IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 21, Issue 2, Ser. II (Mar - Apr 2019), PP 48-52
www.iosrjournals.org

Power Management System and Theft Detection Using Internet of Things (IOT)

B. Dhanalakshmi[1], E.Shalini[2], M. Nivedha[3]
[1]*Assistant Professor, Computer Science Department, JEPPIAAR SRR Engineering College, Chennai*
[2]*UG Student, Computer Science Department, JEPPIAAR SRR Engineering College, Chennai*
[3]*UG Student, Computer Science Department, JEPPIAAR SRR Engineering College, Chennai*
Corresponding Author: B. Dhanalakshmi

Abstract: *The main motivation is to manage the power usage at residential home and control the yielding of high power. The illegal usage of power must be solved by electronic means without any human interaction. The purpose of this work is to provide an implementation methodology for power management and theft detection. It includes microcontroller based embedded technology and wireless communication method to find out the power theft. A Global System for Mobile communication (GSM) based technology is used to transmit the meter reading and detection alert automatically to the authorized power provider via an alert message, through wireless Fidelity authorized user get an alert mail and meter reading taken automatically using GSM technology, then Power cut will happen when it crosses the threshold limit. The authorized user can check the power usage in the webpage through IP address. Now the attacks like power theft can be identified and user can report to the power administrator.Hence forth the above study showed that authorized user can manage the power by checking the webpage the value of power consumed will be displayed and detecting the theft*

Date of Submission: 11-03-2019 Date of acceptance: 27-03-2019

I. Introduction

Electricity theft is very communal problem in many developing countries. Theelectricity theft can be classified in a form of meter tampering, illegal connection, billing indiscretions. In previous it shares false incremental cost information to disturb the convergence of the consensus algorithm and break the balance between the generation and demand. A malicious distributed generator (DG) shares false utilization ratio to mislead other DGs, with the objective to increase its own income. Malicious attacker could manipulate the power schedule result by sharing false information. User cannot get proper report because they couldn't find out where the account has been hacked, where the prices advertised to smart meters are compromised by scaling factors(so consumers use the wrong prices)and by corrupted timing information. Limitation of existing system malicious generation units injects false generation cost parameters, to increase the total generation cost and decrease the generation efficiency. The aforementioned attacks cause the imbalance between the generation and demand. Security and privacy cost. Monitoring power consumption at each home. Here user can limit the power supply to home by pre-default setting threshold value to be consumed When the power reaches the threshold amount, then it automatically sends an alert mail to the user.The attacker or any other third parties using threshold amount of power user get an alert mail and meter reading taken automatically using GSM technology, then Power cut will be happen when it crosses the threshold limit. The authorized user can also check the power usage in the webpage through IP address.

II. Related Works

Several techniques were used for power management and theft detection. Few related works are as follow:

JieDuan, Mo-Yuen Chow [1], proposed a Novel Data Integrity Attack on Consensusbased Distributed Energy Management Algorithm using Local Information. User show that by sending out elaborately falsified information during the consensus iterations, attackers could manipulate the system operating point and gain extra economic benefits. Meanwhile, the system-level and device-level constraints are still satisfied, e.g., the power generation and demand are balanced and the operation of individual device respect physical constraints. This data integrity attack has two major features: 1) attackers only rely on local information to complete the attack, no additional information about system topology nor additional colluders are required; 2) the attacking effect is accumulative, which enables attackers to choose to finish in either single or multiple iterations. By revealing such vulnerability of consensus-based applications to data integrity attack, this conveys the message that besides the efforts of designing novel distributed energymanagement algorithms to address the renewable energy integration challenges, it is equally important to protect the distributed energy management algorithms from possible malicious attacks to avoid potential economic losses. The proposed attack is illustrated in the Future Renewable Electric Energy Delivery and Management (FREEDM) system.

