International Journal of Technology Engineering Arts Mathematics Science
Vol. 1, Iss. 2, July-December 2021, pp. 14~18
ISSN: 2583-1224

Energy Meter Tamper Detection and Alert Messaging System

Yash Amol Rathod, Abhijeet Babu Peddawad, Kshitij Jitendra Jagtap, Nikhil Nagendra Gangnelu, Dr. S. M. Bakre, Dr. Mrs. A. D. Shiralkar
Dept. of Electrical Engineering, AISSMS-IOIT, Maharashtra, India.
Corresponding Author: Abhijeet Peddawad (abhijeet007peddawad@gmail.com)

Article Information

Article history:

Received December 12, 2021
Revised January 13, 2022
Accepted January 13, 2022

ABSTRACT

The theft of electricity is a matter of concern for the distribution utility today. The AT&T loss of Maharashtra State Electricity Distribution Company is 20.72% for the year 2020-21. The main cause of such a higher loss is theft of electricity. Various wireless communication systems are available to detect the theft of electricity, but the utilities do not have the infrastructure to operate them. The aim of the paper is to develop a novice cost effective system for monitoring the power consumed by the load and detect the theft of electricity. This work also focuses on sharing theft information with the distribution utility through the Internet of Things (IoT) technology. As a network comprises of connected devices such as sensors, it can exchange information in real time via the internet. In this project, NodeMCU is used which sends alert to the authorized persons. The main benefit of the proposed system is saving in power consumption. The proposed system is a novice, feasible and economically viable.

KEYWORDS: Tampering, ESP8266, NodeMCU, Current sensors, Blynk Mobile App, IoT

1. INTRODUCTION

Maharashtra State Electricity Distribution Company (MSEDCL) is one of the largest distribution utilities in India and Asia. It has a vast consumer base of more than 2 Crore 70 lakh consumers. The overall Aggregate Technical and Commercial (AT&C) loss in the year 2006-07 of the company was as high as 33.89%. The measures were taken such as replacement of faulty meters, providing metering cubicles and metering boxes and appropriate sealing arrangements. As result, the AT&C losses were reduced to 20.73% for the year 2020-21. In order to further reduce losses, it is necessary to detect theft cases and take action. Following are some of methods of tampering of energy meters.

- Neutral current reversed
- Phase current reversed
- Phase and neutral current reversed
- Current bypass method
- Partial load earthed and neutral current reversed
- Partial load earthed and phase current reversed
- Full load earthed returned
- Full load earth and current reversed
- Partial load earthed returned

This paper presents a novice method of detection of theft.

2. THE PROPOSED METHOD

The proposed method involves use of hardware and software resources as discussed below [1].

2.1. Hardware Tools

The pin connection diagram of ESP 8266 microcontroller is shown in **Fig. 1**. ESP 8266[2] can be described as a computer on a chip. It is an integrated chip that is usually a part of an embedded system. It is a self-contained, independent and yet functions as a tiny, dedicated computer. It also supports IoT Applications due to built-in Wi-Fi connectivity [3].

It is a system-on-chip (SoC) that incorporates a 32-bit microcontroller, antenna switches, power amplifier,

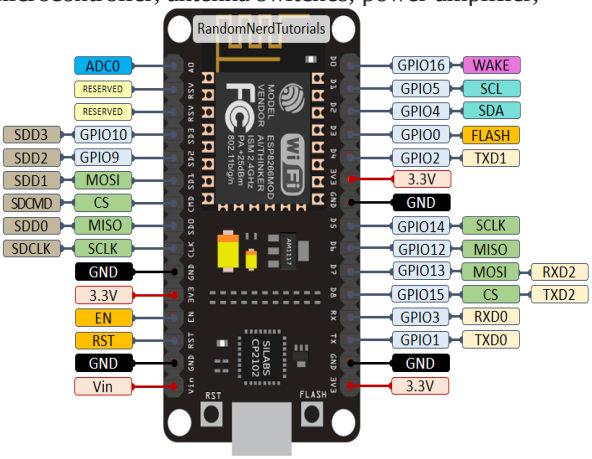

Fig 1. ESP 8266 Microcontroller

and filters. It is compatible of 2.4 GHz, Wi-Fi (802.11 b/g/n), general-purpose input/output (16 GPIO), Inter-Integrated Circuit, Analog-to-Digital Conversion (10-bit ADC), Serial Peripheral Interface (SPI), I²S interfaces with Direct Memory Access-DMA (GPIO), Universal Asynchronous Receiver Transmitter-UART (GPIO2), and Pulse-Width Modulation (PWM). This tiny module enables microcontrollers to link to a Wi-Fi channel and create basic TCP / IP connections [4].

