



e-ISSN: 2319-8753 | p-ISSN: 2347-6710

# IJIRSET

International Journal of Innovative Research in  
**SCIENCE | ENGINEERING | TECHNOLOGY**



# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 11, Issue 9, September 2022

**ISSN** INTERNATIONAL  
STANDARD  
SERIAL  
NUMBER  
INDIA

Impact Factor: 8.118



9940 572 462



6381 907 438



ijirset@gmail.com



www.ijirset.com

# Smart Metering for Power Monitoring & Theft Detection using IOT

Meghana M S<sup>1</sup>, Amanulla<sup>2</sup>

<sup>1</sup>PG Scholar, Dept. of Electrical & Electronics, Ghousia College of Engineering, Ramanagara, India

<sup>2</sup>Assistant Professor, Dept. of Electrical & Electronics, Ghousia College of Engineering, Ramanagara, India

**ABSTRACT:** Power stealing, at low voltage side is a regarding about the issues such as that Electricity distribution companies will have losses of billions of Rupees revenue yearly. Smart meters using Information Communication Technology (ICT) can be used to identify and notify the power thief in the smart grid. Power theft detection and real-time smart meters monitoring are described in this study using the Internet of Things (IoT). Customers and distributors' smart meters are constantly monitored using Linear Regression to identify power stealing. In the event of a theft, Android apps may be used to notify the police and track usage and billing information. Meter bypass, meters tampering, and direct line hooking may all be detected by this technology. Distribution authorities may now directly manage smart meters to provide individual consumers with access or restriction of power supply. An ATmega328 microcontroller board with Arduino and a Wi-Fi module is used to build a prototype circuit for test the proposed system.

**KEYWORDS:** Power stealing, IoT(Internet of Thinks), ThinkSpeak, Cloud Storage, Arduino, DNO(Distribution Network Operator).

## I. INTRODUCTION

A stunning 46% of the country's total electrical generation is lost because to faulty wiring or other unauthorized alterations. As the name suggests, power theft is the act of stealing energy for one's own purpose. Companies involved in the production and distribution of electricity suffer as a result. One of the most critical concerns in a distribution network system is the risk of power loss. There are several ways to measure the amount of power that is lost in a process.

Technical and non-technical losses are two order to categorize this power loss. Non-technical losses account for the vast majority of power failures. Illegal or unrecorded use of electricity from distribution utilities is known as power theft. This power theft costs the distribution utilities a lot of money. Thieves in India are expected to steal between 6 and 10 billion rupees every year.

Consumers commit power theft in a variety of methods, including by bypassing meters, connecting directly to power lines, and by interfering with meters. An easy approach to circumvent meters is to plug the supply wire straight into the distribution network in place of the meters. Additionally, tampering with the meters is a common method of stealing power in rural and suburban regions, where foreign items or magnetic interfering materials are inserted into meters or meters terminals are shorted to prevent the meters from operating. In addition to this, customers can connect directly to low-voltage overhead wires via direct line hookup. Since power stealing directly affects a utility's profitability, it is an important matter for distribution utilities..

Power theft detection algorithms have been the subject of extensive research. Some use consumer load profile analysis to demonstrate power theft strategies. However, there is a disadvantage to these approaches: they are unable to detect thefts committed entirely through bypass or line hooking. Using meters data and transformer information, they create temperature-based forecasting models.

An algorithm for detecting power theft while maintaining user privacy was created by utilizing a kalman faltering technique in the course of my professional activity. In order to detect theft, the linear regression approach is presented. Instead than working on real-time implementation, it primarily focuses on mathematical design of a theft detection method. The magnetic oscillation of the distribution line is used in this work to create inspection equipment that can detect power theft. The detection of power stealing has been the subject of several techniques in the literature. Although these approaches are more difficult to implement, the utility must spend in the construction of a specialised infrastructure on the premises of the customer, which is impractical. More study has to be done on developing communication technology to notify authorities of theft, as the bulk of solutions focus solely on detection.

