International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 04 Issue: 06 | June -2020 ISSN: 2582-3930

COST EFFETIVE ELECTRICITY THEFT DETECTION USING IOT

Ujjwal Kumar[#1] Shivank shikhar Tripathi[#2] Paras Sangwan[#3] Kaushal Kumar[#]4, Mr. Satyajeet

Department of Electrical engineering

JSS Academy of technical education Sector 62 Noida UP India

Abstract— The project aims at providing a state of the art technology to counter the illegal and immortal act of energy theft by domestic consumers. Theft in the development countries cost a heavy toll on the revenue generated that amount to thousands of crores of currency.
Electricity theft is one of the major challenges faced by the power companies. It prevents the power companies from making adequate money from the sale of electricity. This paper presents the development of a cost effective electricity theft detection and prevention system using the Internet of Things (IoT) technology.
Internet of Things (IoT) is making next transformation within the world of web. It provides intelligent amenities to the society. India is also not lagging behind to make use of IoT technology and because of this more cities are becoming smart in the country. Even though, 70% population in Indian towns is facing many challenges like garbage management, electricity and water supply. Electricity board in the township has many issues to provide the service at the expected level. One of the major issues is related to electricity losses which are of two types, technical and non-technical losses. Technical losses happen due to properties of materials utilized in transmission and dispersion system. Non-technical losses are electricity theft which includes tampering meters, unpaid bills, electric line tampering. Majority of the meter tampering issues have been resolved by taking smart meters into the picture but the line tampering issue still persists. The steps to solve line tampering problems include placing smart meters by removing lines which is exorbitant and time consuming. Thus, the paper provides unadorned and efficient way to solve the problem by IoT to detect the amount of electricity theft. There is provision for automatic cut of power using Arduino Uno and ATMega 328 when lines are connected in parallel, the electricity received is more than provided. Theft location is reported to the admin via sms using ESP8266 WIFI module. These things are monitored and managed by admin from remote place on the application to save the investigation time, energy, cost in a most efficient way possible. The results obtained are the comparisons between current v/s time with and without tampering. Also, the cost recurred when tampering is avoided. For the prevention of meter tampering an IR sensor is used for sensing any kind of tampering in the energy meter by infrared rays.

Keywords—IoT, Line Tampering, Detection, Prevention,Electricity Theft

I. INTRODUCTION

Electricity is one of the basic needs of population. In the current scenario many villages are facing the problem of electricity. India's electricity theft costs around loss of $4.5 billion.If we can prevent the theft of electricity then we can easily provide electricity to every corner of country. Electricity theft is done by means of tampering Either "METER" Or "LINE".

We are going to prevent this theft using ARDUINOs and IOT technique so that whenever there is any detection of theft, distribution to that location will be stopped for that instant. The previous project consists of two energy meters for a residential load.

The slave meter will be in access of consumer but not master meter. Both the meter records the energy consumption. In case of any theft the slave meter will show the error reading but the master one still show the correct reading as it cannot be tampered. The microcontroller sense the readings of the two meters and in case of any difference it will instruct GSM module attached to it to send a message to regulatory authority regarding the theft and its location.

II. LITERATURE SURVAY

The first paper on theft issue was published in year 1995 by UK department of electricity. It talked about the ways, types and physical solutions for it. And it represented some acts and laws for theft prevention.

The methods used for detection of theft are as follows-

- Outside sources
- Information from general employees
- Specific directed efforts

By these methods they estimated the loss by theft.[1]

Another paper we studied was published in year 2004 in IEEE Africon. It talked about study conducted to determine the optimumstationary time period for detecting electricity theft in the areasbased on available consumption data in the area. This paperdiscusses simulations and models based on data from pre-paidmeters in order to determine the feasibility and method ofoperation for B remote check meter.
When running the simulation a time period t in monthsis chosen and a number of n iterations are done. This isthen evaluated for each of the different configurations, bycomparing the results from the experiment against the casewhere no electricity theft is present in the simulation.
The last step is to determine whether a sweep team shouldhe sent into the area for auditing the meters.[2]

