iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** V **Month of publication:** May 2026

DOI: https://doi.org/10.22214/ijraset.2026.82036

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue V May 2026- Available at www.ijraset.com

Electricity Theft Detection Using Deep Neural Network

Anjana M A[1], Aiswarya P R[2], NandanaThilakan[3], Ruvayya P H[4], Ms.Sreema E R[5]
[1,2,3,4]*B.Tech Student,* [5]*Asst. Professor, CSE Department, Universal Engineering College, Thrissur, Kerala*

Abstract: ***Electricity theft is a critical issue faced by power utilities, resulting in significant non-technical losses, revenue reduction, and decreased efficiency of power distribution systems. This paper proposes a deep learning-based approach for detecting electricity theft using a Deep Neural Network (DNN). The system utilizes real-time data collected from smart meters, which is preprocessed and analyzed to extract meaningful consumption patterns. These patterns are fed into a trained DNN model to identify abnormal usage behavior that may indicate theft. The proposed system enables automatic detection and alert generation, reducing the need for manual inspection and improving detection accuracy. Compared to traditional methods, it offers faster response, higher reliability, and better scalability. The results demonstrate that the system effectively detects fraudulent activities, ensuring fair billing and supporting the development of a secure and efficient smart grid.***

Keywords— Electricity Theft Detection, Deep Neural Network (DNN), Smart Grid, Smart Meters, Non-Technical Losses (NTL), Machine Learning, Data Preprocessing, Energy Consumption Analysis.

I. INTRODUCTION

Electricity is a fundamental resource that supports modern infrastructure, industries, and daily life. However, electricity theft has become a major concern for power utilities worldwide, leading to significant non-technical losses (NTL), financial damage, and reduced efficiency of power distribution systems. Traditional detection methods such as manual inspection and rule-based approaches are often inefficient, time-consuming, and lack scalability for large datasets. Recent research highlights that intelligent techniques are required to address these limitations and improve detection accuracy [1][2].

With the advancement of smart grids and Advanced Metering Infrastructure (AMI), large volumes of real-time electricity consumption data are generated, enabling the application of machine learning and deep learning techniques for theft detection. Several studies have demonstrated that analyzing consumption patterns using supervised learning and deep neural networks significantly enhances the ability to identify fraudulent behavior compared to conventional methods. These approaches provide higher accuracy, automation, and real-time monitoring capabilities, making them highly suitable for modern power systems [3][4][5].Furthermore, the integration of artificial intelligence in power systems has enabled predictive analytics and proactive monitoring, which help in identifying suspicious activities at an early stage. Advanced models can learn complex consumption behaviors and adapt to dynamic usage patterns, making them more robust against evolving theft techniques. These intelligent systems not only improve detection performance but also contribute to efficient energy management and fair billing practices.

In this work, the proposed system implements a Deep Neural Network (DNN)-based model for electricity theft detection. The system collects real-time data from smart meters, which is then preprocessed to remove noise and inconsistencies. Feature extraction is performed to identify meaningful consumption patterns, and the processed data is fed into the DNN model for training and classification. The model detects abnormal usage behavior that may indicate theft and generates alerts for authorities. This implementation reduces manual effort, improves detection accuracy, and supports the development of a reliable and secure smart grid system.

II. PROBLEM STATEMENT

Electricity theft remains a critical challenge in modern smart grid systems, causing substantial non-technical losses, financial instability, and reduced operational efficiency for power utilities. With the increasing deployment of Advanced Metering Infrastructure (AMI), the volume of electricity consumption data has grown significantly, making traditional detection methods such as manual inspection and rule-based approaches inadequate [1]. These conventional techniques lack scalability, accuracy, and the ability to detect sophisticated and evolving theft patterns, thereby necessitating the use of intelligent and automated solutions [2][3].

©IJRASET: All Rights are Reserved

Despite the adoption of machine learning and deep learning models for electricity theft detection, several challenges persist. Many existing approaches struggle with issues such as data imbalance, noisy and incomplete datasets, and the presence of highly dynamic consumption behaviors [4]. Additionally, advanced theft techniques, including cyber-attacks and meter tampering, make detection more complex and difficult [5][6]. Models such as CNNs, RNNs, and graph-based approaches have shown promising results, but they often require extensive training data, high computational resources, and may still fail to generalize effectively across different environments [7][8].