The conventional meters have been replaced with smart meters, which may be upgraded with communication technologies and connect with a central hub/server for real-time monitoring, thanks to the advent of the smart grid. With the use of Internet of Things (IoT), modern communication technologies may be used to send the consumption information of consumers to a central server, and any sort of power stealing at the distribution transformer level can be recognised and alerted. Few studies have been done on the use of IOT in smart meters and theft detection. A smart meters with sophisticated features including meters tampering alerts is the subject of this presentation. This system, on the other hand, does not provide theft detection.

A smart meters with the capability of sending all metered data to a server is demonstrated in this study. One controller is used for communication and the other for processing, making this device unaffordable for most users. Building a system to identify power theft using the Internet of Things (IoT) and a smart meter monitoring system requires a linear regression technique. To make it workable, the system under consideration is designed to be both computationally light and economically efficient.

## **II. LITERATURE REVIEW**

Many related works are available in the literature for power monitoring and power stealing detection which is implemented by using different technology. As the advancement in science and technology it as provided a way for efficient use of internet. By applying this concept in Electrical field, Complete power system can be automated which make the system monitoring and control and data exchange easier.

Presented below are the works which describes the uses of IoT technology for power monitoring, and power stealing detection.

Power tamper detection using IoT is developed in [1]. The incoming current is measured to use a voltage divider circuit, and the voltage value is communicated to the Internet of Things (IoT). Simultaneously the alert signal message is sent to the distribution network operator (DNO) through Web. The Web message consists of current, voltage values consumed by the consumers. Utilizing an electronic device such as a smart phone, the DNO may keep tabs on individual units' energy usage through their site.

In [2] the power monitoring system and power stealing detection is developed by using fuzzy logic technology. The proposed system is able to alert users of how many units they've consumed. Here, the amount of energy used is automatically assessed, and invoices are created automatically due to the Internet of Things (IoT). The technology notifies the distributors if any power theft occurs.

An IoT-based real-time power theft detection and smart meters monitoring system has been developed by the author of [3]. Detecting power theft is feasible with a linear regression model. The power theft detection and alarm messages are communicated via an IOT-based architecture.

An AC signal is removed using a rectifier and filter in [4], after which measurements are made with a current and potential transformer in the last stages of measurement. Analog signals are digitalized using ADC converter. The raspberry Pi receives these digital values. Python code sets the voltage and current values, which cannot be altered. When more load is added, the buzzer starts warning, and power theft is recognized. In this implementation.

Detecting when a meter's sensitive portion is opened by a person is made possible through the use of a Passive Infrared Sensor. A solid-state relay connects loads to the distribution network. Thingspeak.com's IoT Analytic platform is used by the electricity company to create a webpage that displays the meter's current status. Researchers are employing the IOT concept, first proposed in [5], to try to discover and prevent cases of electricity theft.

An IoT power theft detecting kit has been suggested in this research and the same has been done using GSM for the purpose of backup protection ([6]). In the event of an internet outage, a text message will be sent to notify you. The crime of stealing power may be decreased by using GSM and IoT methods.

## **III. METHODOLOGY**

### **A. Block Diagram of Proposed System**

Consumers may manage their electricity by periodically checking their energy use. The meter's pulses are recorded by the IOT, which is connected to it, and shown on the LCD display. It is also determined by the current

transformer, which is linked in series with the load, which will be shown on the LCD. Computers at Substation get this information. The data is obtained over the Internet and shown on the LCD screen. The information about the theft is transmitted to the web server, but it cannot be conveyed to the neighboring line worker through message under this system..

