A REVIEW ON IOT BASED POWER THEFT DETECTION

Akhil K. George Abraham[1], Alen Joseph[2], Joel Benny Thomas[3], K Kanchana[4],
Sneha Priya Sebastian[5]
[1,2,3]UG Students,[4,5]Professors,
Department of EEE,
Mar Baselios Christian College of Engineering and Technology
Kuttikkanam, Peermade, Kerala, India.

Abstract : Power theft detection and control system using the IOT give a better and less costly way to transfer the power to the consumer wirelessly as power theft is a serious problem faced by all utilities. This method is used to detect the theft of electricity which can be done by using power which is not read by the energy meter. In this paper, main purpose is to monitor the power consumed by a model organization such as household consumers, various industries etc. Detection and control of power has been done by calculating the electricity consumed by the user with the help of meter. Electricity meter consists theft detection unit which will notify company side in the event of meter tempering or theft practice occur in electricity meter and also it will send information regarding theft detection by using modem and the theft detected will be displayed on the terminal screen or window of the company side, so that they send message to the registered contact number of the customer as a warning. Due to this, customer receive the warning message even though they are continue using the excess power then Electricity board section will cut the power supply of the customer. IOT operation can be performed by Wi-Fi device which sending meter data to the web page through the IP address. The IOT technology is used so that Electricity board section can conduct online monitoring of the consumption of power and billing information that is calculated using microcontroller.

Index Terms - ***Internet of things, detection, electricity theft, microcontroller, IP address, electricity meter.***

I. INTRODUCTION

Energy utilities lose large amounts of cash each year due to fraud by means of electricity customers. Electricity fraud can be defined as a dishonest or unlawful use of electrical equipment or service so that it will avoid billing price. It is difficult to distinguish between sincere and dishonest clients .Realistically, electric powered utilities will never be capable of getting rid of theft. It is possible, however to take measures to detect, prevent and reduce indecent activities[1]. Investigations are tested via electric application agencies to evaluate the effect of technical losses in the technology, transmission and distribution networks, and the general overall performance of power networks. [2]–[5]. Energy monitoring cannot be done efficiently mainly because consumers are not aware of their energy consumption. They will get an idea about their consumption only when the electricity bills are issued [6].

The installed capacity of the power sector in India is 356.10 Giga Watts as of March 2019, which includes renewable and non renewable sources. The per capita electricity consumption in India in 2016-2017 was 1,122 kWh [7]. The IOT has recently become world wide to highlight the vision of a global structure of interconnected physical objects. As more range of power-eating products entering daily lives, together with electrical motors and superior heating, air flow, and air con structures, load demand increases dramatically and energy required at high quantity [10 So in this paper proposed an electricity theft detection system to hit upon the theft that's made via the most commonplace manner of doing the theft and this is , with the aid of using excess energy beyond the restrict of meter. At this point of technological improvement, the hassle of illegal usage of power can be solved electronically without any human manage beside meters are related to the net using IOT idea. So there's a provision for the customers to music their power intake from time-to-time with a view to manipulating their consumption as they desire.

This method is beneficial for each client and the provider. This system permits the supplier to disconnect the connection from a distant server in case the purchaser fails to pay his/her power invoice. This approach eliminates the want of human electricity at some point of disconnection and reconnection of the burden. any other essential benefit of this approach is that it will tell the dealer side about any theft that is happening inside the system.

II. LITERATURE SURVEY

In [12], a brand new method towards Nontechnical loss (NTL) detection in electricity utilities the usage of synthetic intelligence-based method and pattern category method so that you can locate and pick out load intake patterns of fraud customers. on this device client committing fraud activities before the 2 year length will not be detected by means of the FDM. In [13], [14] and [15] numerous theft detection approach was proposed, based totally on purchaser no longer paying the bill, bypassing the poles, reception of misused power, tapping on a transmission line as defined. In [16], unearths out on which electrical line there may be tapping. this is a real time machine. wi-fi records transmission and receiving technique is used. this could offer an extra facility of wireless meter studying with the identical technique and in identical price. this will shield the distribution network from strength theft carried out by means of tapping, meter tampering and so forth. The proposed gadget located to be a little bit complex as far as distribution community is concerned, however, it's an automated gadget of theft detection. In [17], incidents of power theft wherein cheating customers might decrease their strength payments by using tampering with their meters. The physical attack can be extended to a community assault by means of fake records injection (FDI).

