Journal Homepage: - www.journalijar.com

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH (IJAR)

Article DOI: 10.21474/IJAR01/23326
DOI URL: http://dx.doi.org/10.21474/IJAR01/23326

ISSN (O): 2320-5407
ISSN (P): 3107-4928

CONFERENCE PAPER

PREDICTIVE ANALYTICS FOR ELECTRICITY THEFT DETECTION USING MACHINE LEARNING

Sibasish Panda[1], Anjan Kumar Sahoo[2], Debarpita Roul [2], Ranjan Kishore Mohanty[2], Jagatjyoti Ranjan Das[2] and Gopal Krishna Mohanty[2]

1. Associate Professor Electrical Engineering Department, College of Engineering Bhubaneswar, Odisha, India.
2. Assistant Professor, Electrical Engineering Department, College of Engineering Bhubaneswar, Odisha, India.

Manuscript Info

Manuscript History
Received: 10 February 2026
Final Accepted: 12 March 2026
Published: April 2026

Key words:-
Energy Meter, Convolutional Neural Network, Advanced Meter Infrastructure, System Operators, Smart Grid

Abstract

In recent years, efficient energy utilization has become critically important, particularly in the context of electricity consumption. One of the major contributors to non-technical losses (NTLs) in power distribution networks is electricity theft, which poses significant challenges to power grids by degrading supply quality and reducing operational revenue. With the deployment of Advanced Metering Infrastructure (AMI), smart meters (SMs) are installed at the consumer end to transmit fine-grained energy consumption data at regular intervals for purposes such as load monitoring, energy management, and billing.However, malicious consumers may launch cyber-attacks by manipulating or falsifying meter readings to reduce their electricity bills unlawfully. Such activities not only result in financial losses but also adversely affect grid performance, as these readings are used for critical grid management decisions. To detect such fraudulent behavior, existing approaches often employ machine learning models based on detailed consumption data. Nevertheless, these methods raise significant privacy concerns, as they may inadvertently reveal sensitive information about consumers' lifestyles.In this paper, we propose an efficient and privacy-preserving scheme for electricity theft detection, billing, and load monitoring. The proposed approach utilizes symmetric encryption to secure consumer data, ensuring privacy, while employing the K-means clustering algorithm to identify anomalous consumption patterns indicative of electricity theft.

Introduction:-

An energy meter, also known as a kilowatt-hour (kWh) meter, is a device used to measure the amount of electrical energy consumed by residential, commercial, or industrial users.

Corresponding Author:- Sibasish Panda
Address:- Associate Professor Electrical Engineering Department, College of Engineering Bhubaneswar, Odisha, India.

Typically calibrated in billing units, these meters are read periodically during each billing cycle. Power loss in transmission and distribution systems is a significant challenge faced by electricity utilities worldwide. These losses are broadly classified into technical losses (TLs) and non-technical losses (NTLs). Technical losses are inherent to the power system and occur due to physical processes in components such as transmission lines and transformers. In contrast, non-technical losses represent the difference between total losses and technical losses, and are primarily caused by electricity theft and other irregularities. Electricity theft commonly occurs through physical tampering methods such as illegal line tapping, meter manipulation, or bypassing metering devices. These fraudulent activities result in substantial financial losses for utility companies. With the deployment of Advanced Metering Infrastructure (AMI) in smart grids, utilities can now collect large volumes of fine-grained energy consumption data at frequent intervals from smart meters installed at consumer premises. AMI enables bidirectional communication between energy meters and the system operator (SO), facilitating real-time load monitoring, energy management, and automated billing. However, in smart grid environments, fraudulent consumers may manipulate their smart meters to report lower energy consumption, thereby reducing their electricity bills illegally. Such deceptive practices not only cause economic losses but also compromise grid operations, as inaccurate data can mislead load forecasting and decision-making processes. In severe cases, this may lead to grid instability or even blackouts. In this paper, we address the challenge of designing a system that enables efficient load monitoring, accurate billing, and effective detection of fraudulent consumers, while simultaneously preserving user privacy.