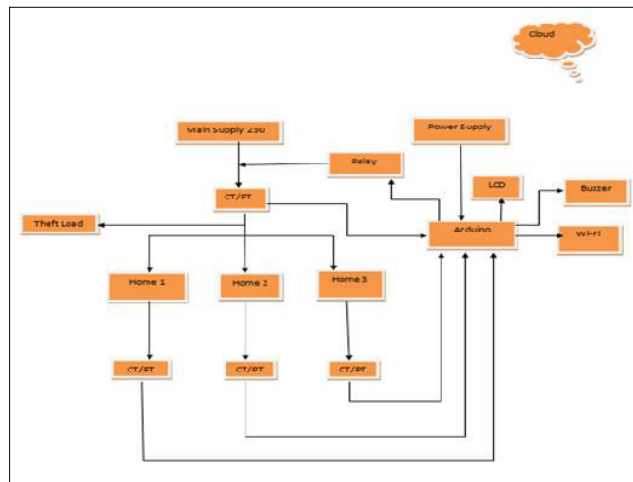


Figure.1 Block Diagram of Proposed Power Monitoring System

CT - Current Transformer

PT - Potential Transformer

## B. Hardware Description

### 1. Arduino ATMAGA 2560:

CMOS 8-bit embedded systems, such as the Arduino ATMEGA 2560, consume very little power because of the AVR's improved RISC architecture. It has a small size and low power consumption..

### 2. Regulated Power Supply:

Dissipative arrangement controller circuits and a large mains transformer are included in power supply plans to separate the information from the outputs. For a controller circuit, a single Zener diode or three-terminal direct arrangement can supply the yield voltage.

### 3. Relay Circuit:

Positive and ground must be connected to the correct terminals on the hand-off loop for the hand-off to work correctly. An electromagnet loop used to open and close switches is a basic example of a hand-off. The Internet of Things makes use of Cayenne.com's cloud services (IoT). Cayenne is the first online tool for creating Internet of Things (IoT) projects. The server records every measurement of voltage and current. Alerts can be scheduled on a server.

### 4. Wi-Fi Module (ESP8266):

It is feasible to use the Wi-Fi module ESP8266 to connect an existing microcontroller project via a serial UART connection to Wi-Fi. A separate Wi-Fi device can be made out of the module.

### 5. Current Sensor:

Use of power transformer allows for the adjustment of primary operation amplifier stages and amplification of second operation amplifier phases.

### 6. Voltage Sensor:

An AC framework may be transformed into DC motion for use by a microcontroller using this voltage detection circuit. Making a DC flag is made simple with this circuit's specific instructions. A potential transformer measures the voltage, and the flag is set to a true price at the primary operation amp stage and raised again at the primary operation amp stage's second operation amp arrangement..

### C. Experimental Work

The device layer, the client layer, and the server layer make up the three parts of the stacks. A device layer is formed by the smart meters installed at various points. Through the internet, APIs and HTTP requests are used to interact across these many levels. The server connects, updates, fetches, and deletes data via four different types of requests. To get data from the server, you can use GET, while to make changes to the database, you can use PUT, while to provide a continuous stream of real-time data to the server, while you can use POST to delete an entry from the database. According to the proposed system, the power flow characteristics are first read and sent to a server by all of the smart meters located at individual customer sites, as well as the smart meters installed near the distribution transformer itself. Power flow information from the transformer is compared to the total consumption of all consumer meters in the server to determine if there has been a theft. To determine whether or not a theft has occurred, the server looks for any evidence of meters manipulation or bypass. The authorities will be notified if there is any tampering or bypassing of the system. There will be no theft if all of the meters have not been tampered with or bypassed. Consequently, this information is sent to law enforcement agencies so they can investigate illegal direct access.