Another paper we studied was published in year 2010 by National Tenaga University Malsiya. This paper presents an approach towards detection of Non-technical Losses (NTLs) of Large PowerConsumers (LPC) in Tenaga Nasional Berhad (TNB) Malaysia.The main motivation of this study is to assist Tenaga NasionalBerhad (TNB)

Sdn. Bhd. in Malaysia to reduce its NTLs in theLPC distribution sector. Thisstudy develops a NTL detection framework for detection offraudulent and abnormal load consumption patterns usingRMR consumption data and meter event logs.A tamper proof system for the smart meters using IoT technology was developed in. Although this system is applicable to both the green field and brown field approach of the Internet of Things, it utilized two separate boards, one as a controller and the other as network interface.[3]

Another paper we studied was published in year 2017 in IEEE 3rd international conference on electro-technology for national development. Thispaper presents the development of a cost effective electricity theftdetection and prevention system using the Internet of Things(IoT) technology.
In this work, a single board (Arduino MKR1000) performsthe functions done by the two separate boards above (theArduino Mega 2560 and the Arduino WiFi shield 101).The cost of Arduino MKR1000 is $44.95. Comparing thetotal cost of the Controller and the network interface of which is $84.95 to $44.95 which is the cost of an amalgamatedboard that has a controller and the network interface together,it can be clearly understood that the cost has been drasticallyreduced.[4]

Another paper we studied was published in year 2018 in IEEE internet of things journal.This paper developsan energy detection system called Smart Energy Theft System(SETS) based on machine learning and statistical models.
In this paper, an innovative Smart Energy Theft System(SETS) is proposed for energy theft detection. A Multi-ModelForecasting System based on the integration of machinelearning models such as Multi-Layer Perceptron (MLP), RecurrentNeural Network (RNN), Long Short Term Memory(LSTM), and Gated Recurrent Unit (GRU) was developed aspart of SETS. Additionally, a statistical model called SimpleMoving Average (SMA) was also further developed into SETS.
These algorithms enable SETS to efficiently detect energytheft activities.[5]

Another paper we studied was published in year 2019 in IEEE transaction on smart grid. This letter introduces a gradient boosting theft detector (GBTD) based on the three latest gradient boosting classifiers (GBCs): extreme gradient boosting (XGBoost), categorical boosting (CatBoost), and light gradient boosting method (LightGBM). While most of existing ML algorithms just focus on fine tuning the hyperparameters of the classifiers, our ML algorithm, GBTD, focuses on the feature engineering-based preprocessing to improve detection performance as well as time-complexity.
This letter presented a SG theft detection algorithm, called GBTD, based on the three GBCs (XGBoost, CATBoost, LightGBM). Out of the three GBCs, in terms of DR, both LightGBM and CATBoost outperformed XGBoost. However, LightGBM appeared to be the fastest classifier with highest FPR while CATBoost performed the slowest with lowest FPR. We also numerically proved that GBTD with feature engineering not only minimizes FPR but also reduces customer data storage space as well as processing time.[6]

Another paper we studied was published in year 2019 in JETIRIn 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.
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.[7]

Another paper we studied was published in year 2019 in International Conference on Electrical, Communication and computer engineering, Pakistan.This paper presents the condition of electricity theft in Pakistan.
This paper presents a novel solution to tackle both metertampering and Hooking thefts. This system is anautomated system and requires no human interaction forits working once the system is installed. The proposedsystem provides an effective and easy way to detectelectrical theft and gives effective solution for problemsfaced by Pakistan's electricity distribution system such aspower theft on distribution line. The proposed systemconsists of two consumer nodes which measure theamount of power consumed and creates a load profile ofthe consumers. The intermediate node calculates the difference in the power values and through load profilechecks for power thefts. A pre-defined limit of 200W isset as threshold for theft detection. Once a theft isdetected, the prevention process disconnects all legalconsumers from the line and then through the tappingtransformer, high voltage is fed to the line to make illegal loads in-operational. The proposed solution is cheap andeffective.[8]

