

REDUCTION OF ELECTRICITY THIEF USING IOT

Submitted in partial fulfillment of the requirements for the award of

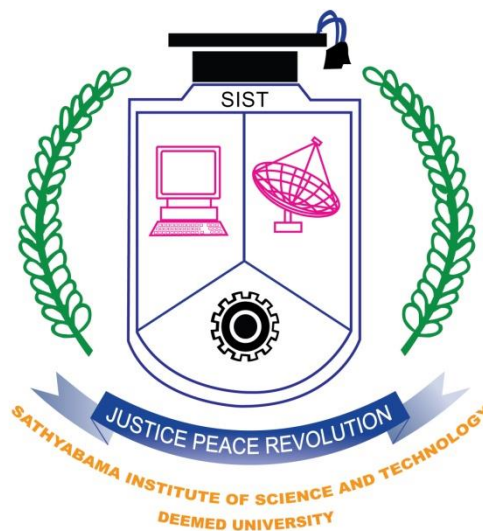
Bachelor of Engineering Degree in

Electrical and Electronics Engineering

by

NIKESH KUMAR S (Register No. 39140034)

JEEVANANTHAM D S (Register No. 39140019)



**DEPARTMENT OF ELECTRICAL AND ELECTRONICS ENGINEERING
SCHOOL OF ELECTRICAL AND ELECTRONICS**

SATHYABAMA

**INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)**

Accredited with Grade "A" by NAAC

JEPPIAAR NAGAR, RAJIV GANDHI SALAI, CHENNAI - 600 119

APRIL 2023



SATHYABAMA

INSTITUTE OF SCIENCE AND TECHNOLOGY

(DEEMED TO BE UNIVERSITY)

Accredited "A" Grade by NAAC | 12B Status by UGC | Approved by AICTE

www.sathyabama.ac.in

DEPARTMENT OF ELECTRICAL AND ELECTRONICS ENGINEERING

BONAFIDE CERTIFICATE

This is to certify that this Project Report is the bonafide work of **NIKESH KUMAR S** (Reg. No. 39140034) and **JEEVANANTHAM D S** (Reg. No. 39140019) who carried out the project entitled "**REDUCTION OF ELECTRICITY THIEF USING IOT**" under our supervision from November 2022 to April 2023.

Dr. S. JAYAPRAKASH
Internal Guide

Dr. V. SIVACHIDAMBARANATHAN
Head of the Department

Submitted for Viva voce Examination held on_____

Name:

Signature:

Internal Examiner

External Examiner

DECLARATION

We **NIKESH KUMAR S** (Reg. No. 39140034) and **JEEVANANTHAM D S** (Reg. No. 39140019) hereby declare that the Project Report entitled “**REDUCTION OF ELECTRICITY THIEF USING IOT**” done by us under the guidance of **Dr. S. JAYAPRAKASH** is submitted in partial fulfillment of the requirements for the award of Bachelor of Engineering degree in Electrical and Electronics Engineering.

1.

2.

DATE:

PLACE:

SIGNATURE OF THE CANDIDATES

ACKNOWLEDGEMENT

We are pleased to acknowledge our sincere thanks to Board of Management of **SATHYABAMA** for their kind encouragement in doing this project and for completing it successfully. We are grateful to them.

We convey our thanks to **Dr. N. M. Nandhita, Dean, School of Electrical and Electronics Engineering** and **Dr. V. Sivachidambaranathan, Head of the Department, Dept. of Electrical and Electronics Engineering** for providing us necessary support and details at the right time during the progressive reviews.

We would like to express our sincere and deep sense of gratitude to our Project Guide **Dr. S. JAYAPRAKASH** for his valuable guidance, suggestions and constant encouragement paved way for the successful completion of our project work.

We wish to express our thanks to all Teaching and Non-teaching staff members of the Department of Electrical and Electronics Engineering who were helpful in many ways for the completion of the project.

ABSTRACT

In this project Arduino based power theft detection and protection system is designed. An increase in the demand of electric power for household, commercial and industrial loads lead to management of electric distribution system become more complicated. Lack of information at the bases station regarding status of the distribution network has been identified as the major bottleneck to its effective monitoring and controlling. Electrical power theft detection and protection system is used to detect and protect an unauthorized tapping on distribution line. In this project ACS712 series current sensor has been used as the interfacing instrument between the power line current and Arduino. To isolate power line from power theft system relay used as switching gear. Arduino control all operations that all devices do. This system would provide a simple way to detect and prevent an electrical power theft without any human interference, maximize the profit margin of power utility company and Prevent fault due to overload. The theft detection of electricity also became possible by using this system through which server received the message when users by passed the meter. This system provides billing activity in addition to detection and protection power theft.

TABLE OF CONTENTS

CHAPTER NO.	TITLE	PAGE NO.
	ABSTRACT	v
	LIST OF FIGURES	ix
	LIST OF TABLES	xi
	LIST OF SYMBOLS AND ABBREVIATIONS	xii
1	INTRODUCTION	
	1.1 GENERAL	1
	1.2 MOTIVATION FOR THE SELECTION OF PROBLEM	2
	1.3 OVERVIEW	2
2	LITERATURE SURVEY	
	2.1 MAJOR FINDINGS FROM LITERATURE SURVEY	4
	2.2 EXISTING BLOCK DIAGRAM	8
	2.3 OPEN PROBLEMS IN EXISTING SYSTEM	8
	2.4 DISADVANTAGES	8
	2.5 IEEE STANDARDS FOLLOWED	9
	2.6 CONSTRAINTS	10

2.7	TRADEOFF	10
2.8	PREREQUISITES	11
3	AIM AND SCOPE OF THE PRESENT INVESTIGATION	
3.1	AIM OF THE PROJECT	13
3.2	SCOPE OF THE PROJECT	13
3.3	OBJECTIVES	14
3.4	ADVANTAGES	14
4	HARDWARE AND PROJECT DESCRIPTION	
4.1	HARDWARE CIRCUIT DIAGRAM	16
4.2	EXPLANATION	16
4.3	HARDWARE COMPONENTS	17
4.3.1	Arduino UNO	18
4.3.2	Power supply circuit	25
4.3.3	Voltage sensor	26
4.3.4	Current sensor	27
4.3.5	Battery	28
4.3.6	LCD	30
4.3.7	Buzzer	35
4.3.8	Relay	36
4.3.9	NodeMCU	38
4.4	SOFTWARE REQUIRED	40

	4.4.1	Arduino IDE	40
	4.4.2	Embedded C	42
	4.4.3	Thingspeak	43
	4.5	BLOCK DIAGRAM	45
	4.6	PROPOSED SYSTEM EXPLANATION	46
	4.7	WORKING MODULES	46
	4.8	ADVANTAGES	47
	4.9	APPLICATIONS	48
5		RESULTS AND DISCUSSIONS	
	5.1	HARDWARE OUTPUT	49
	5.2	SIMULATION OUTPUT	50
	5.3	IOT DATA	50
6		SUMMARY AND CONCLUSIONS	
	6.1	SUMMARY	52
	6.2	FUTURE SCOPE	52
	6.3	CONCLUSION	53
		REFERENCES	55

LIST OF FIGURES

FIGURE NO.	TITLE	PAGE NO.
2.1	Existing system block Diagram	8
4.1	Circuit diagram	16
4.2	Arduino UNO	19
4.3	Arduino UNO pinout	21
4.4	Pin Diagram	25
4.5	Power Supply Circuit	25
4.6	Voltage Sensor	26
4.7	Current Sensor	27
4.8	Battery	29
4.9	2x16 Line Alphanumeric LCD display	30
4.10	Basic LCD screen	31
4.11	LCD Screen	32
4.12	LCD Background	32
4.13	Character LCD pins with 1 Controller	33
4.14	Character LCD pins with 2 Controller	34
4.15	Buzzer	35
4.16	Relay	37
4.17	Node MCU	38
4.18	Block Diagram	45
4.19	Methodology	47
5.1	Hardware Output	49

5.2	Simulation Output	50
5.3	Photocopy of current graph using IOT	51
5.4	Photocopy of voltage graph using IOT	51
5.5	Photocopy of power graph using IOT	51

LIST OF TABLES

TABLE NO.	TITLE	PAGE NO.
4.1	Arduino UNO specifications	20
4.2	Buzzer Pin Configuration	36

LIST OF SYMBOLS AND ABBREVIATIONS

IoT	- Internet of Things
AMI	- Advanced Metering Infrastructure
SCADA	- Supervisory Control and Data Acquisition
AI	- Artificial Intelligence
ML	- Machine Learning
OCR	- Optical Character Recognition
RFID	- Radio-Frequency Identification
DMS	- Distribution Management System
EMS	- Energy Management System
TCP/IP	- Transmission Control Protocol/Internet Protocol
MQTT	- Message Queuing Telemetry Transport
AES	- Advanced Encryption Standard
PKI	- Public Key Infrastructure
kWh	- Kilowatt Hour

CHAPTER 1

INTRODUCTION

1.1 GENERAL

Generation, transmission and distribution of electrical energy involve many operational losses. Whereas losses implicated in generation can be technically defined, but transmission and distribution losses cannot be precisely quantified with the sending end information. This illustrates the involvement of nontechnical parameter in transmission and distribution system. Overall technical losses occur naturally and caused because of power dissipation in transmission lines, transformers, and other power system components was discussed in. Technical losses in transmission and distributions computed with the information about total load and energy billed. On the other hand, nontechnical losses cannot be precisely computed. It can be estimated from the difference between the total energy supplied to the customers and the total energy billed. This kind of loss can be a power theft in the form of meter tampering, stealing or illegal connections billing irregularities, and unpaid bills. power theft, so has become a serious concern for the utility company and the government. It has also different impact like financial and quality of supplied power.

The financial impact of power theft has two-fold manifestations, first there is income lost or not collected after delivery of the service, second the income lost due to not charging customers more. If there is power theft, it also leads to non-efficient utilization of generated power. So, now a day merely generating more power is not enough, controlling the electrical system has become very important. This can improve power quality to a great extent and prevent power theft of different forms. But some forms of electricity are difficulty to measure, and thus to control. For example, theft that involves tampering with meter to distort the billing information or direct information to the power system results in commercial loss, is nearly impossible to measure. Since there is lack of information on both commercial and the legitimate loads in the system, it is difficult to measure commercial loss. This is due to insufficient inputs for any meaningful loss calculation. Despite the best efforts by utility, the current results of commercial losses measurements are often inaccurate, because the figure rely heavily on the records of

detected cases, rather than actual measurement of the electrical power system. Even if utility do have some control over the magnitude of commercial losses, they are not able to have full control. This has led to a huge lose for electric utilities.

1.2 MOTIVATION FOR THE SELECTION OF PROBLEM

Electricity thefts are increasing every year across domestic as well as industrial domains which affect the economic status of the country. Various wireless communication systems are available to detect the power theft, but lacks the required infrastructure needed to employ them. The project's aim is to design a system to monitor the power consumed by load and to detect and eliminate the power theft in transmission lines and energy meters. This work is also focused on communicating the theft information to Electricity Board (EB) through IoT. As a network of devices is connected like sensors it has the ability to exchange real time information through internet. In this project Raspberry Pi is utilized to detect power theft and send command to GSM module which sends the theft information message to EB. The implementation of this system will help save large amount of electricity.

1.3 OVERVIEW

Arduino-based automatic power theft detection technique for electricity is proposed. In an electricity metering system, tampering is done basically for the purpose of electricity theft. To protect the electrical energy meter from this theft, attempt a relay is used at the opening of the meter. The relay is connected to the interrupt pin of the driver. Hence closed switch applies 12V to the interrupt pin and opened relay drives the voltage to zero. The relay normally closed when the meter chassis is closed. If someone tries to open or tamper with the electricity energy meter, that switch gets opened, and the interrupt pin gets triggered as 0V is sensed by it.

