© JUN 2026 | IRE Journals | Volume 9 Issue 12 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I12-1718574

Detecting and Minimizing Energy theft in Smart Grid Network Using Artificial Neural Network (ANN)

EZE ERNEST CHUKWUEMEKA[1], ELEJE NELSON EMEKA[2]
[1]*Computer Engineering Department, Enugu state Polytechnic, Iwollo, Enugu state.*
[2]*Electrical and Electronic Engineering Department, Enugu state Polytechnic, Iwollo. Enugu state*.

Abstract- ***Detecting and minimizing Energy (Electricity) theft in smart grid network using artificial intelligent (AI) based scheme is work aimed to proffer solution on reducing electricity theft without the traditional or conventional method.Energy theft is a treat to the reliability and sustainability of smart grid network. A Dataset of energy consumption by 5,567 households were collected from November 2011 to February 2014. Data wrangling and model training were done on Nvidia's Tesla T4 GPU(40 cores, 300GB/s bandwidth) (colab.research.google.com, n.d.) and using packages that provide Python bindings around CUDA framework for parallel computations, other components used are Tensor Flow and scikit-learn for machine learning as well as Matplotlib for visualization. The dataset is standardized for each household to ensure a complete and uniform dataset. Generation of anomalous sample was done to train the system and these synthetic samples are critical for training supervised machine learning models. The ANN detect and minimize energy theft through prioritizing inspections, real-time alerts and tampering detection through changes in waveform signature due to tampering.***

Keywords: Smart Grid, ANN, Energy Theft, Cyber-Attack. Dataset, Machine Learning and Deep Learning.

I. INTRODUCTION

Electricity generation, transmission and distribution has undergone a lot of improvement and innovation since the introduction of smart grid system. Many nations especially in developing countries are still operating traditional grid system which is unidirectional in nature. The smart grid concept is the result of a confluence of economic, social, political, technological, and environmental factors. Distribution systems are arguably the section of smart grid network in which smart grid technologies are probably having highest impact on power supply infrastructure. By facilitating two-way communication to increase the efficiency, stability, economy, and sustainability of generation, transmission, and distribution of electrical power, the smart grid is expected to fundamentally change the present traditional power system.

Smart Grid system is known for having Smart appliances, Smart meters, renewable energy sources, and energy-efficient resources which constitute the operational and energy-saving features that make up a smart grid, (Jema.D.N, 2022). Smart Grid has so many definition to accommodate its technologies for the provision of electricity efficiency. According to European technology, smart grid is an intelligent network that integrates user actions in delivery efficient, economical and sustainable electricity to the consumers connected to its power generators (Edeh. V.C, 2024) Smart grid is defined by the United states Energy department as electrical system that utilizes digital technologies for the improvement of reliable, secure and efficient electricity delivery to consumers, incorporating several storage and generation and generation resources (D.T Ton et al, 2011). Another definition is by the international electrotechnical commission (IEC) as a growing network of controls, transmission lines and advanced technologies cooperating in response to immediate electricity demand (M. E. El-Hawary, 2014). A Power system network, where the bidirectional flow of electricity and data is obtained using digital technologies for communication, is known as smart grid. The purpose of a smart grid is to transform traditional electricity networks into the modern grid with the help of information and communication technologies (ICTs)(Kabalci, E and Kabalci. Y, 2019). Smart grid is an improved development of the traditional power grid or the traditional power grid which enhance the interconnection of all the essential power system elements like power generators and transformers, synchronous machines, transmission substations,

© JUN 2026 | IRE Journals | Volume 9 Issue 12 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I12-1718574

transmission lines, distribution lines and substations, and other types of loads with an automated system.

The followings are the smart grid technologies that are used in Nigeria, they are information and communication ntegration (ICI), Wide Area Monitoring and control (WMC), Advanced distribution Automation (ADA), Costomer Side System (CSS), Demand Response (DR), Advanced Metering Infrastructure (AMI), Transmission Enhancement Applications (TEA) and Distributed Energy Resources (DER) (Folasade et al, 2022)

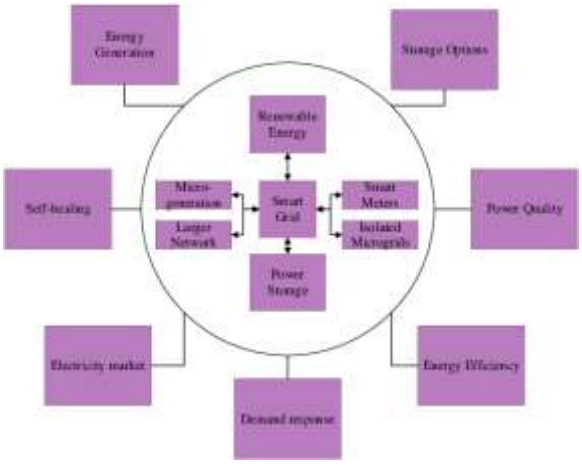

Fig 1.1 Schematic diagram of Smart Grid Network.