Jinsoo Han, Moonok Choi, Ilwoo Lee, And Sang-Ha Kim[5], proposed aPhotovoltaic Energy Sharing System in a Multifamily Residential House to Reduce Total Energy Costs.The community-shared PV system is connected to each home, monitors each home's energy use, and assigns more energy to a large energy-consuming home. Under increasing block tariffs, this architecture contributes to reducing total energy costs.

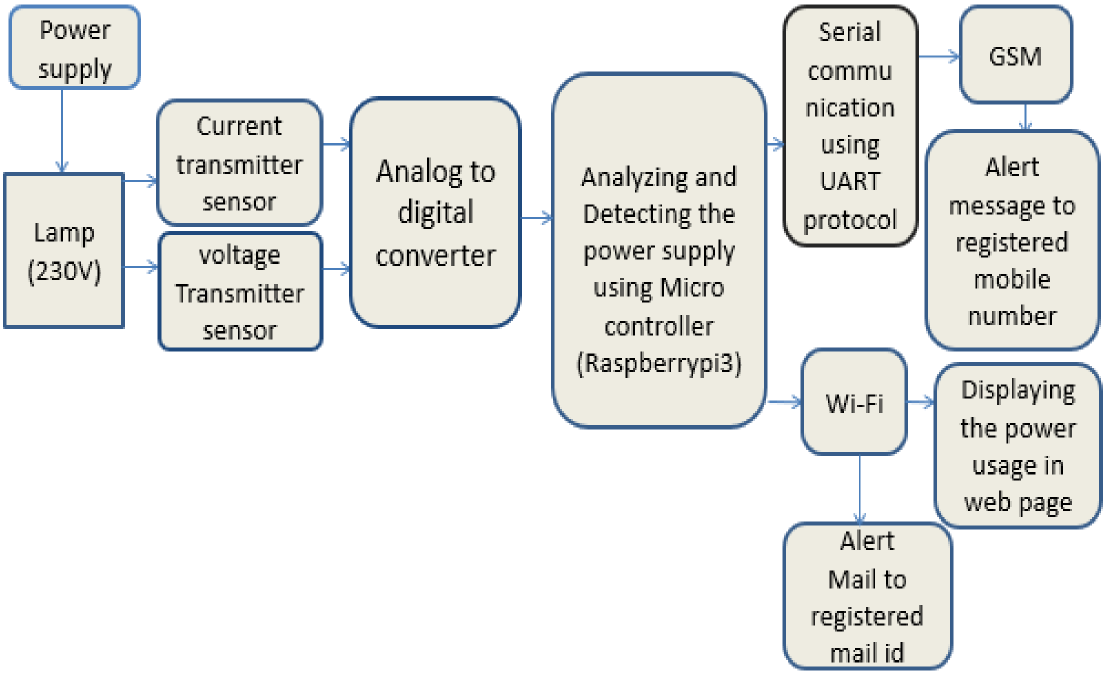
J. E. G. Salas, R. M. Caporal, E. B. Huerta, Member, J. J. Rodriguez and J. J. R. Magdaleno[6], proposed aSmart Switch to Connect and Disconnect Electrical Devices at Home by Using Internet. The development of a firmware for a Smart Switch, which can control the on-off of any electrical device at home by using internet. The Smart Switch is connected to internet via Wi-Fi, through a computer, smartphone, tablet or any device with internet access. Then, the user will select in automatic mode the network, the security type, and the user must have written a passphrase. Once this information is uploaded and saved, it is necessary to restart the Smart Switch in order to get access to internet, from which the user can control the Smart Switch simply sending a number one or a number zero to switch the electrical device, this process is done in principle via the internet, but it can be done without the use of internet, i.e. by using a local network.

