



e-ISSN: 2278-8875

p-ISSN: 2320-3765

# International Journal of Advanced Research

in Electrical, Electronics and Instrumentation Engineering

Volume 11, Issue 3, March 2022

**ISSN** INTERNATIONAL  
STANDARD  
SERIAL  
NUMBER  
INDIA

Impact Factor: 7.282

9940 572 462

6381 907 438

ijareeie@gmail.com

www.ijareeie.com



# IOT Based Power Monitoring System and Power Theft Detection: A Review

Ms Aerica Ramteke<sup>1</sup>, Ms Devika Bankar<sup>2</sup>, Ms Achal Punwatkar<sup>3</sup>, Ms Trupti Meshram<sup>4</sup>,  
Mr Shreyash Borkar<sup>5</sup>, Mrs Jyoti Sathe<sup>6</sup>

UG Student, Dept. of Electrical Engineering, Priyadarshini College of Engineering, Nagpur, Maharashtra, India<sup>1</sup>

UG Student, Dept. of Electrical Engineering, Priyadarshini College of Engineering, Nagpur, Maharashtra, India<sup>2</sup>

UG Student, Dept. of Electrical Engineering, Priyadarshini College of Engineering, Nagpur, Maharashtra, India<sup>3</sup>

UG Student, Dept. of Electrical Engineering, Priyadarshini College of Engineering, Nagpur, Maharashtra, India<sup>4</sup>

UG Student, Dept. of Electrical Engineering, Priyadarshini College of Engineering, Nagpur, Maharashtra, India<sup>5</sup>

Assistant Professor, Dept. of Electrical Engineering, Priyadarshini College of Engineering, Nagpur, Maharashtra, India<sup>6</sup>

**ABSTRACT:** India is a hotbed of electricity theft especially in rural areas and in the middle and upper populations. Electricity theft is increasing every year in the homes and industries that affect the state of the country's economy. Power theft is usually done in two ways by jumping or hooking. To see it, a proposed system (current measurement and comparison) is proposed in which the distribution of family power is done indirectly from the distribution box to each house.

It is currently being rated from time to time in the distributor box and sent to the server of each used house server GSM / GPRS module. It is currently being rated from time to time in the distributor box and sent to the server of each used house serve GSM / GPRS module. It is currently being rated from time to time in the distributor box and sent to the server of each used house server GSM / GPRS module. The aim of this project is to design a system to monitor energy consumption and to detect and eliminate theft of electricity from transmission lines and electricity meters.

**KEYWORDS:** Electricity Theft, Monitoring System, Algorithm, Power Line Communication, Power Theft, IoT, NodeMCU

## I. INTRODUCTION

Electrical theft is a criminal practice of stealing power. As the population grows the demand for electricity increases. Power plants have been installed to meet the growing demand. Due to the depletion of natural resources the gap between supply and demand is growing steadily. A large amount of energy is required for the integrated steel plants to meet this requirement

In some areas the distribution of electricity exceeds the capacity given to that area. This leads to the theft of power or power exercised by unwanted users or unknown users. We need a system that can detect theft in power lines to avoid unnecessary power consumption. By using this example we can detect theft and possibly save a lot of electricity that can be used effectively on metal plants.

## II. LITERATURE SURVEY

### IoT based Power Theft Detection (IJIET 2017)

In the program proposed by R Giridhar Balakrishna, P Yogananda Reddy, M L N Vital To avoid power theft they use the IoT system to detect power theft and is done using Arduino, GSM, LCD, ESP module and current transformer. Between two CTs one is connected to the source side and the other is connected to the loading side and the signals of both CTs are supplied to Arduino. Arduino basically compares both data obtained in CTs from source and load side. If any difference is more than tolerable it means that there is a connection theft, then using the IoT and ESP module that works online this data is sent to the channel, If the internet has failed to use the GSM module used to send a message to the station where that line is connected when the stolen cargo is found. In this system energy recovery is done using



IoT and GSM. In the event of a failure of the IoT system GSM will work well to ignore this major global threat of power theft in the power network. [20]