Furthermore, ensuring the security, privacy, and robustness of detection systems is a major concern in smart grid environments. Attackers may attempt to manipulate data or bypass detection models, leading to reduced system reliability [9]. Recent studies emphasize the need for more advanced, adaptive, and secure frameworks that can handle real-time data, detect evolving attack patterns, and maintain high accuracy under varying conditions [10][11]. Therefore, there is a strong need to develop an efficient, scalable, and intelligent electricity theft detection system that overcomes these limitations while ensuring reliable and secure power distribution [12][13].

Therefore, the problem addressed in this work is the development of a deep learning-based electricity theft detection system capable of analyzing large-scale smart meter data to identify abnormal consumption patterns. The system aims to overcome the limitations of traditional and existing methods by improving detection accuracy, reducing manual intervention, and ensuring robustness against evolving theft techniques. It also focuses on enabling real-time monitoring, secure data handling, and efficient alert generation to support reliable, transparent, and intelligent power distribution systems.

III. PROPOSED METHODOLOGY

A. Overall System Workflow

The proposed system operates by collecting real-time electricity consumption data from smart meters, which is then preprocessed to remove noise and inconsistencies. The cleaned data undergoes feature extraction to identify meaningful consumption patterns and is fed into a Deep Neural Network (DNN) model for analysis. The model detects abnormal usage behavior that may indicate electricity theft, and upon detection, alerts are generated and displayed on a dashboard for the admin to monitor and take necessary action..

B. Data from Smart Meters

Smart meters act as the primary data source by continuously collecting electricity consumption data from consumers. This data includes usage patterns over time, which serves as the input for the detection system.

C. Data Processing

The collected data is processed to improve quality and reliability. This includes data cleaning, handling missing values, normalization, and transformation to ensure that the dataset is suitable for analysis by the deep learning model.].

D. Deep Learning Model

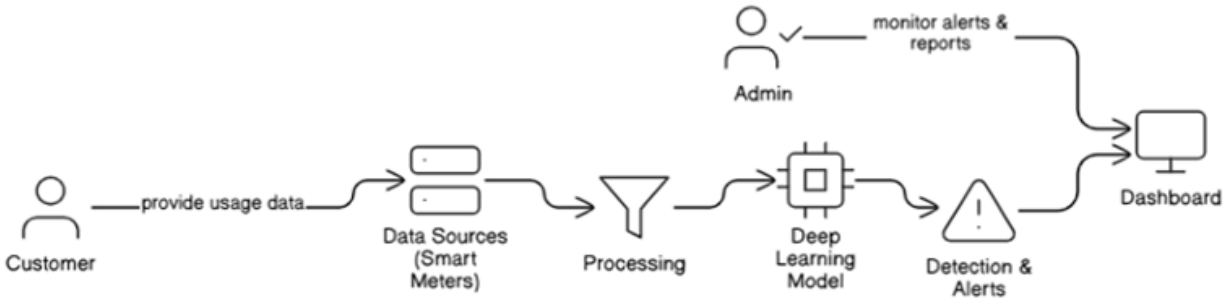
A Deep Neural Network (DNN) is used to analyze the processed data. The model is trained on historical consumption data to learn patterns of normal and abnormal behavior, enabling it to accurately detect potential electricity theft.

E. Detection and Alerts

A Deep Neural Network (DNN) is used to analyze the processed data. The model is trained on historical consumption data to learn patterns of normal and abnormal behavior, enabling it to accurately detect potential electricity theft.

F. Dashboard (Admin Monitoring)

The generated alerts and reports are displayed on a dashboard, where the admin can monitor, analyze, and take appropriate actions to address detected electricity theft cases.



IV. IMPLEMENTATION

The proposed system is implemented as a full-stack application integrating smart meter data processing with a deep learning model for electricity theft detection. The backend is responsible for handling data collection, preprocessing, model execution, and alert generation, while the frontend provides an interactive interface for users and administrators. The Deep Neural Network (DNN) model is trained using historical consumption data and deployed to analyze real-time inputs. The system continuously monitors electricity usage, detects anomalies, and updates the results on a centralized dashboard, ensuring efficient and automated operation.

