



## IOT BASED POWER THEFT MONITORING SYSTEM

Rekha.P<sup>1</sup>, Assistant professor, Knowledge Institute of Technology,  
 Dinesh B<sup>2</sup>, Assistant Professor, Knowledge Institute of Technology,  
 Sathiyapriya.V<sup>2</sup>, M.E. Embedded System Technologies  
 Knowledge Institute of Technology, Salem  
[preee@kiot.ac.in](mailto:preee@kiot.ac.in)<sup>1</sup>, [bdeee@kiot.ac.in](mailto:bdeee@kiot.ac.in)<sup>2</sup>, [2k20est04@kiot.ac.in](mailto:2k20est04@kiot.ac.in)<sup>3</sup>

### ABSTRACT

*In today's public services sector, those automations are the latest trend in transforming labor-dependent services into semi-automated or fully automated sectors. People's incomes are increasing as the country is enlightened for globalization. The word "busy" is now an important part of everyone's life. Therefore, the government prefers to provide citizens with not only quality services, but also corrupt, error-free services. This project aims to provide our customers with high quality service without any problems and to significantly reduce recurring energy thefts. From a technical point of view, theft of electricity is a non-negligible crime that has a direct impact on the country's economy but is highly preventable. Theft of electricity is a social evil and therefore must be completely eliminated. Power consumption and loss should be carefully monitored in order to use the generated power as efficiently as possible. This white paper describes the development of a low-cost power theft detection and prevention system using Internet of Things (IoT) technology. Using a PIC microcontroller that controls and monitors the output of the two current sensors, if the output of the current sensor changes, the controller considers this a power theft and EB automatic SMS via the connected GSM modem. Send to the bureau system. Also share the location. In addition, the relay is connected to the controller, and if the output of the current sensor is different, the load is automatically cut off and it is regarded as theft of electricity. This proposed system presents an IoT-based power theft monitoring system and implements simulation using PROTEUS software.*

### 1.INTRODUCTION

The main purpose of the electricity theft monitoring / notification system of a local substation using IoT technology is to indicate the place where electricity was stolen. Electricity theft is a big problem in India, so it is necessary to detect electricity theft. Thanks to this, system owners and administrators are notified about system features or any kind of error. The goal is to find improvements compared to previous surveillance systems. This model reduces manual labor and theft management. To integrate different parts, you

first need to understand the behavior of the different parts you are integrating.

Power theft is the biggest problem today and is causing huge losses to power companies. And to make up for these losses, prices will be raised. Therefore, if you can prevent this theft, you can save a lot of power. If the current flows and the energy pulse is normal, the current will not be stolen. If power is being supplied and no energy pulse is coming, this indicates power theft. Therefore, the microcontroller triggers o / p on the relay. This information is sent to the substation via GPS. Line failures can be caused by overcurrent or

ground faults. If there is a connection between the two phases, an overcurrent fault will occur. Ground faults occur because the phase line is grounded by a cross arm or the like. Monitoring electricity theft is an important research in the field of electricity, and prevention of electricity theft has become a major issue for electricity.

Theft of electricity is a long-term problem. However, each power supply sector has made huge investments in human resources and materials, and the power theft prevention phenomenon has increased and has not decreased. Also, the method of power theft is continuously improving. The act of stealing power not only causes enormous economic loss to the power industry, but also jeopardizes the safety and reliability of the mains. You can develop effective and efficient systems for remote monitoring of power consumption and detect electricity theft in the right place in an accurate and cost-effective way. You can prevent such a large loss. This kind of money could definitely be spent on developing quality power supply services.

## 2. METHODS OF THEFT

The methods used to commit theft fall into the following broad categories:

- Connection of unmetered supply: Connection of unmetered supply after interruption by a "tort" who occupies a non-payment or vacant property.
- Cable bypass of the meter: Embedded in the supply side of the meter installation (that is, the meter connection, meter cable, recess, or service cable).
- Interference to slow down or stop the meter: A disc that contains the use of electrical equipment (called a "black box") that stops or reverses the meter.
- Intervention in time control: A device used for two charges to get a cheaper charge.

