

ELECTRICAL POWER THEFT LOCATION AND TRACKING USING IOT

S.Venkatesh Kumar¹, D.Kishoth Kumar², V.Gokula Krishnan³

¹Assistant Professor(Sr.Gr), ^{2,3}UG Student,

Department of Electrical and Electronics Engineering, Sri Ramakrishna Engineering College, Tamilnadu, India ***

Abstract - Our proposed system claim to detect power theft in real time along the location of theft. The system will have an online database which store all the data related to the distribution system along with the time and data. This data include power dispatched voltage consumed at a pole and the serial no of the electrical pole. The voltage value will be plotted against time. The pole number gives us with the location of the theft of power; we will compare the sending end and receiving end voltage levels, see demand of load if the difference is more than permitted value then close check must be scheduled to look into abrupt rise of power demand. The System consists of Microcontroller based monitoring system with receiver measurement instrument to collect data from the consumer side.

Key Words: Microcontroller, Location, voltage levels, **Online Database, Electrical pole.**

1. INTRODUCTION

The internet of things is about connecting the unconnected things. It allows for thing to accessible from the internet that historically has not been. The internet of things is able to improve quality of life for everyone by taking advantage of these connected thing and data produced. The billions of m2m connection make possible in everything on IOT. The process element leverages the connection between data thing and people to deliver the right information. To right thing or person, at the right time, it is these billions of connection that add value. Distribution Transformers have a long life if they are operated under appraised conditions. However, their life is essentially decreased if they are overloaded, resulting in unexpected failures and loss of supply to an expansive number of customers hence affecting system unwavering quality. Overloading and ineffective cooling of transformers are the major significant reasons for failure in distribution transformers.

1.1 Internet of Things (IOT)

The Internet of Things (IoT) is an environment in which objects, animals or people are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction. IoT has evolved from the convergence of wireless technologies, micro-electromechanical systems (MEMS) and the Internet. The concept may also be referred to as the Internet of Everything.

A thing, in the Internet of Things, can be a person with a heart monitor Implant, a farm animal with a biochip transponder, an automobile that has built-in sensors to alert the driver when tire pressure is low -- or any other natural or man-made object that can be assigned an IP address and provided with the ability to transfer data over a network.

IoT board designed to meet a variety of online application needs with distinct advantages that enable the embedded system designer to easily, quickly and seamlessly add internet connectivity to their applications.

The module's UART update feature and webpage control make them perfect for online wireless applications such as biomedical monitoring, environmental sensors, and data's from portable battery operated wireless sensor network devices. Lumisense. IoT board featured with SIM900 GPRS modem to activate internet connection also equipped with a controller to process all input UART data's to GPRS based online data.

Below, it is provided a glossary defining the Internet of Things:

• Internet of Things: A network of internet connected objects able to collect and exchange data using embedded sensors.

• Internet of Things device: Any stand-alone internet-connected device that can be monitored and/or controlled from a remote location.

• Internet of Things ecosystem: All the components that enable businesses, governments, and consumers to connect to their IoT devices, including remotes, dashboards, networks, gateways, analytics, data storage, and security.

• Entity: Includes businesses, governments, and consumers.

• Physical layer: The hardware that makes an IoT device, including sensors and networking gear.

• Network layer: Responsible for transmitting the data collected by the physical layer to different devices.

• Application layer: This includes the protocols and interfaces that devices use to identify and communicate with each other.

• Remotes: Enable entities that utilize IoT devices to connect with and control them using a dashboard, such as a mobile application. They include smart phones, tablets, PCs, smart watches, connected TVs, and nontraditional remotes.

• Dashboard: Displays information about the IoT ecosystem to users and enables them to control their IoT ecosystem. It is generally housed on a remote.

• Analytics: Software systems that analyze the data generated by IoT devices. The analysis can be used for a variety of scenarios, such as predictive maintenance. Data storage: Where data from IoT devices is stored.

• Networks: The internet communication layer that enables the entity to communicate with their device, and sometimes enables devices to communicate with each other.

2. WORKING PRINCIPLE

There are various types of electrical power theft, including Tapping a line or bypassing the energy meter. According to a study[citation needed], 80% of worldwide theft occurs in private dwellings and 20% on commercial and industrial premises.

The various types of electrical power theft include:

2.1 Direct Hooking from Line

What's known as "Cable Hooking" is the most used method. 80% of global power theft is by direct tapping from the line. The consumer taps into a power line from a point ahead of the energy meter. This energy consumption is unmeasured and procured with or without switches.