The characteristics of smart grid networks are; reliability, flexibility in network topology, efficiency, load adjustment, Pricing of time of consumption and peak curtailment, sustainability, improvement of electricity marketing, etc.

1.1 ELECTRICITY THEFT

There are numerous power outages in Nigeria's transmission and distribution networks. A total of 40% of transmission and distribution losses occur in Nigeria's electricity grid.(Anumaka, M.C, 2012). Electricity theft is an illegal or unauthorized use of electrical power for the purpose of avoiding payment and it is one of the attacks on smart grid network as many would want to use electricity without paying for it. Electricity (energy) theft is a common phenomenon in distribution systems of electricity in which the utility companies like DISCOs losses revenue due inability to get the full payment of the electricity sold to consumers in both developed and underdeveloped countries.

Electricity (energy) theft is also known as actions taken by individuals, businesses or organizations to bypass the legal metering or billing system of the electricity provider for the purpose of reducing or avoiding electricity charges. In Pakistan and India electricity (energy) theft alone costs hundreds of millions of dollars every year to electricity distribution companies. Due to electricity theft and other illegal activities, about 30% of electricity supplied by the utility companies is lost in Ghana (Yakubu, O et al, 2018 and Obafemi.O et al, 2021). Similarly, UMEME Ltd, the main electricity distribution companies in Uganda losses $30million to theft of electricity, hence electricity (energy) theft is serious problem to UMEME Ltd (Obafemi, O et al, 2021). In Turkey, investigation in 2008 alone showed that 196,000 electricity consumers out of 4.8 million consumers were using electricity illegally causing huge loss in revenue to the electricity provider (Tasdoven, H.B et al, 2012). It shows that electricity theft is a crime committed in every countries of the world. It occurs in Africa, Asia, Europe and America.

1.1.1 COMMON ELECTRICITY THEFT

a). Meter bypass: It is a form electricity theft in which a person alters the electrical wiring so that some or all the electricity consumed are not recorded by the meter. This is the shorting circuiting of the terminals at both input and output side of the electricity meter with a wire so that energy consumed will not be registered in electricity meter. Meter bypass are done through direct connection to main supply, looping wire round the meter, Reversing meter connections, using magnets or devices, Bridging Internal circuits.

Fig 1.1 Meter bypass (shokoya and Raji, 2020).

© JUN 2026 | IRE Journals | Volume 9 Issue 12 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I12-1718574

b). Illegal Tapping. This is a situation where a person connect directly to power line without passing through the meter or through a neighbor's connection without getting approval from the distribution company. Ways of doing illegal tapping includes; connecting below the meter, connecting to another person's line like neighbors in a compound, using jumpers on pole lines etc.

Fig 1.2 Illegal tapping (Shokoya and Raji, 2020)

C). Meter Tampering; This is a kind of electricity theft where the meter is tampered by connecting the neutral wire to the earth which makes the meter to enter a mode known as incomplete circuit mode while the meter is still reading. Meter tampering are classified in the followings; conventional meter with total earth temper, conventional meter with reverse temper, conventional meter with partial earth temper, conventional meter with shorting the Phase Line temper.

