Cape Peninsula
University of Technology

DEVELOPMENT OF ELECTRICITY THEFT DETECTION AND MITIGATION IN SMART GRID

by

NURUDEEN OLATUNDE SHOKOYA

Thesis submitted in fulfilment of the requirements for the degree

Doctor of Engineering: Electrical Engineering

in the Faculty of Engineering and the Built Environment

at the Cape Peninsula University of Technology

Supervisor: Prof. AK Raji

Bellville

October 2024

DECLARATION

I, Nurudeen Olatunde Shokoya, declare that the contents of this thesis represent my own unaided work, and that the thesis has not previously been submitted for academic examination towards any qualification. Furthermore, it represents my own opinions and not necessarily those of the Cape Peninsula University of Technology.

23-02-2025

Signed **Date**

ABSTRACT

Electricity theft (ET) is a ubiquitous problem ravaging all electric utilities worldwide. Theft of electricity is caused by so many factors, but developing a formidable anti-theft solution is one of the major problems facing electric utilities globally. Like a virus, ET is slowly wreaking havoc on power utilities worldwide and its dreaded curves need to be flattened. Since ET cannot be totally eradicated in power grids, the motivation for this research is to profoundly detect and mitigate ET in electric networks. ET must be utterly detected and mitigated to uncover the power pilferers, promote healthier electricity grids, generate more income for the utilities, improve the reliability and sustainability of power systems, and consequently help in salvaging the economies of nations worldwide. Power losses occasioned by ET could be redressed by either generating more power to compensate for the theft-inflicted power shortfalls or by mitigating the theft, but mitigating the theft is more significant and more cost effective. Artificial intelligence-based (AI-based) machine learning (ML) methods are the state-of-the-art and superior approach for the detection of ET or non-technical losses (NTL) in power grids when compared with the conventional methods of electricity-theft detection (ETD).

The experimental work in this thesis centres on the detection of ET using the real-world energy consumption dataset provided by the State Grid Corporation of China (SGCC), a state-owned SG electric system, and the largest electric utility company in the world. The case-study dataset which has thus been obtained from the smart meters of electricity consumers is formidable because it has been used extensively in the existing literature by many researchers to develop various ETD models. This gives room for comparison of results among several ETD models developed using same SGCC dataset. In the experiments, ETD is performed with the infusion of the features from convolutional neural network (CNN) model into random forest (RF) model to form a hybrid model termed CNN-RF. The hybridization of the models is done in a quest to achieve better NTL prediction results, as the combined strengths of CNN and RF achieves complete elimination of undesirable false positives in the composite model. RF is noted to be highly effective and efficient in resolving classification problems, hence it is a choice candidate for the hybrid solution. Meanwhile, before finally adopting the proposed CNN-RF model, the performances of CNN and RF models were individually checked. Simulations were performed using Python, in a Google Colaboratory (Colab) Integrated Development Environment (IDE).

The performance metrics employed to evaluate the developed models are precision, recall, F1 score, accuracy, Matthews correlation coefficient (MCC), area under the receiver operating characteristic curve (AUC), area under the precision-recall curve (PR-AUC), true negative rate (TNR), false positive rate (FPR), and false negative rate (FNR). The proposed model show very interesting and reliable performance results, achieving 100.00% precision, 98.36% recall, 99.17% F1 score, 99.20% accuracy, 98.40% MCC, 99.13% AUC, 99.55% PR-AUC, 100.00% TNR, 0.00% FPR, and 0.02% FNR.

Overall, the proposed model outperformed other SGCC dataset-based ETD model results presented in previous research. The proposed model achieves unprecedented high hit ratio, making it more-effective and more-efficient in detecting NTL. Higher performance scores from ETD models are proportional to greater mitigation of NTL attainable by utility inspectors or technicians during onsite inspections. The feat achieved in this research by profoundly detecting ET in SG, with its anticipated increased onsite mitigation prospects, is a fulfilment of the aim and objectives of the research. Besides, the higher detection capability achieved by the proposed model has also simultaneously proffered answers to the research questions. The proposed model is therefore recommended as a suitable ETD solution for deployment by electric utilities of various economies of the world.

ACKNOWLEDGEMENTS

I wish to thank:

- Almighty Allah, the supreme, for this invaluable opportunity of a doctoral degree in a reputable university like the Cape Peninsula University of Technology (CPUT).

- My supervisor, Prof. AK Raji, for his guidance, encouragement, patience, compassion, and support. Thank you for your assistance in bringing me to the University. Prof. Raji is someone I can always count on. He possesses one of the best human characters that are worthy of emulation. He is non-partisan, cosmopolitan and very diligent. Whenever I send him emails, even in the wee hours, he responds promptly. At times, I wonder if he ever sleeps. He is very reliable and always there to assist. I will always be grateful to him. A huge recognition also goes to his amiable wife, Mrs Folashade L. Raji, for behind every great man there is an exceptional woman.

- My wife, children, parents and siblings for their perseverance, support, and prayers. I thank them for their unrelenting support, understanding and compassionate love.

- My friend Dr NA Azeez who introduced me to my supervisor. He also did a lot of follow-ups with my supervisor to ensure that my admission came to fruition. I thank him so much.

- Dr IB Adefeso for his brotherly advice, support and care. He helped me to settle down when I arrived the Rainbow Nation.

- Dr Sheriff Salisu and his amiable wife, Mrs Yetunde Salisu for always being there. They are parental replica to me in South Africa. They go extra mile to make others comfortable. May the Almighty be with them, reward them abundantly and grant their heart desires.

- Engr WB Ajao and Engr AA Raji for their assistance and brotherly compassion.

- Dr DN Luta, Dr AO Giwa, Akeem Otun and other friends for their assistance and encouragements.

- All the members of the Centre for Distributed Power and Electronic Systems (CDPES) in the Electrical, Electronic and Computer Engineering Department, Cape Peninsula University of Technology, for the interesting and thorough study environment.

- The Centre for Postgraduate Studies (CPGS) at the Cape Peninsula University of Technology for their support.

- Lastly, I immensely appreciate the financial assistance given by CPUT Postgraduate Bursary, and the research materials provided by CPUT University Research Fund (URF).

DEDICATION

This thesis is dedicated to my wife, children, parents and siblings for their unwavering support, undying love, and affection. It is also dedicated to all those who have assisted me in one way or the other towards the actualization of the doctoral degree.

PUBLICATIONS

Published papers

Shokoya, N.O. & Raji, A.K. 2019. Electricity theft: A reason to deploy Smart Grid in South Africa. In *Proceedings of the 27th International Conference on the Domestic Use of Energy, DUE 2019.* 96-101. https://ieee.org/abstract/document/8734431.

Shokoya, N.O. & Raji, A.K. 2019. Electricity theft mitigation in the Nigerian power sector. *International Journal of Engineering and Technology,* 8(4): 467-472. https://doi.org/10.14419/ijet.v8i4.29391.

Papers under review

Shokoya, N.O. & Raji, A.K. (2024 submitted). Electricity theft detection in Smart Grid using convolutional neural network model. *Energies*, under review.

Shokoya, N.O. & Raji, A.K. (2024 submitted). Hybrid CNN-RF model for the detection of electricity theft in Smart Grid. *Journal of Electrical and Computer Engineering*, under review.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ABBREVIATIONS AND ACRONYMS

1D-CNN/Conv1D	One-dimensional convolutional neural network
2D-CNN/ Conv2D	Two-dimensional convolutional neural network
3D-CNN/Conv3D	Three-dimensional convolutional neural network
3G	Third-generation technology in cellular communications
3SLS	Three-stage least squares
4G	Fourth-generation technology in cellular communications
ABC	Artificial bee colony
AC	Alternating current
AdaBoost	Adaptive boosting
Adam	Adaptive Moment Estimation
ADASYN	Adaptive synthetic sampling
ADASYNENN	Adaptive synthetic edited nearest neighbour
ADC	Analogue-to-digital converter
ADOMS	Adaptive Oversampling Minority Samples
AE	Absolute error
AE-BiGRU	Autoencoder and bidirectional gated recurrent unit
AI	Artificial intelligence
AL	Active learning
AMI	Advanced metering infrastructure
AMIDS	AMI intrusion detection system
AMR	Automatic meter reading
ANN	Artificial neural network
ANOVA	Analysis of variance
AP	Affinity propagation
APLSTM	AlexNet and peephole long short-term memory
APLSTM-ESNN	AlexNet and peephole long short-term memory echo state neural network
ARMA	Auto-regressive moving average
ARIMA	Auto-regressive integrated moving average
AUC	Area under the receiver operating characteristic curve
BDR	Bayesian detection rate
Bi-LSTM	bidirectional long short-term memory
Bi-WGAN	Bidirectional Wassertein generative adversarial network

BiGRU	Bidirectional gated recurrent unit
BIRCH	Balanced iterative reducing and clustering using hierarchies
BLS	Broad learning system
BP-MLP	Multilayer perceptron with backpropagation
BPL	Broadband over Power Lines

C&R	Classification and regression tree
CatBoost	Categorical boosting
CBOS	Cluster-based oversampling
CDMA	Code Division Multiple Access
CNCP	Convolution-non-convolution parallel deep network
CNN	Convolutional neural network
CNN-RF	Convolutional neural network and random forest
CNN-XGB	Convolutional neural network and extreme gradient boosting
Colab	Colaboratory
CS	Clustering-based sampling
CPBETD	Consumption pattern-based energy theft detector
CS-SVM	Cost-sensitive support vector machine
CSLSTM	Cost-sensitive learning and long short-term memory
CSV	Comma-separated values
CT	Current transformer
CT-WGAN	Convolutional transformer-Wasserstein generative adversarial network
CUSUM	Cumulative sum
CVLR-ETDM	Categorical Variable-Enhanced Linear Regression-based scheme for Detection of Energy Theft and Defective Smart Meters
CWGAN	Cconditional Wasserstein generative adversarial network
CWGAN-GP	Cconditional Wasserstein generative adversarial network gradient penalty
CWR	Credit worthiness rating

DANN	Deep artificial neural network
DAL	Deep active learning
DBS	Distance-based sample
DBSCAN	Density-Based Spatial Clustering of Applications with Noise
DC	Direct current
DCNN	Deep convolutional neural network
DE-RUSBoost	Differential evolution random undersampling boosting

DenseNet-FCN	Densenet-fully convolutional network
DenseNet-GRU-LightGBM	Densenet-fully convolutional network and gated recurrent unit with a light gradient boosting machine
DES	Density estimation-based sampling
DER	Distributed energy resources
DKNN	Decomposed k-nearest neighbours
DL	Deep learning
DLI	Distribution Line Carrier
DNN	Deep neural network
DR	Detection rate
DRF	Distributed random forest
DSDB	A dual-scale and a dual-branch structure
DSDBGWT	Hybrid of DSDB and GWT
DSL	Digital subscriber line
DSN	Deep siamese network
DSP	Digital signal processor
DT	Decision tree
DWMCNN-RF	Day, week, and month convolutional neural network and random forest
EEPROM	Electrically erasable programmable read-only memory
EISA	Energy Independence and Security Act
ELU	Exponential Linear Unit
EMD	Empirical mode decomposition
ENN	Edited nearest neighbour
ESNN	Echo state neural network
ET	Electricity theft
ETD	Electricity-theft detection
EV	Electric vehicle
EWMA	Exponentially-Weighted Moving Average
FA-XGBoost	Firefly algorithm-based extreme gradient boosting
FBS	Fraud class-based sample
FC	Fully connected layer
FDI	False data injection
FIS	Fuzzy interference system
FL-SE-GRU	Federated learning-based stacking ensemble gate recurrent unit

FN	False negative
FNR	False negative rate
FP	False positive
FPR	False positive rate
FractalNet	Fractal network
FRESH	Feature extraction and scalable hypothesis
FRTU	Feeder remote terminal unit
GA	Genetic algorithm
GANCNN	Self-attention generative adversarial network and convolutional neural network
GAM	Generalized additive model
GAT	Graph attention network
GBDT	Gradient boosting decision tree
GCAE	Gate convolutional autoencoder
GCN	Graph convolutional neural network
GDP	Gross domestic product
G-mean	Geometric mean
GMM	Gaussian mixture model
GPRS	General Packet Radio Service
GRU	Gated recurrent unit
GSM	Global System for Mobile Communications
GPU	Graphics processing unit
GWO	Grey wolf optimization
GWT	Gaussian weighting
HAN	Home Area Network
HDI	Human development index
HDR	Hybrid data resampler
HGC	Hybrid of GRU and CNN
HOUBC	Hybrid oversampling and undersampling using both classes
HV	High voltage
HVAC	Heating, ventilation, and air conditioning
HVDC	High-voltage direct current
Hz	Hertz
iANN	Improved artificial neural network

IC	Integrated circuit
ICT	Information and communications technology
IDE	Integrated Development Environment
IDS	Intrusion detection system
IES	Integrated expert system
IMF	Intrinsic mode function
IO	input and output
IONB	Interpolation, outlier detections, normalization, and balancing
IOS	Interpolation, outliers handling, and standardization
IoT	Internet of things
IP	Internet Protocol
IQMOT	Interquartile minority oversampling technique
IV-GMM	Instrumental variable generalized method of moments
Jaya-RUSBoost	Jaya random undersampling boosting
JPS	Jamaica Public Service Company
KNN	K-nearest neighbours
KPCA	Kernel Principal Component Analysis
KTBoost	Kernel and Tree Boosting
kVA	Kilovolt-ampere
kVArh	Kilovolt-ampere reactive hour
kW	Kilowatt
kWh	Kilowatt-hour
LAN	Local Area Network
LCD	Liquid crystal display
LED	Light-emitting diode
LGB	Light gradient boosting
LightGBM	Light gradient boosting machine
LK-SVM	Linear kernel support vector machine
LLE	Locally linear embedding
LOF	Local outlier factor
LoRAS	Localized Random Affine Shadowsampling
LR-ETDM	Linear Regression-Based Scheme for Detection of Energy Theft and Defective Smart Meters
LReLU	Leaky Rectified Linear Unit

LSTM	Long short-time memory
LV	Low voltage
MAE	Mean absolute error
MAP	Mean average precision
MAPE	Mean absolute percentage error
MCC	Matthews correlation coefficient
MCT	Minority Cloning Technique
MCNN-BiGRU	Multiscale convolutional neural network-bidirectional gate recurrent unit
MCU	Microcontroller unit
MDMS	Meter Data Management System
MDP	Minimum detectable power
ML	Machine learning
MLP	Multilayer perceptron
mRMR	Minimum redundancy maximum relevance
MSE	Mean squared error
MV	Medium voltage
MVD	Medium voltage distribution
NaN	Not a Number
NAN	Neighbourhood Area Network
ND-CP	NTL detection contrastive prediction coding
NILM	Non-intrusive load monitoring
NIST	National Institute of Standards and Technology
NPV	Negative predictive value
NTL	Non-technical losses
NTLD	Non-technical losses detection
OC-SVM	One-class support vector machine
OPF	Optimum path forest
OS-CNN	Omni-Scale convolutional neural network
P2P	Peer to peer
PCA	Principal Component Analysis
PCHIP	Piecewise Cubic Hermite Interpolating Polynomial
PDC	Phasor data concentrator
PELT	Pruned Exact Linear Time

PF	Power factor
PFSC	Data preparations, first and second order classification
PHED	Port Harcourt Electricity Distribution Company
PLC	Power Line Carrier
PMU	Phasor measurement unit
PPV	Positive predictive value
PR-AUC	Area under the precision-recall curve
PReLU	Parametric Rectified Linear Unit
ProWSyn	Proximity Weighted Synthetic Oversampling
PSTN	Public Switched Telephone Network
RAM	Random access memory
RBFK-SVM	Radial basis function kernel support vector machine
RDAE-AG-TripleGAN	Relational denoising autoencoder attention guided triple generative adversarial network
ReLU	Rectified Linear Unit
ResNet	Residual network
RF	Random forest
RFID	Radio frequency identification
RICA	Reconstruction independent component analysis
RMSE	Root mean squared error
RMSProp	Root Mean Square Propagation
RNN	Recurrent neural network
ROBC	Random oversampling using both classes
ROC	Receiver operating characteristic curve
ROS	Random oversampling
ROSE	Random Oversampling Examples
RS	Random sampling
RTC	Real time clock
RTU	Remote terminal unit
RUS	Random undersampling
SAE	Sparse auto encoder
SAGAN	Self-attention generative adversarial network
SALM	SMOTEENN-AlexNet-LGB
SG	Smart Grid
SGCC	State Grid Corporation of China

SGD	Stochastic Gradient Descent
SHAP	SHapley Additive exPlanation
SM	Smart meter
SMOBD	Synthetic Minority Oversampling Borderline-Data
SMOTE	Synthetic minority oversampling technique
SMOTEENN	Synthetic minority oversampling technique and edited nearest neighbour
SMOTE-NM	synthetic minority oversampling technique with near miss
SMOTE-Tomek	Synthetic minority oversampling technique and tomek links
SMS	Short Message Service
SPRC	sequential preprocessing, resampling, and classification
SRM	Structural risk minimization
SSA	Salp swarm algorithm
SSA-GCAE-CSLSTM	Combination of SSA, GCAE, and CSLSTM
STL	Seasonal and trend decomposition using loess
SVM	Support vector machine
T&D	Transmission and distribution
Tanh	Hyperbolic tangent
TBSSVM	Tomek link borderline synthetic minority oversampling technique with support vector machine
TCN	Temporal convolutional network
TCN-EMLP	Temporal convolutional network with enhanced multilayer perceptron
TEDAŞ	Turkish Electricity Distribution Company
TL	Technical losses
TLENET	Time Series Lag Embedded Network
TLGRU	Theft attacks-based LSTM and GRU
TLSGAN	Time least square generative adversarial network
TN	True negative
TNR	True negative rate
TP	True positive
TPR	True positive rate
TPU	Tensor processing unit
UBS	Uncertainty-based sample
VGG-16	Visual Geometry Group with 16 deep layers

WAN	Wide Area Network
WDCNN	Wide and deep convolutional neural network
WiMAX	World Interoperability for Microwave Access
WLS	Weighted-least squares
XGBoost/XGB	Extreme gradient boosting

CHAPTER 1

INTRODUCTION

1.1 Background

Electricity is an indispensable commodity (Hassan et al., 2022:2; Khalid et al., 2024:1), and the root of modernity (Breeze, 2014:1; French, 2017:123). It is an invisible commodity that is largely produced based on the precept of Faraday’s law of electromagnetic induction, and conveyed through wires (David, 2017:1-2; French, 2017:4). Electricity is the most significant blessing that science has bestowed on humanity (Aziz et al., 2020; Pamir, Javaid, Qasim, et al., 2022:56863). It is also the most versatile (Porcu et al., 2021:8), and the most useful and used source of energy in our everyday lives (Aslam, Javaid, et al., 2020:1). The unique commodity called electricity is fundamental to modern inventions and civilizations (Edris & D’Andrade, 2017:37).

Electricity need is universal, and its usage traverses almost all occupations and endeavours (Hassan et al., 2022:2). Human daily activities in the modern world strongly depend on the availability of electrical energy (Stracqualursi et al., 2023:1; Iftikhar et al., 2024:01). The modern-day technology and innovations like electric vehicles (EVs), electric trains, computers, Internet, broadcast media, telecommunications, medical equipment, etc., would not have been possible without electricity (Breeze, 2014:1, 3). Electricity plays an invaluable role for a sound, successful, and sustainable economy (Nayak & Jaidhar, 2023:1). Apart from the economy, national security and the health and safety of citizens are also dependent on reliable electricity (USDOE, 2008; Casey et al., 2020). No country in the world could develop without a reliable electricity (Aliyu et al., 2013:354).

However, like any other essential and valuable commodity, electricity is being stolen and its continuous availability threatened (Stracqualursi et al., 2023:1; Wabukala et al., 2023:3). One of the causes of electricity crisis is electricity losses, which especially occurs when the energy generated falls short of the energy consumed (Fragkioudaki et al., 2016:44; Iftikhar et al., 2024:01). Electricity theft (ET) is the principal contributor to electricity losses that threaten the steady availability of electricity supply (Saeed et al., 2020:1; Barros et al., 2021:1). ET is the illicit act of using electricity with the primary intent of avoiding utility charges (Yurtseven, 2015:70).

ET pervades all electric systems and no power system could be 100% protected from it

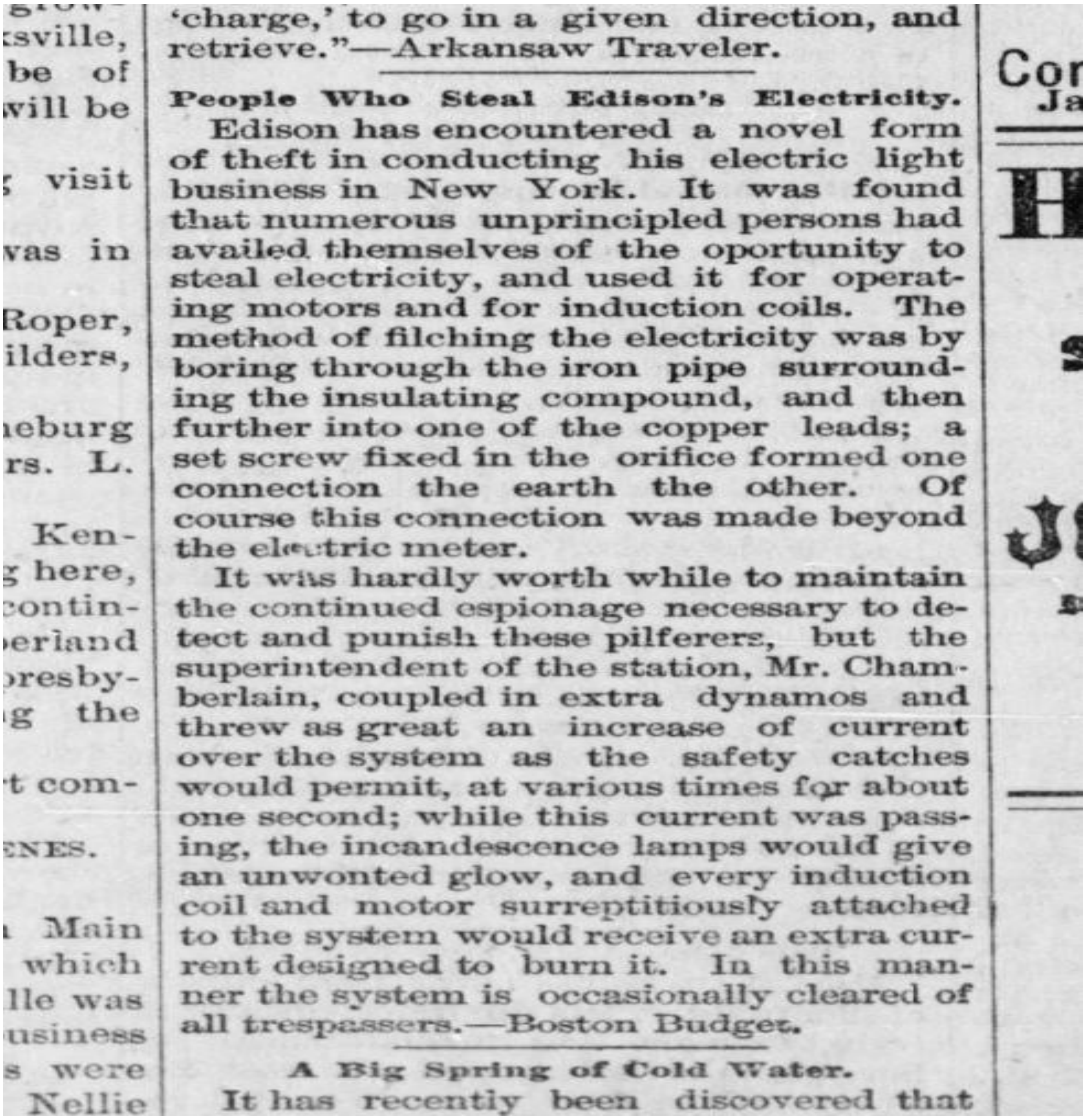
(Smith, 2004:2067). Consequently, it causes dire financial and technical consequences (Messinis & Hatziargyriou, 2018:251). ET is a wearisome social iniquity (Afridi et al., 2021:1829) which has been officially declared a felony in Liberia (Dodoo, 2022), and has also been decreed a sin in Pakistan (Reuters, 2009; Depuru et al., 2011a:1012). Electricity is one of the most-plundered commodities globally (Appiah et al., 2023:1), such that, it is ranked the third most-stolen commodity in the world after credit-card details and cars (Ahmed et al., 2022:579). The detection of this peculiar stealing instance is one of the biggest challenges confronting all electric utilities worldwide (Kwarteng et al., 2023:7).

Stolen electricity is the power supplied but which the electric utilities cannot account for, since the electricity filchers took the commodity without the awareness of the utility providers (Otcenasova et al., 2019:6). Such act of circumventing the utilities is illegal, a serious crime that is punishable under the law. Theft of electricity is malevolent, a deliberate act of swindling the utilities (Kambule & Nwulu, 2021:42; Hassan et al., 2022:2).

1.1.1 History of electricity theft

ET in the power sector is an age-long problem prevalent in all electric systems all over the world (Stracqualursi et al., 2023:1). It is a tricky scourge which all electric utilities have been grappling with for over a century. The first reported case of ET took place in New York City, United States, in the late nineteenth century, specifically in the year 1886 (Glauner, 2019:2; Xia et al., 2022:274). It was at this period that the commercialization of electricity started when electric utilities began to distribute electricity for public consumption (Glauner, 2019:2).

The Daily Yellowstone Journal was the official newspaper of Custer County located in Miles City, Montana, United States. The newspaper reported the first ET incident in one of its articles on page two of its publication on Saturday 27 March 1886 (Daily Yellowstone Journal, 1886:1-2). The article which reported the incident was titled “People Who Steal Edison’s Electricity”. Espionage to uncover suspected pilferage of electricity was carried out by the Edison power station, and an occurrence of ET was established. As a measure to mitigate the theft, the superintendent of the power station sent power surge into the distribution lines to destroy the illegally connected loads impinging on the lines (Pickering, 2016; Megger, 2020). The exact portion of the article relating the theft of Edison’s electricity in 1886 (Daily Yellowstone Journal, 1886:2) is shown in Figure 1.1.



'charge,' to go in a given direction, and retrieve."—Arkansaw Traveler.

People Who Steal Edison's Electricity.

Edison has encountered a novel form of theft in conducting his electric light business in New York. It was found that numerous unprincipled persons had availed themselves of the oportunity to steal electricity, and used it for operating motors and for induction coils. The method of filching the electricity was by boring through the iron pipe surrounding the insulating compound, and then further into one of the copper leads; a set screw fixed in the orifice formed one connection the earth the other. Of course this connection was made beyond the electric meter.

It was hardly worth while to maintain the continued espionage necessary to detect and punish these pilferers, but the superintendent of the station, Mr. Chamberlain, coupled in extra dynamos and threw as great an increase of current over the system as the safety catches would permit, at various times for about one second; while this current was passing, the incandescence lamps would give an unwonted glow, and every induction coil and motor surreptitiously attached to the system would receive an extra current designed to burn it. In this manner the system is occasionally cleared of all trespassers.—Boston Budget.

A Big Spring of Cold Water.

It has recently been discovered that

Figure 1.1: Newspaper report on the stealing of Edison's electricity in 1886

(Daily Yellowstone Journal, 1886:2)

The content of the newspaper article is transcribed as follows:

"Edison has encountered a novel form of theft in conducting his light business in New York. It was found that numerous unprincipled persons had availed themselves of the opportunity to steal electricity, and used it for operating motors and for induction coils. The method of filching the electricity was by boring through the iron pipe surrounding the insulating compound, and then further into one of the copper leads; a set screw fixed in the orifice formed one connection the earth the other. Of course, this connection was made beyond the electric meter.

“It was hardly worth while to maintain the continued espionage necessary to detect and punish these pilferers, but the superintendent of the station, Mr. Chamberlain, coupled in extra dynamos and threw as great an increase of current over the system as the safety catches would permit, at various times for about one second; while this current was passing, the incandescence lamps would give an unwonted glow, and every induction coil and motor surreptitiously attached to the system would receive an extra current designed to burn it. In this manner the system is occasionally cleared of all trespassers.”

The confirmation of this maiden ET incident in 1886 by the Edison power station launched the era of the ET menace. Since then, the ET problem has however proven to be endemic in all power systems worldwide, such that, the scourge can no longer be completely eradicated in any electricity grid, but could only be managed by continual mitigation (Lewis, 2015:128-129; Kocaman & Tümen, 2020:1). The Edison power station was the first electric utility in the world (Malik, 2013:140; Tuballa & Abundo, 2016:715). More on the Edison power station concerning its establishment, characteristics, and the associated tussle for survival and supremacy in the face of competition are further discussed under the review of electricity grid in Sections 2.2.1, 2.2.1.1, 2.2.1.2 and 2.2.1.3 of Chapter 2.

1.1.1.1 Some other early instances associated with electricity theft

In some of the earlier court judgements in Germany, ET was not considered a crime. An example of this was in the two rulings of the Imperial Court of Justice of Germany in 1896 and 1899 (Glauner, 2019:2). The Court ruled that, there was no inclusion of ET in the German Criminal Code. The Court in its adjudications believed that electricity could not actually be stolen since it was not regarded as a physical object, hence the offence relating to pilfering of electricity could not be subsumed as theft. Subsequently, the German Parliament brought up a new law in 1900 to criminalize ET and made it punishable under the law (Schuster, 1901:120-121; Glauner, 2019:2-3). The new law stipulated a five-year imprisonment and a fine as punishments for electricity thieves.

In another jurisdiction, the issue of ET had already been addressed in the criminal law of France. The Court of Cassation of France had earlier ruled that ET had been accommodated in the extant criminal law of the country, and that there was no need to enact a new law to criminalize it (Glauner, 2019:3). Like in the previous situation in Germany, the United Kingdom (UK) also believed that electricity could not be stolen, since it is not a physical or concrete substance (Dick, 1995:91). However, the Theft Act 1968 was eventually enacted in the UK to declare ET as an offence.

1.2 Technical and non-technical losses

The total amounts of electricity generated from the power stations have always not been same as the net electricity distributed for consumption (Karimi et al., 2020; Adam et al., 2021). The difference between the electricity generated and distributed for consumption in the power system is known as loss (Adam et al., 2021). Although, a few inevitable energy losses are peculiar to the power system but most of the energy losses in an electric system are artificially induced. Electrical energy losses are energy not delivered for consumption from the supply chain, and/or not paid for by the consumers. Technical losses (TL) and non-technical losses (NTL) are the two types of energy losses in power systems (Khalid et al., 2024:2; S. Zhu et al., 2024:15477). These losses take place during the generation, transmission, and distribution of electricity.

TL are inherent natural losses in the power system, which inevitably occur due to the dissipation of electrical energy in the power system components like generators, transmission and distribution (T&D) lines, transformers, metering devices, and other equipment which make up the power system (Karimi et al., 2020; Poudel & Dhungana, 2022:109). These power components are all the necessary equipment used in accomplishing the T&D of electricity (Viegas et al., 2017:1260). There are also TL due to heat dissipation by virtue of the material properties of the power system components and their resistances to the flow of current (Wu et al., 2018:3073). In addition, there are also TL by irradiation (Viegas et al., 2017:1256).

TL are systemically caused by intrinsic or internal factors within the power grid (Hassan et al., 2022:2). TL are inevitable system losses (Aslam, Ahmed, et al., 2020:221768) which could be reduced by routine preventive maintenance with qualitative and advanced T&D technology (Smith, 2004:2068). Scheduled maintenance, while ensuring quality power components, also improves system efficiency. Utilities should always improve and maintain the efficiency of their power systems to ensure they operate at a power factor (PF) greater than 0.95, in order to reduce the TL in their networks (ESI Africa, 2019). PF whose values range between 0 and 1, is the proportion of the real or active power consumed by devices to that of the apparent or total power supplied to the devices, and is used as indicator to show the efficiency level of power distribution systems (Ramos et al., 2018:679; Saeed et al., 2020:5). PF values closer to 1 indicates higher efficiency and vice versa. The losses in the generation subsystem of the power system are technical, and could be defined and precisely computed (Tatte et al., 2019:175) by using the fundamental laws of electrical engineering (Osypova, 2020:11).

In contrast to TL, NTL are avoidable non-natural losses caused by deliberate human dishonest actions, errors and other third-party activities external to the power grid (Otcenasova et al., 2019:6; Poudel & Dhungana, 2022:110). Since the causes of NTL are multifarious in nature, hence NTL cannot be represented as a function of specified actions (Depuru et al., 2011a:1007). NTL take the largest portion of the cumulative electrical losses in the power system (Petrlik et al., 2022:420). NTL occur both in Smart Grid (SG) and conventional electricity grid systems. However, the SG with its embedded smart meters (SMs) in the advanced metering infrastructure (AMI) significantly prunes NTL to an appreciable degree when compared with the conventional grid, but with the introduction of novel security risks (Shahzadi et al., 2024:1).

Meanwhile, the losses in the T&D networks of the power grid are a combination of TL and NTL (Lewis, 2015:122; Viegas et al., 2017:1256; Onat, 2018:165). Unlike the generation losses which could be technically determined, T&D losses cannot be precisely determined from the amount of energy supplied from the power plants to the distribution feeders (Tatte et al., 2019:175). This fundamental characteristic clearly confirms the involvement of NTL in the T&D of electricity, and to the total amount of energy losses in the power system. Usually, there is a need to firstly compute the value of TL before the determination of the approximate value of NTL in the T&D networks (Viegas et al., 2017:1256).

In very efficient systems like in the US and Western Europe, T&D losses are less than 6%, which includes ET of around 1-2% (Smith, 2004:2070; Yurtseven, 2015:70). T&D losses in less efficient systems are around 9-12% and over 15% in inefficient systems (Smith, 2004:2070). NTL proportions are up to 30% of the total electricity generated in countries like Bangladesh and Türkiye (Turkey) (Kambule & Nwulu, 2021:42), up to 40% of the overall electricity distributed in countries like India, Brazil, Lebanon and Malaysia (Glauner et al., 2016:254; Glauner et al., 2017:761; Kambule & Nwulu, 2021:43), and up to 50% of the entire electricity generated in the sub-Saharan Africa (Lepolesa et al., 2022:39638).

The T&D networks of the electricity system are divided into low voltage (LV), medium voltage (MV) and high voltage (HV) electric networks (Althobaiti et al., 2021:159294). To attain these voltage levels, the T&D voltages are being transformed. Transformation is the use of transformers in stepping up and/or down of electrical voltages before electricity transportation (Jamil & Ahmad, 2019:454). The HV transmission networks are used to transmit power over longer distances to primary distribution substations where voltages are stepped down to MVs via the primary distribution transformers. MVs are transported to the secondary distribution substations where they are further stepped down by secondary distribution transformers to LVs and supplied to end users for consumption via LV distribution networks. Figure 1.2 shows the different kinds of TL and NTL in the power system.

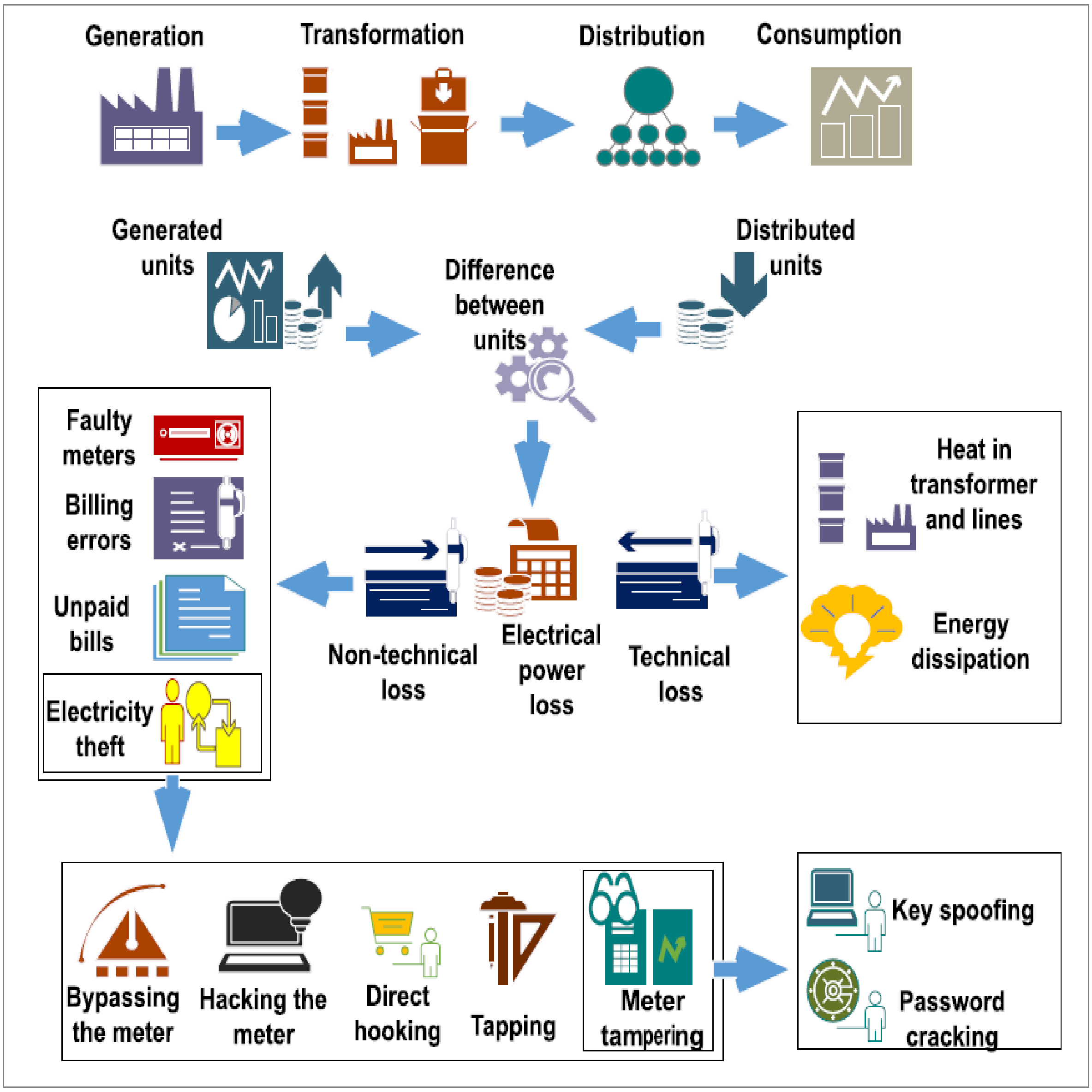


Figure 1.2: Losses in the power system

(Aldegheishem et al., 2021:25038)

NTL are primarily domiciled in the LV distribution networks (Adam et al., 2021) and hence cause serious problems for the electricity distributors. ET is exclusive to LV distribution networks, since the distribution grids are more prone to being affected by illegal activities. LV networks are more attractive to electricity thieves because voltages at this level of the grid may not be retransformed before being put to direct use and are also safer when compared with the MVs and the HVs. The MV and HV networks of the power system are not so susceptible to ET because of the fatal risk of electric shock associated with voltages at these levels. This is the obvious reason electricity thieves avoid venturing into theft at such more-dangerous voltage levels. Besides the fatal risk of electric shock involved, MVs and HVs still need to be transformed before being put to direct use.

