IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 7.39 ⁜ Vol. 11, Issue 3, March 2022

DOI: 10.17148/IJARCCE.2022.11328

Power Monitoring and Power Theft Detection System Using Iot

Ms Aerica Ramteke[1] , Ms Devika Bankar[2] , Ms Achal Punwatkar[3], Ms Trupti Meshram[4], Mr Shreyash Borkar[5], Mrs Jyoti Sathe[6]

UG student, Dept. of Electrical Engineering, Priyadarshini College of Engineering, Nagpur, Maharashtra, India[1-5]

Assistant professor, Dept. of Electrical Engineering, Priyadarshini College of Engineering, Nagpur, Maharashtra, India[6]

Abstract: India is a hotbed of electricity theft especially in rural areas and in the middle and upper populations. Electricity theft is increasing every year in the homes and industries that affect the state of the country's economy. Power theft is usually done in two ways by jumping or hooking. To see it, a proposed system (current measurement and comparison) is proposed in which the distribution of family power is done indirectly from the distribution box to each house. It is currently being rated from time to time in the distributor box and sent to the server of each used house server GSM / GPRS module It is currently being rated from time to time in the distributor box and sent to the server of each used house serve GSM / GPRS module It is currently being rated from time to time in the distributor box and sent to the server of each used house server GSM / GPRS module. The aim of this project is to design a system to monitor energy consumption and to detect and eliminate theft of electricity from transmission lines and electricity meters. This work also focuses on transmitting theft information to the Electricity Board (EB) via IoT. As the network of devices connected as sensors has the ability to exchange real-time information via the Internet. Power is periodically measured in the distributor box and sent to each house server website using a basic IoT dashboard. During the installation of electricity meter user information is stored in a database using a friendly mobile application that includes address, location. The power will be continuously measured in the distribution box and individual meters. Power values will be uploaded to the server on a distributed and one-sided server. This power will be monitored through an IoT dashboard that will be a "Blynk IoT dashboard". In this project, we will look at the power delivered from an AC source to a user and the power consumption by that user. We consider only one user for this project and one distribution box. On the basis of an effective comparison between the current values from the distribution box and the electric meter in the house, if we find the difference between the current from the distribution box and the user meter then theft is detected.

Keywords: Electricity Theft, Monitoring System, Algorithm, Power Line Communication, Power Theft, IoT, NodeMCU.

I.INTRODUCTION:

Electrical theft is a criminal practice of stealing power. As the population grows the demand for electricity increases. Power plants have been installed to meet the growing demand. Due to the depletion of natural resources the gap between supply and demand is growing steadily. A large amount of energy is required for the integrated steel plants to meet this requirement. In some areas the distribution of electricity exceeds the capacity given to that area. This leads to the theft of power or power exercised by unwanted users or unknown users. We need a system that can detect theft in power lines to avoid unnecessary power consumption. By using this example we can detect theft and possibly save a lot of electricity that can be used effectively on metal plants. In this energy theft detection and power monitoring project, a current sensor and controller will be used. This current sensor provides the current state of the energy value from the ac source. There will be two pairs of current sensor and controller to use. One pair will be used in the distribution box (meter to AC source) and one pair will be connected to the user's meter to monitor the actual current and current usage of the user. The IoT mobile app used by "Blynk" is a free mobile software application that connects the controller to the internet and has a live monitoring feature that helps the user to monitor power and detect theft in a remote location. The Blynk app will display readings on the meter gauge or in any other way. To provide internet access to objects (IoT), a NodeMCU microcontroller integrated with a single-board Wi-Fi module is used. NodeMCU is a Wi-Fi module that provides internet service on a small controller to run a given user command. NodeMCU is used to control performance.it will receive data from the current sensor and according to the value will show results in the Blynk and LCD application. The controller provides the data to the Io-based application and then according to the instructions provided or the system will provide command signals to the relay or switch that will control the load. Current sensor is usedACS712 which is 5ampere current sensor detecting the overload current from the AC source. A voltage sensor in

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 7.39 ⁜ Vol. 11, Issue 3, March 2022

DOI: 10.17148/IJARCCE.2022.11328

the form of transformer will also use to detect voltage range but normally voltage doesn't change its value so we are focusing over current variations. For display the output LCD display is used which is connected to the controller.

