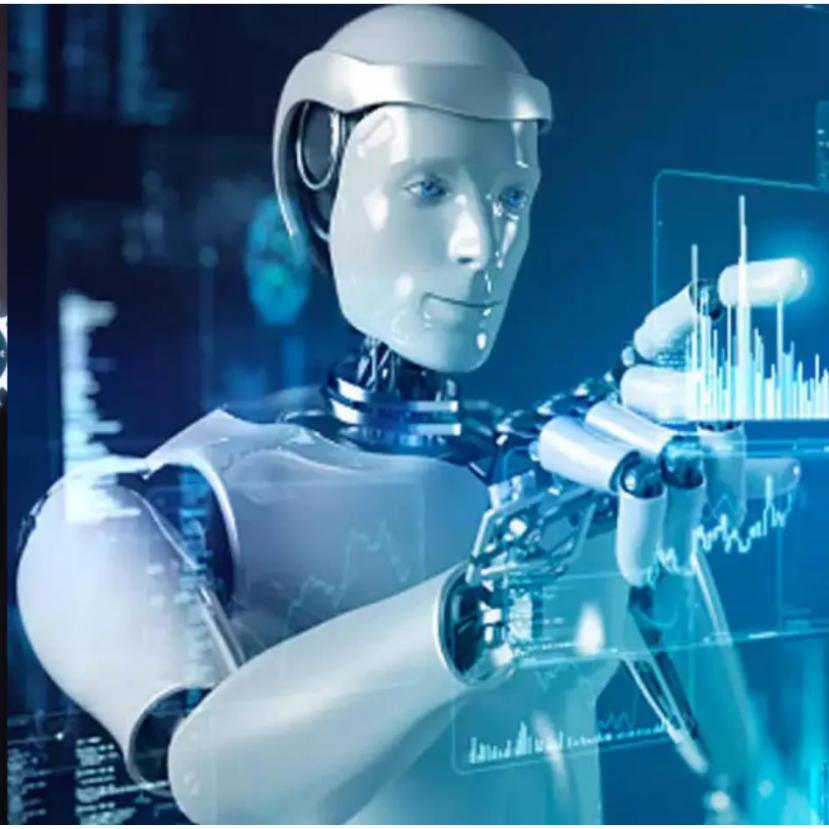
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.699

Volume 14, Issue 8, August 2025

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 8, August 2025

|DOI: 10.15680/IJIRSET.2025.1408042|

Smart Grid Data Analysis and Security using Deep Learning

Vinay Kumar K.R, Astha Tiwari

PG Student, Dept. of MCA, City Engineering College, Bengaluru, Karnataka, India

Assistant Professor, Dept. of MCA, City Engineering College, Bengaluru, Karnataka, India

ABSTRACT: The global epidemic of energy theft is showing a significant impact on both utilities and power customers. It disrupts the economic growth of utility companies, impacts consumers' high energy costs, and generates electric dangers. In order to build smart grids, massive volumes of data are generated, which includes data on consumer usage. This data has the potential to be utilised to identify instances of energy theft through the application using deep learning and machine learning algorithms. This research introduces a novel method for identifying theft that employs a classification strategy uses deep neural networks and takes use of rich data in the frequency and temporal domains. We address dataset problems including missing information and class imbalance using techniques like data interpolation or synthetic data generation. After analysing and evaluating the features' contributions in the frequency and time domains, we employ principal component analysis to conduct experiments in reduced and merged feature spaces, and finally, we use a minimum redundancy maximum relevant technique to validate our most significant features.

KEYWORDS: Smart Grid,Smart ,MeteringEnergy ,Management System,Load Forecastin, Renewable Energy Integration, Demand Response,Distributed Energy Resources, Grid Monitoring, Power Quality Analysis

I. INTRODUCTION

Theft of electrical power is an issue that impacts utility companies all over the globe. Annually, utility companies around the world lose around $96 billion to Non-Technical Losses (NTLs), with energy theft being the main cause [1]. The World Bank says nearly 50% of the energy generated in sub-Saharan Africa is stolen [2]. illegally use electricity without being charged either not pay the utility company for the energy they use or to pay less than the original figure actually used [3, 4]. A large sum of money is thus lost by utility providers due to power theft. The countries of Russia ($5.1 billion), Brazil ($10.5 billion), and India $16.2 billion were the losers in 2015.