Another paper we studies was published in year 2019 by KLE Technological University.The paper provides unadorned and efficient way to solve the problem by IoTto detect the amount of electricity theft. There is provisionfor automatic cut of power using Arduino Uno andRaspberry Pi3 when lines are connected in parallel, theelectricity received is more than provided. Theft location isreported to the admin via sms using SIM808 module.
This chapter states the brief explanation of the issueconsidered, work carried out, results obtained and comparisonof the work with similar works done.The work has been successfully carried out and it is better thanthe others in the way that it gives solution for line tampering which isn't looked upon much unlike others.[9]

An internet of things is simply a network of internet connected objects which able to collect and exchange data. It is invented by Kevin Ashton in 1999. In simple way we have things that sense and collect data and send it to the internet. It can be used to monitor and control mechanical, electrical and electronic systems used in various type of sectors. An system of IOT consist of sensors which talk to the cloud withsome kind of connectivity, once the data gets to the cloud, software processes it and might decide to perform an action such as sending alert or automatically adjusting the sensors. Using this technology of IOT in the field power we can detect any illegal activity of power theft which is the major problem face by Utility providers.

A. Transmission And Distribution losses

Transmission and distribution (T&D) loss are amounts that are not paid for by users. Distribution Sector considered as the weakest link in the entire power sector. Transmission losses are approximately 17%

while distribution losses are approximately 50%. There are two types of transmission and distribution losses:

1. Technical Losses
2. Administration Losses
3. Non-Technical Losses (illegal use of electricity)

B. Technical Losses

The technical losses are due to energy dissipated in the conductors, equipment used for transmission line, transformer, sub- transmission line and distribution line and magnetic losses in transformers. Technical losses are normally 22.5%, and directly depend on the network characteristics and the mode of operation. The major amount of losses in a power system is in primary and secondary distribution lines. While transmission and sub-transmission lines account for only about 30% of the total losses. Therefore, the primary and secondary distribution systems must be properly planned to ensure within limits. The unexpected load increase was reflected in the increase of technical losses above the normal level Losses are inherent to the distribution of electricity and cannot be eliminated.

C. Administration Losses

Administration losses are given by unknown connections (but not due to the illegal use of electricity) or missing meters in the network. The administration errors represent about 14% of total losses, see Fig.1.

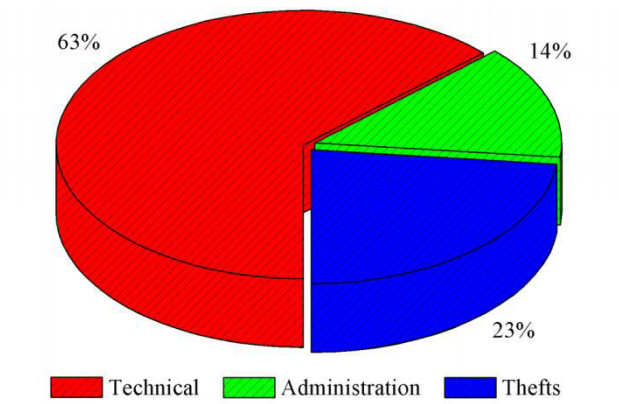

Figure 1

D. Non Technical Losses

NTLs are mainly related to electricity theft and customer management processes in which there exist a number of means of consciously defrauding the utility concerned. In most developing countries, transmission and distribution (T&D) losses account for a large portion of NTLs, which implies that electric utilities have to concentrate on reducing NTLs prior to reducing technical losses . NTLs generally include the following activities :

1) Tampering with meters so that meters record lower rates of consumption;
2) Stealing by bypassing the meter or otherwise making illegal connections;
3) Arranging false readings by bribing meter readers;
4) Arranging billing irregularities with the help of internal employees by means of such subterfuges as making out lower bills, adjusting the decimal point position on bills, or just ignoring unpaid bills.

By default, the amount of electrical energy generated should equal the amount of energy registered as consumed. However, in reality, as some power loss is inevitable, steps can be taken to ensure that it is minimized. Several measures have been applied to this end, including those based on technology and those that rely on human effort and ingenuity. Reduction of NTLs is crucial for electricity utility companies, as these losses are concentrated in the high voltage (HV) network and are most critical at higher levels in industrial and large commercial sectors such as factories. As the current method of dealing with NTLs imposes high operational costs due to onsite inspection and requires extensive use of human resources.