II.METHODOLOGY

Objectives :

• Monitor the power at distributor box and user meter.
• Connect IOT dashboard to the controller for monitoring and detection.
• Collect the data from distributor box and from sub meter at Blynk dashboard.
• To detect the power theft automatically without engaging any man powers by developing a cost effective and efficient system.
• To detect the power theft automatically without engaging any man powers by developing a cost effective and efficient system.
• To develop a web based mobile app for the authorized officials of electricity board to keep track of all the thefts, area of thefts and the direction to reach the area under theft.
• To maintain the record of the total number of electric units consumed by users in the server database periodically and makes online bill payment system.
• To develop a global website that would maintain the analytics of the thefts and the probable area under theft using multi-color graphs and pictorial representations which would make the theft analysis easier and can also predict the thefts that may happen in future.
• Notify when theft is detected.

III.HARDWARE DESCRIPTION

A. Node MCU controller: NodeMCU is an open-source Lua based firmware and development board specially targeted for IoT based Applications. It includes firmware that runs on the ESP8266 Wi-Fi SoC from Espressif Systems, and hardware which is based on the ESP-12 module.

Features:

• 5V power supply.
• Serial I2C control of LCD display using PCF8574.
• Backlight can be enabled or disabled via a jumper on the board.
• Contrast control via a potentiometer.
• Can have 8 modules on a single I2C bus (change address via solder jumpers) address, allowing.

B. LCD DISPLAY: Liquid Crystal Display is a display which uses its first form of operation. Here the load is monitored continuously by the Arduino UNO. If there are increases in load the message is sent regarding power usage to the electric board and display on the LCD.A liquid-crystal display (LCD) is a flat-panel display or other electronically modulated optical device that uses the light-modulating properties of liquid crystals combined with polarizers.

Features:

• 20 characters wide, 4 rows.
• White text on the blue background.
• The module can easily interface with an MCU.
• The module is a low-power consumption character LCD Module with a built-in controller.
• Single LED backlight included can be dimmed easily with a resistor or PWM.
• Can be fully controlled with only 6 digital lines! (Any analog/digital pins can be used).

C. Current Sensors: A current sensor is a device that detects and converts current to an easily measurable output voltage, which is proportional to the current through the measured path. There are a wide variety of sensors, and each sensor is suitable for a specific current range and environmental condition. Among these sensors, a current sensing resistor is the most commonly used. It can be considered a current-to-voltage converter, where inserting a resistor into the current path, the current is converted to voltage in a linear way. The technology used by the current sensor is important because different sensors can have different characteristics for a variety of applications.

Features:

• Low-noise analog signal path.
• Device bandwidth is set via the new FILTER pin.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 7.39 ⁜ Vol. 11, Issue 3, March 2022

DOI: 10.17148/IJARCCE.2022.11328

• 5 µs output rise time in response to step input current.
• Small footprint, low-profile SOIC8 package.
• 2.1 kVRMS minimum isolation voltage from pins 1-4 to pins 5-8.
• Supply Voltage: 4.5V~5.5V DC.
• Measure Current Range: 30A.
• Sensitivity: 100mV/A.

D. I2C MOUDULE: I2C Module has a inbuilt PCF8574 I2C chip that converts I2C serial data to parallel data for the LCD display. These modules are currently supplied with a default I2C address of either 0x27 or 0x3F. To determine which version you have check the black I2C adaptor board on the underside of the module. If there 3 sets of pads labelled A0, A1, & A2 then the default address will be 0x3F. If there are no pads the default address will be 0x27.

Features:
• 5V power supply.
• Serial I2C control of LCD display using PCF8574.
• Backlight can be enabled or disabled via a jumper on the board.
• Contrast control via a potentiometer.
• Can have 8 modules on a single I2C bus (change address via solder jumpers)address, allowing.
• Size : 41.6 x 19.2 mm.

IV.SOFTWARE DESCRIPTION

Software used:

A. Arduino IDE: The open-source Arduino Software (IDE) makes it easy to write code and upload it to the board. This software can be used with any Arduino board. The Arduino Integrated Development Environment - or Arduino Software (IDE) - contains a text editor for writing code, a message area, a text console, a toolbar with buttons for common functions and a series of menus. It connects to the Arduino hardware to upload programs and communicate with them.