The Arduino immediately sends to the GSM module for sending SMS. Upon receiving an SMS, the authority can take further legal action against it and penalize the theft person.

In conclusion, A Wireless Electricity Theft Detection and monitoring system has been designed and developed with proper integration of both the hardware and the software. Without any human interface this system provides an effective and easy way to detect electrical theft.

The use of IoT helps in achieving the numerous advantages of wireless network communications. we have indicated the theft by increasing the load also and this method is cost efficient. With remote monitoring of the meter reading and sending SMS, whenever there are abnormal readings, in the customer electricity meter, the developed system may able to help Utilities to reduce the incidences of household electricity theft. An automatic circuit breaker can be integrated into the unit so as to remotely cut off the power supply to the house or consumer who tries to indulge in power theft.

CHAPTER 2

LITERATURE SURVEY

2.1 MAJOR FINDINGS FROM LITERATURE SURVEY

Landi, C.; Dipt. Di Ing. Dell' Inf., Seconda Univ. di Napoli, Aversa, Italy; Merola, P.; Ianniello, G, "ARM-based energy management system using smart meter and Web server", IEEE Instrumentation and Measurement Technology Conference Binjiang, pp. 1 - 5, May 2011. This paper focuses on the design and implementation of the EB power monthly calculations. The main part of our work is the fabrication of a cost effective IOT based smart energy meter which displays readings on EB meter, the instant power consumption at user side, which is collects the how much amount of power will consumed per two months. So, the power consumption reading will update at every 6 seconds. So, we can easily note the reading via internet. the readings are updated to internet via IOT module.

Keywords: EB Power, IOT, EB Meter,IOT Module.

Garab, A.; Bouallegue, A.; Ben Abdallah, "A new AMR approach for energy saving in Smart Grids using Smart Meter and partial Power Line Communication". IEEE First International Conference on Renewable Energies and Vehicular Technology (REVET), pp. 263 - 269, March 2012. The growing demand of energy, the capacity limitations of energy management, one-way communication, the need of an interoperability of the different standards, the security of the communication and the greenhouse gas emissions, leads to emerge a new infrastructure grid: Smart Grid. Smart Meters are one of the proposed solutions for the Smart Grid. In this paper, an AMR solution which provides enhanced end-to-end application. It is based on an energy meter with low-power microcontroller MSP430FE423A and the Power Line Communication standards. The microcontroller includes an energy metering module

ESP430CEI. The aim of this work is to realize a real time pricing thanks to the proposed communication infrastructure. This solution is with great interest in economical and low carbon society point of view.

Andrea Zanella, Senior Member, IEEE, Nicola Bui, Angelo Castellani, Lorenzo Vangelista, Senior Member, IEEE, and Michele Zorzi, Fellow, IEEE, "Internet of Things for Smart Cities", IEEE Internet of Things Journal, vol. 1, no. 1, pp. 22-32, February 2014. The Internet of Things (IoT) shall be able to incorporate transparently and seamlessly a large number of different and heterogeneous end systems, while providing open access to selected subsets of data for the development of a plethora of digital services. Building a general architecture for the IoT is hence a very complex task, mainly because of the extremely large variety of devices, link layer technologies, and services that may be involved in such a system. In this paper, we focus specifically to an urban IoT system that, while still being quite a broad category, are characterized by their specific application domain. Urban IoTs, in fact, are designed to support the Smart City vision, which aims at exploiting the most advanced communication technologies to support added-value services for the administration of the city and for the citizens. This paper hence provides a comprehensive survey of the enabling technologies, protocols, and architecture for an urban IoT. Furthermore, the paper will present and discuss the technical solutions and best-practice guidelines adopted in the Padova Smart City project, a proof-of-concept deployment of an IoT island in the city of Padova, Italy, performed in collaboration with the city municipality .

IOT Based Electricity Energy Meter Reading. ' Theft Detection and Disconnection using PLC modem and Power optimization' Darshan Iver N. Dr. K A Radhakrishna Rao [July 2015] . This paper describes PIC18F46k22 Microcontroller based design and implementation of energy meter using IoT concept. The proposed system design eliminates the human involvement in electricity maintenance. The Buyer needs to pay for the usage of electricity on schedule, in case that he couldn't pay, the electricity

transmission can be turned off autonomously from the distant server. The user can monitor the energy consumption in units from a web page by providing device IP address. Theft detection unit connected to energy meter will notify company side when meter tampering occurs in energy meter and it will send theft detect information through PLC modem and theft detected will be displayed on the terminal window of the company side. Wi-Fi unit performs the IoT operation by sending energy meter data to web page which can be accessed through IP address.

The Hardware interface circuit consists of PIC18F46k22 Microcontroller, MAX232, LCD display, theft detection unit, Triac switch circuit, DB18B20 temperature sensor, PIR sensor, PLC modem, and ESP8266 Wi-Fi module. Wi-Fi unit performs the IoT operation by sending energy meter data to web page which can be accessed through IP address.

KEYWORDS: PIC18F46k22, PIC18F2520, ESP8266 Wi-Fi module, PLC modem.

Dietmar P.F. Moller, Hamid Vakilzadian, "Ubiquitous Networks: Power Line Communication and Internet of Things in Smart Home Environments", IEEE, 2014.

Ubiquitous networks in home environments are expanding connectivity to electronic objects/things which can be used to build home network services. This approach uses thing-to-thing or thing-to-gateway connections to access the Internet of Things, allowing data to be stored for cross-referencing and accessing services, such as remote home sensors, etc. In order to make these ubiquitous networks available in the home, power line communication is used. These lines carry data simultaneously with AC electric power. Power lines connect heterogeneous devices through private electrical networks, allowing greater flexibility in the deployment of applications that require important data transfer. Broadband access and advancements in ubiquitous computing have fostered the development of power line communication offering integrated services through a reliable and robust system at the physical and data link layer of the open system interconnection (OSI) model. In this paper we describe application of ubiquitous networks in smart home environment.

M. Anas, N. Javaid, A. Mahmood, S. M. Raza, U. Qasim, Z. A. Khan, "Minimizing Electricity Theft using Smart Meters in AMI", IEEE Seventh International Conference on P2P. Parallel, Grid, Cloud and Internet Computing, 2012, pp. 176-182.

Global energy crises are increasing every moment. Everyone has the attention towards more and more energy production and also trying to save it. Electricity can be produced through many ways which is then synchronized on a main grid for usage. The main issue for which we have written this survey paper is losses in electrical system. Whether these losses are technical or non-technical. Technical losses can be calculated easily, as we discussed in section of mathematical modeling that how to calculate technical losses. Whereas nontechnical losses can be evaluated if technical losses are known.

Theft in electricity produce non-technical losses. To reduce or control theft one can save his economic resources. Smart meter can be the best option to minimize electricity theft, because of its high security, best efficiency, and excellent resistance towards many of theft ideas in electromechanical meters. So in this paper we have mostly concentrated on theft issues.

2.2 EXISTING SYSTEM BLOCK DIAGRAM

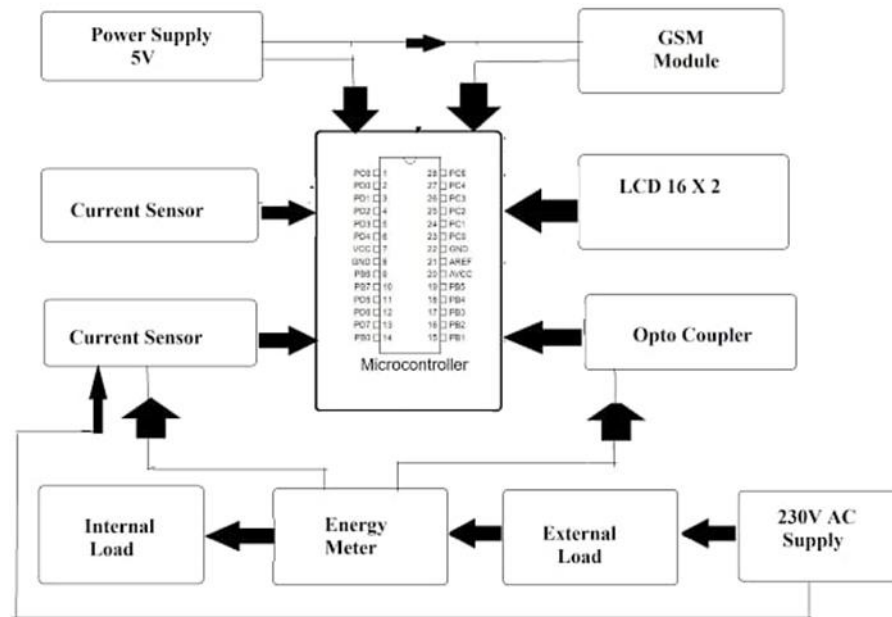


Fig 2.1: Existing system block diagram

2.3 OPEN PROBLEMS IN EXISTING SYSTEM

In this Existing system IT and GSM technology is implemented for transmitting the information about power theft to the EB and prevents the current scenario. This system is being interfaced with Arduino via serial communication and sensors are interfaced with uno to sense the load current and voltage. This will prevent the electricity theft as much as possible. The current system gives solution for the existing problems like power theft, wastage of energy and transmission line fault that are faced by the authorized power suppliers.

2.4 DISADVANTAGES

- Higher costs (time and money).
- Cannot able to send data to cloud.
- Cannot able to turn of load from anywhere.

2.5 IEEE STANDARDS FOLLOWED

The Institute of Electrical and Electronics Engineers (IEEE) has several standards related to the reduction of electricity theft using IoT technology. Some of these standards include:

1. IEEE 802.15.4: This standard specifies the physical and MAC layer specifications for low-rate wireless personal area networks (LR-WPANs). It is a common standard used for IoT devices and can be used for electricity theft reduction.
2. IEEE 802.15.4g: This standard is an amendment to IEEE 802.15.4 and specifies the physical layer specifications for wireless smart utility networks (Wi-SUN). It is designed to support smart grid applications, including electricity theft reduction.
3. IEEE 2030.5: This standard specifies the communication protocols for smart grid energy management systems using Internet Protocol (IP) and web services technologies. It includes security and privacy features that can help prevent electricity theft.
4. IEEE 1547.4: This standard provides guidelines for the design, testing, and certification of distributed energy resources (DER) interfaces with electric power systems. It includes requirements for anti-islanding and anti-tampering measures that can help prevent electricity theft.
5. IEEE P1854.1: This is a draft standard for a framework for the detection and reporting of energy theft. It includes guidelines for the design of energy theft detection systems that can use IoT devices and other technologies .

2.6 CONSTRAINTS

Cost: The cost of implementing IoT-based solutions for electricity theft reduction can be high. IoT devices, sensors, and other components needed for such solutions can be expensive, especially if they need to be deployed on a large scale.

Connectivity: IoT devices rely on connectivity to transmit data and communicate with other devices. However, in some areas where electricity theft is a problem, the connectivity infrastructure may not be well developed, making it difficult to implement IoT-based solutions.

Power supply: IoT devices need a reliable power supply to function. However, in areas where electricity theft is common, the power supply may be unstable, making it difficult to maintain a reliable connection to IoT devices.

Data privacy and security: IoT devices collect and transmit sensitive data related to electricity consumption, which can be vulnerable to cyber-attacks and data breaches. Ensuring the privacy and security of such data can be a challenge.

Regulatory constraints: Some countries or regions may have regulations that limit the deployment of IoT devices or the collection of certain types of data, which can make it difficult to implement IoT-based solutions for electricity theft reduction.

Limited awareness: In some areas, there may be limited awareness or understanding of the benefits of IoT-based solutions for electricity theft reduction, which can make it challenging to gain support and adoption for such solutions.

2.7 TRADEOFF

Cost vs. benefits: The cost of implementing IoT-based solutions for electricity theft reduction may be high, but the benefits of reducing theft can be significant in terms of cost savings, improved revenue collection, and improved grid stability.