E. Factors that influence illegal consumers

There are many factors that encourage people to steal electricity. Of which socio-economic factors influences people to a great extent in stealing electricity. A common notion in many people is that, it is dishonest to steal something from their neighbour but not from the state or public owned utility company. In addition, other factors that influence illegal consumers are:

- Higher energy prices deject consumers from buying electricity. In light of this, rich and highly educated communities also steal electricity to escape from huge utility bills.
- Growing unemployment rate show severe effect on the customer's economic situation.
- Lower illiteracy rate in under developed communities has greater impact on illegal consumers, as they might not be aware of the issues, laws and offenses related to the theft.
- Weak economic situation in many countries has implied its effect directly on common man.
- In view of socio economic conditions of the customer, electricity theft is proportional to the tariff of electricity utilization.
- Countries with weak enforcement of law against electricity theft have recorded high proportion of theft.
- Corrupt political leaders and employees of the utility company are responsible for billing irregularities. In addition, probability that an illegal consumer steals electricity from any distribution feeder depends on the sector where the feeder is located.

F. Effects of electricity theft

Negative effects of electricity theft are severe and dangerous. Primarily, electricity theft affects the utility company and then its customers. In addition, electricity theft overloads the generation unit. Quality of supply is also adversely affected, as the utility company has no estimate or audit about the amount of electricity to be supplied to genuine customers as well as illegal consumers. This overload might result in over voltages that can affect the performance and even damage appliances of genuine customers. This huge amount of NTL might trip the generation unit, which lead to the interruption in power supply to all customers. In view of unpredicted amount of load consumption may lead to brownouts and blackouts during in the peak

load. In order to maintain good power factor and flat voltage profile along the feeders, sufficient reactive power has to be supplied in addition to the supplied electricity. Load shedding should also be done to compensate the voltage collapse during the peak load period. VAR compensation and maintenance of power factor is very difficult without complete information about the total load flow because of the theft. In energy market, utility companies expect their money back from the customers for the electricity supplied, most of which is lost by them due to the NTL. Electricity theft is a serious concern for utility companies as they are under threat of survival because of these incurring economic losses. It is evident that some utility companies in developing countries are losing about 10 to 30 percent of their total revenue, which shows that they could not invest on measures to reduce the electricity theft. These economic losses affect the utility company's interest in development of the devices in view of improving the quality of supply or for electrification process. In addition, utility companies are forced to impose excessive tariff on genuine customers as they cannot bear the total losses just by themselves. In view of these tariff irregularities, it is not ethical to make genuine customers and utility companies pay for the energy consumed by illegal consumers. Also, illegal tapping of electricity raises safety concerns like electric shocks and even the death of a person. Improper handling of the distribution feeder might pose danger to the whole community during extreme weather conditions. These wires might start sparking and may give rise to fire. People start tapping electricity from distribution feeders during scheduled power cuts.

G. Current Practices Of theft Detection

The Distribution Network Operators have made attempts to achieve the most economical operation of distribution network and distribution of energy. Therefore, electricity tampering represents additional losses and a burden for them. Nevertheless, the monetary value of tampering creates a stimulus for detection of illegal use in the distribution network. In order to decrease the amount of tampering, the DNO investigates the possibilities of active search and detection of tampering attempts. However, the current practices are usually based on measurements taken in suspected locations, subsequent analysis and evaluation of the data measured. So far, there is no automated detection system for electricity tampering.

H. The current detection methodology

Firstly, the suspected area is initially investigated (inter alia based on notice of suspected activities). Afterwards, the power quality measurements take place in order to detect the location of illegal abstraction. One of the typical phenomena observed in the distribution networks with occurring theft is the switching of large loads in periodic intervals. This pattern is typical for consumption profiles of the growing farms. The example of periodical switching of a growing farm, measured on one of the feeders on the LV side of the MV/LV substation.

