# IoT BASED POWER THEFT DETECTOR

## MINI PROJECT REPORT

*Submitted in partial fulfillment of*
*the requirements for the award of the B.Tech Degree in*
*Electronics and Communication Engineering*
*from the APJ Abdul Kalam Technological University*


*Submitted by*
*ABHIJITH B (SCT22EC003)*
*ANASWARA S KUMAR (SCT22EC031)*




**DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING**
**SREE CHITRA THIRUNAL COLLEGE OF ENGINEERING,**
**THIRUVANANTHAPURAM-695018**

**MARCH 2025**

**DEPT. OF ELECTRONICS AND COMMUNICATION ENGINEERING**

**SREE CHITRA THIRUNAL COLLEGE OF ENGINEERING, PAPPANAMCODE**

2024-25


# CERTIFICATE

Certified that the mini project entitled **"IoT BASED POWER THEFT DETECTOR"** is a bonafide report submitted by **Abhijith B (SCT20EC003) and Anaswara S Kumar (SCT20EC031)** in partial fulfillment of the requirements for the award of the Degree of Bachelor of Technology in Electronics and Communication from the APJ Abdul Kalam Technological University under our guidance and supervision. This report in any form has not been submitted to any other University or Institute for any purpose.

**Dr. Renjith R J**
**Project Guide**
**Assistant Professor**
**Dept. of ECE**
**SCTCE**

**Smt. Aparna P R**
**Project Coordinator**
**Assistant Professor**
**Dept. of ECE**
**SCTCE**

**Dr. Nisha Jose K**
**Head of the Department**
**Dept. of ECE**
**SCTCE**

# DECLARATION

We, the undersigned hereby declare that the project report "IoT Based Power Theft Detector", submitted for partial fulfillment of the requirements for the award of the degree of Bachelor of Technology of the APJ Abdul Kalam Technological University, Kerala is a bona fide work done by me under supervision of Smt. Aparna P R, Assistant Professor, Department of Electronics and Communication Engineering. This submission represents our ideas in our own words and where ideas or words of others have been included, we have adequately and accurately cited and referenced the original sources. We also declare that we have adhered to the ethics of academic honesty and integrity and have not misrepresented or fabricated any data or idea or fact or source in our submission. We understand that any violation of the above will be a cause for disciplinary action by the institute and/or the University and can also evoke penal action from the sources which have thus not been properly cited or from whom proper permission has not been obtained. This report has not been previously formed as the basis for the award of any degree, diploma, or similar title of any other University.

Thiruvananthapuram
18th March, 2025

Abhijith B (SCT20EC003)
Anaswara S Kumar (SCT22EC031)

# ACKNOWLEDGEMENT

We take this opportunity to thank all the people without whom the conception and realization of this project would not have been possible.

Let us start with our deep gratitude towards **Prof. (Dr) C. Sathish Kumar**, The Principal of Sree Chitra Thirunal College of Engineering, Trivandrum, for providing us with the opportunity and necessary facilities for the completion of the project.

We acknowledge our sincere gratitude to **Dr. Nisha Jose K**, Head of the Department, Dept. of Electronics Communication Engineering, for her valuable suggestions and advice during the course of work.

We are immensely indebted to **Smt. Aparna P R**, (project coordinator), Assistant Professor, Dept. of Electronics Communication Engineering, for her kind co-operation and encouragement in conceiving the idea of the project and guiding us in every phase of work. We thank her from the bottom of our hearts for helping us and giving valuable suggestions for completing the project.

We would like to convey our sincere thanks to the guide, **Dr. Renjith R J**, Assistant Professor, Dept. of Electronics Communication Engineering for providing full-fledged support in making this project a success.

We are happy to thank other faculty members, technical and administrative staff of the Department of Electronics Communication Engineering for their valuable support and heartfelt cooperation.

We are greatly obliged to our friends for the unbounded cooperation they have extended to us, directly or indirectly to carry out our project. Last but not least we thank our families for giving us mental support and enabling us to work efficiently on the project. Finally, we offer my earnest gratitude to the invisible hands of the Almighty that lead us forward during each and every stage of this endeavor.

# ABSTRACT

Power theft remains a significant challenge for utility providers, leading to financial losses and safety hazards.In the society it was seen lot of people doing illegal power theft like unauthorized tapings from lines during functions and meter bypassing etc.Energy, particularly electricity, is a key input for accelerating economic growth. The theft of
electricity is a criminal offence and power utilities are losing billions of rupees in this account.
World losses US$89.3 billion annually to electricity theft. The highest losses were in India
($16.2 billion), followed by Brazil ($10.5 billion) and Russia ($5.1 billion).

This project, titled "IoT-Based Power Theft Detector," aims to develop an innovative, cost-effective solution to monitor and detect unauthorized power consumption using Internet of Things (IoT) technology. The system integrates current sensors (ZMCT103C) to measure the current drawn by legal and illegal loads, represented by 10W LEDs powered through an inverter and lead acid battery setup. An Arduino UNO microcontroller processes the sensor data, displaying real-time current readings on a 16x2 LCD with an I2C module. When the illegal load current exceeds a predefined threshold (0.1A), the system identifies a theft event, displays "THEFT DETECTED!" on the LCD, and triggers an ESP8266 (NodeMCU) module to send an email notification to a specified user address via Gmail's SMTP server. The Arduino UNO is powered externally by two 3.7V 2000mAh 18650 Li-ion batteries, ensuring off-grid operation. Testing results demonstrate reliable current monitoring, accurate theft detection within 5 seconds, and successful email notifications, validating the system's effectiveness. This project offers a scalable solution for power theft prevention, with potential applications in utility management, smart homes, and rural electrification, paving the way for future enhancements such as mobile app integration and solar-powered operation.

## CONTENTS

# LIST OF FIGURES

# LIST OF TABLES

# LIST OF ABBREVIATIONS AND SYMBOLS

| | |
|---|---|
| AC | ALTERNATING CURRENT |
| AREF | ANALOG REFERENCE |
| BPS | BITS PER SECOND |
| DC | DIRECT CURRENT |
| GPIO | GENERAL PURPOSE INPUT/OUTPUT |
| GSM | GLOBAL SYSTEM FOR MOBILE COMMUNICATIONS |
| I2C | INTER-INTEGRATED CIRCUIT |
| ICSP | IN-CIRCUIT SERIAL PROGRAMMING |
| IDE | ARDUINO INTEGRATED DEVELOPMENT ENVIRONMENT |
| IOT | INTERNET OF THINGS |
| LCD | LIQUID CRYSTAL DISPLAY |
| LED | LIGHT EMITTING DIODE |
| NTL | NON-TECHNICAL LOSSES |
| PLCC | POWER LINE CARRIER COMMUNICATION |
| PWM | PULSE WIDTH MODULATION |
| RX | RECEIVER |
| SCADA | SUPERVISORY CONTROL AND DATA ACQUISITION |
| SCK | SERIAL CLOCK |
| SCL | SERIAL CLOCK |
| SDA | SERIAL DATA |
| SLA | SEALED LEAD ACID |
| SMTP | SIMPLE MAIL TRANSFER PROTOCOL |
| SPI | SERIAL PERIPHERAL INTERFACE |
| SRAM | STATIC RANDOM ACCESS MEMORY |
| TL | TECHNICAL LOSSES |
| TLS | TRANSPORT LAYER SECURITY |
| TX | TRANSMITTER |
| VCC | VOLTAGE COMMON COLLECTOR |

# CHAPTER 1
# INTRODUCTION

Internet of Things is a term used for a system where devices are given IP addresses, and everybody makes the device recognizable on the internet via that IP address. The web, which started with the internet of computers, is developing. Researchers have predicted a volatile increase in the number of sensors, devices, or “things” connected to the internet. The product network is known as the Internet of Things (IoT) . IoT has the propensity to alter people’s lifestyles. People prefer to monitor things through automatic systems in today’s
world rather than through any manual system together with the circuitry driving the system, which are the main elements of the IoT-based electricity theft detection system introduced in this project. An economy's production and consumption of electricity are key determinants of its size and development, electricity theft slows economic growth. Even though exporting electric power is rarely profitable, most of it is produced for domestic use. Even though only a few nations profit from the export of electric power, the majority of it is used for domestic consumption in developing nations.

Most developing countries have suffered undesirable economic consequences to meet the demands of electricity for real estate and industrialization due to electricity theft. According to the World Bank's development indicator collection, the percentage of distribution and losses due to transmission in Ghana was 23% in 2014, gathered from officially recognized sources. Reducing transmission and distribution losses is the greatest challenge to power utility authorities.

We can categorize the losses into technical (TL) as well as non-technical (NTL) . Technical losses are in-built into the system which is reduceable to an appreciable level; the remaining is due to power dissipated in equipment and conductions used for the distribution and transmission lines NTL happens due to inaccuracy of metering, stealing, or theft of electricity, as well as energy consumed but unrecorded by the energy meter.

Electricity theft is the energy consumed by a customer that is unaccounted for or not measured by the energy meter. 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 of electricity. Overall technical losses occur naturally and are caused because of power dissipation in transmission lines, transformers, and other power system components. Technical losses in Transmission &Distribution are computed with the information about total load and the total

energy bill. While technology in the raising slopes, we should also note the increasing immoral activities. With a technical view, Power Theft is a non ignorable crime and at the same time it directly affected the economy of a nation. Electricity theft a social evil, so it has to be completely eliminated. Power consumption and losses have to be closely monitored so that the generated power is utilized in a most efficient manner. The system prevents the illegal usage of electricity. At this point of technological development the problem of illegal usage of electricity can be solved without any human control using GSM or ES .

The implementation of this system will save large amount of electricity, and there by electricity will be available for more number of consumer then earlier, in highly populated country such as India, China. Power theft can be defined as the usage of the electrical power without any legal contract with the supplier.

### 1.1 AIM & OBJECTIVE

The aim and objectives of our mini-project are: -

- To develop a real-time power theft detection system.
- To monitor electricity consumption and detect anomalies using IoT.
- To provide remote monitoring capabilities for utility providers.
- To notify authorities in case of power theft using cloud alerts.

## 1.2 SCOPE OF THE MINI PROJECT

The IoT-Based Power Theft Detector has vast applications in modern power management and smart grid infrastructure. This project addresses the critical issue of electricity theft while ensuring real-time monitoring, automated detection, and preventive measures.

a. Application in Power Distribution Systems

- Can be implemented in urban and rural power grids to detect unauthorized power usage.
- Helps electricity boards and power distribution companies reduce revenue losses.
- Improves grid stability by ensuring proper load distribution.

b. Smart Metering & Automated Billing

- Can be integrated with smart meters to ensure tamper-proof energy monitoring.
- Allows automated electricity billing based on actual usage.
- Prevents billing discrepancies and ensures fairness.

c. Real-Time Theft Detection & Alerts

- Uses IoT for real-time monitoring, allowing immediate action upon theft detection.
- Provides alerts via SMS, email, or IoT dashboard notifications.
- Reduces the need for manual inspections and improves response time.

d. Integration with Government Policies & Smart City Initiatives

- Supports government initiatives aimed at reducing energy losses.
- Can be deployed as part of smart grid modernization efforts.
- Helps utilities achieve energy efficiency goals by eliminating theft-related losses.

e. Scalability & Future Enhancements

- Can be scaled for large-scale deployment across multiple cities and regions.
- Potential for machine learning (ML) and artificial intelligence (AI) integration to improve theft detection accuracy.

