International Journal of Microwave Engineering and Technology

ISSN: 2455-0337

Volume- 10

Issue- 02

Year- 2024

Review article

Date of Receiving- 8th Oct 2024

Date of Acceptance- 17th Oct 2024

Date of Publication- 27th Oct 2024

Effective Power Theft Identification in Advanced Metering Infrastructure with the Use of Smart Metre Data-A Review

Akshay Bharat Dimbar*

Student, Department of Electrical

Engineering

Sanjivani College of Engineering

Kopargaon, India

akshaydimbarwari@gmail.com

Bhushan Kadam

Student, Department of Electrical

Engineering

Sanjivani College of Engineering

Kopargaon, India

Dipesh Pardeshi

Student, Department of Electrical

Engineering

Sanjivani College of Engineering

Kopargaon, India

Abstract- Power theft, also known as the unlawful act of stealing electrical energy, encompasses a range of illegal actions such as tampering with meters, unauthorized connections, billing discrepancies, and unpaid bills. With advancements in electronic meters, tampering and magnetic locking have become virtually impossible. Consequently, the most common types of power theft today involve direct hooking from the power line, physical obstructions, and bypassing the energy meter. Power consumer dishonesty is a critical issue faced by utilities, and to combat this, the government of India has implemented the use of smart meters. The identification of effective methods for detecting fraudulent electricity consumption has been a significant area of research in recent years. In this power theft detection project, the focus is on detecting and bringing attention to unauthorized power consumption in order to safeguard the efficient use of power resources.

Keyword- Power Theft, Meter Tampering, microcontroller, amplifier.

I. INTRODUCTION

Electricity has been intertwined with humanity since the beginning of civilization. In modern times, it has become an indispensable component of our daily existence. Without electricity, our lives would come to a standstill. As our reliance on electricity increases, so does the occurrence of electricity theft. No place in the world is immune to this crime. Just like any valuable resource, electricity can be both utilized and exploited. Power theft encompasses unauthorized connections, tampering with meters, fraudulent billing, and unpaid bills. This illegal act robs electricity providers of billions of dollars every year in countries such as India. The current energy crisis has brought the pressing issues of energy distribution and consumption to the forefront of discussion. In particular, the act of "theft" - deliberately manipulating meter equipment to avoid recording low energy usage - has become a major concern. This issue disproportionately affects developing economies, with power utilities estimated to lose over $21 billion annually due to theft. Companies are now implementing a solution known as the Advanced Metering Infrastructure (AMI), which involves installing smart meters at the customer's location. Energy distribution and consumption have become pressing issues due to the significant energy debt. In this context, "theft" refers to a deliberate act of stealing a considerable amount of energy by ensuring that the metering equipment does not record low energy usage. This problem is particularly prevalent in developing economies, where power theft is estimated to cost power utilities over 21 billion dollars annually worldwide. To combat this issue, companies have introduced a new Smart Grid called Advanced Metering Infrastructure (AMI). This involves installing smart meters at customers' homes, allowing for two-way communication between the customer and supplier. Now, it is no longer possible to manipulate readings by bribing the reading agents or tampering with the meter, thanks to AMI technology. "Introducing a modern form of theft known as cyber-interventions, targeting smart meters. We have devised a powerful system that utilizes consumption data to detect dishonest customers. As a result, the need for manual inspections of every meter will be greatly reduced as our system effectively identifies potential offenders, leading to significant cost savings.".

II. LITRATURE REVIEW

[1]Power has been an essential requirement for human life since its discovery. A consistent and affordable source of power is essential for every economy, but developing economies particularly so, and it has fueled the industrial revolution. However, power theft poses a serious risk to electric firms, disasters for power distributors, and causes financial harm. One way to prevent corruption is to conduct routine manual inspections of every client, but this approach is exceedingly time and money-consuming. Advanced Metering Infrastructure (AMI) is a system that uses smart metres to automate the monitoring of electric energy use and provides two-way communication between the consumer and the supplier.