Literatu Rereview:-

Energy theft remains a critical issue in modern power systems, leading to substantial economic losses and reduced grid reliability. With the evolution of the Smart Grid as a next-generation power system, significant advancements have been made to enhance efficiency, sustainability, and security. Key components such as smart meters and Advanced Metering Infrastructure (AMI) enable system operators to collect real-time electricity consumption data and facilitate efficient energy management. However, these advancements also introduce new vulnerabilities, particularly in the form of cyber-attacks that make electricity theft easier and more sophisticated.Several research efforts have been directed toward detecting electricity theft using advanced computational techniques. A centralized energy theft detection algorithm based on the Kalman filter, referred to as SEK, has been proposed to efficiently identify fraudulent users. While effective in detection, this approach lacks privacy preservation, as it requires access to detailed user consumption data [1]. To address this limitation, a privacy-preserving variant known as PPBE was developed, which decomposes the Kalman filter into parallel components to detect anomalies without directly exposing user data.Another approach focuses on consumption pattern-based detection by leveraging the predictability of normal and malicious usage behaviors. By utilizing distribution transformer data, regions with a high likelihood of electricity theft can be identified, and abnormal consumption patterns can be detected using classification and clustering techniques. This method enhances robustness against non-malicious consumption variations and achieves high detection accuracy with low sampling rates, while also preserving consumer privacy [2]

Privacy concerns have been further addressed through schemes such as PPETD, which employ techniques like secret sharing and secure multi-party computation. In this framework, consumers transmit masked energy readings that can be aggregated for billing and load monitoring without revealing individual consumption patterns. Additionally, machine learning models, including convolutional neural networks (CNNs), are evaluated on encrypted or masked data to detect fraudulent activities while maintaining data confidentiality [3].Other studies have explored the use of deep learning techniques for improved detection performance. For instance, recurrent neural network (RNN)-based models, particularly those utilizing gated recurrent units (GRUs), exploit the temporal characteristics of electricity consumption data to identify anomalies more effectively [4]. These models demonstrate superior performance compared to traditional machine learning approaches, especially when optimized through hyperparameter tuning techniques such as random search [5].Furthermore, some architectures propose a dual-entity framework where one trusted entity performs decryption and fraud detection using machine learning models, while another untrusted entity aggregates encrypted data for load monitoring. Although such methods aim to balance privacy and functionality, they rely heavily on trust assumptions and may not fully support dynamic billing mechanisms [6].In addition, widely used machine learning libraries such as Scikit-learn provide a comprehensive set of tools for implementing both supervised and unsupervised learning algorithms, facilitating the development and evaluation of electricity theft detection models in both academic and industrial contexts [7].Despite these advancements, existing methods often face trade-offs between detection accuracy, computational efficiency, and user privacy. Therefore, there remains a need for robust, efficient, and privacy-preserving solutions for electricity theft detection in smart grid environments.

Proposed Work:-
In this work, a secure and intelligent framework is proposed for electricity theft detection and energy management. The system employs symmetric encryption to ensure secure transmission and storage of consumer energy data, thereby preserving user privacy. For theft detection, a K-means clustering algorithm is utilized to identify abnormal consumption patterns indicative of fraudulent activities.

The proposed system is capable of performing real-time load monitoring and dynamic electricity billing. It operates in multiple stages, integrating both consumer-side and utility-side (EB section) data. The implementation is carried out using the Django **framework**, with the NumPy **library** for efficient numerical computations in Python. All collected data from different sections are stored in a MySQL database for further analysis and future reference.

The preprocessing stage of the proposed framework includes verification of discrepancies to determine whether mismatches occur during power transmission or due to potential theft. Furthermore, a Convolutional Neural **Network (CNN)** is incorporated to automatically learn and extract temporal features from large-scale smart meter data. By analyzing variations across different hours of the day and across multiple days using convolution and down-sampling operations, the model enhances the accuracy and robustness of electricity theft detection.