Aside the fact that TL are inherent to the electric system, errors in technical-loss calculations also contribute to NTL (Yip, Wong, et al., 2017:230; Osypova, 2020:12-13). As previously averred, majority of the losses in the electricity system is owing to NTL (Aslam, Ahmed, et al., 2020:221768; Petrlik et al., 2022:420); therefore, regardless of the contribution of TL to the power system losses, mitigating NTL is more significant and brings about major reduction in the overall power losses in the electricity grid (Fragkioudaki et al., 2016:44). Significant degree of NTL triggers the need to generate more power to compensate for the resulting power inadequacies caused, but increasing generation is not as cost-effective as reducing NTL in the power distribution system (Abaide et al., 2010:1).

NTL are commercial losses (Poudel & Dhungana, 2022:109; Kwarteng et al., 2023:7). Commercial losses, as the name infers, are NTL associated with the commercialization of electricity (Ramos et al., 2011:181), which also cause disruptions in commercial activities by slowing down the production of goods and services (Osypova, 2020:11). Commercial losses are the electrical energy that the utilities received for distribution and eventually pushed to the consumers, but which was not billed for or invoiced owing to ET (Osypova, 2020:11). The total amount of lost energies in an electricity system is determined through the addition of TL and NTL (Poudel & Dhungana, 2022:109), and is also calculated by subtracting the total electricity billed or sold to the consumers from the total electricity supplied or fed into the power distribution system (Pereira & Saraiva, 2021:1). NTL could only be estimated by finding the difference between the total energy losses and the TL (Poudel & Dhungana, 2022:110), but cannot be expressly calculated like TL (Depuru et al., 2011a:1007).

NTL is otherwise known as ET (Jamil & Ahmad, 2019:454). NTL is the common term used primarily to refer to ET and other irregularities in power distribution systems (Yakubu et al., 2018:611). This is further established in Figure 1.2 where NTL is described as ET. NTL is alternatively known as ET because ET is the primary and predominant cause of NTL, and hence takes the largest percentage in its constitution (Appiah et al., 2023:1). To affirm the fact that ET is the prevailing cause of NTL, the authors in Dimf et al. (2023:1) have also asserted that about 80% of NTL in power systems are affiliated to ET. In other words, ET contributes the greatest amount of NTL in electricity systems (Appiah et al., 2023:1). It is on this ground that both NTL and ET are interchangeably used in the literature (Kgaphola et al., 2024), and will also be used synonymously in this thesis.

Apart from NTL being referred to as ET, energy theft (Mohammad et al., 2023) and power theft (Dimf et al., 2023) are alternative terms used for ET in the literature. Like a typical NTL, ET cannot be accurately calculated or measured by either using formulas or electric meters, but could only be estimated (Dick, 1995:90; Smith, 2004:2070; Osypova, 2020:11).

1.3 Forms of electricity theft

Electricity abstraction is manifested in four ways in all power systems. ET could be in the form of stealing, fraud, billing irregularities, and non-payment of electricity bills (Onat, 2018:166; Jamil & Ahmad, 2019:454). All these forms or types of ET are interrelated because they all cause revenue losses to the utilities (Lewis, 2015:121). Electricity customers engage in one form of theft or the other in a bid to lower or to entirely avoid electricity bills (Depuru et al., 2011a:1010). Conscious dubious actions or errors which are external or extrinsic to the electricity grid are responsible for NTL (Poudel & Dhungana, 2022:110). All the various forms of ET or NTL are represented in Figure 1.3. The figure is a schematic model showcasing all the probable sources of NTL, and meant to simplify and aid quick overview of the entirety of the different forms of ET available in the power system.

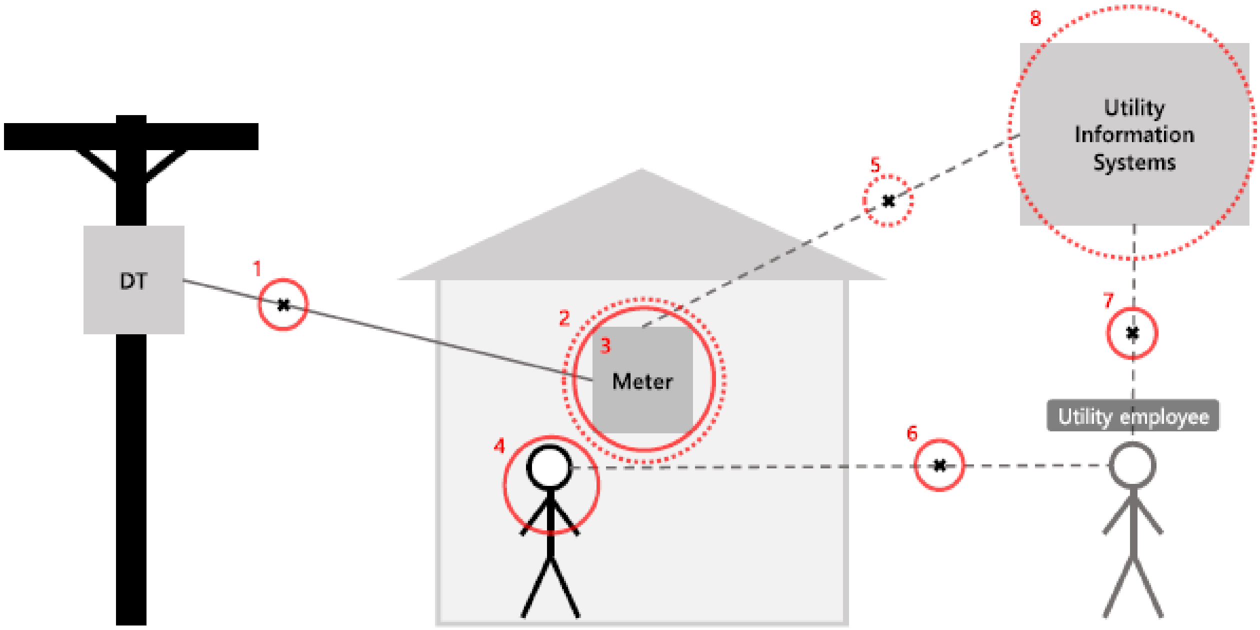


Figure 1.3: Sources of NTL or NTL vulnerability points

(Viegas et al., 2017:1258)

Viegas et al. (2017:1258, 1260) have shown in Figure 1.3 that the unbroken line depicts the physical connection of electricity from the pole-mounted distribution transformer, while the broken or dashed lines are the channels of communication. There are eight points or sources of NTL labelled in the figure. Those points are the attack or vulnerability points at the distribution line and/or service cable before the meter, at the meter in the premises of the customer, and at areas which affect billing by the utilities.

Point 1 in Figure 1.3 depicts the distribution line that supplies the premises of the electricity customer; point 2 represents the software of the customer's meter; point 3 represents the physical hardware and components of the electric meter; point 4 refers to the electricity customer; point 5 denotes the communication link between the meter and the electric utility; point 6 represents the interaction or relationship between the utility employees and the electricity customers; point 7 is the point of communication or interaction between the utility and its employee; while point 8 represents the information systems of the electric utility (Viegas et al., 2017:1260). Electricity pilferers achieve their devious objectives by leveraging on these vulnerability points at various network levels of the electricity grid to steal the priced commodity.

1.3.1 Stealing

Stealing of electricity occurs when the electricity users rig wires and connect directly to the distribution lines; or by way of bypassing the electric meters to connect indirectly to the utility distribution lines through the service cables or the cut-out fuses (Mehdary et al., 2024:1). Stolen electricity is such that the supposed units associated with consumptions at the points where the electricity is being abstracted are completely unregistered, and such consumptions are in essence utterly unknown to the utilities (Winther, 2012:111-112). Stealing is attributable to physical attacks on the grid.

Point 1 in Figure 1.3 is before the meter, and it is a depiction of the distribution lines which supplies the homes of electricity customers. A real illustration of the scenario in point 1, where electricity is being stolen by hooking illegal wires directly on the distribution lines is shown in Figure 1.4. Lewis (2015:119, 121) calls these Illegal wires “throw-ups”. Throw-ups are also known as “spider webs” (Smith, 2004:2069; Lewis, 2015:119). Throw-ups are illegal-wire connections on the grid distribution lines used to siphon electricity (Lewis, 2015:119, 121, 129, 133).

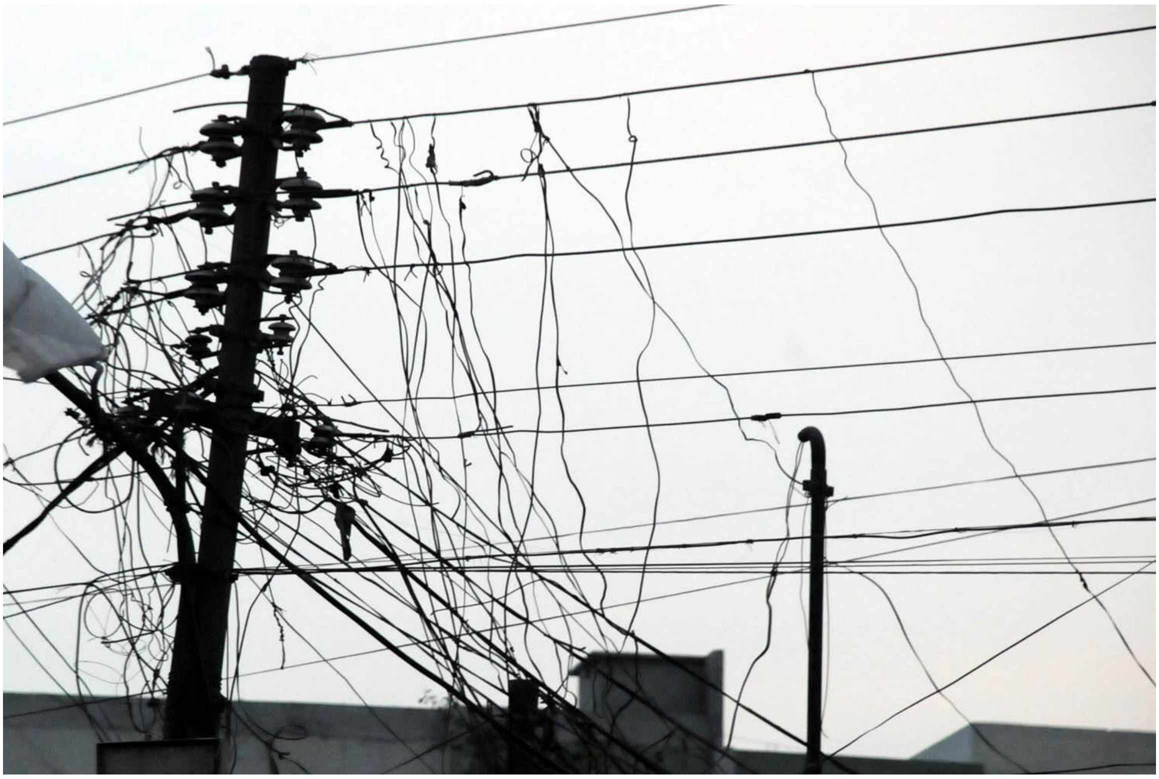


Figure 1.4: Stealing electricity directly from the distribution lines via throw-ups (Express Tribune, 2016)

Apart from throw-ups on the distribution lines, electricity is also being stolen before the meter within the consumers' premises by bypassing the electric meter as shown in Figure 1.5. The red cables in the figure were used to bypass the meter. Bypassing the meter is the act of circumventing the electric meter and tapping power directly through the service cables coming from the distribution lines to the consumers' premises. The electricity consumed at the point of bypass is not registered as the electric meter installed after this point is oblivious of those consumptions taken at that point. Power is rerouted to an alternate path at the point of bypass, and such renders the meter redundant as its primary essence of registering energy consumptions has thus been defeated.

Another method of bypassing the meter, especially via electromechanical energy meters, is by unconventionally connecting the load between the phase (live wire) from the meter and a separate wire attached to the earth (i.e., earth wire). This earth wire is used as a return path instead of the neutral or return wire supplied by the utilities, which normally completes the electric circuit by returning the phase current from the load to the supply source, that is, the distribution transformer (Anas et al., 2012:178; Avancini et al., 2019:711). With this method of bypassing the electric meter, the electromechanical meter considers that the electric circuit is incomplete and assumes that the voltage between the phase and the earth wire (pseudo neutral) is zero, implying that no energy has been consumed and hence, the meter registers no reading (Depuru et al., 2011a:1009).

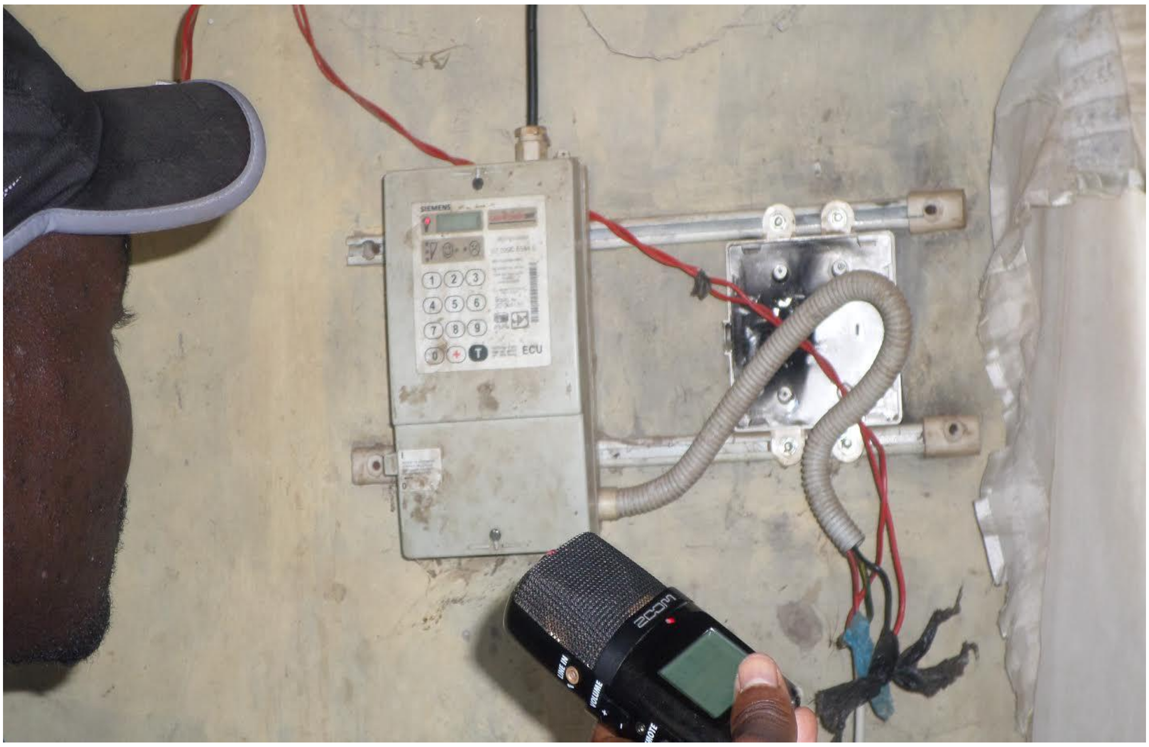


Figure 1.5: Bypassing the electricity meter

(MyBroadband, 2015)

Stealing of electricity is also achieved through the swapping of the connections of the supply or input terminals and the load or output terminals of electromechanical meters. In this method, the supply or service cables are incorrectly connected to the load terminals of the meter, while the load cables which are supposed to provide the equipment or load of the customers with electricity are also inappropriately connected to the supply terminals of the meter in an interchanged manner. The swapping of the terminals is done in a bid to give lower billable readings, as this causes the rotating disc of electromechanical meters to move in a reverse direction (Depuru et al., 2011a:1008; Anas et al., 2012:178; Avancini et al., 2019:711).

1.3.2 Fraud

Fraud covers all the sharp practices on electric meters and the utility billing systems, as orchestrated by electricity fraudsters, to give inaccurate meter readings or billings (Poudel & Dhungana, 2022:110). Fraud is committed when electricity customers intentionally deceive the electric utilities. Fraud is ascribable to physical, cyber and data attacks on electric meters and/or billing infrastructure. A popular means of defrauding the utilities is by tampering with the electric meters to hinder their normal operations (Mehdary et al., 2024:1). This is to dishonestly reduce the actual consumption levels of the meters vis-a-vis lowering the electricity bills payable to the utilities (Kambule & Nwulu, 2021:43; Poudel & Dhungana, 2022:110). By defrauding, malicious customers deliberately outwit the electric utilities, while the latter continue to believe that all is well with the metering devices of the customers, their energy billings, and the transactions between them.

Electricity fraud also involves the physical and/or hacking (remote or cyber-based attacks) the smart electric meters and/or their communication links to the utilities, in a bid to modify the normal electric readings to give lower or erroneous readings (Naeem, Aslam, et al., 2023:59496). Hacking or cyber-attack on electric meters is exclusive to SMs and its communication infrastructure in SG. Cyber-attack on SMs and their communication links to the utilities is a novel form of attack due to the advent of the SG system (Aggarwal & Kumar, 2021:466). The primary aim of the cyber and data attacks is to commit electricity fraud by compromising consumers' electricity consumption data (Yan & Wen, 2021). Several methods of committing fraud through electricity meters take place at points 2, 3, 5, and 8 of Figure 1.3.

Hitting the energy meter to cause shock or damage to its inner electromagnetic coils; inserting an external object to stop the rotating disc; inverting the meter to cause it to run backwards and reversing its readings; physically obstructing the rotating disc with a foreign object; putting a magnet on the meter to affect its magnetic field lines in an effort to slow down the rotating disc of the meter or to absolutely stop the rotating disc if a strong magnet is placed on the meter (Bihl & Hajjar, 2017:274) are exclusive ways to fraudulently abstract electricity via electromechanical meters. The electromechanical meter is discussed in detail in Section 2.3.2.1 of Chapter 2.

Putting a magnet on an electromechanical meter subverts the functionality of the current sensing components of the meter and alters the magnetic flux produced by it. This affects the normal metrology of the meter by slowing down the spinning of the rotating disc, thereby giving lower than expected readings. Magnets generally affect the voltage and current sensing mechanisms of electromechanical meters by changing its electrical characteristics and cause them to malfunction by lowering or stopping (in the presence of strong magnets) the energy measurement of the meter. Voltage and current sensing mechanisms of electromechanical meters are made of magnetic materials and are therefore affected by external magnetic field which causes the meter to falter. Making changes to the internal wire connections of an electricity meter is also one of the methods of swindling the electric utilities (Bihl & Hajjar, 2017:274).

1.3.3 Billing irregularities

Irregularities in electric billings could occur for so many reasons. The most common act that ultimately leads to billing irregularities is the corruption collusion between the electricity customers and the utility employees, an act which is more popular in the developing countries (Lewis, 2015:121; Osypova, 2020:12; Ahmed et al., 2022:581). Some corrupt utility employees dishonestly register lower than the actual readings on the electric meters, because of the financial gratifications or bribes they expect in return from the electricity customers (Smith, 2004:2069; Kambule & Nwulu, 2021:43). This fraudulent association between the consumers and the utility employees leads to inaccurate meter readings, causing incomplete invoicing (Onat, 2018:166) and ultimately resulting in billing irregularities (Depuru et al., 2011a:1007). Billing irregularities could take place at points 3, 6, 7 and 8 of Figure 1.3.

Other forms of billing irregularities that contribute to NTL and loss of revenue to the utilities are energy accounting errors or billing errors, utility employees' errors in reading the electric meters or errors in meter readings owing to faulty electric meters; and estimated billings for unmetered customers or even at times for metered customers (Glauner et al., 2017:761; Kambule & Nwulu, 2021:43). Cyber-attack frauds on SG billing system as mentioned in Section 1.3.2, and customers who fail to pay their electricity bills (as described next in Section 1.3.4) also cause billing irregularities (Viegas et al., 2017:1260).

1.3.4 Non-payment of electricity bills

Like other forms of ET, non-payment of electricity bills is also tantamount to stealing electricity, since it ultimately leads to shortfalls in utility revenues (Naeem, Aslam, et al., 2023:59496). Non-payment of electric bills is a situation whereby customers do not pay the bills they owe to the electric utilities. This attitude among electricity customers is not only limited to those in developing countries, but is also a cause for concern among electricity customers in the developed countries (Smith, 2004:2069). In contrast to the unpaid electricity bills by regular customers who have been correctly charged by the utilities as discussed in this section, all the previously highlighted forms of ET in Sections 1.31, 1.32, and 1.33 all result in unbilled energy usages, as the electric utilities are completely oblivious of those consumptions. However, non-payment of billed electricity also contribute to NTL because the benefit of unpaid electricity is equal to the units of stolen electricity (Jamil & Ahmad, 2019:453). Non-payment of electricity bills occurs at point 4 of Figure 1.3.

1.4 Statement of the research problem

Electricity losses is one of the determinants of energy crisis that undermines the power grid (Fragkioudaki et al., 2016:44; Iftikhar et al., 2024:01). ET causes major power losses, financial losses and equipment damage in the electrical power system (Depuru et al., 2011a:1007). ET is a pervasive problem (Sharma et al., 2016:41), and no power system anywhere in the world is completely free from it (Smith, 2004:2067). ET hampers the reliability and sustainability of electricity grids and impedes national economic growths, causing interruptions that lead to economic downturns and job losses (Naeem, Aslam, et al., 2023:3; Huang et al., 2024:1).

Since ET cannot be totally eradicated in the power systems (Lewis, 2015:128-129; Kocaman & Tümen, 2020:1), the motivation for this research project is to profoundly detect ET in the electricity grids so as to mitigate it to the barest minimum. ET pruning is more significant and more cost-effective than generating more power to compensate for the energy losses occasioned by NTL (Abaide et al., 2010:1; Fragkioudaki et al., 2016:44).

1.5 Research aim and objectives

The aim of this research is to detect and mitigate ET in SG, by using the energy consumption data of utility consumers to develop efficient NTLD model that would achieve higher detection performances to enhance better onsite mitigation of ET. The objectives of the research are:

(a) to extensively review the existing literature on ETD or NTLD methods.

(b) conduct ETD simulations. The simulations are done primarily to improve the predictive powers or detection performances of existing ETD models in a bid to develop cost-effective and more-efficient ETD model with excellent detection performances.

(c) to prudently shortlist ET suspects and recommend them for onsite inspections, such that cost-effective manual onsite inspections of the very suspicious customers are carried out to establish the ET culprits. After the theft culprits have been established, necessary fines and other correctional measures are imposed on them by the utilities within the scope of the existing laws to further discourage such heinous acts from recurring. This measure tend to mitigate ET in power grids.

1.6 Research questions

This research project is about ETD and ET mitigation in the SG using consumers' real-world electricity consumption data. Thus, the primary research question is: "how do we detect ET better in SG?" The next crucial and complementary question to the first question would then be: "how do we mitigate ET better in SG?" After the detection of ET, the mitigation of it is the next natural priority. The latter research question is premised on the former, since the performance success achieved by the proposed ETD model would translate directly to the accomplishments attainable during onsite ET mitigation efforts. The greater the efficiency achieved by the proposed ETD model as depicted by their higher performance results, the greater the mitigation successes achievable during onsite inspections by the utility technicians or inspectors who affirm and prosecute theft culprits in a bid to mitigate the ET scourge.

1.7 Delineation of the research

This research project centres on the detection and mitigation of ET, and has precluded cybersecurity of the utility infrastructure. Probable cyber and data attacks (Yan & Wen, 2021) to the information systems of electric utilities have not been considered in this research. Electric utilities should endeavour to strengthen the security of their information systems, as SG communication systems are expected to be highly reliable and secure (Rastogi et al., 2016:14). This is to ensure that intruders whose ulterior motives of compromising, manipulating, and delivering fraudulent readings to the utilities do not gain remote access to the electricity consumption data of the customers via the SMs and their communication links in the AMI (Knapp & Samani, 2013:49-50; Viegas et al., 2017:1257). The twenty-first century SGs and their SMs should be resilient against cyber and physical attacks (Edris & D'Andrade, 2017:38; Avancini et al., 2019:712).

1.8 Significance of the research

The quality and the economy of the power system are the prime priorities of electricity providers (Rastogi et al., 2016:13). The effects of ET are highly damaging, hence, a more efficient and reliable anti-theft approach is needed (Mujeeb et al., 2020). This research project is important in that it provides the means to remarkably reduce NTL and help increase utility revenues and profits, protect honest electricity customers, improve the reliability, sustainability, and security of power systems, and thereupon save national economies (Liao, Zhu, et al., 2024:5075). The traditional manual onsite NTLD scheme, which was the only means of mitigating ET is very expensive and unattractive with many social and technical limitations (Huang et al., 2024:1; Liao, Zhu, et al., 2024:5075). ET is the major hitch plaguing the AMI and therefore calls for the development of effectual theft-detection techniques (Jiang et al., 2014:106). AI-based approach for NTLD has been the attractive choice because it renders a high hit ratio, cost-effective and efficient, and requires less manpower (Ghori et al., 2020:16033-16034; Poudel & Dhungana, 2022:110).

1.9 Contributions of the research

The primary contribution of this research project is based on the improvement of ETD efficiencies in SG. NTLD models with higher performance scores spur greater detection and subsequent reduction of NTL in the power grids. The proposed ETD model developed in this research project perform better and is more accurate in detecting ET when compared with other NTLD models presented in the previous research. The models which have been compared with the proposed model are those that have been developed using the same energy consumption dataset employed in this research in the various literature where they have been presented. The proposed NTLD model completely expunges false positives (FPs) which tend to prevent unnecessary and expensive onsite inspections (Aldegheishem et al., 2021:25051; Pamir, Javaid, Qasim, et al., 2022:56866, 56870). This is a significant improvement in what was earlier achieved in the previous research studies. Onsite inspection is a follow-up process to confirm the fraudulent electricity customers who have been pinpointed by the proposed ETD model in a quest to mitigate NTL. The greater the performance scores achieved by evaluation metrics, the more the resources saved by electric utilities on probable unnecessary onsite inspections.

1.10 Outline of the thesis

This section describes the arrangement of the thesis. This thesis is structured into five chapters. Apart from Chapter 1, which is an introduction to the research study, the remaining part of the thesis is structured as follows:

Chapter 2 expounds review of the literature on the components relating to the research. In this chapter, reviews have been made on electricity grid, electricity metering, causes and effects of ET, and the various methods used to prevent, detect, and mitigate ET.

Chapter 3 focusses on the methodology used in the modelling of the ETD system developed in this thesis.

Chapter 4 analyses the results of the NTLD experiment carried out in Chapter 3, and discusses the interpretations of the results obtained.

Chapter 5 is the final chapter, and thus signifies the closing of the thesis. The chapter entails the summary of the research findings and its contributions, and also recommends future directions that could further enhance the research results to supplement the current ETD and ET mitigation efforts.

1.11 Conclusion

This chapter introduces the concept of ET by accentuating the role of electricity in our daily lives and establishing the ET problem along with its history and forms. The research statement and questions, aims and objectives, delineation, significance, and contributions of the research were also further discussed, including how the thesis has been structured. The next chapter is a literature review on electricity grid, electricity metering, and NTL solutions. The chapter also touches on the causes, effects, detection and mitigation of ET, and established that AI-based ML techniques are the state-of-the-art approach for ETD.

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

This chapter is a review of the literature, and has been structured into three parts. The first part explores the electricity grid from the traditional grid to the current developmental state known as the Smart Grid (SG). The second part examines the evolution of electric meters from the first-invented Gardiner meter to the state-of-the-art smart meter (SM) used in SG electric systems. The last part constitutes the core of this research project, and analyses the existing detection and mitigation methods of non-technical losses (NTL) in the power grid, by surveying how electricity theft (ET) has been forestalled, determined, and curtailed. Meanwhile, the causes and effects of ET have also been discussed.

Any NTL detection (NTLD) method which may have been proposed by researchers in the field of NTLD must belong to one or a combination of the categories of NTL solutions reviewed in this chapter. However, artificial intelligence-based (AI-based) machine learning (ML) approach is the state-of-the-art and the most-efficient method used in detecting ET in power grids (Glauner et al., 2017:761; Glauner, 2019:31, 110; Ghori et al., 2020:16033-16034; Saeed et al., 2020:1; Guarda et al., 2023:4; Stracqualursi et al., 2023:12, 16; Coma-Puig et al., 2024:2704), as already established in Sections 2.4.5 and 2.4.5.1. Electricity must be generated, transmitted and distributed before it reaches the consumers, and it must also be measured to determine whether it is being stolen or not.

2.2 Electricity grid

The grid, power grid, electricity grid, electric grid, or electrical grid is one of the engineered most-complex systems in the world (Khoussi & Mattas, 2017:226). The essence of electricity grid is to deliver power from the point of generation to load centres (Breeze, 2014:6; Khoussi & Mattas, 2017:227). The basic quantities of electricity are the flowing electrons (current), and the pressure or electric potential (voltage) from the power source which propel the current through conductors. The electricity grid is also known as electric power system (Qazi, 2017:4).

Electricity grid is a critical infrastructure for the generation, transmission, and distribution of electrical energy. The grid consists of power supply components like the power generators, transmission lines, transformers, and the distribution lines. Power is conveyed directly from the power generation plants through the transmission lines and substations to the consumers at their various premises (Khoussi & Mattas, 2017:226-227; Kathiresh & Subahani, 2020:177). Electricity grid is the interconnection of these power supply components or the interconnection of power subsystems from generation where the power is being produced, through the transmission lines and distribution lines, to consumption or load centres where the power is being put to direct use, covering broad geographical area and forming a large electric network (Qazi, 2017:4). This large electric network is usually being referred to as the "largest machine" in the world owing to its immense size (Porcu et al., 2021:8).

Electricity consumers derive all their power needs from the grid, and connect to the grid whenever they switch on their bulbs or plug-in their residential, commercial, or industrial devices (Erenoğlu et al., 2019:14).

2.2.1 The pioneer electricity grid

After Thomas Edison succeeded in making the first commercially viable incandescent electric lamp in 1879 (Sulzberger, 2003b:64; Lobenstein & Sulzberger, 2008:84), his power station known as the Pearl Street Station which was located in lower Manhattan, New York City, United States, began to generate electricity on 4 September 1882 (Lobenstein & Sulzberger, 2008:86; Sulzberger, 2013:78; Bîrleanu et al., 2019:609).

Edison who in 1880 decided to construct a permanent power station (the Pearl Street Station), had purposely founded a corporation called Edison Electric Illuminating Company of New York in the same year, under which to carry out the proposed power station project (Rutgers, 1882:423; Sulzberger, 2003b:65; Lobenstein & Sulzberger, 2008:85; Sulzberger, 2013:78). Edison's decision to establish the Pearl Street Station was primarily to commercialize his invented incandescent lamps or bulbs, by generating and distributing electricity to power the invented bulbs for his prospective customers (Sulzberger, 2003b:64; Tuballa & Abundo, 2016:715). The commencement of operations by the Pearl Street power generating station on 4 September 1882 launched the era of commercial incandescent electric lighting (Hughes, 1958:143). Incandescent lamps are the predecessor light bulbs typical of the more-efficient and longer-lasting modern energy-saving light bulbs used today (Bîrleanu et al., 2019:609).

The Pearl Street Station was a low-voltage (LV) direct current (DC) power utility (Sulzberger, 2003b:64), and the first electric power station in the world (Malik, 2013:140).

The Station, which cogenerated electricity and heat, was also the first commercial and permanent central power plant in the world (Lobenstein & Sulzberger, 2008:85-86; Lovett, 2013:1; Sulzberger, 2013:76, 78). Figure 2.1 shows the sketch of the exterior view of the Pearl Street Station of the Edison electric utility. The horse-drawn cart seen in front of the power-station building in the figure was used to transport coal to the power plant for the running of the steam engines, which was used to turn the dynamos. The coal was taken into the power station through a sidewalk vault into the coal storing room known as cellar (Essig, 2009:63-64).

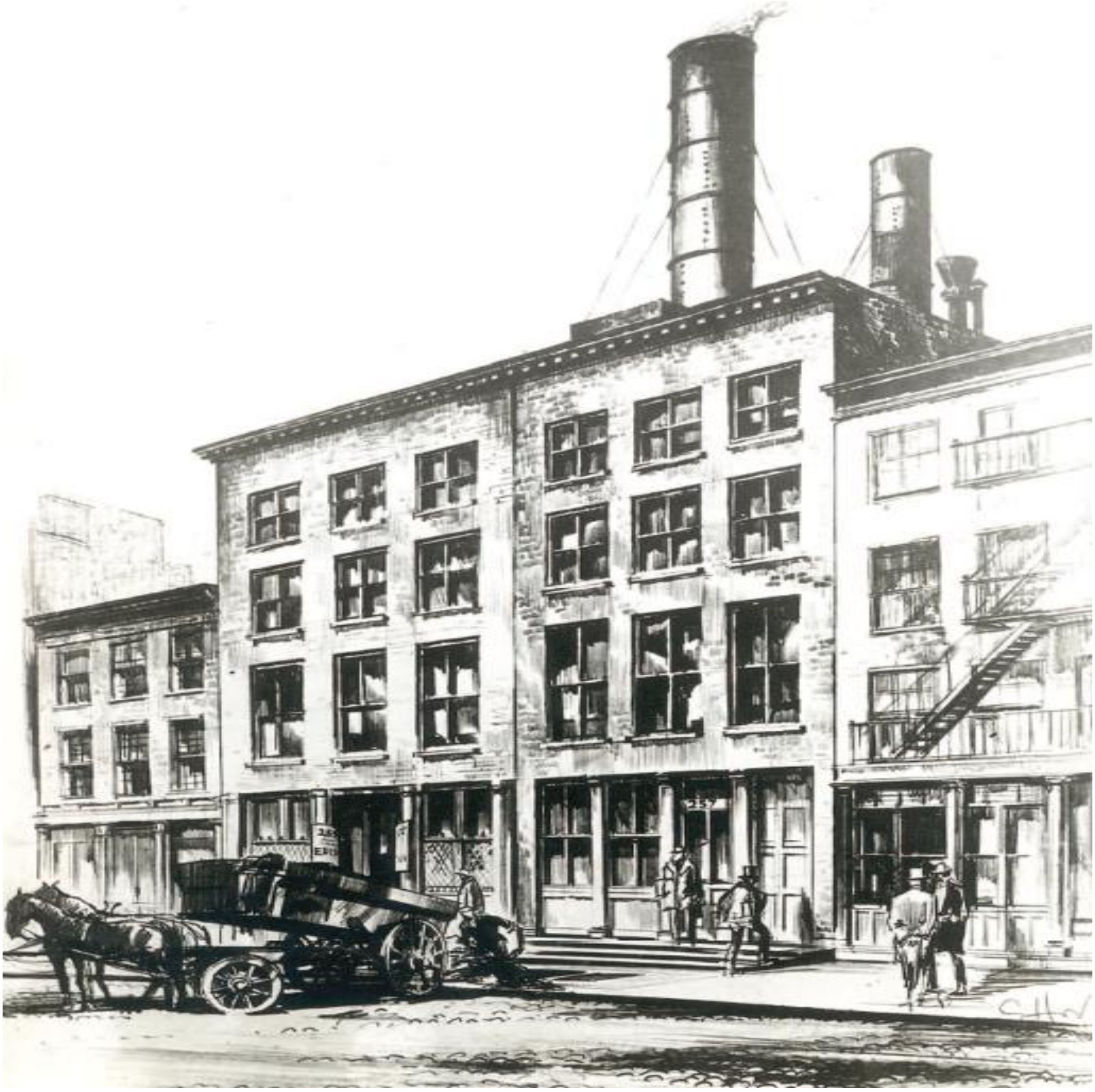


Figure 2.1: Exterior-view sketch of the Pearl Street Station

(Sulzberger, 2013:76)

Dynamos were the earliest outmoded DC generators used to produce commercial DC electricity before the advent of alternating current (AC) generators or alternators used to produce large-scale AC electricity (Owens, 2019:1). Alternators or AC generators replaced the dynamos owing to the advantages of AC over DC as discussed in Section 2.2.1.3. Electricity has been produced in the form of DC or AC and conveyed through cables for consumption by the end users (Erenoğlu et al., 2019:14). DC flows in one direction while the AC is sinusoidal and thus flows back and forth (Sulzberger, 2003b:66).

Figure 2.2 shows the sketch of the dynamo room of the Pearl Street generating station of the Edison electric utility. Each of the six dynamos in the room had a capacity of 100 kW and could supply up to 1200 lamps at 110 Vdc when it began operation (Rutgers, 1882:425; Lobenstein & Sulzberger, 2008:85-86). As apprised in the description of Figure 2.1 above, coal-fired steam engines were the prime movers used to drive the DC dynamos of the Edison power plant (Lobenstein & Sulzberger, 2008:85; Tuballa & Abundo, 2016:715).

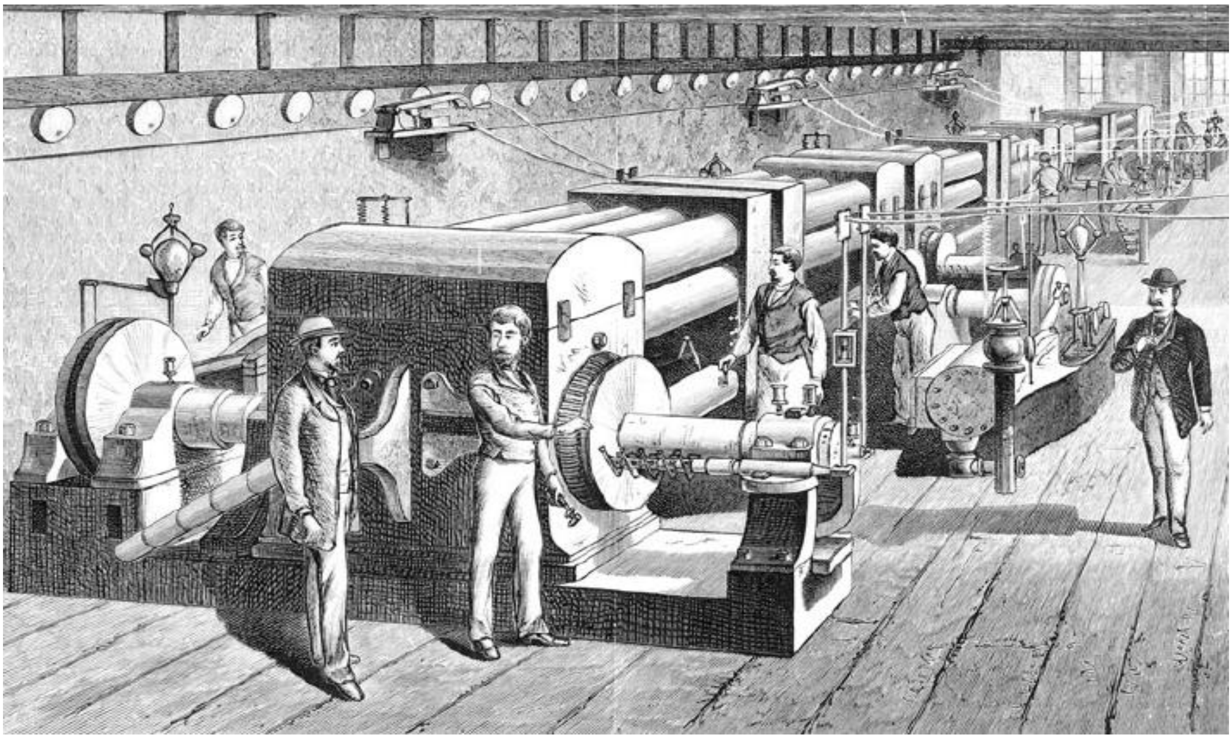


Figure 2.2: Sketch of the dynamo room of the Pearl Street Station

(Rutgers, 1882:425)

The distribution system for Pearl Street Station was an underground distribution system as shown in Figure 2.3. It consisted of manhole for underground access, and conduits where the distribution cables of the electric utility were laid for onward delivery of electricity to the consumers. The Edison Pearl Street central power generating station, with its distribution system formed the revolutionary first electricity grid system (Tuballa & Abundo, 2016:715). The Edison electric utility which initially served 85 customers with about 400 lamps on the day it commenced operation (Lobenstein & Sulzberger, 2008:86) was an original model, a foundational prototype and the evolutive forerunner of the intricate electricity grid system of today, comprising central power generation, distribution, and consumption (Tuballa & Abundo, 2016:715; Erenoğlu et al., 2019:12).