Programs written using Arduino Software (IDE) are called **sketches**. These sketches are written in the text editor and are saved with the file extension .ino. The editor has features for cutting/pasting and for searching/replacing text. The message area gives feedback while saving and exporting and also displays errors. The console displays text output by the Arduino Software (IDE), including complete error messages and other information. The bottom right hand corner of the window displays the configured board and serial port. The toolbar buttons allow you to verify and upload programs, create, open, and save sketches, and open the serial monitor.

B. Blynk Android Application: Blynk was designed for the Internet of Things. It can control hardware remotely, it can display sensor data, it can store data, visualize it and do many other cool things.

There are three major components in the platform:

Blynk App - allows to you create amazing interfaces for your projects using various widgets we provide.

Blynk Server - responsible for all the communications between the smartphone and hardware. You can use our Blynk Cloud or run your private Blynk server locally. It's open-source, could easily handle thousands of devices and can even be launched on a Raspberry Pi.

Blynk works over the Internet This means that the hardware you choose should be able to connect to the internet. Some of the boards, like Arduino Uno will need an Ethernet or Wi-Fi Shield to communicate, others are already Internet-enabled: for example like the ESP8266, Raspberri Pi with WiFi dongle, Particle Photon or SparkFun Blynk Board.

Features:
• Similar API & UI for all supported hardware & devices
• Connection to the cloud using:
• Wi-Fi
• Bluetooth and BLE
• Ethernet
• USB (Serial)
• GSM
• Set of easy-to-use Widgets
• Direct pin manipulation with no code writing
• Easy to integrate and add new functionality using virtual pins

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 7.39 ⁜ Vol. 11, Issue 3, March 2022

DOI: 10.17148/IJARCCE.2022.11328

• History data monitoring via SuperChart widget
• Device-to-Device communication using Bridge Widget
• Sending emails, tweets, push notifications, etc.

V.METHOD

• The method includes receiving meter data of the:
• measured power consumed by a customer,
• receiving delivered power data that includes data of the power delivered to the customer,
• determining that the difference between the meter data and the delivered power data is greater than a predetermined amount
• Indicating a discrepancy if the difference between the meter data and the delivered power data is greater than a predetermined amount.
• We will collect value from distributor box as well as user meter with the help of current sensor (ACS712) used. This sensor is connected to the controller; sensor is sending current values to the controller which will indicate on LCD and also on IOT dashboard (Blynk app).

VI.WORKING AND PRINCIPLE

In this project to detect power theft and monitor power, pair of current sensor and controller is going to use. This current sensor provides the current status of power value from the ac source. There will be two pair of current sensor and controller going to use. One pair will use at distributor box (meter at AC source) and one pair will be connected at user meter to monitor actual current and current consumed by user.

The IOT mobile application used is “Blynk” app is free mobile application software that connects controller with the internet and it has a live monitoring feature which helps the user to monitor power and to identify theft from a remote location. Blynk app will indicate a reading in meter gauge or in any other form. To provide internet of things (IoT) access, NodeMCU which is a microcontroller integrated with the Wi-Fi module on a single board is used

NodeMCU is a Wi-Fi based module that provides an internet service to the microcontroller to execute the given command from the user. NodeMCU is used to control the operation.it will get data from current sensor and according to the value it will show the results on Blynk app and LCD. Controller give the data to the IOT based application and then according to the commands given or the programming it will give command signals to the relay or switch which will control the load.

VII.LITERATURE SURVEY

In a research project conducted by P. Jokar et al. [1], the authors introduced a power theft detector based on a usage pattern, find a suspicious use pattern. Areas with high potential for malicious use patterns are marked, and with extraordinary vigilance in usage patterns, suspicious customers are identified. Separation and integration methods are used. Also, the use of transformers and non-standard detectors, makes the algorithm stronger against aggressive change of application pattern and provides higher and adjustable performance at a lower sample rate.