## 3. OBJECTIVES

The purpose of developing an IoT-based power theft monitoring system is to save power and use it in the future. This reduces power loss and makes it more cost effective. Electricity theft

also carries the fatal risk that many people can pay in their lives during the electricity theft. Electricity theft is not only dangerous to those who are stealing, even if you are on the same line, but you may also pay for their attempted theft. You can reduce them by protecting them from theft of electricity. Power lines can be overloaded with electrical energy and can damage electronic devices and appliances designed to handle certain quantities of electricity. This can have a dangerous impact on our household items and can reduce these. Theft of electricity reduces the reliability of electrical services and the quality of paying customers. Power thieves can even unknowingly feedback energy to power lines. It has dangerous implications for transmission line personnel who normally assume that the power line they are working on is dead. This can be prevented by using electric theft monitoring.

## 4. EXISTING SYSTEM

Since electricity is essential for domestic and industrial development activities, it is necessary to protect it for efficient power supply to consumers. There are two types of losses: technical losses and non-technical losses. According to the Energy Ministry WAPDA Company's loss

of over 1.25 billion, utilities pay an average of 20-30% line loss each year. T & D losses are a problem for India's power sector. Because these were very high compared to other developed countries. Current T & D losses, including unrecovered energy, are around 30%, and these losses need to be reduced through efficient management and O & M best practices for transmission and distribution. When talking about T & D loss, this also includes theft of electricity, which is part of the commercial loss, but there is no way to distinguish between theft and T & D loss. In reality, we know the billed energy and the input energy. The difference between the two is T & D loss. Obviously, theft is included in this loss.

SERC and Mop also require T & D loss and commercial loss to be separated, but no one can tell how to separate these losses because the theft is built into T & D. Theft of electricity is

attracting attention all over the world, but theft of electricity in India has a great impact on the Indian economy. The loss equivalent to the theft is reflected in the utility's ARR. Therefore, these costs are regularly passed on to customers in the form of higher energy prices. Electricity theft can take many forms and thrive with the support of people from a variety of disciplines, including utilities, consumers, union leaders, political leaders, bureaucrats, and senior utilities. The problem facing power companies around the world is power. This is the use of power from the power company without the consent of the company.

## 5. PROPOSED SYSTEM

Theft of electricity is an obvious problem in the power system, causing great economic loss and leading to unstable power supply. Theft of electricity can easily be defined as the use of electricity without the knowledge of the supplier. It has become a major issue in India and it is a crime. Electricity theft can occur in a variety of ways. For example, a registered customer bypasses the meter, that is, connects the meter to the company's hot line, or tampers with the meter to reduce meter consumption or hide it at all. In order to eradicate the theft of electricity, it needs to be identified. In society, there are many people who commit illegal electricity theft, such as disconnecting wires or bypassing meters during an event.

The IoT is a technology that has recently emerged. Here the prototype was developed to identify energy theft using the Industrial IoT. The IoT was chosen due to its rapid technological growth and significant use of the IoT. Currently, the system is manually controlled and energy consumption is unknown. You can develop effective and efficient systems for remote monitoring of power consumption and detect electricity theft in the right place in an accurate and cost-effective way. You can prevent such a large loss. This kind of money could definitely be spent on developing high quality power supply services.

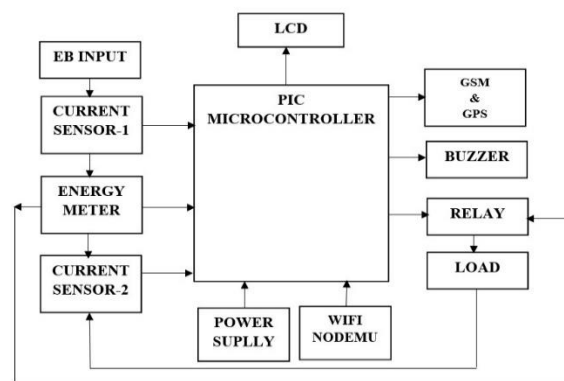


Fig 5.1 Block Diagram

## 6. WORKING PRINCIPLE

This proposed system uses an IoT-based power theft monitoring system. As shown in the block diagram, this system uses two current sensors. The output of both current sensors is continuously monitored, and when the output changes, the buzzer sounds first and the message "Power theft" is generated. The message is sent via GPS and GSM to the authorized person along with the location of the theft. If the output of the current sensor fluctuates over a long period of time, the consumer load will automatically turn off.

With IoT-based systems, consumers can monitor the power they are consuming and easily determine if it has been stolen. This proposed system is used to prevent theft of electricity. With technological developments, the IoT will be used to prevent theft of electricity without human intervention. This electricity theft can be reduced in many ways. Profitable businesses need to welcome consumers to report on theft of electricity. If your system experiences negative values, you can use the IoT to identify power theft. Therefore, this power-stealing system overcomes previously encountered problems. This system helps us save energy and evenly distribute power.