A hybrid detection framework is evolved to come across anomalous and malicious sports so that the community observability and detection accuracy may be advanced by means of grid-located sensor deployment. The hindrance of the proposed technique is confined to a one-participant attack. p.c's are used for excessive overall performance installation protection system. it is able to be received only at the fee of fantastically complicated relay scheme. The design of an electric Meter for lengthy-distance data

information transfers which based totally upon GPRS is proposed in [18]. these systems can't be carried out so easily because the everyday use of GPRS is still a dream to the commonplace humans. A GSM-based totally concept is used to generate a bill is to be had as SMS on the time of era itself and hard copies are to be had to the consumer as postal mail. A smooth reproduction can be ship to the client's e-mail if the consumer is registered together with his e mail deal with [19].

These days, the set of factors has come to be a famous time period for describing eventualities in which internet connectivity and computing functionality make bigger to the diffusion of objects, devices, sensors, and ordinary gadgets. Whilst the time period "net of things" is quite new [20]. The concept of mixing computers and networks to reveal and manage devices has been round for decades. effective information fusion strategies broaden for improving occupancy monitoring accuracy is proposed in [21] using a multitude of resources for the occupancy series of data, IR sensors are used for the detection of the existence of the persons and it's going to be counted the humans in the homes coming into. IOT comes into the photograph with the involvement of smartphones, and wi-fi APs. a unique design approach of minimizing the queue is discussed in [22], the power billing counters and to restrict the usage of energy mechanically, if the invoice isn't always paid and also reduces the loss of energy and sales because of strength thefts and different unlawful activities. This module will reduce the complexity of providing energy by establishing the connection easily and no theft of power will take place.

In [23] and [24] system eliminates the human involvement in electricity maintenance. The system is inefficient in terms of monitoring our energy consumption. Also, the provision for generating bills automatically is limited and inefficient.

III. CONCEPT AND DESIGN

The proposed system is conceptualized in a manner that it will in shape both the inexperienced-area method or the Brown- area technique of incorporating the internet of factors era to a system. as the idea is showed, meter producers can start integrating it into power meters for the duration of manufacture to make certain a clever power control ecosystem.IoT era involves the gathering of information, the transmission of facts to the internet and the evaluation of the statistics. As a result, normally, an IoT system will comprise sensors, processors and network interfaces as its essential elements.

The block diagram of IoTETPS is shown in figure 1. It must be stated that the software program part of an IoT tool is chargeable for the conduct of the device and its written in the Ardiuno platform for this research.

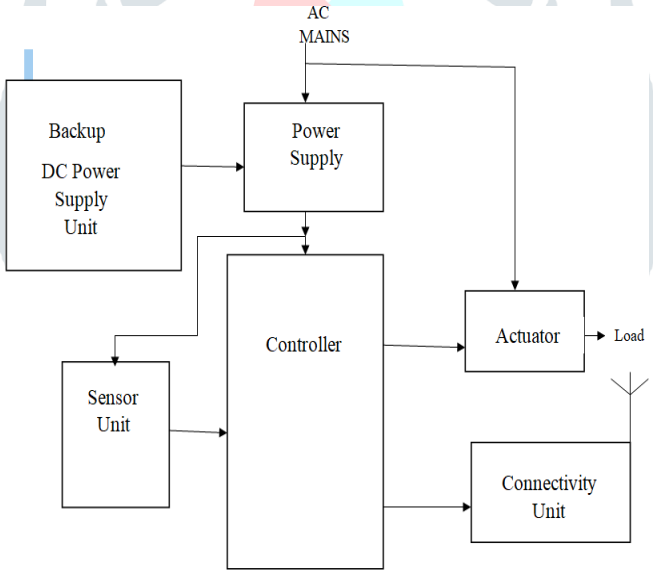

Figure 1: block diagram of IOT electricity meter tamper prevention system (IOTETPS).

- The Controller

The controller is the heart or the brain of the entire system; it coordinates the functionality of other parts of the system. It can be any microcontroller, for this research, an Arduino microcontroller board was used for easy prototyping, implementation, and emulation of embedded systems.

- The Sensor Unit

The sensor unit is major reason for detecting when the meter has been tampered. Upon detection of any tampering activity, it sends signals to the microcontroller which in turn connects the proper response of other parts of the system.

In this approach, whenever the sensitive part of a meter is opened, the sensor unit will signal the controller that the meter has been tampered with. For an electromechanical meter, the responsive part can be considered as the rotating disc or the part where connections are made to the meter, while the responsive part of an electronic meter is considered as the terminals where connection are being made to the meter or the board where the electronic circuits are located.

For this research, the sensor unit is a Passive Infrared Sensor (PIR), placed in the meter cover. The PIR sensor will detect the presence of anybody who opens the meter cover or tries to bypass the meter; and send a signal to the controller.

- The Connectivity Unit

For any device to be able to connect to the Internet, it must first of all connect to a network that is Internet-ready. The connectivity unit of the proposed system performs the tasks of connecting the device to a network and subsequently connecting the system to the Internet. In this case, the system can connect to a Wi-Fi network and then connect to the Internet. The Arduino Wi-Fi Shield 101 which is designed for IoT technology is used for this research [12].