#### **Power Theft Identification Using GSM Technology**

In the system proposed by Rhea Prakash, E. Annie Elisabeth Jebaseeli, Y.S.U.Sindhu crime detection was done using a PIC microcontroller, sensor, GSM module and LCD display. As we know that theft of electricity is usually done by passing meters. The heart of the system is Arduino control as it contains two microcontrollers. The project basically consists of two CTs one is mounted on one part of the pole and the other is connected to the other end of the pole and the local voltage pattern is processed by the output of two CTs in the Arduino control when the power goes down the limit exceeds the maximum allowable number of resources provided it means that the theft load is connected to the system received by the Arduino controller and delivers the message to the service using the GSM module installed in the Arduino kit. The data provided to Arduino is collected and analysed using MATLAB and the location of the theft is retrieved and action taken. In this project the theft is detected using real-time data without any human interface. [21]

#### **IoT Based Power Theft Detection And Monitoring System (IJIREICE 2017)**

In the system proposed by N Kunan1, Poornima BK2 used an intelligent power meter connected to the beginning of the transmission line and one to the side of the load, signals from both supplied to Arduino. Arduino collects data from each consumer's smart meter and compares that data with the current source given to the source side smart meter if the difference is within tolerance means there is no connected theft load, if the difference is greater than tolerance then the theft load is connected to the system and the system will be divided using a relay circuit and a message will be sent to the service company using the GSM module. The whole process was done using Arduino and continuously using the black Beagle bone system. Therefore, in this system online power theft is detected and the necessary action is taken without human interference. [17]

#### **GSM Based Electricity Theft Detection (ISSN 2016)**

In the program proposed by Nilesh Mohite1, Rinkuraj Ranaware2, Prakash Already 3 Provided a solution for the detection of various forms of energy theft. To alleviate this global threat of electricity theft, the project provides an effective mechanism to reduce the illicit use of electricity and to reduce the risk of theft. The project contains a collection of automated learning and crime detection without human interference. In this system the supply is made mainly using GSM, current transformer, PIC 18F4520 and power meter. As we know the most common ways to commit theft is to break the meter using a piece of wire before or after connecting the meter. In this system two CTs are used, one is connected to the input side and the other is connected to the house line distribution, both signals from two CTs are given PIC18F4520 in case the meter reading from the entry side does not match the buyer or the load side without tolerating the given loss and then that there is a power theft occurring over the meter and the message is delivered to the service using the GSM module. In some cases if there is a meter interference, an IR sensor is connected to the meter so that the indicator is supplied using the GSM plug-in to the PLC kit and theft is detected without any manual interface. Therefore, in this project the discovery of power theft is done in a simple way without being handled. [19]

#### **Electric Power Theft Detection And Location Tracking Using IoT**

In the program proposed by Ajay Mahato, Abhishek Nanda, Ajay Kumar Pal, Chandan Kumar To overcome this global threat by introducing power theft and location tracking using IoT. In this way there is a current sensor and voltage connected before the cable is connected to the meter and a connection from the power meter is also provided with a small PIC controller that compares both current values and if the difference is heard by the PIC microcontroller it means theft has occurred in the system, and that circuit will be separated from the supply using the referred circuit and the message will be sent to the service company using the GSM module. Therefore, in this system online power theft is detected and the necessary action is taken without human interference. [15]

#### **Distribution Line Monitoring System for the Detection of Power Theft Using Power Line Communication**

In the proposed system there is a condition for the theft of electricity using the connection of power lines. Basically for this system high frequency is added to the maximum power between 3 kHz to 500 kHz according to Indian power standards. When the power cord is switched off and there is a fluctuation in the system frequency that is analysed at the station using the Matlab System and the location of the power supply is detected and due to the provision of high frequencies the equipment connected to the stolen load fails. In this operation the theft of electricity is detected and action is taken without human interference. [16]



### Electrical theft detection and Wireless meter reading (IJIRISSET)

In the proposed program provided by Sagar Patil, Gopal Pawaskar, Kritikumar Patil, used digital meters, wireless data transmitter and cable connection to detect cable theft. Basically in this system one digital meter is attached to a pole and the other is connected to the customer position or to the side of the load. The digital meter on the load side collects data and sends it continuously to the digital meter next to the pole where a small controller is installed with the help of a wireless transmitter. The microcontroller retrieves both data from the source side and the loading side, with the help of a wireless receiver and compares the data, if the difference is below the tolerance band there will be no theft of the power cord. In some cases if the difference is more than tolerable it means that the theft occurs on the cable obtained by the microcontroller and the required information is sent to the station through a cable connection, and then other steps are taken, hence the power cord. theft is detected and the line is protected from theft using this system. And by using the same data provided by the side load meter the consumer meter reading is extracted. [22]