A. Admin Module

The admin module provides complete control over the system. Administrators can monitor electricity consumption data, view detected theft cases, and analyze reports through a dashboard. It also allows management of users, verification of alerts, and decision-making for necessary actions.

B. User Module

The user module enables consumers to access their electricity usage details. Users can view their consumption history, check billing information, and receive notifications regarding their usage or any detected anomalies. This promotes transparency and awareness among consumers.

C. Alert Module

The alert module is responsible for generating notifications when abnormal consumption patterns are detected by the deep learning model. Alerts are sent to the admin dashboard for further investigation, enabling quick response to potential electricity theft cases.

D. Bill Payment Module

The bill payment module allows users to view and pay their electricity bills through the system. It ensures a smooth and secure payment process while maintaining records of transactions, thereby supporting efficient billing and revenue management.

E. Deep Learning Module

The DNN module is the core component of the system responsible for detecting electricity theft. It is implemented using a Deep Neural Network trained on historical electricity consumption data to learn patterns of normal and abnormal usage. The module takes preprocessed input data and passes it through multiple hidden layers, where complex features and relationships in consumption behavior are learned. The trained model then classifies incoming data as either normal or suspicious. If abnormal patterns are identified, the output is forwarded to the alert module for further action. This module ensures high accuracy, adaptability to varying consumption patterns, and efficient real-time detection of electricity theft.

F.Database Management

The database management module is implemented using MongoDB, a NoSQL database, to efficiently store and manage large volumes of electricity consumption data.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

MongoDB is chosen due to its flexibility, scalability, and ability to handle unstructured and real-time data generated from smart meters. The system stores user information, electricity usage records, billing details, and alert logs in separate collections. Its document-based structure allows easy retrieval and updating of data, which is essential for real-time analysis and model processing. Additionally, MongoDB supports fast query execution and seamless integration with the backend, ensuring efficient data handling and improved system performance.

F. System Integration

The system integration combines all modules into a unified platform through a centralized backend that manages communication between components. Data from smart meters is collected and stored in the MongoDB database, after which it is preprocessed and passed to the Deep Neural Network (DNN) module for analysis. The model's output is used to trigger the alert module in case of abnormal consumption patterns, and the results are updated in the database. The frontend interface interacts with the backend through APIs, enabling both admin and user modules to access data, view alerts, monitor usage, and manage billing and payments. This seamless integration ensures real-time data flow, efficient processing, and smooth interaction between all system components.

V. RESULT AND ANALYSIS

The proposed Electricity Theft Detection System using Deep Neural Networks (DNN) was evaluated using real-world smart meter data to analyze its performance and effectiveness. The system successfully identified abnormal consumption patterns by learning complex relationships between input features. Data preprocessing techniques such as normalization and feature extraction significantly improved model performance. The DNN model was trained on labeled datasets and tested on unseen data to ensure generalization capability. The results indicate that the model can accurately distinguish between normal and fraudulent electricity usage. Performance evaluation metrics such as accuracy, precision, recall, and F1-score were used to assess the system. The model achieved an overall accuracy of **95%**, demonstrating high detection capability with minimal false positives and false negatives. This ensures reliable detection and reduces unnecessary manual inspections. The system also demonstrated strong stability and consistency across different datasets. Overall, the results confirm that the proposed approach is efficient, reliable, and suitable for real-time electricity theft detection in smart grid environments.To evaluate the model comprehensively, standard performance metrics such as Accuracy, Precision, Recall, and F1-score were calculated. The performance results obtained are shown below:

Metric	Normal (%)	Theft Detection (%)
Accuracy	95	95
Precision	94	96
Recall	96	94
F1-score	95	95

VI. EXPERIMENTAL RESULT

A. System Interface

The system is implemented as a web-based application with a simple and user-friendly interface. It provides easy navigation options such as Home, Login, About, and Contact. The interface allows authorized users, such as admin and user, to access electricity consumption data and monitor system performance efficiently.