Md. Manirul Islam1, Mohiuddin Ahmad, Md. Ajijul Islam, Abu Farzan Mitul, M. F. Malek, and M. A. Rashid[12], suggested anElectronic Energy Meter with Remote Monitoring and Billing System. Measurement of energy, remote monitoring, preparing of bill and billing system is presented. Low cost ATMEGA8L microcontroller is used here to control the whole system. Sampling of voltage and current is done by it. Then it processes data to achieve power in that instant. Then it stores the value of total energy consumed by the consumer and can calculate energy charge according to the tariff. LCD display is attached with this system to show total energy consumed, power factor and amount of charge etc. Communication between central energy distribution office and energy meter is done through power line. Complex tariff rate set up and cash card-based billing ispossible in this system. Electronic meter gives high accuracy for nonlinear loads than conventional rotating disc type electro-mechanical meter. Greater accuracy and stability can be maintained in this system.

III. Proposed System

Monitoring power consumption at each home. Here user can limit the power supply to home by pre-default setting threshold value to be consumed When the power reaches the threshold amount, then it automatically sends an alert mail to the user. The attacker or any other third parties using threshold amount of power user get an alert mail and meter reading taken automatically using GSM technology, then Power cut will be happen when it crosses the threshold limit. The authorized user can also check the power usage in the webpage through IP address. Advantage of the proposed system reduce the cost efficiency, reduce the peak demand of power supply, Enhanced reliability.

SYSTEM ARCHITECTURE


Power supply
Lamp (230V)
Current transmitter sensor
voltage Transmitter sensor
Analog to digital converter
Analyzing and Detecting the power supply using Micro controller (Raspberrypi3)
Serial communication using UART protocol
GSM
Alert message to registered mobile number
Wi-Fi
Displaying the power usage in web page
Alert Mail to registered mail id

IV. Methodology

Procedure methodology: The main aim is to manage the power usage at residential home and control the yielding of high power. The illegal usage of power must be solved by electronic means without any human interaction. The purpose of this work is to provide an implementation methodology for power management and theft detection. The project consists of about four modules by which it satisfies its above-mentioned aim. The modules are for various actions such as Measuring power utilization using sensors, designing microcontroller about power leakage, analyzing and detecting power theft and intimate the report about power theft. The modules are hereby explained below.

1. Measuring power utilization using sensors
2. Designing microcontroller about power leakage
3. Analyzing and detecting power theft
4. Intimate the report about power theft

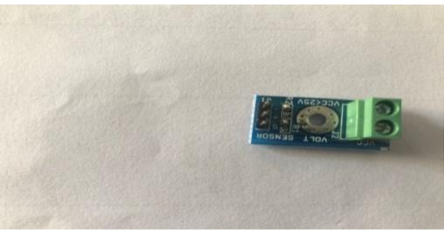
Description of the modules

Power supply to the lamp(230V) is connected to the current transmitter sensor is used to measure the current and voltage transmitter sensor is used to measure the voltage both sensors is used to measure the value of power. Designing the microcontroller as raspberry pi when it crosses the threshold limit. User analysis that power has been theft and intimate report about the power value through message, mail and webpage.

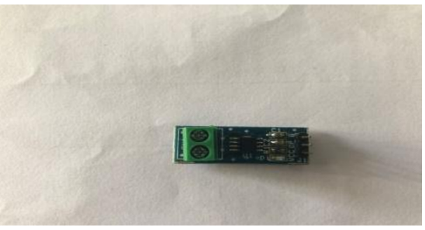
1. Measuring power utilization using sensors

A current sensor is a device that detects electric current (AC) in a wire, and generates a signal. The generated signal could be analog voltage or current. It can be then utilized to display the measured current. The generated signal can be utilized for control purpose.

A voltage sensor is going to be able to determine and even monitor and measure the voltage supply. It is then able to take those measurements and turn them into a signal. The generated signal can be utilized for control purpose.