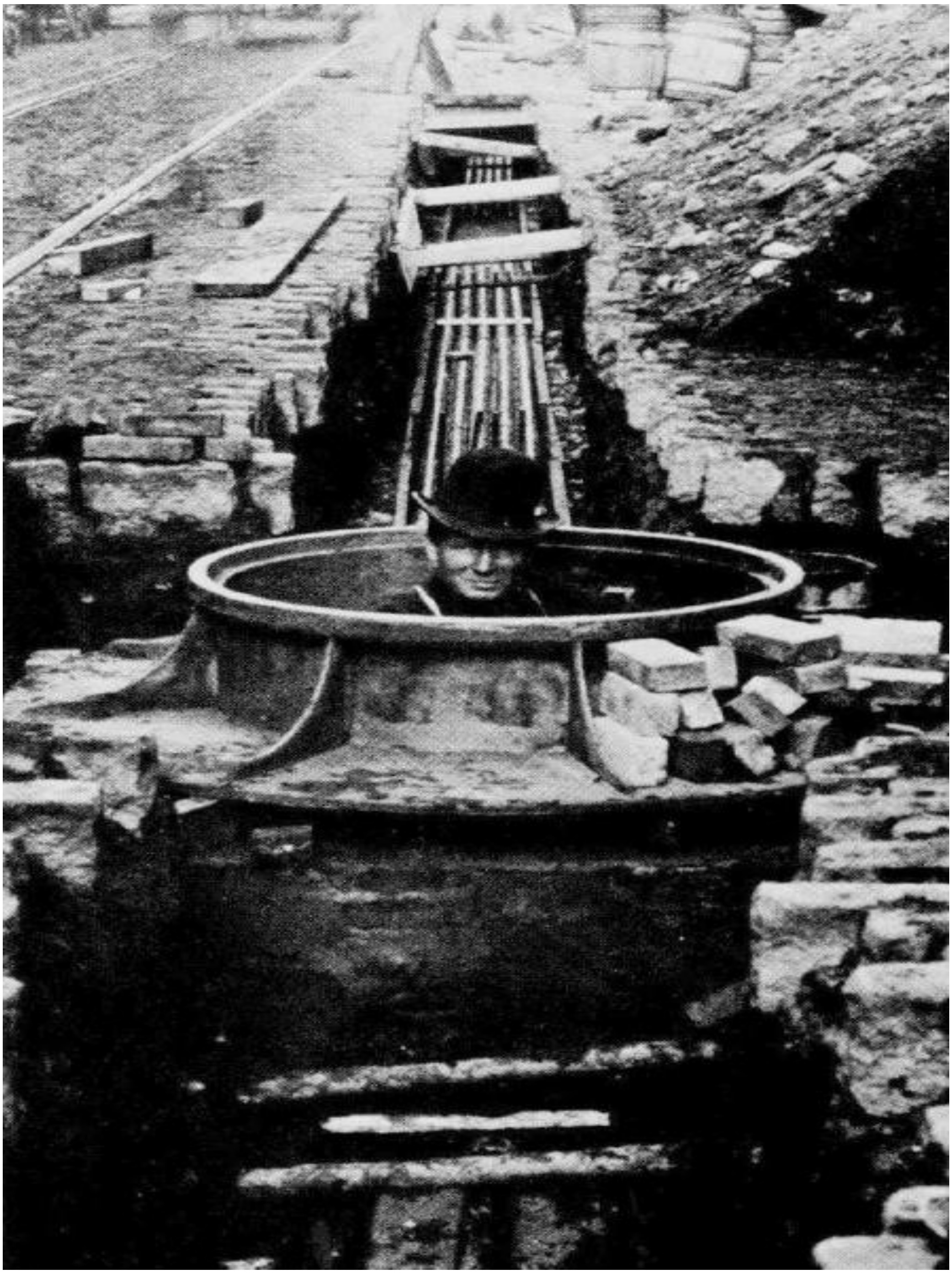


Figure 2.3: The underground distribution system of the Pearl Street Station

(Lobenstein & Sulzberger, 2008:86)

Edison’s electricity was reportedly stolen in New York in 1886 as discussed in Section 1.1.1 of Chapter 1. It was the first-ever case of ET incident that had been reported. That incident established that the first electric power system (Malik, 2013:140; Tuballa & Abundo, 2016:715) did not escape the plague of ET (Glauner, 2019:2; Megger, 2020). Similarly, all other power systems of today have also not been spared of the endemic menace (Winther, 2012:111; Sharma et al., 2016:40). All electric utilities worldwide are therefore battling with the daunting ET problem (Yip, Wong, et al., 2017:230; Yip et al., 2018:190) and devising ways to mitigate it, to ease its harmful effects on electric grids and national economies (Viegas et al., 2017:1258; Shokoya & Raji, 2019a:96).

2.2.1.1 Shortcomings of the pioneer electricity grid and the ensued rivalry

Edison’s DC electric system suffered a setback, in that, it started to lose voltage when an attempt was made to distribute the DC electricity over distances longer than a mile (Sulzberger, 2003b:66; Cowdrey, 2006:89). The main rival to Edison in the electricity market was George Westinghouse, an inventor of the railway braking system, who became interested in the AC electricity business and commercialized it (Hughes, 1958:153; Sulzberger, 2003b:66). The rivalry between them began in 1886 after Westinghouse founded the Westinghouse Electric Company (renamed Westinghouse Electric and Manufacturing Company), in Pittsburgh, Pennsylvania, United States; to promote the development of the AC electric system, an alternative electric system for commercial electricity (Hughes, 1958:143).

Westinghouse purchased transformer patents (Sulzberger, 2003b:66; Cowdrey, 2006:91) and incandescent lamp patents that were different from Edison’s (Kommajosyula, 2017:38) for his AC electric lighting business. Westinghouse who wanted more than lighting, also purchased the complete polyphase AC system and the induction motor patents from Nikola Tesla who he also hired in 1888 to work in his company (Ruch, 1984:1397; Sulzberger, 2003a:70, 72; Cowdrey, 2006:91). With the polyphase systems, and its associated components like the transformers and transmission lines, the maiden three-phase electric-line network commenced operation in 1893 (Sulzberger, 2003a:72-73). The AC electric power system and the AC induction motor that are still being used currently all over the world were the original inventions of Nikola Tesla (Sulzberger, 2003b:67; King, 2013). Tesla’s inventions were ranked to be the most valuable after the telephone (King, 2013).

Edison acknowledged the range limitation of his DC system and had earlier sought a remedy from Tesla who he hired in 1884 (before Westinghouse later hired him) to help solve the entrenched DC short-range issue (Sulzberger, 2003b:67; Cowdrey, 2006:90; King, 2011). Tesla had advised Edison that the solution to the short range of DC and the future of electricity distribution for long-range transmission was in the AC electric system; but Edison who knew taking Tesla's advice would render his DC system obsolete rejected Tesla's advice and grimly told him he was not interested (Sulzberger, 2003b:67; Cowdrey, 2006:90; King, 2011). Tesla parted ways with Edison in 1885 after the latter reneged on a financial promise made to the former as a form of compensation after accomplishing the given task upon which the pledge was based (King, 2011; King, 2013).

Westinghouse leveraged on the range-limited shortcoming of the DC to promote the AC, which could be transmitted efficiently over longer distances (Cowdrey, 2006:91) to load centres at a relatively cheaper cost (Coltman, 1988:92). Edison who did not want to lose his electricity-purveyor monopoly (Cowdrey, 2006:91) and the royalties he was getting from his DC patents (Lantero, 2014) felt threatened and launched fierce attacks against the competing AC electric system (Sulzberger, 2003b:64).

2.2.1.2 War of the currents

The business rivalry between Edison and Westinghouse led to the epic and shocking competition dubbed the "war of the currents" (King, 2011). The war of the currents or the battle of the currents started in 1888 (Sulzberger, 2003a:70; Sulzberger, 2003b:67). The ensued 'war' was a legal and publicity battle (Coltman, 1988:92) between the duo entrepreneurs, who had to vie to make a case for the commercial acceptance of either of their DC or AC current for the generation, transmission, and distribution of electricity (Hughes, 1958:143; Sulzberger, 2003b:64). Aside Edison and Westinghouse who were the gladiators in the electric current tussle, other proponents and/or opponents who also got involved in the battle of the currents were scientists, engineers and the businessmen; even the lawmakers and the public were also in the picture and played a remarkable role in it (Hughes, 1958:144).

Edison persistently exhibited the disadvantages of AC, while Westinghouse rather focused on the technical advantages of AC (Cole & Chandler, 2019:21). Edison's criticisms were that the AC high voltage was perilous to work with as it could electrocute (deadly current), which made it more dangerous to human lives; and hence, not a feasible option for the electric system (Cowdrey, 2006:90). Edison who at a point could no longer contest the popularity and the significant economic advantage of the AC system over his DC system, went a step further to launch an offensive and vigorous smear campaign against the AC system (Hughes, 1958:144-145; Rapp & Mensink, 2011:142).

Edison and the DC proponents were adamant about their anti-AC standpoints, as they wanted the AC outlawed and tried every means to associate it with death (Hughes, 1958:145-146, 152, 154, 160). An electrician and an AC opponent, Harold Brown, referred to AC as "executioner's current", and worked surreptitiously in alliance with Edison to malignly prove the potency of AC in causing death (Hughes, 1958:147, 151, 154, 157; Sulzberger, 2003a:71). Harold Brown carried out public electrocution of animals and dispatched them with AC electricity (Hughes, 1958:148-149, 151; Cowdrey, 2006:91). Edison supported death penalty by electrocution (on an electric chair) using the Westinghouse's AC and was also instrumental to its realization (Hughes, 1958:151, 160, 164-165; Sulzberger, 2003a:70-71; Cowdrey, 2006:91; Rapp & Mensink, 2011:142). Edison had abhorred human capital punishment before the battle of the currents, but backed death by electrocution as an alternative to the conventional hanging method, in an opportunity to deviously defame Westinghouse's AC (Hughes, 1958:151, 160, 164-165; Cowdrey, 2006:91).

Edison also coined and introduced the new word "Westinghoused" to the public. He formed the new word from the last name of his main rival in the electricity business. He used this word in his speeches to indicate that those criminals who had been found guilty by the authority and sentenced to death for committing various capital offences would be executed using the AC electricity (King, 2011; Rapp & Mensink, 2011:142). He also advocated for the official adoption of his contrived word, but "electrocuted" was endorsed instead (Rapp & Mensink, 2011:142). Edison's antics against the competing AC were basically meant to get rid of the rivalry from Westinghouse, protect his DC electricity business, and restore the earlier monopoly he enjoyed in the electricity market. However, the macabre marketing tactics adopted and deployed by Edison and his cohorts were unorthodox and went beyond the bounds of conventional competition (Hughes, 1958:143, 145).

2.2.1.3 The triumph of alternating current over direct current

In 1892, when the war of the currents was still at its height, Westinghouse won the bid to illuminate the proposed 1893 Chicago World's Fair (Cowdrey, 2006:92). The 1893 exhibition in Chicago was an all-electric fair, and the first of its kind which had 27 million visitors in attendance (Sulzberger, 2003a:72; Cowdrey, 2006:92; Essig, 2009:254). Westinghouse was able to underbid his main rival (Edison) by less than half to win the contract (Cowdrey, 2006:92; Essig, 2009:254). The underbidding was feasible owing to the cheaper nature of the AC system as against the DC system (Sulzberger, 2003a:72; Cowdrey, 2006:92). The 1893 Chicago World's Fair otherwise known as Columbian Exposition, where about 130,000 incandescent lamps and 8,000 arc lamps were lit up was a huge success (Sulzberger, 2003a:72; Essig, 2009:254) . Those lamps were powered by 12,750 kW two-phase 60 Hz alternators, as the buildings at the fair were luminously turned to "city of light". The awesome exposition gave credence to the AC system and enhanced it to expeditiously eclipse the DC system (Sulzberger, 2003a:72).

Leveraging on the success achieved at the Columbian Exposition, the cheaper nature of the AC system coupled with its ability to transmit power over longer distances, in conjunction with another round of underbidding, Westinghouse in 1893 also won the bid to exploit the immense power of the waterfalls of the Niagara River located at Niagara Falls in New York (Sulzberger, 2003a:73; Cowdrey, 2006:92). The Niagara Falls hydroelectric power plant project was also delivered and commissioned in 1895 (Cowdrey, 2006:92). Dominion of the AC system over its counterpart DC was further entrenched with the successful development of the Niagara Falls hydroelectric power station (Sulzberger, 2003a:72). The Niagara Falls Project became the first-ever hydroelectric power plant, its delivery consolidated the superiority of AC over DC, symbolized victory for the AC, and thus signalled the end of the battle of the currents (Sulzberger, 2003a:72; Essig, 2009:257). Henceforth, the AC system became the dominant and the undisputable de facto standard in the electricity industry (Sulzberger, 2003a:73).

In the end, the negative propaganda approach employed by Edison to discredit and create public exasperation about the AC ultimately failed (Cowdrey, 2006:91). The war of the currents was won in 1895 in favour of Westinghouse's AC after the successful execution of the Niagara Falls Project (Hughes, 1958:144, 165; Coltman, 1988:92; Cowdrey, 2006:92).

The AC is scalable as its voltage could be increased with step-up transformers or lowered with step-down transformers. The fact that the AC system is cheaper and that its voltage could be increased (by lowering its current) with the help of a step-up transformer for transmission over longer distances gave the AC system the unique advantage and triumph over the DC system (Hughes, 1958:144-145; Sulzberger, 2003b:66; Cowdrey, 2006:91-92). The stepped-up voltages could later be stepped down within the vicinity of the consumers to lower voltages by a step-down transformer for end-use (Sulzberger, 2003b:66; Cowdrey, 2006:91; Essig, 2009:258). The fact that the AC is transformable or scalable is the primary advantage for its economic transmission over lengthy distances. The stepping up and/or down of voltages is done by transformers (secondary generators) during the process of transformation (Sulzberger, 2003b:66; Cowdrey, 2006:91; Jamil & Ahmad, 2019:454). The sinusoidal current (AC) has since then been accepted for universal use and adopted as the industry standard for the electric system. Edison eventually regretted not heeding Tesla's advice (King, 2011).

2.2.2 Modern electric power system

The battle of the currents had a far-reaching effect. The contest was incidentally not only about partisan business rivalry, but also instrumental and vital to the future direction and development of the electricity industry all over the world (Hughes, 1958:145; Sulzberger, 2003a:73). The modern electricity grid is mainly AC-based. The AC had taken precedence after its triumph over the DC as mentioned previously in Section 2.2.1.3. The AC electric system is still referred to as "modern" because it is still in use till today. The complete AC-based legacy electricity grid system is known as the conventional grid. The conventional grid is currently being improved upon to the state-of-the-art Smart Grid electric system to cater for some of its inherent challenges (Khoussi & Mattas, 2017:228-229; Kularatna & Gunawardane, 2021:28).

The conventional grid and the Smart Grid are the two main types of electricity grid system. The conventional grid and Smart Grid electric systems are discussed in Sections 2.2.3.1 and 2.2.3.2 respectively. Electricity is generated, transmitted, distributed, and consumed in the modern electricity grid (Khoussi & Mattas, 2017:227), unlike in the pioneer DC electricity grid where electricity was only generated, distributed, and consumed without being transmitted (Tuballa & Abundo, 2016:715), owing to the DC short-range limitation issues stated earlier.

i. Generation

The centralized AC-generated power system is economical, efficient, reliable, and long-distance enabled, as it is usually located far away from the end users (Erenoğlu et al., 2019:14-15; Kularatna & Gunawardane, 2021:1, 27). The AC generation plants are the central source of power in the electricity grid, with generators that are either driven by steam turbines, gas turbines or hydro turbines, etc. (Kularatna & Gunawardane, 2021:1). A turbine is a prime mover that serves as the source of rotational mechanical energy which drives the generators. Turbines produce mechanical energies by converting the kinetic energies of steam, gas, or water, etc. into whirling energies to turn the generators. The generated power needs to leave the remote locations where it is being generated and get closer to the users.

This is literally like taking a product to the market. These remote locations where power is generated are mainly places where the natural energy sources (waterfalls or fuels) that drive the turbines are abundant and readily available (Cowdrey, 2006:91).

ii. Transmission

Transmission is the transportation of the generated electricity via the transmission lines. Transmission is accomplished by stepping up the AC voltages of the generated power at the transmission substations by step-up transformers, so that it would be able to travel over longer distances to the distribution substations nearby the electricity consumers. Transmission should be efficient with lower losses at low cost (Erenoğlu et al., 2019:16). High voltage transmission allows power to be transmitted over longer distances through cheaper cables of smaller diameters, thereby reducing power and heat losses (Hughes, 1958:44; Papalexopoulos, 2013:227-229).

iii. Distribution

At the distribution substations where transmission lines terminate, voltage step-down takes place using primary distribution transformers, to reduce the AC voltage level from transmission voltage to primary distribution voltage for subsequent distribution to the secondary distribution transformers via the primary distribution lines (Khoussi & Mattas, 2017:227). The primary distribution voltage at the secondary distribution phase of the grid is further stepped down to service voltage by the secondary distribution transformers, and taken to the premises of the consumers or service locations via the secondary distribution lines for consumption (Cowdrey, 2006:91; Khoussi & Mattas, 2017:227).

iv. Consumption

Consumption takes place at the demand-side or consumer-end of the grid. It is the final stage of the grid where electricity at its service voltages is delivered to customers at their various locations for direct utilization (Khoussi & Mattas, 2017:227). The use of electricity to power appliances in homes and offices, and machines in industries by the consumers are examples of putting electricity to direct use. Consumers of electricity are meant to use the product judiciously and efficiently without causing NTL. Electricity must be accessible to the consumers because the power that is generated but fails to get delivered to the intended consumers would eventually not worth its while. Consumption must be fulfilled to complete the value chain of electricity.

- **Characteristics of alternating current**

In contrast to the continuous current of DC, the AC varies as it reverses several times in a second and undergoes electromagnetic induction or magnetic effect in the iron cores of transformers. This current induction from the primary coils to the secondary coils of transformers causes a corresponding voltage effect from the primary coils to the secondary coils. The number of turns of the secondary-coil windings with respect to the number of turns of the primary-coil windings of a transformer determines whether the transformer is a step-up or a step-down transformer. A step-up transformer has a greater number of turns of coils in the secondary windings when compared with the number of turns of coils in the primary windings; while a step-down has a lesser number of turns of coils in the secondary windings when compared with the number of turns of coils in the primary windings (Cowdrey, 2006:91; Essig, 2009:102; Crawford, 2019).

The primary coil of the transformer is connected directly to the primary mains supply of the utility, while transformation takes place at the secondary coil via induction. To induce voltage in the secondary coil, the magnetic field produced by the flow of current in the primary coils needs to keep changing constantly, as it is only a changing magnetic field that causes voltage induction (in the secondary coil) via a process known as electromagnetic induction. For this reason, it is only the AC that is transformable, that is, it is only the AC that could be stepped up or down using a transformer. Transformers do not transform an unvarying DC current that flows with a constant magnetic field because the direction of the DC voltage and current are not changing or switching (Essig, 2009:101-102; Crawford, 2019; Owens, 2019:14).

AC electricity is produced and consumed in real time; hence, grid operators ensure that power is supplied in accordance with demand in a bid to stabilize and optimize the grid (Soliman et al., 2021:3712). Although, energy storage is possible nowadays, but it is very expensive (Khoussi & Mattas, 2017:228-229). Power system frequency is an indicator of the grid stability (Arief et al., 2020:2). The grid is stable if its frequency does not deviate or does deviate within an acceptable limit (OBAID et al., 2019:10; Kruse et al., 2021:1-2). Frequency stability means that there is a balance between the power generated and the power consumed (OBAID et al., 2019:10; Bevrani et al., 2021:1). With stable grid frequency, corresponding stable grid voltage is simultaneously maintained, ensuring good power quality and technical stability of the entire power system (Osypova, 2020:25). The frequency of the power grid measured in Hertz (Hz) is equivalent to the number of times (number of alternations) in a second that alternating current and its voltage change direction or switch polarity to make a complete cycle (Alhelou, 2019:202).

National grid frequencies of either 50/60 Hz are the mains frequencies, the reference grid frequencies or the nominal operating frequencies in most countries of the world (Kruse et al., 2021:1-2). 50 Hz AC reference frequencies mean that the directions of voltage and current of the alternating current constantly switch directions fifty or sixty times per second, making a corresponding fifty or sixty cycles during the same one-second period. Grid frequency increases if the demand falls below the supply, but if the grid frequency drops, it means the demand is higher than the supply (Soliman et al., 2021:3712). The rotor of standard AC generator oscillates, alternates, or turns and completes a cycle fifty or sixty times in a second, corresponding to the mains frequency (50/60 Hz) used in a particular country or region. These oscillations which correlates with the mains frequencies are proportional to the speed of rotation of the AC synchronous generators (Bevrani et al., 2021:1). Countries that use 50 Hz grid frequencies tend to use single-phase LVs between 220-240 V range, while those realms that use 60 Hz frequencies use single-phase LV range between 100-120 V (Brown, 2013:1-2; Zaitsu et al., 2018:352).

- **Latest trend**

Although, the conventional AC system still remains the pervasive and predominant electricity system delivering most of the needed electrical energy worldwide (Hammerstrom, 2007:1; Kularatna & Gunawardane, 2021:27, 29), but the DC system is gradually coming back to prominence (Van Hertem & Delimar, 2013:144). DC renewable-energy deployments are also growing rapidly. The revival of DC comes in the form of high-voltage direct current (HVDC), whereby the DC is gradually competing again with the conventionally established AC system for long distance power transmission after it lost the war of the currents in 1895.

2.2.2.1 Conventional grid

The conventional grid, legacy grid, traditional grid, or classical grid is the existing electricity grid of the last century (Khoussi & Mattas, 2017:226-229; Bîrleanu et al., 2019:608). The conventional grid has existed for more than 100 years (Khoussi & Mattas, 2017:227), and was designed to meet the power requirements of that era. The legacy grid is basically a radial (Ma et al., 2013:36), and hierarchical (Bansal & Singh, 2016:174) network. The traditional grid allows power flow in one direction from the generating stations to the distribution substations, and to the consumers (Khoussi & Mattas, 2017:227; Kularatna &

Gunawardane, 2021:28); hence, can only transmit and distribute electrical energy (Tuballa & Abundo, 2016:712). Figure 2.4 is a depiction of a conventional grid system.

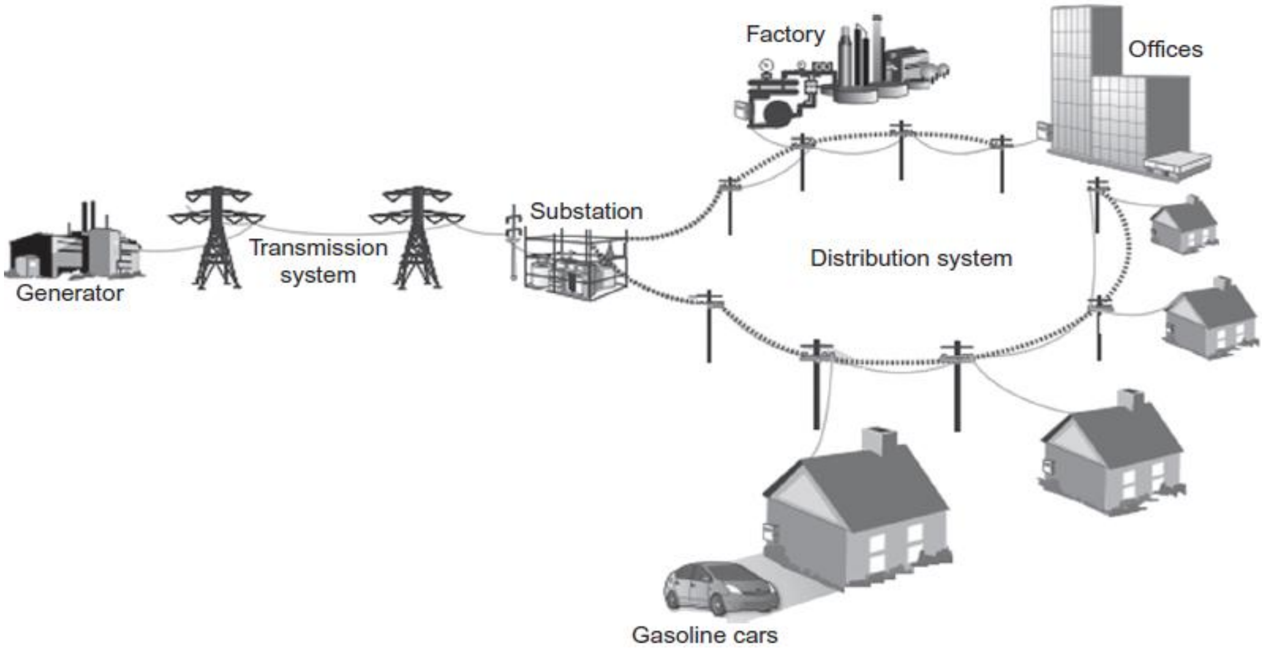


Figure 2.4: Conventional grid

(Khoussi & Mattas, 2017:229)

Apart from power flow, communication flow is also unidirectional in the conventional grid (Bansal & Singh, 2016:174). Information flows from the generating stations to the utilities and from the utilities to the customers, but not the other way round. The consumers cannot send information to the utilities in the traditional grid system. Power is generated centrally in the conventional grid system and the grid is also manually restored in case of faults (Ma et al., 2013:36). The conventional grid is no longer suitable for the power requirements of today, and needs an upgrade (Jiang et al., 2014:105).

2.2.2.2 Smart Grid

The conventional grid is faced with several challenges that need to be fixed in order to enhance its capacity and efficiency. Some of these challenges are: increase in electricity demand, need for diversification of the centralized power generation to cater for the increased energy demand, conservation of energy, reduction in carbon emissions, demand response, and optimal deployment of the available grid assets for efficient performance, etc. (Khoussi & Mattas, 2017:228-229; Kularatna & Gunawardane, 2021:28).

To overcome the challenges and achieve the ambitious goals highlighted in the preceding paragraph, we are expected to modernize, optimize, or make the existing grid smarter (Khoussi & Mattas, 2017:226), so that the generation, transmission and distribution subsystems and the end-user demand side of the power grid could be efficiently managed. Modernizing the conventional grid evolves an enhanced electricity grid or an intelligent electrical network known as Smart Grid (SG), which constitutes telecommunications, Internet and consumers' electronic devices in addition to the existing power system components (Dlodlo et al., 2014:2, 13). The word "smart" means intuitive, responsive and adaptive in operation, culminating into grid intelligence from power generation to consumption (Tuballa & Abundo, 2016:712; Khoussi & Mattas, 2017:226; Zhou et al., 2017:73). The SG self-heals grid-related problems swiftly, and reduces human level of involvement in the operation, management and planning of the grid (Bihl & Hajjar, 2017:274; Shokoya & Raji, 2019a:98). This allows humans to only deal exclusively with the exceptions which automated machine intelligence may not be able to handle. Figure 2.5 is a depiction of a SG system, showing enhancements or improvements to the underlying conventional grid system portrayed in Figure 2.4.

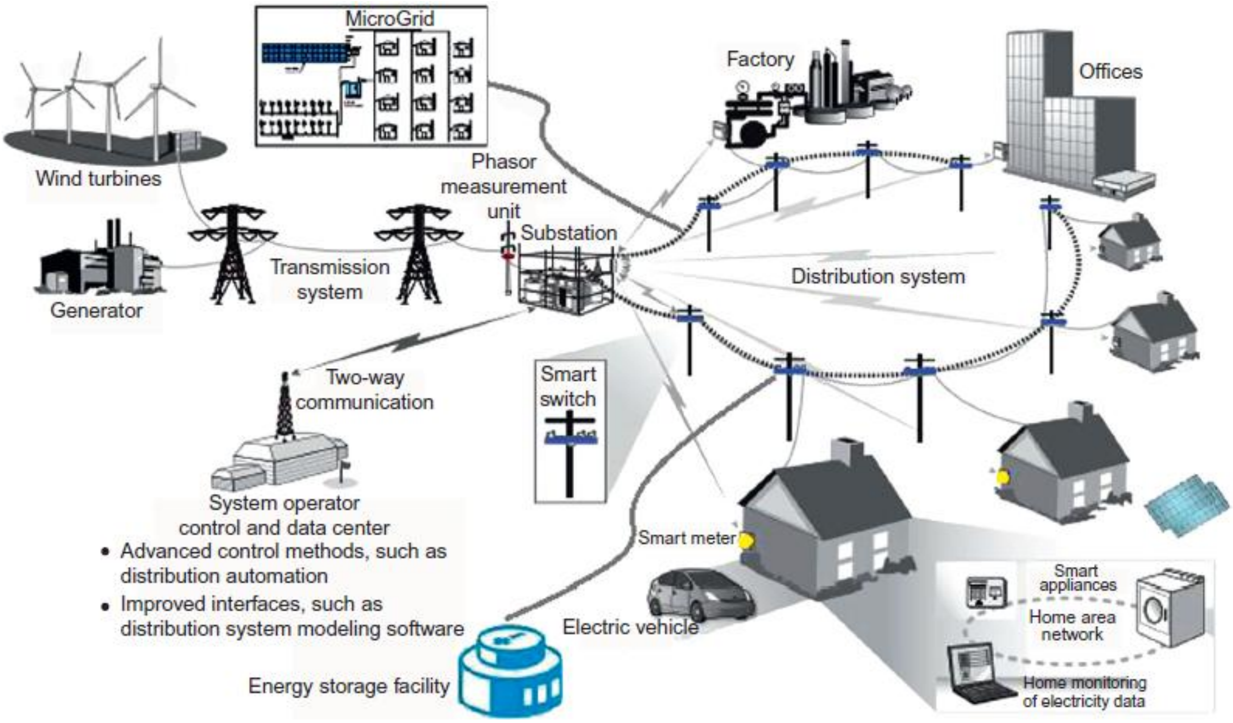


Figure 2.5: The Smart Grid

(Khoussi & Mattas, 2017:233)

The concept of SG came about due to the need to improve the power delivery of the legacy grid, to make it greener, more reliable, more secure and more efficient (Tuballa & Abundo, 2016:711; Edris & D’Andrade, 2017:37-38; Khoussi & Mattas, 2017:231). The SG tends to proffer solutions to the challenges posed by the conventional grid outside the confines of the legacy grid itself; such that, the revitalized electricity grid will be able to meet up with the energy demands of the twenty-first century (Kularatna & Gunawardane, 2021:28). The SG is both evolutionary and revolutionary (Khoussi & Mattas, 2017:231; Tsiatsis et al., 2019:257; Ahmed et al., 2022:580) in terms of the transformation of the power grid. The transformation is about the optimization and intelligent integration of the whole power system (Viegas et al., 2017:1256) by informatizing and intellectualizing the existing grid (Sun & Liang, 2016:900).

The pace for the modernization of the electric grid was set when the Energy Independence and Security Act (EISA) of 2007 was enacted in the United States. The EISA of 2007 proposed the attributes of the modern electricity grid to promote energy efficiency and to stipulate the characteristics of the generation, transmission, distribution, and consumption subsystems of the electricity grid (Tuballa & Abundo, 2016:713; Kabalci & Kabalci, 2019:5-6). The National Institute of Standards and Technology (NIST) coordinates the SG standards, by providing conceptual blueprints and the framework to achieve interoperability between devices in the SG system (Khoussi & Mattas, 2017:230). These efforts were geared towards achieving the ambitious goal of modernizing the grid.

SG is the next-generation electricity grid meant to replace the existing conventional grid (Bîrleanu et al., 2019:607; Kularatna & Gunawardane, 2021:28). The SG forms a convergence between the conventional grid and information and communications technology (ICT) (Porcu et al., 2021:8). Sometimes, the SG is called a modernized grid, since it is an improvement or upgrade on the ancestral conventional grid (Khoussi & Mattas, 2017:231) and addresses its peculiar deficiencies (Kularatna & Gunawardane, 2021:28). SG is the modernization of the conventional grid (Mashima & Cárdenas, 2012:210; Knapp & Samani, 2013:17) to a digitally-enabled (El Bassam et al., 2013:202), networked (Bansal & Singh, 2016:174), and self-sufficient electricity-grid system. This modernization involves the upgrade of the generation, transmission, distribution, and the metering system of the conventional grid (Knapp & Samani, 2013:17).

Upgrading the conventional grid to SG involves a conglomeration of embedded technologies that enhances the generation, transmission, distribution, and consumption subsystems of the electricity network with better efficiency and reliability (Aggarwal & Kumar, 2021:456). These technologies include communication, controls, automation, management tools, information technology and other new technologies, to deliver a robust, optimized, efficient, secure, reliable, intelligent, and automated power grid (Khoussi & Mattas, 2017:231; Viegas et al., 2017:1256; Shokoya & Raji, 2019a:98), while creating greater transparency and providing choices that are beneficial to the electricity customers (Mashima & Cárdenas, 2012:210).

The SG also intends to solve the inherent ET problem, and eradicate other inadequacies associated with the antiquated conventional grid (Faria et al., 2016:362; Yip, Wong, et al., 2017:230). A very important feature of the SG system is the replacement of the traditional electromechanical meters with SMs (Jiang et al., 2014:105; Yip, Wong, et al., 2017:230). SG and its innate SMs allow a significant reduction in NTL and guard against amateur physical tampering (Ahmed et al., 2022:580). Although, novel security risks and pilferage strategies have also emerged owing to the emergence of SG (Yip, Wong, et al., 2017:230; Ahmed et al., 2022:580; Xia et al., 2022:273).

Existing method of electricity-theft detection (ETD) is centred solely on the availability of specific metering hardware devices which forms the fulcrum of the theft and its detection, but electricity could also be stolen remotely via the advanced metering infrastructure (AMI) of the SG system without physical contacts with the metering hardware. The AMI network is a key component of the SG that facilitates bidirectional communication between the electric utilities and the meters of their customers (Mujeeb et al., 2020; Aggarwal & Kumar, 2021:463). The constituents of AMI and the SM are discussed in detail in Section 2.3.2.2. The availability of vast consumption data of customers with increased granularities has increased tremendously owing to SG roll-out. These datasets of customers could then be used for ET predictions by detecting anomalies in energy consumptions using AI-based ML methods (Jiang et al., 2014:109; Glauner et al., 2017:761; Yip, Wong, et al., 2017:231; Guarda et al., 2023:1-2), as discussed in Sections 2.4.5 and 2.4.5.1.

In addition to the customary central power generation plants, SG also allows for the stable integration of smaller power generation units known as distributed energy resources (DER) like residential batteries, electric vehicles (EVs), microgrids and renewable energies into the underlying conventional grid (Khoussi & Mattas, 2017:233; Kathiresh & Subahani, 2020:177). This energy diversification is to decentralize generation, enhance capacity for sustainability to meet growing consumers' demand. Apart from distributed energy addition to the grid, SG also allows for the efficient transmission of energy (Viegas et al., 2017:1256), bidirectional energy flow with a two-way digital communication and control capabilities that enable the customers to participate and contribute to the sustainability of the electricity grid (Khoussi & Mattas, 2017:231; Viegas et al., 2017:1256).

The two-way communication flows in SG allow customers to make informed economic decisions on their energy usage when they react to the demand-response prompt information they receive from the utilities via their SMs; while the two-way energy flows also allow customers to contribute to grid generation capacities by selling their excess DER back to the utilities (Viegas et al., 2017:1256; Shokoya & Raji, 2019a:96). The connection between the smart energy meters of the customers and the utility information systems is to deliver real-time energy information to the utilities and vice versa in a two-way communication mode via the AMI; while the bidirectional energy flows including the trade flows between the utilities and their customers form the Energy Internet (Sun & Liang, 2016:900). With SG, power systems are being transformed into data-driven systems with increased communications and digital controls (Xia et al., 2022:273; Kim et al., 2024:1).

❖ **Demand response**

Demand response is a powerful tool and one of the main strategies peculiar to the SG concept, whereby power demand by electricity consumers is being managed in response to the supply (Ekanayake et al., 2012:100; Osypova, 2020:26). Demand response is a load-shifting or load-curve flattening strategy that brings about consumers' load reduction, by transferring loads from a period of high demand to a period of low demand. It is the inclusion of the demand-side management mechanism into the grid operations for the overall efficient management of the SG system. This improves the interaction between the utilities and their customers to assuage supply-demand mismatch, for the regulation and sustainability of the electricity grid. Demand response is mainly facilitated by applying variable tariffs or rates by electric utilities to units of electricity consumed during the peak and/or off-peak periods, as a control measure to match supply to demand (Dlodlo et al., 2014:2-3, 6-7, 9, 12). The matching of supply to demand is done by controlling, adapting, or synchronizing demand in accordance with the available supply.

Electricity tariffs are relatively higher during peak periods when demand is higher and lower during the off-peak periods when there is less energy demand. This enhances electricity customers to make smart or informed decisions about their energy usage. The customers tend to react to real-time increase in electricity tariffs when grid load increases especially during the peak periods; or react to the load reduction alert prompted by the electric utilities via their SMs to prevent supply shortage during peak periods (Dlodlo et al., 2014:5-6; Shokoya & Raji, 2019a:99). The utilities may take the prerogative of disconnecting consumers remotely if the load-reduction notifications they sent through the customers' SMs were not being adhered to, or reconnecting them when the grid is more stable (Gupta et al., 2022:12). These remote disconnections or reconnections are owing to the ability of the SMs to execute remote commands in addition to its execution of local commands (Depuru et al., 2011b:2736).