2.2 Bypassing the Energy Meter

In this method, the input terminal and output terminal of the energy meter is short-circuited, preventing the energy from registration in the energy meter.

2.3 Injecting Foreign Element into the Energy Meter

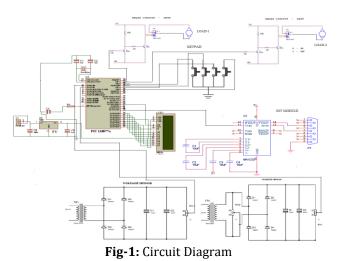
Meters are manipulated via a remote by installing a circuit inside the meter so that the meter can be slowed down at any time. This kind of modification can evade external inspection attempts because the meter is always correct unless the remote is turned on.

2.4 Physical Obstruction

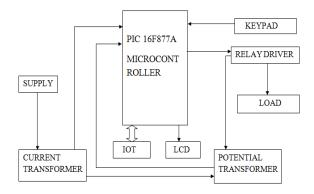
This type of tampering is done to electromechanical meters with a rotating element. Foreign material is placed inside the meter to obstruct the free movement of the disc. A slower rotating disk signals less energy consumption.

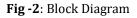
2.5 ESD Attack on Electronic Meter

This type of tampering is done on electronic meter to make it either latent damage or permanent damage. Detection can be done correctly in high end meters only. The three phase parameter i.e. voltage of overhead line will get continuously sensed using phase voltage sense section. Once the fault takes place in overhead line, voltage and current values deviates from their nominal ranges. The faults like all series & shunt faults get detected & classified here. During occurrence of any series voltage get sensed and respective signals are given to microcontroller. Relay is connected for detecting fault in fault display section. Relay is operated by micro-controller and switched after the occurrence of faulty condition. Microcontroller programing is done on the basis of characteristics conditions of overhead line voltages on occurrence of fault. The type of fault gets analyzed by microcontroller. If the fault gets occurred wireless technology GSM (global system for mobile communication) is used to send SMS to a responsible person on mobile. Type of fault will display on fault display section. Simultaneously fault will clear. The fault clearing system uses various protection devices such as relays and circuit breakers to detect and clear the fault. The three phase voltage sensed is continuously given to microcontroller. The implemented system completely meets the demand of low cost by using the microcontroller and mobile communication technology with the aim to detect the abnormality and fault occurred in the overhead electric line.



This unit consists of transformer, rectifier, filter and regulator. A.C. voltage typically 230V rms is connected to a transformer which steps that AC voltage down to the level to the desired AC voltage. This resulting DC voltage usually has some ripple or AC voltage variations. A regulator circuit can use this DC input to provide DC voltage that not only has much ripple voltage but also remains the same DC value even the DC voltage varies somewhat, or the load connected to the output DC voltages changes. Liquid crystals are organic (carbon) compounds, which exhibit both solid and liquid properties. The message will be given to the interfacing media according to coding system. An LCD interfacing program is also in built in microcontroller. If any abnormalities occur it will be displayed on LCD. Once the circuit is tripped it must be reset for further use using button. In either case, the microcontroller is reset programmed so as to show the status of the output on the LCD interfaced to it.





3. CONCLUSION

An Electrical Power Theft Location Using Iot for transformer was designed, implemented and tested. It is quite useful as compared to manual monitoring and also it is reliable as it is not possible to monitor always the load voltage and load current manually. A server module can be added to this system to periodically receive and store transformer parameters information about all the power transformers in a database application. After receiving message on any abnormality we can take immediate action to prevent any catastrophic failures of power transformers.

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] L. Atzori, A. Iera, and G. Morabito, 2010, The internet of things: A survey, Comput. Network, vol. 54, no. 15, pp. 2787–2805.
- [8] Dimitrios Georgakopoulos, Prem Prakash Jayaraman, 2016, Internet of things: from internet scale sensing to smart services, in Springer-Verlag Wien, ISSN: 0010-485X.
- [9] 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.
- [10] 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.
- [11] 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.
- [12] 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.

- [13] 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.
- [14] 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.
- [15] U. Grasselli, A. Prudenzi, 1990, Utilization of a PLC in power system protection applications, IEEE Applications of Industrial Electronics Systems.
- [16] 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: 978-1-4673-5090-7.
- [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.