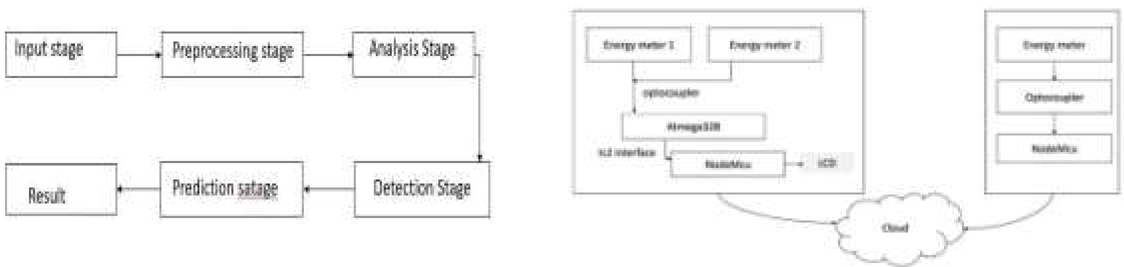

Fig. 1. Proposed process and System Architecture

We have mainly two section, one is consumer section and other is power station section. In consumer section we have two energy meter, optocoupler, Atmega328, ic2 interface, Node mcu, and LCD. Our proposed system can be placed either in existing energy meter or can be placed separately.An energy meter is a device that measures the amount of electric energy consumed by an electrically powered device. energy meter measures the total power consumed over a time interval and generates the pulse. Optocoupler is used to decode the pulse and feed into the Atmega328 Microcontroller, which is used to calculate how many units is consumed, then it will passed to Node Mcu. By using Internet, the information is stored in cloud.In the Admin section we have Energy meter, Optocoupler and Node Mcu. Here we use the same operation performed in Consumer section. The total unit of energy supply is stored in cloud.

Result:-
If there any mismatch in supplied and consumed units in the cloud storage, which indicate the theft. When the theft is identified it will inform the EB office by sending an alert message immediately by getting alert message the EB office will assist the inspecting team to identify where the theft is occurred. The inspecting team will use consumers bill history for the past one year, it may help the team to identify the fraudulent consumer. It can be done using machine learning algorithm along with iOT devices.

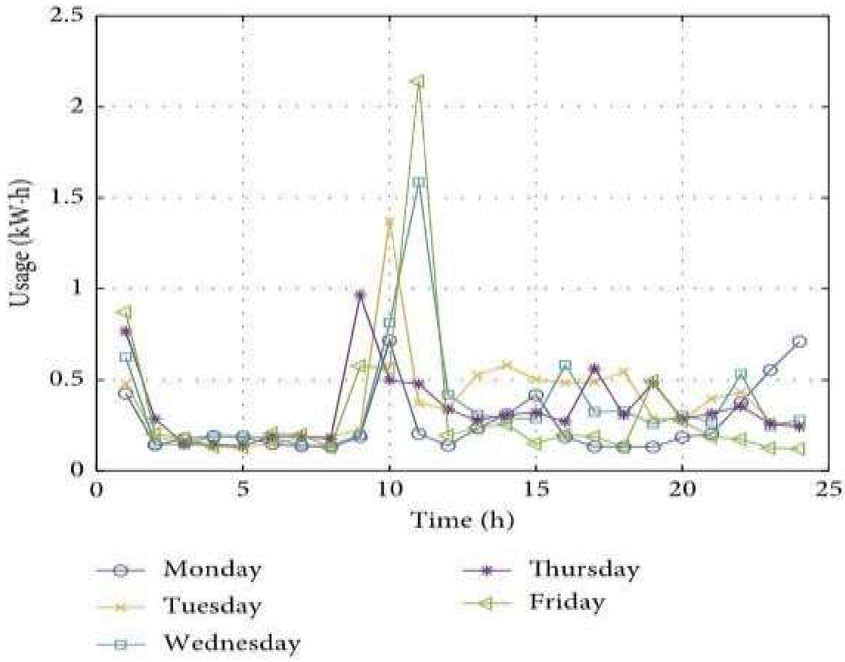

Fig. 2 Electricity usage with respect to time.

Conclusion:-

In this paper, we propose a novel and efficient scheme that utilizes encrypted fine-grained electricity consumption data reported by energy meters (EMs) for electricity theft detection, load monitoring, and dynamic billing. The proposed framework ensures consumer privacy by preventing any entity from accessing or inferring individual consumption patterns. To achieve this, each consumer employs symmetric encryption to secure their energy usage data before transmission.At the system operator (SO) side, a symmetric decryption key is used to process the aggregated data for computing electricity bills, monitoring overall load demand, and evaluating a machine learning model for detecting electricity theft. The integration of encryption with data analytics enables secure and reliable system operation without compromising user privacy.Furthermore, extensive simulations have been conducted using real-world datasets to evaluate the performance of the proposed scheme. The results demonstrate that the system can accurately identify fraudulent consumers while preserving data confidentiality, with acceptable communication and computational overhead.