The essence of demand response is to encourage reduction in energy usage, to control and reduce the total energy demand and lessen the grid burden. With demand response, no power outage is experienced but the electricity customers receive rate increase alerts and/or energy reduction prompts which they are obliged to react to (Ma et al., 2013:36-37). Demand response allows consumers to have more control of their energy bills and helps prevent blackouts during peak hours (Dlodlo et al., 2014:12). Demand response in SG ensures balance between energy generation and consumption, so that power is produced and used at the capacity constraints of the grid (Shokoya & Raji, 2019a:99). This is to lower the production cost and to ensure successful demand-side management and security of the grid. Maintaining a balance between generation and consumption is achieved by the utilities using the precise information of the load they need to cater for in real time. The load information is seamlessly available in real time owing to the peculiar two-way communication between the consumer and the utility, as provided for by the AMI in a SG system, for the efficient management of the grid (Mujeeb et al., 2020; Aggarwal & Kumar, 2021:463). Information on the consumers' load allows the utilities to match power supply to demand and thus generate electricity in accordance with demand. This prevents the burning of more fossil fuels, thereby saving the environments and the economies of realms worldwide (Ramchurn et al., 2012:86-89). Demand response functionality is not available with the conventional grid and its meters.

❖ Smart Grid: the overview

In summary, the cyber-physical system called SG improves the efficiency, reliability, and sustainability of the traditional power grid by drastically reducing system losses (Shahzadi et al., 2024:1). Elements of reliability improvement in the SG are self-healing, addition of alternative energies to the grid for capacity increment, promoting the economical use of electricity, and providing cyber and physical security to the grid information systems. The SG is efficient because power generation, transmission and distribution within the grid are cost-effective with reductions in generation and distribution losses. Demand response at the demand side of the grid introduces more flexibility to electricity tariffs and consumptions by allowing the engagement of customers in the management of the grid, ensuring that the SG is sustainable while also creating a level-playing field, promoting a mutually beneficial scenario, and a fostering harmonious relationship between the electric utilities and their customers. The following six essential features distinguish SG from the conventional grid: addition of renewable energies to bolster the grid capacities and to reduce carbon emissions, reliable two-way communication from generation to consumption endpoints, advanced metering infrastructure, reliable energy storage abilities, management and processing of data, and lastly cyber-physical security (Aggarwal & Kumar, 2021:461-467).

Deployment of AI techniques have been proposed and adapted to SGs for optimizing demand-side management, dynamic load profiling, automatic resolution of grid-related issues and for several other application areas that are crucial to the resilience and reliability of SGs. The unique cognitive characteristics of the SG responsible for its astute edge over the legacy grid is not without the powerful technical support provided by AI (Stracqualursi et al., 2023:3). In fact, AI is the driver behind the intelligence of SGs (SAP, 2021). Deployment of SG in Africa will reduce power crises on the continent owing to the ability of SGs in allowing the incorporation of renewable energies, including its better energy-management prowess (Shokoya & Raji, 2019b:467, 470). Reliable electricity may snowball Africa into a production hub rather than her current perpetual consumption state.

2.3 Electricity meters

An electricity meter, electric meter, energy meter or kilowatt-hour meter is a device used by electric utilities to measure the consumptions of electrical energy for billing and monitoring purposes (Babuta et al., 2021:1; Bajpai & Reddy, 2021:65), and to reduce the effect of NTL (Depuru et al., 2011a:1011). Electricity meters are cash registers which serve as direct revenue interfaces between the utilities and their customers (Ajenikoko & Adelusi, 2015:99). Electricity meter is installed at the premises of consumers, either in the residential or industrial buildings, to measure the energy consumed by all the electrical loads situated in the buildings, or at times to measure the consumption of a particular standalone device (Sowmya et al., 2016:4368). Metering is fundamental and crucial to the commercial management of electricity (Hashmi & Priolkar, 2015:1424). There must be a reliable means of measurement to evaluate the power transfer by the utilities and the consumers' energy consumptions to determine whether electricity is being stolen or not (Babuta et al., 2021:1). When utility revenues fall noticeably short of what they anticipated, then ET is suspected.

2.3.1 Historic electricity meters

To deeply understand the essence of electric meters in the power system, there is need to go down memory lane to perceive how important electric meters had been and why the early inventors made them priorities. Quantity measurement is critical to businesses to promote transparency and to instill transactional trusts among customers. Even though electricity is an invisible commodity, the quantity of its consumption still need to be measured and doing so incontrovertibly to generate revenues. That was the original motivation behind the production of electricity meters. So many efforts had been put into the art of electricity metering in the past. Historic electric meters were the earliest meters deployed to determine the amount of electricity consumed when the production of electricity started, before the advent of the modern electromechanical meters and the later introduction of the more-accurate and more-efficient electronic meters (Ekanayake et al., 2012:84, 87; Weranga et al., 2014:18, 26).

2.3.1.1 Edison chemical meter

Thomas Edison was the first to set up an electric utility as discussed in Section 2.2.1. He was also the first to start the commercial electric metering in 1881 (Ricks, 1896:61; Dyer, 2001:875), when he developed and made available DC electric meters that were deployed to measure the level of consumption of his then forthcoming commercial product (DC electricity) in an effort to generate revenue (AIEE, 1941:421). Edison had already invented and produced the chemical meters before his Pearl Street DC power station began commercial electricity generation on 4 September 1882. That was a smart business move by Edison who ensured that the then proposed power station started to generate income immediately after it commenced operations. Edison meter was technically an electrolytic-deposit meter in which the weight of its deposited mass would later be measured to determine the current consumed (AIEE, 1941:421).

The Edison meter was industrially known as Edison chemical meter, and was used to measure electricity consumption using the concept of electrolysis, by taking advantage of the chemical effects of electrical current (AIEE, 1941:421; SEI, 2006).The Edison meter was a coulomb meter which was used with direct currents only, to determine the amounts of direct currents consumed (Ricks, 1896:61). A small amount of current was made to pass through the electrolytic cells of the meter by shunting the meter with the main circuit to prevent the whole circuit current from flowing through the meter. If not for this, the meter would had required huge meter resistance to cater for the large main-circuit current (Ricks, 1896:62; Jones, 1982:30). The Edison chemical-based electric meter system was independent of electrical voltage (AIEE, 1941:421). The meter consisted of a copper sulphate electrolyte (Ricks, 1896:62) in a jar with two copper electrodes and was used to determine the ampere-hour of electricity consumed (Ricks, 1896:62; AIEE, 1941:421). The electrolytic process began after the passage of current through the electrolyte via the electrodes. There were two versions of the Edison chemical meter. The original version of the meter was made up of a balanced beam, with copper plates suspended in copper sulphate solution at both arms of the meter beam as shown in Figure 2.6.

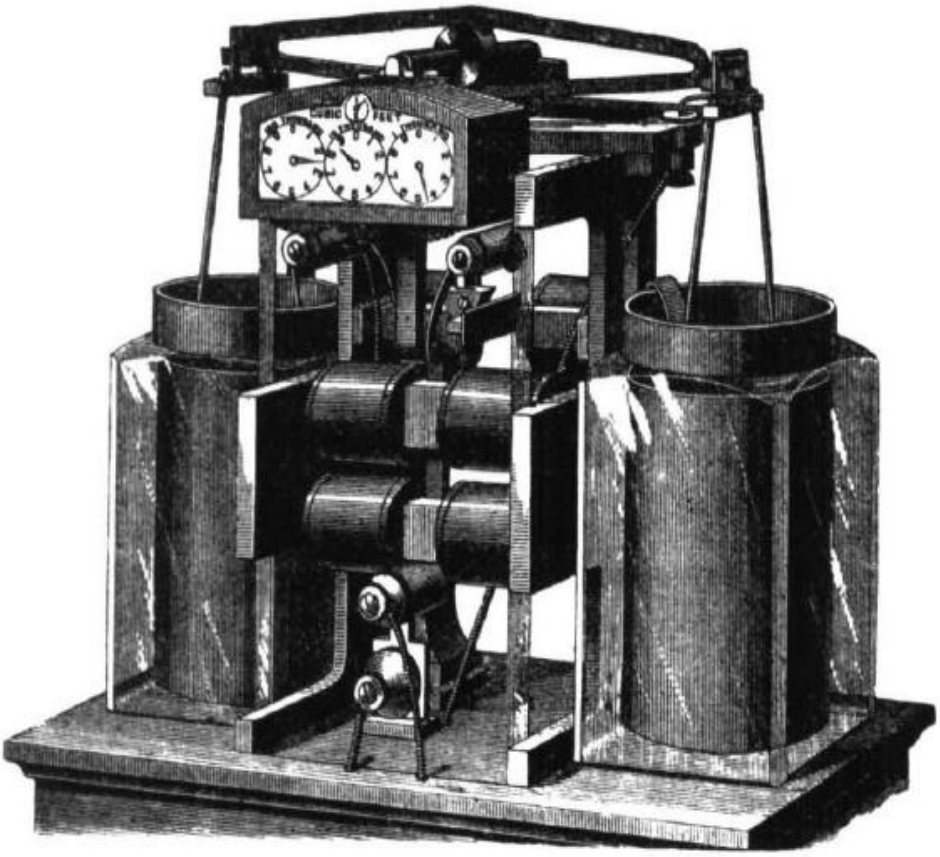


Figure 2.6: Original version of the Edison chemical meter

(Ricks, 1896:62)

The copper plates as seen in Figure 2.6 were the electrodes. As the electrolytic process continued, copper was transferred from the heavier anode to the lighter cathode, until the cathode was heavy enough to turn over the beam. When this happened, a unit would be registered on the counting mechanism of the meter and the direction of current would be reversed. The reversal of the direction of the current changed the polarity of the electrodes and the electrolytic process would continue unabatedly. The beam turnover allowed continual making and breaking of electrical contacts and the eventual reversal of the direction of the current through the meter. Also, the more the current flowed in the main circuit, the more the temperature of the main circuit increased and went higher than the temperature of the copper sulphate electrolyte of the meter. That translated to an increase in the resistance of the main circuit and a relative decrease in the resistance of the electrolyte, which allowed more current flow through the electrolyte of the meter. The temperature variations of the electrolyte affected the accuracy of the meter (Ricks, 1896:61-62; AIEE, 1941:421). The original Edison chemical meter was refurbished to cater for these shortcomings. The refurbished or the improved version of the Edison chemical meter is shown in Figure 2.7.

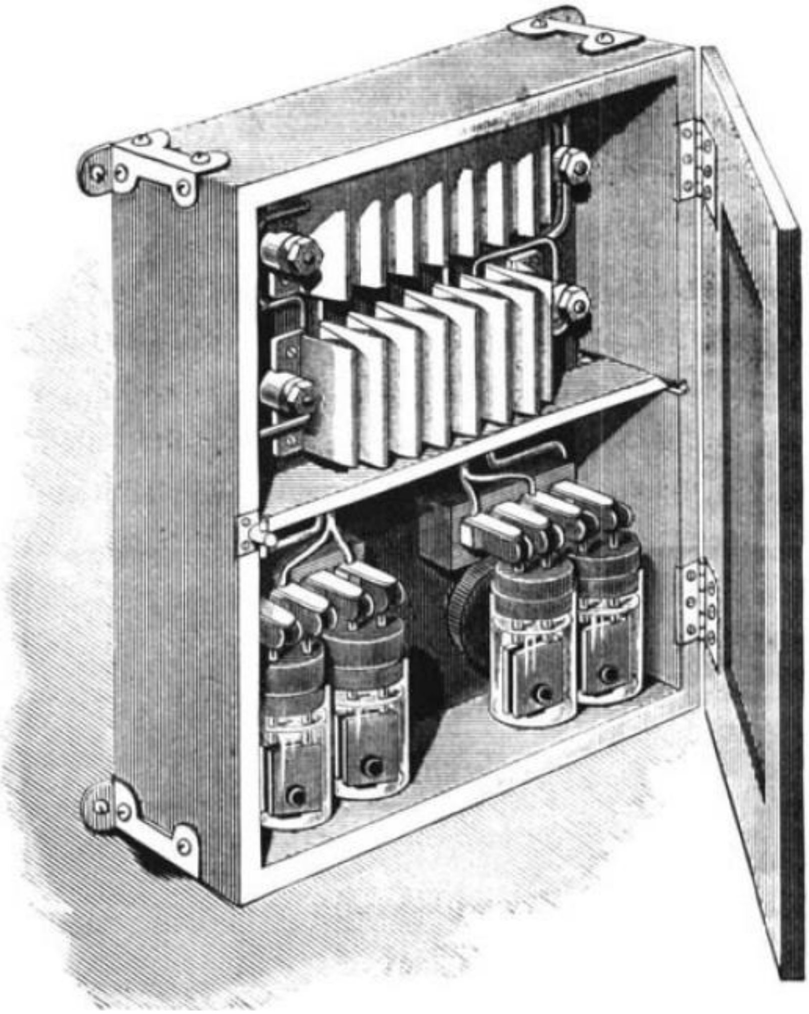


Figure 2.7: Improved version of the Edison chemical meter

(Ricks, 1896:63)

In the improved version of the Edison chemical meter, the amount of electricity consumed was determined by weighing the measurement of the cathode at the start, and at the end of the billing period (Dyer, 2001:875). The anode was heavier while the cathode was lighter. The weight of the anode metal transferred to the cathode during the electrolytic process was equivalent to the amount of electricity (in ampere-hours) that had passed through the meter for that billing period. The difference between the original weight of the cathode and its weight after the electrolytic process determined the exact weight of the copper transferred from the anode to the cathode and also determined the actual amount of electricity consumed. The cathode weight was proportional to the power utilized for a given billing period (Ricks, 1896:63; AIEE, 1941:421; SEI, 2006).

In the previous Edison meter, the current that flowed through the meter increased owing to the increase in the temperature of the main circuit, while the current flow through the meter also reversed intermittently due to the making and breaking of electrical contacts. To correct these shortcomings of the previous version of the Edison meter, the mechanical switching (making and breaking of electrical contact) in the original meter was absent in the updated version, as the current in the improved version of the meter then flowed in one direction only. Also, a copper resistance or German silver was placed in series with the electrolyte, such that the increase in the copper resistance due to increase in the circuit temperature was equivalent to the supposed decrease in the resistance of the electrolyte. The copper resistance or German silver placed in series with the electrolyte was to cater for the temperature coefficient of resistance of the electrolyte and cancel out the effect that the temperature of the main circuit would have had on the electrolyte of the meter. That helped to remove the variation of the flow of current through the meter. Alternatively, amalgamated zinc plates could also be used as electrodes and immersed in zinc sulphate electrolyte, instead of copper electrodes and copper sulphate electrolytes as described earlier (Ricks, 1896:62-63; AIEE, 1941:421).

One of the disadvantages of the refurbished version of the Edison chemical meter was that the customers could not determine their electricity consumptions by direct reading from the meter (Ricks, 1896:63). The customers could not read their meters themselves directly from the device, but the cathode weight measurement was done in their presence to promote transparency and customer goodwill. Removing and weighing of the electrodes was a tedious task for the meter reader who was otherwise known as ‘calculator’ in those days (Ricks, 1896:63-64; AIEE, 1941:421-422). Previously used electrodes were replaced with fresh ones when they wore out. Also, Incandescent lamp was located within each meter, which was left burning to prevent the freezing of the copper sulphate or zinc sulphate electrolytes (Ricks, 1896:62; Jones, 1982:30).

2.3.1.2 Gardiner DC lamp-hour meter

The first known electricity meter was the DC lamp-hour electromagnetic meter produced and patented in 1872 by Samuel Gardiner (Bîrleanu et al., 2019:609; Coelho et al., 2019:98; Ezhilarasi & Ramesh, 2019; Martins et al., 2019:90). Unlike the Edison chemical meter discussed earlier, the Gardiner lamp-hour meter was not deployed commercially. The

Gardiner lamp-hour meter was produced when the need to monitor electricity usage arose, because lighting which was the first mass application of electricity needed to be monitored and billed (SEI, 2006). The Gardiner DC lamp-hour meter was the first-ever electric meter produced and preceded the Edison chemical meter, but the Edison chemical meter was more popular in practice because it was deployed for commercial use. The Gardiner DC lamp-hour meter is shown in Figure 2.8.

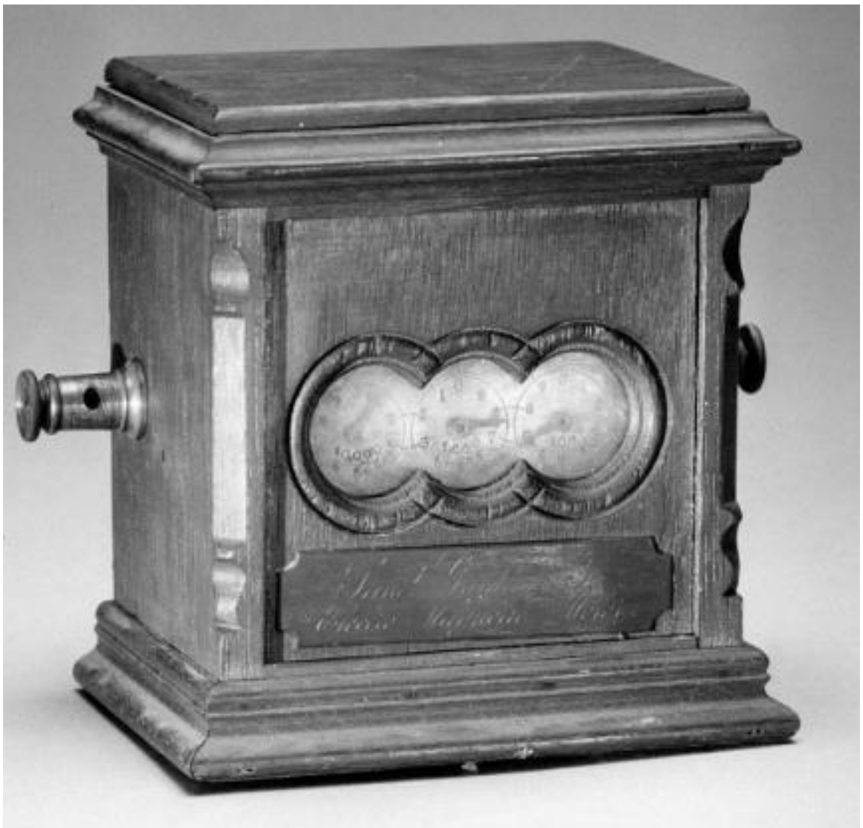


Figure 2.8: Gardiner DC lamp-hour meter

(Smithsonian, 2019)

The Gardiner DC lamp-hour meter used a simple electromagnet to control the start and stop of the timer or clock mechanism revealed in Figure 2.8 when current passed through it (Malik, 2013:140; Bîrleanu et al., 2019:609; Coelho et al., 2019:98). The meter was used to measure the electricity consumed by the earliest DC arc lamps (Primicanta, 2013:10). The arc lamps were centrally controlled by a switch and the current drawn by the lamps were constant (SEI, 2006; Primicanta, 2013:10). The cost of the electricity consumed was determined by the number of arc lamps powered per hour, as read from the current-flow duration registered on the Gardiner meter (SEI, 2006; Primicanta, 2013:10; Bîrleanu et al., 2019:609). The DC arc lamps went obsolete with the introduction of Edison incandescent lamps (SEI, 2006). Unlike the arc lamps that consumed more power and produced high intensity of light appropriate for outdoor lighting, Edison incandescent lamps consumed low power, provided less illumination suitable for indoor use and made possible the replacement of an arc lamp with several incandescent lamps, by technically subdividing the supposed intense radiance expected of a single arc lamp into several incandescent lighting units (Smithsonian, 2001; Sulzberger, 2003b:64-65; SEI, 2006).

2.3.1.3 Shallenberger meters

Oliver Shallenberger was the chief electrician at the Westinghouse Electric Company (renamed Westinghouse Electric and Manufacturing Company), Pittsburgh, Pennsylvania, United States (Guarnieri, 2013:52). In 1888, he invented the self-indicating and direct-reading induction ampere-hour meter (a coulomb meter) shown in Figure 2.9 (Ricks, 1896:67-68; AIEE, 1941:423; Sulzberger, 2003a:70).

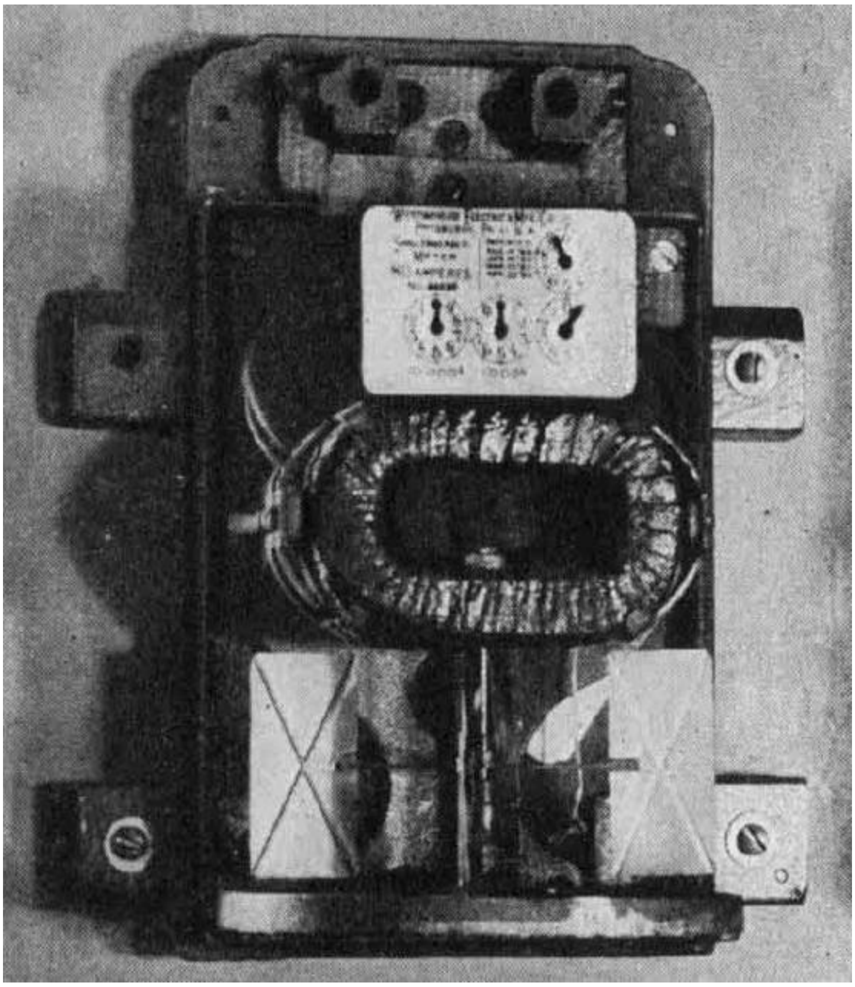


Figure 2.9: Shallenberger ampere-hour meter

(AIEE, 1941:424)

This Shallenberger ampere-hour meter was the first commercial and successful AC electric meter, which was used to measure the amount of AC current consumed by electricity users by leveraging on the rotary effect of magnetic field (AIEE, 1941:423). The meter was put into commercial production by the Westinghouse Electric Company. Shallenberger's ampere-hour meter then became the cash register of the electricity industry (Ruch, 1984:1397) used for accurately billing of customers. The Shallenberger ampere-hour meter eventually solved the lingered metering and billing issues associated with AC electricity (Coltman, 1988:92). The greatest discovery of the electric metering art took place in 1894 when Shallenberger developed the induction watt-hour meter (AIEE, 1941:423-424). Shallenberger used the basic principles of his ampere-hour meter to produce the subsequent Shallenberger AC watt-hour meter (Sowmya et al., 2016:4369). The discovery made it possible for Shallenberger's earlier ampere-hour meter which registered readings only in ampere-hours to be upgraded to measure readings in watt-hours or energy (AIEE, 1941:424). Figure 2.10 shows the Shallenberger watt-hour meter.

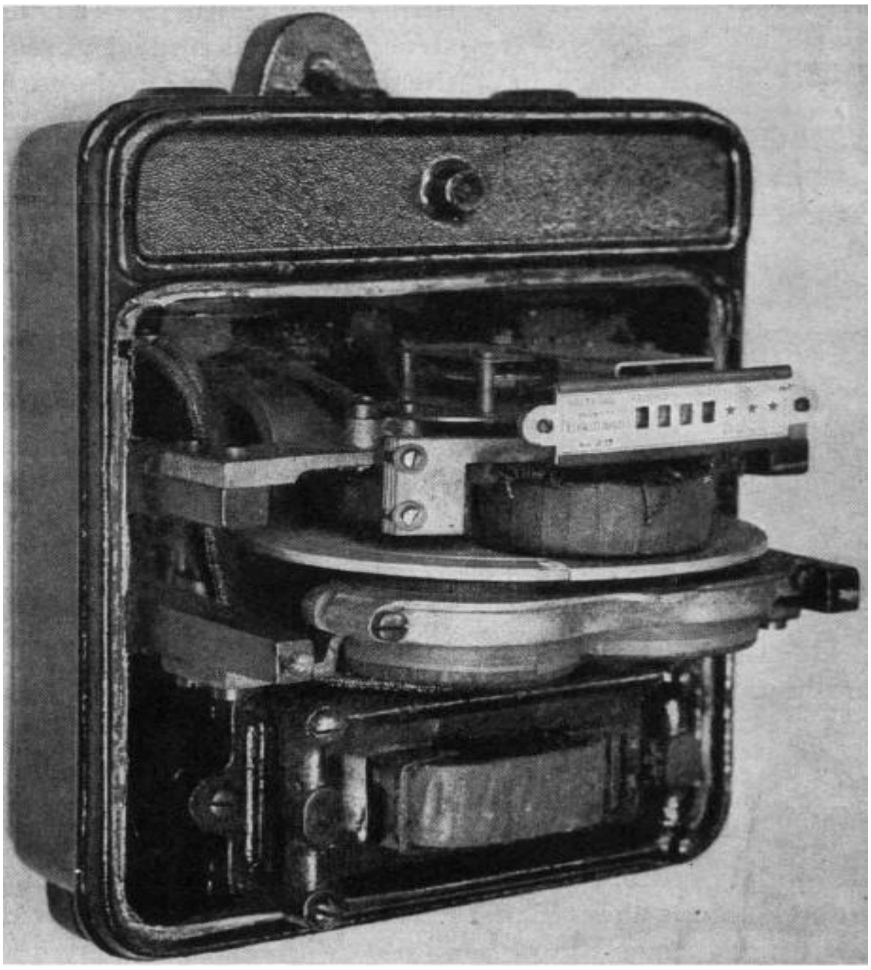


Figure 2.10: Shallenberger watt-hour meter

(AIEE, 1941:426)

Although, Ottó Bláthy in 1889 made the first specimen of the AC induction watt-hour energy meter based on the principle of the Shallenberger ampere-hour meter (Ricks, 1896:422; AIEE, 1941:422), and later in the same year, Elihu Thomson also developed the commutator-type watt-hour meter, which could be used with either DC or AC electricity to measure energy consumptions (Ricks, 1896:66-67; AIEE, 1941:422-424; Sowmya et al., 2016:4369). However, despite Bláthy's and Thomson's works on watt-hour meters for the registration of AC electricity consumptions, Shallenberger's AC induction watt-hour meter developed in 1894 remained the only forerunner meter typical of the modern electromechanical meters, providing the cutting edge and setting new standard in the art of electric metering (Primicanta, 2013:11; Sowmya et al., 2016:4369).

2.3.2 Modern electricity meters

The modern electricity meters are conventional energy meters that have been recently deployed by electric utilities for use by the electricity consumers. The mode of operation of the modern electricity meter is that it continually measures the instantaneous current and voltage of the load circuit and calculates the product of the two to determine the power consumed; while the consumed power is later integrated with respect to time to determine the energy consumed (Bajpai & Reddy, 2021:65; Ghosal et al., 2022:160). This principle of operation took after the working principle of the Shallenberger watt-hour induction energy meter.

Analogue and digital or electronic meters are the two basic categories of the modern electricity meter (Kathiresh & Subahani, 2020:177; Xia et al., 2022:279). Analogue meters are electromagnetic, while digital meters are electronic. The analogue electric-meter readings are displayed by a pointer-type or dial-type register mechanism, while the readings on digital meters are displayed on a liquid crystal display (LCD) or on a light-emitting diode (LED) screen (Ekanayake et al., 2012:95; Gopinath et al., 2013:429; Kathiresh & Subahani, 2020:178). The prominent example of analogue meter is the electromechanical meter, while that of digital meter is the SM (Rastogi et al., 2016:13).

Since the electromechanical meter could only measure the consumed electrical energy, there was the need for an electronic meter which could not only measure the amount of instantaneous energy used, but also able to measure and communicate other electrical load and supply parameters like the frequency, phase currents, phase voltages, reactive power, active power, apparent power, power quality measurement, maximum demand and power factor (PF) to the utilities, to allow them have more control over efficiency and capacity

(Ekanayake et al., 2012:87; Weranga et al., 2014:17-18; Avancini et al., 2019:705; Kathiresh & Subahani, 2020:178).

Unlike the electromechanical meters, the working of electronic meters is not affected by external magnets or the orientation or positioning of the meters (Weranga et al., 2014:26). Electronic meter is more flexible, reliable, stable, provides higher accuracy in measurement, updates and gives measured data timeously (Ekanayake et al., 2012:87; Weranga et al., 2014:26). A standard electronic meter consists of a microcontroller, an LCD and its digital counter-type display, communications ports, a power supply, and a real time clock (RTC) (Weranga et al., 2014:25) with no moving parts. Prepaid or prepayment meter is a kind of electronic meters which allows customers to pay their electricity bills in advance before power usage, to reduce revenue losses and the risks of unpaid electricity bills (Ajenikoko & Adelusi, 2015:100). Customers then lose access to electricity after they have exhausted their pre-purchased electricity units.

Electronic meter communication was one way before the advent of SMs. The one-way communication capability was added when electronic meter in a conventional grid was automatized with automatic meter reading (AMR) to relate consumers' basic status information and consumption records to the utilities. This was before the emergence of AMI with SMs in SG that allows for a two-way power flow and a two-way communication flow between the electric utilities and the consumers (Xia et al., 2022:280). Before the introduction of AMR and its one-way communication capability (Ekanayake et al., 2012:84-85; Xia et al., 2022:274, 280), early electronic meters even though had display units like LCDs were read manually onsite for billing purposes (Ekanayake et al., 2012:87).

A SM is an advanced electronic meter and the state of the art in electricity metering, which has evolved owing to improvements on the previous electronic meters (Weranga et al., 2014:27; Oloruntoba & Komolafe, 2018:15). Aside the mentioned two-way communication capability for SMs in AMI, power-outage detection and notification, load profiling, tamper detection, remote disconnection and reconnection of power supply by the utilities, ability to display information on multi-tariffing and on the current source of power supply (renewable or conventional), including other energy usage information, etc., are other features peculiar to SMs (Mashima & Cárdenas, 2012:210; Weranga et al., 2014:23; Gupta et al., 2022:12). Electromechanical meters are more susceptible to ET when compared with electronic meters (Weranga et al., 2014:23).

- **Units and costs of electricity**

The electric meter captures the units of electricity consumed by the customers to determine the amount of bills payable to the utilities. The unit of the active electrical energy consumed is measured in kilowatt-hour (kWh) (Oladokun & Asemota, 2015:37). The kWh is the most common commercial standard unit of the electric meter for measuring the amount of electrical energy consumed by the consumers for billing purposes (Ghosal et al., 2022:160). The kWh of energy consumption in modern meters is measured by the integral of the real power consumed via the load circuit with respect to time (Bajpai & Reddy, 2021:65; Ghosal et al., 2022:160).

One unit of electricity (1 kWh) is the electrical energy consumed when 1000 watts or 1 kW of electrical power is consumed and maintained for a period of one hour (Oladokun & Asemota, 2015:37; Abdul-Aziz et al., 2023:250), or when 1 watt of electrical power is consumed over a period of 1000 hours. Multiplying the power rating (in watts) of a device or an appliance by the duration of time (in hours) during which the device is turned on divided by 1000, indicates the energy consumption of the device in kWh (Abdul-Aziz et al., 2023:249). For example, a 60-watt rated bulb turned on for a one-hour period would consume 60 watt-hour (0.06 kWh) of electrical energy, that is, 0.06 unit of electricity has been consumed in one hour. Ten bulbs of the same power rating turned on for ten hours would consume 6000 watt-hour (6 kWh) of electrical energy, that is, 6 units of electricity have been consumed in ten hours. The cost of the electricity consumed is based on the total energy usage measured in kWh multiplied by the tariff per unit of the used electricity.

Electricity tariff or rate is a regulated price charged per unit of electricity consumed. The bills payable to the utilities by their customers are based on the units of electricity they have consumed with respect to the rate charged per unit of it by the respective utilities. The amounts charged per unit of electricity consumed by every utility are determined by the stipulated tariffs implemented by electric utilities in different countries, as approved by their various electricity regulatory authorities. Electricity tariffs are expected to be realistic as to allow for utility revenues that will enable gradual recovery of initial-investment costs on electricity infrastructures, and also viable to cater for the running costs of grid operations and maintenances (Oladokun & Asemota, 2015:37), while ensuring sufficient profits.

2.3.2.1 Electromechanical meter

Electromechanical meter or watt-hour meter is an analogue energy meter and the most common type of electricity meter used for registering energy consumptions (Ahmad et al., 2016:90; Avancini et al., 2019:705). The meter is the oldest type of modern meter which has been in use for over a century (Weranga et al., 2014:18; Ahmad et al., 2016:90). The modern electromechanical energy meter works on the principle of electromagnetic induction (Bajpai & Reddy, 2021:65), and is very identical to the AC induction watt-hour meter developed by Shallenberger in 1894, as discussed earlier in Section 2.3.1.3. The Shallenberger watt-hour meter was the forebearer of the current electromechanical meters as they work on the same principle (Primicanta, 2013:11; Sowmya et al., 2016:4369). Figure 2.11 shows a sample of a single-phase electromechanical energy meter.

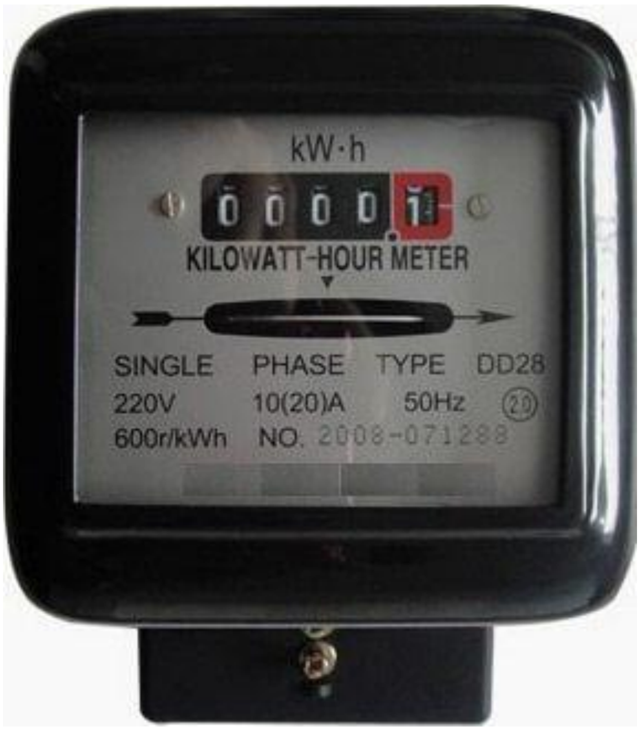


Figure 2.11: Single-phase electromechanical meter

(Gopinath et al., 2013:429)

The meter readings on the electromechanical meters are manually read onsite by the utility employees, usually once in a month and manually entered to the utility databases (Gopinath et al., 2013:428; Weranga et al., 2014:23; Rastogi et al., 2016:13) in a process known as static load profiling. Manual onsite meter readings are inevitable in analogue metering because the conventional electricity meters lack advanced communication capacities (Knapp & Samani, 2013:47). Manual meter readings require the deployment of large human resources, and it is time consuming (Kathiresh & Subahani, 2020:178). The readings on the analogue counter-type dials of electromechanical meters are used to prepare the monthly electricity bills for the customers. Subtracting the current meter readings from the previous meter readings gives the current billable readings. Electromechanical meters have five analogue counter dials (four black dials and one red dial). Only the digits on the black dials are read and used for billing purposes by the electric utilities. The digit on the red dial after the decimal point is neither read nor used for billing purposes, but measures the number of rotations of the central aluminium disc. The rotational speed of the aluminium disc at the centre of the meter is correlative to the instantaneous active power being consumed through the load circuit at any point in time (Masnicki & Mindykowski, 2018:0183; Avancini et al., 2019:705; Kathiresh & Subahani, 2020:177-178).

The electromechanical meter is basically a special kind of an induction electric motor (Ahmad et al., 2016:90; Bajpai & Reddy, 2021:65), consisting of electromagnets (stator) and rotating aluminium disc (rotor) that spins within the air gap between the electromagnets. The aluminium disc at the centre of the meter is supported by a shaft or a vertical spindle, which turns gear arrangements or gear trains connected to the register mechanism on the front of the electric meter (Kathiresh & Subahani, 2020:178; Bajpai & Reddy, 2021:67). The current coil and the load circuit are connected in series with, while the voltage coil is connected across the supply (Weranga et al., 2014:19).

An induction coil (known as current coil or series coil) which is excited by the load current is wound around the series magnet; while another induction coil (known as voltage coil, pressure coil, shunt coil or potential coil) with higher number of turns (more inductive than the current coil) is excited by the current of the supply voltage and is wound around the central limb of the shunt magnet (Weranga et al., 2014:19; Bajpai & Reddy, 2021:66-67; Dimkpa et al., 2023:2639). The series and shunt magnets are laminated electromagnets (Bajpai & Reddy, 2021:66) with their magnetic fields induced by the voltage and current coils (Ekanayake et al., 2012:86). A single-phase electromechanical meter uses a single voltage and current induction coils, while a three-phase electromechanical meter uses more than one voltage and current induction coils (Gopinath et al., 2013:428; Kathiresh & Subahani, 2020:178).

Power is fed into the meter through the induction coils (electromagnets), which eventually produce current-coil magnetic flux and voltage-coil magnetic flux. The magnetic flux generated by the current coil is proportional and also in phase with the load current, while the current and its produced magnetic flux in the voltage coil lags the supply voltage by 90^o, giving rise to eddy currents in the aluminium disc (Weranga et al., 2014:19; Ahmad et al., 2016:90; Kathiresh & Subahani, 2020:177; Bajpai & Reddy, 2021:66; Dimkpa et al., 2023:2639). It is the interaction between the changing magnetic fields of the electromagnets (current and voltage coils) with the conductive aluminium disc that gives rise to eddy currents being induced in the aluminium disc. Eddy currents are induced in conductors placed in changing or alternating magnetic fields. The internal components of the single-phase electromechanical meter shown in Figure 2.11 are depicted in Figure 2.12.