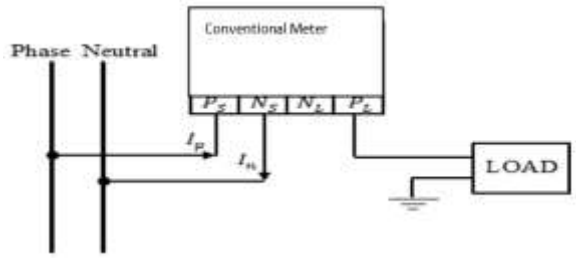

Fig 1.3 Meter tampering (Afolayan and Ibiyemi, 2020).

d). False metering reading: This occurs when there is an inaccurate report of electricity consumption information from electricity meter either deliberately or accidentally which can result to overcharging or undercharging. This act is mostly made possible by corrupt electricity workers that collude with customers to rob the distribution company. Sometimes it occur due to fault in the electricity meter. Another cause is hacking into digital meters to report false consumption data.

e). Smart Meter Hacking: This unauthorized access, manipulation and control of smart meter's hardware and software system to change data, alter operation or commit electricity theft. This is cyber-attack and smart meters are digital and connected to communication network makes the vulnerable to cyber – attacks. This theft is done through the following ways: firmware modification, man – in – the – middle (MITM), backdoor exploitation, replay attacks and physical port access.

f). Remote signal Jamming: This is a cyber-attack in which a person transmits disruptive radio signals to block or interrupt wireless communication between smart meters and distribution system or central monitoring system. Mostly radio frequency (RF), Zigbee, Wi – Fi or power line carriers (PLC) are used by smart meters to transmit consumption data and interference happens when a stronger or noisy signal is transmitted on the same frequency to prevent successful communication. Such signal jamming include; Constant jamming, deceptive jamming, Random Jamming and reactive jamming.

g). Data Manipulation: This a type of cyber-attack in which persons alter, falsify and inject incorrect data into the smart grid communication systems or devices. It affects the integrity of data for the purpose of misleading operators, disrupt operations and enable elcctricity theft. This data manipulation attack of electricity is achieved through; False datainjection attack (FDIA), Load Profile scoring, Billing fraud, topology manipulation, control command alteration and time – stamp modification.

h). Cloning Devices: This is another type of cyber – attack and is known as copying or replication of authentic metering or communication devices to avoid monitoring, spoof data or manipulate billing systems with the aim of deceiving electricity provider. This makes the customer steal electricity look like he/she is using a valid, unaltered system while secretly stealing power. Ways of cloning meters include meter ID cloning, Token cloning, communication spoofing, RFID/NFC card cloning.

© JUN 2026 | IRE Journals | Volume 9 Issue 12 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I12-1718574

Consumers pay for the Generation, Transmission and Distribution of Electricity and any loss in revenue will affect the service delivery of the utility company negatively. Electricity losses abound in the transmission and distribution System of Nigeria's power Network. Nigeria's power grid has a total transmission and distribution loss of 40%. On the contrary, new developments in artificial intelligence (AI) approaches have garnered increasing interest and offer strong and promising tools for stability analysis and control in smart grids.

II. ARTIFICIAL INTELLIGENT (AI)

Artificial intelligence (AI) techniques have drawn a lot of attention since traditional computational methods are unable to handle the massive volume of data that smart grid systems introduce. Since these AI techniques leverage large-scale data to further enhance smart grid efficiency, a significant amount of research was dedicated to studying them in order to overcome the issues. AI can be subdivided into Machine learning and Deep learning.

Recent studies have captured the potential of AI in improving various aspects of smart grid operations. Specifically, detection systems based on deep – learning have been developed to detect and mitigate cyber-attacks, such as scanning, buffer overflow, and service denial attacks in the advanced metering infrastructure. Moreover, AI techniques have also been used to automate and increase the output of smart grid applications, including the addition of renewable energy resources, demand outcome, grid health monitoring and, systems for energy storage (Ali & Choi, 2020). One promising approach involves the use of AI algorithms to continuously monitor the smart grid's state and rapidly respond to potential disruptions. By analyzing the large volume of data generated by IoT devices and Smart grid components, AI-powered systems can detect anomalies, predict grid instability, and initiate appropriate countermeasures to maintain grid stability and resilience (Ali & Choi, 2020). Additionally, reinforcement learning algorithms can aid in optimizing energy dispatch decisions and demand management strategies, ensuring a balanced supply-demand equilibrium even during unexpected events (Azad et al., 2019). Artificial intelligent techniques enhance the operations of Smart grid network including detecting and reducing energy theft through the following ways; anticipatory maintenance, fault detection and diagnosis, energy management, grid stability and optimization, automated control, data analysis and visualization, Cybersecurity, etc.