Annually, power theft costs South Africa an estimated 1.31 billion dollars (R20 billion) in revenue [2]. Power theft not only lowers income, but it also poses a hazard to the safety and lives of reliability of electricity grids [3]. The potential for power surges, electrical equipment overload, and electric shocks makes it a public safety concern [4]. how well the system works energy tariff increases, which are bad for consumers overall [3]. According to [4], smart grids are a great way to combat the common problem of power theft. A smart grid is a conventional electrical system that also includes smart meters, detectors, and Allows for monitoring and control of operate the grid using computers [6]. Smart meters et sensors can collect data on consumption of electricity, grid status, pricing, and more.

Many utilities sought to decrease power theft in conventional systems by investigating meter architecture and installation, looking for line bypass, and other similar issues [4]. These approaches go beyond being merely costly and ineffective, They go on to miss cyberattacks. [4, 7]. Researchers have now attempted to identify power theft by utilising publicly accessible demographic and socioeconomic indicators machine learning classification algorithms. The reasonable cost of various theft detection systems has been established [8]. The existing classification algorithms have a serious performance bottleneck since they just consider time-domain features.

II. SYSTEM MODEL AND ASSUMPTIONS

System Model

The proposed model integrates smart grid infrastructure, data analytics platforms, and deep learning-based security mechanisms to enable real-time monitoring, predictive analysis, and cyberattack prevention.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 8, August 2025

|DOI: 10.15680/IJIRSET.2025.1408042|

Data Acquisition Layer
Includes smart meters, phasor measurement units (PMUs), sensors, and IoT-enabled devices for collecting real-time data on energy consumption, voltage, frequency, and power quality.

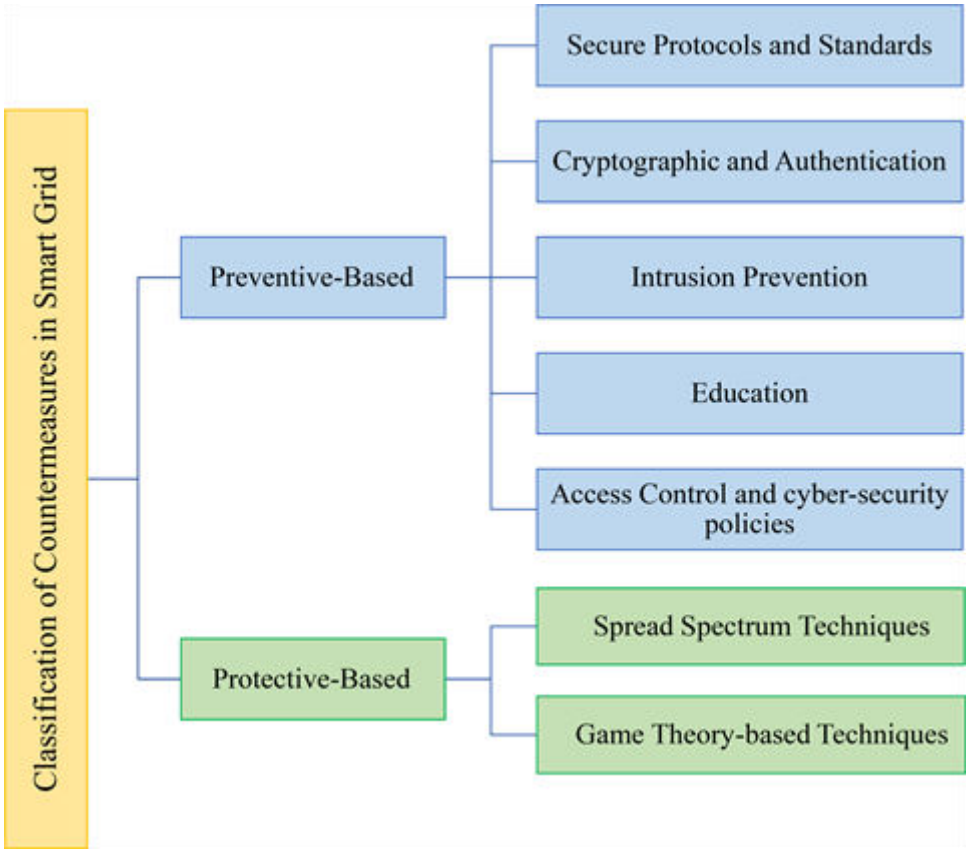
Communication Layer
Uses secure wired and wireless channels (Fiber optics, 5G, Zigbee, LoRaWAN) with encryption protocols (TLS, SSL, IEC 61850) to transmit data between field devices and control centers.

Processing & Analytics Layer
Hosts cloud or edge computing platforms where deep learning models (CNN, LSTM, Autoencoders) are deployed for:

- Load forecasting
- Anomaly detection
- Intrusion detection
- Fault prediction

Control Layer
Interfaces with the grid's supervisory control and data acquisition (SCADA) systems for automated response to operational changes or detected threats.