- The Actuator

The actuator in this regard is responsible for either connecting the meter to the load or disconnecting the load from the meter when there is tamper activity. A solid State Relay (SSR) is used in this regard.

- The IoT Electricity Tamper Prevention System Implementation

The Arduino WiFi Shield 101 was mounted on top of the Arduino Mega 2560 board (just like other shields). The output of the PIR sensor was connected to the A0 analogue input pin of the Arduino WiFi Shield 101. The input of the Solid State Relay (SSR) was connected to digital pin 5 of the Arduino WiFi Shield 101. The Power Supply Unit was constructed and connected to the other parts of the system using a power jack.

- System Operation and Simulation

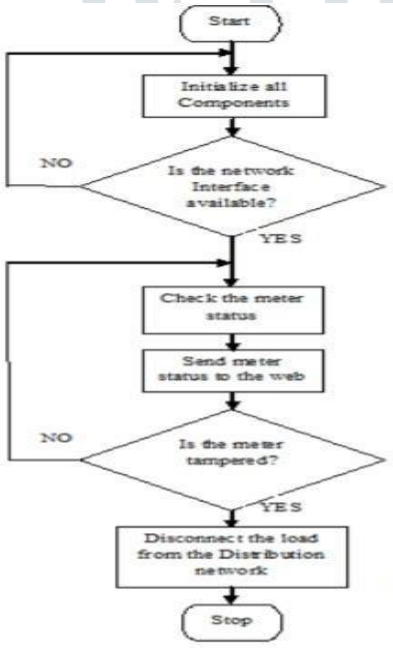

Figure 2: block diagram of IOTt electricity meter tamper prevention system (IOTETPS).

The algorithm that illustrates the mode of operation of the system is represented as a flowchart in Figure 3. Once the device is powered ON, all components will be initialized. The system will check if the connectivity interface is in proper working condition. If the connectivity interface is working properly, the system constantly checks if the meter is tampered with. As soon as the meter is tampered with, the sensor will send a signal to the processor which will in turn trigger the connectivity interface to send message to the Web that the meter has been tampered with. At the same time, the load connected to the meter is disconnected from the distribution network.

IV. PROCESS AT CONSUMER END

At the consumer end, power supply unit supply the power to those entire components which requires power. Microcontroller acquire the relevant information from the electricity meter and also perform the control process and sends the required information such as number of units consumed with the help of Wi-Fi unit. The purpose of LCD module is to get visual information about the number of units, and Wi-Fi configuration.

V. PROCESS AT SUPPLIER END

At the supplier end, if any theft is detected the theft detection unit acts as a modem and it sends the necessary command. If consumer used the power beyond the limit of meter or fails to pay the electricity bill amount within the time limit mentioned by the supplier the disconnection and reconnection can also done by sending the appropriate command to the controller.

VI. COMPARISON BETWEEN EXISTING ELECTRICITY ENERGY METERING METHOD AND SMART ELECTRICITY ENERGY METERING METHOD

a) Existing Electricity Energy Metering Method: - As we know in our country the electricity energy billing duration is either end of one month or end of two months. During the month electricity consumer cannot how much power consumed, they can know at the end of one or two months when the bill issue. The major drawback of this method is user cannot manage the power consumption. Another disadvantage of this system is theft caused by excess amount of power can be done easily and such practices are happening and increasing rapidly which is one of the major causes of power crises.

b) Smart Electricity Energy Metering Method: - In this method we try to eliminate the drawback and limitations of existing electricity metering method. In this method there is a provision for the supplier that they can monitor the power consumed by consumer to find the exact location where theft occurred at the time when theft occurred and provides the information at the event meter tempering and power theft. Such information will be very useful to control the practices of power theft and reduce the power crises. Also it is helpful if consumer fails to pay their electricity billed amount within the time period mentioned by the supplier, the supplier can be disconnect the power automatically from the distant end.

This method is not only providing the facility to supplier end but also it is more helpful to consumer end also. As there is a provision for the consumer that they can see their power consumption time to time so they have an opportunity to manage the power consumption as they desire.

VII. CONCLUSION

IOT based Power theft detection and control systems were proposed in this paper. The system would provide a simple way to detect an electrical power theft without any human interface. In this system we are looking forward to implement smart meter. As the Indian Government has also proposed formation of Smart Cities which will have a effective energy management, transportation, waste disposal and resource conservation strategy using primarily Internet of Things based sensors as done globally.