[2] Fraud, which includes metre manipulation, unauthorised connections, anomalous invoicing, and unpaid bills, is what is commonly referred to as electricity theft. Financial statistics show that power theft accounts for the majority of electricity theft. Metre manipulation and magnetic locking are not possible with modern electronic metres. As a result, connecting straight from the distribution lines is currently the most popular method of power theft. All power companies deal with the issue of dishonest electricity consumers. The development of effective metrics for identifying fraudulent power use has been a busy field of study in recent years. In order to avoid planter theft, this idea focuses on detecting illegitimate power usage and bright lighting.

[3]In order to identify any theft involving energy, this paper suggests studying the topic of electricity and power theft detection. Everyday living depends heavily on electrical energy, which also serves as the backbone of the business. Since energy is a necessary component of daily life and plays a significant part in many aspects of it, power theft related to electricity is rising along with the demand for it. electricity theft is a serious issue that still affects the nation's electricity industry. This project's goal is to create a system that will prevent people from becoming upset when they steal electricity, regardless of whether the electricity was used or not.

[4] Fraud, which includes meter manipulation, unauthorized connections, anomalous invoicing, and unpaid bills, is what is commonly referred to as electricity theft. Financial statistics show that power theft accounts for the majority of electricity theft. Metre manipulation and magnetic locking are impossible with contemporary electronic meters. Thus, customer dishonesty is the most prevalent kind of power theft these days, and it is an issue that all power providers must deal with. The development of effective metrics for identifying fraudulent power use has been a busy field of study in recent years. The goal of this initiative is to identify and provide information on illegitimate power usage to the TNER Keyword.

III. OVERVIEW

A. What is Power Theft?

Electricity theft is defined by Section 135 of the Electricity Act 2003 as tapping electricity lines, tampering with electricity metres or transformers, using a device that obstructs or damages equipment, such as electric metres, or using electricity for purposes other than those permitted. If power theft is discovered, the electric gadget has the ability to cut off the electricity supply right away. A fine equivalent to "three times the financial gain on account of this type of theft of electricity" is imposed for such an infraction. Should the individual commit the same crime again, their access to electricity will be restricted for a minimum of three months and a maximum of two years. Power theft is a severe problem that is exceedingly risky in addition to being illegal. When someone tries to avoid paying the electric metre at a service panel, they are engaging in power theft. Tampering can lead to dangerous situations that could include an explosion, fire, electrical shock, or even death. The Modes to Irrigation District, or MID, has the authority to cut off power to anybody caught stealing electricity. According to Rule No. 11 [5] of the MID's Electric Service Rules, "the District may discontinue or refuse service or refuse to re-establish service if any part of a customer's wiring or equipment or uses of either unsafe or in violation of law, until such apparatus shall have been placed in a safe condition or the violation remedied and all related charges and fees for metre tampering, power theft energy diversion and broken or damaged District equipment have been paid by customer if they had w Without giving a client advance warning, the district may stop providing services if the district judgement finds that using the customer's equipment poses a risk.[6]

B.Types of power theft

1. Direct hooking from line -The most popular technique is cable hooking. Direct line tapping accounts for 80% of all power theft worldwide. From a location ahead of the energy metre, the customer taps into a power line. Direct hooking from line shown in Figure 1. This energy use is measuredless and may be obtained with or without switches.[7] It may result in a serious electric shock or a fire.

Figure 1. Direct hooking from line

2.Bypassing the energy meter-

By bridging the energy meter's input and output terminals, this approach keeps energy from registering in the energy metre.

3.Injecting Foreign elements in the energy meter-

By placing a circuit within the metre, which allows it to be slowed down at any time, metres may be controlled using a remote.[8] The reason this type of update can elude external inspection attempts is that, until the remote is switched on, the neter is always right. Electromechanical metres that have a revolving element are tampered with in this manner. Injecting Foreign elements in the energy meter shown in Figure 2. To

prevent the disc from moving freely, foreign objects are inserted inside the metre.