Privacy vs. security: IoT devices collect sensitive data related to electricity consumption, which can be vulnerable to cyber-attacks and data breaches. Balancing the need for data privacy and security is a critical tradeoff in implementing such solutions.

Coverage vs. granularity: IoT devices can provide granular data on electricity consumption, but the coverage area of such devices may be limited. Balancing the need for broad coverage and granular data is an important tradeoff in implementing IoT-based solutions for electricity theft reduction.

Reliability vs. complexity: IoT devices can provide reliable data on electricity consumption, but the complexity of such devices and the associated software can make them more challenging to implement and maintain.

Energy consumption vs. functionality: IoT devices need a reliable power supply to function, but the energy consumption of such devices can be significant, which can impact their functionality and deployment.

2.8 PREREQUISITES

IoT infrastructure: A reliable and robust IoT infrastructure is needed to support the deployment of IoT devices and sensors for electricity theft reduction. This includes a network architecture that can support the collection, transmission, and processing of data from these devices.

Data management: An effective data management strategy is critical for IoT-based solutions for electricity theft reduction. This includes data collection, storage, analysis, and visualization to help identify patterns of electricity theft and enable real-time response.

Analytics and machine learning: Advanced analytics and machine learning algorithms are needed to analyze the large volumes of data generated by IoT devices and sensors for electricity theft detection and prevention. These algorithms can help identify anomalies, patterns, and trends that may indicate electricity theft.

Regulatory compliance: IoT-based solutions for electricity theft reduction must comply with relevant regulations and laws, including data privacy and security regulations.

Stakeholder buy-in: Successful implementation of IoT-based solutions for electricity theft reduction requires stakeholder buy-in from both utilities and customers. This includes educating customers about the benefits of such solutions and ensuring that utilities have the necessary resources and support to deploy and maintain these solutions.

Technical expertise: IoT-based solutions for electricity theft reduction require technical expertise in areas such as IoT device design, data analytics, cybersecurity, and network infrastructure. Ensuring that the necessary technical expertise is available is critical for successful implementation.

CHAPTER 3

AIM AND SCOPE OF THE PRESENT INVESTIGATION

3.1 AIM OF THE PROJECT

The aim of the reduction of electricity thief using iot is Arduino based power theft detection and protection system is designed. An increase in the demand of electric power for household, commercial and industrial loads lead to management of electric distribution system become more complicated. Lack of information at the bases station regarding status of the distribution network has been identified as the major bottleneck to its effective monitoring and controlling. Electrical power theft detection and protection system is used to detect and protect an unauthorized tapping on distribution line. In this project ACS712 series current sensor has been used as the interfacing instrument between the power line current and Arduino. To isolate power line from power theft system relay used as switching gear. Arduino control all operations that all devices do.

3.2 SCOPE OF THE PROJECT

This system would provide a simple way to detect and prevent an electrical power theft without any human interference, maximize the profit margin of power utility company and Prevent fault due to overload. The theft detection of electricity also became possible by using this system through which server received the message when users by passed the meter. This system provides billing activity in addition to detection and protection power theft.

3.3 OBJECTIVES

- IOT use things to things connection to access the internet of things, allow data to store and access services. Services over internet of things development according to need of person to person and thing to person, machine to machine interaction without human interaction.
- As there is limited non-renewable resources are present in our daily life, Electricity is one of them which utilized in every country that results abundant losses due to electricity larceny. Power theft is going to be the key challenges.
- A smart energy meter is used to minimize the electricity larceny. Basically, energy meter is a device that calculates the cost of electricity consumed by homes, business, or an electrical device. It reduces the theft of electricity.

3.4 ADVANTAGES

Cost savings: Reducing electricity theft using IoT can help save costs for both electricity providers and consumers. Electricity providers can reduce their losses due to theft, and consumers can benefit from reduced electricity bills.

Increased revenue: With the reduction in theft, electricity providers can increase their revenue by accurately billing their customers and charging them for the electricity they use.

Improved efficiency: IoT can provide real-time monitoring of electricity consumption and identify any anomalies or theft attempts. This can help utilities quickly identify and resolve issues, thereby improving efficiency.

Improved safety: Electricity theft can be dangerous and can result in accidents and fires. By reducing theft, IoT can help improve safety for both consumers and electricity providers.

Environmental benefits: Reduction in electricity theft can lead to a reduction in overall electricity consumption, thereby reducing greenhouse gas emissions and environmental impact.

Improved reliability: IoT can help identify areas where electricity theft is prevalent and where there is a high demand for electricity. This can help utilities improve their infrastructure and ensure a more reliable electricity supply.

CHAPTER 4

HARDWARE AND PROJECT DESCRIPTION

4.1 HARDWARE CIRCUIT DIAGRAM

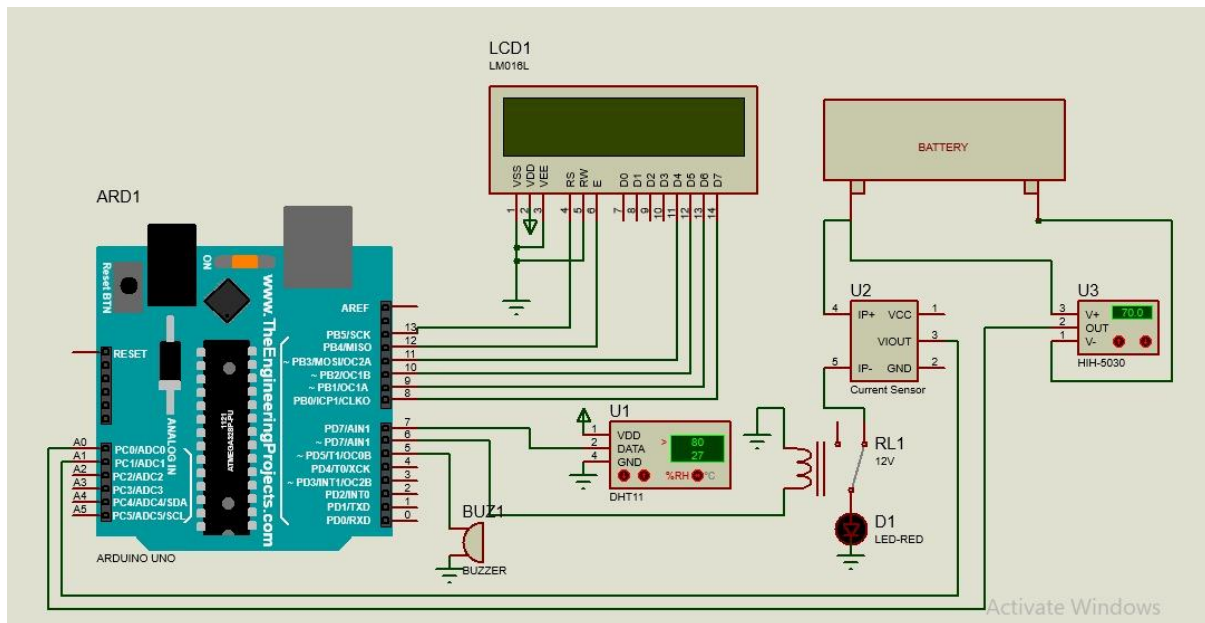


Fig 4.1: Circuit diagram

4.2 EXPLANATION

IoT devices and sensors: These devices can be deployed in electrical infrastructure, such as power lines, to monitor electricity consumption and detect anomalies that may indicate electricity theft.

Communication network: A communication network, such as a cellular network or Wi-Fi network, can be used to transmit data from the IoT devices and sensors to a central database for processing and analysis.

Central database: The data collected by the IoT devices and sensors can be stored in a central database, where it can be processed and analyzed to identify patterns of electricity theft.

Data analytics and machine learning: Advanced data analytics and machine learning algorithms can be used to analyze the data collected by the IoT devices and sensors to identify anomalies and patterns that may indicate electricity theft.

Alerts and notifications: If the system detects anomalies or patterns that indicate electricity theft, alerts and notifications can be sent to relevant stakeholders, such as utilities or law enforcement agencies, to enable real-time response.

Control systems: Control systems can be used to monitor and control electricity distribution to prevent electricity theft. For example, if the system detects that electricity theft is occurring in a particular area, the control systems can be used to cut off power supply to that area until the issue is resolved.

User interface: A user interface can be developed to provide real-time information on electricity consumption and to enable utilities and customers to monitor electricity usage and identify potential issues.

4.3 HARDWARE COMPONENTS

The list of hardware components that are required are:

- Arduino Uno R3
- Voltage Sensor
- Current Sensor
- Load

- Iot Wifi Modem
- Power Supply Unit
- Lcd

Software Requirement

- ARDUINO IDE
- Embedded C

4.3.1 Arduino UNO

Arduino is an open-source electronics platform based on easy-to-use hardware and software. Arduino boards are able to read inputs - light on a sensor, a finger on a button, or a Twitter message - and turn it into an output - activating a motor, turning on an LED, publishing something online. You can tell your board what to do by sending a set of instructions to the microcontroller on the board. To do so you use the Arduino programming language (based on Wiring), and the Arduino Software (IDE), based on Processing.

Over the years Arduino has been the brain of thousands of projects, from everyday objects to complex scientific instruments. A worldwide community of makers - students, hobbyists, artists, programmers, and professionals - has gathered around this open-source platform, their contributions have added up to an incredible amount of accessible knowledge that can be of great help to novices and experts alike.

Arduino was born at the Ivrea Interaction Design Institute as an easy tool for fast prototyping, aimed at students without a background in electronics and programming. As soon as it reached a wider community, the Arduino board started changing to adapt to new needs and challenges, differentiating its offer from simple 8-bit boards to products for IoT applications, wearable, 3D printing, and embedded environments. All Arduino boards are completely open-source, empowering users to build them

independently and eventually adapt them to their particular needs. The software, too, is open-source, and it is growing through the contributions of users worldwide.

4.3.1.1 Input and Output

Arduino - ArduinoBoardUno Each of the 14 digital pins on the Uno can be used as an input or output, using `pinMode()`, `digitalWrite()`, and `digitalRead()` functions. They operate at 5 volts. Each pin can provide or receive a maximum of 40 mA and has an internal pull-up resistor (disconnected by default) of 20-50 kOhms.

The Uno is one of the more popular boards in the Arduino family and a great choice for beginners.