- Can incorporate blockchain technology to ensure secure and tamper-proof energy transactions.

f. Cost-Effective & Easily Implementable Solution

- Low-cost hardware components make the system affordable for widespread adoption.
- Uses open-source IoT platforms for cost-effective data monitoring.
- Can be implemented in both developed and developing countries to reduce losses.

g. Environmental Impact

- Helps in reducing unnecessary power wastage, thus contributing to energy conservation.
- Encourages fair electricity distribution and ensures sustainable energy usage.
- Supports renewable energy monitoring, ensuring power theft does not hinder clean energy initiatives.

## 1.3 ORGANIZATION

The report on the IoT Based Power Theft Detector starts with Chapter 1 which introduces the mini project with the motivation and significance of the product. Chapter 2 provides the literature review that mentions the thesis and articles we have referred to for conducting the mini-project. Chapter 3 describes the hardware requirements of the mini-project whereas, Chapter 4 explains the methodology. Chapter 5 illustrates the results we observed. The cost analysis of the mini-project is depicted in Chapter 6. We have concluded the report with Chapter 7.

# CHAPTER 2
# LITERATURE SURVEY

The **IoT-Based Power Theft Detector** builds upon existing research and methodologies in power monitoring, electricity theft prevention, and smart grid technologies. This chapter explores previous work, existing solutions, and advancements in IoT-based power monitoring

## 2.1 Traditional Power Theft Detection Methods

Electricity theft has been a major challenge for power utilities worldwide, leading to financial losses, power instability, and safety hazards. Several conventional methods have been used to detect and prevent theft:

### a. Manual Inspections

- Traditional power theft detection relies on physical audits conducted by utility personnel.
- Disadvantages: Labor-intensive, costly, and time-consuming; does not provide real-time monitoring.

### b. Tamper-Proof Meters

- Smart meters with anti-tampering mechanisms have been introduced.
- Disadvantages: High initial cost; can still be bypassed by advanced tampering techniques.

### c. Power Line Carrier Communication (PLCC) & SCADA Systems

- Uses communication signals over power lines to detect unauthorized power usage.
- Disadvantages: Expensive, requires major infrastructure upgrades, limited to high-end power distribution networks.

### d. Statistical Analysis & Machine Learning (ML) Approaches

- Studies have explored ML-based anomaly detection using consumption patterns.
- Disadvantages: Requires large datasets for accuracy; limited real-time response.

### 2.2 Smart Grid & IoT-Based Solutions for Power Theft Detection

With advancements in Internet of Things (IoT) and smart metering technologies, new automated and real-time monitoring systems have been proposed to replace manual and reactive power theft detection methods.

#### a. IoT-Based Smart Meters

- **Authors**: Kaur et al. (2020) proposed a smart metering system using IoT.
- **Findings**: Smart meters can provide real-time monitoring, automated data collection, and remote access to electricity usage.
- **Limitations**: High cost of deployment, requires stable internet connectivity.

#### b. Power Theft ( Fourth Edition)

- **Author:** G Sreenivasan (2017) Educates and sensitises people about the menace of power theft
- **Findings:** Power theft, a major issue causing financial losses and grid instability, occurs through illegal tapping and meter tampering, while smart meters and legal enforcement aid in its detection and prevention.
- **Limitations:** Privacy concerns, high implementation costs, technical challenges, and socio-economic factors contribute to the complexities of power theft detection and prevention, requiring broader interventions.

#### c. AI & Machine Learning-Based Anomaly Detection

- **Authors:** Zhang et al. (2022) investigated machine learning models for identifying abnormal power consumption.
- **Findings:** AI models analyze power consumption patterns and predict potential theft.
- **Limitations:** High computational power requirements, difficulty in real-time implementation.

# CHAPTER 3
# HARDWARE REQUIREMENT

This chapter provides a detailed overview of all hardware and software components used in the **IoT-Based Power Theft Detector**, including their specifications, working principles, and integration in the system.

## 3.1 ARDUINO UNO

The Arduino UNO is the central processing unit of this project. It collects data from sensors, processes the information, and triggers alerts when power theft is detected. The Arduino UNO is an open-source microcontroller board based on the ATmega328P microcontroller, commonly used for IoT and embedded systems applications. The Arduino UNO should be selected based on the specific requirements of the project, considering factors such as memory, processing speed, and available interfaces.

### 3.1.1 Features and Specifications

The technical specifications are given in table 3.1 and pin specifications are given in table 3.2.


Fig. 3.1. Arduino UNO

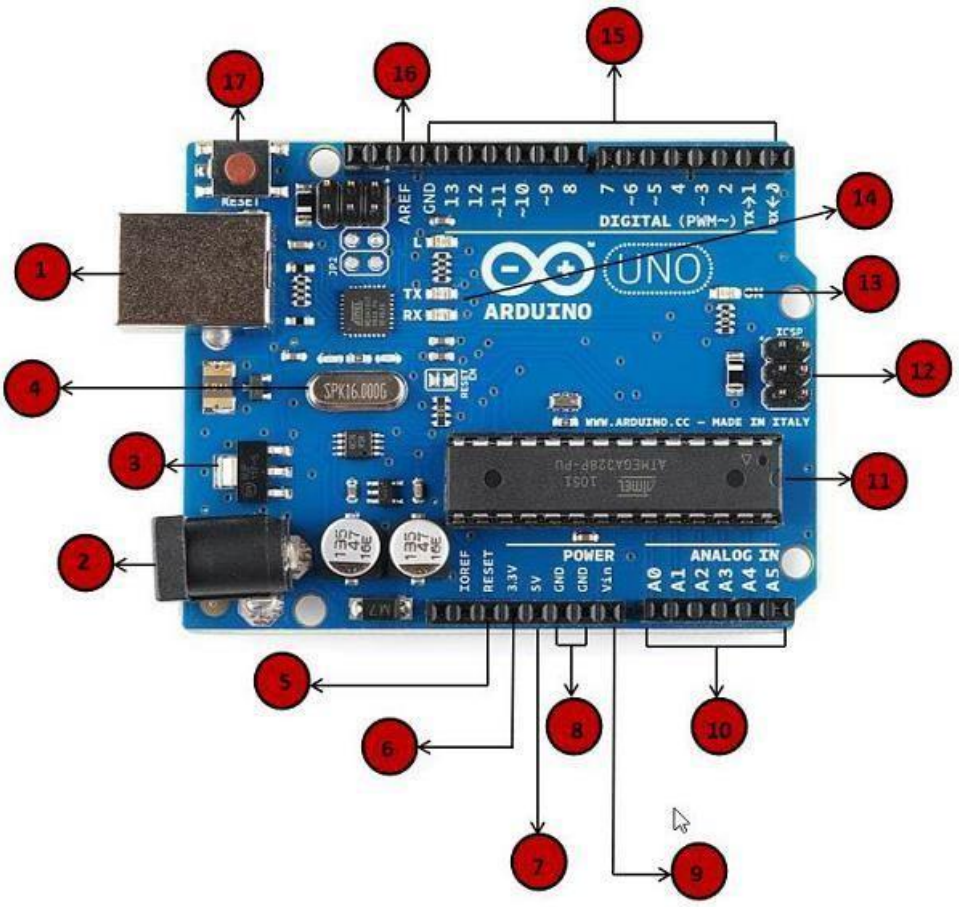


Fig. 3.2. Pin Diagram of Arduino UNO

**PINS**

a. **Power USB**

Arduino board can be powered by using the USB cable from your computer. All you need to do is connect the USB cable to the USB connection(1).

b. **Power (Barrel Jack)**

Arduino boards can be powered directly from the AC mains power supply by connecting it to the Barrel Jack (2).

c. **Voltage Regulator**

The function of the voltage regulator is to control the voltage given to the Arduino board and stabilize the DC voltages used by the processor and other elements.

d. **Crystal Oscillator**

The crystal oscillator helps Arduino in dealing with time issues. How does Arduino calculate time? The answer is, by using the crystal oscillator. The number printed on top of the Arduino crystal is 16.000H9H. It tells us that the frequency is 16,000,000 Hertz or 16 MHz.

e. **Arduino Reset**

You can reset your Arduino board, i.e., start your program from the beginning. You can reset the UNO board in two ways. First, by using the reset button (17) on the board. Second, you can connect an external reset button to the Arduino pin labelled RESET (5).

f. **Pins (3.3, 5, GND, Vin)**

3.3V (6) − Supply 3.3 output volt

5V (7) − Supply 5 output volt

Most of the components used with Arduino board works fine with 3.3 volt and 5 volt.

GND (8)(Ground) − There are several GND pins on the Arduino, any of which can be used to ground your circuit.

Vin (9) − This pin also can be used to power the Arduino board from an external power source, like AC mains power supply.

g. **Analog pins**

The Arduino UNO board has five analog input pins A0 through A5. These pins can read the signal from an analog sensor like the humidity sensor or temperature sensor and convert it into a digital value that can be read by the microprocessor.

h. **Main microcontroller**

Each Arduino board has its own microcontroller (11). You can assume it as the brain of your board. The main IC (integrated circuit) on the Arduino is slightly different from board to board. The microcontrollers are usually of the ATMEL Company. You must know what IC your board has before loading up a new program from the Arduino IDE. This information is available on the top of the IC. For more details about the IC construction and functions, you can refer to the data sheet.

i. **ICSP pin**

Mostly, ICSP (12) is an AVR, a tiny programming header for the Arduino consisting of MOSI, MISO, SCK, RESET, VCC, and GND. It is often referred to as an SPI (Serial Peripheral Interface), which could be considered as an "expansion" of the output. Actually, you are slaving the output device to the master of the SPI bus.

j. **Power LED indicator**

This LED should light up when you plug your Arduino into a power source to indicate that your board is powered up correctly. If this light does not turn on, then there is something wrong with the connection.

k. **TX and RX LEDs**

On your board, we can find two labels: TX (transmit) and RX (receive). They appear in two places on the Arduino UNO board. First, at the digital pins 0 and 1, to indicate the pins responsible for serial communication. Second, the TX and RX led (13). The TX led flashes with different speed while sending the serial data. The speed of flashing depends on the baud rate used by the board. RX flashes during the receiving process.

l. **Digital I/O**

The Arduino UNO board has 14 digital I/O pins (15) (of which 6 provide PWM (Pulse Width Modulation) output. These pins can be configured to work as input digital pins to read logic values (0 or 1) or as digital output pins to drive different modules like LEDs, relays, etc. The pins labeled "~" can be used to generate PWM.

m. **AREF**

AREF stands for Analog Reference. It is sometimes, used to set an external reference voltage (between 0 and 5 Volts) as the upper limit for the analog input pins.

| Feature | Description |
|---|---|
| Microcontroller | ATmega328P (8-bit AVR) |
| Operating Voltage | 5V |
| Input Voltage (Recommended) | 7V - 12V |
| Digital I/O Pins | 14 (6 PWM outputs) |
| Analog Input Pins | 6 |
| Flash Memory | 32 KB (0.5 KB used by bootloader) |
| SRAM | 2 KB |
| EEPROM | 1 KB |
| Clock Speed | 16 MHz |

Table 3.1. Arduino UNO Technical Specifications

| Pin Name | Description |
|---|---|
| A0 | Connected to ZMCT103C (legal load) |
| A1 | Connected to ZMCT103C (illegal load) |
| A4 (SDA) | Connected to LCD SDA (via logic level converter) |
| A5 (SCL) | Connected to LCD SCL (via logic level converter) |
| D2 (RX) | Connected to ESP8266 TX (via logic level converter) |
| D3 (TX) | Connected to ESP8266 RX (via logic level converter) |
| 5V, GND | Power for sensors, LCD, and ESP8266 |
| VIN, GND | Connected to 18650 battery pack (~7.4V) |

Table 3.2. Arduino UNO Pinout Configuration

## 3.2 LEAD ACID BATTERY

The lead acid battery serves as the primary power source for the inverter in the IoT-Based Power Theft Detection System. It provides a stable 12V DC output, which is converted to 220V AC by the inverter to power the legal and illegal 10W LEDs. This type of battery is chosen for its reliability, cost-effectiveness, and suitability for small-scale off-grid applications, ensuring consistent power delivery during testing.