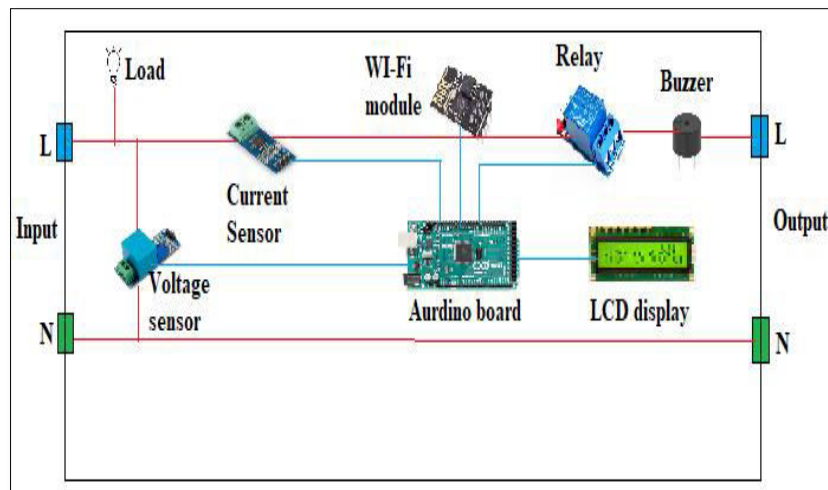


Figure 2: Schematic Diagram of Working Model

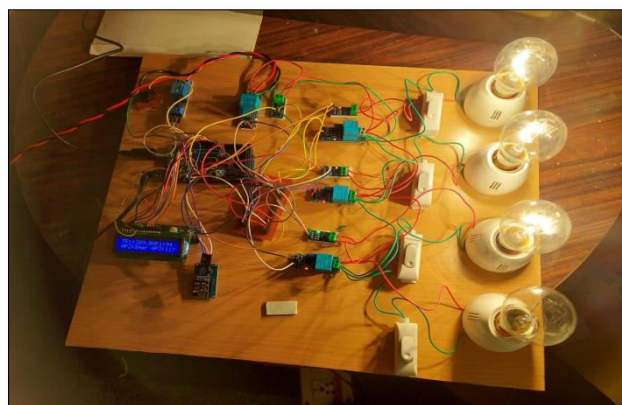


Figure 3: Working Model of Power Monitoring & Theft Detection System

The above picture presents the proto type circuit diagram of power stealing detection system. The IOT server is linked to the power system via communication characteristics. Wi-Fi module and AURDINO controller are required for internet access. Sensors that measure voltage and current are used to produce an analogue output corresponding to the data measured by the sensors. For the purpose of calculating actual power consumption in kilowatt-hours (Kwh),

these analogue signals are sent to AURDINO. These values are updated to cloud through Wi-Fi module. When power stealing or power tampering is detected the relay senses the tampering power and actuates the buzzer which makes the system to shut down. The theft information can be known by the distribution network operator by accessing the cloud. The system is restarted after pressing reset button provided in AURDINO board. LCD display is used to display the status of the system.

The presented system consists of four loads which is considered equitant to four home namely (Home1, Home2, Home3, Home4). In the implemented circuit Home4 is designed to demonstrate the power stealing detection situation. During normal operation the measured input power from supply side is equal to the measured output power from load side.

$$\sum_{k=0}^n (P_{in}) = \sum_{k=0}^n (L_1 + L_2 + L_3)$$

When the connected load consumes more than the supplied input then there will be the chance of power stealing in any one of the connected load.

$$\sum_{k=0}^n (P_{in}) = \sum_{k=0}^n (L_1 + L_2 + L_3 + L_{thf})$$

Where :