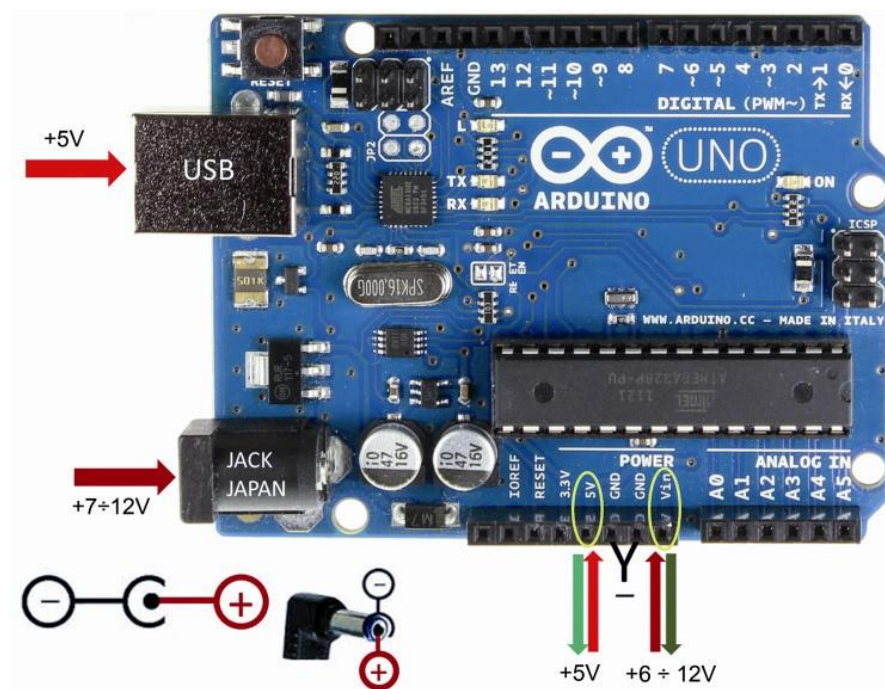


Fig 4.2: Arduino UNO

Table 4.1: Arduino UNO specifications

Microcontroller	ATmega328P – 8 bit AVR family microcontroller
Operating Voltage	5V
Recommended Input Voltage	7-12V
Input Voltage Limits	6-20V
Analog Input Pins	6 (A0 – A5)
Digital I/O Pins	14 (Out of which 6 provide PWM output)
DC Current on I/O Pins	40 mA
DC Current on 3.3V Pin	50 mA
Flash Memory	32 KB (0.5 KB is used for Bootloader)
SRAM	2 KB
EEPROM	1 KB
Frequency (Clock Speed)	16 MHz

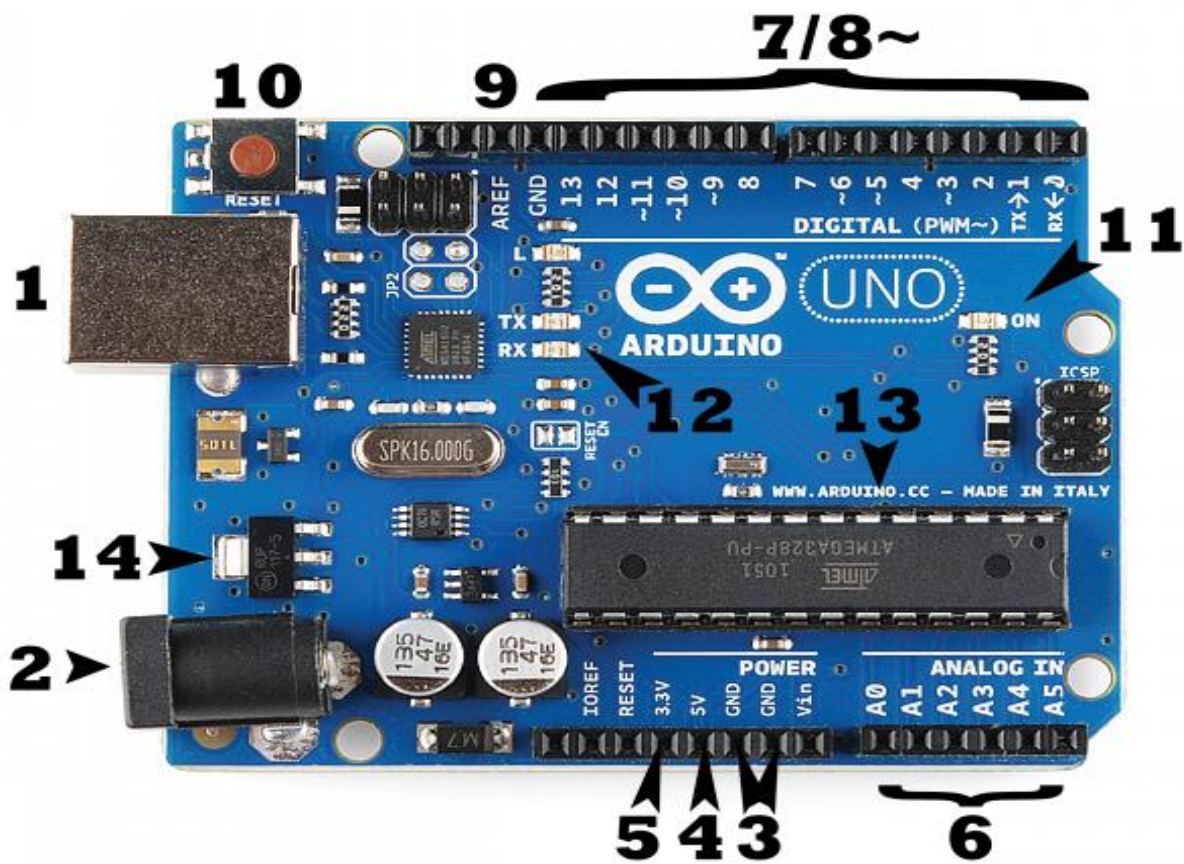


Fig 4.3: Arduino UNO pinout

4.3.1.2 Power (USB / Barrel Jack)

Every Arduino board needs a way to be connected to a power source. The Arduino UNO can be powered from a USB cable coming from your computer or a wall power supply that is terminated in a barrel jack. In the picture above the USB connection is labelled **(1)** and the barrel jack is labelled **(2)**. The USB connection is also how you will load code onto your Arduino board.

4.3.1.3 Pins (5V, 3.3V, GND, Analog, Digital, PWM, AREF)

The pins on your Arduino are the places where you connect wires to construct a circuit (probably in conjunction with a breadboard and some wire).

They usually have black plastic 'headers' that allow you to just plug a wire right into the board. The Arduino has several different kinds of pins, each of which is labelled on the board and used for different functions.

GND (3): Short for 'Ground'. There are several GND pins on the Arduino, any of which can be used to ground your circuit.

5V (4) & 3.3V (5): As you might guess, the 5V pin supplies 5 volts of power, and the 3.3V pin supplies 3.3 volts of power. Most of the simple components used with the Arduino run happily off of 5 or 3.3 volts.

Analog (6): The area of pins under the 'Analog In' label (A0 through A5 on the UNO) are Analog In pins. These pins can read the signal from an analog sensor (like a temperature sensor) and convert it into a digital value that we can read.

Digital (7): Across from the analog pins are the digital pins (0 through 13 on the UNO). These pins can be used for both digital input (like telling if a button is pushed) and digital output (like powering an LED).

PWM (8): You may have noticed the tilde (~) next to some of the digital pins (3, 5, 6, 9, 10, and 11 on the UNO). These pins act as normal digital pins, but can also be used for something called Pulse-Width Modulation (PWM).

AREF (9): Stands for Analog Reference. Most of the time you can leave this pin alone. It is sometimes used to set an external reference voltage (between 0 and 5 Volts) as the upper limit for the analog input pins.

4.3.1.4 Reset Button

Just like the original Nintendo, the Arduino has a reset button (**10**). Pushing it will temporarily connect the reset pin to ground and restart any code that is loaded on the Arduino.

This can be very useful if your code doesn't repeat, but you want to test it multiple times. Unlike the original Nintendo however, blowing on the Arduino doesn't usually fix any problems.

4.3.1.5 Power LED Indicator

Just beneath and to the right of the word "UNO" on your circuit board, there's a tiny LED next to the word 'ON' **(11)**. This LED should light up whenever you plug your Arduino into a power source. If this light doesn't turn on, there's a good chance something is wrong. Time to re-check your circuit.

4.3.1.6 TX RX LEDs

TX is short for transmit RX is short for receive. These markings appear quite a bit in electronics to indicate the pins responsible for serial communication.

In our case, there are two places on the Arduino UNO where TX and RX appear once by digital pins 0 and 1, and a second time next to the TX and RX indicator LEDs **(12)**.

These LEDs will give us some nice visual indications whenever our Arduino is receiving or transmitting data (like when we're loading a new program onto the board).

4.3.1.7 Main IC

The black thing with all the metal legs is an IC, or Integrated Circuit **(13)**. Think of it as the brains of our Arduino.

The main IC on the Arduino is slightly different from board type to board type, but is usually from the AT mega line of IC's from the ATMEL company. This can be important, as you may need to know the IC type (along with your board type) before loading up a new program from the Arduino software. This information can usually be found in writing on the top side of the IC. If you want to know more about the difference between various IC's, reading the datasheets is often a good idea.

4.3.1.8 Voltage Regulator

The voltage regulator **(14)** is not actually something you can (or should) interact with on the Arduino. But it is potentially useful to know that it is there and what it's for.

The voltage regulator does exactly what it says – it controls the amount of voltage that is let into the Arduino board. Think of it as a kind of gatekeeper; it will turn away an extra voltage that might harm the circuit. Of course, it has its limits, so don't hook up your Arduino to anything greater than 20 volts.

4.3.1.9 ATmega 328

ATmega-328 is basically an Advanced Virtual RISC (AVR) micro-controller. It supports the data up to eight (8) bits. ATmega-328 has 32KB internal built in memory. This micro-controller has a lot of other characteristics.

ATmega 328 has 1KB Electrically Erasable Programmable Read Only Memory (EEPROM).

This property shows if the electric supply supplied to the micro-controller is removed, even then it can store the data and can provide results after providing it with the electric supply.

Moreover, ATmega-328 has 2KB Static Random Access Memory (SRAM). Other characteristics will be explained later. ATmega 328 has several different features which make it the most popular device in today's market. These features consist of advanced RISC architecture, good performance, low power consumption, real timer counter having separate oscillator, 6 PWM pins, programmable serial USART, programming lock for software security, throughput up to 20 MIPS etc. ATmega-328 is mostly used in Arduino.

ATmega328 is an eight (8) bit micro-controller. It can handle the data sized of up to eight (8) bits. It is an AVR based micro-controller. Its built-in internal memory is around 32KB. It operates ranging from 3.3V to 5V. It has an ability to store the data even when the electrical supply is removed from its biasing terminals. Its excellent features include the cost efficiency, low power dissipation, programming lock for security purposes, real timer counter with separate oscillator.