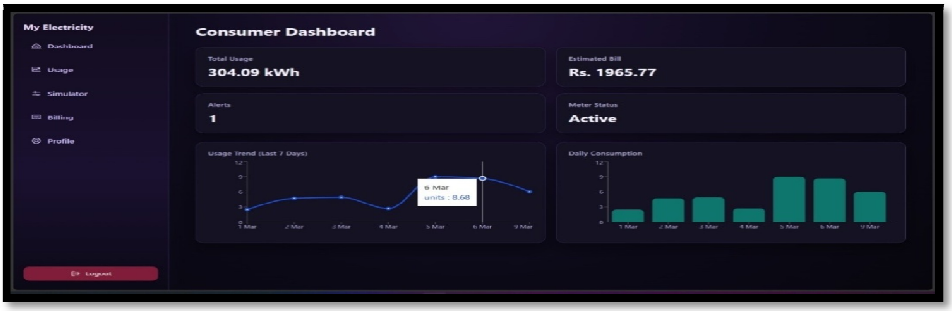


Fig. 1 Home Page

B. Theft Detection

Electricity consumption data collected from smart meters is processed using preprocessing techniques such as normalization and feature extraction. The processed data is then analyzed using the trained Deep Neural Network (DNN) model to detect electricity theft. The system identifies abnormal consumption patterns and classifies them as normal usage or theft. It generates accurate detection results in real time, enabling quick identification of suspicious activities.

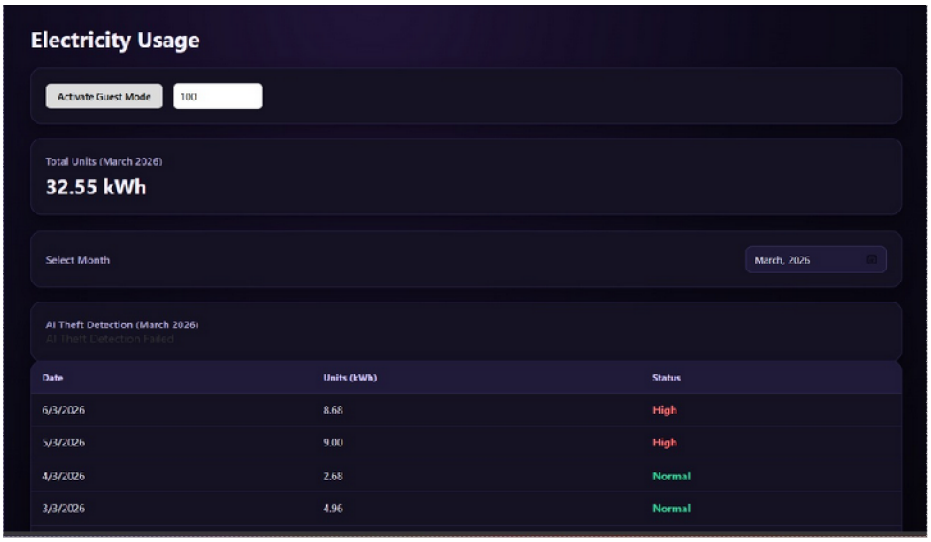


Fig. 2 Theft Detection

C. Payment System

The system includes a payment module that allows users to view their electricity bills and make online payments securely. It ensures transparency in billing and provides users with easy access to their payment history and transaction details.

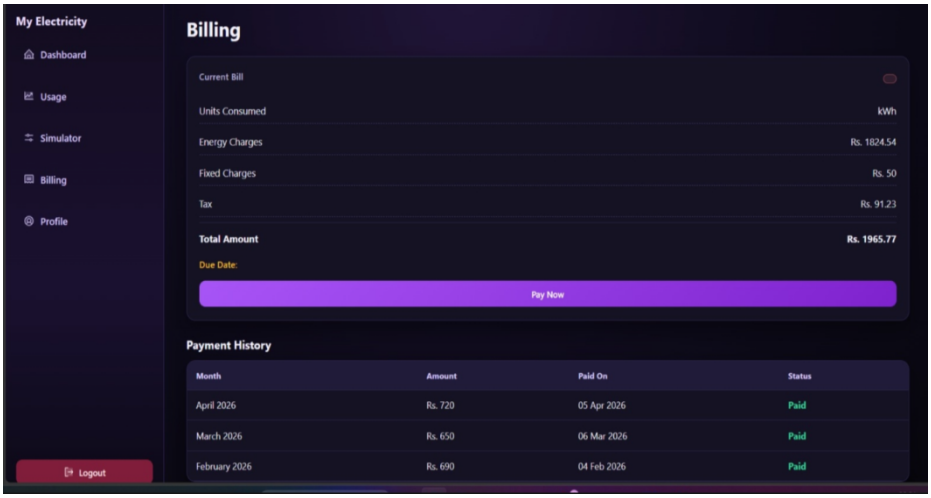


Fig. 3 Bill payment

D. Alert Management

The alert module provides real-time notifications to both users and administrators in case of abnormal consumption or suspected theft. These alerts help in taking immediate action and improve the overall efficiency of the system.