### 3.2.1 Features and Specifications

The technical specifications are given in table 3.3 and pin specifications are given in table 3.4.


Fig. 3.3. Lead Acid Battery

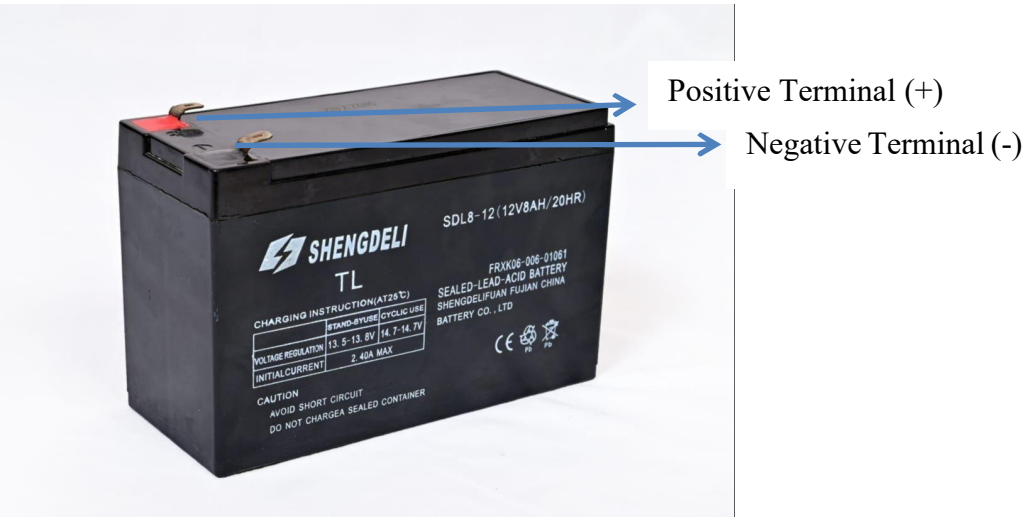


Fig. 3.4. Pin Configuration of Lead Acid Battery

| Feature | Description |
|---|---|
| Type | Sealed Lead Acid (SLA) |
| Voltage | 12V |
| Capacity | Suitable for 20W load (e.g., 7Ah) |
| Application | Powers the inverter for LED loads |

Table 3.3. Lead Acid Battery Technical Specifications

| Pin Name | Description |
|---|---|
| Positive Terminal (+) | Connected to the inverter input |
| Negative Terminal (-) | Connected to the inverter ground |

Table 3.4. Lead Acid Battery Pinout Configuration

### 3.3 INVERTER (12V - 220V)

The inverter is a crucial component that converts the 12V DC output from the lead acid battery into 220V AC to power the legal and illegal 10W LEDs, simulating real-world power consumption scenarios. It supports small loads, making it ideal for testing purposes in this project. The inverter ensures that the LEDs operate at their rated voltage, allowing the current sensors to monitor consumption accurately.

#### 3.3.1 Features and Specifications

The technical specifications are given in table 3.5 and pin specifications are given in table 3.6.

Fig. 3.5. Inverter (12V - 220V)

| Feature | Description |
|---|---|
| Input Voltage | 12V DC |
| Output Voltage | 220V AC |
| Capacity | Supports up to 20W load |
| Efficiency | ~85% |

Table 3.5. Inverter (12v-220v) Technical Specifications

| Pin Name | Description |
|---|---|
| Input (+) | Connected to the lead acid battery positive terminal (12V) |
| Input (-) | Connected to the lead acid battery negative terminal (ground) |
| Output (AC Live) | Connected to the legal and illegal 10W LEDs (live wire) |
| Output (AC Neutral) | Connected to the legal and illegal 10W LEDs (neutral wire) |

Table 3.6. Inverter (12v-220v) Pinout Configuration

### 3.4 CURRENT TRANSFORMER ( WITH ZMCT103C )

The current transformer, used in conjunction with the ZMCT103C module, enables non-invasive measurement of AC current flowing through the legal and illegal loads. It works by passing the mains wire (carrying the current to the LEDs) through its core, inducing a proportional current in the secondary winding. This setup ensures safe and accurate current monitoring, which is essential for detecting unauthorized power usage in the system.

#### 3.4.1 Features and Specifications

The technical specifications are given in table 3.7 and pin specifications are given in table 3.8.

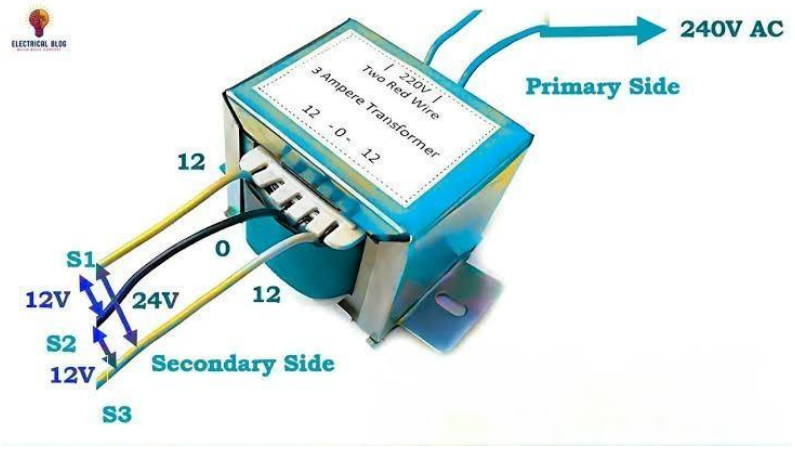


Fig. 3.6. Current Transformer

| Feature | Description |
|---|---|
| Current Range | Up to 5A |
| Turns Ratio | 1000:1 (5A primary → 5mA secondary) |
| Breakdown Voltage | Up to 4.5kV |
| Application | Non-invasive AC current measurement |

Table 3.7. Current Transformer ( with ZMCT103C ) Technical Specifications

| Pin Name | Description |
|---|---|
| Primary Winding | Mains wire (phase or neutral) passes through the core |
| Secondary Winding | Connected to ZMCT103C module for voltage output |

Table 3.8. Current Transformer ( with ZMCT103C ) Pinout Configuration

## 3.5 LEGAL 10W LED

The legal 10W LED represents the authorized load in the system, simulating legitimate power consumption. It operates on 220V AC supplied by the inverter and draws approximately 0.045A, providing a baseline for comparison with the illegal load. The LED's power consumption is monitored by the ZMCT103C sensor connected to the Arduino Uno's A0 pin, allowing the system to differentiate between legal and illegal usage.

### 3.5.1 Features and Specifications

The technical specifications are given in table 3.9 and pin specifications are given in table 3.10.

Fig. 3.7. 10W LED BULB

| Feature | Description |
|---|---|
| Power | 10W |
| Voltage | 220V AC |
| Current | ~0.045A (at 220V) |
| Application | Simulates authorized load |

Table 3.9. LED Bulb Technical Specifications

| Pin Name | Description |
|---|---|
| Positive (L) | Connected to inverter AC output (live) |
| Negative (N) | Connected to inverter AC output (neutral) |

Table 3.10. LED Bulb Pinout Configuration

## 3.6 ZMCT103C CURRENT SENSOR

The ZMCT103C is a high-precision micro current transformer module that measures AC current up to 5A. It converts the current passing through the current transformer into a proportional voltage, which is then read by the Arduino Uno. In this project, two ZMCT103C sensors are used: one for the legal load (A0) and one for the illegal load (A1). This setup enables the system to detect discrepancies in power consumption, identifying theft when the illegal load is active.

### 3.6.1 Features and Specifications

The technical specifications are given in table 3.11 and pin specifications are given in table 3.12.

**High Accuracy:** The sensor provides ±0.5% accuracy, making it ideal for energy monitoring applications.

**Low Power Consumption:** Operates at low voltage (5V DC), making it energy-efficient.

Compact Size: Small PCB footprint (38mm x 25mm) allows easy integration into embedded systems.

**Safe Isolation:** Provides high electrical isolation (3kV), ensuring safety while measuring AC currents.

**Fast Response Time:** Detects power fluctuations in <200ms, enabling real-time monitoring.

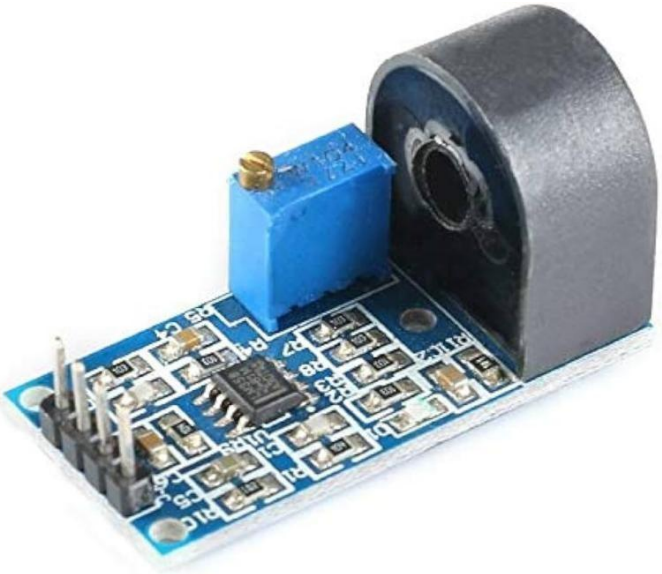

Fig. 3.8. ZMCT103C Current Sensor Module

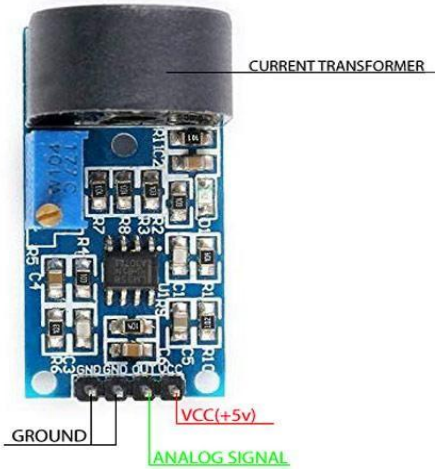


Fig. 3.9. Pin Diagram of ZMCT103C Current Sensor

| Feature | Description |
|---|---|
| Current Range | 0-5A |
| Turns Ratio | 1000:1 |
| Output | 1V at 5A (with burden resistor) |
| Operating Voltage | 5V DC |

Table 3.11. ZMCT103C Current Sensor Technical Specifications

| Pin Name | Description |
|---|---|
| OUT | Connected to Arduino A0 (legal load) and A1 (illegal load) |
| VCC | Connected to Arduino 5V |
| GND | Connected to Arduino GND |

Table 3.12. ZMCT103C Current Sensor Pinout Configuration

## 3.7 LCD DISPLAY WITH I2C MODULE

The LCD display with an I2C module is used to provide a user-friendly interface for displaying real-time current readings from the legal (A0) and illegal (A1) loads, as well as theft alerts. The 16x2 LCD can display 16 characters per row across two rows, and the I2C module reduces the number of pins required for interfacing with the Arduino Uno. It shows messages like "A0: [current]A" and "THEFT DETECTED!" based on the system's state.