### Smart Meter Data Analysis for Power Theft Detection

In this proposed system there is a supply of power supply made using arduino uno controller, Smart power meter and GSM method. In this CT one is connected to a distribution box and the data is fed to a small station periodically using a GSM module and data from a power meter installed in the consumer area is designed to measure the applied power and transmit it periodically using the GSM module to a small station. . At substation data from both end of the distribution and from the place the buyer collected and compared if there is a difference in learning occurs in addition to the permissible tolerance then it simply means that the theft load is connected to the system and since there is GPRS connected to poles and electricity meters installed. other steps. In this project power theft is detected without manual interference using real-time data. [18]

In a research project conducted by P. Jokar et al. [1], the authors introduced a power theft detector based on a usage pattern, find a suspicious use pattern. Areas with high potential formalicious use patterns are marked, and with extraordinary vigilance in usage patterns, suspicious customers are identified. Separation and integration methods are used. Also, the use of transformers and non-standard detectors, makes the algorithm stronger against aggressive change of application pattern and provides higher and adjustable performance at a lower sample rate. In a research project conducted by M. Tariq et al. [2], stochastic Petri net formalism is used in this paper to identify and localize the occurrence of crime in grid-assembled MGs. Disruption at any time in the form of resistance beyond the limit of intelligent data collected, regardless of the operating method, initiates a modification given to the arc, which informs the transmission module. Affected changes and suspicious user information are sent to the Meter Data Management System (MDMS) for local theft. In testing, it calculates technological and nontechnical losses with complete accuracy without having to know the exact topology of the power distribution network.

In a research project conducted by A. J. Dick [3], a researcher looks at income-generating activities within the UK to combat the problem of electricity theft, which is estimated to cost the electricity industry (EI) approximately 50 meters per year. It first analyses the nature and severity of the problem, notes the incidents related to different types of theft and interference, and then indicates the legal framework. Then a report is made on the stated process. In a study conducted by N. Mohammad et al. [4], researchers are proposing a cost-effective measurement system to control power theft. Smart meters are used and installed on all customer units and the server is maintained. Both the meter and the server are equipped with a GSM module, which allows for two connections. Several ways to combat electrical-related malpractice have been described. Electricity theft can be reduced by using these methods. In a research work done by A. Jindal et al. [9], the authors have focused on nontechnical losses, mainly due to the theft of electricity, this has been a major concern for the energy system industry for a long time. There is a gap between demand and supply thus creating energy issues. Thus, the need arises to develop a system that can detect these threats accurately on complex power networks. Therefore, by finally focusing on these points, this paper proposes a complete overhead system based on decision-making (DT) and vector support systems (SVM). This program is unique in that it can detect theft in both transfers and distributions. The proposed system is based on the integration of DT and SVM phases in order to rigorously analyze the collected electricity consumption data. In other words, the proposed system can be considered as a two-level data processing and analysis system, as DT-processed data is provided input into the SVM separator. In addition, the results obtained show that the proposed scheme reduces false perceptions to a large extent and is effective enough to be used in real-time situations.

In a research work done by J. Nagi et al. [10], the authors' work on finding effective estimates of counterfeit electricity has been an effective research topic in recent years. This paper introduces a way to deal with non-technical losses using