Figure 2. Injecting Foreign elements in the energy meter

Power theft occurs anywhere in the globe. Increased electricity costs, reduced utility bills.[9] Power theft occurs anywhere in the globe. The major reasons of energy theft were determined to be higher electricity rates, low quality power delivered, corruption, lax enforcement of the legislation against electricity theft, and the PURC's lack of advocacy for consumer interests. Such an all-encompassing failure is acknowledged to be primarily caused by inadequate infrastructure, inadequate capacity, and inadequate control of the electrical supply. [10] Regarding governance, it has been proposed that over 20 percent of India's total power production is Stolen. he act of stealing electricity is generally referred to as theft of electricity. It is a crime that carries a fine or reincarnation penalty. It concerns losses that aren't technological. Losses resulting from actions outside of the power system are referred to as non-technical losses.[11]

IV. METHODOLOGY

There is a structured methodology involved in using smart meter data to identify power theft in Advanced Metering Infrastructure (AMI).

Gather data: Utilize smart meters to gather data as they capture usage and additional pertinent details. Periodically (for example, hourly) this data can be collected.[12-13]

Data preprocessing: Make sure the data is clean and ready for analysis. Outlier detection, data normalization, and handling missing data are all included in this.

Utilization patterns of each customer should be taken into account when creating load profiles. When these profiles diverge, it could be a sign of possible theft.

Anomaly Detection: To find anomalies in the data, apply machine learning and statistical techniques. Unusual consumption trends or abrupt increases may be signs of energy theft.[14-15]

Using clustering analysis, you can find outliers or customers with notable deviations by grouping customers with similar load profiles.

Examine how consumption patterns are distributed geographically using geospatial analysis. Certain trends may be evident in areas with high rates of power theft.

Pattern Recognition: Create algorithms to identify particular patterns connected to prevalent forms of power theft, like bypassing or tampering with meters.

Generate alerts for additional investigation in the event that anomalies or possible indicators of theft are found.

User Engagement: Let customers know when you notice any suspicious activity so they can adjust any invoice errors.

Perform on-site examinations or utilize remote validation to validate suspicions of power theft.[16]

Legal Action: File the proper paperwork to hold the perpetrator accountable if power theft is proven.

Ongoing Monitoring: To find new cases of power theft, conduct ongoing monitoring as well as recurring audits.

Data Security: Make sure that the data from smart meters is secure, and follow any rules pertaining to data privacy.

Build load profiles for every client based on their usage habits with load profiling. Any deviations from these profiles could be signs of impending theft.

Examine the distribution of consumption patterns geographically using geographic analysis. Certain trends may be seen in areas where power theft is common.

Continuous Improvement: Update and improve the process on a regular basis to make it more accurate and flexible in response to changing theft tactics.[17]

Legal and regulatory compliance: Verify that the power theft identification methodology complies with all applicable laws and regulations.

Instruction and Education: Teach utility employees how to operate the system efficiently and educate consumers about preventing power theft.

The quality of the data from smart meters and the strength of the analysis methods employed determine how effective this methodology is. Power theft identification accuracy can be improved with the use of machine learning models and advanced analytics.[18]

V. WHY PUBLIC FILTER ENERGY?

1. People are constantly searching for ways to save money on their utility bills.

2. Industries that heavily rely on electricity for production, such as steel and plastic injection molding, often resort to illegal methods in order to keep their costs competitive. This is also seen in businesses like ice factories and commercial establishments.

3. In order to bypass certain regulations and restrictions, such as power cuts and peak load periods, individuals may engage in electricity theft. This type of theft is prevalent in countries where there is a scarcity of electricity.

4. Additionally, some industries, such as steel, ice, cloth, and yarn, may try to avoid other taxes by underreporting their electricity consumption. This is because in certain countries, taxes like excise, sales, and income tax are calculated based on the recorded electricity usage. A similar

situation occurs in pitch mills, where labor costs are based on the amount of electricity used.[19]

5. The act of power theft is often labeled as a form of white-collar crime, driven by a desire to portray a false image to the public.

6. Additionally, some individuals take pleasure in the challenge it presents, deriving a sense of intellectual superiority if they are able to successfully steal.