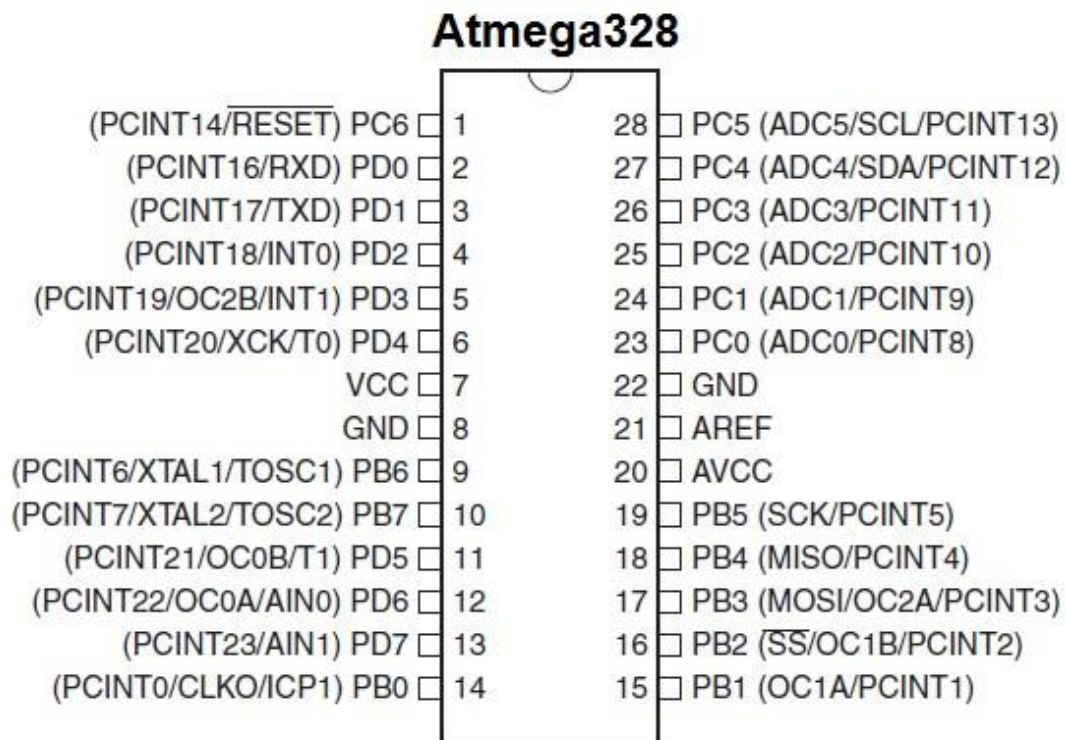


Fig 4.4: Pin diagram

4.3.2 POWER SUPPLY CIRCUIT:

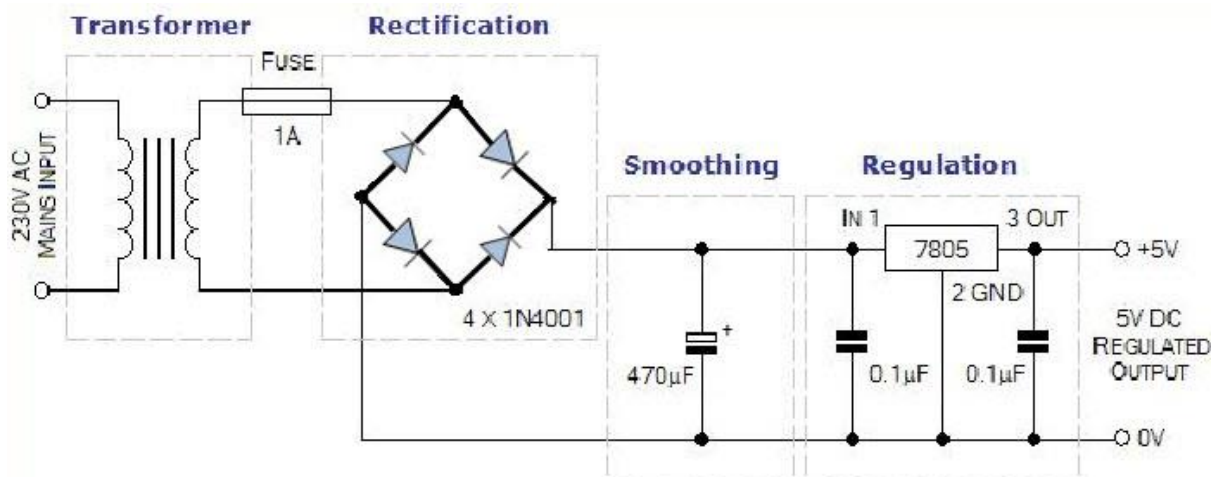


Fig 4.5: Power supply circuit

4.3.3 Voltage sensor

A voltage sensor is an electronic device that measures and monitors the electrical potential difference, or voltage, between two points in an electrical circuit. It is commonly used in various applications, including power systems, industrial processes, consumer electronics, and automotive systems. The voltage sensor plays a critical role in ensuring the safe and efficient operation of electrical equipment by providing accurate voltage measurements and transmitting the information to other devices or systems for further processing or control.



Fig 4.6: Voltage sensor

A typical voltage sensor consists of several key components, including a sensing element, signal conditioning circuitry, and an output interface. The sensing element is the part of the voltage sensor that comes into contact with the electrical circuit and converts the electrical voltage into a measurable signal, which is then processed by the signal conditioning circuitry. The signal conditioning circuitry amplifies, filters, and isolates the signal to ensure accurate and reliable measurements. The output interface provides the means for transmitting the processed voltage measurement to other devices or systems, such as analog or digital output signals, communication protocols, or display interfaces.

4.3.4 Current sensor

A current sensor is an electronic device used to measure and monitor the flow of electric current in a circuit. It is widely used in various applications, including power systems, motor control, battery management, renewable energy systems, and industrial processes. Current sensors play a crucial role in providing accurate current measurements, which are essential for monitoring and controlling electrical systems, ensuring safety, efficiency, and performance.

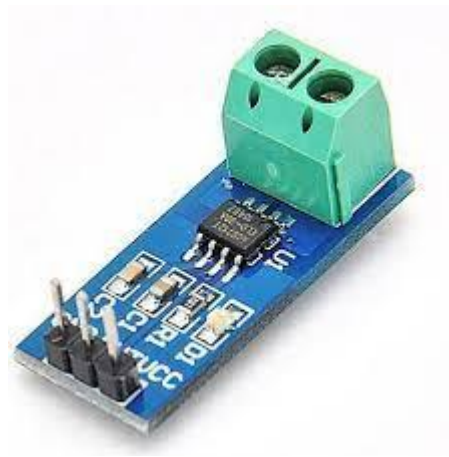


Fig 4.7: Current sensor

A typical current sensor consists of several key components, including a sensing element, signal conditioning circuitry, and an output interface. The sensing element is the part of the current sensor that comes into contact with the electrical current-carrying conductor and generates a measurable signal proportional to the current. The signal conditioning circuitry processes the signal, providing amplification, filtering, and isolation to ensure accurate and reliable measurements. The output interface provides the means for transmitting the processed current measurement to other devices or systems, such as analog or digital output signals, communication protocols, or display interfaces.

Current sensors can be designed to measure different types of current signals, including DC (direct current) or AC (alternating current) currents, and can have various input and output current ranges, accuracy levels, and response times depending on the specific application requirements. They can also measure different current levels, ranging from low currents in milliamperes to high currents in kiloamperes or even higher.

Some current sensors also incorporate additional features, such as overcurrent protection, temperature compensation, fault detection, or galvanic isolation, to enhance their performance and reliability in challenging environments or critical applications.

In conclusion, a current sensor is a critical component in electrical systems that enables accurate measurement and monitoring of current levels. It plays a crucial role in various applications by providing essential current measurements for monitoring, control, and protection. By converting current into measurable signals, processing them, and providing output interfaces for communication or control, current sensors contribute to the safety, efficiency, and performance of electrical systems. Proper selection, installation, and calibration of current sensors are essential to ensure their accurate operation and reliable performance in diverse applications.

4.3.5 Battery

A 12V battery is a type of rechargeable battery that provides a nominal voltage of 12 volts. It is commonly used in a wide range of applications, including automotive, marine, recreational vehicles, uninterruptible power supply (UPS) systems, solar power systems, and portable electronics. The 12V battery is a popular choice for powering various devices and systems due to its relatively high voltage output and versatility.



Fig 4.8 Battery

A typical 12V battery is composed of one or more electrochemical cells connected in series to produce a total voltage of 12 volts. The cells are usually enclosed in a durable plastic or metal case and contain an electrolyte and one or more electrodes that undergo chemical reactions to generate electrical energy. The most common types of batteries used to produce 12V output are lead-acid batteries and lithium-ion batteries.

Lead-acid batteries are a type of rechargeable battery that uses lead plates and sulfuric acid as the electrolyte. They are widely used in automotive applications and other high-current applications due to their ability to deliver high power outputs. Lead-acid batteries are relatively inexpensive and have a long history of reliable performance, although they are relatively heavy and require periodic maintenance.

Lithium-ion batteries are a type of rechargeable battery that uses lithium ions to generate electrical energy. They are known for their high energy density, lightweight, and long cycle life. Lithium-ion batteries are commonly used in portable electronics, electric vehicles, and solar power systems due to their high-power density and lightweight design. They are generally more expensive than lead-acid batteries but offer higher performance and convenience in many applications.

In conclusion, a 12V battery is a common type of rechargeable battery that provides a nominal voltage of 12 volts. It is widely used in various applications due to its versatility, including automotive, marine, recreational vehicles, UPS systems, solar power systems, and portable electronics. Whether it's a lead-acid or lithium-ion battery, proper handling, charging, and maintenance are essential to ensure its safe and reliable operation. The selection of the appropriate type of 12V battery depends on the specific requirements of the application in terms of power output, energy density, weight, and cost considerations.

4.3.6 LCD

To display accurate messages, we use the LCD Module. Analyzing A smart two-line LCD display, 16 characters per line used to directors. The (handshake) presentation session is as follows it emerged. Although D0 to D7th bit are Data lines, RS, RW and EN pins only control rods and anchors remaining + 5V, - 5V and GND should be provided to feed. Where RS is the Select Register, RW is Read Write and EN pin Allow.

The most popular type t LCD regulator is a HITACHI 44780 that provides a visual interface in the middle controller and LCD. These LCDs are very easy to work with regulator as they have financial knowledge



Fig 4.9: 2x16 Line Alphanumeric LCD display

The LCD requires three control lines (RS, R / W and EN) and 8 (or lines of information. The number in the information lines depends on the operating system. Whenever it works in 8-bit mode and then 8+ information lines and three control lines for example 11 lines are required. In addition, whenever a 4-bit mode is used and then 4+ information lines and three control lines for example 7 lines are required. How can we choose which mode to use? It is straightforward with the possibility that you have enough information lines to go in 8-digit mode and if there is a binding time.

The ENABLE pin is used to link existing information to information pins. A low-level signal is needed to connect the data. LCD deciphers also make our order right now the EN line is dropped down. If you do not lower EN, your lead will never be implemented.

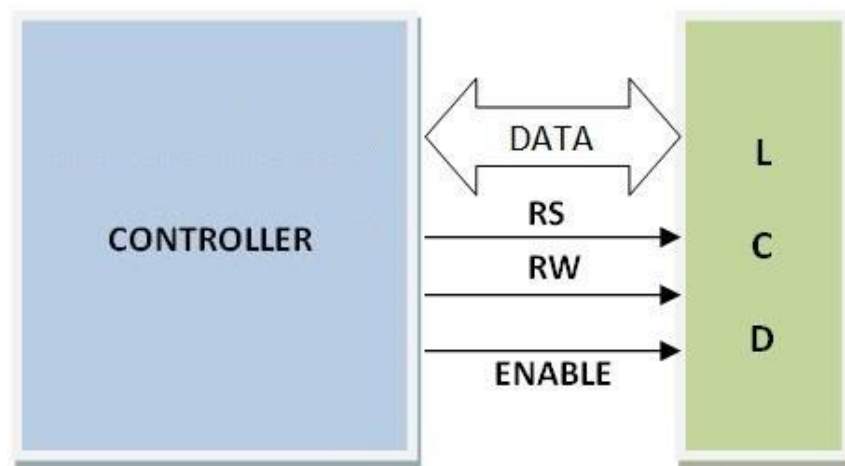


Fig 4.10: Basic LCD screen

4.3.6.1 Description

This is the 16th feature in the 2-line display. Dark content on Green foundation. It uses the same HD44780 optical chipset. Interface code is clearly accessible. We will need 11 standard I / O pins to connect to this LCD screen. Includes LED backlight.

4.3.6.2 Pin

Most LCDs with 1 controller have 14 pins and LCDs with 2 regulators with 16 pins (two pins are added to both LED backlights). The display of the pin appears in the table below.



Fig 4.11: LCD screen



Fig 4.12: LCD Background

4.3.6.3 LCD Background

Fortunately, there is a popular standard that allows us to talk to many LCDs that do not pay much attention to their manufacturer. The standard is referred to as the

HD44780U, which refers to the controller chip that receives data from an external source (8051) and communicates directly with the LCD.

Pin No.	Name	Description
Pin no. 1	VSS	Power supply (GND)
Pin no. 2	VCC	Power supply (+5V)
Pin no. 3	VEE	Contrast <u>adjust</u>
Pin no. 4	RS	0 = Instruction input 1 = Data input
Pin no. 5	R/W	0 = Write to LCD module 1 = Read from LCD module
Pin no. 6	EN	Enable signal
Pin no. 7	D0	Data bus line 0 (LSB)
Pin no. 8	D1	Data bus line 1
Pin no. 9	D2	Data bus line 2
Pin no. 10	D3	Data bus line 3
Pin no. 11	D4	Data bus line 4

Fig 4.13: Character LCD pins with 1 Controller

4.3.6.4 Circuit Description

Above is a very straightforward program. Control Port is an open source / open channel producer. While many of the same ports have internal pull-out pins, not much

is missing. So by mixing two 10K external pull-outs, the circuit is more integrated with a wider range of PCs, some of which may not have internal drawing addresses.