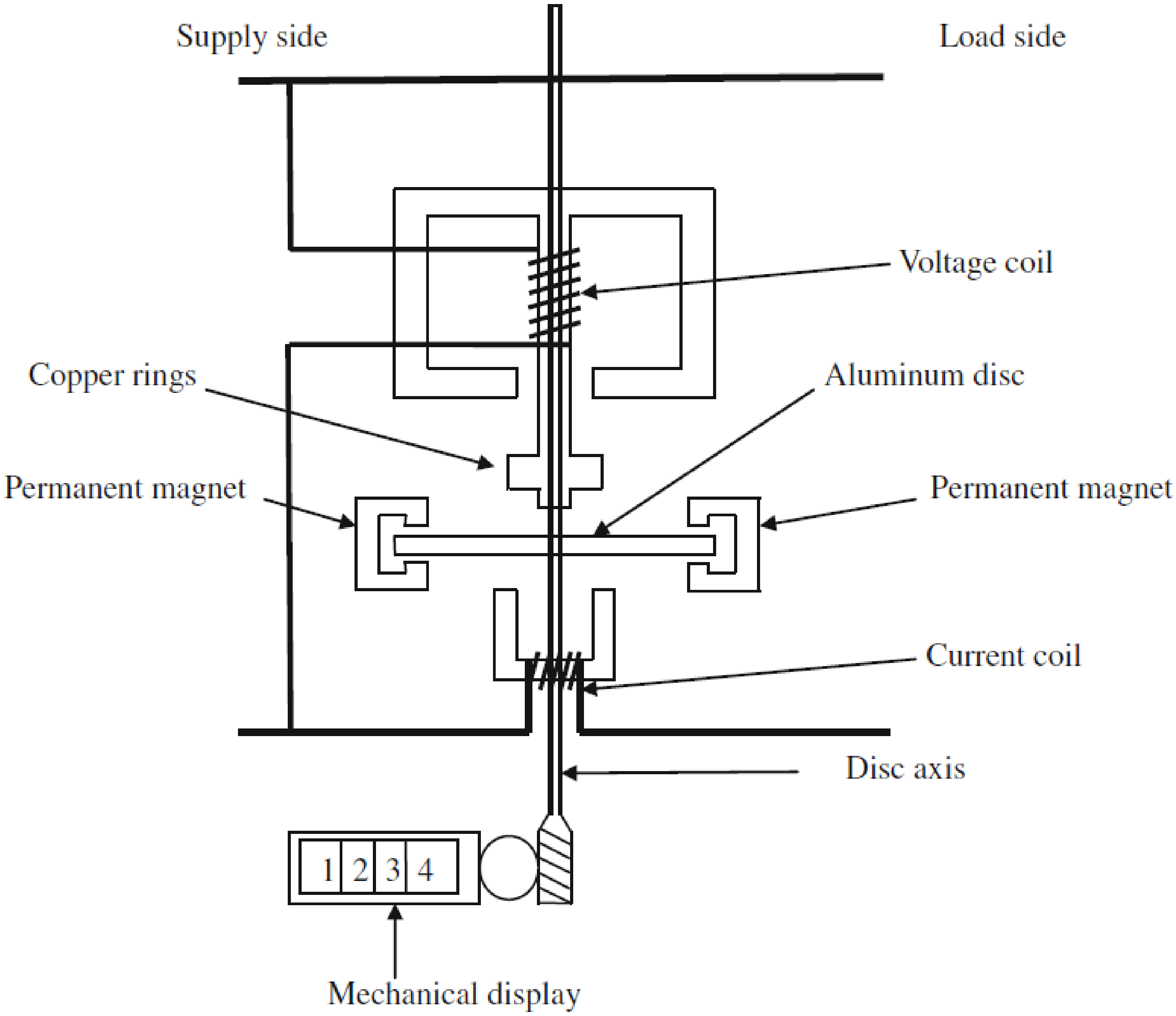


Figure 2.12: Internal components of the single-phase electromechanical meter

(Weranga et al., 2014:19)

The 90^{o} current and magnetic flux phase lags or phase delays in the voltage coil (owing to its highly inductive nature) can be calibrated using a lag coil (with its series connected lag-adjusting resistor located between the voltage coil and the disc, but not shown in Figure 2.12) and an adjustable copper rings (lag plate) on the central limb of the shunt magnet in a bid to maintain unity PF within the meter, so as to enhance accurate measurements (Kathiresh & Subahani, 2020:177; Bajpai & Reddy, 2021:66; Dimkpa et al., 2023:2639). The

90^{o} phase lags mentioned in the preceding paragraph is maintained using a lag coil or using the adjustable copper rings (adjusted in such a way that the magnetic flux produced by the voltage coil lags the supply voltage by a displacement angle of 90^{o} (Weranga et al., 2014:19; Kathiresh & Subahani, 2020:177; Bajpai & Reddy, 2021:66-67; Dimkpa et al., 2023:2639). Although, a few electromechanical meters use the lag coil with its lag-adjusting resistor to maintain the 90^{o} phase lags in the voltage coil (Weranga et al., 2014:19); but most electromechanical meters use the adjustable copper rings instead, an instance when the adjustable resistor of the lag coil will be undisturbed. The lag coil with its lag-adjusting resistor and the adjustable copper rings are also known as PF compensators (Bajpai & Reddy, 2021:67). The meter works at unity PF (after being calibrated by the lag coil or the copper rings), but still maintains the 90^{o} current and magnetic-flux phase lags with the supply voltage to ensure that the meter functions properly.

The interaction between the magnetic flux generated by the current coil and that produced by the voltage coil with the induced eddy currents in the aluminium disc causes a driving torque that spins or rotates the aluminium disc (Ahmad et al., 2016:90; Avancini et al., 2019:705; Bajpai & Reddy, 2021:67-68). The torque or force exerted on the meter disc is proportional to the product of the instantaneous voltage and current (instantaneous true power) consumed via the load circuit (Ekanayake et al., 2012:86; Kathiresh & Subahani, 2020:178; Bajpai & Reddy, 2021:67), as well as proportional to the number of rotations made by the aluminium disc (Ahmad et al., 2016:90; Bajpai & Reddy, 2021:67), while compensating for friction. A rotation in this regard means a complete spin of the aluminium disc of the meter from one point to another, which is also referred to as a revolution. When the aluminium disc rotates, it turns series of gears via the disc shaft, which resultantly move the register dials and record energy consumption in kilowatt-hours (Bajpai & Reddy, 2021:67). This is done by integrating the speed of rotation of the meter disc over time through the count of the number of disc revolutions (Weranga et al., 2014:19; Dimkpa et al., 2023:2639).

The rotation speed of the aluminium disc is controlled by the brake magnet (an adjustable permanent magnet positioned at the edge of the disc), with the help of the eddy currents induced in the disc by the magnetic fluxes produced by the electromagnets. The aluminium disc also spins between the gaps of the brake magnet as it does between the electromagnets. Eddy currents react with the magnetic flux of the brake magnet to provide the required opposing torque equal to the rotational speed of the aluminium disc. The opposing torque stalls the spinning of the disc when no power is being drawn by the load circuit. These two opposing equilibrium forces from the aluminium disc and the permanent or brake magnet allow the disc to rotate in accordance with the amount of the power being consumed through the load circuit (Kathiresh & Subahani, 2020:178; Bajpai & Reddy, 2021:67; Dimkpa et al., 2023:2639).

The meter constant, which is the number of revolutions per kWh of energy consumption (Bajpai & Reddy, 2021:70) of the meter is 600, as conspicuously written as 600 r/kWh on the nameplate of our sample electromechanical meter shown in Figure 2.11. This means that the meter disc makes 600 revolutions to register one unit (1 kWh) of energy consumed. We can approximately rewrite the meter constant as 1.7 watt-hour per revolution of the meter disc. The electromechanical meter constant is usually denoted by the symbol "Kh" (Dimkpa et al., 2023:2639). The more the active loads on the load circuit, the less time it takes the meter disc to make a revolution. The meter constant varies from meter to meter (Apogee, 2001), as the amount of energy consumed per revolution of the meter disc depends on vendor-design specifications (Primicanta, 2013:11). If for example an electrical appliance rated at 100 watts is connected to our sample electromechanical meter as load, it would take 60 seconds for the meter disc to make a revolution and register approximately 1.7 watt-hour of energy. The time per revolution of any electromechanical meter disc can be calculated using Equation 2.1 (Dimkpa et al., 2023:2639).

$$P = \frac{3600 \times Kh}{T} \tag{2.1}$$

The time (T in seconds) per revolution of the meter disc can be calculated from Equation 2.1 by making T the subject of formula, and then substituting for the values of the meter constant Kh and that of the power (P in watts) consumed by the load circuit into the rearranged equation. It should be noted again that the meter constant Kh of electromechanical meters is vendor-specific and varies for meters with different manufacturers. Electromechanical meters are still very common in the developing countries, but the developed countries are phasing them out in favour of the more-accurate and more-efficient electronic meters (Ahmad et al., 2016:90; Avancini et al., 2019:705).

2.3.2.2 Advanced metering infrastructure

Unlike the electromechanical meter in conventional grids which is a standalone metering device, metering in SG constitute a system (Anas et al., 2012:178) called the advanced metering infrastructure (AMI). The AMI is an integral component of the SG, which is an integrated hierarchical network system (Jiang et al., 2014:106-107; Yip et al., 2018:191), and comprises of SMs, communication networks, data collectors or concentrators, AMI server, and Meter Data Management System (MDMS) in its architecture, for intelligent control, better grid load management, and data management in the SG system (Yip et al., 2018:191; Yan & Wen, 2021; Nayak & Jaidhar, 2023:1). The AMI brings about an end-to-end electric metering between the consumers and the utilities (Althobaiti et al., 2021:159295), as shown in Figure 2.13.

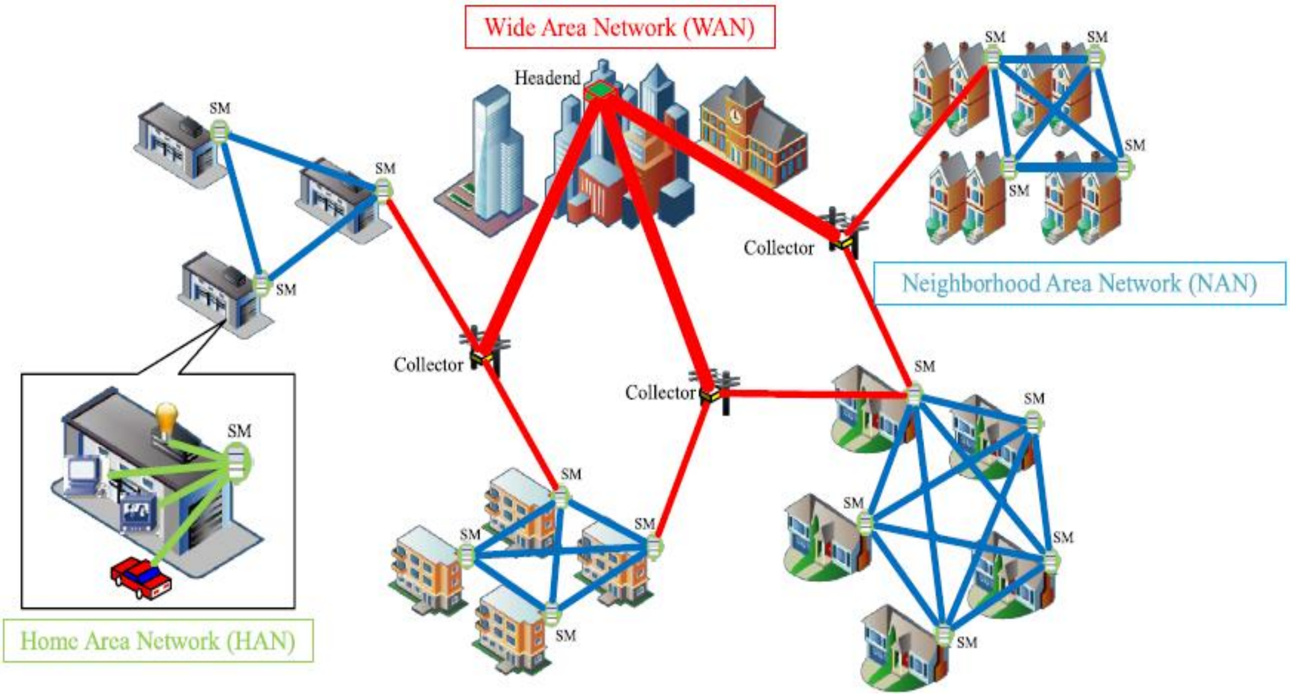


Figure 2.13: Architecture of the AMI

(Jiang et al., 2014:106)

The idea of the AMI to improve the demand-side management and promote energy efficiency started the SG concept (Fang et al., 2012:945). AMI is the modernization of the conventional electricity metering system by replacing the old electromechanical meters with SMs (Mashima & Cárdenas, 2012:210; Jiang et al., 2014:105; Yip, Wong, et al., 2017:230; Micheli et al., 2019:330), and allowing two-way reliable communication between electricity customers and the utilities (Aggarwal & Kumar, 2021:463).

AMI is an integrated and computerized metering system, a key technology and a core part of SG, with SMs, data management systems and bidirectional communication network links to the utilities (Jokar et al., 2016:216; Aggarwal & Kumar, 2021:463). The AMI system monitors electricity consumption, serves as a tool used for energy management and for billing purposes. The advent of AMI has opened the door for novel vulnerabilities in the electricity system because of the embedded communication layer (Aggarwal & Kumar, 2021:466; Xia et al., 2022:273-274). The AMI two-way communication allows the SMs to be read remotely and to implement and execute other grid management controls (Depuru et al., 2011b:2736; Jiang et al., 2014:105-106). The SG AMIs and their SMs has made the gathering of data used for ETD easier (Liao, Zhu, et al., 2024:5075). Data-driven ETD is less expensive and more efficient (Mujeeb et al., 2020; Kim et al., 2024:7).

Although, SMs with advanced networking and software tools are difficult to hack and tamper with (Depuru et al., 2011b:2741), but they are not totally immune to physical tampering, bypassing, and other conventional means of stealing electricity, despite the fact that SMs more robust and provide the cutting edge when compared with their conventional-meter counterparts (Shokoya & Raji, 2019a:98-99). This fact has still invariably makes ET a big issue in SG (Jiang et al., 2014:105; Aldegheishem et al., 2021:25036). Electromechanical meters could only be physically tampered with locally, attacks on SMs could be done locally and remotely (Jokar et al., 2016:216).

Attacks in AMI could be accomplished before the meter by preventing the meter from registering the energy consumed, at the meter by tampering with the stored data in the SM, and modifying the network by intercepting it and injecting false data into the communication link between the SM and the utility (Jiang et al., 2014:109; Jokar et al., 2016:216; Avancini et al., 2019:711). The attackers could also hack into the SG, disconnect the consumers remotely and compromise system operations of the utilities (Jiang et al., 2014:106; Viegas et al., 2017:1257). These attacks lead to disruption of normal readings, resulting to erroneous readings and causing NTL. Cyber-attacks on smart electric meters could compromise the software of the meter and cause it to start to send erroneous or fraudulent readings to the utilities (Viegas et al., 2017:1257; Yan & Wen, 2021).

- **AMI communication networks and technologies**

As could be seen from Figure 2.13, the AMI constitute different communication networks such as the Home Area Network (HAN), the Neighbourhood Area Network (NAN) and the Wide Area Network (WAN), making the SG a network of networks (Saponara & Bacchillone, 2012:1, 3; Bîrleanu et al., 2019:612; Micheli et al., 2019:330). The communication between these networks are Internet Protocol-based (IP-based) (Bîrleanu et al., 2019:612), and are used for data collection in the SG system (Jiang et al., 2014:106-107; Rastogi et al., 2016:15). IP-based networks and communications are more secure and efficient (Bîrleanu et al., 2019:612). Figure 2.14 takes a closer look at NAN architecture with its electrical and communication network flows in the AMI.

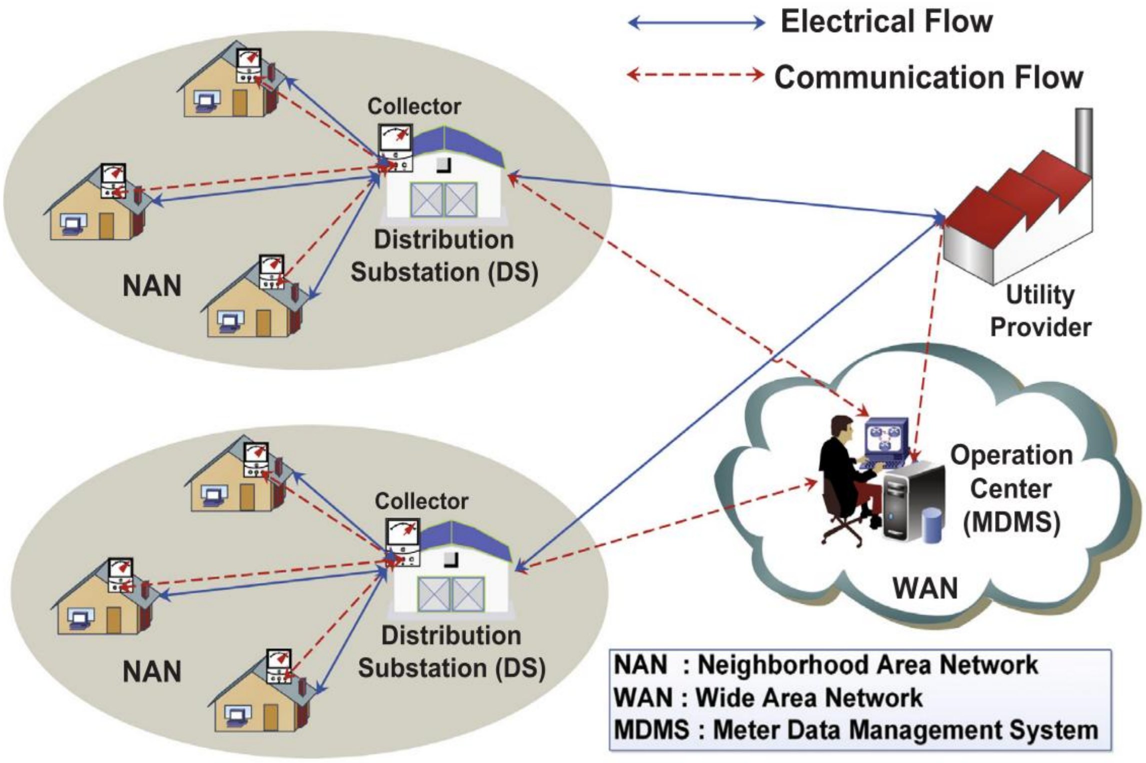

Electrical Flow
Communication Flow
Collector
Distribution Substation (DS)
NAN
Collector
Distribution Substation (DS)
NAN
Utility Provider
Operation Center (MDMS)
WAN
NAN : Neighborhood Area Network
WAN : Wide Area Network
MDMS : Meter Data Management System

Figure 2.14: The NAN architecture of the AMI

(Yip et al., 2018:191)

HAN is somewhat a Local Area Network (LAN) having the SM as its core (Jiang et al., 2014:107), with other home appliances and devices like smart sockets, smart appliances, in-home display, HVAC (heating, ventilation, and air conditioning) systems, EVs, microgenerators, etc., forming an integrated system (Ekanayake et al., 2012:95-96; Micheli et al., 2019:330). The NAN is a LAN network (Bîrleanu et al., 2019:612) of several neighbouring HANs or group of HANs with NAN data collector, a local access point, and metering data aggregation unit for the data of the neighbouring interconnected SMs of different homes (Jiang et al., 2014:107; Micheli et al., 2019:330). The NAN collector aggregates the cumulative SM data of several HANs in the same zone or service area and send it to headends at utility operation centres via WAN (Yip et al., 2018:191). The utility operation centres consists of headends and control centres. The WAN is however the network which connects all the NAN data collectors to utility headends (Yip et al., 2018:191; Micheli et al., 2019:330).

For the SMs to communicate with each other and the utility servers in the AMI, different available media or communication technologies are employed. Wired communication technologies that could be used are digital subscriber line (DSL), coaxial cables, optical fibre, Power Line Carrier (PLC) or Distribution Line Carrier (DLC), Ethernet, cable modems, Public Switched Telephone Network (PSTN), and an advanced form of PLC called Broadband over Power Lines (BPL); while the wireless communication technologies employed are IEEE 802.11s, ZigBee, Wavenis, Z-Wave, Bluetooth, Insteon, infrared, peer-to-peer (P2P), World Interoperability for Microwave Access (WiMAX), radio-frequency mesh, satellite communication, and network technologies affiliated to mobile communications like, Global System for Mobile Communications (GSM), Code Division Multiple Access (CDMA), General Packet Radio Service (GPRS), and 3G/4G technologies (Ekanayake et al., 2012:96; Saponara & Bacchillone, 2012:3-4; Rastogi et al., 2016:14-15; Porcu et al., 2021:8-9). 3G is the third-generation technology in cellular communications, while 4G is the fourth-generation technology in cellular communications. Internet is also used as a communication medium in the AMI, and may be used to connect a SM directly to the utility headend (Rastogi et al., 2016:14).

Low power short-distance wireless radio-frequency communication technologies like Wi-Fi, Bluetooth, ZigBee, Wavenis, Z-Wave and Insteon are HAN network solutions used to connect the appliances in the home with the SM (Saponara & Bacchillone, 2012:3-4; Rastogi et al., 2016:15), and allows appliance monitoring and control for better economic usage (Jiang et al., 2014:107). ZigBee is the most reliable and cost-efficient of all the HAN network solutions (Weranga et al., 2014:36). The communication technology deployed in NAN depends on the size of data being transferred (Ekanayake et al., 2012:98). Wi-Fi wireless radio technology has been suggested for NAN to send SM data to the collectors, but cellular or WiMAX technologies could also be employed (Jiang et al., 2014:107). For the WAN transmission of data to the utility headend, optical fibre Is proposed, but cellular and WiMAX technologies are also used as options (Jiang et al., 2014:107; Weranga et al., 2014:36). According to Rastogi et al. (2016:14), PLC is the best communication technology for establishing connection between the SMs of different households in NAN, because it does not require a separate communication medium, but the usage of the existing power lines. PLC could also be employed to send SM data from HAN to the collection points at the distribution stations (Weranga et al., 2014:36).

As previously established in Section 2.2.2.2, the electrical network and the communication network in the AMI are overlaid, and their flows are in a two-way fashion (Fang et al., 2012:944; Yip, Wong, et al., 2017:231). The electrical network of NAN allows power flow, while its communication network allows information flow which constitutes data and control signals (Depuru et al., 2011b:2737-2738; Yip, Wong, et al., 2017:238). The NAN comprises of the household SMs and their communication and electrical networks, the collector located at the distribution substation (secondary distribution substation) as shown in Figure 2.14. The utility control centres monitor the electrical and communication networks of the distribution system.

Usually, the SMs of various households in a NAN and the collector at the secondary distribution substation communicates wirelessly, while the collector at the secondary distribution substation, the primary distribution substation, and the headends at the operation centre communicate via a wired medium (Yip, Wong, et al., 2017:232). The utility distributes electricity from the primary distribution substation to the secondary distribution substation located in the neighbourhood of the electricity consumers. The secondary distribution substation provides electricity to all the consumers in the locality, and its endowed collector or master SMs aggregate all the household consumption profiles in the neighbourhood (Yip, Wong, et al., 2017:232; Yip et al., 2018:191). Interfaces on SMs which make connections using various communication technologies are available by default on the meter via its embedded radio adapters for wireless communications, and connection ports for wired communications (Knapp & Samani, 2013:48) as depicted in Figure 2.16.

- **Smart meter**

SM is a digital meter, an advanced and intelligent electronic meter used for energy measurement and communication (Khan et al., 2024:9). It is an improvement on the conventional electric meters (Kabalci & Kabalci, 2019:49), a next-generation electric meter (Ahmad et al., 2016:90), and the latest device in the art of electricity metering (Oloruntoba & Komolafe, 2018:15). The SM is like a computer in the interconnection of a vast SG network. Unlike the electromechanical meters which are manually read by the utility employees, the SM readings are automatically read and sent to the utility information systems in real time, giving accurate details on the use of energy (Rastogi et al., 2016:13-14; Micheli et al., 2019:330).

A digital electronic meter is genuinely “smart” if it is part of the AMI network, allowing the electric companies to read and monitor the customers’ electricity consumptions remotely and allowing the SMs of the customers to receive information from the utilities via a two-way communication channel in real time (Micheli et al., 2019:330). If an electronic meter is not part of the AMI, it is not being referred to as a SM (BSE, 2021; DeBoer, 2021). The SM is an entity in AMI (Anas et al., 2012:178) and one of the many applications of Internet of Things (IoT) (Rastogi et al., 2016:13). While the SM is the regarded as the heart of the AMI and the cornerstone of the modernized grid (Reinhardt & Pereira, 2021:1), the AMI is also considered as the heart of the entire SG system (Bîrleanu et al., 2019:611). The two-way communication between SMs and utilities via the AMI makes the SMs stand out from other forms of electronic meters. SMs are installed at the premises of electricity customers to record real-time electricity consumption and transmit the data to the utilities through a two-way communication channel. Like the electromechanical meters, SMs also exist as single or three-phase meters (Weranga et al., 2014:26). SMs optimize the use of electricity by assisting consumers to manage their loads to conserve energy and to consequently reduce their electricity bills. The intelligent smart energy meter is depicted in Figure 2.15.

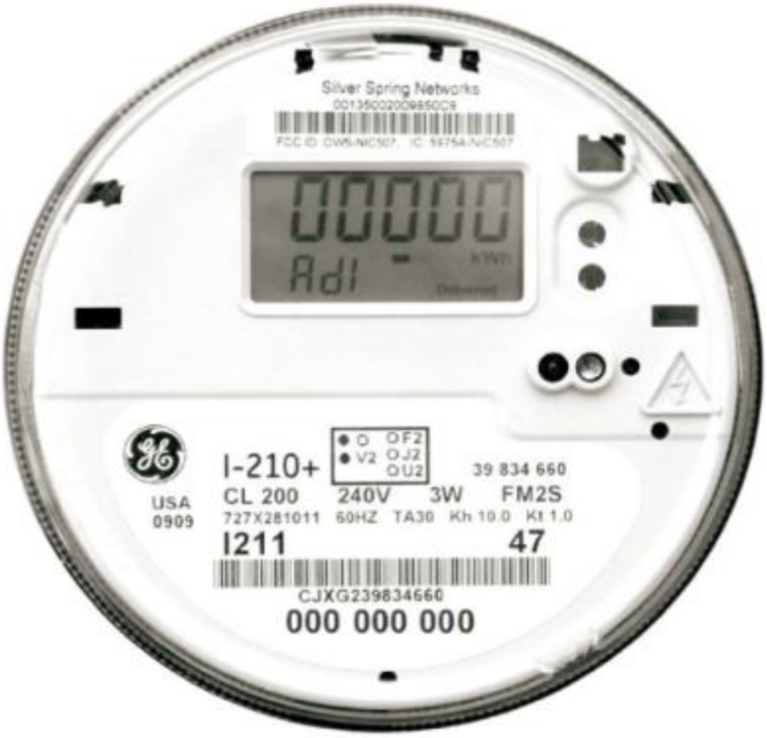


Figure 2.15: Smart meter

(Kabalci, 2016:309)

The key elements of a SM are the solid-state device itself, a microprocessor, and a communication network (Knapp & Samani, 2013:48). The microprocessor and local memory are for storing and transmitting the digital-meter measurements to the utilities via the communication network. Since we now have the more-robust and powerful microcontrollers at low cost, most SM processors are currently made of microcontrollers (Aurilio et al., 2014:1459).

Traditional electromechanical meters could only be compromised by physical tampering, while the introduction of AMI with its inherent SMs and the addition of a cyber layer in SG has opened new vulnerabilities for the electricity thieves to explore (Yip, Wong, et al., 2017:230; Aggarwal & Kumar, 2021:466; Xia et al., 2022:273-274). Physical tampering on SMs is easily detected by the utilities (Rastogi et al., 2016:13). Any zero reading on the meter is also being detected as the energy pilferers are effortlessly being identified by the utilities, since the utilities would be informed of such null reading through the AMI (Anas et al., 2012:178; Avancini et al., 2019:711; Shokoya & Raji, 2019a:100). The installation of SMs are expected to increase after the year 2020 (Ekanayake et al., 2012:84).

The SM is a hardware used for the periodical acquisition of the real-time energy consumption data (load or consumption profiles) that are being delivered to the utilities (Micheli et al., 2019:330). SMs record the energy consumed at stipulated time intervals per day (depending on the specific AMI deployments) and deliver them to the utilities (Mashima & Cárdenas, 2012:215). The utilities manage the timestamped SM load profiles using a software known as MDMS (Bîrleanu et al., 2019:611; Rendroyoko et al., 2021:405).

The MDMS, which is the data repository of the AMI, receives the SM data or the SM readings through the AMI server via the AMI communication medium, and then validate, adjust, and store them (Rendroyoko et al., 2021:403) in a real-time process known as dynamic load profiling. The stored SM data are then used for billing, ETD (by identifying potential fraudulent electricity consumers from among the SM readings or consumption profiles of consumers), outage control, demand response management to prevent system overloads, fault detection, and to determine which consumer are eligible to be connected and/or needed to be disconnected remotely, etc. (Jiang et al., 2014:106; Rendroyoko et al., 2021:405). The massive volume of data provided by SMs through AMI in SG have enhanced the opportunity of developing ETD technology driven by data (Liao, Zhu, et al., 2024:5075).

- **Hardware components of a smart meter and their functions**

The hardware components of a typical SM are power supply unit, voltage and current sensing unit, energy measurement unit (i.e., energy metering integrated circuit or energy metering IC), microcontroller unit (MCU), RTC, and communicating unit (Weranga et al., 2014:28), as shown in Figure 2.16. Basically, the SM works by continuously acquiring current and voltage signals from the utility supply, conditions the signals and convert them from analogue to digital via the analogue-to-digital converter (ADC), computes and communicates the output signals to the utilities or perhaps receive control signals or commands from the utilities (Ekanayake et al., 2012:87-99; Weranga et al., 2014:27-28).

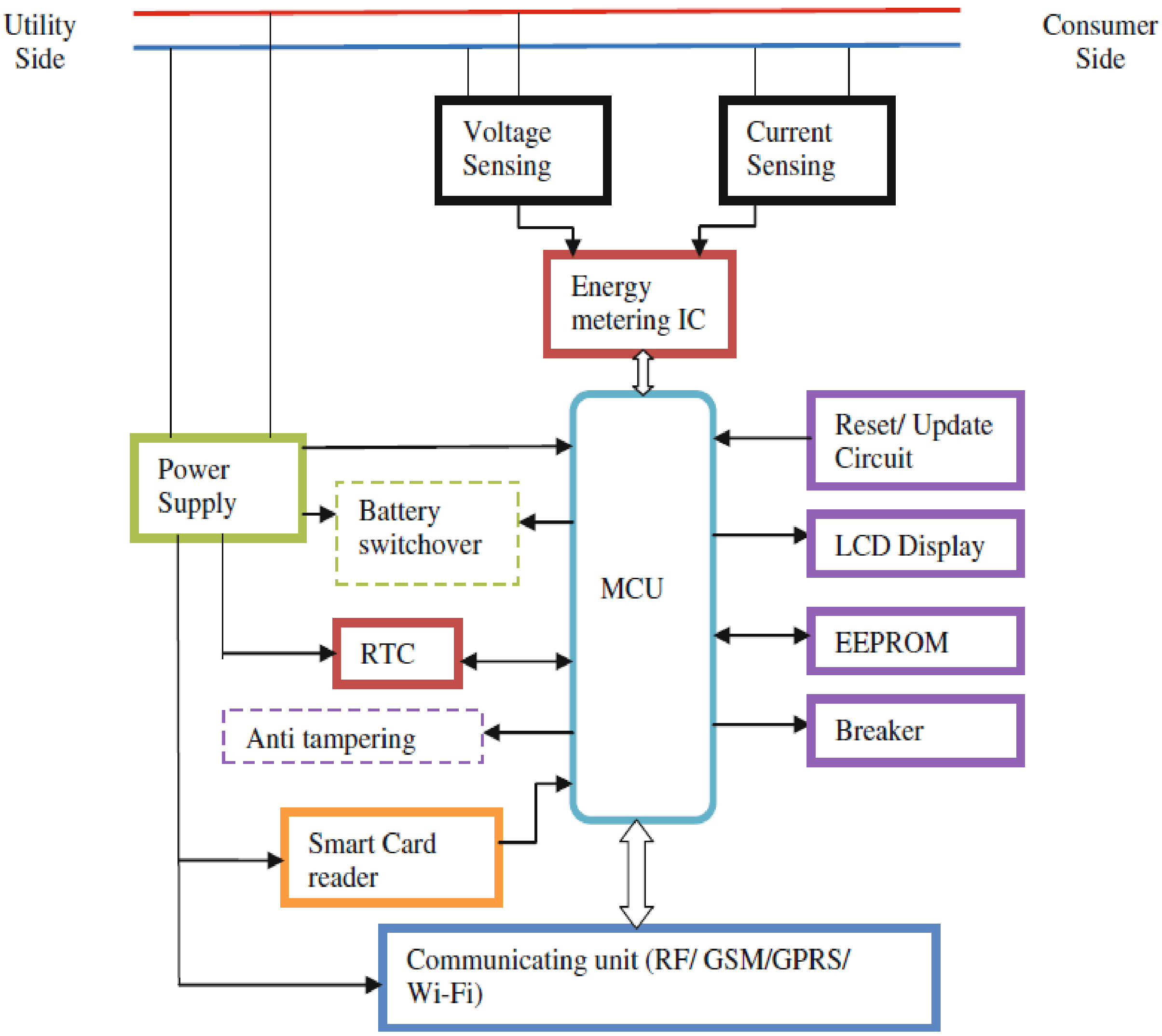


Figure 2.16: Internal hardware components of a smart meter (Weranga et al., 2014:28)

The power supply unit powers the SM by driving its hardware components. The battery-switchover circuitry is used to switch over to the meter rechargeable backup-battery, to power the SM in case there is mains power failure from the utilities. The backup battery is being charged and controlled by the filtered system power output from the power supply unit. The voltage sensing unit is a voltage sensor, while the current sensing unit is a current sensor, employed to capture the voltage and current input signals from the utility supply. Typically, low-cost SMs use shunt resistors as current sensors, and simple resistor dividers as voltage sensors. Other available current sensors used in SMs are hall effect-based linear current sensors, current transformers (CTs), and Rogowski coils. Signal conditioning, analogue-to-digital conversion by the ADC and computation or energy calculations take place in the energy measurement unit or the energy metering IC (Ekanayake et al., 2012:87-89; Weranga et al., 2014:28-31, 33-34).

Signal conditioning is the preparation of analogue input signals for digital conversion. Signal conditioning is done by the digital signal processor (DSP) embedded in the energy metering IC. Computation involves performing arithmetic operations (energy calculations) on the voltage and current input signals, timestamping or time-referencing the energy consumption data and preparing them for communication to the output peripherals, etc. The energy consumption calculation is done by multiplying the digital values of the voltage and current it collects from the voltage sensor and the current sensor of the meter. This metrological procedure is done at steady intervals to determine the energy used or consumed. Before computation takes place, the voltage and current values from the voltage and current sensor circuits are converted from analogue to digital by the ADC of the energy metering IC. The energy metering IC also provides information on active, reactive, and apparent power, etc. Energy metering IC in a SM could be a single-phase or a three-phase chip. Single-phase SMs use single-phase energy metering ICs while three-phase SMs use three-phase energy metering ICs. For SMs that do not have a separate energy metering IC, the MCU would be built to perform its functions (Ekanayake et al., 2012:89-95; Weranga et al., 201434-35).

The MCU is referred to as the core of the SM where all the meter functions take place. The functions of other hardware components of the SM are controlled by the MCU. The MCU controls power management, tamper detection, reading of the smart card for the available units of electricity, and the display of electrical parameters like the time-of-use or time-of-day tariff, electricity cost, and power outages on the LCD of the meter and on an in-home display. The in-home display is a separate handy display unit placed at any convenient place within the home to make the SM data easily accessible to the customers. The MCU does data calculations depending on the data received and then manages the data with electrically erasable programmable read-only memory (EEPROM). It also communicates with the energy metering IC and other communication devices associated with the meter. The RTC of the SM (equipped with a dedicated clock battery meant strictly for providing continuous power during maintenance or power failure) provides information about alarm signals, time of the day, and the current date. Timestamping of energy consumption data is done by RTC during their computations (Ekanayake et al., 2012:95; Weranga et al., 2014:35-36).

SMs are also equipped with breaker, anti-tampering circuitry and reset/update circuitry (Weranga et al., 2014:28). Breaker or the SM circuit breaker trips off the power when consumers consume more than their subscriptions or beyond the energy capacity allocated to them by the power companies, or when the breaker responds to remote command from the utilities to connect/disconnect power into the building. For those customers who may want to fiddle with their SMs in a bid to steal electricity, the meter is equipped with anti-tampering sensors. Anti-tampering is a tamper detection security feature for forestalling tampering and protecting the device (Ngamchuen & Pirak, 2013). When the customer tampers with the meter, the SM anti-tampering sensor detects it, and the anti-tampering circuitry sends signals to the utilities through the communication unit via the MCU, informing them of the illicit act. The reset/update circuitry allows the meter to be reset to factory settings and/or to update the SM software.

2.4 Electricity theft: causes, effects, detection and mitigation techniques

There is a need to discuss the causes, effects, detection and mitigation of electricity theft or NTL before delving fully into its various curtailing methods and solutions that are mentioned in the literature.

2.4.1 Causes of electricity theft

Several factors drive consumers to indulge in illegal electricity consumption. Some of these factors are controllable, while some are almost uncontrollable because of unpredictable human behaviours (Jiang et al., 2014:109; Gao et al., 2023:4565). The motivation behind ET is the bait to completely evade payment, manipulate energy meters to read less than the actual consumption and/or partly hide some stolen energy (to convey less overall consumption) in a bid to reduce the entirety of bills payable to the utilities (Depuru et al., 2011a:1010; Appiah et al., 2023:1). Some consumers use electricity legally for minor household loads, and tap it illegally to operate hefty loads (Ahmad et al., 2018:2917). This is commonly done at night times when the possibility of utility-employee inspection is relatively low (Depuru et al., 2011c:2).

The utility companies do not have the knowledge of how the energy deficits caused by theft are taken out of the grid. The cause of NTL is unexplainable within the ambience of the electricity grid system, until superficially detected and confirmed. This further establishes the fact that those factors that cause ET are external to the electric grid system. Utilities cannot account for such losses, which would consequently resort to unbilled electric units. The only losses the utilities are aware of are the unpaid bills. When customers fail to pay their bills, the utility suffers revenue losses; and such revenue paucity ultimately counts towards NTL (Jamil & Ahmad, 2019:453).

The parameters that cause ET are multifarious and complex in nature (Depuru et al., 2011a:1007). Some of these parameters are social, some are economical, some are managerial, some are political, while some are caused by the criminal and corruption tendencies on the part of the electricity consumers and the utility employees, etc.

The main cause of ET in the developing countries is related to poverty (Yurtseven, 2015:70). High unemployment rate, a causal effect of most of the severe economic conditions faced by electricity customers, is a huge factor responsible for most ETs (Depuru et al., 2011a:1009; Shokoya & Raji, 2019a:97; Shokoya & Raji, 2019b:469). Poor or low income is another financial-limiting factor which causes ET (Mirza & Hashmi, 2015:602). Weak financial situation of electricity consumers is one of the causes of ET and is mainly responsible for non-payment or non-remittance of electricity bills by the customers (Depuru et al., 2011a:1007). Some consumers who had been genuine and used to paying their electricity bills regularly could as well turn to start stealing electricity owing to their prevailing unfavourable financial conditions.