Current transmitter sensor

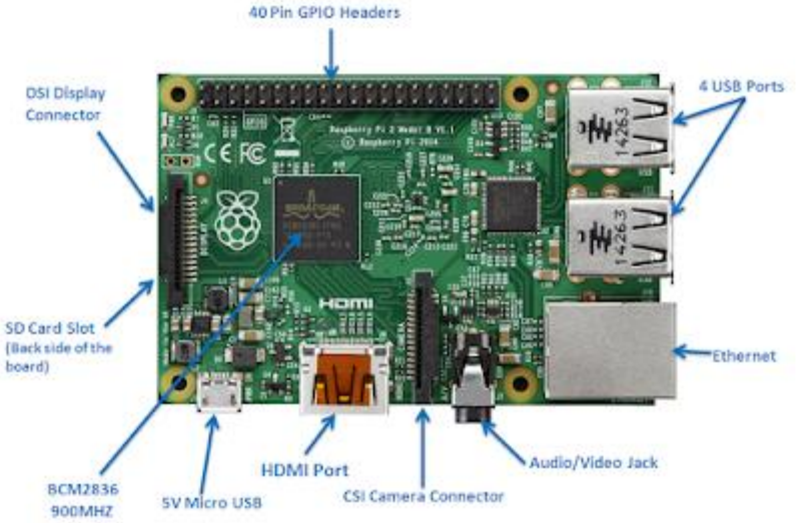


Voltage transmitter sensor

2.Designing microcontroller about power leakage

UART protocol used for communication between the micro controller and the GSM,which is used to transmit and receive the signal. The Raspberry Pi is a series of small single-board computers developed in the United Kingdom by the Raspberry Pi Foundation to promote the teaching of basic computer science in schools and in developing countries.PIR (Passive infrared) sensor interface into the raspberry pi3 and intimate through GSM.

Peripherals (including keyboards and mouse) are not included with the Raspberry Pi. Some accessories however have been included in several official and unofficial bundles.Meter reading taken automatically using GSM technology, using relay drive Power cut will be happen when the power crosses the threshold limit



Micro controller(raspberry pi3)

3. Analyzing and detecting power theft

UART protocol used for communication between the micro controller and the GSM,which is used to transmit and receive the signal Global system for mobile communication (GSM) is a globally accepted standard for digital cellular communication. The GSM are interfaced with the micro controller when it crosses the threshold limit voltage the GSM module send SMS to the registered mobile number.

Global system for mobile communication

4. Intimate the report about power theft

In distribution network smart meter is connected to the secondary side, which will pound the illegal user intimating management when non-technical losses increase its promulgated limit, this reported data will be sent to the electric load controllers, rectifying it by taking some yielding actions. The advance metering infrastructure monopolies the consumers, uplifting the theft control. If third person use the existing amount of the power supply, then it considers as a power theft and authorised user have a proof to generate a report to the power administrator with the valid reason. Then the alert mail and alert message will be sent to the authorised user with the usage of voltage and the current value.

V. Result and discussion

The authorized user gets an alert message to the registered mobile number and get an alert mail to the registered mail ID, through IP address authorized user can check the value of power supply.This reduce the power theft and help for managing the power.

VI. Conclusion

In developing countries power theft is common problem in remote areas, involves tampering with meters to distort billing information or direct connection to power system. The electricity losses are nearly impossible to measure using traditional power system analysis tools.

To solve this problem authorized user using the sensor to limit the power supply. If the third parties use the existing amount of power then automatically user get an alert message through a mail and get a text message to the registered mobile number at that time. The authorized user can check the power usage through IP address in web page.

VII. Future Enhancements

Future enhancement could be to develop countermeasures to detect the false information and try to identify the trade-off between time of detection, frequency of the attack, and number of false alarms. Tracking the location where the theft happened and face detection can also be included.

References

[1]. JieDuan, Mo-Yuen Chow, “A Novel Data Integrity Attack on Consensus based Distributed Energy Management Algorithm using Local Information”, IEEE Transactions on Industrial Informatics, June 2018.