This is the heart and the brain of the proposed paper as it accepts the input from the sensors and initiates action according to the code entered in Embedded C Language. The programming Software used for this purpose is Arduino IDE [5].

2) Current Sensor-(ACS712): -In this method, two Current sensors [3] are used (At source side and load side). The sensor is connected in series with the load from the source to the load side. The current rating is 5 Amp ranging from 0 to 30 Amp.

3) Switches -Switches are used to Power ON / OFF the Load at the theft side as well as at the actual load Side. These switches are of 10 Amp ratings each [6].

4) Load-In this system, we have used bulb as the load. As such, the load is resistive. Approx. power rating of the bulb is 5-9 Watt. This load is connected at the theft side as well as at the actual side. Although the experiment is performed using resistive load, any type of load is preferred [7].

5) Buzzer- the buzzer is a mechanical, electromechanical, or piezoelectric, audio signal device. The common uses for buzzers and beeps include alarms, timers, and confirmation of user inputs such as mouse clicks and keystrokes. In this project, the buzzer plays an important role in alerting authorized people when theft is detected.

6) Power Supply- the 9 Volt battery is used to power the control circuit of the project. Controller supports from 7-12 Volt DC Supply. Once the power is received, it generates the 5V and 3.3V signal across its V_{CC} and GND Pins.

The functional block diagram of ESP 8266 Microcontroller is shown in **Fig. 2** [8]. As shown in Fig.2, the current sensors based on the load side and source side are used and the input current given by sensors is converted to digital where Arduino compares the value, i.e. difference between the values of current sensors and if there is difference greater than zero, it displays the alert message on the LED panel as well the alert notification goes to the authorized person's mobile via Blynk App thus helping them to know theft defection and if there is no difference in values then no alert is detected[9].

2.2 Software Tools

Following are the software tools required for processing data and report generation [3].

Blynk Mobile App: -

It is the advanced Cloud platform that supports IoT Projects and provides the platform to design the Graphical user Interface (GUI). Below is the step to integrate the GUI in Mobile App.

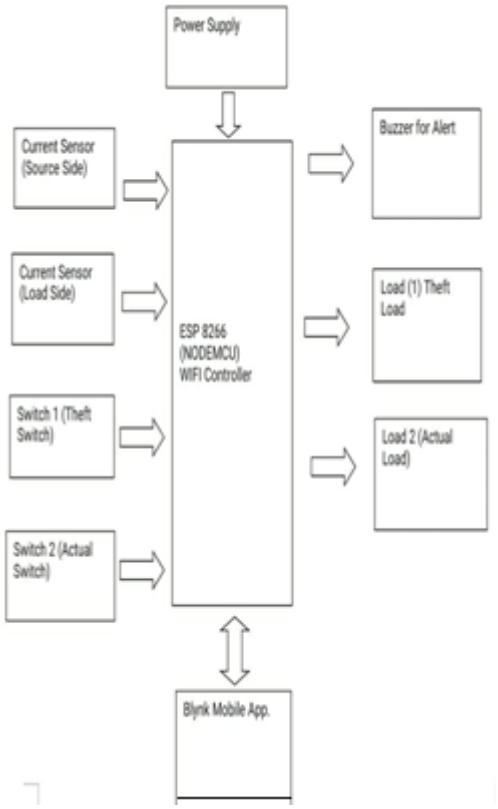

Fig. 2. Functional Block diagram

The link is connected in parallel to the meters. The following equations are established [10].

$$V=I_L R \quad (1)$$

$$V=Is R \quad (2)$$

Where V is the applied voltage in volts across the link.