a new technology-based approach, Vector Support Machine (SVM). The main impetus for this study is to help Tenaga Nasional Berhad (TNB) in Malaysia reduce its NTLs to the distribution sector due to power theft. The proposed model prepares customers suspected to be tested locally for fraud based on misconduct and misconduct. Here customer usage patterns are recorded. It is obtained using an unusual usage pattern. Suspicious users are shortlisted. This method is better proven compared to existing methods, In a research work done by J. Nagi et al. [11], the authors have been working on finding effective ways to detect electrical fraud which has been the subject of active research in recent years. This paper introduces a mixed approach to non-technical (NTL) loss of electronic resources using genetic algorithm (GA) and vector support (SVM). The main impetus for this study is to help Tenaga Nasional Berhad (TNB) in Malaysia reduces its NTLs in the distribution sector. This hybrid GA-SVM combination prepares customers suspected to be tested locally for fraud based on unusual use. The proposed method uses customer load profile information to expose unusual behaviours that are known to be strongly associated with NTL activities. GA provides increased integration with SVM hyper-fully-effected parameters worldwide using a combination of random and human-generated genomes. The result of the fraud detection model identifies the separate classes used to screen potential fraud suspects for local investigation. Imitation results confirm that the proposed method is more effective when compared to current actions taken by TNB to reduce NTL operations.

In a study conducted by T. B. Smith [12], worked on the issue of theft of electricity can be a form of fraud (meter fraud), theft (illegal communication), breach of billing rules, and unpaid bills. Electricity theft statistics in 102 countries were collected. Electricity theft and various forms of opposition are discussed. In a research work done by R. F. Ghajar et al. [13], the authors work on the fact that one of the biggest pitfalls of any network are the distribution of power losses experienced by the system There are two types of technical losses and non-technical losses, technological losses. F. Ghajar et al. [13], the authors work on the fact that one of the major pitfalls of any network is the distribution of energy losses experienced by the system. Two types of technical and non-technical losses, technical losses are highly dependent on network material, while non-technical losses (sometimes the most important type of loss) are the result of theft or fraud caused by meter interruptions, false reading, illegal communication or unpaid bills. The results of this study and the cost / benefit analysis of the proposed program are summarized in this paper.

In a research project conducted by K. L. Joseph et al. [14], the authors have worked on the fact that persistent theft, corruption, and declining price structure have made it almost impossible for government services in India to improve power service. As a result, industrial buyers across India are moving out of a state-owned system and relying on power generation on their site to ensure a stable and reliable source of electricity. The Electricity Act of 2003 promotes the continuous production of energy from these captive plants through its open access clause. By encouraging the growth of these captive power stations, politicians in India established a dual track economy, where state run production and market operations coexist. This strategy allows politicians to promote the involvement of the private sector in the electricity market, without compromising the support of key political regions at the state level.