2.1 Machine Learning and Deep Learning

The modelling tools used in this work is machine Learning and Deep learnig algorithms. Machine learning is a transformative field of artificial intelligence (AI) that empowers computers to learn and improve from experience without being explicitly programmed. Instead of relying on a set of predetermined instructions, machine learning algorithms are designed to identify patterns and make predictions from data. This allows them to tackle complex problems and adapt to new information, making them a cornerstone of modern technology. At its core, machine learning involves feeding vast amounts of data to an algorithm. The algorithm then builds a mathematical model based on this data. This model can be used to make predictions or decisions on new, unseen data. The more data the algorithm is exposed to, the more it "learns" and the more accurate its predictions become. Machine learning is broadly categorized into three main types, each distinguished by the way the algorithm learns from the data and they are, supervised learning, unsupervised learning and reinforcement learning.

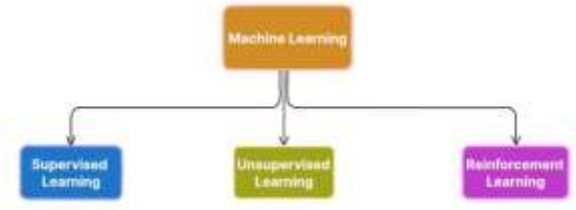

Fig 2.1: Machine Learning Division

DEEP LEARNING

Deep learning is a specialized and advanced type of machine learning that uses complex, multi-layered neural networks to learn from vast amounts of data. Its structure is inspired by the human brain, allowing it to learn and make intelligent decisions on its own. The foundation of deep learning is artificial Neural Network (ANN). Examples of deep learning includes

the following; Feedforward Neural Network (FNN), Convolutional Neural Network (CNN), Recurrent Neural Network (RNN), Long Short – Term Memory (LSTM), Gated Recurrent Units (GRU). Utoencoders, Generative Adversarial Network (GAN) etc. The type of model used in this work is CNN model. Neural networks, also known as artificial neural networks (ANNs) that provide the basis of deep learning approaches. Their name and shape are derived from the human brain, and they mimic how genuine neurons interact with one another. Artificial neural networks (ANNs) are massively parallel systems made up of many linked basic processors (Roheen & Baqar, 2023).

2.2 Overview of Convolutional Neural Network (CNN)

Convolutional Neural Networks (CNNs) are a class of deep neural networks optimized for processing grid-like data, such as images. They leverage spatial hierarchies through convolutional operations, enabling automatic feature extraction (LeCun et al., 1998). CNNs have become foundational in computer vision tasks, including image classification, object detection, and segmentation. They are characterized by their ability to automatically learn hierarchical feature representations directly from raw input data through convolutional, nonlinear, and pooling operations.

CNNs apply learnable filters (or kernels) to the input data. Conceptually, an operation of convolution involves sliding a small matrix (the filter) above the input and computing the dot product at every spatial position. The convolutional layer applies learnable filters (kernels) to input data to extract spatial features. Each filter performs a cross-correlation operation by sliding over the input. For an input I and kernel K, the output feature map S is computed as:

$$S(i,j) = (I * K)(i,j) = \sum_{m} \sum_{n} I(i+m, j+n) . K(m,n)$$

(2.2)

Where $*$ denotes cross-correlation. Filters are shared across the input (parameter sharing), reducing computational complexity (Goodfellow et al., 2016).

Following the convolution, a nonlinear activation function such as the Rectified Linear Unit (ReLU) is typically applied:

$$ReLU(x) = max(0,x)$$

2.3

ReLU mitigates the vanishing gradient problem and accelerates convergence (Nair & Hinton, 2010).

Pooling layers are interleaved between successive convolutional layers to progressively reduce the spatial dimensions of the data, lowering the computational load and helping control over fitting. Everyday pooling operations include max pooling, which selects the maximum value within a given region, and average pooling, which computes the average value. Pooling imparts a degree of translation invariance to the learned features.

After several convolutional and pooling layers, the feature maps are typically flattened into a one-dimensional vector and passed through one or more fully connected layers. These layers act as high-level reasoning parts of the network, making final predictions based on the features extracted by the preceding layers. The network is trained end-to-end using back propagation, where the weights of both the convolutional and fully connected layers are updated to minimize a chosen loss function.

Regularization techniques, such as dropout, are often employed to prevent over fitting by randomly deactivating a subset of neurons during each training iteration. This encourages the network to learn more robust features that generalize to unseen data.