R is the resistance of the link in ohms

L is the length of link in meters

A is the area of cross section of link in sq. meter

P is resistivity of link in ohm-meter.

such that

$$R = \rho l / A \quad (3)$$

3. METHDOLOGY

The methodology used in the proposed method is based on the IoT based theft detection system. The ESP8266 (NodeMCU) microcontroller and GSM system is used to detect theft. In this method, the current sensors are used which will be connected to the source side as well as load side which will measure amount of current supplied and units consumed by the load. Ideally current sensed by source sensor and the load sensor should be equal. However, considering electric losses the minimum limit is introduced to trigger alarm. But if there is power theft the total load will be equal to the theft load plus the actual load, hence the alarm will be triggered if theft is detected. In the same way the notification will be sent via Blynk App [4] technology.

Figure 3 shows a flow chart explaining a flow of logic in a proposed system. The logic is based on polled approach. The current sensed by the current sensor is the analog quantity [11].

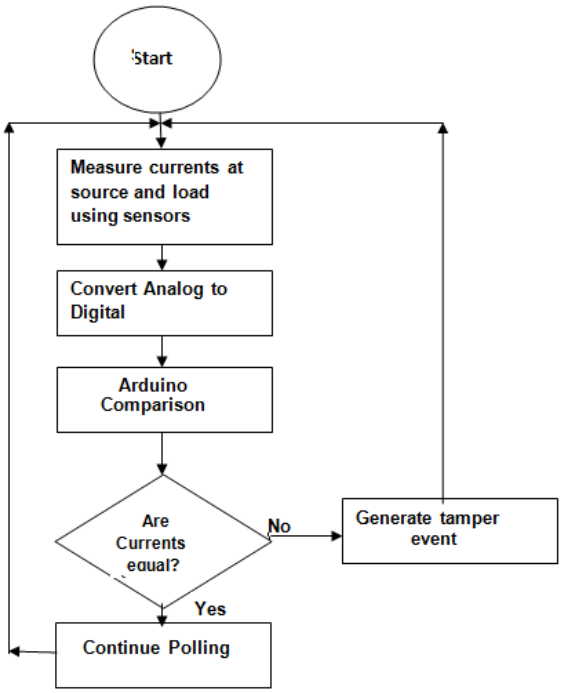

Fig.3. Flow chart

In order to convert this analog quantity into digital form as required by the Arduino processor, the ADC is used. The values of source current and load current are compared by the processor. If the values are unequal the tamper event is generated and messaged. Further, the theft consumption is added to the billed units of the consumer. If the currents are equal the system is assumed to be normal and the process of polling is continued [5].

4. METER TAMPERING THROUGH PARALLEL RESISTANCE

As shown in Fig. 4, the meter is tempered by connecting resistor is parallel with the meter so that the incoming current is bifurcated into billing current and resistive current. In this way the billing current is reduced by dividing it in two parts. For example, as shown in Fig. 4, the billing current is 5 Amp. By connecting resistor in parallel with meter the 5 Amp current is reduced to 2 Amp and balance 3 Amp current flows through the resistor or a link. Thus, instead of 5 Amp the billing would be done on 2 Amp. Unfortunately, the microcontroller provided in numeric meter would be unable to detect this tamper event as it is based on 3 Amp input current. How to detect this tamper event is therefore a matter of concern. The processor of the meter cannot detect that the current is diverted to resistive path. Therefore, no tamper event is generated. Using IoT technology, it is possible to detect tamper through parallel, series and series parallel combination [5]. Therefore, it is required to provide IoT based smart sensors for the detection for such cases. The detection of tamper event by connecting resistor in parallel with meter can be worked out as follows. Select two identical CT Sensors suitable to the secondary current of meter CTs. Such sensors are usually available with the manufacturers of instrument transformers [6].

5. OBSERVATIONS

The condition of tampering of a single-phase static meter was developed in a laboratory. This was named as a main meter. In order to compare the consumption, the main meter was connected in series with the check meter. The condition of tamper was created by connecting link across the main meter to get an idea of parallel resistance. See Fig. 4. The resistance was chosen in such a way that 2 Amp current flows through meter and 3 Amp through a parallel resistance link. The consumption was recorded for the period of one hour. Some readings were noted by connection link and some by removing link at different load conditions [7].

Three parameters were recorded namely- Current, kWh of main meter and kWh of check meter. In all, 10 observations were recorded during the period of one hour. The difference of consumption between main meter and check meter was computed. A very low difference is truncated as zero. Refer Table 1. When the difference is not zero, the tamper indication is generated and the amount of difference is added to the kWh consumption of main meter.