K= Total number of load connected, L= Load,  $L_{thf}$ = theft Load

#### D. Algorithm & Flow Chart of the System

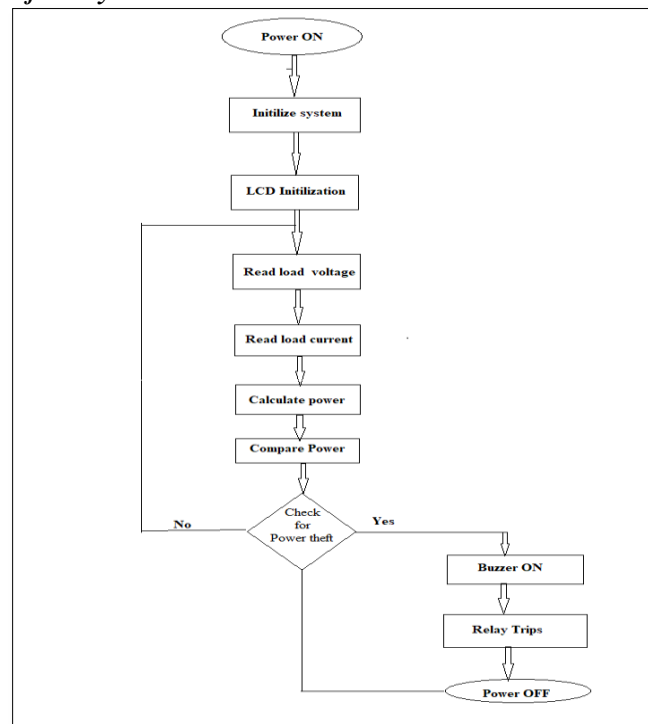


Figure 4: Flow Chart of Power Monitoring & Theft Detection System

1. All of the circuit's components are reset as soon as the system is switched on..( includes LCD initialization, AURDINO initialization)
2. The loads are connected to the distribution network.
3. It's able to quantify voltage and current with the various sensors.

4. Determine the load's energy usage.
5. Compare the amount of power used by the load to the amount of power provided by the supply.
6. Check for power stealing.
7. If the load's output power in watts is about equal to the input power in kilowatts, then the apply the information. In this case, the system reports that there is no evidence of power theft. Hence the system go back to step 3, and this loop is executed until power stealing is detected.
8. After the check the system update the power consumption data to the cloud through AURDINO IDE.
9. When the load's power consumption exceeds the input power, the system detects power theft.
10. This actuates the buzzer and relay sense the status which makes the breaker to open. Hence the system goes to auto shut down.