The cost associated with the procurement of the Arduino Nano and Arduino WiFI Shield 101 boards is high, relative to the cost of a single board, hence; there is need for a cheaper and effective system. In, a tamper proof electricity meter with IoT technology was developed with ATMega 328 embedded system module. This system is costly because of the cost of the ATMega 328 board relative to other embedded system boards like the Arduino. Also, the Raspberry pi is not an open source platform. The board is manufactured by only one vendor unlike other platforms like Arduino.

Hence, there is need to develop a system that will utilize an open source platform whose boards can easily be manufactured by various companies.

III. WAY TO THEFT ELECTRICITY

Theft of electricity is the criminal practice of stealing electrical power. It is a crime and is punishable by fines and/or incarceration. It belongs to the non-technical losses.

- Direct hooking from line
- Bypassing the energy meter
- Injecting foreign element in the energy meter
- Physical obstruction
- ESD attack on electronic meter

IV. METHODOLOGY

A. SYSTEM BLOCK DIAGRAM

Figure 1 shows the block diagram of the electricity theftdetection and prevention system. The system simply connectsthe meter to the Internet so that the utility company can beaware of the status of the electricity meter, in order todetermine when the meter is tampered with; hence the IoTconcept.

One good thing about the system is that the controller andthe network interface units are packed in a single module so asto reduce cost, associated with the procurement of two separate boards, one as the controller and the other as thenetwork interface.

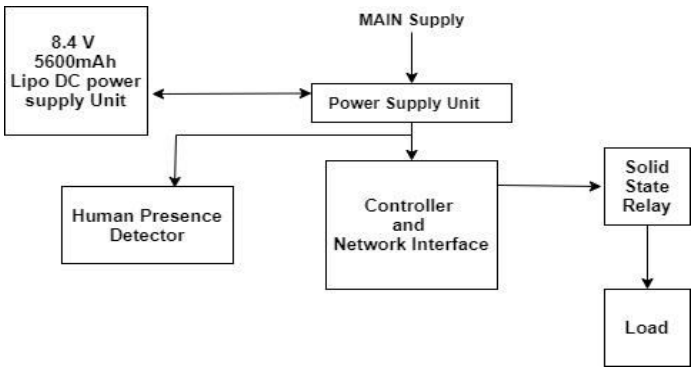

Figure 2

The system comprises of the following blocks:

A. Electricity Theft Detection Unit

For the purpose of this study, any attempt to open thesensitive part of the meter is considered a theft activity. Inorder to detect when the sensitive part of the meter is opened,a passive infrared sensor is chosen as the sensory element todetect the presence of a human whenever the meter enclosureis opened.

B. Controller and Network Interface

The controller coordinates the functions of all other partsof the system while the network interface is responsible forconnecting the system to a WiFi network and subsequently tothe Internet for data exchange.

To reduce cost, a single module is selected to act as acontroller and a network interface, instead of choosingseparate units for the controller and network interface. For thispurpose, the bi-functional Arduino ATMEGA328 board is chosento reduce cost and also reduce the number of components.

C. Electricity Theft Prevention Unit

To prevent electricity theft, it will be wise to disconnectthe loads of a suspected electricity thief from the distributionnetwork. A Solid state relay is utilized in connecting the loadsof a consumer to the distribution network in normal operationand in disconnecting the affected consumer from thedistribution network, when the meter is tampered with.

D. Power Supply Unit

This block provides the entire power needed by the systemto function. The 220V AC mains supply is reduced to 9V ACby a step down transformer, rectified using a pair of diodesthat formed a bi-phase full wave rectifier. A capacitor isemployed as a filter to remove the ripples in the signal whilethe LM7805 monolithic Integrated Circuit is employed forvoltage regulation to produce a constant 5V DC.
Also this power supply charges the DC Backup so thatwhen there is no power from the utility company, the DCBackup can energize the system.