The architectural design of CNNs, characterized by local receptive fields, weight sharing, and spatial hierarchies, makes them particularly well-suited for tasks in computer vision, such as image classification, object detection, and segmentation (Krizhevsky, Sutskever, & Hinton, 2012). Moreover, their principles have been extended to other domains, including natural language processing and time-series analysis, where data exhibits spatial or temporal structure. Major Conmopenets of a CNN are, input Layer, Convolutional Layer, activation function, pooling layer (Subsampling), fully connected (dense) layer, output layer

© JUN 2026 | IRE Journals | Volume 9 Issue 12 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I12-1718574

Advantages of CNN are automatic feature extraction, Parameter sharing, translation invariance, hierarchical feature learning, reduced computational cost, high accuracy for spatial data and robustness to noise.

III. MODELLING USING REAL TIME DATASET

Models are as good as the data they are trained on, therefore we cannot model without first analysis the dataset used in this work. High-quality, representative data enables the model to identify patterns and make accurate predictions. This means accessing energy consumption data with features that can inform the detection of legitimate usage and fraudulent activities. Obtaining local data is not feasible as local distribution companies do not release individual energy usage data, possibly due to privacy concerns or a lack of sensing setups to do this effectively. Our approach uses non-local datasets with characteristics similar to Nigeria's power distribution systems to ensure the obtained model can easily adapt to the local context. A well-designed model should be able to generalize its learnings to new scenarios and the following steps are taking in the modelling,

a). Cleaning of missing or corrupted values,
b). Resampling of data in daily, weekly and monthly usage profiles,
c). Normalization or standardization of datasets collected,
d). Generation of anomalous samples,
e). Packaging of dataset for modelling.

The project collected household energy consumption data from November 2011 to February 2014. The dataset is publicly hosted on the London data store. The dataset has detailed electricity data of 5,567 London households consumption gotten between November 2011 and February 2014. This is a very important step in this work. The quality and volume of the data impact the performance of any AI model directly. In this work, a dataset of household of 167,932,474 records with three main columns was obtained and the dataset comprises detailed energy consumption data from 5,567 London households collected between November 2011 and February 2014.

Fields in the Dataset
a). Household Identifier (LCLid): A unique identifier of the form MAxxxxx assigned to each participating household. It can also be seen a meter number for each household.
b). Timestamp (DateTime): The date and time when the energy consumption reading was recorded.
c). Energy Consumption (KWH/hh): The amount of electricity consumed recorded half hourly and unit in kilowatt-hours.
d). Tariff Type (std or dTou): Indicates the electricity tariff applied to the household, such as standard or dynamic time-of-use (stdorToU).
e). Dynamic Pricing Signal (for dToU participants): The pricing signal received by the household during the specified time interval, categorized as High, Low, or Normal.

3.1.1 Exploratory Data Summary

This is a summary of the statistics or data used in this work as shown in appendix 1 and Table 3.1
The dataset consists of 167,932,474 records with three main columns: LCLid (unique identifier), DateTime (timestamp), and KWH (energy consumption in kilowatt-hours). There are 5560 missing values in the KWH column. The energy consumption (KWH) has a mean value of 0.2118 kWh with a standard deviation of 0.2973 kWh, indicating variability in energy usage. The minimum recorded value is 0 kWh, while the maximum reaches 10.761 kWh, suggesting significant fluctuations in consumption. Energy Usage Patterns of the datatset were considered for daily, weekly and monthly usage pattern.

Table 3.1: Summary statistics of the LCL dataset (Generated using Appendix B)

statistic	LCLid	DateTime	KWH
str	str	str	f64
count	167932474	167932474	1.67926814e8
null_count	0	0	5560.0
mean	null	2013-03-28 05:35:22.133249	0.211763
std	null	null	0.297259
min	null	2011-11-23 09:00:00	0.0
25%	null	2012-10-21 20:30:00	0.058
50%	null	2013-03-30 05:30:00	0.117
75%	null	2013-09-10 09:00:00	0.239
max	null	2014-02-28 00:00:00	10.761

© JUN 2026 | IRE Journals | Volume 9 Issue 12 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I12-1718574

The dataset spans from November 23, 2011, to February 28, 2014, with the median timestamp falling on March 30, 2013. This timeline provides a broad period for analysis and highly valuable for long-term energy consumption studies. A slice of the dataset is shown in Table 3.2.

