theft: NO



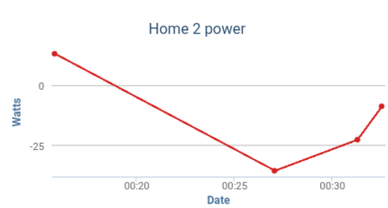


Fig 3.7 Monitoring app with meter tampering at home 1

Figure 3.7 shows that when a theft is detected at home 1, the app automatically shows the same. The power which was sent from the pole 1 was 85Watts and the power being measured at home 1 was 60Watts, therefore there was some kind of meter tampering going on at the meter at home1, this information is recorded and displayed at the user interface and the respective authority will be alerted.

CHATPER 5 – CONCLUSION

Most power utilities worldwide suffer severe revenue losses due to the issue of power theft, mainly meter tampering and illegal connections. The proposed real-time power theft monitoring and detection system with a double metering system showed good simulation results to identify if there is meter tampering and illegal connections in the power system network [1]. At the same time, the hardware project showed how the smart electric meters of the proposed double metering system can be practically implemented in the distribution system network. The hardware project also showed how the proposed system can practically monitor and detect any illegal electricity connections on the distribution feeders and meter tampering when a consumer manipulates its smart electric meter. It further showed how the received power consumption data is displayed when read from the cloud storage using a computer or a smartphone. Therefore, it is expected that the proposed system will play a significant role in countries such as India in detecting or alleviating power theft. Including revenue recovery by the municipalities of the different cities or the power utility the benefits of implementing the proposed system are reducing asset loss and improving revenue, increasing the visibility of the power network, reducing line losses (mainly Non-Technical Losses).

CHAPTER 6 – REFERENCES

1. Electricity Theft In India: An Analysis Authored by- Pritee R. Deotale

2. Real-time power theft monitoring and detection system with double connected data capture system Celimpilo Lindani Zulu

3. Deepa S, Haritha D, Kabilan P, KarthickRaja G, Karthikeswari V (2018) Power theft identification system using IoT. Int J Pure Appl Math – IJPAM

4. Yao D, Wen M, Liang X, Fu Z, Zhang K, Yang B (2019) Energy theft detection with energy privacy preservation in the smart grid. IEEE Int Things

5. Pawade A, Shaikh N, Chowdhri B, Shariq A (2015) Power theft detection using wireless system: a distributed approach for power theft prevention. Int J Student Res Technol Manag - IJSRTM