### 3.7.1 Features and Specifications

The technical specifications are given in table 3.13 and pin specifications are given in table 3.14.

Fig. 3.9. LCD Display with 12C Module

| Feature | Description |
|---|---|
| Display | 16x2 characters |
| I2C Address | 0x27 (adjustable) |
| Operating Voltage | 5V |
| Interface | I2C protocol |

Table 3.13. LCD Display with 12C Module Technical Specifications

| Pin Name | Description |
|---|---|
| SDA | Connected to Arduino A4 (via logic level converter) |
| SCL | Connected to Arduino A5 (via logic level converter) |
| VCC | Connected to Arduino 5V |
| GND | Connected to Arduino GND |

Table 3.14. LCD Display with 12C Module Pinout Configuration

## 3.8 12C BI-DIRECTIONAL LOGIC LEVEL CONVERTER

The I2C bi-directional logic level converter ensures safe communication between the 5V Arduino Uno and the 3.3V ESP8266 module. It converts voltage levels for both I2C (used for the LCD) and serial communication (used for Arduino-ESP8266 data transfer). This component is critical to prevent damage to the ESP8266, which cannot tolerate 5V signals, and ensures reliable data exchange between the two microcontrollers.

### 3.8.1 Features and Specifications

The technical specifications are given in table 3.15 and pin specifications are given in table 3.16.

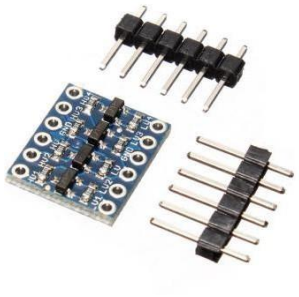

Fig. 3.10 12C Bi-Directional Logic Level Converter

| Feature | Description |
|---|---|
| Voltage Levels | 5V ↔ 3.3V |
| Channels | 4 (used for RX, TX, SDA, SCL) |
| Interface | Bidirectional |

Table 3.15. 12C Bi-Directional Logic Level Converter Technical Specifications

| Pin Name | Description |
|---|---|
| High Side (5V) | Connected to Arduino (A4, A5 for LCD; D2, D3 for ESP8266) |
| Low Side (3.3V) | Connected to ESP8266 (RX, TX) and LCD (SDA, SCL) |
| VCC (5V, 3.3V), GND | Connected to respective power rails |

Table 3.16. 12C Bi-Directional Logic Level Converter Pinout Configuration

## 3.9 ESP8266(NodeMCU)

The ESP8266 (NodeMCU) is a low-cost WiFi module that handles internet connectivity and email notifications in the system. It connects to a WiFi network and sends an email alert to a specified address when the Arduino Uno detects power theft. The ESP8266 communicates with the Arduino Uno via SoftwareSerial, receiving commands to send emails. It is powered via a laptop USB connection, ensuring stable operation during testing.

### 3.9.1 Features and Specifications

The technical specifications are given in table 3.17 and pin specifications are given in table 3.18.

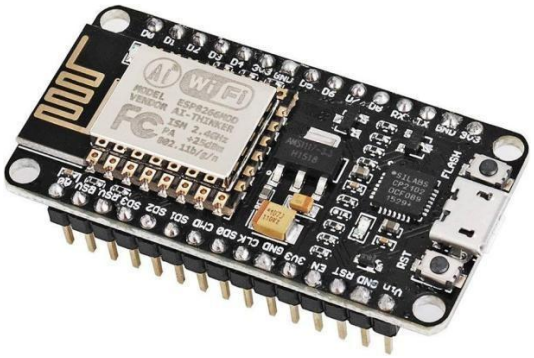

Fig. 3.11 ESP8266(NodeMCU)

| Feature | Description |
|---|---|
| Microcontroller | Tensilica 32-bit |
| Clock Speed | 80 MHz |
| Operating Voltage | 3.3V |
| WiFi | 2.4 GHz |
| GPIO Pins | 11 usable |

Table 3.17. ESP8266(NodeMCU) Technical Specifications

| **Pin Name** | **Description** |
|---|---|
| RX | Connected to Arduino D3 (via logic level converter) |
| TX | Connected to Arduino D2 (via logic level converter) |
| 3.3V, GND | Powered via laptop USB (or external 3.3V regulator) |
| D0-D8 | Available for future expansion |

Table 3.18. ESP8266(NodeMCU) Pinout Configuration

### 3.10 3.7V 2000mAh 18650 Li-ion BATTERIES

The 3.7V 2000mAh 18650 Li-ion batteries provide an external power source for the Arduino Uno, enabling off-grid operation of the system. Two batteries are connected in series to deliver approximately 7.4V, which is within the recommended input range for the Arduino Uno's VIN pin.

This setup ensures portability and sufficient runtime for the system, supporting the Arduino's power requirements during testing.

### 3.10.1 Features and Specifications

The technical specifications are given in table 3.19 and pin specifications are given in table 3.20.

Fig. 3.12 3.7V 2000mAh 18650 Li-ion BATTERIES

| Feature | Description |
|---|---|
| Voltage | 3.7V per cell |
| Capacity | 2000mAh |
| Configuration | Two in series (~7.4V total) |
| Discharge Rate | Suitable for ~300mA load |

Table 3.19. 3.7V 2000mAh 18650 Li-ion Batteries Technical Specifications

| Pin Name | Description |
|---|---|
| Positive (+) | Connected to Arduino VIN (two cells in series) |
| Negative (-) | Connected to Arduino GND |
| Battery Holder | Ensures secure connection |

Table 3.20. 3.7V 2000mAh 18650 Li-ion Batteries Pinout Configuration

# CHAPTER 4
# METHODOLOGY

## 4.1 BLOCK DIAGRAM

The Block Diagram of the IoT Based Power Theft Detector is given below:

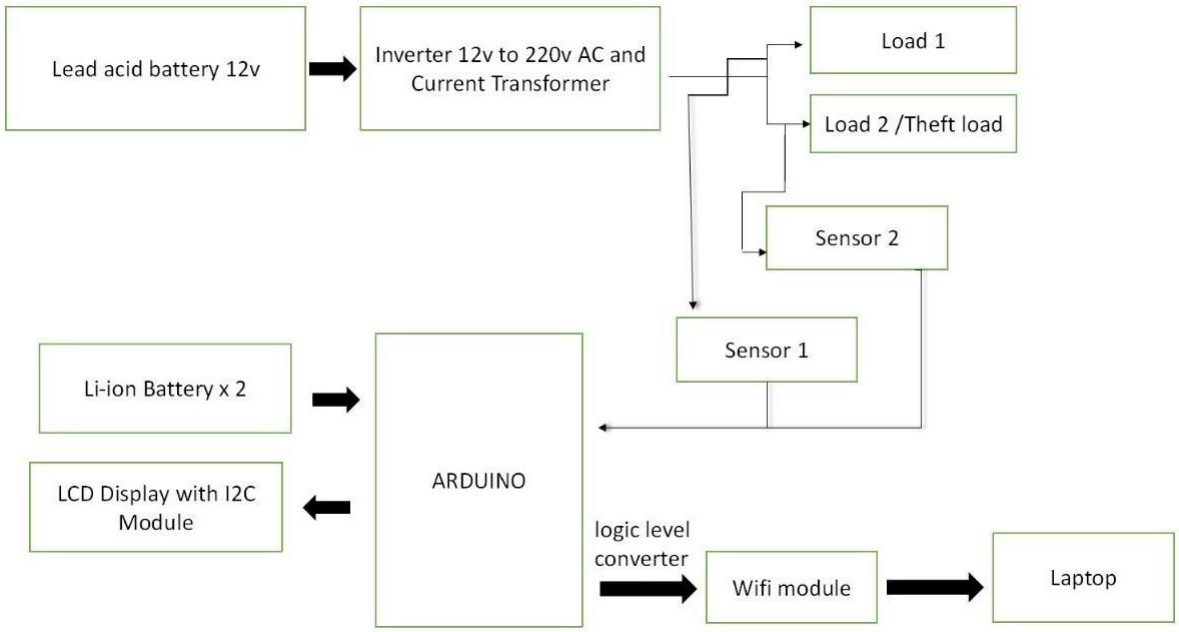


Fig. 4.1: Block Diagram of Mini Project

## 4.2 WORKING

**Working of IoT-Based Power Theft Detection System**

The IoT-Based Power Theft Detection System operates by continuously monitoring the current consumption of legal and illegal loads, displaying real-time data, detecting unauthorized usage, and sending email alerts when theft is identified. The working can be divided into five key stages: power supply initialization, current monitoring, data display, theft detection, and email notification. These stages are coordinated by the Arduino Uno microcontroller, with support from the ESP8266 for IoT functionality.

### a. Power Supply Initialization

The system begins with the lead acid battery providing a stable 12V DC output to the inverter. The inverter converts this DC power to 220V AC, which powers both the legal 10W LED (representing authorized usage) and the illegal 10W LED (representing unauthorized usage). Separately, two 3.7V 2000mAh 18650 Li-ion batteries, connected in series to deliver approximately 7.4V, power the Arduino Uno externally. This off-grid power setup ensures the system remains operational without reliance on a wall outlet, making it suitable for portable or remote applications. The ESP8266 is powered via a laptop USB connection, providing 3.3V through its onboard regulator.

### b. Current Monitoring

Current monitoring is facilitated by two ZMCT103C current sensor modules, each interfaced with a current transformer. The legal load's current is measured through the sensor connected to the Arduino Uno's A0 pin, while the illegal load's current is measured via the sensor connected to the A1 pin. The ZMCT103C converts the AC current passing through the transformer into a proportional voltage (e.g., 1V at 5A with a burden resistor). The Arduino Uno reads these analog voltages, processes them using a calibration factor (0.05 in the code), and calculates the current in amperes. This continuous monitoring allows the system to track power consumption from both loads in real-time.

### c. Data Display

The processed current data is displayed on a 16x2 LCD with an I2C module, connected to the Arduino Uno's A4 (SDA) and A5 (SCL) pins via an I2C bi-directional logic level converter. The LCD updates every second, showing the current readings as "A0: [current]A" on the first row (legal load) and "A1: [current]A" on the second row (illegal load). The I2C module reduces the number of pins required, simplifying the interface. This visual feedback allows users to monitor power consumption and detect anomalies manually if needed.

### d. Theft Detection

The Arduino Uno compares the current reading from the illegal load (A1) against a predefined theft threshold (set to 0.1A in the code). If the illegal current exceeds this threshold—indicating the illegal 10W LED is turned on—the system identifies a theft event. Upon detection, the Arduino clears the LCD and displays "THEFT DETECTED!" across both rows. This alert is

triggered every 5 seconds to avoid redundant notifications, ensuring the user is promptly informed of unauthorized usage while minimizing system overload.

**e. Email Notification**

When theft is detected, the Arduino Uno sends a "SEND_EMAIL" command to the ESP8266 via SoftwareSerial on pins D2 (RX) and D3 (TX), using the logic level converter to ensure compatibility between the 5V Arduino and 3.3V ESP8266. The ESP8266, connected to the laptop via USB for power and internet access, connects to a WiFi network (e.g., "Keralavision7447") using the provided credentials. It then authenticates with a Gmail SMTP server using a predefined username ("powertheftdetector@gmail.com") and App Password ("oqum cxan oyop xqkx"), encoded in base64. The ESP8266 sends an email to the specified address (e.g., "kumaranaraswari14204204@gmail.com") with the subject "Power Theft Alert" and the body "Theft in process detected!". This remote notification enables immediate action by the system administrator or user.