7. On the other hand, there are those who view laws with dissent and believe they can justify breaking them without consequences, whether it be through small infractions like violating traffic rules or more serious offenses like committing crimes.

8. In order to successfully cultivate marijuana, the use of high intensity lighting is crucial. And when it comes to festival seasons and the need for illumination, many individuals believe that.[20]

VI. CHALLENGES/ PROBLEMS IN SMART METER

1. Processing and analysis in real-time or almost real-time is challenging due to the volume of data generated by smart meters. The quality of data can be compromised by a number of things, including malfunctioning devices, communication issues, and meter tampering.

2. This is a serious problem because managing data from smart meters requires handling sensitive information about the energy consumption habits and personal preferences of customers, which needs to be safeguarded against abuse and illegal access.[21]

3. It can be challenging to strike a balance between data privacy and the necessity of identifying and stopping theft, though. It mainly depends on finding anomalies in power consumption patterns, which necessitates the use of complex algorithms to determine what constitutes anomalous or acceptable variations

4. Solving, detecting meter tampering to manipulate data can be difficult. It is especially difficult to uncover without the use of sophisticated techniques due to covert tampering.

5. Furthermore, since smart meters depend on communication networks to transfer data, these networks must be dependable in order to detect power theft in a timely manner. As a result, maintaining the reliability of communication networks is essential for precise and timely data analysis.[22]

VII. PROBABLE SOLUTIONS TO THE CHALLENGES

1."Efficiently Managing Data: Real-time or near-real-time analytics must be implemented in order to manage the enormous volumes of data generated by smart meters. This makes it possible to identify anomalies or cases of power theft quickly

2. Leveraging Advanced Technology: The key to effectively managing the massive volumes of data is incorporating big data technologies and making use of scalable cloud platforms. By doing so, processing and analysis can be expedited, and the available data can be fully utilized.

3. Ensuring Data Security and Privacy: It is crucial to protect the confidentiality of client information. Sensitive data is safeguarded by encrypting smart meter data both in transit and storage, and by putting strict access control measures in place."

4. Using Machine Learning to Detect Anomalies: Our objective is to create and implement machine learning algorithms that can dynamically learn from historical data and adapt in order to detect anomalies with accuracy.

5. Understanding Customers: By developing thorough profiles of each customer, we can learn more about how they use our services and improve our ability to spot any unusual activity.

6. Stopping Meter Tampering: Making Use of Advanced Sensors In order to quickly identify physical tampering, we are integrating state-of-the-art tamper detection sensors into our smart meters

7. Ensuring Data Integrity: To quickly spot any anomalies or warning signs in the transmitted meter data, our system incorporates strong data integrity checks.

VIII. RESULT AND DISCUSSION

Measuring the accuracy of a power theft detection system goes beyond simply reporting on its precision. By including key metrics such as true positives, false positives, true negatives, and false negatives, a more comprehensive picture of the system's effectiveness can be presented. Let us not forget to highlight the overall detection rate, as well as any significant improvements that have been made. While accuracy is essential, the rate of false alarms also plays a crucial role in the success of a detection system. Any false alarms can lead to unnecessary disruptions and can cause mistrust in the system. It is crucial to discuss efforts made to reduce false alarms, whether through algorithm improvements or data quality control measures. Real-life examples speak louder than words. Hence, it is vital to include case studies that illustrate successful power theft identifications. These case studies should highlight the techniques used and the results achieved, providing tangible evidence of the system's ability to detect and prevent power theft.

IX. CONCLUSION

In essence, our utility has seen significant benefits from leveraging smart meter data to create a power theft detection system as part of our Advanced Metering Infrastructure. Our efforts have resulted in notable progress in identifying and preventing power theft, while prioritizing the protection of customer information and privacy through the integration of state-of-the-art techniques, data analysis, and cybersecurity measures. Our power theft identification system has proven to be highly effective in detecting unusual energy consumption patterns, enabling us to quickly identify and address instances of theft. Furthermore, our commitment to quality control has led to a low rate of false alarms and a high rate of accurate detections, providing a reliable and trustworthy platform for managing power theft detection

REFERENCES

[1] Y. Chen, G. Hua, D. Feng, H. Zang, Z. Wei and G. Sun, "Electricity Theft Detection Model for Smart Meter Based on Residual Neural Network," 2020 12th IEEE PES Asia-Pacific Power and Energy Engineering Conference (APPEEC), Nanjing, China, 2020, pp. 1-5, doi: 10.1109/APPEEC48164.2020.9220523.