Table 3.2: Slice of the LCLid dataset (see Appendix 2 for the codes)

LCLid	DateTime	KWH
cat	datetime[µs]	f32
MAC000002	2012-10-12 21:00:00	0.197
MAC000002	2012 10 12 21:30:00	0.342
MAC000002	2012-10-12 22:00:00	0.27
MAC000002	2012 10 12 22:30:00	0.325
MAC000002	2012-10-12 23:00:00	0.269
…	…	…
MAC000002	2012-10-13 14:30:00	0.263
MAC000002	2012-10-13 15:00:00	0.134
MAC000002	2012-10-13 15:30:00	0.235
MAC000002	2012-10-13 16:00:00	0.124
MAC000002	2012 10 13 16:30:00	0.184

The final cleaning step is packing the dataset into a suitable data structure for modeling. 3d tensor was used as a container. Each element of the tensor is a 2d matrix representing a household. The rows of the matrix represent days, while the columns represent the hours of the day. The readings have a granularity of 1 hour which gives each matrix 24 columns The rows are stacked to form the 2d household matrix. The shape of the tensor is of the form:

$$(number\ of\ households, number\ of\ rows, 24$$

3.2 Anomalous samples were generated.
The six methods described by (Jokar et al, 2016) were adapted and used in generating anomalous energy consumption samples.

Any given household matrix consists of rows whose elements are daily energy consumption recorded hourly. Denote a row element of the matrix by

$$x = \{x_1, \ldots x_{24}\} \quad 3.1$$

the following methods are used to derive anomalous equivalents:
Uniform scaling

$$h_1(x_t) = \alpha x_t \quad 3.2$$

This function scales all hourly consumption values by a constant factor α, randomly selected between 0.1 and 0.8. This simulates attacks where customers uniformly reduce reported consumption across all periods, such as tampering with meter calibration or intercepting communication signals to suppress measurements proportionally.

Time – Window Suppression

$$h_2(x_t) = \beta_t x_t \quad 3.3$$

A random time window within the 24-hour period is selected, during which consumption values are set to zero. (where β_t=0 within the window and 1 otherwise). The window duration ranges from 4 to 24 hours, mimicking scenarios where meters are physically disconnected or cyber-attacks block data transmission during high-usage intervals
Random Per – slot Scaling

$$h_3(x_t) = \gamma_t x_t \quad 3.4$$

Each hourly consumption value is multiplied by a unique random factor γ_t ϵ [0.1,0.8].

This equation models sporadic tampering, where attackers dynamically adjust reduction rates to evade detection, such as selectively altering readings during peak tariff periods.

Fractional Daily Average Reporting

$$h_4(x_t) = \gamma_t \,.mean(x) \quad 3.5$$

Consumption values are replaced with a random fraction of the daily mean. This attack exploits flat-rate billing structures by underreporting usage while maintaining a consistent daily profile, avoiding abrupt anomalies that might trigger suspicion.

Exact Daily Average Reporting

$$h_5(x_t) = mean(x) \quad 3.6$$

All hourly values are replaced with the exact daily average. This strategy neutralizes time-of-use pricing by shifting high consumption from peak to off-peak

© JUN 2026 | IRE Journals | Volume 9 Issue 12 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I12-1718574

periods, effectively reducing costs without altering total daily usage.

Temporal Reversal

$$h_5(x_t) = x_{24-t} \quad 3.10$$

The order of hourly consumption values is reversed. By mirroring the load profile, this attack misrepresents peak usage during low-tariff intervals, circumventing dynamic pricing schemes while preserving the total energy reported.

To generate an anomalous sample given a normal household usage pattern in the 2d matrix, an anomalous sample is generated according to algorithm 1. A sample anomalous sample is shown in Figure 4.1

Algorithm 1:

$$Given\ a\ normal\ sample\ X = \{x_n\}$$
$$Define\ an\ anomalous\ sample\ Y = \{y_n\}$$
$$n \in \{1, 2\ ..\ total\ number\ of\ days\}$$

For

$$n = 1\ to\ total\ number\ to\ days, do$$
$$h = random(h_1, \ldots h_6)$$
$$y_n = h(x_n)$$

Modelling of Convolutional Neural Network (CNN) for energy theft feature extraction.

The general workflow (Figure 3.2) is to extract features from the input data (2d matrix representing household) using a CNN and pass the features to specialized classifiers to output the final class: anomalous or normal electricity consumption.