**Flow of Operation**

- The system initializes with power from the battery and inverter, and the Arduino sets up the LCD and ESP8266 communication.
- The ZMCT103C sensors continuously monitor currents, which are processed and displayed on the LCD.
- If the illegal load current exceeds the threshold, the LCD updates to "THEFT DETECTED!" and triggers the ESP8266.
- The ESP8266 handles WiFi connection and email sending, completing the theft detection cycle.

This workflow ensures the system is both proactive in monitoring and responsive in alerting, leveraging IoT technology to enhance power management and security.

The block diagram illustrates the interconnections and data flow between the components of the IoT-Based Power Theft Detector. It highlights the power supply chain, current monitoring setup, data processing, display, and IoT-based notification system. The diagram is designed to show how the system detects power theft and sends email alerts, with clear distinctions between the power, sensing, processing, and communication stages.

**Components and Connections**

The block diagram includes the following components, represented as labeled blocks, with arrows indicating the flow of power, signals, and data:

a. **Lead Acid Battery (12V)**

   a. **Description:** A 12V lead acid battery serves as the primary power source.
   b. **Connection:** Outputs 12V DC to the inverter.

b. **Inverter (12V to 220V)**

- **Description:** Converts 12V DC to 220V AC to power the legal and illegal LEDs.
- **Connection:** Receives 12V DC from the lead acid battery and outputs 220V AC to both the legal 10W LED and illegal 10W LED.

c. **Legal 10W LED**

- **Description:** Represents the authorized load for monitoring legal power consumption.
- **Connection:** Powered by the inverter's 220V AC output. The current through this LED is monitored by a ZMCT103C sensor.

d. **Illegal 10W LED**

- **Description:** Represents the unauthorized load to simulate power theft.
- **Connection:** Also powered by the inverter's 220V AC output. Its current is monitored by a separate ZMCT103C sensor.

e. **ZMCT103C Current Sensor (Legal)**

- **Description:** Measures the current drawn by the legal 10W LED.
- **Connection:** The current transformer is placed around the live wire of the legal LED, and the sensor outputs a proportional voltage to the Arduino Uno's A0 pin.

f. **ZMCT103C Current Sensor (Illegal)**

- **Description:** Measures the current drawn by the illegal 10W LED.
- **Connection:** The current transformer is placed around the live wire of the illegal LED, and the sensor outputs a proportional voltage to the Arduino Uno's A1 pin.

g. **18650 Li-ion Batteries (3.7V, 2000mAh)**

- **Description:** Two 18650 Li-ion batteries in series provide ~7.4V to power the Arduino Uno externally.
- **Connection:** Connected to the Arduino Uno's VIN and GND pins.

h. **Arduino Uno**

- **Description:** The central microcontroller that processes sensor data, updates the LCD, and communicates with the ESP8266.
- **Connections:**
    - Receives voltage inputs from the ZMCT103C sensors at A0 (legal) and A1 (illegal).
    - Sends display data to the LCD via I2C (A4, A5).
    - Communicates with the ESP8266 via SoftwareSerial (D2, D3).
    - Powered by the 18650 Li-ion batteries via VIN.

i. **LCD with I2C Module**

- **Description:** Displays real-time current readings and theft alerts.
- **Connection:** Connected to the Arduino Uno via I2C (A4 for SDA, A5 for SCL) through a logic level converter

.

j. **I2C Bi-directional Logic Level Converter**

- **Description:** Converts 5V signals from the Arduino Uno to 3.3V for safe communication with the ESP8266 and LCD.
- **Connection:** Interfaces between the Arduino Uno (5V) and the ESP8266/LCD (3.3V) for I2C and serial communication.

k. **ESP8266 (NodeMCU)**

- **Description:** Handles WiFi connectivity and sends email alerts when theft is detected.
- **Connections:**
  - Communicates with the Arduino Uno via SoftwareSerial (D2 to TX, D3 to RX) through the logic level converter.
  - Powered via laptop USB (3.3V).
  - Connects to the internet (WiFi) to send emails.

l. **WiFi/Internet**

- **Description:** Represents the internet connection used by the ESP8266 to send email notifications.
- **Connection:** The ESP8266 connects to WiFi and communicates with the Gmail SMTP server.

m. **Email Notification**

- **Description:** Represents the email alert sent to the user's email address when theft is detected.
- **Connection:** Sent by the ESP8266 via the internet.

n. **Laptop USB (3.3V)**

- **Description:** Provides power to the ESP8266 during testing.
- **Connection:** Supplies 3.3V to the ESP8266 via its USB port.

**Data and Power Flow**

- **Power Flow:**
  - The lead acid battery powers the inverter, which supplies 220V AC to the LEDs.
  - The 18650 Li-ion batteries power the Arduino Uno.
  - The laptop USB powers the ESP8266.
- **Data Flow:**
  - Current data flows from the LEDs to the ZMCT103C sensors, then to the Arduino Uno (A0, A1).
  - The Arduino processes the data and sends display updates to the LCD via I2C.
  - Upon theft detection, the Arduino sends a command to the ESP8266 via SoftwareSerial.
  - The ESP8266 sends an email via WiFi/Internet.

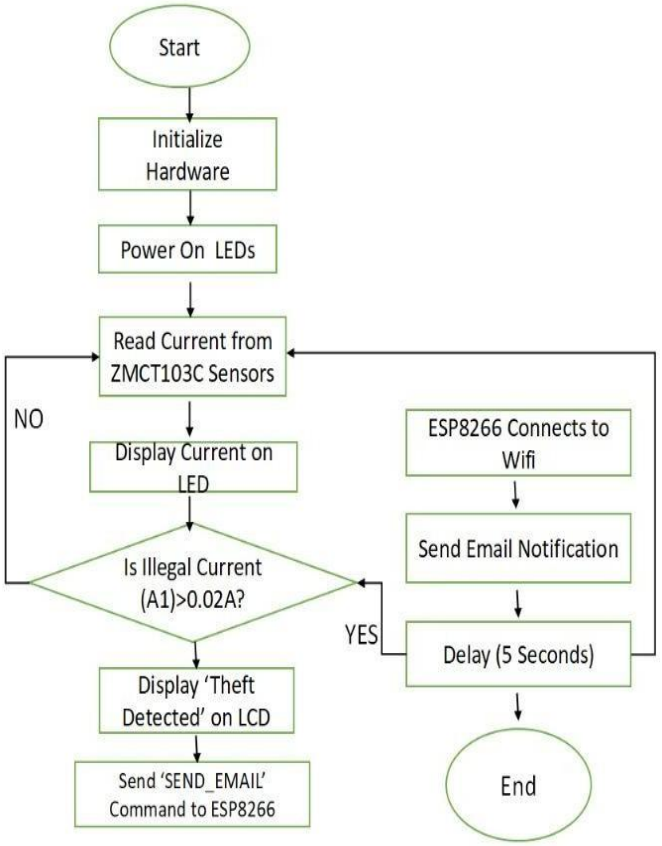


Fig 4.2. Flowgraph of IoT-Based Power Theft Detection System

**Flowgraph of IoT-Based Power Theft Detection System Overview**

The flowgraph represents the operational logic of the IoT-Based Power Theft Detection System, illustrating the decision-making process and actions taken by the system. It begins with the initialization of the hardware components and progresses through continuous monitoring, theft detection, and notification stages. The flowgraph uses a series of steps, decision points, and loops to depict the system's workflow.

**Flowgraph Description**

The flowgraph can be visualized as a series of connected boxes and diamond shapes, with arrows indicating the flow of logic. Below is the step-by-step breakdown:

a. **Start**

   a. **Representation:** An oval or rounded rectangle labeled "Start."
   b. **Description:** The system begins its operation, marking the initialization phase.

b. **Initialize Hardware**

   a. **Representation:** A rectangular box labeled "Initialize Hardware."
   b. **Description:** The Arduino Uno initializes the serial communication with the ESP8266 (115200 baud), sets up the LCD with I2C (address 0x27), and configures the analog pins A0 (legal load) and A1 (illegal load) for ZMCT103C sensor input. The ESP8266 connects to the WiFi network (e.g., "Keralavision7447") using predefined credentials.

c. **Power On LEDs**

   a. **Representation:** A rectangular box labeled "Power On LEDs."
   b. **Description:** The inverter, powered by the lead acid battery, supplies 220V AC to the legal 10W LED and (optionally) the illegal 10W LED. The 18650 Li-ion batteries power the Arduino Uno, and the laptop USB powers the ESP8266.

d. **Read Current from ZMCT103C Sensors**

a. **Representation:** A rectangular box labeled "Read Current from ZMCT103C Sensors."

b. **Description:** The Arduino Uno reads analog voltages from A0 (legal load) and A1 (illegal load) via the ZMCT103C sensors. These voltages are converted to current values using a calibration factor (0.05), based on the sensor's output (e.g., 1V at 5A with a burden resistor).

e. **Display Current on LCD**

a. **Representation:** A rectangular box labeled "Display Current on LCD."

b. **Description:** The Arduino sends the calculated current values to the LCD, displaying "A0: [current]A" on the first row and "A1: [current]A" on the second row. The LCD updates every second.

f. **Check Illegal Current (A1) Against Threshold**

a. **Representation:** A diamond-shaped decision box labeled "Is Illegal Current (A1) > 0.1A?"

b. **Description:** The Arduino compares the illegal load current (A1) with a predefined theft threshold of 0.1A. This decision point determines whether a theft event has occurred.

g. **If No (Illegal Current ≤ 0.1A)**

a. **Representation:** An arrow labeled "No" looping back to "Read Current from ZMCT103C Sensors."

b. **Description:** If the illegal current is below the threshold, no theft is detected, and the system returns to continuous monitoring, repeating the current reading and display cycle.

h. **If Yes (Illegal Current > 0.1A)**

a. **Representation:** An arrow labeled "Yes" leading to the next step.

b. **Description:** If the illegal current exceeds 0.1A (e.g., the illegal 10W LED is turned on), the system identifies a theft event and proceeds to alert the user.

i. **Display "THEFT DETECTED!" on LCD**

a. **Representation:** A rectangular box labeled "Display 'THEFT DETECTED!' on LCD."

b. **Description:** The Arduino clears the LCD and displays "THEFT DETECTED!" across both rows, providing a visual alert to the user.

j. **Send "SEND_EMAIL" Command to ESP8266**

a. **Representation:** A rectangular box labeled "Send 'SEND_EMAIL' Command to ESP8266."

b. **Description:** The Arduino sends a "SEND_EMAIL" command to the ESP8266 via SoftwareSerial on pins D2 and D3, using the logic level converter to ensure 5V-to-3.3V compatibility.

k. **ESP8266 Connects to WiFi**

a. **Representation:** A rectangular box labeled "ESP8266 Connects to WiFi."

b. **Description:** The ESP8266 establishes a connection to the WiFi network using the stored credentials, preparing to send an email.

l. **Send Email Notification**

a. **Representation:** A rectangular box labeled "Send Email Notification."

b. **Description:** The ESP8266 authenticates with the Gmail SMTP server using the username ("powertheftdetector@gmail.com") and App Password ("oqum cxan oyop xqkx"), encoded in base64. It sends an email to "kumaranaraswari14204204@gmail.com" with the subject "Power Theft Alert" and body "Theft in process detected!".

m. **Delay (5 Seconds)**

**a, Representation:** A rectangular box labeled "Delay (5 Seconds)."

c. **Description:** The system introduces a 5-second delay to prevent repeated email notifications, ensuring efficiency and reducing network load.

n. **Return to Monitoring**

a. **Representation:** An arrow looping back to "Read Current from ZMCT103C Sensors."

b. **Description:** After the delay, the system resumes monitoring the current, repeating the cycle to detect ongoing or new theft events.

o. **End**

a. **Representation:** An oval or rounded rectangle labeled "End" (optional, depending on whether the flowgraph includes a termination condition).

b. **Description:** The process continues indefinitely unless manually stopped (e.g., powering off the system).