Using the blynk app we get an alert notification that the theft has been detected. Fig. 5 shows the pattern of consumption through the check meter, main meter and link.

Table I. Recording of one hour consumption

Current Amp	5	4.34	**4.7**	**5**	**4.5**	3	2	1	**1**	2.8
kWh Main Meter	1.15	0.998	**0.59**	**0.57**	**0.529**	0.69	0.46	0.23	**0.5**	0.60
kWh Check Meter	1.16	0.999	**1.08**	**1.15**	**1.03**	0.69	0.47	0.232	**1.23**	0.64
Theft Units (kWh)	0	0	**0.49**	**0.58**	**0.501**	0	0	0	**0.73**	0

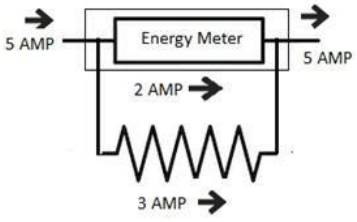

Fig.4. Meter tampers through parallel resistance

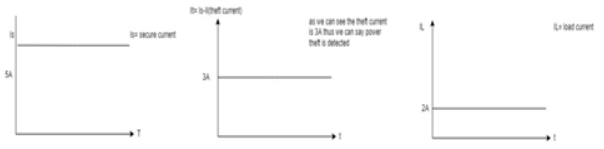

Fig 5 (a) Check meter

Fig 5(b) Main meter

Fig 5(c) Parallel resistor or Link

Fig.5. Pattern of current through meter and link

5. CONCLUSION

The main hurdles in revenue generation of the distribution utility are high AT&C losses. Higher losses indicate probability of theft of electricity. The single-phase billing meters installed at consumer installations are static meters. The existing arrangement is unable to detect tampering of meter done through parallel resistors connected across the meter in form of link. This paper has discussed an act of tampering of meter by inserting resistance in parallel with the meter. The novice and cost-effective method to detect this event using IoT Sensors and microcontroller (ESP 8266, Node MCU) and Blynk mobile app is suggested in this paper. The proposed method is found to be suitable and feasible.

REFERENCES

[1] Mucheli, N.K., Nanda, U., Nayak, D., Rout, P.K., Swain, S.K., K Das, S., & Biswal, S.M. (2019). *Smart Power Theft Detection System. 2019 Devices for Integrated Circuit (DevIC)*, 302-305.

[2] V. K. Jaiswal, H. K. Singh and K. Singh, "Arduino GSM based Power Theft Detection and Energy Metering System," *2020 5th International Conference on Communication and Electronics Systems (ICCES)*, 2020, pp. 448-452.

[3] Pallavi Sethi, Smruti R. Sarangi, "Internet of Things: Architectures, Protocols, and Applications", *Journal of Electrical and Computer Engineering*, vol. 2017, Article ID 9324035, 25 pages, 2017

[4] S. Manocha, V. Bansal, I. Kaushal and A. Bhat, "Efficient Power Theft Detection using Smart Meter Data in Advanced Metering Infrastructure," *2020 4th International Conference on Intelligent Computing and Control Systems (ICICCS)*, 2020, pp. 765-770.

[5] K. V. Blazakis, T. N. Kapetanakis, and G. S. Stavrakakis, "Effective Electricity Theft Detection in Power Distribution Grids Using an Adaptive Neuro Fuzzy Inference System," *Energies*, vol. 13, no. 12, p. 3110, Jun. 2020, doi: 10.3390/en13123110.

[6] Financial report published by Maharashtra State Electricity Distribution Co. Ltd (MSEDCL), Corporate Office, Prakashgad, Mumbai for the year 2019-20 (www.mahadiscom.in).

[7] Maharashtra State Electricity Distribution Co. Ltd-14th Annual Report, 2018-19).

[8] M. Uvais, "Controller Based Power Theft Location Detection System," *2020 International Conference on Electrical and Electronics Engineering (ICE3)*, 2020, pp. 111-114,

[9] Ramesh Gaonkar, 'Fundamental of microcontrollers in embedded systems', PHI Publishing.

[10] RMD Sundaram, K.Vasudevan, Abhishek Nagarajan, 'Internet of Things', Wiley Publishing House.

[11] Dr. Shashikant Bakre,'Electricity metering in easy steps, an outline book on smart energy meters for every one', Amezon KDP Publishing