## 7. HARDWARE DESCRIPTION

### 7.1 LCD DISPLAY

The LCD displays are one of the most sophisticated display devices they use. Once you learn how to connect, it will be the easiest and most reliable output device you will use. In addition, the debugger is not always available for

microcontroller-based projects. In this way, you can test the output using the LCD display. Obviously, as a last possibility, you need to know how to use something like this pretty well. Most of the LCD displays on the market are 16X2 (that is, LCD displays can display 2 lines of 16 characters each) and 20X4 LCD displays (4 lines, 20 characters). There are 14 pins. It uses 8 lines and 3 control signals for parallel data, 2 connectors for power supply, 1 for contrast adjustment and 2 connectors for LED backlight.

## 7.2 RELAY

The relay is an electric switch. The current flowing through the relay coil creates a magnetic field that attracts the lever and changes the contacts of the switch. Since the coil current can be turned on or off, the relay has two switch positions and is double throw. Relays allow one circuit to switch between the second circuit. The second circuit can be completely separated from the first circuit. For example, a low voltage battery circuit can use a relay to switch the 230V AC line circuit. There is no electrical connection within the relay between the two circuits, the connection is magnetic and mechanical. The coil of the relay carries a relatively large current.

Normally, it is 30mA for a 12V relay. However, for relays designed to operate at lower voltages, it can be as high as 100mA. Most ICs (chips) cannot supply this current, and transistors are typically used to boost small IC currents to the large values required for relay coils. Relays are usually SPDTs or DPDTs, but can have more sets of switch contacts. For example, a relay with four sets of switching contacts is readily available. See the switch page for more information on switch contacts and their descriptions. Most relays are designed for PCB mounting, but you can solder the wires directly to the pins if you are careful not to melt the relay's plastic case.

The terminals of a relay switch are usually labeled COM, NC, and NO. • COM = common, always connected. This is the moving part of the switch.

- NC = normally closed, COM is connected when the relay coil is off.

- NO = normally open, COM is connected when the relay coil is on.

- If you want to turn on the switch circuit when the relay coil is on, connect it to COM and connect it to NO.

- If you want to turn on the switch circuit when the relay coil is off, connect it to COM and NC.

## 7.3 BUZZER

A buzzer is a mechanical, electro mechanical, magnetic, electro magnetic, electroacoustic, or piezo electric acoustic signal generator. Piezo electric buzzers can be driven by vibrating electronic circuits or other audio signal sources. A click, beep, or ring may indicate that a key has been pressed.

### 7.3.1 PIEZO BUZZER

Piezo buzzer is a convenient sound generator used to display audio in electronic circuits. It is often used as an alarm generator for electronic devices. Available in a variety of designs and sizes to suit your needs. The piezo buzzer contains a piezo disk and an oscillator. When the buzzer is powered, the oscillator produces a frequency of approximately 2-4kHz, which causes the piezo element to vibrate and produce sound. A typical piezo buzzer operates at a DC of 3-12 volts.

## 7.4 ELECTRICAL LOAD

An electrical load is a component or component of the circuit that converts electricity into light, heat, or mechanical motion. Examples of loads include light bulbs, resistors, and motors. If an electrical circuit has a well-defined output terminal, the circuit connected to that terminal (or its input impedance) is the load.

## 7.5 PIC16F877A MICRO CONTROLLER

PIC (Programmable Interface Controllers) microcontrollers are the worlds smallest microcontrollers that can be programmed to carry out a huge range of tasks. These microcontrollers are found in many electronic devices such as phones, computer



control systems, alarm systems, embedded systems, etc. Various types of microcontrollers exist, even though the best are found in the GENIE range of programmable microcontrollers. These microcontrollers are programmed and simulated by a circuit-wizard software.

Every PIC microcontroller architecture consists of some registers and stack where registers function as Random Access Memory (RAM) and stack saves the return addresses. The main features of PIC microcontrollers are RAM, flash memory, Timers/Counters, EEPROM, I/O Ports, USART, CCP (Capture/Compare/PWM module), SSP, Comparator, ADC (analog to digital converter), PSP (parallel slave port), LCD and ICSP (in circuit serial programming) The 8-bit PIC microcontroller is classified into four types on the basis of internal architecture such as Base Line PIC, Mid Range PIC, Enhanced Mid Range PIC and PIC18.