[2] R. Andore, S. S. Kulkarni and A. G. Thosar, "Energy Meter and Power Theft Monitoring System," 2023 IEEE International Students' Conference on Electrical, Electronics and Computer Science (SCEECS), Bhopal, India, 2023, pp. 1-6, doi: 10.1109/SCEECS57921.2023.10062967.

[3] Y. B. Najgad, S. Namdev Munde, P. S. Chobe, D. B. Pardeshi and P. William, "Advancement of Hybrid Energy Storage System with PWM Technique for Electric Vehicles," 2022 6th International Conference on Intelligent Computing and Control Systems (ICICCS), 2022, pp. 238-242, doi: 10.1109/ICICCS53718.2022.9788135.

[4] R. B. Ghoderao, S. Raosaheb Balwe, P. S. Chobe, D. B. Pardeshi and P. William, "Smart Charging Station for Electric Vehicle with Different Topologies," 2022 6th International Conference on Intelligent Computing and Control Systems (ICICCS), 2022, pp. 243-246, doi: 10.1109/ICICCS53718.2022.9788143.

[5] S. S. Gondkar, P. William and D. B. Pardeshi, "Design of a Novel IoT Framework for Home Automation using Google Assistant," 2022 6th International Conference on Intelligent Computing and Control Systems (ICICCS), 2022, pp. 451-454, doi: 10.1109/ICICCS53718.2022.9788284.

[6] D. S. Navare, Y. R. Kapde, S. Maurya, D. B. Pardeshi and P. William, "Robotic Bomb Detection and Disposal: Application using Arduino," 2022 7th International Conference on Communication and Electronics Systems (ICCES), 2022, pp. 479-483, doi: 10.1109/ICCES54183.2022.9836011.

[7] 3.S. Sahoo, D. Nikovski, T. Muso and K. Tsuru, "Electricity theft detection using smart meter data," 2015 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT), Washington, DC, USA, 2015, pp. 1-5, doi: 10.1109/ISGT.2015.7131776.

[8] S. Mittra, A. Aprameya and B. K. Mohanta, "Smart Grid Power Theft and Fault Detection using IoT and Blockchain," 2021 International Conference on Advancements in Electrical, Electronics, Communication, Computing and Automation (ICAECA), Coimbatore, India, 2021, pp. 1-5, doi: 10.1109/ICAECA52838.2021.9675491.

[9] S. S. Saheb, P. B. N. Kiran, B. U. Bhaskara Ganesh, N. Roopalatha, S. M. Syed and P. William, "Artificial Neural Networks Based Risk Management Analysis of Modern Commercial Banks Using Behavioral Finance Theory," 2023 4th International Conference on Computation, Automation and Knowledge Management (ICCAKM), Dubai, United Arab Emirates, 2023, pp. 1-6, doi: 10.1109/ICCAKM58659.2023.10449627.

[10] P. William, A. Agrawal, N. Rawat, A. Shrivastava, A. P. Srivastava and Ashish, "Enterprise Human Resource Management Model By Artificial Intelligence Digital Technology," 2023 4th International Conference on Computation, Automation and Knowledge Management (ICCAKM), Dubai, United Arab Emirates, 2023, pp. 01-06, doi: 10.1109/ICCAKM58659.2023.10449624.

[11] P. William, A. Panicker, A. Falah, A. Hussain, A. Shrivastava and A. K. Khan, "The Emergence of Artificial Intelligence and Machine Learning in Contemporary Business Management," 2023 4th International Conference on Computation, Automation and Knowledge Management (ICCAKM), Dubai, United Arab Emirates, 2023, pp. 1-6, doi: 10.1109/ICCAKM58659.2023.10449493.