Non-payment of electricity bills is not only restricted to poor communities or indigent citizens, but also to rich and influential citizens who know their power connections would not be interrupted whether they pay their bills or not (Smith, 2004:2069; Yakubu et al., 2018:611). Some government agencies also default in paying their electricity bills (Depuru et al., 2011a:1010-1011). Non-payment of electricity bills itself is a form of NTL as discussed in Section 1.3.4 of Chapter 1, no matter the reasons or excuses behind the consumers' inability to pay (Lewis, 2015:118, 121; Bihl & Hajjar, 2017:272-273). Non-payment of electricity bills is an indirect way of engaging in theft, since the benefit of unsettled bills is equivalent to the units of stolen electricity (Jamil & Ahmad, 2019:453). Also, poor power infrastructure and inconsistencies in distribution systems and metering cause ET in the developing countries (Jiang et al., 2014:108).

In South Africa, vandalizing utility equipment, stealing of electric cables, scooping oil from transformers at substations, and selling of illegal prepaid vouchers (ghost vending) also contribute to NTL (Shokoya & Raji, 2019a:97; Kambule & Nwulu, 2021:43).

In the developed countries like the United States and Canada, some citizens who unlawfully grow marijuana steal electricity to conceal their huge overall electricity usage, as a means to avoid suspicion and subsequent inspection and prosecution by the law enforcement agents (Depuru et al., 2011a:1010; Jiang et al., 2014:108). Electricity is also popularly stolen by Bitcoin miners to operate their Bitcoin-mining machines. Bitcoin miners engage in stealing electricity due to the high electricity consumption required by Bitcoin-mining computers during Bitcoin production, and in the production of cryptocurrencies in general (Dindar & Gül, 2021).

While some unscrupulous electricity customers tend to try to bribe their way out after being caught to have stolen electricity either by meter tampering, meter bypassing, or direct hooking of wires on the distribution lines etc. (Smith, 2004:2069), some corrupt utility employees also tend to subscribe to these crooked gestures and collude with them to arrange and negotiate settlements. At times, some unprincipled utility employees initiate the corruption process themselves by offering to help the customers tamper their meters to lower their billable readings. This is in a bid to influence the customers to offer them bribes in return, instead of being forthright and carrying out their duties appropriately according to their work ethics. This customer-employee corruption connivance spurs ET, as the action reduces the tendencies of the defaulting customers being detected, fined, or prosecuted. This infamous mutual corruption does not only embolden the dishonest electricity customers to continue to indulge in the despicable acts of stealing electricity, but also generate unofficial incomes for the vicious employees (Jamil & Ahmad, 2019:452, 458; Ghori et al., 2020:16033). This employee-customer collusion causes a form of NTL called billing irregularities (Depuru et al., 2011a:1007).

Billing irregularities are caused when the utility employees intentionally record lower readings as against the actual readings on the energy meter to fulfil their part of the corruption deal. This is different from the billing irregularities occasioned by errors in meter readings (Sharma et al., 2016:43) and accounting errors made during the preparation of customers' billing invoices (Bihl & Hajjar, 2018:271), which are entirely due to human errors (Glauner et al., 2017:761). Some corrupt politicians also cause billing irregularities by aiding and abetting ET (Depuru et al., 2011a:1009-1010; Gaur & Gupta, 2016:129). ET and corruption are intertwined. High rates of ET are evidences of corruption within the electric utility companies. ET thrives where corruption thrives (Smith, 2004:2072). The concept of billing irregularities as one of the forms of ET has been discussed in Section 1.3.3 of Chapter 1.

The erroneous belief that stealing from neighbours, family, or friends is criminal, while stealing from the state or publicly owned utility companies is acceptable, also contributes to

ET (Depuru et al., 2011a:1009; Shokoya & Raji, 2019a:97). Some dishonest customers derive their motivation for engaging in power theft from this fictitious notion. Such a notion is most common amongst the citizens of developing countries. They believe anything that comes from the state or publicly-owned sectors should be given free of charge. Some of these citizens particularly presume that electricity should be regarded as a social service (Onat, 2018:166; Ojoye, 2019; Shokoya & Raji, 2019b:469) or be given by entitlement (Robinson, 2014). This belief system is malicious and criminal, as electricity is not free anywhere in the world or given deliberately on an entitlement or right basis. Electric utilities and other public utilities are not charities, but business institutions that need to make sufficient profits to maintain and sustain them.

Unmetered supply which gives rise to estimated billings (Gaur & Gupta, 2016:130; Shokoya & Raji, 2019b:469; Soyemi et al., 2021:1); and defective or faulty meters (Hashmi & Priolkar, 2015:1424) which generate erroneous or false readings are also some of the causes of NTL.

Some places are a no-go area for the utility employees because they are dangerous territories. Going to inspect or claim electricity bills in these areas could be a perilous mission. However, the utilities have already supplied those areas with electricity. Most residences in these areas are informal, while most residents there are poor and connect to the grid through illegal connections. Unmanageable areas with high crime rates such as favelas in Brazil, and slums in other countries have such characteristics. Inhabitants of such areas are potentially hostile to the utility employees who come around with the motive of removing their illegal connections, fining them, compelling them to pay their bills or entirely disconnecting them from the grid if they are not able to pay. Utility employees fear physical attacks in such areas and avoid going there for inspections, let alone attempting any disconnection. The utilities generate very low income or at most times, are unable to generate any income from those uncontrollable areas. Cases like this cause loss of revenues to the utilities and eventually contribute to NTL (Antmann, 2009:26, 33; Glauner, 2019:6).

Other factors that cause ET are higher energy tariffs. Higher electricity prices discourage some electricity customers from wanting to pay their bills (Smith, 2004:2069-2070) irrespective of whether they are customers of developed countries or not. Illiteracy amongst electricity consumers about the fact that that there are established laws that criminalize ET and make them prosecutable if found culpable (Depuru et al., 2011a:1009; Shokoya & Raji, 2019a:97; Shokoya & Raji, 2019b:469) is also a contributory factor. Epileptic supply

(Shokoya & Raji, 2019b:467-469) or outright lack of electricity supply (Depuru et al., 2011a:1010) in some locations are also reasons some fellows indulge in stealing electricity.

Finally, weak enforcement of the law against ET culprits encourages them to carry on (Yakubu et al., 2018:611-612, 614, 616). Countries that do not strictly enforce the law to punish electricity offenders create enabling environment for the menace to thrive and such countries record high proportions of ET (Depuru et al., 2011a:1009).

2.4.2 Effects of electricity theft

The effects of ET focus on the impacts of stealing electricity. ET is costly (Lewis, 2015:119, 121), as it comes with critical consequences and also very challenging to detect and curtail (Fei et al., 2022:1; Stracqualursi et al., 2023:1). The difficulty in curtailing ET is due to the various tricky means by which it is pilfered, and also owing to the fact that stealing of electricity could be carried out intermittently and may not always be done continuously (Gao et al., 2023:4565; Wang et al., 2023:1, 20).

2.4.2.1 Economic effects

The electricity sector is very crucial to the economic development of every nation (Stracqualursi et al., 2023:2). According to surveys, ET has caused economic losses to countries around the world (S. Zhu et al., 2024:15478). The direct adverse effect of power theft is that it causes losses of huge revenues to the utilities (Arango et al., 2017:570; Zheng et al., 2018:1606). Revenue losses to the utilities is the most-significant negative effect of ET mentioned in the literature (Smith, 2004:2072; Messinis & Hatziargyriou, 2018:251). Since ET is a global phenomenon (Stracqualursi et al., 2023:1), electric utilities of all countries of the world lose a lot of revenue annually, and thus contributing to national financial losses. Apart from the direct financial losses to electric utilities worldwide, the effect of poor electricity supply owing to ET undermines economic activities of countries, leading to corresponding reduction in national revenues as evaluated through losses in gross domestic products (GDPs) in various realms. GDP losses also immensely contribute to the annual cumulative financial losses of nations globally (Ahmed et al., 2022:579; Wabukala et al., 2023:2).

The total annual financial losses incurred globally by all electric utilities due to ET is estimated to be around US$100 billion (Coma-Puig et al., 2024:2705; Kim et al., 2024:2; Shahzadi et al., 2024:2; L. Zhu et al., 2024:256). Out of this whopping US$100 billion in losses, the developing countries are responsible for losses of up to around US$64.7 billion, while the rest of the world account for about US$31.3 billion in financial losses (Energy Central, 2019; Khan et al., 2023:537).

To establish how prevalent the ET scourge is biting around the world, some approximate country-specific annual financial losses across the developed and the developing countries will be mentioned. These revenue losses to the utilities create a setback in financial and economic prosperities of the different countries (Petrlik et al., 2022:420; Naeem, Javaid, et al., 2023:3). The huge national financial losses inflicted by ET as discussed in the succeeding paragraphs are estimated values, based on the fact that it is not possible to precisely measure ET or NTL (Fragkioudaki et al., 2016:44; Viegas et al., 2017:1260).

In the developed countries, the United States loses about US$6 billion (Khan et al., 2024:1), United Kingdom loses around £173 million (Ullah et al., 2022:18681), Australia loses an estimate of A$15 million (Robinson, 2014), while Germany, Spain, and Italy lose around €504 million, €426 million, and €408 million respectively (Kwarteng et al., 2023:7) to ET every year.

Still in the developed terrain, the yearly financial losses brought about by ET in Canada have been reported on provincial basis. Most of the ETs in Canada occur majorly due to marijuana-grow operations (Tweed, 2013). ET costs the Ontario province of Canada around C$500 million yearly (Kelly-Detwiler, 2013). BC Hydro, an electric utility in the British Columbia province of Canada reportedly loses approximately C$100 million to ET annually (Kambule & Nwulu, 2021:42); while Hydro-Québec, an electric utility in the Québec province of the North American country could lose up to C$75 million per annum on account of ET (Jones, 2021). The sum of the reported financial losses caused by ET per annum from the already mentioned three provinces of Canada (out of the total ten provinces and three territories that make up the entirety of Canada) is obviously above C$500 million. This is in consonance with the Canadian Government's estimate that the country loses over C$500 million in annual utility losses due to ET, as reportedly remarked by Zach Pollock in Tweed (2013).

In the developing countries, larger sums (with respect to the size of the economies of the different nations) are lost to ET every year. South Africa loses at least R20 billion (Mujuzi, 2020:79) every year to ET. Mozambique loses US$100 million (Kambule & Nwulu, 2021:43), while Zimbabwe loses around Z$237 billion (Kambule & Nwulu, 2021:43). In Nigeria, the eleven electricity distribution companies in the country lose about ₦33 billion monthly to ET, which cumulatively translates to around ₦396 billion in energy-theft losses per year (Okwumbu-Imafidon, 2020). Ghana loses over US$1 billion (Otchere-Appiah et al., 2021:3), Kenya loses about KSh18 billion (Amadala, 2021), Rwanda loses FRw1.9 billion (Iribagiza, 2020), Liberia loses around US$48 million (Boayue, 2022), Tunisia loses US$106.8 million (North Africa Post, 2021), Morocco loses MAD 1.2 billion which is equivalent to US$131.4 million (Mebtoul, 2020), Russia loses about US$5.1 billion (Lepolesa et al., 2022:39638), while Türkiye loses approximately US$1 billion (Yurtseven, 2015:71) every year to ET.

Further on the financial losses to ET in the developing countries, Malaysia’s losses were up to RM500 million (Abdullateef et al., 2012:250) annually, Pakistan loses over Rs53 billion (Aziz et al., 2020) which is an equivalent of US$0.89 billion (Javaid, 2021:162936) yearly to ET. Taiwan loses around NT$1 billion (Su et al., 2016:493), China as a whole loses US$560 million every year (Yao et al., 2023:11162), while Fujian, a province in the Southeastern coast of China, loses more than CN¥100 million (Pamir et al., 2023:3576) per year on account of ET. Jamaica loses approximately US$46 million (Lewis, 2015:128), Honduras loses approximately US$13 million (Naeem, Aslam, et al., 2023:59496), Puerto Rico loses US$400 million (Anwar et al., 2020:2138), Ecuador loses around US$200 million (TBY, 2014), Mexico loses Mex$25.7 billion (Serrano, 2019), Peru loses S/103 million (Petrlik et al., 2022:420), and Brazil loses around US$10.5 billion (Ali et al., 2023:2) to ET every year. Meanwhile, India, the country with the highest financial losses to ET (Xia et al., 2022:274), loses at least US$16.2 billion (Ali et al., 2023:2) annually to the ET menace.

The ET-inflicted financial losses of some countries as stated in the preceding paragraphs tend to spur GDP losses in those realms (Ahmed et al., 2022:579; Wabukala et al., 2023:2). ET has compounded the economic misfortunes of Nigeria and the power crisis in the West African country has also demystified its supposed economic mightiness amongst fellow African nations (Shokoya & Raji, 2019b:467, 469). Financial losses due to ET contribute immensely to the economic woes of any country of the world (Aslam, Javaid, et al., 2020:2) and also result in lack of investments in the power sectors (Fragkioudaki et al., 2016:44; Jamil & Ahmad, 2019:452).

As already intimated, theft of electricity and its resulting economic impasse impacts negatively on national GDPs of countries (Wabukala et al., 2023:2). The ET menace caused about 1.5% reduction in the GDP of India (Otchere-Appiah et al., 2021:2), and could averagely cause losses greater than 0.5% of GDP in the sub-Saharan Africa, and as much as 1.2% of GDP losses in some other countries within the sub-Saharan African terrain (Antmann, 2009:9). The GDP losses in India owing to ET have recently been reported to be up to 2.5% from the initial 1.5%, translating to about US$14.8 billion in India's financial losses (Ahmed et al., 2022:579). Generally, power interruption causes approximate GDP losses in the range of 1% to 5% in the sub-Saharan African countries (Trace, 2020). These economic losses also contribute to a decline in the human development index (HDI) of every country. High level of NTL exists in the developing countries, while the developed countries record low NTL cases (Viegas et al., 2017:1256; Stracqualursi et al., 2023:1). NTL variations among countries are broadly dependent on their level of developments as revealed by their respective HDIs and GDPs (Glauner, 2019:7; Osypova, 2020:14). Renowned metrics such as HDI and GDP are typical indicators published periodically by the United Nations to determine the development statuses of countries (Conceição & UNDP, 2019; Glauner, 2019:7; Osypova, 2020:14).

The growth and sustainability of any industry is hinged on capacity building. The economic effect of ET is huge, as it hinders the electric utility companies from investing in system rehabilitation and capacity improvement (Jamil & Ahmad, 2019:452; Hassan et al., 2022:2). Capacity addition to the electricity supply infrastructure is very important to shrink the cleavage between the demand and supply of electricity, and to promote sustainability. Capacity addition takes care of the events when there are excessive demands for electricity. Private sectors which are expected to invest in the electricity sector to increase capacity are unwilling to do so because of ET (Jamil & Ahmad, 2019:458).

ET makes the electricity sector an unattractive venture to potential investors. The horrible effects of ET discourage electricity stakeholders from wanting to invest their hard-earned monies in the power sector, and such investment dearth would eventually lead to supply shortfall (Jamil & Ahmad, 2019:458). The potential private investors' fear of ET is notable and understandable because no one wants to get involved in any business that may be dead on arrival owing to the persistent ET scourge right from inception. Theft of electricity also hinders human development. The utilities may not be able to improve the existing members of staff by sending them on trainings that would improve their quality of services, and may also be unable to employ more members of staff because of the financial paucity brought about by ET (Lewis, 2015:121).

2.4.2.2 Technical effects

Apart from the immense revenue losses (Zheng et al., 2018:1606) which come as a huge drawback to the sustainability of the electric supply companies, ET also undermines the efficiency and security of the electricity grid (Fragkioudaki et al., 2016:44). Stealing of electricity overloads the utility generating units and could ultimately trip or shut generators down abruptly (Depuru et al., 2011a:1008; Shokoya & Raji, 2019a:97). Overload is a form of TL caused by commercial losses (Abaide et al., 2010:2; Poudel & Dhungana, 2022), because the unanticipated or emergency increase in grid load causes corresponding increase in TL beyond the expected levels (Karimi et al., 2020). Overvoltage and/or congestion stress and overstretch the network equipment. Overloading the generating units is the potential cause of overvoltage and performance drop (Depuru et al., 2011a:1008; Fragkioudaki et al., 2016:44). All these lead to irregularities in power supplies, damage to the grid infrastructure and thus cause system failures (Yip, Wong, et al., 2017:230; Shokoya & Raji, 2019b:469).

System overloads as triggered by erratic load increase occasioned by ET cause supply shortfalls, power interruptions or disruptions, system failures, instabilities and decrease in grid frequencies (Anas et al., 2012:180; Lewis, 2015:121; Kocaman & Tümen, 2020:1). The more the ET-inflicted damage caused by overloading the generating units and stressing the grid equipment, the more the maintenance costs increase. Since the utilities are insolvent in meeting up with their financial obligations towards the maintenance and upgrade of the electricity grid owing to the liquidity crunch caused by ET, the unexpected and unpredictable additional loads brought about by theft consequently lead to electricity interruptions which cause reliability issues. As hinted earlier, these Interruptions come in the form of a drop in the quality of power supply known as brownout, or a complete power outage otherwise known as blackout (Depuru et al., 2011a:1008; Lewis, 2015:119, 121; Fragkioudaki et al., 2016:44; Kruse et al., 2021:1; Petrlik et al., 2022:420). Electrical surge caused by load imbalance (overload) was one of the causes of the blackout that occurred in North America in August 2003 (Casey et al., 2020:1, 3).

Persistent overloading of the electric power system may eventually lead to power rationing known as load shedding (Anas et al., 2012:180) or rolling blackouts (Nduhuura et al., 2020:2; Nduhuura et al., 2021:7). ET causes load shedding after wreaking energy shortfall (Anas et al., 2012:180; Mujuzi, 2020:78). Load shedding is a power management measure which helps to distribute power demand and prevent countrywide blackouts. With load-shedding scheme, power supply is mandatorily rationed, and supply to some designated locations is temporarily shut down when the power system is constrained, that is, when supply is insufficient to cater for demand. Load shedding could be used to compensate for power shortage and to ascertain security of supply. Load shedding is an emergency event implemented to salvage the power generating units of utilities from imminent breakdown, prevent a nationwide power outage (total blackout), and protect electricity grids (Eskom, 2013). Power shutdowns owing to load shedding are scheduled and controlled to prevent complete power system collapse (Trace, 2020). Load shedding is temporarily discomforting to the electricity customers, but the endurance would just be for a short while, serving as a provision for preventing longer hideous power outage situations. Load shedding scheme could also be used to manage peak-period demand pressure, to ascertain energy balance in the power system (Depuru et al., 2011a:1008).

Load shedding, which started in recent years in South Africa (Grootes, 2019), is now a popular occurrence in the Southern African country. Load shedding occurs mainly because of the undue pressure caused by power system overload (Trace, 2020). ET is one of the stimulators of power-system overload which causes electricity shortage that eventually leads to incessant load shedding in South Africa (Shokoya & Raji, 2019a:96-97; Mujuzi, 2020:78-79). To cater for the persistent power generation deficits (worsened with the spate of ET) bedevilling Nigeria, load shedding is inevitably and perpetually implemented in the country (Shokoya & Raji, 2019b:467-468). Load shedding is also being implemented across many other developing countries, owing to limited generation capacities (Oluwasuji et al., 2018;1590; Oluwasuji et al., 2020:1-2), and because of the added grid-strains caused by ET (Nduhuura et al., 2020:2).

Generally, overloading the grid hampers electricity quality, reliability and sustainability (Depuru et al., 2011a:1008; Yip, Wong, et al., 2017:230; Guarda et al., 2023:1). Aside the mentioned detrimental ET effects of overloading the grid, overloading may also cause damage to the appliances of honest legitimate customers (Depuru et al., 2011a:1008; Fragkioudaki et al., 2016:44), or even cause instigation of power surges that could damage electric wirings and cause fire outbreaks (Zheng et al., 2018:1606; Petrlik et al., 2022:420).

2.4.2.3 Environmental effects

ET is detrimental to public safety (Zheng et al., 2018:1606; Khan et al., 2024:2), as electricity thieves ignore this important factor when carrying out their illicit acts. Electricity thieves do not care, notwithstanding they put the lives of others in danger just to accomplish their malevolent objectives. Cables are carelessly laid when they steal electricity, and hence they imminently put the lives of others in danger. Electric shock hazards and/or fatalities to innocent persons may occur due to carelessly laid cables, and at most times, the power filchers themselves put their lives in jeopardy by risking great injuries or death (Hall, 2015; Petrlik et al., 2022:420; Stracqualursi et al., 2023:1). Apart from these, the electric utility employees too also stand a great risk of these hazards during maintenance and inspection activities (Meuse, 2016).

More carbon emission occurs while burning more coal, gas, or other limited natural resources (Ma et al., 2013:36; Kocaman & Tümen, 2020:1) during the generation of more electricity to stabilize the grid and to make up for the power deficits caused by ET (Fragkioudaki et al., 2016:44). This causes more atmospheric pollution (Glauner et al., 2017:761), and also make the Earth vulnerable to climate change (Osmanski, 2020).

2.4.3 Electricity-theft sufferers

Worthy of separate mention are those that are at the receiving end of the ET menace. ET causes financial losses to the utilities and inflict technical damages to the grid infrastructure. Moreover, the electricity crises caused by power theft affect economic activities causing drops in national GDPs. This is in addition to the risk of poor-quality supply that could damage the appliances of honest customers, outright supply outages, or even at times fire outbreaks. These adverse effects of electricity pilferage have been discussed in Sections 2.4.2, 2.4.2.1, 2.4.2.2, and 2.4.2.3. Those who get the direct backlashes of ET have also been somewhat mentioned in those sections during discussions. The burden of ET is shared amongst electricity supply companies, honest legitimate consumers or customers, and nations at large (Antmann, 2009:7; Viegas et al., 2017:1256).

To retrieve part of the financial losses caused to the utilities by electricity thieves, the utilities also tend to apportion part of the huge theft-driven revenue losses by passing them to the legal paying customers (Kocaman & Tümen, 2020:2; Guarda et al., 2023:1). Passing part of the revenue shortfalls caused by ET to honest customers is done by increasing the electricity tariff or rate (Depuru et al., 2011a:1008-1009; Anas et al., 2012:180; Guarda et al., 2023:1), and/or sharing part of the huge pecuniary losses amongst benign legitimate customers to shrink the financial-loss gaps (Yurtseven, 2015:71; Yakubu et al., 2018:611; Kocaman & Tümen, 2020:1-2). Each honest electricity customer in the UK has been reported to be paying extra £30 on their yearly electricity bills owing to ET (Xia et al., 2022:274). Unfortunately, this is the sad reality of ET, an unavoidable ripple or domino effect of it. The loss sharing is harsh and unfair on the honest consumers, but the utilities are handicapped in this situation, since they cannot bear all the theft-inflicted economic encumbrances alone (Kocaman & Tümen, 2020:2; Xia et al., 2022:274).

To buttress the fact that honest consumers also shoulder part of the burdens of the adverse effects of ET, Jay McCoskey, the Chief Executive Officer of Port Harcourt Electricity Distribution Company (PHED), in an interview said that ET is the problem of everyone, because if our neighbours steal electricity, they indirectly steal from us (Spark Media, 2016). If one neighbour steals electricity, it means they are stealing obliquely from all their other benign neighbours, because the unfavourable effects of the theft would ultimately reach those neighbours who do not steal (Kelly-Detwiler, 2013). Honest customers should know that they indirectly foot the bills for the thefts of electricity, since the nefarious acts practically take money off their wallets (Kelly-Detwiler, 2013), and they in essence subsidize those who steal electricity (Antmann, 2009:6).

Therefore, legitimate customers should see themselves as stakeholders in the campaign against ET. They should endeavour to offer helping hands voluntarily and report known cases of theft in their neighbourhoods to the utility companies. This is to express their disapproval of the illicit acts, and to assist in combating the scourge collaboratively (Jamil & Ahmad, 2019:457-458). Electricity customers should help the utilities to help themselves. As the legitimate electricity customers do their bits by giving credible information on known ET, the utilities should also be proactive in always keeping NTL under control in the overall best interest of all the parties involved. In summary, the adverse effects of ET reach everyone directly or indirectly.

2.4.4 Detection and mitigation of electricity theft

ET is a major impediment to electricity reliability and sustainability (Winther, 2012:111; Sharma et al., 2016:40), and hence needs to be detected and significantly mitigated, so as to conserve it and to enhance its effective use (Nayak & Jaidhar, 2023:1). ET could be mitigated by preventing it from taking place; detecting and halting it if it has already taken place; recovering some of the associated revenue losses owing to the theft, and debarring such horrid incident from reoccurring (Dick, 1995:92). Researchers have made tremendous efforts in finding lasting solutions to this plaguing problem of ET. NTL detection (NTLD) techniques and approaches have been researched and presented in a lot of literature. Existing ET prevention, detection and mitigation methods have been profoundly reviewed in Section 2.5.

The ET imbroglio could be assuaged by many methods. These methods are either technical, non-technical, or a combination of both, to achieve better results (Glauner, 2019:3-4). The non-technical methods are implemented by addressing some of the underlying socio-economic factors (Stracqualursi et al., 2023:1) which influence some consumers who indulge in stealing electricity, and those factors that led some utility employees into collecting bribes from defaulting customers. Other methods of controlling ET are manual onsite inspections, imposing fines on defaulters, government giving electricity subsidies to deserving indigent citizens of developing countries to encourage them to become legal consumers, enforcing other elements of the existing laws to prosecute offenders; while technical methods involve deploying electric meters, applying artificial intelligence-based (AI-based) machine learning (ML) methods, including methods from other fields of knowledge like cybersecurity/intrusion detection, distribution network analysis and anomaly/outlier detection, etc. (Messinis & Hatziargyriou, 2018:251-252; Shokoya & Raji, 2019a:98; Kgaphola et al., 2024:336-337). To limit NTL owing to unpaid bills as discussed in Section 1.3.4 of Chapter 1, utilities may cut off electricity supply to the non-paying customers, or reach realistic payment-solution agreements with them on the modalities of their debt payments (Glauner, 2019:111).

In addition to the electricity-theft detection (ETD) and ET mitigation methods mentioned above, naming and shaming of theft culprits by publishing their names and other particulars in the media is also one of the veritable regulatory strategies of curbing ET (Antmann, 2009:24). Leading Nigerian electricity distribution companies have also launched this peculiar approach to restrict ET within their distribution networks. They have introduced the naming and shaming of those customers who are involved in stealing electricity, including the utility employees who may engage in any corrupt activities in collaboration with the customers, by publishing their names and addresses in all the available public media (Bolaji, 2020). This strategy is supplementary to the arrests and the prosecution of ET culprits. Also, confidential whistleblowing platforms have been launched, which assures payment of incentives to those who are committed and courageous enough to report those who engage in ET (Vanguard, 2021). Utilities in Jamaica (Observer, 2017), Ghana (GhanaWeb, 2018), Liberia (Sainworla, 2021), Pakistan (Dawn, 2009), and India (Upadhyay, 2018), etc. have also embraced this method. All the rules guiding this NTL cutback approach have been injected within the purview of the power-sector laws and regulations of every realm. This theft-prohibitive measure is highly commendable and should be sustained as one of the potent methods that could be employed to assuage the hydra-headed ET problem.

To reduce NTL in the high-crime or unmanageable areas mentioned in Section 2.4.1, medium-voltage distribution (MVD) has been implemented by a Brazilian electric distribution company in such areas, whereby shielded networks are installed to connect customers to electricity supply, while each customer’s connection and the MV/LV distribution transformer that supply a group of customers are provided with dedicated meters in a shielded panel located close to the transformer, and the consumers' meter readings could be read via repeating displays at their premises and remotely by the utility through the AMI (Antmann, 2009:26, 32-33). With the MVD concept, the shielded networks which are supplied directly by the pole-mounted MV/LV transformers prevents illegal connections, the shielded panel prevents meter tampering, while the LV distribution network is completely excluded. Identifying unmanageable areas with high NTL is of no essence if no corrective measure could be taken to stem the losses.

2.4.4.1 Characteristics of electricity-theft mitigation

Mitigation or minimization of NTL in the power grids is the only panacea to the obstinate ET problem (Lewis, 2015:128-129; Kocaman & Tümen, 2020:1). Mitigating ET is the most important and the cost-effective means of curtailing power losses (Abaide et al., 2010:1; Fragkioudaki et al., 2016:44). Apart from maintaining stable and healthy electricity grid and assuring financial prosperities to the electric utilities, another benefit of mitigating ET is the reduction in atmospheric pollution caused by carbon emissions (Depuru et al., 2011a:1007; Fragkioudaki et al., 2016:44). The more the success achieved in deterring and mitigating ET, the more the reduction in carbon emissions into the atmosphere (Fragkioudaki et al., 2016:44). This in turn tend to lower the risks of greenhouse effects that later cause global warming and climate change (Osmanski, 2020). Mitigating ET creates a low-carbon and energy-efficient environment and also promotes energy security (Depuru et al., 2011a:1007; Fragkioudaki et al., 2016:44; Khan et al., 2024:7).

It is pertinent to reiterate that in reality, it is impossible to completely eradicate ET or NTL in the power systems, but it is possible to reduce it to an acceptable and tolerable level (Lewis, 2015:128-129; Kocaman & Tümen, 2020:1). The unpredictable human nature involved, and the financial considerations that surrounds ET compounds its intractability (Jiang et al., 2014:109). So, ET is difficult to control in its entirety even with the most advanced equipment; but could be cut down to a reasonable level by deploying variety of solutions (Jiang et al., 2014:109; Jamil & Ahmad, 2019:458). Mitigation of ET is crucial and becomes the only inevitable option to save various power utilities and national economies (Poudel & Dhungana, 2022:109-110, 117) . ET mitigation helps the utilities to overcome major revenue losses and increase electricity reliability by reducing dubious demands owing to pilfered electricity and thus make more power available to boost economic activities.

Sizeable reduction of ET will unburden the electricity grid and enhance its healthiness and efficiency, thereby improving power quality and reliability, and ensuring financial profits to the utility companies (Abaide et al., 2010:2; Shokoya & Raji, 2019a:100). Additionally, ET mitigation also guards the honest consumers against paying for what they did not consume. This prevents electric utilities from distributing part of the ET-inflicted financial deficits amongst the legal honest customers (Depuru et al., 2011a:1008-1009; Anas et al., 2012:180) or imposing higher electricity tariffs on them (Yurtseven, 2015:71; Yakubu et al., 2018:611; Kocaman & Tümen, 2020:1-2; Guarda et al., 2023:1). The ET albatross must be significantly reduced, if not, it will subdue the electric utilities and inflict unthinkable harm on national economies (Guarda et al., 2023:1; Khan et al., 2024:8) and the environment (Depuru et al., 2011a:1007; Fragkioudaki et al., 2016:44; Khan et al., 2024:8).

2.4.5 Electricity-theft detection: the state of the art

Conventional or traditional methods like the exclusive onsite inspections (Messinis & Hatziargyriou, 2018:251), T&D loss analysis (Smith, 2004:2070-2074), or finding the difference between the consumed and billed electricity within a community by using a central observer meter (Ghori et al., 2020:16034) have been used to detect ET. These conventional methods have several drawbacks in terms of social and technical limitations (Messinis & Hatziargyriou, 2018:251; Savian et al., 2021:1-2). Exclusive onsite-inspection method, which involves the onsite inspection of all available electricity customers on the grid is less efficient, requires a significant amount of time to execute, and prohibitively very expensive (Yip, Wong, et al., 2017:230; Zheng et al., 2018:1606; Liao, Zhu, et al., 2024:5075).

The huge running cost involved in the large-scale deployment of human resources for exclusive onsite inspections makes the conventional approach for detecting ET very expensive and less attractive (Yip, Wong, et al., 2017:230; Messinis & Hatziargyriou, 2018:251; Zheng et al., 2018:1606; Liao, Zhu, et al., 2024:5075). Some T&D data calculations are inconsistent and inaccurate (Smith, 2004:2070), while the use of an observer meter could only help to determine the area where ET is taking place, but not the actual theft culprits (Ghori et al., 2020:16034). The pilfering methods of electricity that spur eventual onsite inspections have been mentioned in Sections 1.3, 13.1, 13.2, 1.3.3, and 1.3.4 of Chapter 1. With the obvious inadequacies of the conventional methods, there is a need to explore other methods that will further assist in stemming the ET menace and its horrendous effects.

AI techniques are the state-of-the-art methods employed for the detection of ET (Glauner et al., 2017:761; Glauner, 2019:31, 110; Ghori et al., 2020:16033-16034; Saeed et al., 2020:1; Guarda et al., 2023:4; Stracqualursi et al., 2023:12, 16; Coma-Puig et al., 2024:2704). This approach is proficient and predominant when compared with other methods used for NTLD. Machine learning (ML), an AI-based method, is deployed in the data-oriented NTLD methods (Messinis & Hatziargyriou, 2018:259; Saeed et al., 2020:9) discussed under Section 2.5.3.2, and have also been exhibited in the experimental part of the thesis. The AI-based methods for NTLD perform better than the traditional methods (Saeed et al., 2020:1). AI-based NTL models identify irregular electricity or energy consumptions in real time and such anomalous consumption patterns are indications of ET (Jiang et al., 2014:108; Glauner et al., 2017:761; Yip, Wong, et al., 2017:231; Poudel & Dhungana, 2022:110; Guarda et al., 2023:1-2). ETD or NTLD is technically a binary classification problem because it involves the determination of theft and non-theft cases (Chen et al., 2022:5).

2.4.5.1 Artificial intelligence

The term artificial intelligence (AI) was first coined by John McCarthy in 1956 to describe a new field of knowledge associated with “thinking machines”, during a six-week Summer Research Project Conference at Dartmouth College in Hanover, New Hampshire, United States (Nilsson, 2013:77-78; Glauner, 2019:16). The 1956 Dartmouth Conference which was organized by John McCarthy birthed AI and initiated it as a new discipline (Nilsson, 2013:77; Cao, 2022:3). Other notable scientists who attended the conference and also assisted in its organization logistics were Claude Shannon, Marvin Minsky and Nathaniel Rochester (Glauner, 2019:16).

AI has kept evolving ever since it was birthed in 1956 (Cao, 2022:4-8). It has continued to experience exponential growth and has found applications in almost every discipline. According to John McCarthy: “AI is the science and engineering of making intelligent machines” (Hamet & Tremblay, 2017:S36-S37; Amisha et al., 2019:2328). AI refers to the usage of digital computers and machines to simulate human intelligence (Raschka et al., 2020:1). The objective of AI is to create intelligent machines that act effectually in novel conditions (Russel & Norvig, 2021:19).

AI involves the incorporation of humanlike-intuition technology into machines by building intelligent systems or models that allow machines to perform tasks that are normally associated with humans (Choi et al., 2020:1). The operation of such models are automated and require little or no human involvements (Hamet & Tremblay, 2017:S36). Humanlike-intuition technology constitutes algorithms that allow machines to imitate humans by replicating their mental prowess to solve problems (Janiesch et al., 2021:686). Initially, building an intelligent analytical AI model would require explicit programming using algorithms to produce a model or computer program with cognitive capabilities. After the intelligent model must have been developed, it can then reason critically to discover meanings, learn from previous experience, generalize and make predictions, recommendations, or generate answers, rules, etc. (Janiesch et al., 2021:686, 688; Russel & Norvig, 2021). Application of AI solutions by implementing various branches of AI cut across different fields of knowledge and are used to solve many discipline-specific problems (Hamet & Tremblay, 2017; Amisha et al., 2019). But the application of AI in this research project is restricted to ETD or NTLD in the power distribution systems.

Recent advancement in knowledge in the field of AI has brought about a more efficient and superior approach to detecting NTL when compared with the conventional NTLD methods (Saeed et al., 2020:1; Poudel & Dhungana, 2022:110). AI-based methods for ETD are the most popular (Fragkioudaki et al., 2016:51), and the growing trend of AI-based research articles on NTLD is a pointer to this fact (Saeed et al., 2020:1; Poudel & Dhungana, 2022:110). There is a need to monitor electricity consumption to be able to control ET. ET can lead to unusual patterns in electricity consumption profiles. We can use AI-based ML methods to discover abnormal patterns in electricity consumption data to uncover electricity thieves (Jiang et al., 2014:109; Glauner et al., 2017:761; Yip, Wong, et al., 2017:231; Guarda et al., 2023:1-2). Consumption profiling can also be used to improvise methods to regulate electricity loads, so as to maintain and sustain the existing generation capacities (Ahmad et al., 2018:2916-2917).

AI methods for ETD allows us to scrutinize and analyse the meter-reading records, the consumption records, the consumption history, or consumption profiles of the electricity consumers taken over a period and use them to determine irregular consumption behaviours embedded in the consumption records in a bid to detect ET (Jiang et al., 2014:109; Glauner et al., 2017:761; Yip, Wong, et al., 2017:231; Guarda et al., 2023:1-2). This would assist us to detect customers with abnormal tendencies in their consumption, which would eventually trigger probable inspections. To mitigate the theft, the utility technicians would then carry out onsite inspections to fish out customers who may have tampered with their power infrastructure in a bid to steal electricity. In the developing countries, it may not be realistic enough to determine the theft of electricity from the perspective of energy balance calculations used in electrical engineering. This is owing to changes in network topology and the irregularities associated with grid infrastructure, as well as the probable inconsistent measurements derived from several grid elements. Hence, there is a need for exploiting the AI techniques, a more-proficient approach, for the detection of ET (Glauner et al., 2017:761).

Many NTLD solutions have been mentioned in the literature, but ETD by employing AI methods are the predominant and advanced anti-theft approach used in latest research to detect customers who may be stealing electricity (Glauner et al., 2017:761; Glauner, 2019:12, 31, 110; Poudel & Dhungana, 2022:110). This latest and the most-advanced ETD approach uses the consumption data of the electricity customers to reveal irregular power consumptions, and to uncover the very suspicious customers who are liable for onsite inspections (Glauner, 2019:31, 110; Guarda et al., 2023:1-2). Deployment of AI methods for NTLDs prevent unnecessary and expensive onsite inspections (Barros et al., 2021:1-2). The conventional means of ETD adopt an indiscriminate and unilateral onsite inspection approach which condones a lot of unnecessary, expensive, and time-wasting inspections (Yip, Wong, et al., 2017:230; Messinis & Hatziargyriou, 2018:251; Zheng et al., 2018:1606; Liao, Zhu, et al., 2024:5075).

AI-based NTLD methods are classified into ML and deep learning (DL) algorithms or models (Arif et al., 2021:2). Meanwhile, DL is a subset or a type of ML (Janiesch et al., 2021:686), while ML itself is a subfield (branch) of AI or a technique to achieving AI (Brown, 2021; Janiesch et al., 2021:686-687). NTLD using ML (Yip, Wong, et al., 2017:231; Guarda et al., 2023:5) is the implementation and application of one of the branches of AI to solve the perennial ET problem. However, the large volume of data generated by SMs via the AMI in SG have made it possible for the application of technologies which are data-driven, including the implementation of AI techniques for ETD (Liao, Zhu, et al., 2024:5075; S. Zhu et al., 2024:15477).