REFERENCES

1. R. Jiang, H. Tagaris, A. Lachsz, and M. Jeffrey, 2002, Wavelet based feature extraction and multiple classifiers for Electricity fraud detection, in Proc. IEEE/Power Eng. Soc. Transmission and Distribution Conf. Exhibit. Asia Pacific, vol. 3, pp. 2251–2256.
2. C.R.Paul, 1987, System loss in a metropolitan utility network, Power Eng. J., vol. 1, no. 5, pp. 305–307.
3. N.Tobinand N.Sheil, 1987, Managing to Reduce Power Transmission System Losses, in Transmission Performance. Dublin, Ireland: Publ. Electricity Supply Board Int
4. R. L. Sellick and C. T. Gaunt, 1998, Load Data Preparation for Losses estimation, in Proc.7th Southern African Universities Power Engineering Conf. , Stellenbosch, South Africa, vol. 7, pp. 117–120.
5. I. E. Davidson, A. Odubiyi, M. O. Kachienga, and B. Manhire, 2002, Technical loss computation and economic dispatch model in T&D systems in a deregulated ESI, Power Eng. J., vol. 16, no. 2, pp. 55– 60.
6. Ajeeba A A, Anna Thomas, Risa Rasheed, 2017, IoT Based Energy Meter Reading, Theft Detection and Disconnection, in International Research Journal of Engineering and Technology (IRJET), Volume: 04, Issue: 04, e-ISSN: 2395 -0056.
7. Government in India, Ministry of power, 2017, Executive Summary Power Sector.
8. L. Atzori, A. Iera, and G. Morabito, 2010, The internet of things: A survey, Comput. Network, vol. 54, no. 15, pp. 2787–2805.
9. Dimitrios Georgakopoulos, Prem Prakash Jayaraman, 2016, Internet of things: from internet scale sensing to smart services, in Springer-Verlag Wien, ISSN: 0010- 485X.
10. Jawad Nagi, Keem Siah Yap, Sieh Kiong Tiong, Syed Khaleel Ahmed and Malik Mohamad, 2010, Nontechnical Loss Detection for Metered Customers in Power Utility Using Support Vector Machines, IEEE Transactions on power delivery, VOL. 25, NO. 2, Print ISSN: 0885-8977, Electronic ISSN: 1937-4208.
11. R. E. Ogu1, G. A. Chukwudebe, A. Ezenugu, 2016, An IoT Based Tamper Prevention System for Electricity Meter, American Journal of Engineering Research (AJER), e-ISSN: 2320-0847, p-ISSN: 2320-0936, Volume-5, Issue-10, pp-347-353.
12. M.V.N.R.P.kumar, Ashutosh kumar , A.V. Athalekar, P.G. Desai, M.P. Nanaware, 2015, Electrical Power Line Theft Detection, International Journal of Research in Advent Technology, Vol.3, No.5, e-ISSN: 2321-9637.
13. Raksha Kala, 2016, Energy Conservation and Monitoring System for Smart City using Internet of Things, SSRG International Journal of Computer Science and Engineering (SSRG-IJCSE), volume 3 Issue 8.

14. G. L. Prashanthi, K. V. Prasad, 2014, Wireless power meter monitoring with power theft 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.

15. Chun-Hao Lo and Nirwan Ansari, 2013, CONSUMER: A novel hybrid intrusion detection system for distribution networks in Smart Grid, IEEE Transactions on Emerging Topics in Computing Volume: 1, Issue: 1, Electronic ISSN: 2168-6750.

16. U. Grasselli, A. Prudenzi, 1990, Utilization of a PLC in power system protection applications, IEEE Applications of Industrial Electronics Systems.

17. Yujun Bao and Xiaoyan Jiang, 2009, Design of electric Energy Meter for long-distance data information transfers which based upon GPRS, International Workshop on Intelligent Systems and Applications.

18. Ashna.k,Sudhish N George, 2013, GSM Based Automatic Energy Meter Reading System with Instant Billing, IEEE Automation, Computing, Communication, Control and Compressed Sensing (iMac4s), Electronic ISBN: 978-1-4673-50907.

19. Other views on the converging market trends driving IOT's growth include Susan Conant's article, The IOT will be as fundamental as the Internet itself, available at internetitself.html and Intel Corporation's statement to U.S. House of Representatives hearing on IOT.

20. Shivaji G. Shinde, Bhagyashri G. Jaind, 2016, IOT framework for energy efficient smart building, International Journal of Application or Innovation in Engineering & Management (IJAIEM) Volume 5, Issue 4, ISSN 2319 – 4847.

21. L. Deepika, B. Divya, P. Jeevitha, P. Ramkumar, T. Boobalan, 2016, IOT Based Prepaid Electricity, International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET) Volume 2, Issue 2,ISSN : 2395-1990. Ajeeba A A, Anna Thomas, Risa Rasheed, 2017, IOT Based Energy Meter Reading, Theft Detection and Disconnection, International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 - 0056 Volume: 04, Issue: 04, p-ISSN: 2395-0072.