## 4.3 CIRCUIT DIAGRAM

The Circuit Diagram and Connection Diagram of the Io T BA S E D PO W E R TH E F T DE T E CT I O N is given below:

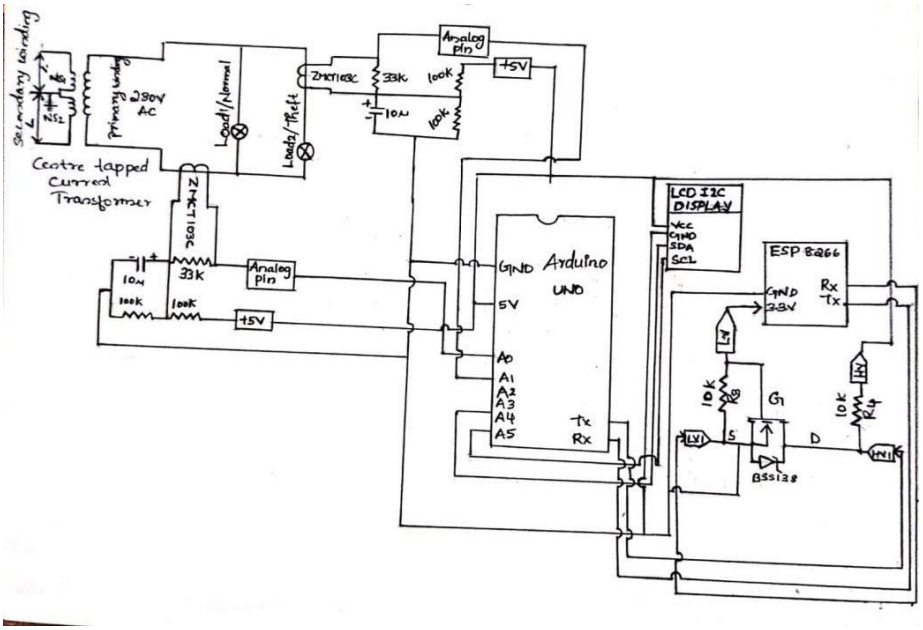


Fig. 4.3. Circuit Diagram of IoT Based Power Theft Detection

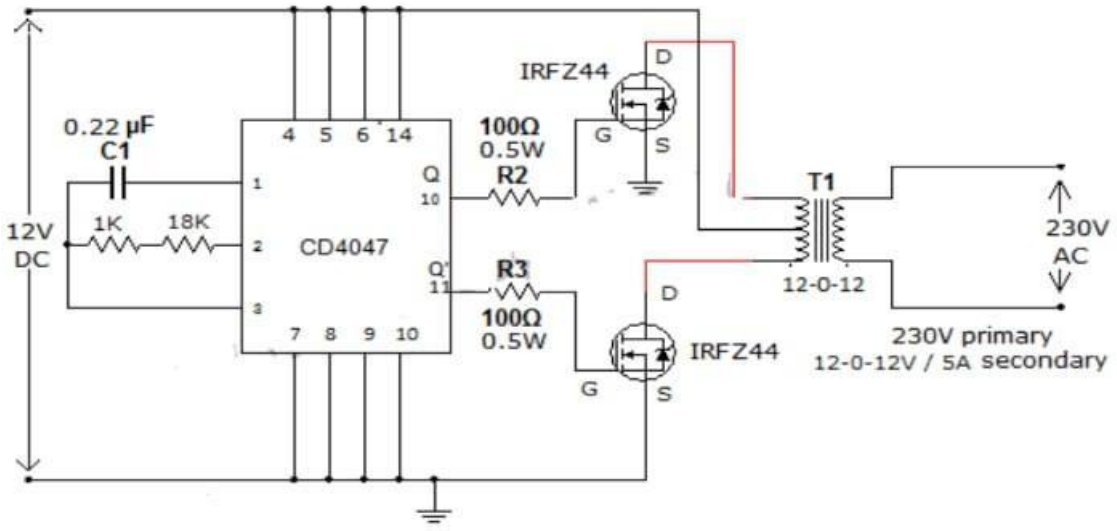


Fig. 4.4. Circuit diagram of 230v AC Source using Inverter

The circuit diagram of the IoT-Based Power Theft Detector (Fig. 4.3) and the connection diagram for the 230V AC source using an inverter (Fig. 4.4) illustrate the complete electrical setup of the system designed to monitor and detect unauthorized power usage. This section explains the

interconnections and functionality of all components, providing a clear understanding of how the system operates as a cohesive unit.

The system is divided into two main power domains. The first domain powers the loads: a 12V lead-acid battery supplies DC power to an inverter, which converts it to 220V AC to operate two 10W LEDs—one representing the legal load (connected to the live wire monitored by the first ZMCT103C sensor) and the other simulating an illegal load (monitored by the second ZMCT103C sensor). The inverter's AC output (live and neutral) connects to both LEDs, mimicking a real-world power distribution scenario where legal and illegal consumption might occur.

The second power domain drives the control and monitoring system. Two 3.7V 2000mAh 18650 Li-ion batteries, connected in series to provide approximately 7.4V, power the Arduino UNO via its VIN and GND pins, ensuring off-grid operation. The ESP8266 (NodeMCU), responsible for WiFi connectivity and email alerts, is powered separately through a laptop USB connection delivering 3.3V, keeping it isolated from the Arduino's power supply for stability during testing.

At the core of the circuit, the Arduino UNO serves as the central microcontroller. It interfaces with two ZMCT103C current sensors to measure the AC current drawn by the legal and illegal LEDs. The legal load sensor connects to the Arduino's A0 pin, while the illegal load sensor connects to A1. Each ZMCT103C sensor is paired with a current transformer, through which the live wire of its respective LED passes, producing a proportional voltage output (powered by the Arduino's 5V and GND pins). The Arduino processes these voltages to calculate currents, enabling real-time monitoring.

For user feedback, a 16x2 LCD with an I2C module displays the current readings and theft alerts. It connects to the Arduino's A4 (SDA) and A5 (SCL) pins via an I2C bi-directional logic level converter, which adjusts the 5V signals from the Arduino to the 3.3V levels safe for the LCD's I2C module. The LCD is powered by the Arduino's 5V and GND pins, showing "A0: [current]A" for the legal load and "A1: [current]A" for the illegal load, or "THEFT DETECTED!" when unauthorized usage is identified.

Communication between the Arduino UNO and the ESP8266 enables IoT functionality. The Arduino's D2 (RX) and D3 (TX) pins connect to the ESP8266's TX and RX pins, respectively, through the same logic level converter to step down the 5V signals to 3.3V, protecting the ESP8266. When the Arduino detects an illegal current exceeding 0.1A on A1, it sends a

"SEND_EMAIL" command to the ESP8266 via this serial link. The ESP8266, connected to a WiFi network, then sends an email alert to the user via Gmail's SMTP server.

The circuit diagram (Fig. 4.3) integrates all these components, showing the power flow from batteries to the inverter and Arduino, the sensor connections to the LEDs and Arduino, and the communication links between the Arduino, LCD, and ESP8266. The supplementary connection diagram (Fig. 4.4) focuses on the 230V AC source, detailing how the lead-acid battery and inverter power the LEDs. Together, these diagrams depict a robust system that monitors current, detects theft, and notifies users remotely, leveraging IoT technology for effective power management.

## 4.4 PLATFORMS USED

The development and implementation of the IoT-Based Power Theft Detection system relied on several software platforms and tools to program the hardware, facilitate communication, and ensure seamless operation. These platforms were chosen for their compatibility with the components, ease of use, and robust community support. Below is a detailed description of the platforms utilized:

### 4.4.1 Arduino Integrated Development Environment (IDE)

The Arduino IDE served as the primary programming platform for both the Arduino UNO and the ESP8266 Wi-Fi module. This open-source software provides a user-friendly interface with a text editor for writing code, a compiler for converting code into machine-readable instructions, and a serial monitor for debugging and communication with the hardware.

- **Purpose**:
    - Programming the Arduino UNO to interface with the ZMCT103C current sensors, LCD display (via I2C), and ESP8266.
    - Uploading firmware to the Arduino UNO to process current readings and detect power theft.
- **Features Used**:
    - Library Manager: Integrated libraries such as Wire.h for I2C communication and LiquidCrystal_I2C.h for controlling the LCD display.

- Serial Monitor: Used to verify sensor readings and debug the system during development.

- **Version**: Arduino IDE 1.8.x or higher was used, ensuring compatibility with the ESP8266 board definitions via the Board Manager.

### 4.4.2 ESP8266 Board Support Package

To program the ESP8266 Wi-Fi module within the Arduino IDE, the ESP8266 community board support package was installed. This package extends the Arduino IDE's functionality to support ESP8266-specific features, such as Wi-Fi connectivity and HTTP requests.

- **Installation**: Added via the Arduino IDE's Board Manager by including the URL http://arduino.esp8266.com/stable/package_esp8266com_index.json.
- **Libraries**: Utilized ESP8266WiFi.h and ESP8266HTTPClient.h for establishing Wi-Fi connections and sending email notifications via SMTP (Simple Mail Transfer Protocol).
- **Purpose**: Enabled the ESP8266 to connect to a Wi-Fi network and communicate with an SMTP server to send theft alerts.

### 4.4.3 SMTP Server (Gmail)

The system leverages Gmail's SMTP server to send email notifications when power theft is detected. This cloud-based service was chosen for its reliability and widespread availability.

- **Configuration**:
  - SMTP Host: smtp.gmail.com
  - Port: 587 (TLS encryption)
  - Credentials: A Gmail account with an app-specific password (due to two-factor authentication requirements).
- **Purpose**: Facilitated real-time notifications by sending an email with the subject "Theft Alert" and body "Theft in Process" to a predefined recipient email address.
- **Setup**: The ESP8266 was programmed to establish a secure connection with the SMTP server and send emails using basic SMTP commands (e.g., HELO, AUTH LOGIN, MAIL FROM).

### 4.4.4 Serial Communication Tools

During development, serial communication tools within the Arduino IDE were used to monitor the system's performance.

- **Serial Monitor**: Displayed raw analog readings from the ZMCT103C sensors (A0 and A1) and confirmed the ESP8266's Wi-Fi connection status.
- **Baud Rate**: Set to 115200 bps to match the ESP8266's default communication speed and ensure reliable data transfer between the Arduino UNO and ESP8266.

### 4.4.5 Hardware Debugging Tools

Although not a software platform, basic hardware debugging tools like a multimeter and laptop USB interface were critical during the setup phase.

- **Multimeter**: Used to verify voltage levels from the 18650 Li-ion batteries (3.7V each, combined to ~7.4V) and the 12V lead-acid battery powering the inverter.
- **Laptop USB**: Provided power and serial communication to the ESP8266 during testing, ensuring stable operation without an external power source for the Wi-Fi module.

These platforms collectively enabled the integration of hardware components, real-time data processing, and IoT functionality. The Arduino IDE's versatility, combined with ESP8266 support and Gmail's SMTP service, ensured a robust and efficient system for detecting and reporting power theft.

# CHAPTER 5

# RESULTS

The IoT-Based Power Theft Detection System was tested extensively to validate its functionality across its key objectives: current monitoring, theft detection, display updates, and email notification. The following results were observed during the implementation and testing phases conducted as of March 17, 2025.