### III. CONCLUSION

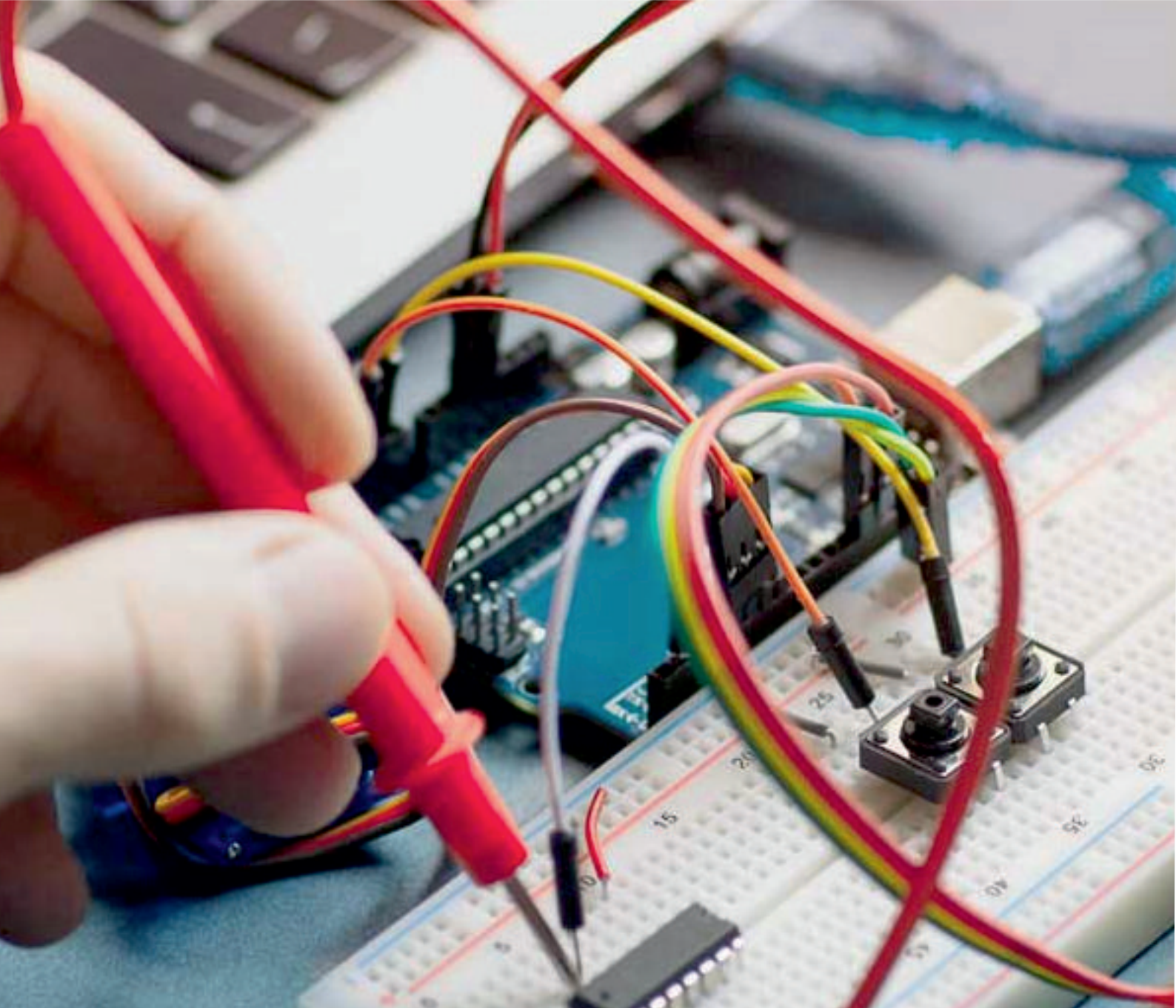
The expected outcome of this study is that there will be a variety of ways to deal with the major problem of electricity theft and to provide a comprehensive and comparative study between these economic-based approaches as well as the diversity. The expected outcome of the end of the study is to design and replicate these approaches and therefore come up with effective solutions to support the strength and economic situation of our country and the world. We were able to spot the theft of electricity successfully. Local practice is an opportunity that can be taken to make the process more dynamic.

### REFERENCES

- [1] P. Jokar, N. Arianpoo and V. C. M. Leung, "Electricity Theft Detection in AMI Using Customers' Consumption Patterns", IEEE Transactions on Smart Grid, Vol. 7, Issue 1, Jan. 2016, pp. 216-226. Doi: 10.1109/TSG.2015.2425222
- [2] M. Tariq and H. V. Poor, "Electricity Theft Detection and Localization in Grid-Tied Micro grids", IEEE Transactions on Smart Grid, Vol. 9, Issue 3, May 2018, pp. 1920- 1929. Doi: 10.1109/TSG.2016.2602660
- [3] A. J. Dick, "Theft of electricity-how UK electricity companies detect and deter", Proc. Of European Convention on Security and Detection, 1995, Brighton, UK, 16-18 May 1995, pp. 90- 95. Doi: 10.1049/cp: 19950476
- [4] N. Mohammad, A. Barua and Muhammad A. Arafat, "A smart prepaid Energy metering System to control electricity theft", Proc. of 2013 International Conference on Power, Energy and Control (ICPEC), Sri Ranganalathum Dindigul, India, 6-8 Feb. 2013, pp. 562-565. Doi: 10.1109/ICPEC.2013.6527721