References :-[1] D. Yao, M. Wen, X. Liang, Z. Fu, K. Zhang, and B. Yang, “Energy theft detection with energy privacy preservation in the smart grid,” IEEE Internet of Things Journal, vol. 6, no. 5, pp. 7659–7669, Oct. 2019

[2] 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, no. 1, pp. 216–226, Jan. 2016

[3] M. Nabil, M. Ismail, M. M. E. A. Mahmoud, W. Alasmary, and E. Ser pedin, “PPETD: privacy preserving electricity theft detection scheme with load monitoring and billing for AMI networks,” IEEE Access, vol. 7, pp. 96334–96348, Jun. 2019

[4] F. Pedregosa et al., “Scikit-learn: Machine learning in Python,” Journal of Machine Learning Research, vol. 12, pp. 2825–2830, Oct. 2011

[5] S. Salinas and P. Li, “Privacy-preserving energy theft detection in microgrids: A state estimation approach,” IEEE Transactions on Power Systems, vol. 31, no. 2, pp. 883–894, Mar. 2016

[6] D. Yao, M. Wen, X. Liang, Z. Fu, K. Zhang, and B. Yang, “Energy theft detection with energy privacy preservation in the smart grid,” IEEE Internet of Things Journal, vol. 6, no. 5, pp. 7659–7669, Oct. 2019

[7] M. Nabil, M. Ismail, M. Mahmoud, M. Shahin, K. Qaraqe, and E. Ser pedin, “Deep recurrent electricity theft detection in AMI networks with random tuning of hyper-parameters,” in 24th International Conference on Pattern Recognition (ICPR), pp. 740–745, Aug. 2018

[8] S. Salinas, M. Li, and P. Li, “Privacy-preserving energy theft detection in smart grids: A P2P computing approach,” IEEE Journal on Selected Areas in Communications, vol. 31, no. 9, pp. 257–267, Sep. 2013

[9] V. C. Gungor, D. Sahin, T. Kocak, S. Ergut, C. Buccella, C. Cecati, and G. P. Hancke, "A survey on smart grid potential applications and communication requirements," IEEE Transactions on Industrial Informatics, vol. 9, no. 1, pp. 28–42, Feb. 2013

References:-

[1] A. L. Hanees and M. M. M. Mufassirin, "Development of IoT Based Smart Energy Meter Reading and Monitoring System", 7th International Symposium 2017 (IntSym 2017) - SEUSL, 2018.
[2] F. Abate, M. Carratù, C. Liguori, M. Ferro, V. Paciello, "Smart Meter for the IoT", Proc. of the IEEE Instrumentation and Measurement Technology Conference, I2MTC 2018, Houston, TX, USA, May 2018.
[3] Chang W. F., Wu Y. C., Chiu C. W., "Development Of A Web-Based Remote Load Supervision And Control System", Int. J. Electr. Power Energy Syst, 2006, Vol. 28, pp. 401–407.
[4] Praveenkumar H. S., Rakesh B. S. and Preetha P. S., "GSM Based Automatic Energy Meter Reading With Load Control", International Journal of Science, Engineering and Technology Research (IJSETR), 2015, Vol. 4, Issue 5, pp. 1428–1432.
[5] S. Elakshumi and A. Ponraj, "A server based load analysis of smart meter systems," 2017 International Conference on Nextgen Electronic Technologies: Silicon to Software (ICNETS2), 2017, pp. 141–144, doi: 10.1109/ICNETS2.2017.8067916.
[6] G. Dudek, A. Gawlak, M. Kornatka and J. Szkutnik, "Analysis of Smart Meter Data for Electricity Consumers," 2018 15th International Conference on the European Energy Market (EEM), 2018, pp. 1–5, doi: 10.1109/EEM.2018.8469896.
[7] Young-sung Son, Topi Pulkkinen, Kyeong-deok Moon and Chaekyu Kim, "Home Energy Management System Based On Power Line Communication", IEEE Transactions on Consumer Electronics, 2010, Vol. 56, Issue 3, pp. 1380–1386.