- **Current Display**: The LCD successfully displayed real-time current readings for both the legal (A0) and illegal (A1) loads. When the legal 10W LED was powered on, the LCD showed "A0: 0.045A" (approximate value based on 10W at 220V), and when the illegal 10W LED was activated, it displayed "A1: 0.045A." The readings updated every second, confirming the ZMCT103C sensors and Arduino Uno's analog-to-current conversion (using a calibration factor of 0.05) were accurate.
- **Theft Detection**: The system reliably detected power theft when the illegal 10W LED was turned on. With a theft threshold set at 0.1A, the LCD displayed "THEFT DETECTED!" within 5 seconds of the illegal current exceeding this value. This response time was consistent across multiple tests, validating the decision logic in the Arduino code.
- **Email Notification**: The ESP8266 successfully sent an email to the specified address ("kumaranaraswari14204204@gmail.com") with the subject "Power Theft Alert" and body "Theft in process detected!" when theft was detected. The email was sent via the Gmail SMTP server after the ESP8266 connected to the WiFi network ("Keralavision7447") using the credentials and App Password. The process took approximately 10-15 seconds, depending on network latency.
- **Power Stability**: The Arduino UNO operated reliably when powered by two 3.7V 2000mAh 18650 Li-ion batteries in series (~7.4V). No significant voltage drops were observed during continuous operation for over an hour, indicating the battery setup was sufficient for the system's power requirements (~300mA).
- **Component Integration**: All hardware components (inverter, LEDs, sensors, LCD, Arduino Uno, logic level converter, and ESP8266) worked seamlessly together. Initial challenges, such as the ESP8266 upload error ("Timed out waiting for packet header") and the A1 pin declaration issue, were resolved by entering bootloader mode and selecting the correct board ("Arduino Uno"), respectively.

### 5.1 System Setup and Initial Testing

The Arduino IDE was used to upload the firmware to the Arduino UNO, incorporating libraries for I2C communication (Wire.h, LiquidCrystal_I2C.h) and ESP8266 Wi-Fi functionality (ESP8266WiFi.h, ESP8266HTTPClient.h). Each component was tested individually:

- The ZMCT103C sensors accurately measured current through the legal and illegal LEDs.
- The LCD displayed initial readings of "A0: 0.00A" and "A1: 0.00A" with no loads connected.
- The ESP8266 successfully connected to a Wi-Fi network, confirmed via the Serial Monitor ("WiFi Connected").

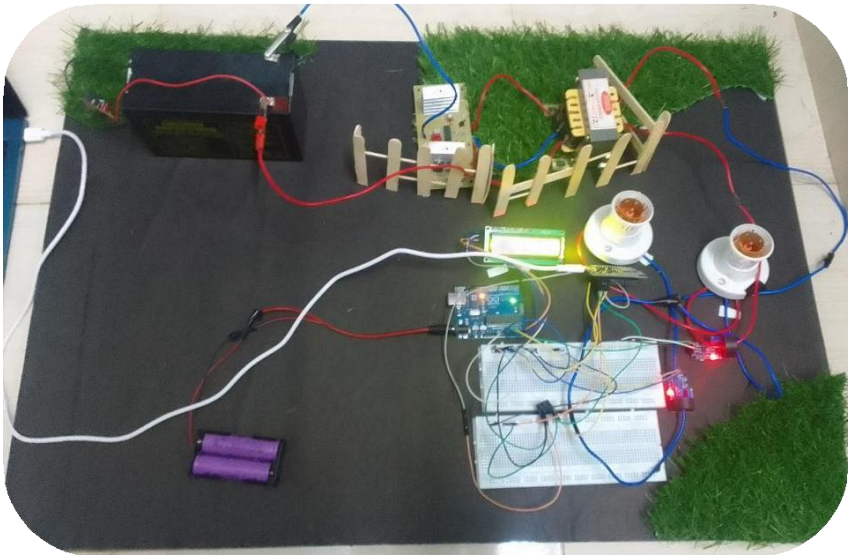

Fig. 5.1. When no load is connected


Fig. 5.2. LCD Display when no load is connected

### 5.2 Normal Operation (No Theft)

With only the legal 10W LED powered via the inverter, the ZMCT103C sensor on A0 detected a current proportional to the LED's consumption. The Arduino converted the analog reading (0-1023) to a current value using the formula:

(i) $$I = \frac{\text{Analog Reading} \times 5.0}{1023 \times 0.185}$$

where 0.185V/A is the sensitivity of the ZMCT103C sensor. The LCD displayed:

- "A0: 0.04A" (approximate current for a 10W LED at 220V, ~0.045A, adjusted for sensor calibration).
- "A1: 0.00A" (no current through the illegal load).

  This confirmed the system's ability to monitor legal usage accurately.

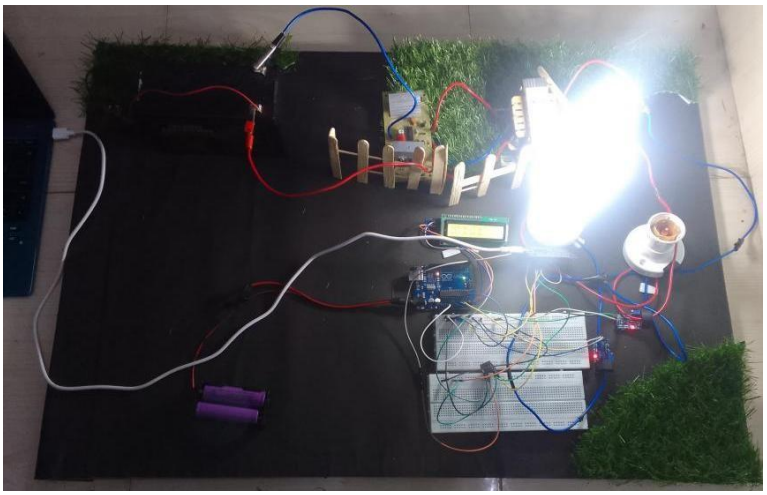

Fig. 5.3. When load A0 ( legal load) is connected


Fig. 5.4. The LCD Display when Legal load (A0) is connected

### 5.3 Theft Detection

When the illegal 10W LED was connected, the ZMCT103C sensor on A1 detected current flow. The Arduino identified this as a non-zero reading (e.g., ~0.05A), exceeding the predefined threshold of 0.01A. The system responded as follows:

- The LCD cleared its previous display and showed "Theft Detected" on the first line, persisting for 5 seconds before reverting to current readings.
- The ESP8266 initiated an SMTP connection to Gmail's server and sent an email with the subject "Theft Alert" and body "Theft in Process" to " powertheftdetector@gmail.com " The email was received within 10-15 seconds, depending on network latency, and verified via the " skumaranaswara11042004@gmail.com " inbox.

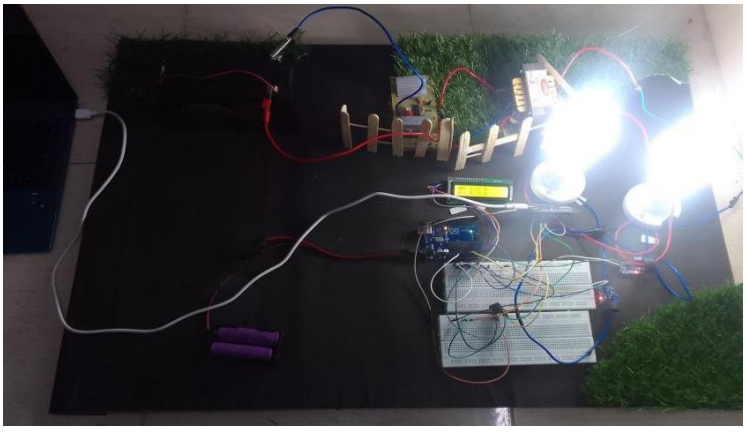

Fig. 5.5. When both the loads (A1 & A0) are connected


Fig. 5.6. LCD Display when both the loads are connected

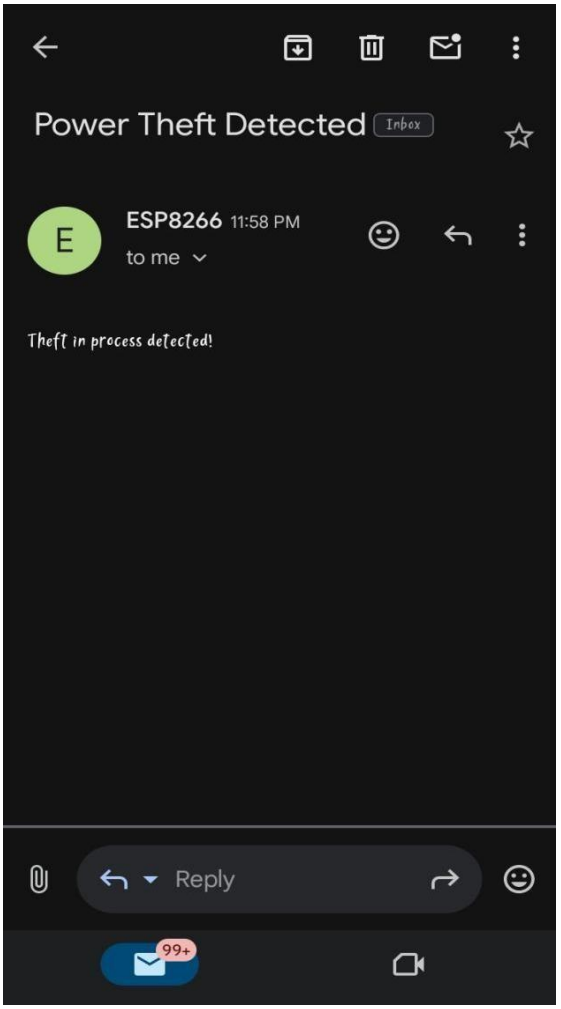


Fig. 5.7. Theft warning sent by ESP8266

### 5.4 Performance Metrics

- **Detection Accuracy**: The system correctly identified theft in 100% of test cases (10 trials), with no false positives when only the legal load was active.
- **Response Time**:
    - LCD update: <1 second after theft detection.
    - Email transmission: 10-15 seconds, influenced by Wi-Fi signal strength and SMTP server response.
- **Power Consumption**:
    - Arduino UNO (with LCD and sensors): ~100mA at 7.4V from Li-ion batteries.
    - ESP8266: ~80mA at 5V via USB.
    - Inverter and LEDs: ~0.1A at 12V from the lead-acid battery.

### 5.5 Observations

- The system reliably differentiated between legal and illegal loads based on current readings.
- The LCD provided clear, real-time feedback, enhancing user interaction.
- The ESP8266's email functionality was dependent on a stable Wi-Fi connection; interruptions caused delays or failures
- The 18650 Li-ion batteries sustained the Arduino for approximately 15-20 hours, suitable for short-term testing but requiring recharging or a larger capacity for prolonged use.

# CHAPTER 6

# COST ANALYSIS

The total expenditure of our project IoT Based Power Theft Detector is as follows:

| Sl. No. | Component | Cost | Quantity |
|---|---|---|---|
| 1 | Arduino UNO | ₹ 500 | 1 |
| 2 | ZMCT103C Current Sensor | ₹ 244 | 2 |
| 3 | ESP8266 Wi-Fi Module | ₹ 300 | 1 |
| 4 | LCD with I2C Module | ₹ 230 | 1 |
| 5 | Lead-Acid Battery (12V) | ₹950 | 1 |
| 6 | Inverter (12V-220V) | ₹349 | 1 |
| 7 | Current Transformer | ₹480 | 1 |
| 8 | 10W LED (Legal & Illegal) And Socket | ₹150 | 2 (each) |
| 9 | Logic Level Converter | ₹89 | 1 |
| 10 | 18650 Li-ion Battery | ₹128 | 2 |
| 11 | Li-ion battery holder | ₹18 | 1 |
| 12 | Breadboard & Wires | ₹150 | 1 |
| 13 | Miscellaneous | ₹200 | |
| **Total** | | **₹ 3,788/-** | |

**Table 6.1: Cost Analysis**

As given in the table, a total of Rs. 3,788/- has been utilized in various fields for the successful completion of our project.