- [5] S. Kumar, Electricity Theft: Empowering People and Reforming Power Sector, Manohar Publications, New Delhi, 2004
- [6] “Indian Power Sector Loses \$16.2b To Theft Every Year”, ASIANPOWER, 21 January, 2015. [Online]. Available: <https://AsianPower.Com/Ipp/In-Focus/Indian-PowerSector-Loses-162b-Theft-Every-Year> (Accessed: 21 July, 2018)
- [7] A. Agarwal, “Power Theft in India”, PROJECT GURU, 10 December, 2012. [Online]. Available: <https://www.projectguru.in/publications/power-theft-india/> (Accessed: 21 July, 2018)
- [8] P. Kelly-Detwiler, “Energy Theft: A Bigger Issue Than You Think”, Forbes, 23 April, 2013.[Online]. Available: <https://www.forbes.com/sites/peterdetwiler/2013/04/23/electricity-theft-a-bigger-issue-than-you-think/#693d7aa75ed7> (Accessed: 21 July, 2018)
- [9] A. Jindal, A. Dua, K. Kaur, M. Singh, N. Kumar and S. Mishra, “Decision Tree and SVM Based Data Analytics for Theft Detection in Smart Grid”, IEEE Transactions on Industrial Informatics, Vol. 12, Issue 3, June 2016, pp. 1005-1016. Doi: 10.1109/TII.2016.2543145
- [10] J. Nagi, A. M. Mohammad, K. S. Yap, S. K. Tiong and S. K. Ahmed, “Non-Technical Loss Analysis for detection of electricity theft using support vector machines”, Proc. of 2008 IEEE 2<sup>nd</sup> International Power and Energy Conference, Johor Bahru, 1-3 Dec. 2008, pp. 907-912. Doi: 10.1109/PECON.2008.4762604
- [11] J. Nagi, K. S. Yap, S. K. Tiong, S. K. Ahmed and A. M. Mohammad, “Detection of Abnormalities and electricity theft using genetic Support Vector Machines”, Proc. of TENCON 2008 - 2008 IEEE Region 10 Conferences, Hyderabad, India, 19-21 Nov. 2008, pp. 1-6. Doi: 10.1109/TENCON.2008.4766403
- [12] T. B. Smith “Electricity Theft: a comparative analysis”, Energy Policy, Vol. 32, Issue 18, December 2004, pp. 2067- 2076. Doi: [https://doi.org/10.1016/S0301-4215\(03\)00182-4](https://doi.org/10.1016/S0301-4215(03)00182-4)
- [13] R. F. Ghajar and J. Khalife, “Cost/benefit analysis of an AMR system to reduce electricity Theft and maximize revenues for Électricité du Liban”, Applied Energy, Vol. 76, Issues 1-3, September-November 2003, pp. 25-37. Doi: [https://doi.org/10.1016/S0306-2619\(03\)00044-8](https://doi.org/10.1016/S0306-2619(03)00044-8)
- [14] K. L. Joseph, “The politics of power: Electricity reform in India”, Energy Policy, Vol. 38, Issue 1, January 2010, pp. 503-511. Doi: <https://doi.org/10.1016/j.enpol.2009.09.041>
- [15] Ajay Mahato, A. N. (2018). Electric Power Theft Detection and Location Tracking Using IoT. International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT) | Volume 4 | Issue 5 | ISSN: 2456-3307,
- [16] Guhesh Swaminathan, M. S. (n.d.). Distribution Line Monitoring System for the Detection Of Power Theft Using Power Line Communication.
- [17] N. K. N. (2017). IoT Based Power Theft Detection and Monitoring System (IJIREICE 2017). International Journal of Innovative Research in Electrical, Electronics, Instrumentation And Control Engineering ISO 3297:2007 Certified Vol. 5,
- [18] Nikovski D, W. Z. (2013). Smart Meter Data Analysis for Power Theft Detection.
- [19] Nilesh Mohite, R. R. (2016). GSM Based Electricity Theft Detection. International Journal of Scientific Engineering and Applied Science (IJSEAS) – Volume-2,
- [20] R. Giridhar Balakrishna, P. Y. (2017). IoT based Power Theft Detection. IJIEET, [21] Rhea Prakash, E. A. (2017). Power Theft Identification Using GSM Technology. International Journal of Advanced Research in Electrical, Vol. 6,
- [22] Sagar Patil, G. P. (2013). ELECTRICAL POWER THEFT DETECTION AND WIRELESS METER READING. International Journal of Innovative Research in Science, Engineering and Technology, vol.2



**INNO**  **SPACE**  
SJIF Scientific Journal Impact Factor  
**Impact Factor: 7.282**



**ISSN** INTERNATIONAL  
STANDARD  
SERIAL  
NUMBER  
**INDIA**



# International Journal of Advanced Research

in Electrical, Electronics and Instrumentation Engineering

 **9940 572 462**  **6381 907 438**  **ijareeie@gmail.com**



[www.ijareeie.com](http://www.ijareeie.com)

Scan to save the contact details