Pin No.	Name	Description
Pin no. 1	D7	Data bus line 7 (MSB)
Pin no. 2	D6	Data bus line 6
Pin no. 3	D5	Data bus line 5
Pin no. 4	D4	Data bus line 4
Pin no. 5	D3	Data bus line 3
Pin no. 6	D2	Data bus line 2
Pin no. 7	D1	Data bus line 1
Pin no. 8	D0	Data bus line 0 (LSB)
Pin no. 9	EN1	Enable signal for row 0 and 1 (1 st controller)
Pin no. 10	R/W	0 = Write to LCD module 1 = Read from LCD module
Pin no. 11	RS	0 = Instruction input 1 = Data input

Fig 4.14: Character LCD pins with 2 Controller

We made no effort to include data transfer in exchange. So we tightened the cords to the R / W line of the LCD board, into writing mode. This will not cause a conflict of interest in the transportation of information lines. We are therefore unable to reverse the interior of the LCD Busy Flag advising us if the LCD consents and threatened to prepare for the final lead. This issue is being addressed by the known embedding of our system.

4.3.7 Buzzer

A buzzer is a small yet efficient component to add sound features to our project/system. It is very small and compact 2-pin structure hence can be easily used on breadboard, Perf Board and even on PCBs which makes this a widely used component in most electronic applications.



Fig 4.15: Buzzer

There are two types are buzzers that are commonly available. The one shown here is a simple buzzer which when powered will make a Continuous Beeeeeeppp.... sound, the other type is called a readymade buzzer which will look bulkier than this and will produce a Beep. Beep. Beep. Sound due to the internal oscillating circuit present inside it. But the one shown here is most widely used because it can be customized with help of other circuits to fit easily in our application.

This buzzer can be used by simply powering it using a DC power supply ranging from 4V to 9V. A simple 9V battery can also be used, but it is recommended to use a

regulated +5V or +6V DC supply. The buzzer is normally associated with a switching circuit to turn ON or turn OFF the buzzer at required time and require interval.

Table 4.2: Buzzer Pin Configuration

Pin Number	Pin Name	Description
1	Positive	Identified by (+) symbol or longer terminal lead. Can be powered by 6V DC
2	Negative	Identified by short terminal lead. Typically connected to the ground of the circuit

4.3.7.1 Applications of Buzzer

- Alarming Circuits, where the user has to be alarmed about something.
- Communication equipments.
- Automobile electronics.
- Portable equipments, due to its compact size.

4.3.8 Relay

A relay is an electromechanical device used to control the flow of electrical current in a circuit. It is commonly used in various applications, including industrial automation, telecommunications, automotive systems, home appliances, and electronic devices. Relays are widely used for their ability to switch high currents or voltages with a low-

power control signal, making them essential components in many electrical and electronic systems.



Fig 4.16: Relay

A typical relay consists of several key components, including a coil, an armature, and contacts. The coil is an electromagnetic winding that is energized when a control signal, typically a low-voltage electrical current, is applied to it. The energized coil creates a magnetic field that attracts the armature, which is a movable component connected to the contacts. The armature moves in response to the magnetic field, causing the contacts to open or close, depending on the relay type and configuration.

The contacts in a relay are the switching elements that control the flow of electrical current. There are typically two sets of contacts in a relay, known as normally open (NO) and normally closed (NC) contacts. In the resting state, the NO contacts are open, and the NC contacts are closed. When the coil is energized, the armature moves, and the contacts change their state. In a NO relay, the contacts close, allowing current to flow through the relay, while in an NC relay, the contacts open, interrupting the current flow.

Relays come in various types and configurations, including electromechanical relays, solid-state relays (SSRs), latching relays, and reed relays, among others. Electromechanical relays use physical contacts and mechanical movement to switch

the current, while SSRs use semiconductor devices to achieve the same function without mechanical parts. Latching relays have two stable states and do not require continuous power to maintain their state, while reed relays use a small hermetically sealed glass tube with contacts that open and close based on the position of a magnet.

In conclusion, a relay is an essential electromechanical device used to control the flow of electrical current in a circuit. It consists of a coil, an armature, and contacts that open or close in response to an energized coil. Relays are widely used in various applications for their ability to switch high currents or voltages with a low-power control signal. Proper selection, installation, and use of relays are crucial for ensuring their reliable operation in different systems and applications.

4.3.9 Node MCU

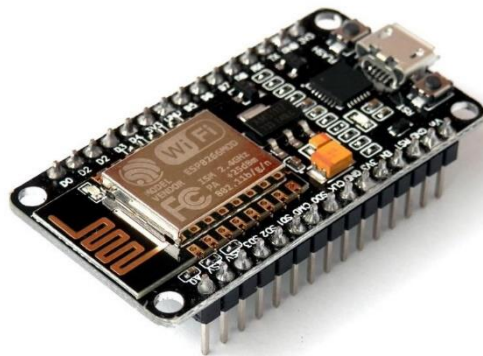


Fig 4.17: Node MCU

The ESP8266 NodeMCU CP2102 board has ESP8266 which is a highly integrated chip designed for the needs of a new connected world. It offers a complete and self-contained WiFi networking solution, allowing it to either host the application or to offload all Wi-Fi networking functions from another application processor.

ESP8266 has powerful on-board processing and storage capabilities that allow it to be integrated with the sensors and other application-specific devices through its

GPIOs with minimal development up-front and minimal loading during runtime. Its high degree of on-chip integration allows for minimal external circuitry, and the entire solution, including the frontend module, is designed to occupy minimal PCB area.

The ESP8266 NodeMCU development board – a true plug-and-play solution for inexpensive projects using WiFi. The module arrives pre-flashed with NodeMCU firmware so they're ready to go – just install your USB driver (below). ESP-12 Lua Nodemcu WIFI Dev Board Internet Of Things board contains a full ESP8266 WiFi module with all the GPIO broken out, a full USB-serial interface, and a power supply all on the one breadboard-friendly package.

This board is pre-flashed with NodeMCU – a Lua-based firmware for the ESP8266 which allows easy control via a neat scripting language – Lua – so you're ready to go in just a few minutes.

The ESP-12 Lua NodeMCU WIFI Dev Board Internet Of Things with ESP8266 is an all-in-one microcontroller + WiFi platform that is very easy to use to create projects with WiFi and IoT (Internet of Things) applications.

The board is based on the highly popular ESP8266 WiFi Module chip with the ESP-12 SMD footprint. This WiFi development board already embeds in its board all the necessary components for the ESP8266 (ESP-12E) to program and upload code. It has a builtin USB to serial chip upload codes, 3.3V regulator, and logic level converter circuit so you can immediately upload codes and connect your circuits.

4.3.9.1 Features

- Open-source, Interactive, Programmable, Low cost, Simple, Smart, WI-FI enabled
- Arduino-like hardware IO
- Integrated TR switch, balun, LNA, power amplifier and matching network
- Integrated PLL, regulators, DCXO and power management units

- Onboard USB to serial chip to easily program and upload codes from the Arduino IDE
- Embeds logic level converter circuits
- Has onboard 3.3V regulator to ensure enough power to function as your go-to WiFi chip.
- Easy access to the GPIO pins for easy prototyping
- ESP-12E Processor
- Easy to use breadboard friendly form factor

4.4 SOFTWARE REQUIRED

- Arduino IDE
- Embedded C
- Thingspeak

4.4.1 Arduino IDE

Arduino is an open-source electronics platform based on easy-to-use hardware and software. Arduino boards are able to read inputs - light on a sensor, a finger on a button, or a Twitter message - and turn it into an output - activating a motor, turning on an LED, publishing something online. You can tell your board what to do by sending a set of instructions to the microcontroller on the board. To do so you use the Arduino programming language (based on Wiring), and the Arduino Software (IDE), based on Processing.

Over the years Arduino has been the brain of thousands of projects, from everyday objects to complex scientific instruments. A worldwide community of makers -

students, hobbyists, artists, programmers, and professionals - has gathered around this open-source platform, their contributions have added up to an incredible amount of accessible knowledge that can be of great help to novices and experts alike.

Arduino was born at the Ivrea Interaction Design Institute as an easy tool for fast prototyping, aimed at students without a background in electronics and programming. As soon as it reached a wider community, the Arduino board started changing to adapt to new needs and challenges, differentiating its offer from simple 8-bit boards to products for IoT applications, wearable, 3D printing, and embedded environments. All Arduino boards are completely open-source, empowering users to build them independently and eventually adapt them to their particular needs. The software, too, is open-source, and it is growing through the contributions of users worldwide.

4.4.1.1 Why Arduino?

The Arduino software is easy-to-use for beginners, yet flexible enough for advanced users. It runs on Mac, Windows, and Linux. Teachers and students use it to build low-cost scientific instruments, to prove chemistry and physics principles, or to get started with programming and robotics. Designers and architects build interactive prototypes, musicians and artists use it for installations and to experiment with new musical instruments. Makers, of course, use it to build many of the projects exhibited at the Maker Faire, for example. Arduino is a key tool to learn new things. Anyone - children, hobbyists, artists, programmers - can start tinkering just following the step-by-step instructions of a kit, or sharing ideas online with other members of the Arduino community.

There are many other microcontrollers and microcontroller platforms available for physical computing. Parallax Basic Stamp, Netmedia's BX-24, Phidgets, MIT's Handyboard, and many others offer similar functionality. All of these tools take the messy details of microcontroller programming and wrap it up in an easy-to-use package. Arduino also simplifies the process of working with microcontrollers, but it offers some advantage for teachers, students, and interested amateurs over other systems:

- **Inexpensive** - Arduino boards are relatively inexpensive compared to other microcontroller platforms. The least expensive version of the Arduino module can be assembled by hand, and even the pre-assembled Arduino modules cost less than \$50
- **Cross-platform** - The Arduino Software (IDE) runs on Windows, Macintosh OSX, and Linux operating systems. Most microcontroller systems are limited to Windows.
- **Simple, clear programming environment** - The Arduino Software (IDE) is easy to-use for beginners, yet flexible enough for advanced users to take advantage of as well. For teachers, it's conveniently based on the Processing programming environment, so students learning to program in that environment will be familiar with how the Arduino IDE works.
- **Open source and extensible software** - The Arduino software is published as open-source tools, available for extension by experienced programmers. The language can be expanded through C++ libraries, and people wanting to understand the technical details can make the leap from Arduino to the AVR C programming language on which it's based. Similarly, you can add AVR-C code directly into your Arduino programs if you want to.
- **Open source and extensible hardware** - The plans of the Arduino boards are published under a Creative Commons license, so experienced circuit designers can make their own version of the module, extending it and improving it. Even relatively inexperienced users can build the breadboard version of the module in order to understand how it works and save money.

4.4.2 Embedded C:

Embedded C is a set of language extensions for the C Programming language by the C Standards committee to address commonality issues that exist between C extensions for different embedded systems. Historically embedded C programming requires nonstandard extensions to the C language in order to support exotic features such as fixedpoint arithmetic, multiple distinct memory banks, and basic I/O operations. Embedded C uses most of the syntax and semantics of standard C, e.g., main() function, variable definition, data type declaration, conditional statements(if,

switch, case), loops (while, for), functions, arrays and strings, structures and union, bit operations, macros, etc. During infancy years of microprocessor-based systems, programs were developed using assemblers and fused into the EPROMs. There used to be no mechanism to find what the program was doing. LEDs, switches, etc. were used to check for correct execution of the program. But they were too costly and were not quite reliable as well. As time progressed, use of microprocessor-specific assembly-only as the programming language reduced and embedded systems moved onto C as the embedded programming language of choice. C is the most widely used programming language for embedded processors/controllers.