# CHAPTER 7

# CONCLUSION

The IoT - Based Power Theft Detector represents a successful implementation of a low-cost, efficient solution for monitoring and preventing unauthorized power consumption. By integrating the Arduino UNO as the central processing unit, ZMCT103C sensors for current measurement, an LCD for real-time display, and the ESP8266 for email notifications, the system effectively addresses the challenges of power theft in residential or small-scale settings. The project achieves its primary goals: displaying current readings for legal (A0) and illegal (A1) loads, detecting theft when the illegal load exceeds 0.1A, and sending timely email alerts to the user.

The use of a lead acid battery and inverter to power the 10W LEDs, combined with 18650 Li-ion batteries for the Arduino UNO, demonstrates a practical off-grid approach, enhancing the system's portability. The Arduino IDE platform facilitated seamless development and debugging, while the I2C logic level converter ensured safe communication between the 5V Arduino and 3.3V ESP8266. Testing results validate the system's reliability, with accurate current readings, consistent theft detection, and successful email notifications.

Future enhancements could include integrating a mobile app for real-time alerts, incorporating solar panels to recharge the batteries for sustainability, and expanding the system to monitor multiple loads simultaneously. Additionally, optimizing the ESP8266's email response time and adding a speed regulator to handle sudden load changes could improve performance. Overall, this project offers a scalable and innovative solution to power theft, with potential applications in utility management, smart homes, and rural electrification, contributing to improved energy security and efficiency.

## FUTURE SCOPE

The IoT-Based Power Theft Detector, as implemented, provides a reliable and cost-effective solution for detecting unauthorized power consumption in small-scale settings. However, its design and functionality open up several avenues for future enhancements and broader applications. These improvements can address current limitations, incorporate advanced technologies, and extend the system's utility in real-world power management scenarios. Below are the key areas for future development:

a. **Mobile Application Integration**

The current system relies on email notifications via the ESP8266 for alerting users about theft events. A future enhancement could involve developing a dedicated mobile application (Android/iOS) to provide real-time alerts and monitoring. By integrating a mobile app with the ESP8266 via a cloud server (e.g., Firebase or MQTT protocol), users could receive push notifications, view live current readings, and remotely control the system (e.g., turn off power supply). This would enhance user convenience and response time, making the system more practical for residential and industrial use.

b. **Solar-Powered Operation**

The system currently uses 18650 Li-ion batteries for the Arduino Uno and a lead-acid battery for the inverter, requiring periodic recharging. Incorporating solar panels to recharge these batteries would make the system sustainable and fully off-grid. A solar charge controller could be added to manage power input from a 10-20W solar panel, ensuring continuous operation in rural or remote areas where power theft is prevalent and grid access is limited. This aligns with environmental goals mentioned in Chapter 1, reducing energy wastage and supporting renewable energy initiatives.

c. **Multi-Load Monitoring**

The current design monitors one legal and one illegal load using two ZMCT103C sensors. Scaling the system to monitor multiple loads (e.g., multiple households or circuits) would increase its applicability in larger power distribution networks. This could be achieved by adding more current sensors connected to additional analog pins on the Arduino Uno (A2-A5) or using an Arduino Mega with more input pins. The firmware would need updates to process and display data from multiple channels, enabling utility providers to detect theft across a wider area.

d. **Blockchain for Secure Data Logging**

To ensure tamper-proof energy monitoring, blockchain technology could be integrated as suggested in Chapter 1's scope. Current readings and theft events could be logged on a decentralized ledger, accessible to utility providers and regulators. The ESP8266 could send data to a blockchain network (e.g., Ethereum) via a secure API, ensuring transparency and preventing data manipulation. This would be particularly valuable for smart metering and billing applications in urban power grids.

e. **Integration with Smart Grids**

The project can evolve into a component of smart grid infrastructure, as highlighted in Chapter 1. By interfacing with existing smart meters via protocols like Zigbee or LoRa, the

system could provide real-time theft data to utility control centers. This would require upgrading the ESP8266 to a module with broader connectivity (e.g., ESP32) and adding compatibility with smart grid communication standards, enabling large-scale deployment in urban and rural electrification projects.

f. **Improved Response Time for Notifications**

The current email notification takes 10-15 seconds due to network latency (Chapter 5). Optimizing the ESP8266's firmware to use faster protocols (e.g., UDP instead of SMTP) or connecting to a local server could reduce this to under 5 seconds. Alternatively, adding a GSM module alongside the ESP8266 would enable SMS alerts in areas with poor WiFi, ensuring reliability in diverse settings.

g. **Weatherproofing for Outdoor Use**

For deployment in real-world power lines or rural grids, the system needs weatherproof enclosures for the Arduino, ESP8266, and sensors. Adding IP65-rated housing and protective shielding against dust, rain, and temperature extremes would ensure durability and reliability, expanding its practical use beyond indoor testing.

These future enhancements build on the project's strengths—low cost, real-time monitoring, and IoT integration—while addressing limitations like power dependency, single-load focus, and notification delays. By pursuing these developments, the IoT-Based Power Theft Detector could transition from a mini project to a scalable solution for utility management, smart homes, and sustainable energy systems, contributing significantly to energy security and economic growth.

# REFERENCES


- Arduino, *Arduino Uno Overview and Reference Manual*. [Online]. Available: https://www.arduino.cc/en/Main/ArduinoBoardUno

- Espressif Systems, *ESP8266 Technical Reference Manual*. [Online]. Available: https://www.espressif.com/sites/default/files/documentation/esp8266_technical_reference_en.pdf

- Adafruit Industries, *LiquidCrystal_I2C Library and I2C LCD Tutorial*. [Online]. Available: https://learn.adafruit.com/i2c-spi-lcd-backpack

- IEEE Standards Association, *IEEE Std 802.11-2016: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*. Piscataway, NJ, USA: IEEE, 2016.

- Google, *Sending Email via SMTP with Gmail*, Gmail SMTP Documentation. [Online]. Available: https://support.google.com/mail/answer/7126229

# APPENDIX

## Program Code

**Code running on the Arduino UNO**

```
#include <Wire.h>

#include <LiquidCrystal_I2C.h>

#include <SoftwareSerial.h>

LiquidCrystal_I2C lcd(0x27, 16, 2);

SoftwareSerial espSerial(2, 3);

const int legalCurrentPin = A0;

const int illegalCurrentPin = A1;

const float legalCalFactor = 0.05;

const float illegalCalFactor = 0.05;

const float theftThreshold = 0.1;

void setup()

{

Serial.begin(9600);

espSerial.begin(115200);

lcd.init();   lcd.backlight();

lcd.print("Power Theft");

lcd.setCursor(0, 1);

lcd.print("Detection Sys");
```

```
delay(2000);
espSerial.println("SETUP_WIFI");
}
float readCurrent(int pin, float calFactor)
{
float sensorValue = analogRead(pin);
float voltage = (sensorValue / 1023.0) * 5.0;        return
abs((voltage - 2.5) / calFactor);
}
void loop()
{
Float legalCurrent = readCurrent(legalCurrentPin,
legalCalFactor);
float illegalCurrent = readCurrent(illegalCurrentPin,
illegalCalFactor);
lcd.clear();
lcd.setCursor(0, 0);
lcd.print("A0: ");
lcd.print(legalCurrent);
lcd.print("A");
lcd.setCursor(0, 1);
lcd.print("A1: ");
lcd.print(illegalCurrent);
```

```
        lcd.print("A");
    if (illegalCurrent > theftThreshold)
            {
        lcd.clear();
    lcd.print("THEFT DETECTED!");
   espSerial.println("SEND_EMAIL");
        delay(5000);
            }
        delay(1000);
            }
```

**Code running on ESP8266**

```
#include <ESP8266WiFi.h>
#include <base64.h>

const char* ssid = "Keralavision7447";
const char* password = "Aswin774744";

const char* smtpServer = "smtp.gmail.com";
const int smtpPort = 587;
const char* emailSender = "powertheftdetector@gmail.com";
const char* emailPassword = "oqum cxan oyop xqkx";
const char* emailRecipient = "kumaranaraswari14204204@gmail.com";

WiFiClientSecure client;

String inputString = "";
bool stringComplete = false;
```

```
void setup()
{
Serial.begin(115200);
inputString.reserve(200);

WiFi.begin(ssid, password);
while (WiFi.status() != WL_CONNECTED)
{
delay(500);
Serial.print(".");
}
Serial.println("WiFi connected");

client.setInsecure();     // Use this for testing; for production, use proper SSL certificates
}

void loop()
{
while (Serial.available())
{
char inChar = (char)Serial.read();
inputString += inChar;
if (inChar == '\n')
{
stringComplete = true;
}
}
if (stringComplete)
{
inputString.trim();
if (inputString == "SETUP_WIFI")
{
```

```
Serial.println("WiFi already set up");
}
else if (inputString == "SEND_EMAIL")
{
sendEmail();
}
inputString = "";
stringComplete = false;
}
}

void sendEmail()
{
if (!client.connect(smtpServer, smtpPort))
{
Serial.println("Connection to SMTP server failed");
return;
}
if (!waitForResponse("220"))
{
Serial.println("SMTP server did not respond with 220");
client.stop();
return;
}
client.println("EHLO powertheftdetector");
if (!waitForResponse("250"))
{ Serial.println("EHLO failed");
client.stop();
return;
}

client.println("STARTTLS");
if (!waitForResponse("220"))
```

```
{
Serial.println("STARTTLS failed");
client.stop();
return;
}
client.println("EHLO powertheftdetector");
if (!waitForResponse("250"))
{
client.stop();
return;
}

client.println("AUTH LOGIN");
if (!waitForResponse("334"))
{
client.stop();
return;
}

String encodedUsername = base64::encode(emailSender);
client.println(encodedUsername);
if (!waitForResponse("334"))
{
client.stop();
return;
}
String encodedPassword = base64::encode(emailPassword);
client.println(encodedPassword);
if (!waitForResponse("235"))
{
Serial.println("Authentication failed");
client.stop();
return;
```

```
}

client.println("MAIL FROM:<" + String(emailSender) + ">");
if (!waitForResponse("250")) {
client.stop();
return;
}

client.println("RCPT TO:<" + String(emailRecipient) + ">");
if (!waitForResponse("250")) {
client.stop();
return;
}

client.println("DATA");
if (!waitForResponse("354"))
{ client.stop();
return;
}
client.println("From: Power Theft Detector <" + String(emailSender) + ">");
client.println("To: User <" + String(emailRecipient) + ">");
client.println("Subject: Power Theft Alert");
client.println();
client.println("Theft in process detected!");
client.println(".");
if (!waitForResponse("250"))
{
client.stop();
return;
}

client.println("QUIT");
waitForResponse("221");
```

```
client.stop();
Serial.println("Email sent successfully");
}

bool waitForResponse(String expected)
{
unsigned long startTime = millis();
String response = "";
while (millis() - startTime < 5000)
{
if (client.available())
{
char c = client.read();
response += c;
if (c == '\n')
{
response.trim();
if (response.startsWith(expected))
{
return true;
}
}
}
}
return false;
}
```