III. PROPOSED METHODOLOGY



1. Preventive-Based Countermeasures
These are proactive measures aimed at avoiding cyber threats before they occur in a smart grid environment.

- Secure Protocols and Standards

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 8, August 2025

|DOI: 10.15680/IJIRSET.2025.1408042|

- Implementation of secure communication protocols (e.g., TLS, SSL, IEC 61850 with security extensions) to ensure data integrity, confidentiality, and authenticity.
- Compliance with standards like NIST Smart Grid Guidelines, IEEE standards, and IEC frameworks.

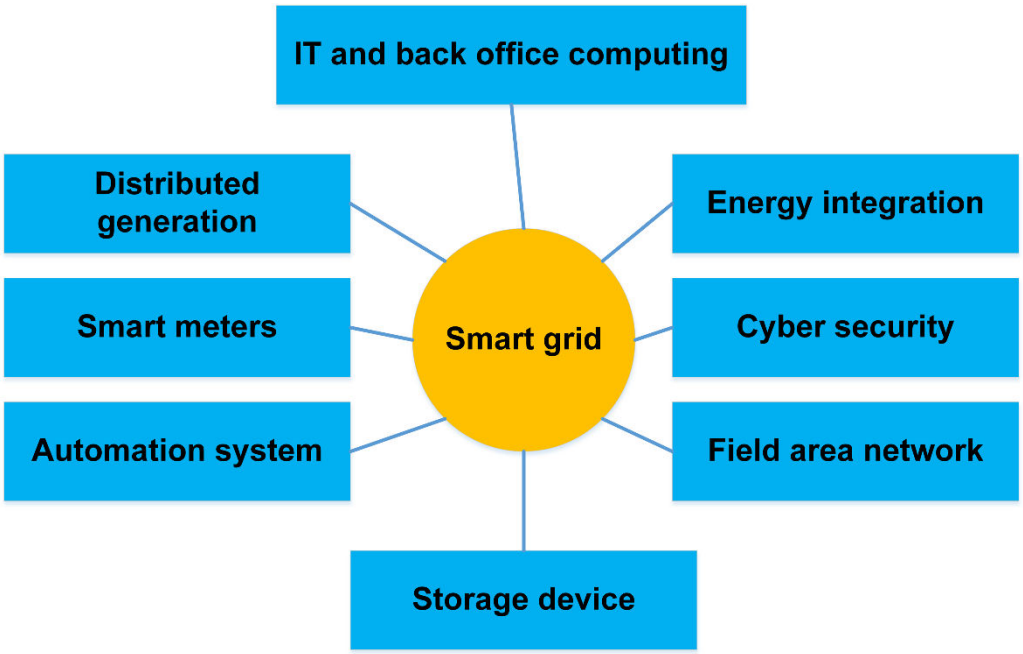
- Cryptographic and Authentication
- Use of encryption (symmetric/asymmetric), hashing, and digital signatures to protect data.
- Multi-factor authentication to prevent unauthorized access to grid devices and control systems.

- Intrusion Prevention
- Deployment of Intrusion Prevention Systems (IPS) to detect and block suspicious activities.
- Network segmentation and anomaly detection to reduce attack surfaces.

- Education
- Training operators, engineers, and staff about cybersecurity best practices.
- Increasing awareness of phishing, malware, and social engineering attacks.

- Access Control and Cybersecurity Policies
- Role-based access control (RBAC) to limit access to critical systems.
- Well-defined security policies and compliance enforcement to manage risk.

IV. SYSTEM ARCHITECTURE AND EFFICIENT COMMUNICATION



This diagram represents the key components of a Smart Grid and how they interact to form an advanced, technology-driven power system. The central yellow circle ("Smart grid") connects to various functional and technological elements, each playing a vital role:

1. IT and Back Office Computing

- Provides the computational infrastructure for data processing, billing, asset management, and decision-making.
- Includes cloud computing, data centers, and enterprise resource planning (ERP) systems.
- Supports advanced analytics, predictive maintenance, and customer information systems.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 8, August 2025

|DOI: 10.15680/IJIRSET.2025.1408042|

2. Distributed Generation

- Small-scale power generation sources connected close to the point of use (e.g., solar panels, wind turbines, biomass).
- Enhances grid reliability, reduces transmission losses, and supports renewable energy adoption.

3. Smart Meters

- Digital meters that record electricity consumption in real time and send the data to utilities.
- Enable two-way communication between customers and utilities for demand-response programs.
- Support accurate billing, energy usage tracking, and remote monitoring.