[2]. W. Zeng, Y. Zhang, and M. Y. Chow, “Resilient Distributed Energy Management Subject to Unexpected Misbehaving Generation Units,” IEEE Transactions on Industrial Informatics, vol. 13, no. 1. pp. 208– 216, 2017.

[3]. N.Rahbari-Asr, Y. Zhang, and M.-Y. Chow, “Consensus-based distributed scheduling for cooperative operation of distributed energy resources and storage devices in smart grids,” *IET Generation, Transmission & Distribution*, vol. 10, no. 5, pp. 1268–1277, 2016.

[4]. C.Chen, J. Wang, and S. Kishore, “A Distributed Direct Load Control Approach for Large-Scale Residential Demand Response,” *IEEE Transactions on Power Systems*, vol. 29, no. 5. pp. 2219–2228, 2016.

[5]. Jinsoo Han, Moonok Choi, Ilwoo Lee, And Sang-Ha Kim, “Photovoltaic Energy Sharing System in a Multifamily Residential House to Reduce Total Energy Costs”, IEEE Transactions on Industrial Informatics, June 2016.

[6]. J. E. G. Salas, R. M. Caporal, E. B. Huerta, Member, J. J. Rodriguez and J. J. R. Magdaleno,” A Smart Switch to Connect and Disconnect Electrical Devices at Home by Using Internet”, IEEE Transactions on Industrial Informatics, Dec 2016.

[7]. Y. Liu, H. Xin, Z. Qu, and D. Gan, “An Attack-Resilient Cooperative Control Strategy of Multiple Distributed Generators in Distribution Networks,” IEEE Transactions on Smart Grid, vol. 7, no. 6, pp. 2923– 2932, 2016.

[8]. A. Wood, B. Wollenberg, and G. Shebleeacute, Power Generation, Operation and Control, 2nd ed. New York : J. Wiley & Sons, vol.5, n0.6,pp.2934-2944,2015

[9]. Y.Xu, W. Liu, and J. Gong, “Stable multi-agent-based load shedding algorithm for power systems,” *IEEE Transactions on Power Systems*, vol. 26, no. 4, pp. 2006–2014, 2013.

[10]. S.Yang, S. Tan, and J.-X. Xu, “Consensus based approach for economic dispatch problem in a smart grid,” *IEEE Transactions on Power Systems*, vol. 28, no. 4, pp. 4416–4426, 2013.

[11]. R.Olfati-Saber J. A. Fax, and R. M. Murray, “Consensus and cooperation in networked multi- agent systems,” *Proceedings of the IEEE*, vol. 95, no. 1, pp. 215–233, 2012.

[12]. Md. Manirul Islam1, Mohiuddin Ahmad, Md. Ajijul Islam, Abu Farzan Mitul, M. F. Malek, and M. A. Rashid”Electronic Energy Meter with Remote Monitoring and Billing System”, IEEE Transactions on Industrial informatics, March 2012.

[13]. C. Zhao, J. He, and P. Cheng, “Analysis of Consensus-based Distributed Economic Dispatch under Stealthy Attacks,” IEEE Transactions on Industrial Electronics, vol. 99, no. 99, 2011.

[14]. Q. Jiang, M. Xue, and G. Geng, “Energy management of microgrid in grid-connected and stand-alone modes,” IEEE Transactions on Power Systems, vol. 28, no. 3, pp. 3380–3389, 2007.

[15]. H. Tang, F. R. Yu, M. Huang, and Z. Li, “Distributed consensus-based security mechanisms in cognitive radio mobile ad hoc networks,” IET communications, vol. 6, no. 8, pp. 974–983, 2007.

IOSR Journal of Computer Engineering (IOSR-JCE) is UGC approved Journal with Sl. No. 5019, Journal no. 49102.

B. Dhanalakshmi. " Power Management System and Theft Detection Using Internet of Things (IOT)." IOSR Journal of Computer Engineering (IOSR-JCE) 21.2 (2019): 48-52.