[12] P. William, G. Sharma, K. Kapil, P. Srivastava, A. Shrivastava and R. Kumar, "Automation Techniques Using AI Based Cloud Computing and Blockchain for Business Management," 2023 4th International Conference on Computation, Automation and Knowledge Management (ICCAKM), Dubai, United Arab Emirates, 2023, pp. 1-6, doi: 10.1109/ICCAKM58659.2023.10449534.

[13] . A. T. El-Toukhy, M. M. Badr, M. M. E. A. Mahmoud, G. Srivastava, M. M. Fouda and M. Alsabaan, "Electricity Theft Detection Using Deep Reinforcement Learning in Smart Power Grids," in IEEE Access, vol. 11, pp. 59558-59574, 2023, doi: 10.1109/ACCESS.2023.3284681.

[14] V. Bugade, O. Shinde, P. Potdar and A. Patil, "IoT Based Theft Detection in Three Phase Distribution Line," 2022 IEEE Pune Section International Conference (PuneCon), Pune, India, 2022, pp. 1-4, doi: 10.1109/PuneCon55413.2022.10014758.

[15] M. Uvais, "Controller Based Power Theft Location Detection System," 2020 International Conference on Electrical and Electronics Engineering (ICE3), Gorakhpur, India, 2020, pp. 111-114, doi: 10.1109/ICE348803.2020.9122940.

[16] S. S. Yeole, S. Vasant Kolhe, R. R. Bibave, V. Shivaji Chavan, B. B. Kadam and V. Sakharam Bodhe, "Design of Two - Wheeler Hybrid Electric Vehicle using Series Parallel Configuration," 2023 Third International Conference on Artificial Intelligence and Smart Energy (ICAIS), Coimbatore, India, 2023, pp. 1595-1598, doi: 10.1109/ICAIS56108.2023.10073870.

[17] V. S. Pund, S. K. Dongare, P. S. Amate, D. R. Jadhav, R. R. Bibave and D. B. Pardeshi, "Soldier Health Monitoring and Position Tracking (E-Vest)," 2023 4th International Conference on Electronics and Sustainable Communication Systems (ICESC), Coimbatore, India, 2023, pp. 257-261, doi: 10.1109/ICESC57686.2023.10193616.

[18] A. S. Warule, V. R. Barde, M. K. Barshile, S. V. Kambhire, R. R. Bibave and D. B. Pardeshi, "Electric Reaping and Fertilizing Machine," 2023 5th International Conference on Inventive Research in Computing Applications (ICIRCA), Coimbatore, India, 2023, pp. 1685-1691, doi: 10.1109/ICIRCA57980.2023.10220941.

[19] R. Bibave, P. Thokal, R. Hajare, A. Deulkar, P. William and A. T. Chandan, "A Comparative Analysis of Single Phase to Three Phase Power Converter for Input Current THD Reduction," 2022 International Conference on Electronics and Renewable Systems (ICEARS), Tuticorin, India, 2022, pp. 325-330, doi: 10.1109/ICEARS53579.2022.9752161.

[20] N. Prabhakaran, S. K. S, B. S. Reddy, D. Deepthi, D. J. Alicia and P. M. Balasubramaniam, "A Survey on Detection of Power theft in Transmission and Distribution," 2022 International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, India, 2022, pp. 1-3, doi: 10.1109/ICCCI54379.2022.9740976.

[21] J. Wang and X. Zhang, "Electricity Theft Detection Based on SMOTE Oversampling and Logistic Regression Classifier," 2023 IEEE 6th International Electrical and Energy Conference (CIEEC), Hefei, China, 2023, pp. 2571-2576, doi: 10.1109/CIEEC58067.2023.10165777.

[22] H. Huang, S. Liu and K. Davis, "Energy Theft Detection Via Artificial Neural Networks," 2018 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe), Sarajevo, Bosnia and Herzegovina, 2018, pp. 1-6, doi: 10.1109/ISGTEurope.2018.8571877.