## 7.6 CURRENT SENSOR

The current sensor measures AC and / or DC current. The sensor described here measures the current and provides some output corresponding to the measured current. The most important difference when choosing a current sensor is whether to measure AC and / or DC current. Another important specification to consider is whether the sensor needs to match the circuit or whether the sensor works by clamping around the wire to be measured. The technology used in today's sensors is important because different sensors can have different characteristics in different applications. For most sensors, the energizing wire works to generate a magnetic field. If you want to measure the current directly in the circuit, use a current sense resistor.

## 7.7 GSM Module

GSM modules are used to establish communication between a computer and a GSM system. Global System for Mobile Communications (GSM) Is the architecture used for mobile communications in most countries. Global Packet Radio Service (GPRS) is an

extension of GSM that enables higher data transmission rates. The GSM / GPRS module consists of a GSM / GPRS modem and a power circuit and communication interface (RS-232, USB, etc.) for the computer. The modem is the soul of such a module.

## 7.8 NodeMCU ESP-12E

The ESP8266 WiFi module is a stand-alone SOC with an integrated TCP / IP protocol stack, which can provide access to the WiFi network to any microcontroller. The ESP8266 can host applications or offload all Wi-Fi networking capabilities to another application processor. Each ESP8266 module is pre-programmed with AT command set firmware. So just plug it into your Arduino device and you'll have as much WiFi functionality as the WiFi Shield offers (ready to use). The ESP8266 module is a very low cost board with a huge and growing community. The ESP8266 is a

very easy-to-use and inexpensive device for providing internet connectivity to your projects. This module can act as both an access point (which can create hotspots) and a station (which can connect to Wi-Fi), making it as easy as possible to retrieve data and upload it to the Internet, making the IoT as simple as possible. Become. You can also use the API to fetch data from the web, which makes your project smarter with access to all the information available on the web. Another exciting feature of this module is that it can be programmed using the Arduino IDE, making it much more user-friendly.

## 7.9 POWER SUPPLY

The operation of power circuits built with filters, rectifiers, and voltage regulators. Starting with the AC voltage, a constant DC voltage is obtained by rectifying the AC voltage, then filtering it to a DC voltage level, and finally adjusting it to get the desired fixed DC voltage. Regulations are typically taken from an IC voltage regulator unit that receives a DC voltage and provides a slightly lower DC voltage that remains the same as the input DC voltage changes or the output load associated with the DC voltage changes. increase. A block diagram showing voltages at various points in common power

supply components and devices. The AC voltage (typically 120Vrms) is connected to a transformer that lowers this AC voltage to the desired level of DC output. The diode rectifier then supplies the full-wave rectifier voltage. This voltage is first filtered with a simple capacitor filter to produce a DC voltage. The resulting DC voltage usually has ripples or AC voltage fluctuations. The regulator circuit uses this DC input, not only the ripple voltage is much lower, but also the input DC voltage fluctuates slightly, even if the DC voltage applied to the output is the DC voltage of the connected load. Can provide a DC voltage that maintains the same DC value. change.