In a research project conducted by M. Tariq et al. [2], stochastic Petri net formalism is used in this paper to identify and localize the occurrence of crime in grid-assembled MGs. Disruption at any time in the form of resistance beyond the limit of intelligent data collected, regardless of the operating method, initiates a modification given to the arc, which informs the transmission module. Affected changes and suspicious user information are sent to the Meter Data Management System (MDMS) for local theft. In testing, it calculates technological and nontechnical losses with complete accuracy without having to know the exact topology of the power distribution network.

In a research project conducted by A. J. Dick [3], a researcher looks at income-generating activities within the UK to combat the problem of electricity theft, which is estimated to cost the electricity industry (EI) approximately 50 meters per year. It first analyses the nature and severity of the problem, notes the incidents related to different types of theft and interference, and then indicates the legal framework. Then a report is made on the stated process.

In a study conducted by N. Mohammad et al. [4], researchers are proposing a cost-effective measurement system to control power theft. Smart meters are used and installed on all customer units and the server is maintained. Both the meter and the server are equipped with a GSM module, which allows for two connections. Several ways to combat electrical-related malpractice have been described. Electricity theft can be reduced by using these methods.

A. Power Theft Identification Using GSM Technology

In the system proposed by Rhea Prakash, E. Annie Elisabeth Jebaseeli, Y.S.U.Sindhu crime detection was done using a PIC microcontroller, sensor, GSM module and LCD display. As we know that theft of electricity is usually done by

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 7.39 ⁜ Vol. 11, Issue 3, March 2022

DOI: 10.17148/IJARCCE.2022.11328

passing meters. The heart of the system is Arduino control as it contains two microcontrollers. The project basically consists of two CTs one is mounted on one part of the pole and the other is connected to the other end of the pole and the local voltage pattern is processed by the output of two CTs in the Arduino control when the power goes down. the limit exceeds the maximum allowable number of resources provided it means that the theft load is connected to the system received by the Arduino controller and delivers the message to the service using the GSM module installed in the Arduino kit. The data provided to Arduino is collected and analysed using MATLAB and the location of the theft is retrieved and action taken. In this project the theft is detected using real-time data without any human interface. [5]

In a research project conducted by K. L. Joseph et al. [6], the authors have worked on the fact that persistent theft, corruption, and declining price structure have made it almost impossible for government services in India to improve power service. As a result, industrial buyers across India are moving out of a state-owned system and relying on power generation on their site to ensure a stable and reliable source of electricity. The Electricity Act of 2003 promotes the continuous production of energy from these captive plants through its open access clause. By encouraging the growth of these captive power stations, politicians in India established a dual track economy, where state run production and market operations coexist. This strategy allows politicians to promote the involvement of the private sector in the electricity market, without compromising the support of key political regions at the state level.

B. Distribution Line Monitoring System for the Detection of Power Theft Using Power Line Communication

In the proposed system there is a condition for the theft of electricity using the connection of power lines. Basically for this system high frequency is added to the maximum power between 3 kHz to 500 kHz according to Indian power standards. When the power cord is switched off and there is a fluctuation in the system frequency that is analysed at the station using the Matlab System and the location of the power supply is detected and due to the provision of high frequencies the equipment connected to the stolen load fails. In this operation the theft of electricity is detected and action is taken without human interference. [7]

C. IoT based Power Theft Detection (IJIET 2017)

In the program proposed by R Giridhar Balakrishna, P Yogananda Reddy, M L N Vital To avoid power theft they use the IoT system to detect power theft and is done using Arduino, GSM, LCD, ESP module and current transformer. Between two CTs one is connected to the source side and the other is connected to the loading side and the signals of both CTs are supplied to Arduino. Arduino basically compares both data obtained in CTs from source and load side. If any difference is more than tolerable it means that there is a connection theft, then using the IoT and ESP module that works online this data is sent to the channel, if the internet has failed to use the GSM module used to send a message to the station where that line is connected when the stolen cargo is found. In this system energy recovery is done using IoT and GSM. In the event of a failure of the IoT system GSM will work well to ignore this major global threat of power theft in the power network. [8]