E. CIRCUIT CONNETION

As a reminder, the controller and the network interface arealready connected on one board

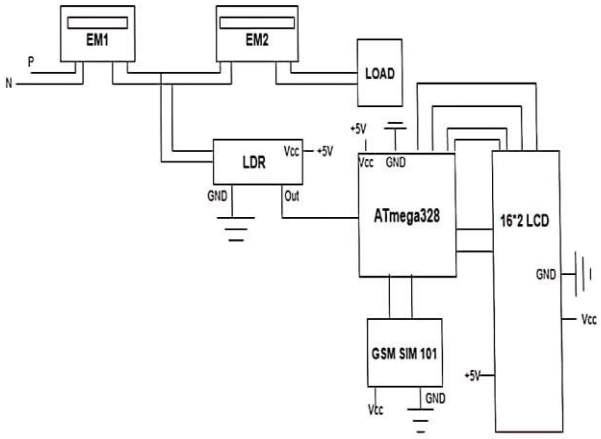

Figure 3

V. SYSTEM ALGORITHM

The following steps illustrate the algorithm of theelectricity theft detection and prevention system.

1. Once the device is powered, all components will beinitialized.
2. The system will connect the loads to the distributionnetwork.
3. The system then checks if the meter is tampered with.
4. After the check, the system will update the Internetwith the status of the meter.
5. The system continues to monitor the meter; once themeter is tampered with, the load connected to themeter is disconnected from the distribution network.

The Flow chart of Figure 3 represents the algorithm ofelectricity theft detection and prevention system. It shows themode of operation of the system

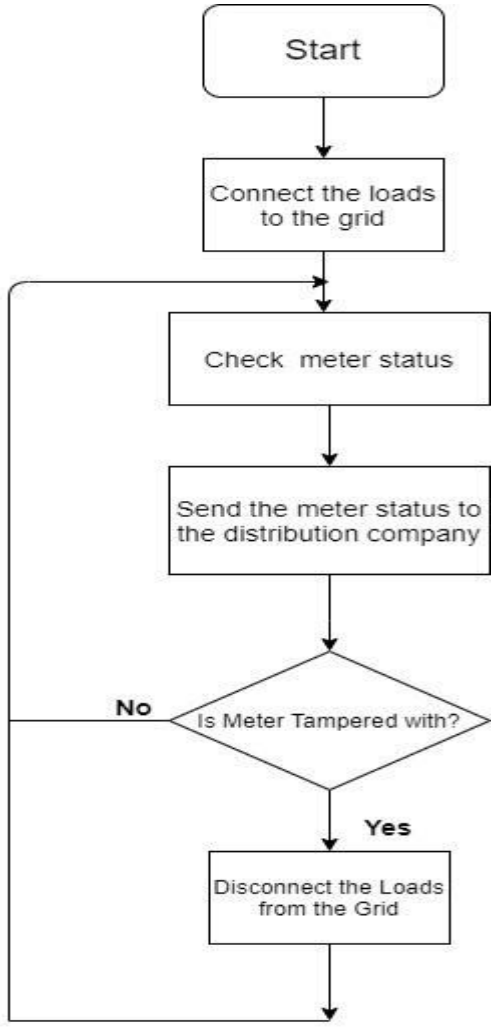

Figure 4

VI. DESIGNED HARDWARE

A. COMPONENT UTILISED

Table. 1 shows the list of major components that we used in our project along with their description and the purpose for which they were used in our project.

Components	**Description**	*Purpose*
Arduino UNO	A microcontroller based on AtMega 328. It has 14 IO pins & 6 analog input pins with operating voltage of 6v	Serial communication
Light Dependant Resistor	LDR is a commonly used photoconductive sensor	For Current sensing
Infrared Sensor	An electronic device which emits in order to sense some aspects of surrounding. Can sense upto 5m	As human sensor
LCD	A 16*2 LCD display with operating voltage of 5v	For displaying different values and information
WiFi	ESP8266 WiFi module	For establishing internet and getting real time values
Battery	12v 1.5A	For power supply

Table 1

VII. RECOMMENDATION

This study only developed a system that detects thepresence of humans tampering with the meter,recommendation is made on any study that will develop asystem to detect both humans and robots tampering with themeter. This is necessary because robots can also be Programmed to tamper with the meter, in such a case; thissystem becomes almost useless.