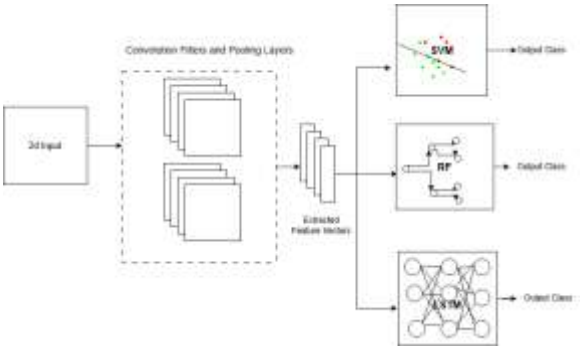

Figure 3.2: CNN Model development Workflow.

IV. RESULTS

Results obtained from the normalization and standardization of the smart grid dataset used are shown in Figure 4.1 and 4.2.

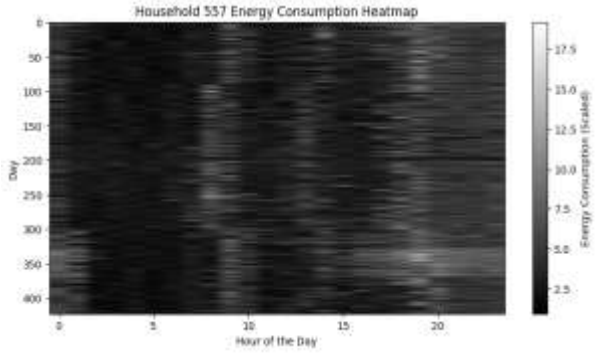

Figure 4.1, Energy profile for household 557

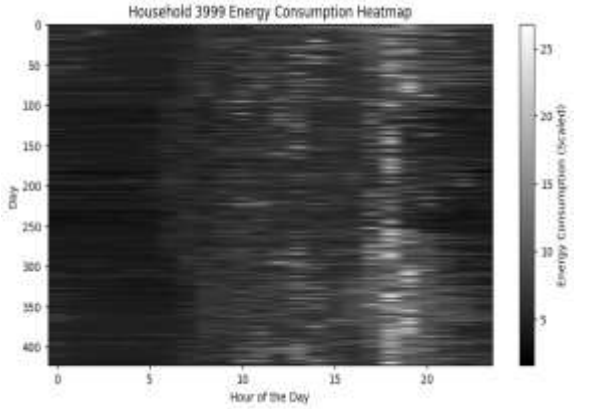

Figure 4.2: Household 557(5a) and 3999's energy usage profile.

The white vertical stripes represent high-energy usage periods

The images reveal distinct energy consumption patterns throughout the day. The lighter vertical strips, particularly around the morning and evening hours, indicate higher energy usage. This aligns with real household operations, where energy demand spikes in the morning as residents wake up and engage in cooking and heating. Similarly, evening peaks reflect increased usage from lighting, cooking, and entertainment after returning home. In contrast, the darker areas during late night and midday suggest lower energy consumption as most people are usually not at home or asleep during those times.

© JUN 2026 | IRE Journals | Volume 9 Issue 12 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I12-1718574

Below is the graph of the generated samples of anomalous sample

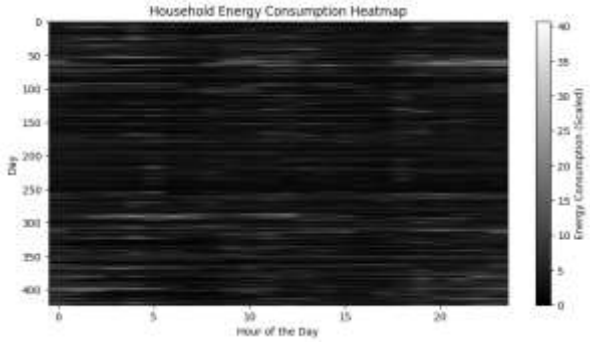

Figure 4.3 Anomalous sample generated using algorithm 1

As shown in Figure 4.3, it is model of a smart grid metering system by generation of Anomalous samples to show energy theft. Obtaining real-world theft samples is inherently challenging due to the rarity of such events for individual customers and the absence of labeled attack data in historical records.
From the results of the figures gotten from the realtime dataset and generated anomalous data, ANN can handle the energy theft detection and minimization more efficiently. ANN can also handle both technical and non-technical losses in Smart grid metering system.