4.4.3 Thingspeak

ThingSpeak is an open-source Internet of Things (IoT) platform that allows users to collect, analyze, and visualize data from IoT devices. It provides a cloud-based infrastructure that enables developers and researchers to build IoT applications quickly and easily.

- **Features:** ThingSpeak offers several features that make it suitable for IoT projects, including data collection and storage, data analysis, data visualization, and support for various IoT protocols such as MQTT and REST API. It also provides integration with other popular platforms such as MATLAB, which allows for advanced data analysis and processing.
- **Data Channels:** ThingSpeak uses data channels to store and manage data collected from IoT devices. Data channels are created based on specific fields, and each field can store a single value at a time. Users can define their own fields and specify data types such as numeric, string, or boolean, depending on the type of data being collected.

- **Data Visualization:** ThingSpeak offers built-in data visualization tools that allow users to create customizable charts, gauges, and maps to visualize their data in real-time. These visualizations can be embedded in websites or shared with others.
- **REST API:** ThingSpeak provides a REST API that allows developers to interact with the platform programmatically. This enables integration with other applications and systems, making it easy to collect and analyze data from IoT devices.
- **MATLAB Integration:** ThingSpeak has native integration with MATLAB, a popular data analysis and processing tool. This allows users to leverage the advanced data analysis capabilities of MATLAB for processing data collected from IoT devices.
- **Customizable IoT Applications:** ThingSpeak allows users to create their own customizable IoT applications by combining different features and tools. Users can define their own data channels, visualizations, and processing rules to build tailored IoT applications to suit their specific needs.
- **Security:** ThingSpeak provides security features such as SSL/TLS encryption, API key authentication, and user access control to ensure data privacy and security.
- **Community and Support:** ThingSpeak has an active community of users and developers who share knowledge, ideas, and resources related to IoT and

ThingSpeak. The platform also provides documentation, tutorials, and technical support to assist users in building their IoT projects.

- **Pricing:** ThingSpeak offers a free tier with limited features, as well as paid plans with additional features and higher usage limits. The pricing model is based on the number of data channels and the frequency of data updates.
- **Deployment Options:** ThingSpeak can be deployed on the cloud or on-premises, depending on the requirements of the project. It supports cloud hosting on the ThingSpeak.com platform or can be self-hosted on your own server.

4.5 BLOCK DIAGRAM

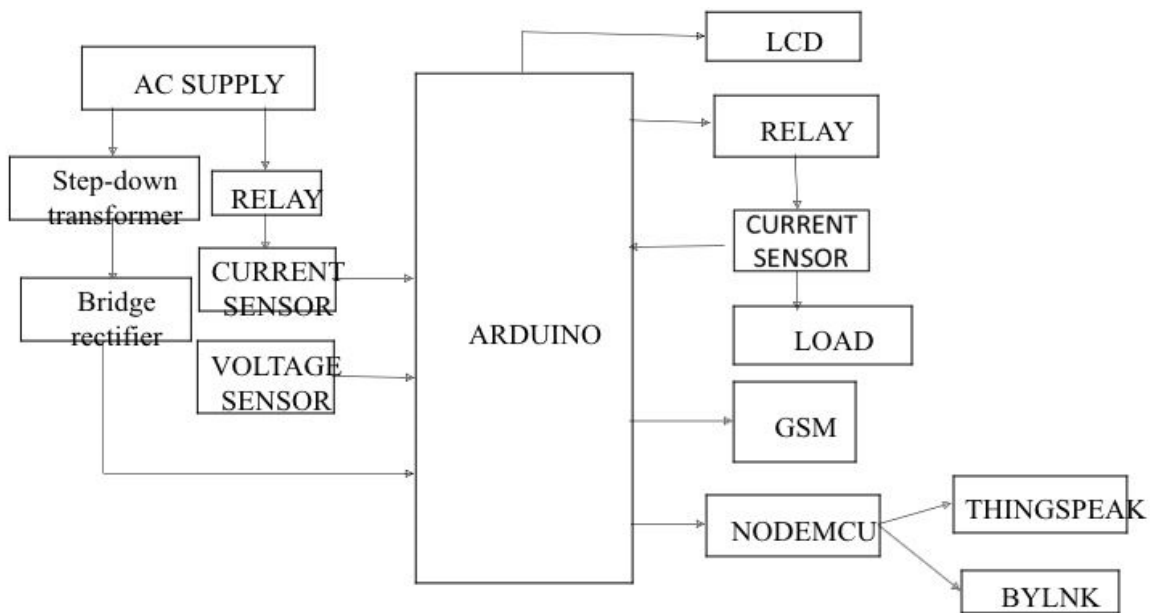


Fig 4.18 : Block diagram

4.6 PROPOSED SYSTEM EXPLANATION

Proposed a method to automate the billing process, better energy management and power theft on distribution lines. This system enables to collect the billing and theft detection data without utilizing manpower.

When the energy consumption exceeds the threshold value the heavy loads will be automatically disconnected.

The paper is concerned with the automation of the electric billing system. The electricity bill sends to office through GSM module.

An LCD display is connected with microcontroller to show the consumed units and cost. Bill records are digitized.

When the energy consumption is more than the threshold value the heavy loads in the home circuit will automatically tripped off using relays.

This method provides an indication system to aware the user about the over energy consumption than the threshold value and sends a SMS to consumers.

4.7 WORKING MODULES

- MODULE -1

Monitoring the current by using current flow. Current will get vary depending on the usage of the load.

- MODULE-2

In LCD, the current value and bill amount will display.

- MODULE-3

The values are sent to thingspeak using nodemcu.

- MODULE-4

The Bill amount automatically send to the consumer via SMS

- MODULE-5

If theft is detected automatically relay will get off.

T

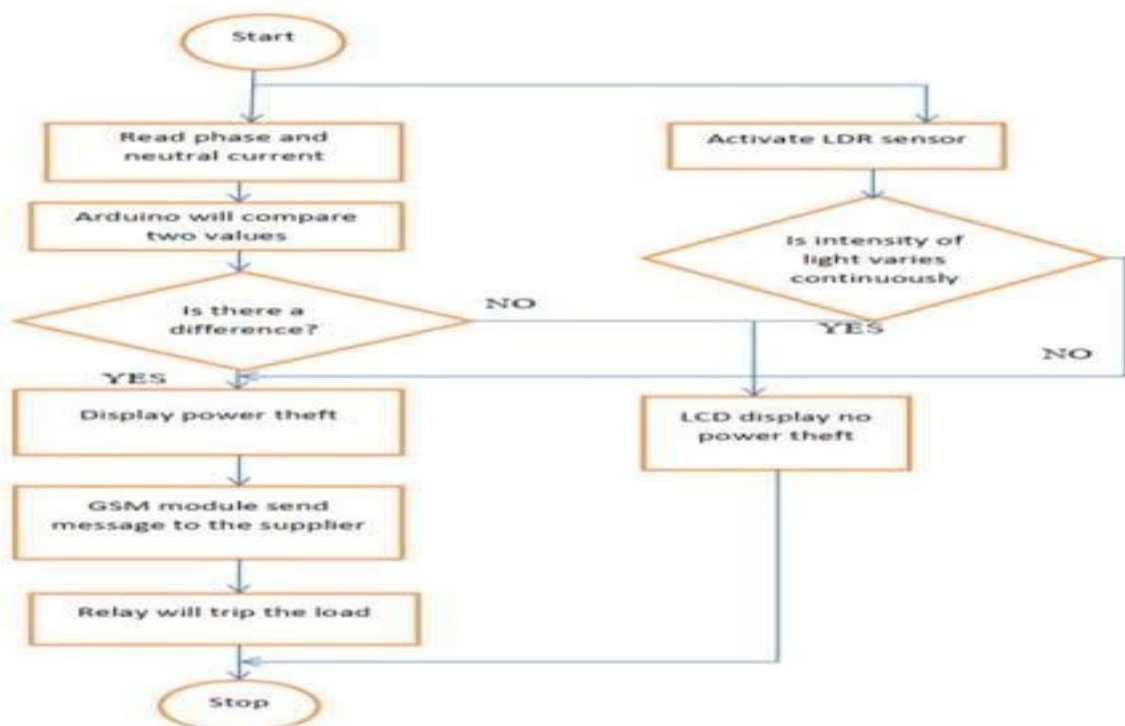


Fig 4.19: Methodology

4.8 ADVANTAGES

Improved detection accuracy: IoT-based solutions can provide real-time monitoring of electricity consumption, which can detect anomalies in the flow of electricity with

high accuracy. This can help in the early detection of electricity theft and reduce the number of false alarms.

Cost-effective: IoT-based solutions are often cost-effective, as they require fewer hardware components and can be easily integrated with existing electrical infrastructure.

Remote monitoring: IoT-based solutions can be monitored remotely, which reduces the need for physical inspections and enables faster response times to electricity theft incidents.

Easy to deploy: IoT-based solutions are relatively easy to deploy, as they do not require extensive modifications to the electrical infrastructure. This makes it possible to deploy them quickly and efficiently.

Scalability: IoT-based solutions are highly scalable, as additional sensors and devices can be easily added to the system as required. This makes it possible to monitor large-scale electrical infrastructure with ease.

Data analytics: IoT-based solutions can use data analytics and machine learning algorithms to analyze the data collected by the sensors. This can help to identify patterns and anomalies in the flow of electricity, which can improve the accuracy of electricity theft detection.

4.9 APPLICATIONS

- Automotive industry.
- Household application.

- Industrial application.