REFERENCES

- A.J. Dick , European Convention on Security and Detection, 76-18 May 1995, Conference publication No. 408, @ IEE, 7995[1]
- W.A. Doorduin , Feasibility study of electricity theft detection using mobile remote check meter,0-7083-8605-1/2004 IEEE Africon[2]
- J. Nagi,NTL detection if electricity theft and abnormalities for large power consumers in TNB Malasiya, 13 - 14 Dec 2010, Putrajaya, Malaysia, 978-1-4244-8648-9/10/$26.00 ©2010 IEEE[3]
- Ogu, R. E., and G. A. Chukwudebe. "Development of a costeffective electricity theft detection and prevention system based on IoT technology." *Electro-Technology for National Development (NIGERCON), 2017 IEEE 3rd International Conference on. IEEE, 2017*[4]
- Weixian Li, A novel smart energy theft system (SETS) for IOT based smart homes, IEEE internet of things journal, 2018[5]

- Rajiv Punmiya,Energy theft detection using gradient boosting theft detector with feature engineering based processing, 1949-3053 (c) 2019 IEEE[6]
- Akhil K, George Abraham,A review on IOT based power theft detection,© 2019 JETIR May 2019, Volume 6, Issue 5[7]
- Muhammad Badar Shahid,Design and development of an efficient power theft detection and prevention system through customer load profiling, Proc. of the 1st International Conference on Electrical, Communication and Computer Engineering (ICECCE) 24-25 July 2019, Swat, Pakistan[8]
- Akshaya U Kulkarni and Prof. Jayalaxmi.G.N. “IOT solution for live wire tampering” KLE Technological University, IEEE, 2018[9]
- Aditya Nandan ,Modelling Of Automatic Meter Reading System For Power Theft Detection , May 2013
- Singh, Maninderpal, and Er Varun Sanduja. "Minimizing electricity theft by internet of things." International Journal of Advanced Research in Computer and Communication Engineering 4.8 (2015)
- Pimentel, Juan R. "An effective and easy to use IoT architecture."Factory Communication Systems (WFCS), 2014 10th IEEE Workshop on. IEEE, 2014
- Kaur, Karandeep. "The idea of Smart villages based on Internet of Things (IoT)."Int. Res. J. Eng. Technol.(IRJET)3.05 (2016):1-4
- Bihl, Trevor J., and Salam Hajjar. "Electricity theft concerns within advanced energy technologies."Aerospace and Electronics Conference (NAECON), 2017 IEEE National. IEEE, 2017
- Saad, Muhammad, et al. "Theft detection based GSM prepaid electricity system." Control Science and Systems Engineering (ICCSSE), 2017 3rd IEEE International Conference on. IEEE, 2017. Exposition-Latin America (PES T&D-LA), 2016 IEEE PES. IEEE, 2016
- P. Kadurek,Theft detection and smart metering practices and expectations in the Netherlands , Student member, IEEE 2001
- Soma Shekara Sreenadh Reddy Depuru, Lingfeng Wang, Vijay Devabhaktuni and Nikhil Gudi,
- Solomon Nunnu ,Measures and Setbacks for Controlling Electricity Theft, A methodology for the design of electricity theft monitoring system , JTATIT ,2011
- Mohamed muzammil Mohamed mufassirin, Energy theft detection and controlling system model using wireless communication media, SEUSL, 2017
- Md. Umar hashmi, Anti theft energy metering for smart electrical distribution system, Conference paper , 2011
- Vasundhara Gaur, The determinants of electricity theft:An empirical analysis of Indian state, ELSEVIER journal, 2016
- D. Dangar, Electricity theft detection technologies for distribution system in GUVNL, ISSN: 2321-9939, 2014
- R. Menal, Power monitoring and theft detection using iot, International conference on physics and photonics process in nano science, 2019
- W.M.Warwick, A primer on electric utilities, deregulation, and restructuring of US electricity market, 2002
- Rouzbeh Razavi, A practical feature engineering framework for electricity theft detection in smart grids, ELSEVIER, 2019
- Sana Sardar, Detection and minimizing electricity theft: A review, 2015