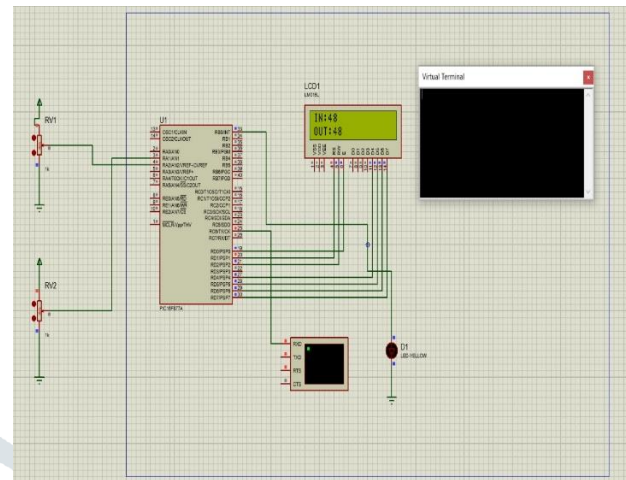
## 8. SOFTWARE DESCRIPTION

### 8.1 PROTEUS SOFTWARE

The Proteus Design Suite is a proprietary software tool suite primarily used for electronic design automation. This software is primarily used by electrical device designers and engineers to create schematics and electronic prints for PCB manufacturing. It was developed by Labcenter Electronics Ltd in Yorkshire, England and is available in English, French, Spanish and Chinese. Proteus Design Suite is a Windows application for schematic capture, simulation, and PCB (printed circuit board) layout design. It can be purchased in different configurations depending on the size of the design you are creating and your microcontroller simulation needs. All PCB design products include automated routers and basic mixed mode SPICE simulation capabilities. Schematic captures from the Proteus Design Suite are used both in the simulation of the design and in the design phase of the PCB layout project. Therefore, it is a core component and is included in all product configurations. Proteus microcontroller simulation works by applying either a hexadecimal file or a debug file to the microcontroller portion of the schematic. It is then co-simulated with the analog and digital devices connected to it. This allows it to be used in a wide range of project prototyping areas such as motor control, temperature control and user interface design. It's also used in the general hobby community and doesn't require any hardware, so it's useful as a training or educational tool.

## 9. RESULTS AND DISCUSSION

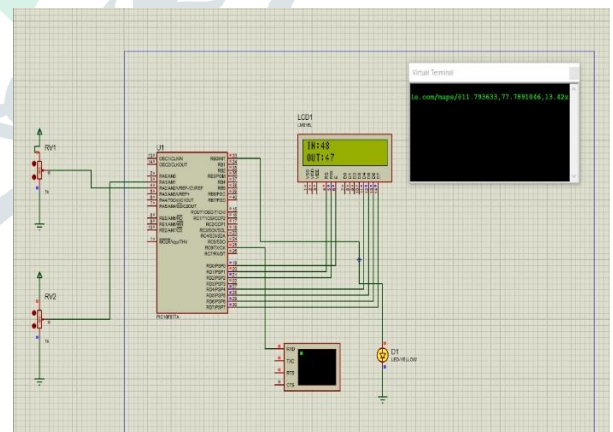
### 9.1 SIMULATION RESULTS AT NORMAL CONDITION



**Fig 9.1 simulation at normal condition**

In this system, depending on the connection, the outputs of the two current sensors are connected to the image controller. Both current sensor outputs are compared by the controller and the output value is displayed on the LCD. If the outputs are the same, they will not be displayed because power theft does not occur.

### 9.2 SIMULATION RESULTS AT POWER THEFT CONDITION



**Fig 9.2 Simulation at power theft condition**

As in Case 1, the controller compares the output of the current sensor. If the output changes, this is considered a power theft and is indicated by an LED. Also, the location of the theft is shown on the display. This will help you easily identify and fix the problem.

## 10. CONCLUSION

Wireless power theft detection and monitoring was designed and developed in the future with the proper integration of Proteus and hardware-based software. Relays and current sensors are connected to the microcontroller and this interface is synchronized throughout the theft detection and monitoring process. Locations of electrical theft are also detected using GPS and GSM modules. The location is shared with the mobile number associated with the device and the consumer load is automatically shut down after a while. Simulation results are obtained using Software Proteus.

## 11. REFERENCES

- [1] Kalaivani R, Gwothami M, Karthick N, Mohanvel S, "GSM Based Theft Identification in Distribution Systems", International Journal of Engineering Trends and Technology(IJETT)-Volume 8 Number 10- Feb 2014
- [2] S Anusha, M Madhavi, R Hemalatha, "Detection of Power Theft Using GSM.", International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)Vol.1, Issue 3, November 2014.
- [3] Seshapu Prasad, D Suneel, "Proximity Sensor Based Security Lock and Theft Detection."- International Journal of Science Technology and Management Vol. No.4, Issue No.12,December 2015
- [4] Q. M. Ashraf and M. H. Habaebi, "Introducing autonomy in internet of things," in 14th International Conference on Applied Computer and Applied Computational Science (ACACOS '15), Kuala Lumpur, 2015.
- [5] V.Soma Sekhar and R.puviarasi "Design of GSM based Power Theft Detection and Load Control,"vol 119, No. 15,pp. 2697-2703, 2018.
- [6] Nilesh, Rinkuraj, Prakash "GSM based Electricity Theft Detection", 2016 IJSEAS, Volume-2.
- [7] Nayan -Thakre, Shreya Vaidya, Prachi Damedhar, "Energy power theft detection in Distribution System", vol. 5,2017.
- [8] S.McLaughlin,B.Holbert, A.Fawaz, R.Bertheir, and S.Zonouz, "A multi-sensor energy theft detection.