#### IV. RESULTS & DISCUSSION

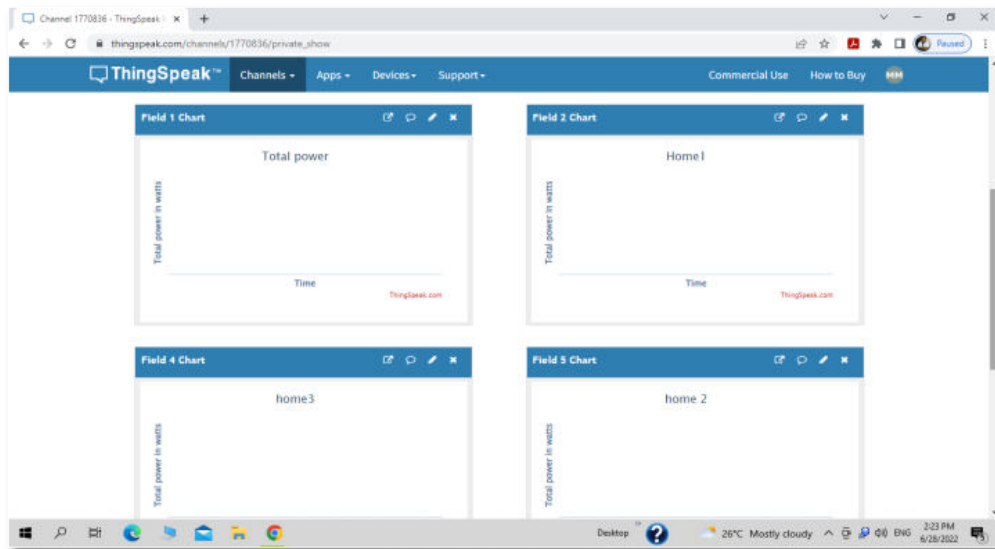


Figure 5: ThinkSpeak channel status before switching ON the system

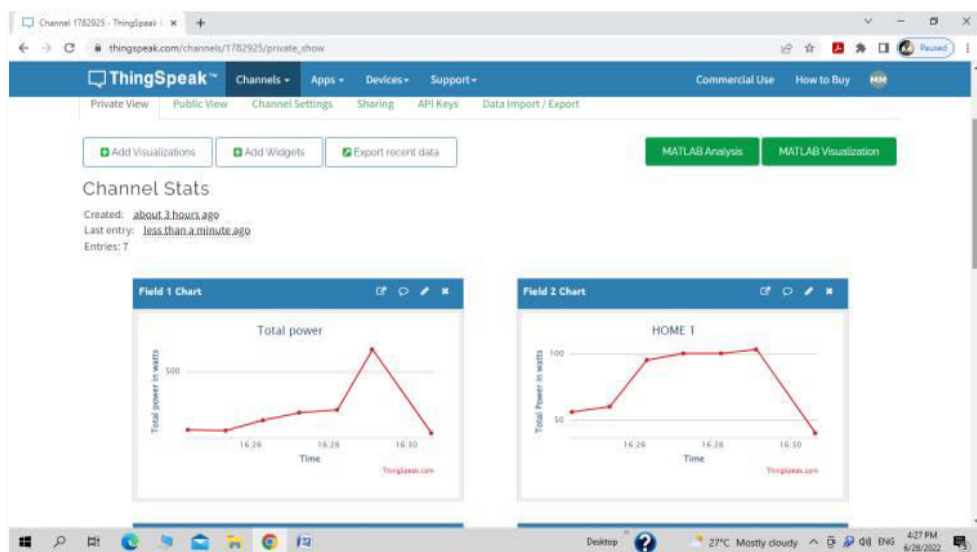


Figure 6: Snapshot of ThinkSpeak channel with loads active

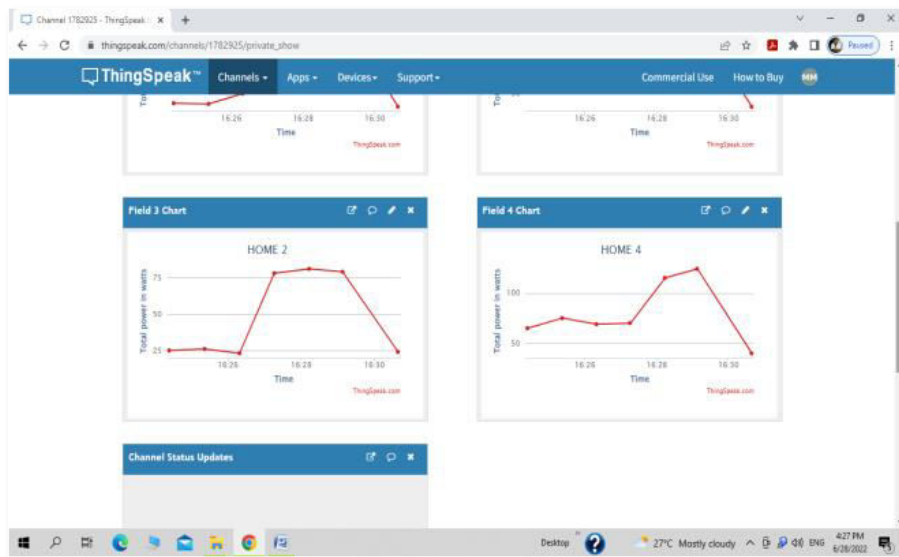


Figure 7: Snapshot of ThinkSpeak channel with theft load active

The images above depict a snapshot of the web browser taken during the system's testing stage. Figure 5 shows a snapshot of the ThinkSpeak channel in the web browser before the system was turned on. During this time, the system will be turned off. That's why there's been no data sent over the internet.

Figures 6 and 7 depict the power system's condition after the module has been turned on. Here, field 1 represents the total input power, field 2 indicates the power absorbed by the load 1, field 2 indicates the power consumed by the load 2, and field 3 indicates the power consumed by the load 3. When the module is switched ON all the power consumption details are feed to the internet, the data consists of power consumed values with respect to the time. The sharp spikes in the waveform indicate the power stealing. The distributor operator can know the power stealing details by accessing the think speak account.