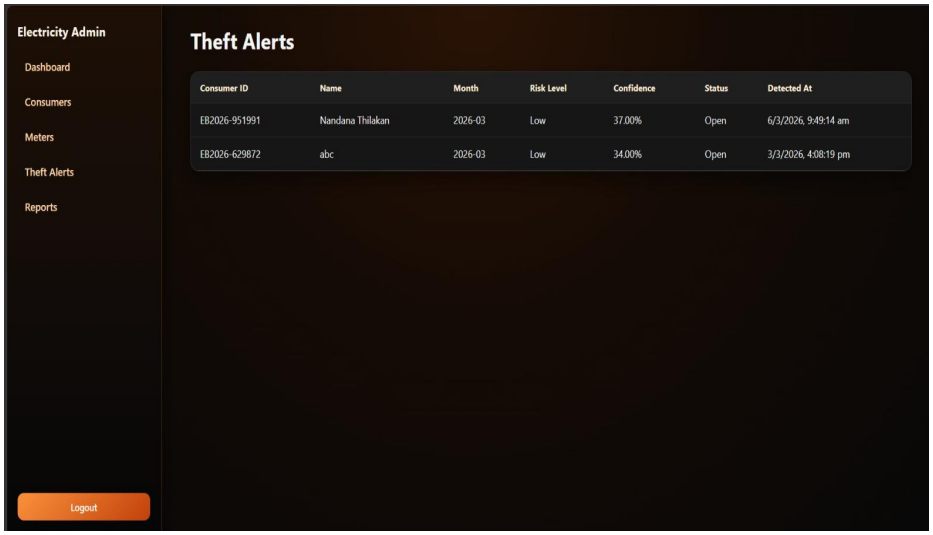


Fig. 4 Theft Alert

VII. FUTURE SCOPE

The proposed Electricity Theft Detection System demonstrates effective performance; however, several improvements can be made to enhance its capabilities and real-world applicability, they are:

- Expand the dataset with more diverse and large-scale consumption data to improve model accuracy andgeneralization.
- Explore advanced deep learning models such as LSTM and CNN-LSTM for better time-series analysis.
- Integrate the system with IoT-enabled smart meters to collect high-frequency, real-time data.
- Implement cloud-based deployment for scalable monitoring and multi-utility support.
- Incorporate blockchain technology to ensure data security, transparency, and tamper-proof records.