CHAPTER 5

RESULTS

5.1 HARDWARE OUTPUT

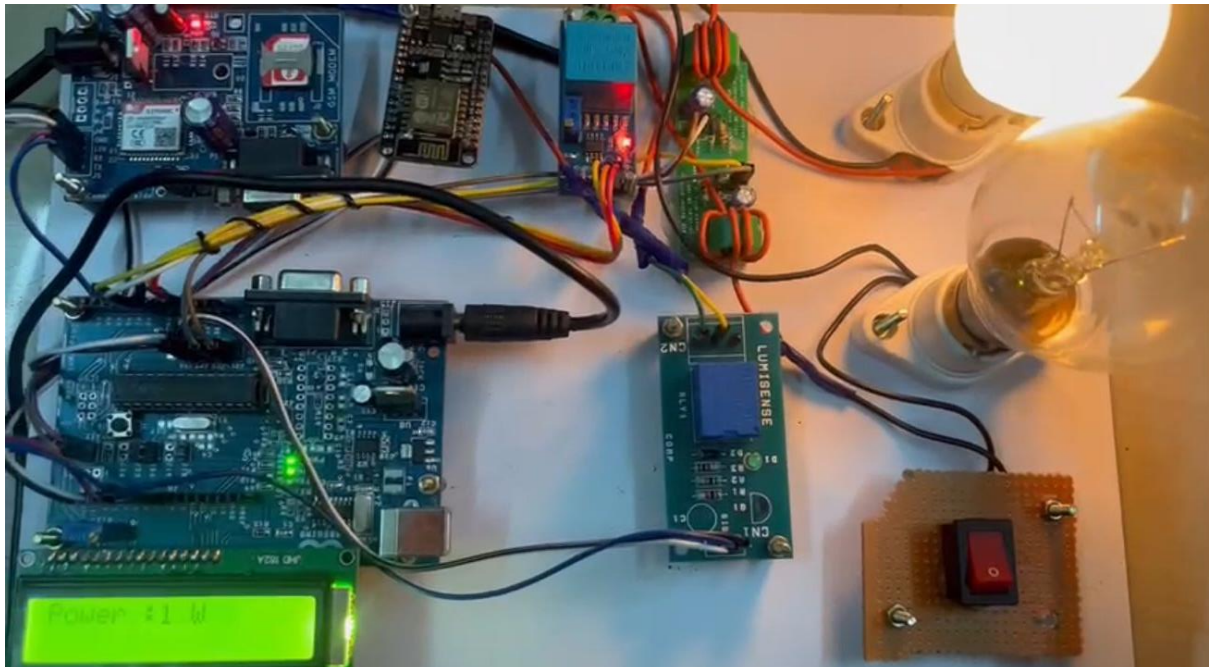


Fig 5.1: Hardware output

5.2 SIMULATION OUTPUT

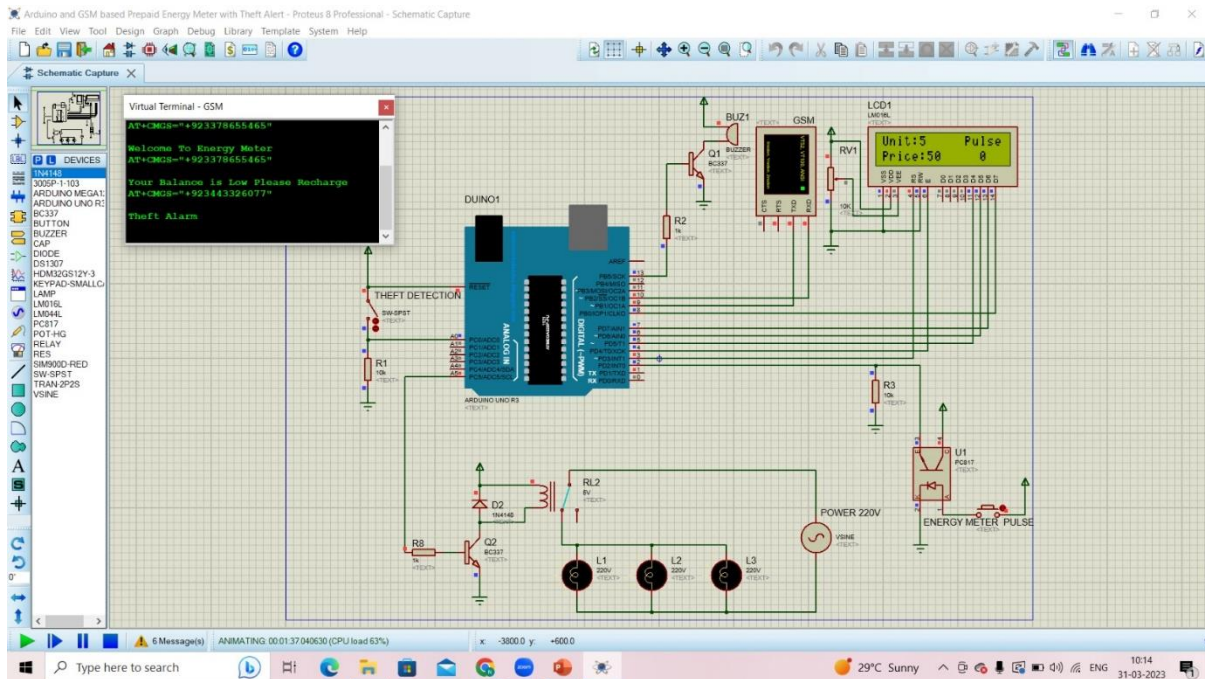


Fig 5.2: Simulation output

5.3 IOT DATA

The NodeMCU plays a vital role in this system, which senses the data from sensors and process the data. The Wi-Fi unit in the NodeMCU is used to send the data to the cloud, this data can be monitored continuously from anywhere in the world (where there is an active internet connection) and also whenever an excess current is detected at the supply the buzzer is activated to alert the administrator.

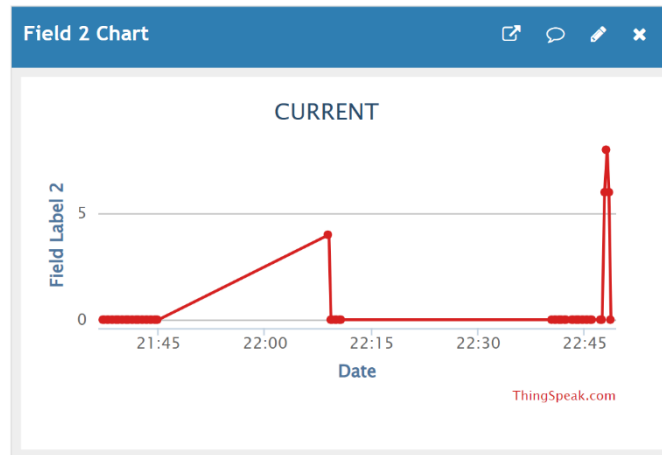


Fig 5.3: Photocopy of current graph using IOT

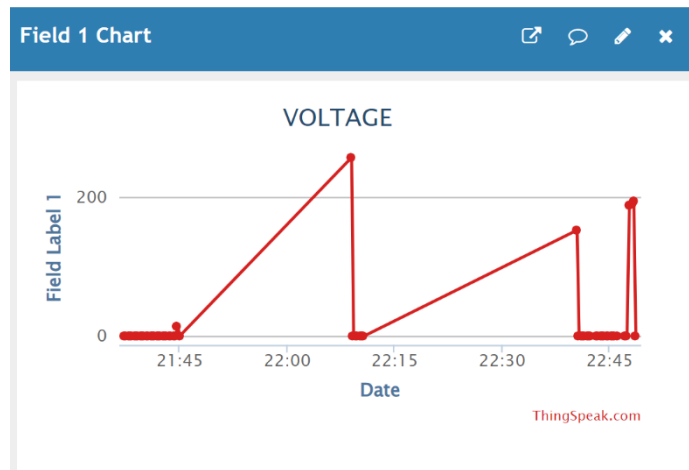


Fig 5.4: Photocopy of voltage graph using IOT

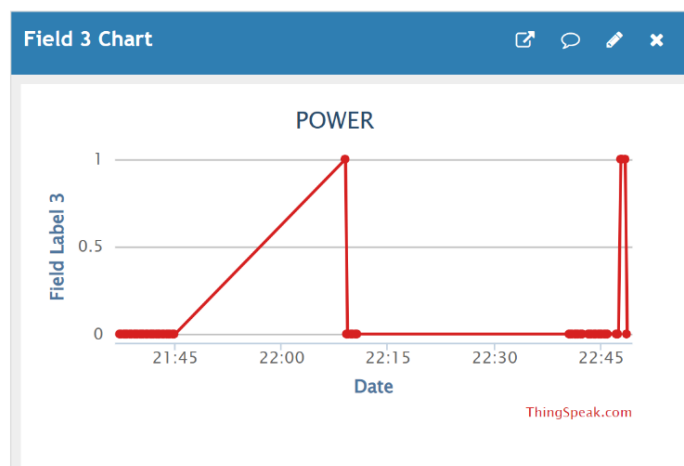


Fig 5.5: Photocopy of power graph using IOT

CHAPTER 6

SUMMARY AND CONCLUSIONS

6.1 SUMMARY

The use of IoT technology for the reduction of electricity theft is a promising solution that involves the deployment of sensors and devices that monitor the flow of electricity in real-time. The system can detect anomalies in the flow of electricity and send alerts to authorities, enabling them to take action and prevent electricity theft. The system can be powered by different power sources such as batteries, solar power, AC power, or energy harvesting. The methodology has several advantages, including improved detection accuracy, cost-effectiveness, remote monitoring, easy deployment, scalability, and the ability to use data analytics to improve detection accuracy. However, there are also constraints and tradeoffs that need to be considered, such as the cost of implementation and maintenance, and the need for a reliable and stable internet connection. Overall, the use of IoT technology for the reduction of electricity theft is a promising solution that can help to reduce energy losses and improve the efficiency of the power grid.

6.2 FUTURE SCOPE

Integration with smart grids: The integration of IoT-based electricity theft reduction systems with smart grids can help to improve the efficiency of the power grid and reduce energy losses. This can be achieved by using real-time data from IoT devices to optimize the distribution of electricity and reduce wastage.

Use of blockchain technology: The use of blockchain technology can help to enhance the security and transparency of the data collected by IoT devices, making it more difficult for hackers to tamper with the data.

Integration with AI and machine learning: The integration of AI and machine learning algorithms can help to improve the accuracy of electricity theft detection by analyzing patterns in the data collected by IoT devices.

Expansion to other industries: The use of IoT-based systems for the reduction of theft can be expanded to other industries such as oil and gas, where theft is also a major concern.

Adoption by governments: Governments can adopt IoT-based systems to reduce electricity theft, which can help to improve the efficiency of the power grid and reduce energy losses. This can also help to increase revenue for energy providers and reduce the burden on taxpayers.

6.3 CONCLUSION

A Wireless Electricity Theft Detection and monitoring system has been designed and developed with proper integration of both the hardware and the software. Without any human interface this system provides an effective and easy way to detect electrical theft. The use of IoT helps in achieving the numerous advantages of wireless network communications. Power theft is actually bypassing the energy meter but in our project we have indicated the theft by increasing the load also and this method is cost efficient. The design, simulation and construction of a IOT-based power theft have been achieved. It has covered various forms of electricity theft which include unaccountability of servicemen, irregularities of billing leading to a reduction of funds by the utility companies has also been achieved as this work prevents one on one contact between the end user and the workers. With remote monitoring of the meter reading and sending SMS, whenever there are abnormal readings, in the customer electricity meter, the developed system may able to help Utilities to reduce the

incidences of household electricity theft. An automatic circuit breaker can be integrated into the unit so as to remotely cut off the power supply to the house or consumer who tries to indulge in power theft. This system design mainly concentrates on single phase electrical distribution system. Automation of the customer billing system has been achieved as the meter keeps track of the consumer's load on a timely basis. This design, therefore, removes the manual reading of meters with its attached consequences of time-consuming system and bill manipulation which affects the company while adding higher bills to the consumer.

REFERENCES

- [1] A. K. Gupta, A. Mukherjee, A. Routray and R. Biswas, "A novel power theft detection algorithm for low voltage distribution network," IECON 2017 - 43rd Annual Conference of the IEEE Industrial Electronics Society, Beijing, 2017, pp. 3603-3608.
- [2] M. Golden, B. Min, "Theft and loss of electricity in an Indian State technical report," Int. Growth Centre 2012.
- [3] Navani JP, Sharma NK and Sapra S. "Technical and non-technical losses in power system and its economic consequence in Indian economy," Int J Electron Comp Sci Eng, Vol 1, pp. 757–61, 2012.
- [4] W. Han and Y. Xiao, "NFD: A practical scheme to detect non-technical loss fraud in smart grid," 2014 IEEE International Conference on Communications (ICC), Sydney, NSW, 2014, pp. 605-609.
- [5] ECI Telecom Ltd., Fighting Electricity Theft with Advanced Metering Infrastructure (March 2011)
- [6] J. Nagi, K. S. Yap, S. K. Tiong, S. K. Ahmed and M. Mohamad, "Nontechnical Loss Detection for Metered Customers in Power Utility Using Support Vector Machines," in IEEE Transactions on Power Delivery, vol. 25, no. 2, pp. 1162-1171, April 2010.
- [7] S.S.S.R. Depuru, "Modeling, Detection, and Prevention of Electricity Theft for Enhanced Performance and Security of Power Grid," The University of Toledo, Aug. 2012.
- [8] J. Nagi, K.S. Yap, S.K. Tiong, S.K. Ahmed, and A.M. Mohammad, "Detection of abnormalities and electricity theft using genetic support vector machines," Proc. IEEE Region 10 Conference TENCON, Hyderabad, India, Jan. 2009, pp. 1–6.
- [9] S. Sahoo, D. Nikovski, T. Muso, and K. Tsuru, "Electricity theft detection using smart meter data," in Innovative Smart Grid Technologies Conference (ISGT), IEEE Power and Energy Society, 2015.
- [10] S. A. Salinas and P. Li, "Privacy-Preserving Energy Theft Detection in Microgrids: A State Estimation Approach," IEEE Trans. Power Syst., vol. 31, no. 2, pp. 883 - 894, 2016 .