## V. FUTURE SCOPE

The suggested approach may be improved in the future by including implemented for automatic electricity billing system, power fault detection system, with further more implementation, this project can be used to locate the power theft location. With further more improvement in the technology the complete electricity network can be designed to monitor the power, losses, and faults causing in the power system which increases the operating efficiency of the system

## VI. CONCLUSION

An IoT-based power monitoring and thief detection system is presented in this study. An IoT-based architecture was used to install the power monitoring and theft detection system. Every year Electricity board losses huge amount of revenue due to power losses, these power losses also includes the illegal power consumption. There is no way to minimise transmission losses, however there is a way to limit income losses to the electricity board by avoiding power theft. This also solves the problem of electricity shortages in developing countries like India. In the proposed system the operator can easily record the power consumption data of consumer by accessing the internet. And auto power cutoff feature will reduces the illegal power consumption which saves the illegal usage off electricity.

## REFERENCES

- [1] Sagar Shinde, Sachin Marker, Anjali pise, Sagar Salunkh "IOT Based Power stealing Dectcion" *Journal of Optical Communication Electronics Volume 5 Issue 1*.
- [2] Aswini R, Keerthihaa v" IOT based smart energy theft detection and monitoring system for smart home" *IEEEICSCON 2020*.



- [3] M J Jeffin, Madhu G M, Akshayata Rao, Gurpreet singh, c vyjayanthi "Internet of things enables power stealing detection and smart meter monitoring system" *International Conference on Communication and Signal Processing*, July 28 - 30, 2020.
- [4] Leninpugalhanthi, Senthil Kumar, Janani.R, mamtha R.V, Keerthana, nidheesh S " Power stealing Identification System" *2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS 2019)*.
- [5] R. E. Ogu and G. A. Chukwudebe "Development of a Cost-Effective Electricity Theft Detection and Prevention System based on IOT Technology" *2017 IEEE 3rd International Conference on Electro-Technology for National Development (NIGERCON)*.
- [6] R Giridhar Balakrishna P Yogananda Reddy M L N Vital " IOT based Power stealing Detection" *International Journal of Innovations in Engineering and Technology (IJJET)* Volume 8 Issue 3 June 2017.
- [7] S.N.Swami, A.B.Ghayal, H.G.Tamboli, R.R.Suryawanshi "Wireless Electricity Theft Detection by using ZIGBEE Technology" *International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering (An ISO 3297: 2007 Certified Organization)* Vol. 5, Issue 3, March 2016.
- [8] R.Meenal, Kevin M Kuruvilla, Adrin Denny, Rejin V Jose, Renoy Roy "Power monitoring and theft detection using IOT" *International Conference on Physics and Photonics Processes in Nano Sciences Journal of Physics: Conference Series 1362 (2019) 012027*.
- [9] Nilam S. Khairnar, Rahul S. Khairnar "IOT based electricity theft detection" *6th International Conference on Recent Trends in Engineering & Technology (ICRTET - 2018)*.
- [10] Dr. S.Thangalakshmi, G.Sangeetha bharath, S.Muthu "Power stealing prevention in distribution system using smart devices" *International Journal of Applied Engineering Research*, ISSN 0973-4562 Vol. 10 No.42 (2015).
- [11] G. L. Prashanthi, K.V.Prasad "Wireless power meter monitoring with power stealing detection and intimation system using GSM and Zigbee networks" *IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)* e-ISSN: 2278-2834, p-ISSN: 2278-8735. Volume 9, Issue 6, Ver. I (Nov - Dec. 2014), PP 04-08.



**INNO SPACE**  
SJIF Scientific Journal Impact Factor  
**Impact Factor: 8.118**



**ISSN** INTERNATIONAL  
STANDARD  
SERIAL  
NUMBER  
**INDIA**



# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

 **9940 572 462**  **6381 907 438**  **ijirset@gmail.com**



**www.ijirset.com**

Scan to save the contact details