❖ Machine learning

ML is a branch or a subdiscipline in AI which forms an intersection between computer science and statistics (Jordan & Mitchell, 2015:255-256; El Bouchefry & de Souza, 2020:225). ML is used to decipher patterns in datasets using algorithms and also used to make new predictions without any explicit task-specific manual programming (Jordan & Mitchell, 2015:255-256; Guarda et al., 2023:5). With ML, algorithms or computer programs are able to perform cognitive tasks and learn from experience through problem-specific data samples (Jordan & Mitchell, 2015:255; Glauner, 2019:12, 16; El Bouchefry & de Souza, 2020:226; Janiesch et al., 2021:686). ML is an inductive process because it allows rules to be derived from examples (Glauner, 2019:20). Questions on how computers that learn from several input data are built, in a bid to anticipate outputs by learning from the input experience and improving performance over time are addressed by ML (Jordan & Mitchell, 2015:255). ML allows humans to build more efficient and intelligent systems by formalizing their knowledge into forms accessible to machines.

Instead of writing static programs to individually input knowledge into computers to solve a particular problem, ML models rather train computers to dynamically learn relationships and patterns from samples and cleverly perform predictions or decisions on new similar samples based on the knowledge acquired through experience without explicitly programming or exclusively codifying the computer to learn the new samples (Jordan & Mitchell, 2015:255; El Bouchefry & de Souza, 2020:225; Janiesch et al., 2021:685). These learned patterns from the sample data are recognized by machines, and predictions are made based on them when new input sample data are fed into the ML algorithms or models (Jordan & Mitchell, 2015:255).

While humans struggle to elucidate all their knowledge and available solutions to complex problems, ML overcomes this limitation by learning through training and improving from experience through increased performances (Jordan & Mitchell, 2015:255; Janiesch et al., 2021:685-686). ML uses algorithms to automatically learn hidden insights and intricate patterns in any data that is subjected to scrutiny (Janiesch et al., 2021:686). This learning allows ML models in computers to automatically reprogram themselves in accordance with the experience they have garnered. A typical example of learning the hidden or latent patterns in a data is shown in Figure 2.17.

The Figure 2.17 is an example of the consumption pattern of a particular customer who engages in stealing electricity (Glauner, 2019:2). The energy consumption pattern is generated from the monthly time-series consumption profile of the customer, and shows a typical example of how ET could be detected and later mitigated using the patterns hidden in the electricity consumption data of the consumer (Glauner et al., 2016:253-254). Using automated statistical methods to learn latent irregularities or fraudulent patterns from datasets containing features of electricity consumptions, with the ulterior motive of gaining insights from the data is achieved using ML (Glauner, 2019:16, 31, 36; Poudel & Dhungana, 2022:110).

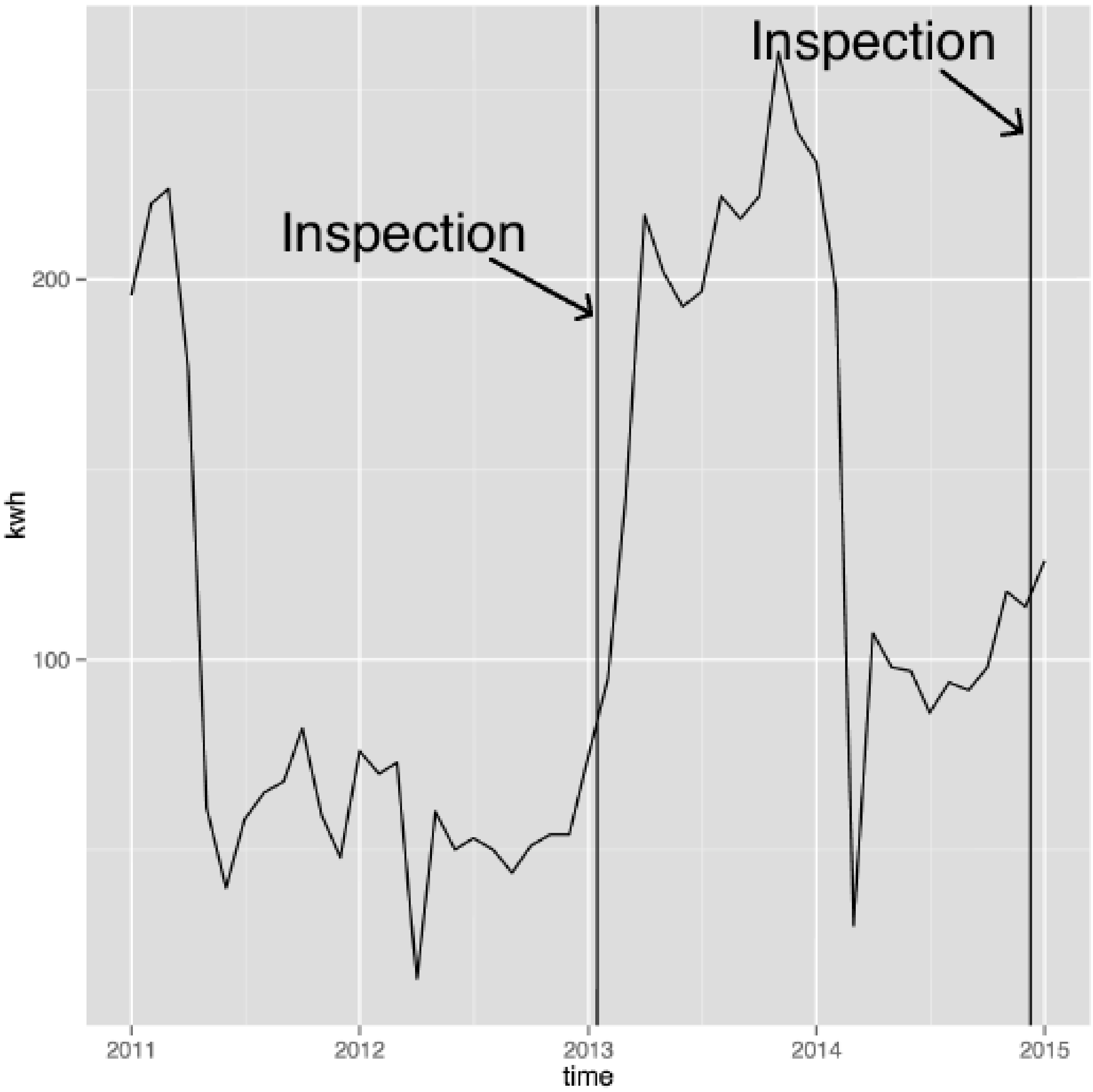


Figure 2.17: Consumption pattern indicating malicious usage of electricity (Glauner, Meira, et al., 2016:254)

There was a sharp drop in the electricity consumption of the customer at the end of 2011 from the case-study consumption pattern shown in Figure 2.17. The drop was about a fifth of the previous consumption. This signified that the electric meter of the customer may have been manipulated. This drop persisted over time, and the customer was suspected of pilfering electricity. The utility inspection team carried out an onsite inspection at the premises of the customer at the beginning of 2013, and an instance of ET was detected. After the theft detection, the electricity-infrastructure manipulation was reverted, and the electricity consumption pattern of the customer went back to normal. In 2014, a year after the previous inspection was carried out, another drastic drop in electricity consumption occurred again, this time to about a third of the previous consumption. This drop brought about another inspection a few months later (Glauner et al., 2016:253-254; Glauner, 2019:4).

Sharp drops or anomalies in electricity usage are peculiar to those customers committing ET (Jiang et al., 2014:109; Glauner et al., 2017:761; Yip, Wong, et al., 2017:231; Guarda et al., 2023:1-2); but in some special cases those drastic drops in consumptions might be because a building is currently uninhabited, the occupier of a building went on holiday, travelled, moved out, or due to change in weather conditions, tariff, or that a factory reduced its production level, etc. (Glauner, 2019:2; Coma-Puig & Carmona, 2022:488; Poudel & Dhungana, 2022:110, 115-116; Guarda et al., 2023:20). This is the reason a physical onsite inspections by utility technicians is very essential and imminent to get site feedbacks for customers with irregular electricity consumption patterns, in a bid to confirm or establish whether those customers with suspicious patterns of consumptions are actually fraudulent or not (Messinis & Hatziargyriou, 2018:259; Liao, Bak-Jensen, et al., 2024).

After establishing the electricity thieves, the stealing customers are tagged as fraudulent while the rest are identified as honest. The honest customers who do not steal electricity or cause NTL are labelled or annotated as “0”, while the fraudulent customers who steal electricity or cause NTL are labelled as “1” after the onsite inspections (Glauner, 2019:48; Munawar, Javaid, et al., 2022:12; Ali et al., 2023:6, 9; Nayak & Jaidhar, 2023:4). Supervised ML models then capitalize on these individual customer labels (Appiah et al., 2023:2) in conjunction with their corresponding energy consumption data to make predictions about new customers who may likely be stealing electricity. Using ML models for NTLDs reveal the suspicious customers liable for onsite inspections, prevent unnecessary inspections and drastically reduce the huge costs associated with indiscriminate onsite inspections (Messinis & Hatziargyriou, 2018:259, 264; Barros et al., 2021:1-2).

Analytical model building tasks are automated using ML algorithms to achieve object detection within the data without any explicit or manual programming. By extracting features from huge databases and learning from earlier computations, ML algorithms assures replicable and dependable decisions from the data (Janiesch et al., 2021:686). ML methods are also known as data mining methods (Ahmad et al., 2018:2916-2917; Glauner, 2019:31, 45). ML methods are a superior approach for the detection of ET because they are more efficient, more accurate, saves time and requires less labour (Ghori et al., 2020:16033; Saeed et al., 2020:1). Different ML algorithms have been developed to adapt to various datasets from different sources to solve different problem types (Jordan & Mitchell, 2015:255; Guarda et al., 2023:5).

The four types of ML are supervised, unsupervised, semi-supervised, and reinforcement learnings (Yang, 2019:139-140; Choi et al., 2020:2; El Bouchefry & de Souza, 2020:227-228; Janiesch et al., 2021:686-687). Examples of supervised ML models are support vector machines (SVM), optimum path forest (OPF), decision tree (DT), k-nearest neighbours (KNN), Bayesian classifiers and rule induction methods, etc., while examples of unsupervised ML methods are clustering algorithms, outlier detection methods, and statistical methods, etc. (Saeed et al., 2020:9, 12; Guarda et al., 2023:5-6, 11-12). The semi-supervised learning method forms a borderline between supervised and unsupervised learnings (Choi et al., 2020:3). Supervised, unsupervised, and semi-supervised methods of learning are further discussed under Section 2.5.3.2. Supervised and unsupervised learnings are applied in anomaly or fraud detections like in ETDs or NTLDs. Applications of reinforcement learning are found in games (Silver et al., 2018), robotics (Singh et al., 2022), and broker systems (Peters et al., 2013).

- **Deep learning**

DL is a subset of ML which learns from the multilayered form of basic hierarchical human brain-like network (or artificial human brain) known as neural network (Islam et al., 2019:9; Montesinos López et al., 2022:379, 384). Neural network was brought about owing to advancement in the field of ML, enabling superior learning algorithms with more proficient preprocessing techniques (Janiesch et al., 2021:686). Artificial neural network (ANN) is a basic neural network which forms the backbone of DL models (Montesinos López et al., 2022:383). The idea of neutral network was motivated by the functions and structure of the biological neurons in the brains of humans, and has thus been modelled after it to make predictions (Glauner, 2019:17; Islam et al., 2019:7; Montesinos López et al., 2022:379-381).

Neural network is modelled after the human brain because the brain is a superior information processing system which computes complex operations (Islam et al., 2019:7; Montesinos López et al., 2022:379). The brain is a component of the human nervous system which is made up of the processing units called neurons where the term “neural” network (network of neurons) derived its name. The neuron or node is the fundamental component of a neural network, representing a simplified model of the neuron in human brains (Lepolesa et al., 2022:39641). Neural network layers are trained to recognize the different features of the input data and consequently produce an output based on the patterns learnt through the hidden layers (Lepolesa et al., 2022:39641; Ali et al., 2023:12). A basic neural network or ANN structure consists of input, hidden, and output layers (Xia et al., 2022:290).

DL models contain multiple hidden layers and dynamically discovers the needed representation commensurate to a specific learning task (Yang, 2019:151; Janiesch et al., 2021:687-688; Montesinos López et al., 2022:383). DL is an improved neural network that is otherwise known as deep neural network (DNN), with depth of layers of multiple neurons, in a deeply nested architecture, which enables it to process more complex data, produce more-accurate predictions and outperform other conventional ML models (Lepolesa et al., 2022:39641; Montesinos López et al., 2022:383). This is achieved because DNN is able to detect patterns or trends which are difficult for other traditional ML models to detect (Lepolesa et al., 2022:39641). Learning via training a DNN is called DL. ANN consists of one or two hidden layers (Mostafa et al., 2020:107), while a neural network that consists of three or more hidden layers is referred to as a DNN (Mostafa et al., 2020:107). Hidden layers share similar information (Montesinos López et al., 2022:386), and are located centrally in a neural network between the input layer and the output layer (Islam et al., 2019:9; Ali et al., 2023:12). The neural network framework comprises of layers of interconnected nodes (artificial or synthetic neurons) or processors, where the output of a node serves as the input source of the next available node (Islam et al., 2019:9) as could be seen in the DNN architecture shown in Figure 2.18.

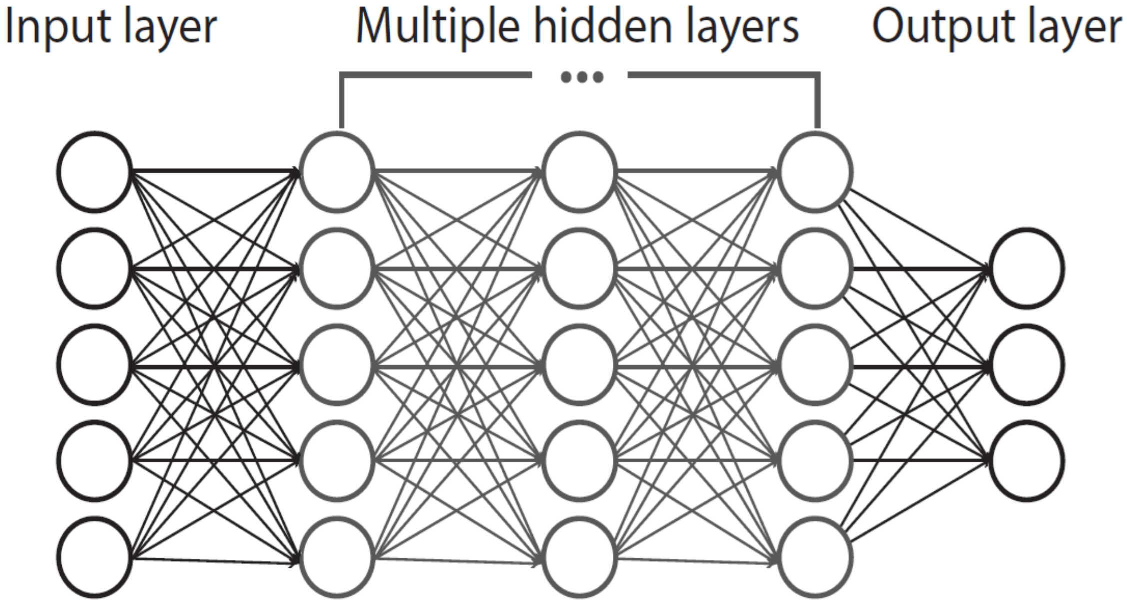


Figure 2.18: Architecture of deep neural network

(Zhu et al., 2022:3)

Signals are transmitted between connected nodes in a neural network. The connection or linkage between a node to another carries a real number value which corresponds to the weight or strength of the transmitted signal (Islam et al., 2019:7, 9; Montesinos López et al., 2022:394). Neural networks learn by updating the weights (Islam et al., 2019:7). Just like the neurons in neural networks imitate the biological neurons in human brains, the unique connection weights between neurons in neural networks also imitate the connections between neurons in human brains (Lepolesa et al., 2022:39641). The input data in a neural network is sent through the input layer to the hidden layer. The hidden layer receives the input data, extracts features or information from it and use the extricated information to update the network weights, while the final model predictions or results are done and produced at the output layer (Islam et al., 2019:7; Ali et al., 2023:12). The number of features in the input data determine the number of neurons at the input layer, while the nature of the task being performed by the neural network (i.e., the number of parameters being predicted) dictates the number of nodes at the output layer (Ali et al., 2023:12). In addition to being able to predict as a model, DL models automatically learn features from datasets and also perform well with the processing of big, unstructured, imbalanced and noisy datasets (Arif et al., 2021:2; Janiesch et al., 2021:688-689; Guarda et al., 2023:23). Examples of DL algorithms are convolutional neural network (CNN), recurrent neural network (RNN), generative adversarial neural network (GAN), distributed representation, and autoencoder, etc. (Janiesch et al., 2021:689-690).

2.5 NTL methods and solutions

NTL could be deterred, determined, and pruned by various techniques and approaches. A typology of NTLD solutions has been proposed based on the overview of various techniques and approaches present in the literature. The typology of these anti-theft techniques and approaches are categorized under theoretical studies, hardware solutions and non-hardware solutions (Viegas et al., 2017:1260; Saeed et al., 2020:7; Appiah et al., 2023:2) as shown in Figure 2.19.

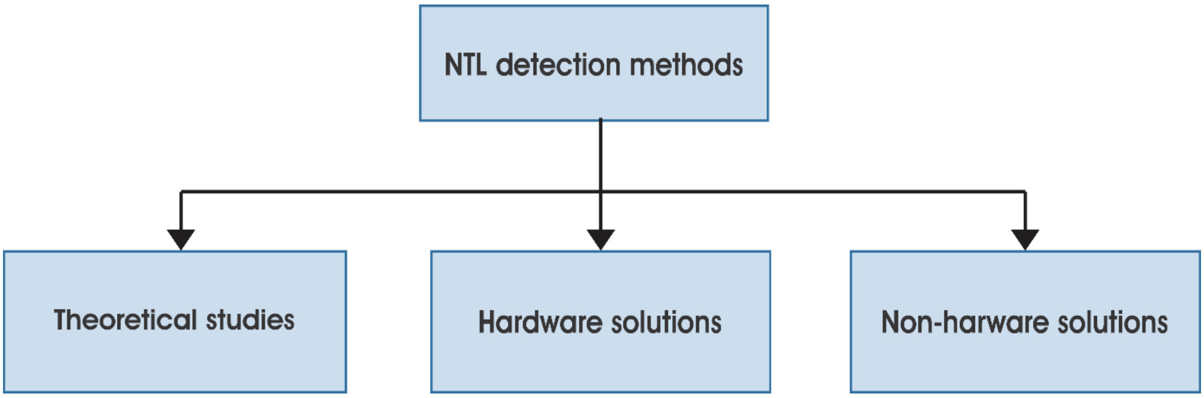


Figure 2.19: Typology of NTL detection methods

Adapted from (Viegas et al., 2017:1260; Saeed et al., 2020:7; Appiah et al., 2023:2)

NTL cutback approaches and techniques could be implemented in both conventional and SGs (Yip, Wong, et al., 2017:231). SM is an intelligent metering device used in SG for the acquisition of energy consumption data and other grid parameters for NTLD using AI techniques. NTLD methods for optimal NTL mitigations are better and are accurately implemented using the energy consumption data obtained from SMs, owing to the readily available fine-grained or high-resolution data it generates in conjunction with other detailed grid information. Data-based NTLD methods are the state of the art, and are further discussed under Section 2.5.3.2.

2.5.1 Theoretical studies

In this NTL solution approach, variable factors that influence the existence of NTL amongst the populace in a geographical area are analysed (Viegas et al., 2017:1260-1261). Theoretical studies-based NTL solutions provide the non-technical means of controlling ET by gathering and analysing information on social, economic, demographic, and market variables that help the electric utilities to understand the root cause of NTL. After the analyses, the variables that drive the illegal behaviours of consumers who cause NTL within a particular topographical population are determined. Statistical techniques are mainly used in leading studies to analyse these variables and to determine the relationships between them (Viegas et al., 2017:1260-1261; Saeed et al., 2020:7-8). Theoretical studies proffer alternative solutions to ET as against the conventional technical or engineering solutions (Yurtseven, 2015:74).

The primary advantage of the theoretical solutions to NTL is that it helps to inspire policy and decision makers in forming and making effective plans and resolutions that would have great effects on ET reduction, and ultimately promote greater efficiency in the electric system. But the major disadvantage of this approach is its limited scope, in that, it typically focusses on case-study country or region at a point in time (Viegas et al., 2017:1261; Saeed et al., 2020:8). The method is therefore insufficient to identify the precise point of theft incident or points of other irregularities in metering or billing. The next subsections under this section examine some theoretical methods which have been used to curb the effects of NTL, as presented in the literature, and also the types of data used for the theoretical analyses.

2.5.1.1 Empirical survey: customer-utility relational approach

Winther (2012) focused on bottom-up approach in combating corruption in the electrical system, by using surveys and ethnographic fieldwork information. The author highlights customer-utility relationship as a means of understanding and curtailing the problem of ET. According to Winther (2012), proactively improving utility reputation amongst the customers tends to prevent the occurrence of ET. The approach of the author was based the on the empirical findings of two different socio-cultural settings of rural Zanzibar in Tanzania, and the Sunderban Islands in West Bangal, India. The two developing geographical references have different provisional systems. The grid supply system in rural Zanzibar is centralized, while that of Sunderban is decentralized. Insights have been obtained through the ethnographic fieldwork in rural Zanzibar, and the fieldwork in Sunderban with customer-staff house survey.

The author argued that relational and people-centred approaches are impactful in the quest to reduce ET. The people-centred approach is about the formation of groups of local users and their participation in helping to enhance the performance of the electricity providers. The participation of these local-user groups gives the customers and the communities a sense of belonging and motivation to trust the process. For example, these groups are consulted when the utilities want to make changes to their tariff, etc. Consequently, these groups feel obligated to report illegal use of electricity within their localities to the utilities. In this study, the way the customers relate with their electricity providers is crucial, and any changes made to such relationship would fundamentally reshape the electricity system in terms of customers' compliance and electricity sustainability.

According to the author's findings on Zanzibar and Sunderban, trust relationship between the customers and the utilities is an antidote to stealing electricity or causing NTL. If trust is promoted between the parties, the customers will have faith in the process, and they would be obliged to pay for what they consume and subsequently adhere to the utility regulations. The device (technical mediator) between the customers and the utilities which enhances trust between them is the electricity meter. Customers' confidence in the proper functioning of the electricity meters and the transparency in the utility accounting system translate to customers being charged only for what they consume (social accountability). This fosters the customer-utility trust relationship. To avoid suspicion on the part of the customers, the utility should endeavour to determine, repair and/or change any dysfunctional meters. This is done in order to always maintain the confidence between them and their customers. The utilities should also educate their customers on billing, accounting, and metering, to increase the customers' awareness of how they get billed. It is always easier for humans to comply with any process they trust, and thereby encourage others to do same. Equal and fair treatment of customers are also particularly very important in the process.

The utilities should also ensure satisfactory power availability because such promotes the trust relationship. Utilities in alliance with the local customer-group members should not condone non-payment of bills because if some customers do not pay their bills and could get away with it, other customers would tend to follow suit. The electricity behaviour of peer groups affects the compliance norms of others. The utilities in collaboration with the user groups would encourage sanctions for defaulting customers. The utilities should reciprocate the customers' trust in them by reinvesting the profits they make into the system to improve service quality and increase capacity. If these are done, the customers would have no cause to have any iota of distrust in the utilities. The utilities should also not violate the trust the customers have in them, as that would encourage the customers to always fulfil their part in the customer-utility relationship or get sanctioned if they do otherwise.

The stakeholder mentality of the consumers ensures the smooth running of the electricity system. These collaborative efforts help curtail activities that may lead to ET, as the electricity customers would not want to destroy or desecrate the arrangement which they are actively part of. The ingredients to ultimately analyse the customer-utility relationship are via the grounded and socio-technical approaches. The grounded approach tries to understand why consumers make illegal connections or refuse to pay their bills. The socio-technical approach is about the electric meters and the customers' confidence in them. The electricity meter was referred to earlier as the technical mediator between the customers and the utilities. The relational-approach analysis of either trust or otherwise is premised on the inferences from the grounded and socio-technical approaches, and the utilities taking other measures as stated previously. The whole process is to make the customers behave in a way that suits the electricity suppliers and the political institutions that govern them. This is in a bid to bring sanity into the electricity system, stem ET and promote sustainable energy utilization and production. In summary, customer-utility relationship is a key factor to maintaining sustainable electricity systems.

While Winther's (2012) research is valuable for its sociological perspective, its applicability to modern SGs, urban-theft contexts, and the integration of ML models with social data analysis is limited.

2.5.1.2 Econometric analysis

In a bid to reduce the effect of ET in the power grid, Yurtseven (2015) presents econometric analysis that examine the socio-economic basis for illegal electricity consumption using Türkiye (Turkey) as a case study. Prevention of ET is the priority of this study. This is achieved by estimating an ET equation by applying different econometric methods. According to the author, if we understand the socio-economic drives behind the stealing of electricity, including the political and natural variables surrounding it, we could prevent it from taking place. To compute the ET estimation equation, the author used the socio-economic data of provinces in the South-Eastern Anatolia Region of Türkiye from 2002 to 2010. According to the 2011 TEDAŞ (Turkish Electricity Distribution Company) report cited by the author, tackling ET in Türkiye has been of paramount importance since an estimate of about 16 billion units (16 billion kilowatt-hours) of electricity is stolen every year in the country. These illegal energy consumptions represent around 15% of the total electricity delivered for consumption, and approximately translate to around US$1 billion in financial losses yearly. The empirical constant-elasticity model equation for ET as developed by Yurtseven (2015) is illustrated in Equation 2.2. The ET model estimates the ratio of illegal electricity consumption.

$$\mathrm{Ln}\, r_{i,t} = \propto + \beta \ln P_t + \gamma \ln I_{i,t} + \sum_h \theta^h \ln Z_{i,t}^h + \varepsilon_{i,t} \tag{2.2}$$

Where $r_{i,t}$ is the proportion of the electricity consumed illegally in province i at time t; P_t is the national tariff or price of a unit of electricity at time t; $I_{i,t}$ is the income per capita of province i at time t; $Z_{i,t}^h$ is the city socio-economic and natural characteristics of type h by province i at time t; $\varepsilon_{i,t}$ is the error term of the model; while $\propto$ is a constant term. To determine the underlying socio-economic reasons behind ET, the ET model is estimated using instrumental variable generalized method of moments (IV-GMM) estimation method, to test the correlation of the model variables and to increase its efficiency. After this, three-stage least squares (3SLS) estimation technique was later used to further confirm the efficacy of the IV-GMM approach.

From the estimations, the author concluded that income, social capital, education, temperature index, agricultural production rate, and rural population rate are the most significant variables that drive ET in the provinces of South-Eastern Anatolia Region of Türkiye. These variables tend to influence the ET ratio to go either higher or lower. However, offering of social tariffs to indigents and low-income earners, increase in general education, and social capital (which ensures that “illegal usage share” are recommended for provinces with high ET ratio to increase social control) have been suggested to reduce illegal consumption of electricity in a bid to lower the ET ratio.

This study presented by Yurtseven (2015) is valuable for identifying socio-economic drivers, and needs to be complemented by consumer-level data, real-time ML detection technologies, and longitudinal approaches which track theft trends over time for a comprehensive NTLD framework. The author should look beyond Türkiye and carry out comparative studies across other countries.

2.5.2 Hardware solutions

Hardware-driven NTLD solutions focus on the description, characterization, design, development, and deployment of metering equipment and/or sensing hardware that assist in the identification, estimation, detection, and mitigation of NTL (Viegas et al., 2017:1261; Saeed et al., 2020:8; Javaid, Jan, et al., 2021:45; Lepolesa et al., 2022:39639; Guarda et al., 2023:2). In addition to the hardware-based electric meters, software is required for the operation of some advanced electronic meters. The software of such electronic meters is used for processing the data produced by the meters. This category of NTL solution can be classified into three types according to the techniques used in presenting the solutions. The classification types of the hardware-based methods deployed for NTL prevention, detection, and/or mitigation are metering hardware, metering infrastructure, and signal generation and processing (Viegas et al., 2017:1261) as shown in Figure 2.20.

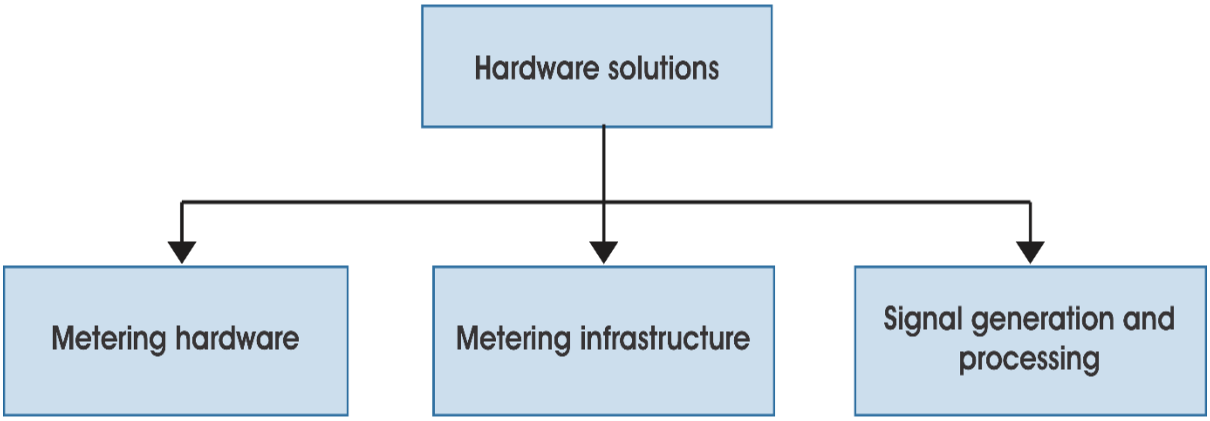


Figure 2.20: Classification of NTL hardware solutions

Adapted from (Viegas et al., 2017:1260-1261)

2.5.2.1 Metering hardware

Metering hardware as a technique for NTLD specifies metering equipment details and their specifications. This NTLD method presents diverse ways of designing new metering hardware or modifying the existing ones to enhance the detection of ET. The advantage of this hardware-based NTL solution is that it can totally detect some kinds of NTL, for example, reversing the meter and the disconnection taking place within the meter zone. The shortcoming of this solution is that it could not detect NTL before and beyond the meter, except for the NTL that emanates within the meter. Metering equipment are expensive and also attract significant costs to install them in customers' premises (Viegas et al., 2017:1259, 1261).

The authors in Ngamchuen and Pirak (2013) proposed metering systems that are based on using specific processors and anti-tampering algorithms to protect the meters from any form of tampering through detection and communication of intrusion activities. Ngamchuen and Pirak (2013) implemented anti-tampering algorithms on an ADE7953 chip, while Dineshkumar et al. (2015) implemented same on an ARM-Cortex M3 processor. The ADE7953 chip was able to detect overcurrent, overvoltage, dropping voltage, no-load situation or outage, and other irregularities, and then sent a disruption signal to the MCU to report the tampering event. In the case of meter cover and terminal tampering, alarm signals are sent immediately to the MCU through the tampering switches connected to the input and output (IO) ports of the MCU. The electric meter designed by Dineshkumar et al. (2015) has a GSM module which automatically sends a Short Message Service (SMS) or text message to the utility server whenever any form of ET (like bypassing the entire electric meter, bypassing of the phase-line wire, tampering the meter, or isolating the neutral wire) is detected.

Ngamchuen and Pirak (2013) and Dineshkumar et al. (2015) contribute to tampering detection and hardware-based solutions, but they lack data-driven anomaly detection approaches and focus primarily on tampering and hardware alerts. Future NTLD models should integrate hardware tampering detection with consumption pattern analysis using ML techniques.

Dike et al. (2015) designed a prepaid electric meter which utilized GSM module, a microcontroller, and an EEPROM, etc. The microcontroller of the electric meter is encrypted with the unique identification (e.g., phone number) of each customer. Simulation results showed that the GSM module of the meter sends SMS alert to the utility whenever an illegal load is connected to the meter after tampering or bypassing it. Bin Yousuf et al. (2016) used a PIC18F452 microcontroller in the design of an ET detector and also simulated it using Proteus software. ET is detected if there was a mismatch between the forward current from the phase line and the reverse current through the neutral line. If ET is detected, the microcontroller sends an alarm command and the alarm system of the device would sound at the instance of ETD.

The authors in Dike et al. (2015) and Bin Yousuf et al. (2016) propose hardware-based anti-theft solutions, they lack ML approaches that leverage SM data to detect consumption anomalies. Future NTLD research should integrate hardware-based tampering detection with data-driven consumption analysis for a comprehensive solution.

Astronomo et al. (2020) designed, fabricated, and tested an Arduino-based ET detector. The circuitry of the ET detector consists of an Arduino Uno, LCD, two current sensors, and GSM module. One of the current sensors is located on the drop wires from the electric poles, and the other on the service cap where the drop wires enter the premises of the customer. Whenever the difference between the current measurements from the two current sensors reaches a threshold, ET is detected. After the theft is detected, microcontroller would instruct the electric meter to alarm, while an SMS notification would then be sent to the utility. Proteus 8 software was used to simulate the theft detector.

While the authors Astronomo et al. (2020) introduce a practical hardware-based tampering detection system with GSM alerts, the approach is limited to physical tampering detection. Combining hardware solutions with ML techniques can enhance detection capability by identifying non-intrusive consumption anomalies. Additionally, addressing scalability, communication resilience, and long-term operational stability will strengthen its applicability to large-scale power systems.

Khoo and Cheng (2011) have proposed the use of radio frequency identification (RFID) systems to protect the ammeter inventory management of an electricity supply company, by using RFID tags on the ammeters to prevent ET. Unique data about the ammeter are captured by the RFID tags to track and manage the ammeters in real time. ET is suspected if the RFID tags on ammeters onsite are not intact, that is, if the tags are either broken or removed.

This study by Khoo and Cheng (2011) provides valuable insights into the cost-benefit analysis of RFID for asset protection in utilities, but it does not address consumption-based ETD, which remains the most prevalent concern for utilities. Combining RFID systems with data-driven approaches and real-time monitoring would offer a more comprehensive NTLD solution. Also, the authors could also evaluate large-scale RFID deployment across multiple utility networks and investigate the robustness of RFID against tampering, spoofing, and signal attacks.

A metering architecture which consists of two reading points has been proposed and tested by Henriques et al. (2014), to enable easier detection of ET. The metering architecture at the LV distribution grid consists of ammeters at the point of supply (local unit) and at another point after the consumer electric meters (remote unit). The measured currents at the local and remote units are transmitted via radio frequency to a receiver unit. Difference between the measured currents at the local and remote units is an indication of ET.

Henriques et al. (2014) introduce a practical hardware tool for detecting physical tampering and bypassing, but their approach is limited to manual inspections and physical discrepancies. Combining ammeter-based tampering detection with smart metering, real-time monitoring, and ML techniques would provide a more comprehensive and scalable NTLD solution. Also, the authors could evaluate hybrid hardware-data systems across large and diverse utility networks should and integrate field inspection devices with AMI systems for real-time tampering alerts.

2.5.2.2 Metering infrastructure

This method of NTLD focuses on metering assets or infrastructure and their characteristics like installation procedures, and the number of equipment that are needed to be deployed based on the specific requirements of a particular geographical location (Viegas et al., 2017:1261). Leading literature on metering infrastructure-based NTL solution focus on placing different data-collection devices at various locations (e.g., premises of the customers, distribution transformers and substations) of the grid, to detect sources of NTL and to estimate the amount of NTL in the electric network (Viegas et al., 2017:1261; Lepolesa et al., 2022:39639). The advantage of this type of NTL solution is that it detects all kinds of NTL before the meter and within the meter zone. The drawbacks of this anti-theft approach are the high costs needed to procure and install the needed equipment (Viegas et al., 2017:1259, 1261).

The authors, Grochocki et al. (2012), presented a comprehensive analysis of various AMI attacks in SG. The primary purpose of these attacks is to steal electricity. In this study, system architecture to counter probable attacks in the AMI has been proposed. The authors surveyed various probable AMI attacks and their techniques, gathered the information needed to effectively detect these attacks which led to producing an extensive attack tree. Hybrid sensing infrastructure which involves the utilization of intrusion detection system

(IDS) and embedded SM sensors has been suggested by the authors to give the widest coverage in monitoring to detect all probable AMI attacks.

It could be seen that the authors Grochocki et al. (2012) have contributed significantly to AMI cybersecurity by defining IDS requirements and deployment strategies, but the study lacks practical validation and integration with ML techniques for anomaly detection. Combining IDS with data-driven NTLD models and physical tampering detection would enhance the robustness of theft detection systems, particularly in developing regions. This study did not also investigate distributed IDS frameworks for large-scale AMI deployments, and did not combine cyber-IDS with physical theft detection methods.

The authors in Paruchuri and Dubey (2012) proposed functional and diagnostic systems in a conventional grid for NTLDs. The functional system consists of SMs installed at the distribution transformers, relays, and consumers' premises. The SMs have in-built GSM modules and use half-duplex communication protocols. The diagnostic system uses software and algorithms to determine the exact location where NTL or ET took place. A unique-code signal is sent from the GSM base to consumers' SMs at regular intervals. This signal could be sent either through power line or wireless communications. The consumers' SMs accept the signal and update themselves. Once the SMs respond to the signal, an LV carrier signal is injected into the grid before the SMs, and the infused signal then travels through the grid. If a new code is sent from the GSM base after a while, the working SMs will nullify the carrier signal and authenticate themselves. In the case of a consumer with malfunctioning meter and/or committing theft, the SM of such customer will not update the new signal or nullify the carrier signal, and there will be a voltage drop in the carrier signal at the point where the theft is taking place. The software used in driving the diagnostic system determines the location of the theft (but not the exact consumer who committed the theft) and sends a notification.

While Paruchuri and Dubey (2012) provide a practical, feeder-level approach to estimating NTL, their method lacks individual consumer-level analysis, smart metering integration, and real-time data analytics. Combining feeder-level estimation with SMs and ML would enhance ETD accuracy and efficiency, especially in developing regions.

2.5.2.3 Signal generation and processing

Signal generation and processing-based NTL solution presents a pragmatic way of detecting and controlling ET directly from their sources. In leading studies, harmonic signals are introduced to distribution lines to clear out illegal consumers on the line. The signals sent to the lines are generated and processed to only execute the goals intended by the sender. The signals are meant to destroy the electric devices or equipment illegally connected to the distribution lines by the electricity thieves. To protect the equipment of honest customers against the power surge sent to the distribution lines by the harmonic signal generator, the utility agents disconnect the meters of all the benign customers before sending the harmonic signals to the lines. This signal negatively affects the illegal equipment connected to the distribution lines. This method has the advantage that it could uncover all kinds of NTL in the electricity grid. The only shortcoming of this method currently is its dependence on smart metering systems (Viegas et al., 2017:1259, 1261).

The authors in Pasdar and Mirzakuchaki (2007) proposed sending high-frequency test signal using the principle of power line carrier communication (PLC) to LV distribution network, in a bid to discover if illegal equipment is connected to the distribution grid or not, after disconnecting the loads of legal electricity consumers on the grid through control signals to their SMs. Characteristics of line impedance that connects the observer SM at the distribution transformer and the SMs of the consumers are calculated using a software which monitors the grid and also discovers the location of illegal electricity usage by calculating the difference between supplied and consumed electricity. Other authors like Christopher et al. (2014) also proposed an ETD technique using the principle of PLC. In this method, a narrow-band PLC signal is injected into the LV distribution line. According to Christopher et al. (2014), a differential change in the amplitude of the narrow-band carrier signal after injecting it to the distribution line is an indication of ET. Variation in the high-frequency carrier signal can be detected effectively even if a high-frequency rejection circuit is connected between the point of electricity abstraction and the load.