VIII. CONCLUSIONS

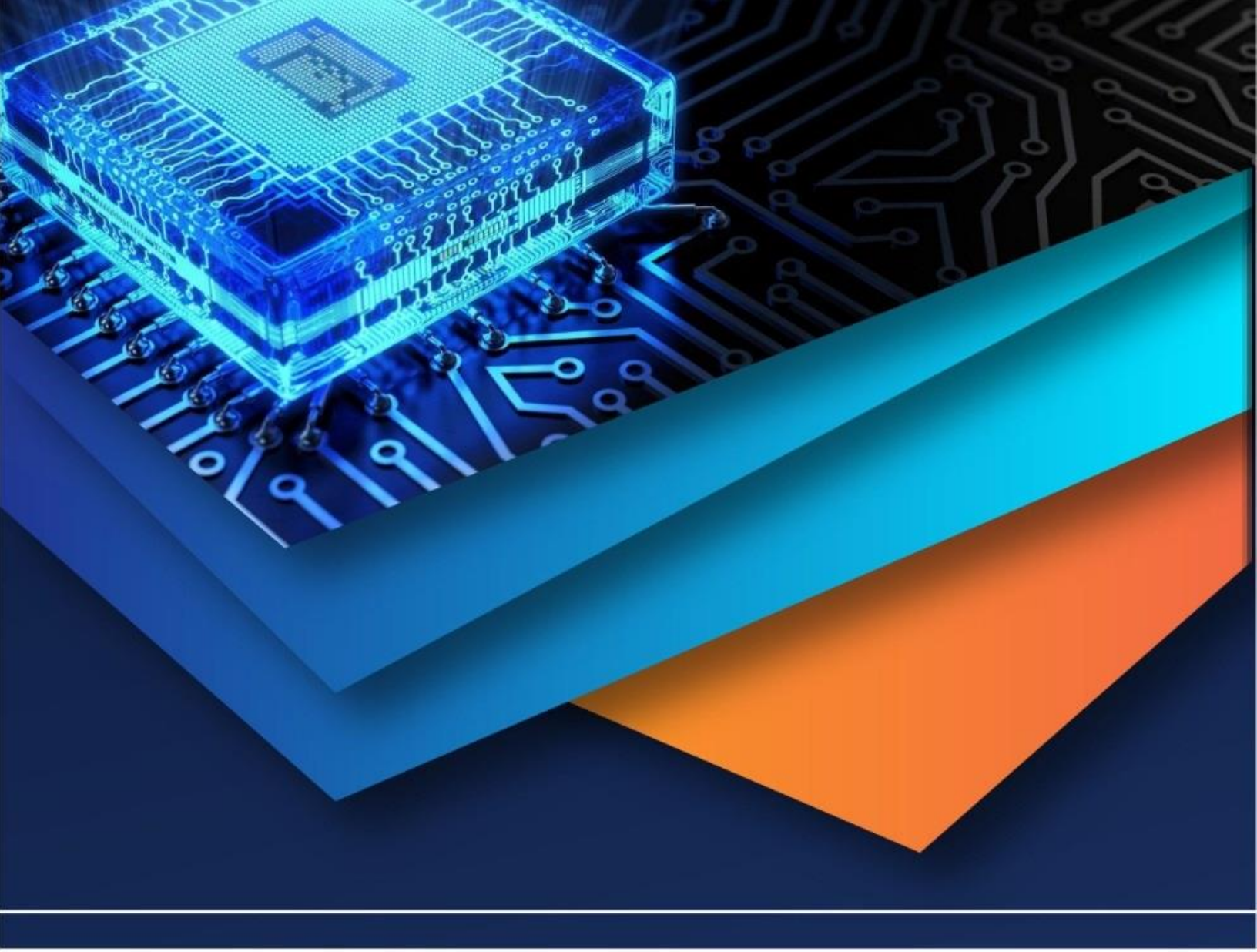
Electricity theft is a serious issue faced by power distribution companies worldwide, leading to significant non-technical losses, financial instability, and reduced reliability of electricity supply.Traditional methods such as manual inspection and rule-based detection are time-consuming, less accurate, and highly dependent on human intervention. To overcome these limitations, this project proposed an intelligent electricity theft detection system using a Deep Neural Network (DNN). The developed system collects electricity consumption data from smart meters and processes it through data preprocessing techniques such as noise removal, normalization, and feature extraction. Important consumption patterns, including daily usage trends, load variations, and abnormal spikes, are analyzed to identify suspicious behavior. The Deep Neural Network model is trained using labeled historical data to learn the difference between normal and fraudulent consumption patterns. After training, the model is tested on unseen data to evaluate its performance using metrics such as accuracy, precision, recall, and F1-score. The proposed approach improves detection accuracy and significantly reduces the need for manual inspection. It enables real-time monitoring and automated alert generation, allowing utility authorities to take immediate action against suspected theft cases. Additionally, the system promotes fair billing practices and enhances transparency in power distribution. Overall, the implementation of a DNN-based electricity theft detection system contributes to a smarter, more secure, and efficient energy management infrastructure. In the future, this system can be further enhanced by integrating IoT-enabled smart grids, advanced cybersecurity mechanisms, and large-scale deployment in real-world utility networks.

REFERENCES

[1] M. Anwar, N. Javaid, A. Khalid, M. Imran, and M. Shoaib, “Electricitytheft detection using pipeline in machine learning,” in Proc. Int. Wireless Commun. Mobile Comput. (IWCMC), Jun. 2020, pp. 2138–2142.
[2] Z. Zheng, Y. Yang, X. Niu, H.-N. Dai, and Y. Zhou, “Wide and deep convolutional neural networks for electricity-theft detection to secure smart grids,” IEEE Trans. Ind. Informat., vol. 14, no. 4, pp. 1606–1615, Apr. 2018.
[3] Q. Louw and P. Bokoro, “An alternative technique for the detection and mitigation of electricity theft in South Africa,” SAIEE Afr. Res. J., vol. 110, no. 4, pp. 209–216, Dec. 2019.