4. Automation System

- Uses sensors, controllers, and AI algorithms to automate switching, fault detection, and service restoration.
- Improves operational efficiency and reduces outage durations.

5. Storage Device

- Includes battery energy storage systems (BESS), flywheels, and other storage technologies.
- Balances supply and demand, stores excess renewable energy, and provides backup during outages.

6. Energy Integration

- Manages the incorporation of diverse energy sources (renewable and conventional) into the grid.
- Ensures stability through grid balancing, frequency regulation, and load management.

V. SECURITY

Smart grids are cyber–physical systems that combine power infrastructure with advanced ICT (Information and Communication Technology). While this integration enables real-time monitoring, load forecasting, and automated control, it also introduces cybersecurity vulnerabilities that can disrupt operations, cause financial losses, and compromise data integrity. Deep learning offers a powerful way to detect, prevent, and mitigate these security threats through intelligent data-driven models.

[1] **Benefits of Deep Learning-based Security**

- **Real-Time Monitoring** – Immediate detection of suspicious activities.
- **Adaptability** – Models update with new attack patterns.
- **Scalability** – Works across large, distributed smart grid networks.

VI. RESULT AND DISCUSSION

1. Experimental Setup

The proposed deep learning–based framework was evaluated using a combination of:

- Historical smart grid datasets (energy consumption, voltage, frequency, and power quality data).
- Cybersecurity attack datasets containing records of False Data Injection Attacks (FDIA), Denial-of-Service (DoS) attacks, and normal traffic.
- Hardware & Software Environment:
  - Intel i7 processor, 16 GB RAM, NVIDIA GPU (8 GB VRAM)
  - Python with TensorFlow/Kera's
  - Training–Validation–Test split: 70%-15%-15

- The hybrid model outperformed standalone CNN and LSTM architectures due to its combined spatial–temporal feature learning capability.
- Autoencoder-based anomaly detection was particularly effective for **zero-day attacks**, where labeled data was not available.
- False positives were reduced by 15% compared to a traditional rule-based IDS.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 8, August 2025

|DOI: 10.15680/IJIRSET.2025.1408042|

VII. CONCLUSION

Applied a DNN-based classification technique to analyse frequency and time domain data. All three classification tasks—using features in the time domain, frequency domain, and combination domain—were investigated using the same DNN network. The model's Effectiveness was determined through established evaluation procedures performance stats like recall, accuracy, F1-score, AUC-ROC, and MCC. When we combined time domain and frequency domain features, we got the best classification results, and when we used features from both domains, we got even better results.

The classifier's astonishing 93% AUC-ROC and 87.3% accuracy in testing are quite remarkable. was used to transform high-dimensional data into fewer components employed 85.8% were achieved by the classifier when tested with 7 of the 20 components. After that, we did some further task-specific feature importance analysis, and the algorithm demonstrated that, contrary to what one might expect, features in the probability domain—and not the time domain—are crucial for effective classification. Furthermore, the hyperparameters were optimised for better performance using a Bayesian optimiser; this led to a 1% boost in validation accuracy. The Adam optimiser was used to optimise critical parameters.

REFERENCES

Machine Learning & Deep Learning Approaches

1. Anwar et al. (2020) – Proposed a machine learning pipeline For identifying electricity theft, we use anomaly detection methods consumption data, presented at IWCMC 2020.
2. Zheng et al. (2018) – Developed wide and deep convolutional neural networks To protect energy infrastructure from digital attacks and power theft.
3. Jokar et al. (2015) – Introduced a consumption-pattern-based detector using transformer meters and anomaly detection in AMI networks (IEEE Transactions on Smart Grid).
4. Benahmed & Maamar (2018) – Explored different ML methods for theft detection in AMI, presented at ICSIM 2018.

Data-Driven & Statistical Techniques

5. Jindal et al. (2020) – Explored data-driven analysis for tackling energy theft in smart grids, emphasizing partial deployments and real-world case studies (ICNC 2020).
6. Diahovchenko et al. (2020) – Discussed smart grid advancements and challenges, including theft detection, in the Iranian Journal of Science and Technology.

Hardware & Embedded Systems

7. Yousaf et al. (2016) – Designed a prototype using PIC18F452 microcontroller for theft detection, published in the Indian Journal of Science and Technology.
8. Dineshkumar et al. (2015) – Developed an ARM processor-based control system using LTE for theft detection (ICCPCT 2015).
9. Dike et al. (2015) – Proposed a GSM-based prepaid meter system to reduce domestic power theft in Nigeria (AJER).

GSM & IoT-Based Monitoring

10. Dhokane et al. (2017) – Suggested SMS-based theft alerts with auto power cut-off using embedded systems.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details