Artificial Neural Network does not stop theft directly but it enhances detection and minimization by using these techniques. a). Prioritizing Inspections which can be achieved using energy usage patterns. b).Real time alerts, ANN also uses the patterns generated from the dataset to flag suspicious events instantly instead of waiting for routine cycles. C). Tampering detection, with the patterns as shown in figure 4.1 – 4.3, ANN can detect any changes in the pattern as tampering changes the waveform signature and the ANN catches it.

V. CONCLUSION

Deep learning, convolutional neural networks, and recurrent neural networks are a few examples of the neural network technology that some modern IDS and IPS solutions are starting to use to analyses network traffic more accurately and address other shortcomings of conventional systems. Even when attacks deviate from known attack vectors, ANNs are better at spotting trends and pinpointing breaches. With ANN being employed to combat energy theft, it will boost revenue of many Utility companies that provide electricity to many consumers. The system will also increase more revenue generation for many DISCOs in Nigeria. Since many consumers pay for the energy consumed, it causes for effective load management. It also reduces corruption among electricity workers.

REFERENCES.

[1] Anumaka. M.C, "Analysis of Technical Losses in Electrical Power System (Nigerian 330kV Network as a case study)", International Journal of Research and Review of Applied Sciences, pp. 320-327, 2012.

[2] D.T.Ton., W. M. Wang, and W. P. Wang, “Smart grid r&d by the us department of energy to optimize distribution grid operations,” in 2011 IEEE Power and Energy Society General Meeting. IEEE, 2011, pp. 1–5.

[3] Edeh Vincent Chukwuemeka, “Detection of false data injection attacks in Smart Grids.” Swinburne University of Technology, 2024.

[4] Folasade M. Dahunsi, Aminat O. Abdul-lateef, Adegoke O. Melodi, Akinolu A. Ponnle, Oluwafemi A. Sarumi and Kazeem A. Adedeji (2022) “ The smart grid System in Nigeria: Prospects, issues, challenges and way forward. FUOYE Journal of Engineering and Technology(FUOYEJET), Vol.7, No 2, June 2022,pp 183 – 192. DOI:10.46792/fuoyejet.v7i2.781

[5] Goodfellow,I., Bengio Y, & Courville, A. (2016) Deep learning. MIT Press.

[6] Jema David Ndibwile (2022) Artificial intelligence –Based Smart Grid Vulnerabilities and Potential Solutions for Fake – Normal Attacks: A Short Review. https://hal.science/hal-03576427v1

[7] Kabalci, E and Kabalci, Y. Smart Grids and Their Communication Systems; Springer: Singapore, 2019.

[8] Krizhevesky, A. Sutskever I. & Hinton, G.E (2012). ImageNet classification with deep

convolutional neural networks. In Advances in Neural Information Processing Systems.

[9] M. E. El-Hawary, "The smart grid—state-of-the-art and future trends," Electric Power Components and Systems, vol. 42, no. 3-4, pp. 239–250, 2014

[10] M.O.Obafemi, E.A.Oluwole, T.E. Omoniyi, P.N. Meduna and A.S. Alaye, (2021). Prevelence of Electricity Theft among Households in Lagos state Nigeria. Nigerian Journal of Technology (NIJOTECH) Vol. 40, No. 5 September, 2021, pp.872 –881. http://dx.doi.org/10.4314/njt.v40i5.13

[11] N.O. Shokoya and A.K.Raji "Electricity theft Mitigation in the Nigeria Power sector". International Journal Engineering & Technology, 8(4)(2019) 467 – 472.

[12] 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, 2016

[13] Roheen Qamar and Baqar Ali Zardari (2023), Artificial Neural Network: An Overview. Mesopotamian Journal of Computer Science, Vol (2023), 2023, pp 130 – 139. DOI: https://doi.org/10.58496/MJCSC/2023/015;

[14] Shokoya and Raji (2020). Electricity theft Mitigation in the Nigeria Power Sector. International Journal of Engineering & Technology, 8(4) (2019) 467 – 472. https://www.researchgate.net/publication/343079926 DOI: 10.14419/ijet.v8i4.29391.

[15] Tasdoven, H. B. Fiedler, A. Garayev, V. "Improving electricity efficiency in Turkey by addressing illegal electricity consumption: A governance approach". Energy Policy, 43, (2012), pg 226-234.

[16] Usman Inayat, Muhammad Fahad Zia, Sajid Mahmood, Tarek Berghout, "Cyber security Enhancement of smart Grid Attacks, Methods, and Prospects" Electronics (Switzerland), volume 11, issue 23, 2024.