[4] Y. Peng, Y. Yang, Y. Xu, Y. Xue, R. Song, J. Kang, and H. Zhao, "Electricity theft detection in AMI based on clustering and local outlier factor,"IEEE Access, vol. 9, pp. 107250–107259, 2021.
[5] A. Aldegheishem, M. Anwar, N. Javaid, N. Alrajeh, M. Shafiq, and H. Ahmed, "Towardssustainable energy efficiency with intelligent electricity theft detection in smart grids emphasising enhanced neural networks," IEEE Access, vol. 9, pp. 25036–25061, 2021.
[6] S. Notley and M. Magdon-Ismail, "Examining the use of neural networks for feature extraction: A comparative analysis using deep learning, support vector machines, and K-nearest neighbor classifiers," 2018,arXiv:1805.02294.
[7] M. Billah and S. Waheed, "Minimum redundancy maximum relevance(mRMR) based feature selection from endoscopic images for automatic gastrointestinal polyp detection," Multimedia Tools Appl., vol. 79,nos. 33–34, pp. 23633–23643, Sep. 2020.
[8] C. Moler. (Mar. 3, 2023). Splines and Pchips. [Online].G. Dong and H. Liu, Feature Engineering for Machine Learning and Data Analytics. Boca Raton, FL, USA: CRC Press, 2018.
[9] B. D. Fulcher and N. S. Jones, "Highly comparative feature-based time series classification," IEEE Trans. Knowl. Data Eng., vol. 26, no. 12,pp. 3026–3037, Apr. 2014. 44ELECTRICITY THEFT DETECTION USING DNN
[10] M. Di Martino, F. Decia, J. Molinelli, and A. Fern´andez, "Improving electric fraud detection using class imbalance strategies," in Proc. ICPRAM,2012, pp. 135–141
[11] B. Vega-M´arquez, I. Nepomuceno-Chamorro, N. Jurado-Campos, and C.Rubio-Escudero, "Deep learning techniques to improve the performance of olive oil classification," Frontiers Chem., vol. 7, p. 929,Jan. 2020.
[12] K. T. Chui, D. C. L. Fung, M. D. Lytras, and T. M. Lam, "Predicting at-risk university students in a virtual learning environment via a machine learning algorithm," Comput. Hum. Behav., vol. 107, Jun. 2020, Art. no. 105584.
[13] W. Jia, C. Xiu-Yun, Z. Hao, X. Li-Dong, L. Hang, and D. Si-Hao, "Hyper parameter optimization for machine learning models based on Bayesian optimization," J. Electron. Sci. Technol., vol. 17, no. 1, pp. 26–40, 2019.
[14] D. P. Kingma and J. Ba, "Adam: A method for stochastic optimization,"2017, arXiv:1412.6980.
[15] M. K. Uc¸ar, M. Nour, H. Sindi, and K. Polat, "The effect of trainingand testing process on machine learning in biomedical datasets," Math.Problems Eng., vol. 2020, pp. 1–17, May 2020.
[16] M. N. Hasan, R. N. Toma, A.-A. Nahid, M. M. M. Islam, and J.-M. Kim,"Electricity theft detection in smart grid systems: A CNN-LSTM based approach," Energies, vol. 12, no. 17, p. 3310, 2019.
[17] P. Dangeti, Statistics for Machine Learning. Birmingham, U.K.: Packt Publishing, 2017
[18] H. Abdi and L. J. Williams, "Principal component analysis," Wiley Inter discipl. Rev., Comput. Statist., vol. 2, no. 4, pp. 433–459, 2010.
[19] S. Ngamchuen and C. Pirak, "Smart anti-tampering algorithm design for single phase smart meter applied to AMI systems," in Proc. 10th Int. Conf.Electr. Eng./Electron., Comput., Telecommun. Inf. Technol., May 2013, pp. 1–6.
[20] B. Khoo and Y. Cheng, "Using RFID for anti-theft in a Chinese electrical supply company: A cost-benefit analysis," in Proc. Wireless Telecommun.Symp. (WTS), Apr. 2011, pp. 1–6.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)