D. IoT Based Power Theft Detection And Monitoring System (IJIREICE 2017)

In the system proposed by N Kunan1, Poornima BK2 used an intelligent power meter connected to the beginning of the transmission line and one to the side of the load, signals from both supplied to Arduino. Arduino collects data from each consumer's smart meter and compares that data with the current source given to the source side smart meter if the difference is within tolerance means there is no connected theft load, if the difference is greater than tolerance then the theft load is connected to the system and the system will be divided using a relay circuit and a message will be sent to the service company using the GSM module. The whole process was done using Arduino and continuously using the black Beagle bone system. Therefore, in this system online power theft is detected and the necessary action is taken without human interference. [9]

In a research work done by J. Nagi et al. [11], the authors have been working on finding effective ways to detect electrical fraud which has been the subject of active research in recent years. This paper introduces a mixed approach to non-technical (NTL) loss of electronic resources using genetic algorithm (GA) and vector support (SVM). The main impetus for this study is to help Tenaga Nasional Berhad (TNB) in Malaysia reduce its NTLs in the distribution sector. This hybrid GA-SVM combination prepares customers suspected to be tested locally for fraud based on unusual use. The proposed method uses customer load profile information to expose unusual behaviors that are known to be strongly associated with NTL activities. GA provides increased integration with SVM hyper-fully-effected parameters worldwide using a combination of random and human-generated genomes. The result of the fraud detection model identifies the separate classes used to screen potential fraud suspects for local investigation. Imitation results confirm that the proposed method is more effective when compared to current actions taken by TNB to reduce NTL operations. In a study conducted by T. B. Smith [10]

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 7.39 ⁜ Vol. 11, Issue 3, March 2022

DOI: 10.17148/IJARCCE.2022.11328

VIII.CONCLUSION

This method reduces the heavy power and revenue losses that occur due to power theft by customers. By this design it can be concluded that power theft can be effectively curbed by detecting where the power theft occurs and informing the authorities. The proposed system will be hidden in electric meters in such a way that as soon as the difference between current crosses the threshold value, an automatic message and email will be sent to the concerned authority along with its location and image of that particular area.

IX.REFERENCES:

1. P. Jokar, N. Arianpoo and V. C. M. Leung, "Electricity Theft Detection in AMI Using Customers' Consumption Patterns", IEEE Transactions on Smart Grid, Vol. 7, Issue 1, Jan. 2016, pp. 216-226. Doi: 10.1109/TSG.2015.2425222
2. M. Tariq and H. V. Poor, "Electricity Theft Detection and Localization in Grid-Tied Microgrids", IEEE Transactions on Smart Grid, Vol. 9, Issue 3, May 2018, pp. 1920- 1929. Doi: 10.1109/TSG.2016.2602660
3. A.J. Dick, "Theft of electricity-how UK electricity companies detect and deter", Proc. of European Convention on Security and Detection, 1995, Brighton, UK, 16-18 May 1995, pp. 90- 95. Doi: 10.1049/cp:19950476
4. N. Mohammad, A. Barua and Muhammad A. Arafat, "A smart prepaid Energy metering system to control electricity theft", Proc. of 2013 International Conference on Power, Energy and Control (ICPEC), Sri Rangalatchum Dindigul, India, 6-8 Feb. 2013, pp. 562-565. Doi: 10.1109/ICPEC.2013.6527721
5. Rhea Prakash, E. A. (2017). Power Theft Identification Using GSM Technology. International Journal of Advanced Research in Electrical,Vol. 6
6. K. L. Joseph, "The politics of power: Electricity reform in India", Energy Policy, Vol. 38, Issue 1, January 2010, pp. 503-511. Doi: https://doi.org/10.1016/j.enpol.2009.09.041
7. Guhesh Swaminathan, M. S. (n.d.). Distribution Line Monitoring System For The Detection Of Power Theft Using Power Line Communication
8. R Giridhar Balakrishna, P. Y. (2017). IoT based Power Theft Detection. IJIET
9. N Kunan, P. B. (2017). IoT Based Power Theft Detection And Monitoring System (IJIREICE 2017). International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering ISO 3297:2007 Certified Vol. 5
10. J. Nagi, K. S. Yap, S. K. Tiong, S. K. Ahmed and A. M. Mohammad, "Detection of abnormalities and electricity theft using genetic Support Vector Machines", Proc. of TENCON 2008 - 2008 IEEE Region 10 Conference, Hyderabad, India, 19-21 Nov. 2008, pp. 1-6. Doi: 10.1109/TENCON.2008.4766403