While both Pasdar and Mirzakuchaki (2007) and Christopher et al. (2014) introduce remote monitoring solutions using smart metering and line monitoring respectively**,** neither of the two papers incorporates advanced ML-based theft detection or consumer-level consumption analysis. Combining smart metering, real-time line monitoring, and ML models would offer a more comprehensive NTLD solution capable of detecting both physical tampering and consumption anomalies.

The authors in Depuru et al. (2011a) proposed the use of harmonic signal generator to introduce harmonic or unwanted signals to the LV distribution grid in an attempt to clear out or destroy the connected equipment of illegal consumers contributing additional loads to the grid. The genuine or legal consumers are isolated from the harmonic signals after disconnecting their loads or appliances from the grid via control signals to their SMs, in a bid to mitigate ET and improve distribution efficiency.

While this method by Depuru et al. (2011a) aims to penalize illegal consumers, it is crucial to recognize the ethical and legal implications of intentionally introducing harmful harmonics into the power supply. Such actions could inadvertently affect legitimate consumers and compromise the overall integrity of the electric grid. Although, the authors also provide a valuable foundational discussion on SMs and policy interventions for ET prevention**,** the study lacks implementation, ML integration, and contextual considerations for developing regions. Combining SMs with data-driven ML models would enhance theft detection capabilities, especially in regions with partial SG coverage.

2.5.3 Non-hardware solutions

Non-hardware NTL solutions or non-hardware NTLD methods involve the use and manipulation of the data generated by measuring devices on the electric grid for ETD (Viegas et al., 2017:1261; Guarda et al., 2023:22). The non-hardware NTLD methods allow electric utilities to use their existing infrastructure for the gathering of consumers' consumption information for the determination of ET, and do not require the procurements of new hardware or equipment (Viegas et al., 2017:1259. 1261; Saeed et al., 2020:8; Guarda et al., 2023:4). Grid observability is increased tremendously with SGs and SMs, and provide increased availability for huge energy consumption data from various consumers, in conjunction with other network data (Guarda et al., 2023:1). The authors in Glauner et al. (2017:761), Glauner (2019:31, 110), Saeed et al. (2020:1), and Coma-Puig et al. (2024:2704) have already established that the use of non-hardware AI methods is the state-of-the-art or the most-advanced technique used for ETD, while the authors in Ghori et al. (2020:16033-16034), Guarda et al. (2023:4), Stracqualursi et al. (2023:12, 16), and Coma-Puig et al. (2024:2704) have also attested to that fact by affirming that ML methods are more efficient and more effective in detecting NTL than several other available methods. The classification of the non-hardware NTLD methods is presented in Figure 2.21.

This category of NTL solution has been latched upon based on the advancement in data processing and in the capacities of modern communications. The energy consumption data or load profiles of electricity customers are analysed and pilferage of electricity is predicted or inferred based on deviations of consumers' consumption patterns from the norm. Other grid data like network topology or network measurements from the distribution grid may also be used for analysis to determine the irregularities between the billed electricity and the actual electricity distributed for consumption. Existing hardware equipment with specified functions are required at various points of the grid to acquire data for analysis (Viegas et al., 2017:1261-1262; Messinis & Hatziargyriou, 2018:251; Saeed et al., 2020:8). Points of irregular patterns which are probable sources of NTL in the consumption data are trends of energy losses and an indication of the presence of NTL in the electrical system. The customers with high irregularities in consumptions show high probability of theft and are therefore inspected (Depuru et al., 2011a:1011; Poudel & Dhungana, 2022:110) and prosecuted if found culpable of stealing electricity (Jiang et al., 2014:111).

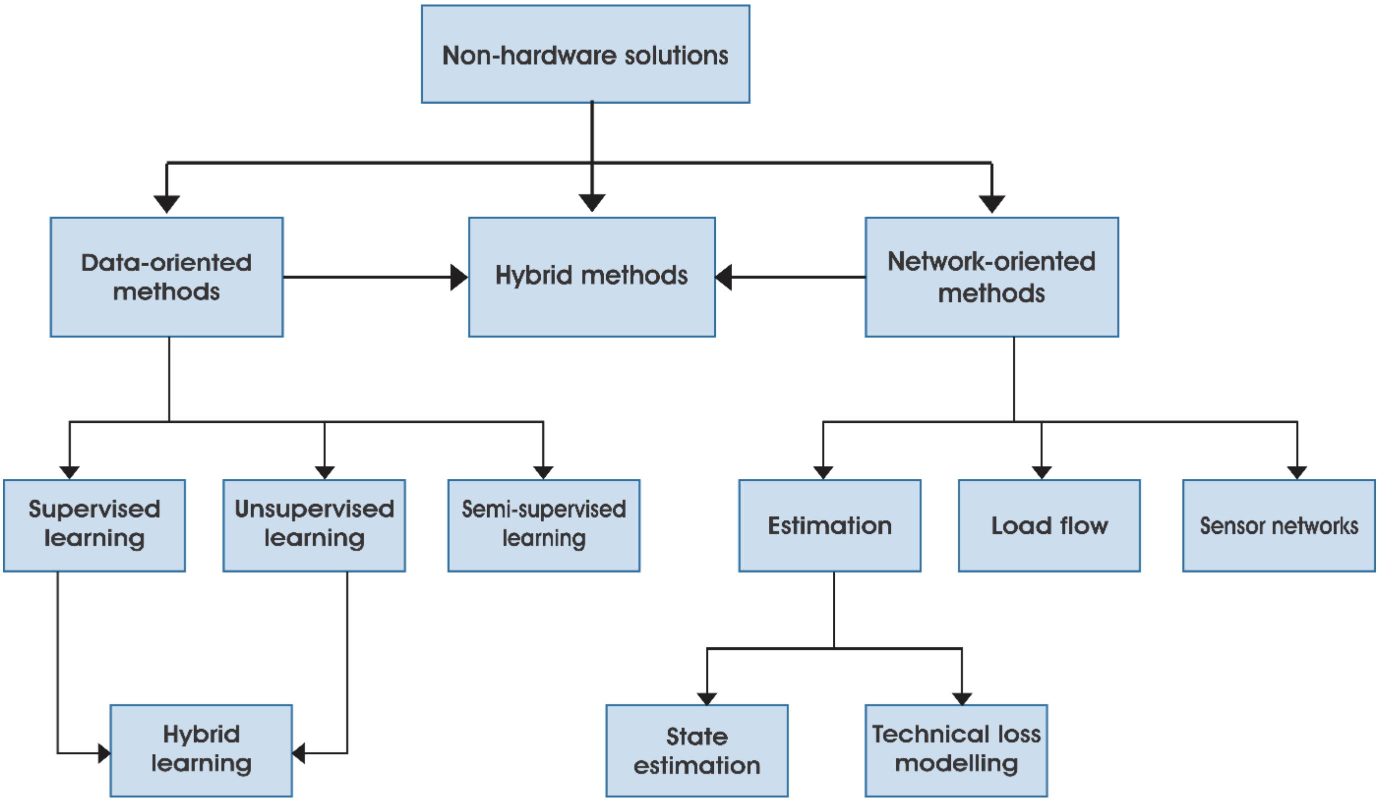


Figure 2.21: Categorization of non-hardware NTL detection methods

Adapted from (Viegas et al., 2017:1260-1263; Messinis & Hatziargyriou, 2018:252; Ghori et al., 2020:16035; Saeed et al., 2020:7-8; Guarda et al., 2023:4-5; Kim et al., 2024:6-7)

2.5.3.1 Tools used for the implementation and evaluation of non-hardware solutions

The classification of the various non-hardware methods for NTLDs has been shown in Figure 2.21. Before reviewing each category of the non-hardware NTL solutions later in Section 2.5.3.2, the tools or parameters (i.e., dataset and their features) required for the implementation of the non-hardware NTLD methods, and evaluations (i.e., performance metrics) of the aftermath NTLD models are discussed in this section.

❖ Dataset

Datasets are like raw materials for the NTLD system, used as inputs into models to produce outputs. The raw dataset used for NTLD can be categorized as Consumer level and Area level datasets according to the location where they are physically sourced (Messinis & Hatziargyriou, 2018:253, 258). Consumer level dataset are sourced from individual electricity consumers, while the Area level dataset relate to the area where the data is taken. Example of consumer level data is active energy consumption, while that of Area level data is network topology. Either of the categories of data could be time series data or static data. The different types of data used in NTLD are shown in Figure 2.22. In SG system, the AMI collects energy consumption readings from SMs and send them to utility companies at different time intervals per day. The time between when readings are dynamically registered (time resolution) are different from one AMI deployment to another, as there is no stipulated timing standard attached to the time resolutions when energy consumptions are registered by SMs (Mashima & Cárdenas, 2012:215). However, some timestamped resolutions or granularities of datasets have been classified whereby consumer level time series data could be high-resolution, medium-resolution, low-resolution active/reactive energy data and SM network data as shown in Figure 2.22.

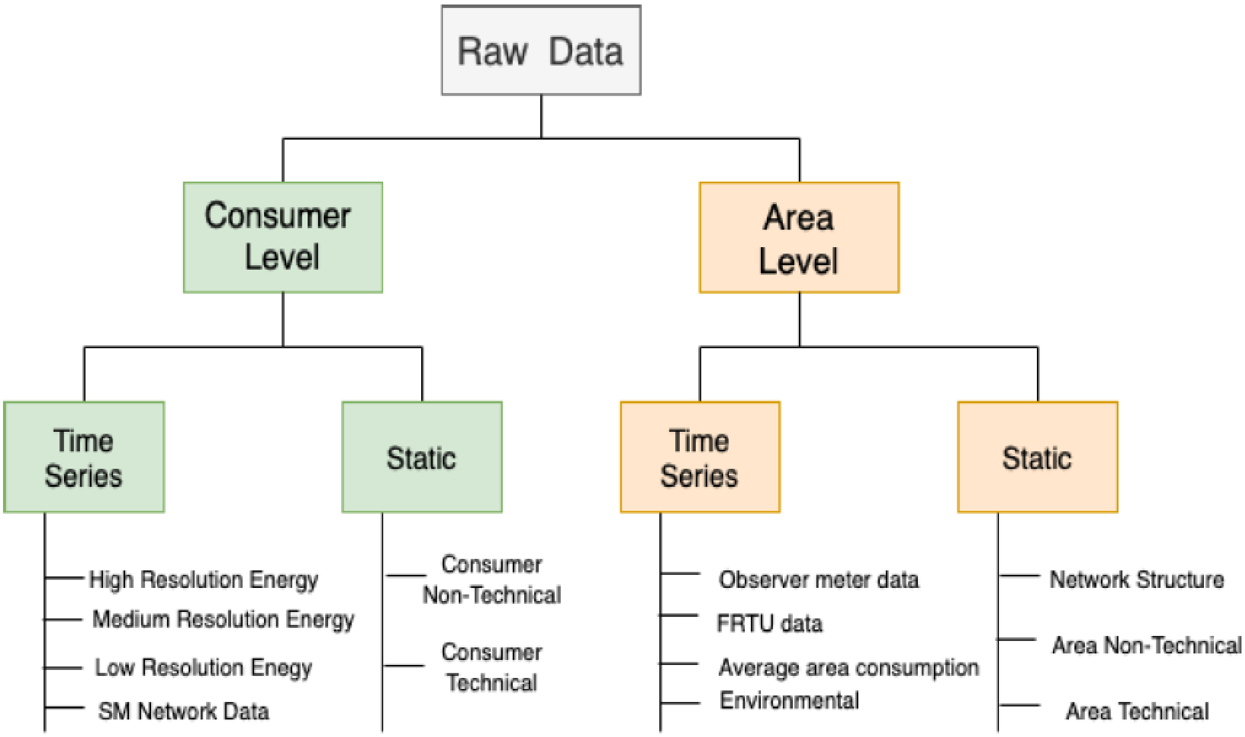


Figure 2.22: Categorization of the data types used for NTL detections

(Messinis & Hatziargyriou, 2018:258)

Resolutions or granularities are the sampling times or time intervals between when consumption data are registered from the different SMs in the AMI before they are being stored in the database of the utilities. High-resolution energy data are data taken within a period that is less or equal to ten minutes, medium-resolution energy data are taken between fifteen minutes and one hour, while low-resolution energy data are taken within the period of a month or further. SM network data is a non-energy consumption data which correlates with alarms, voltage, line resistance or current obtained from SMs. Consumer level static data comprise of consumer non-technical data and consumer technical data. Consumer non-technical data describe the behaviours of the electricity consumers as it regards their economic activities, perceptions on inspections, etc. Consumer technical data is the technical information that has to do with the power infrastructure of the electricity consumers, for example, power installed and power demand in kW, rating of power transformer in kVA, number of line phases, number of the available appliances used, remote-controlled space heating system, etc. (Messinis & Hatziargyriou, 2018:253, 258). The consumer level time-series data is referred to as consumption profile, while the consumer level static data is referred to as additional data (Viegas et al., 2017:1263; Ghori et al., 2020:16035, 16037).

Area level time-series data is further divided into observer meter data, feeder remote terminal unit (FRTU) or simply remote terminal unit (RTU) data, average area consumption data and environmental data. The installed observer meter at the LV side of the secondary transformer of the electricity distribution network measures the voltage, current, and power consumption. The FRTU data are voltage, current, and power measurements obtained from the RTUs installed at the LV or medium-voltage (MV) end of the electricity distribution network. Average area consumption is the average energy consumption of a particular area in question, while the environmental data is basically a measure of temperature, although it may also comprise other factors. Area level static data consists of network structure, area technical and the area non-technical data. The data representing the network structure represent the network topology of the MV and LV network, for example, the percentage of TL or the transformer to which an electricity consumer is connected to. Area technical data are data that reveals the technical characteristics of an area, for example, numbers of transformers being used in an area, the percentage of customers with irregular power consumption, the percentage of irregular consumers using a particular transformer, etc. Area non-technical data are the non-technical data that represents the social and/or economic information of electricity customers, for example, average income, campaign efforts against ET, average number of residents in a particular area, percentage of residents who have access to water, and literacy percentage, etc. (Messinis & Hatziargyriou, 2018:258).

The size of the dataset used for NTLD is dependent on the numbers of consumers involved or the numbers of consumers' consumption data collected and used in NTLD simulations. Datasets from 1000 customers upwards are considered as large or big data. Customer data between 100 customers up to or less than 1000 customers are regarded as medium data, while dataset that is not up to 100 customers are referred to as small data (Messinis & Hatziargyriou, 2018:252). The size of datasets also provides information on the scalability of NTLD algorithms.

- **Features**

Features are the most important components of any ML methods or techniques (Osypova, 2020:35). Features are extracted from raw datasets as input data into ML models to provide suitable representation of the raw datasets in order to make predictions or decisions (Messinis & Hatziargyriou, 2018:252; Janiesch et al., 2021:688). Features are mostly used by researchers in the field of electrical engineering and other related fields for NTLD. A feature is a separate computable characteristic of a system under consideration (Chandrashekar & Sahin, 2014:16). Feature selection involves the methods of finding the most important variables in a dataset for the detection of NTL. These features or variables are selected by domain experts or by using feature selection algorithms (Messinis & Hatziargyriou, 2018:252).

Selecting relevant and optimal set of features reduces data dimension, removes redundancies, and improves prediction performances (Khalid et al., 2014:372; Miao & Niu, 2016:919). Features for NTLD are commonly used with data-oriented methods or sometimes hybrid methods, for the detection of NTL (Messinis & Hatziargyriou, 2018:258). Energy/kWh consumption profiles with varying resolutions are the main features used for NTLD (Ramos et al., 2018:680). Listed and defined below are other common features computed from kWh consumption profiles which are also used for NTLD, as reported in the literature (Messinis & Hatziargyriou, 2018:252; Saeed et al., 2020:5):

(a) **Standard deviation, max/min, average:** Statistical measures calculated over a specified period of electricity consumption.

(b) **Load factor:** It is an index that shows the ratio of the average energy consumed in kWh over a period to the peak or maximum energy consumed in kWh over the same period.

(c) **Streaks:** It is the number of times in which energy consumption curves move up or go down the mean axis. It is also known as the moving mean of the energy consumption curve.

(d) **Wavelet coefficients:** Wavelet coefficients refer to the difference or gap between the consumption curves (or load curves) that are currently being considered for classification, and the wavelet coefficients of the consumption curves of the previous year.

(e) **Estimated readings:** The approximated readings used by the electric utilities to bill electricity customers because the utilities could not obtain the actual readings.

(f) **Predicted kWh:** It is the difference between the expected active-kWh energy consumptions and the observed active-kWh energy consumptions

(g) **Reduction in the consumption of energy:** The reduction in the energy consumed at a particular current period as compared the energy consumed in the past over the same time period.

(h) **Seasonal consumption rates:** The comparison of the total energy consumption in a particular season to the total energy consumption in a different season.

(i) **Euclidean distance to mean customer:** It refers to the Euclidean distance between the overall energy consumption curve and the active energy consumption curve within a dataset, which is a measure of the average consumption of all customers in the dataset.

(j) **Power factor:** Power factor (PF) which has values between 0 and 1 and used to express energy efficiency, is the ratio of the real power consumed in kilowatt (kW) to the apparent power in kilovolt-ampere (kVA).

(k) **Energy factor:** The energy factor, which is also an expression of energy efficiency of appliances and equipment, is the ratio of the reactive energy consumed in kilovolt-ampere reactive hour (kVArh) to the consumed active energy in kWh during the same period of time.

(l) **PCA components:** They are those components or variables derived from the active energy consumption curves as calculated by using Principal Component Analysis (PCA) or Kernel Principal Component Analysis (KPCA).

(m) **Pearson coefficient:** This coefficient shows the correlation between the real energy consumed over a given period of time as measured by a linear equation.

(n) **Skewness:** Is the measure of distortion or asymmetry in a typical dataset that is normally distributed.

(o) **Fractional order dynamic errors:** These are features that shows distinction between a profiled energy consumption data and a time series energy consumption data obtained in real time.

(p) **Mismatch ratio:** It is the difference between the energy consumed as measured at the medium voltage to low voltage (MV/LV) secondary distribution transformer and the sum of energy consumptions registered by the consumers' electric meters including the estimated energy losses due to technical losses (TL), divided by the rated output power released from the primary distribution substation.

(q) **Kurtosis:** Is a measure of the number of outliers available in a normal-distribution data.

(r) **Fourier coefficients:** It is the difference between the calculated Fourier coefficients from the consumption curve that currently is to be classified and the Fourier coefficients derived from the consumption curves of the previous years.

(s) **Decrease in consumption as compared to a previous period:** This is the reduction in energy consumption when compared with the energy consumption of an earlier period of the same length of time.

(t) **Slope of consumption curve:** This is the slope of the line of best fit of time-series active energy consumption curve derived from the linear equation of the line.

(u) **Coefficients of Discrete Cosine Transform:** These coefficients are the first or initial coefficients (i.e., k coefficients) of discrete cosine transform.

(v) **Coefficients of polynomial fit:** It is the difference between the coefficients of the polynomial that fits best the consumption curve to be classified and the coefficients of the polynomial that fits best the consumption curve of the previous years.

(w) **Demand billed:** This is the active power demanded to be consumed and billed. It is measured in kilowatt (kW).

❖ Performance metrics

Performance metrics are evaluation metrics used for the assessment of ETD or NTLD models to determine their prediction efficacies and efficiencies (Messinis & Hatziargyriou, 2018:252; Poudel & Dhungana, 2022:115). These metrics are used to rate or compare the performances of various ETD models (Messinis & Hatziargyriou, 2018:252, 259). The evaluation metrics validate how well NTLD models have been able to execute the given prediction tasks. All the available performance evaluation metrics encountered in the reviewed ETD or NTLD literature have been discussed in this section.

To calculate the performance metrics of NTLD models, the conventional table known as confusion matrix is first calculated (Messinis & Hatziargyriou, 2018:259). Since ETD is a binary classification problem (Chen et al., 2022:5), the traditional 2x2 confusion matrix, which is the classification summary for binary classification models, are being produced through NTLD models to evaluate the potency of their detection capacities (Farid et al., 2023:84; Xia et al., 2023:6). Prediction results from confusion matrix are regarded as "True (T)" when they are rightly classified, and "False (F)" when they are wrongly classified (Saeed et al., 2020:6; Poudel & Dhungana, 2022:115).

The basic 2x2 confusion matrix which contains the summary of the classification results or performance breakdown of ETD or NTLD models is shown in Table 2.1 (S. Zhu et al., 2024:15487).

Table 2.1: Confusion matrix

Actual class	**Predicted class**	
	Positive (1)	Negative (0)
Positive (1)	True positive (TP)	False negative (FN)
Negative (0)	False positive (FP)	True negative (TN)

As could be seen in the confusion matrix presented in Table 2.1, true positive is represented as TP, true negative as TN, false positive as FP, and the false negative is represented as FN (Huang et al., 2024:11; Mehdary et al., 2024:19).

TP refers to the fraudulent electricity consumers who have been correctly predicted as dishonest, TN indicates honest consumers that have been correctly predicted as non-fraudulent, FP relates to honest consumers who have been wrongly predicted fraudulent, while FN denotes dishonest consumers that have been incorrectly predicted honest (Gunduz & Das, 2024:13; Mehdary et al., 2024:18). In the Table 2.1, honest and fraudulent electricity customers are regarded as 'negative' and 'positive' customers, which are also be depicted with "0" and "1" labels respectively (Glauner, 2019:48; Munawar, Javaid, et al., 2022:12). Predicted class represents the honest and fraudulent customers being classified by ML models, while actual class represents the customers' labels given to them by the utility technicians after confirming their NTL statuses during onsite inspections (Lu et al., 2019:5; Khattak et al., 2022:5). FPs are undesirable since they spur unnecessary onsite inspections and contribute to high operational costs to the electric utilities (Messinis & Hatziargyriou, 2018:259, 264; Saeed et al., 2020:6; Aldegheishem et al., 2021:25051; Pamir, Javaid, Qasim, et al., 2022:56866, 56870).

The imbalanced nature of electricity consumption dataset with unequal distribution of labels or classes is characteristic of real-world datasets obtained from electric utilities (Ghori et al., 2020:16034, 16036). This is owing to the fact that electric utilities have more honest customers on their grids than fraudulent customers (Guarda et al., 2023:21). In the class distribution of real datasets, it is natural to discover that honest customers who do not steal electricity are far more than the few unscrupulous customers who steal electricity from the grid. For this reason, most real datasets are found naturally to be imbalanced and biased since they convey more representations of the honest customers. Hence, all real-world datasets that are used to train and validate NTLD models are naturally imbalanced in terms of labels or classes, except if the minority classes in the dataset have been synthetically resampled and balanced during data preprocessing using various class-balancing techniques. Imbalanced datasets negatively affect the consistency of ETD or NTLD models (Khattak et al., 2022:1, 18), and hence affect their performance results. For synthesized, simulated, or fabricated datasets, the class of those customers who steal electricity and those customers who do not steal electricity contain equal distributions (Ghori et al., 2020:16034, 16036, 16040).

Accuracy is the most popular performance metric used in evaluating ML classifier models (Ghori et al., 2023:15336). Accuracy indicates the number of the correctly predicted samples out of all the available validation or test-set samples (Khan et al., 2020:15; Mehdary et al., 2024:19). Equation 2.3 (Gunduz & Das, 2024:14; Huang et al., 2024:11) shows the mathematical expression of the accuracy metric.

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \tag{2.3}$$

TP, TN, FP, and FN in Equation 2.3 indicate the proportions of true positive, true negative, false positive, and false negative respectively as predicted by the classifier model. Normally, increased accuracy shows that the NTLD model or system where the accuracy result is obtained classifies or predicts the negative and positive samples satisfactorily. However, higher accuracy performance may be unreliable or misleading if the datasets used in developing the NTLD model is imbalanced causing overfitting of the majority class (Ghori et al., 2023:15336). Imbalanced dataset means that the samples of those consumers who did not steal electricity (negative samples or negative class) are overly more than those consumers who steal electricity (positive samples or positive class) (Messinis & Hatziargyriou, 2018:259; Ghori et al., 2020:16034). Besides the misleading tendency of the accuracy metric as mentioned, accuracy may also be high with high FPs as shown in the table presented in Poudel and Dhungana (2022:116).

Precision and recall are computed using Equations 2.4 and 2.5 (Huang et al., 2024:12; Iftikhar et al., 2024:10). Precision, assertiveness, confidence or positive predictive value

(PPV) refers to the proportion of the correctly predicted number of consumers who cause NTL (positive samples or positive class) out of the total predicted consumers causing NTL (Messinis & Hatziargyriou, 2018:259; Saeed et al., 2020:6; Lepolesa et al., 2022:39647; Ghori et al., 2023:15336; Mehdary et al., 2024:19), giving a perception into the actual number of predicted electricity thieves in a given dataset (Ghori et al., 2020:16041) as predicted by the NTLD system. The recall metric refers to the success achieved in detecting NTL (Messinis & Hatziargyriou, 2018:259). It is the proportion of the correctly predicted positive samples (fraudulent or malignant customers) out of all the available positive samples, giving an insight into the actual number of electricity thieves in a given dataset (Ghori et al., 2020:16041; Khan et al., 2020:15; Khan et al., 2023:544; Mehdary et al., 2024:19).

$$Precision = \frac{TP}{TP+FP} \tag{2.4}$$

$$Recall = \frac{TP}{TP+FN} \tag{2.5}$$

Recall is also known as detection rate (DR), sensitivity, true positive rate (TPR) or hit rate (Messinis & Hatziargyriou, 2018:259; Pamir, Javaid, Qasim, et al., 2022:56870). If precision increases, it means that most of the correctly predicted positive samples or the actual number of electricity thieves out of the total predicted positive samples by the NTLD model have been classified correctly. Greater values of recall convey that the success attained when predicting fraudulent customers or positive samples (out of all the available positive samples) is high, implying that the NTLD system is performing commendably well.

Precision and recall are disproportional metrics, meaning that when one increases, the other one decreases (Messinis & Hatziargyriou, 2018:259; Saeed et al., 2020:6). Therefore, the balance between the two metrics could be found by combining them. Performance metrics like arithmetic mean, F-measure or F1 score, and F_{β} as expressed in Equations 2.6, 2.7, 2.8, and 2.9 combine the results of precision and recall (Ghori et al., 2023:15336-15337; Gao et al., 2024:15; Gunduz & Das, 2024:14; Huang et al., 2024:12). F-measure or F1 score is also referred to as F-score. Other evaluation metrics like average precision (AP), mean average precision (MAP), and area under precision-recall curve (PR-AUC) are also obtained by combining precision and recall scores, but they are specifically associated with the precision-recall curve. AP, MAP, and PR-AUC are later discussed in the subsequent paragraphs.

$$Arithmetic\ mean = \frac{Precision+Recall}{2} \quad \textbf{(2.6)}$$

$$F - measure = \frac{2\times(Precision \times Recall)}{(Precision+ Recall)} \quad \textbf{(2.7)}$$

$$F1\ score = \frac{2TP}{2TP+FP+FN} \quad \textbf{(2.8)}$$

$$F_\beta = \frac{(1+\beta^2)\times(Precision \times Recall)}{\beta^2\times(Precision+ Recall)} \quad \textbf{(2.9)}$$

The arithmetic mean in Equation 2.6 represents the average of precision and recall scores. F-measure or F1 score expressed in Equations 2.7 and 2.8 gives an insight on precision and recall metrics by maximizing them, and is better suited for assessing imbalanced datasets (Messinis & Hatziargyriou, 2018:259; Ghori et al., 2020:16041; Khan et al., 2020:15; Saeed et al., 2020:6). High F1 score is an indication that the NTLD system detects so many NTL or frauds in the power system (Messinis & Hatziargyriou, 2018:259; Saeed et al., 2020:6). F-measure is an alternative term to F1 score, as either term stands for the weighted average or the harmonic mean of both precision and recall, and gives reliable performance evaluations with imbalanced datasets (Messinis & Hatziargyriou, 2018:259; Khan et al., 2020:15; Bohani et al., 2021:5; Ghori et al., 2023:15337; Xia et al., 2023:6; Mehdary et al., 2024:19). Hence, it should be noted that Equations 2.7 and 2.8 are equal, as Equation 2.8 is derived from Equation 2.7 by substituting for the precision and recall of Equations 2.4 and 2.5 into Equation 2.7 (Ghori et al., 2020:16041; Saeed et al., 2020:7).

Another form of F1 score, F-measure or F-score metric is denoted as F_β in Equation 2.9 (Ghori et al., 2023:15336; Gao et al., 2024:15). In the Equation 2.9, β is a coefficient that is used to adjust the weight or priority of precision with respect to recall. When $\beta = 1$, it means that both precision and recall have equal relative importance or equal priority, but if $\beta > 1$, it means that recall is given more priority than precision, while if $\beta < 1$, precision is given more priority than recall. However, the coefficient value $\beta = 1$ is mostly used when dealing with imbalanced datasets (Ghori et al., 2023:15336). The arithmetic mean in Equation 2.6 is rarely used as it gives no insight into both precision and recall metrics; hence, the F-measure or F1 score (harmonic mean) in either Equation 2.7 or Equation 2.8 is preferred (Ghori et al., 2023:15336-15337). It should be noted that Equations 2.7 and 2.9 will be similar if the value of β in Equation 2.9 is equal to 1 ($i.e., \beta = 1$) (Messinis & Hatziargyriou, 2018:259), conveying that precision and recall are given equal priority (Ghori et al., 2023:15336). At $\beta = 1$, the F_β in Equation 2.9 will be written as F_1, which is where the term F1 score was derived.

Precision-recall curve is a graph of precision against recall at various classification thresholds, showing the trade-off between the two metrics at varying thresholds (Calvo et al., 2020:7). The performance metrics which are based on the precision-recall curve and used for evaluating ETD models are average precision (AP), mean average precision (MAP), and area under the precision-recall curve (PR-AUC) (Xia et al., 2023:6; Khan et al., 2024:12). Equation 2.10 expresses the average precision (AP) metric, where R_n in the equation represents the recall score at the current or nth threshold, R_{n-1} illustrates the recall score at the previous threshold, the weight $(R_n - R_{n-1})$ represents the increase in recall between the current and the previous threshold, while P_n depicts the precision score at the nth threshold (Calvo et al., 2020:7-8; Salman Saeed et al., 2020:12). AP is computed from the precision-recall curve as the average of the precision score at each recall level for every threshold (Calvo et al., 2020:7).

$$AP = \sum_n (R_n - R_{n-1}) P_n \tag{2.10}$$

MAP is a way of summarizing the whole precision-recall curve into a single value which represents the average or mean of all the precision scores available at different recall levels within the curve when a particular threshold is being considered (Liao, Bak-Jensen, et al., 2024). $MAP@N$ (MAP at top N labels) can be calculated using the mathematical expression in Equation 2.11; but before that, the variable $P@k_i$ (precision at location k_i) in Equation 2.11 is calculated first by applying Equation 2.12 (Bai et al., 2023:14; Q. Zhang et al., 2023:4; Liao, Zhu, et al., 2024:5080). k_i is the position or location of the fraudulent or positive individual ith sample among the fraudulent samples where ET is taking place, where $(i = 1, \dots, r)$; while r is the number indicating how many electricity thieves are among the top N users (top N samples) who are being mostly suspected of stealing electricity (Zheng et al., 2018:1612; Bai et al., 2023:14; Xia et al., 2023:6; Liao, Bak-Jensen, et al., 2024). $MAP@N$ is the mean of all the retrieved $P@k_i$ instances in the precision-recall curve from $k = 1$ to $k = N$ (Zheng et al., 2018:1612; Liao, Bak-Jensen, et al., 2024; Liao, Zhu, et al., 2024:5080). Bai et al. (2023:14) used $MAP@ALL$ to represent MAP for all the given samples.

$$MAP@N = \frac{\sum_{i=1}^{r} P@k_i}{r} \quad \textbf{(2.11)}$$

$$P@k_i = \frac{Y_{k_i}}{k_i} \quad \textbf{(2.12)}$$

Before calculating the MAP metric, the samples or electricity users in the test set are sorted first in accordance with their prediction scores (Zheng et al., 2018:1611). After that, top N samples are selected to determine the performance of the model. Test set is the collection of data used in confirming the efficacy of the model after it must have initially been trained using the train sets. Y_{k_i} refers to the number of electricity thieves with the greatest suspicion who have been predicted correctly among the k_i users (Xia et al., 2023:6). The MAP is a location- or position-sensitive evaluation metric, and its values go higher if the fraudulent electricity consumers are ranked higher than the honest consumers (Bai et al., 2023:14). The position-sensitive MAP metric indicate the ability of ETD models to rank fraudulent samples higher than non-fraudulent samples (Bai et al., 2023:14; Liao, Bak-Jensen, et al., 2024).

PR-AUC is the area under the precision-recall curve of a binary classifier. The PR-AUC metric is appropriate for evaluating ML models developed with imbalanced datasets (Khan et al., 2020:15; Gao et al., 2024:16). Increased values of PR-AUC imply that both precision and recall simultaneously achieve high values, indicating a better trade-off between the precision and recall metrics (Gao et al., 2024:16). Such models with higher PR-AUC values have better predictive powers with lower prediction errors (Kulkarni et al., 2021:534). The equivalent mathematical equation for the calculation of PR-AUC is expressed in Equation 2.13 (Gao et al., 2024:16), where m in the equation represents the number of thresholds within the precision-recall curve, $Recall_i$ and $Precision_i$ are the precision and recall values at mth threshold, while $Recall_{i-1}$ is the recall value of the previous threshold.

$$PR - AUC = \sum_{I=1}^{m}(Recall_i - Recall_{i-1}) \times Precision_i \quad \textbf{(2.13)}$$

Some other performance metrics (Saeed et al., 2020:7; Elreedy et al., 2024:4917; Khalid et al., 2024:11; X. Wang et al., 2024:2186) used in the literature for the evaluation of NTLD models are:

$$TPR = \frac{TP}{TP+FN} \quad \textbf{(2.14)}$$

$$FPR = \frac{FP}{FP+TN} \tag{2.15}$$

$$TNR = \frac{TN}{TN+FP} \tag{2.16}$$

$$FNR = \frac{FN}{FN+TP} \tag{2.17}$$

$$NPV = \frac{TN}{TN+FN} \tag{2.18}$$

$$G - mean = \sqrt{Recall \times TNR} \tag{2.19}$$

$$Dominance = TPR - TNR \tag{2.20}$$

$$Recognition\ rate = 1 - 0.5\left(\frac{FP}{N} + \frac{FN}{P}\right) \tag{2.21}$$

$$BDR = \frac{P(I) \times DR}{P(I)\times DR+P(-I)\times FPR} \tag{2.22}$$

$$MCC = \frac{TP\times TN-FP\times FN}{\sqrt{(TP+FP)(TP+FN)(TN+FP)(TN+FN)}} \tag{2.23}$$

It should be noted that TPR of Equation 2.14 and the recall or sensitivity of Equation 2.5 are same (Iftikhar et al., 2024:10). FPR in Equation 2.15 is the false positive rate. FPR is the number of honest customers (negative samples) that have been wrongly classified or predicted as fraudulent (positive samples) divided by the total number of honest customers (negative samples), or FPR is the ratio of false positives to that of total instance of actual negative samples (i.e., the proportion of incorrectly predicted negative samples) (Ghori et al., 2023:15336; Khan et al., 2023:544). TNR in Equation 2.16 is true negative rate, while FNR in Equation 2.17 is false negative rate. TNR or specificity is the proportion of honest consumers (negative samples) who have been correctly identified as honest or benign out of all the available negative samples, while FNR is the proportion of fraudulent consumers (positive samples) who have been wrongly classified as honest consumers (negative samples) out of all the available positive samples (Ghori et al., 2023:15336). TPR can also be determined from (TPR = 1 – FNR), while TNR can as well be calculated from (TNR = 1 – FPR).

Precision, recall or TPR, accuracy, FPR, TNR, FNR and F1 score are common metrics calculated from the confusion matrix and are often used to evaluate NTL classification models (Messinis & Hatziargyriou, 2018:259; Saeed et al., 2020:6). The negative predictive value (NPV) in Equation 2.18 is the proportion of the correctly predicted negative samples out of all the samples predicted as negatives (Ghori et al., 2023:15336). The geometric mean (G-mean) in Equation 2.19 measures how good a classifier has performed for both recall and TNR (Ghori et al., 2023:15337).

The dominance metric in Equation 2.20, which was first proposed by García et al. (2008), measures the influence or dominance between the positive and negative classes. The values of dominance ranges between -1 and +1 (Ghori et al., 2023:15337). Dominance value equals to 1 denotes that the minority class is perfectly predicted, but the majority-class cases are being missed; and vice versa for when dominance value equals to -1. A good prediction accuracy for the positive class is indicated if the dominance value is close to 1, while a good prediction accuracy of the negative class is depicted if the dominance value is close to -1 (Ghori et al., 2023:15337). Recognition rate in Equation 2.21 is also referred to as accuracy rate and measures the percentage of correct predictions in a dataset under consideration (Ramos et al., 2018:682). Recognition rate depicts how well an NTLD system is able to correctly predict the target positive or negative samples in a given dataset. P in the equation refers to the number of the entire real positive samples in a given dataset which is equivalent to (TP+FN), while N in the same equation denotes the overall number of real negative samples in a given dataset which is equal to (TN+FP) (Messinis & Hatziargyriou, 2018:259).

Bayesian detection rate (BDR) is the probability of ET taking place under ETD or NTLD conditions, or BDR is the proportion of NTL detected by NTLD models or intrusions/network attacks in intrusion detection systems (Gu et al., 2022:4571). BDR is not a commonly used metric in NTLD literature (Messinis & Hatziargyriou, 2018:259; Saeed et al., 2020:6). For the BDR metric in Equation 2.22, $P(I)$ is the probability that a consumer commits electricity theft or the probability of intrusion occurrence; $P(-I)$ is the complement of $P(I)$ meaning probability of no electricity theft and is equivalent to $(1 - P(I))$, but the value of $P(I)$ should be high, while a very low FPR is also required to achieve an acceptable high BDR value, in order to reduce false alarms (Jokar et al., 2016:221; Gu et al., 2022:4571).

The Matthews correlation coefficient (MCC) metric as shown in Equation 2.23 (Appiah et al., 2023:4; X. Wang et al., 2024:2186) is the most reliable evaluation metric for evaluating models constructed with imbalanced datasets (Kulkarni et al., 2021:534). MCC gives a high score only on a condition that all the four values of TP, TN, FP and FN in a confusion matrix produce good prediction results (Khan et al., 2020:15; Aldegheishem et al., 2021:25051; Kulkarni et al., 2021:534). The prediction scores of MCC is in the range of -1 to 1, with 1 indicating an incorrect prediction, 0 showing no prediction, close to 1 values showing good prediction, while 1 shows perfect prediction (Khalid et al., 2024:11; X. Wang et al., 2024:2186).

Cohen's kappa coefficient or simply "kappa" as expressed in Equation 2.24 is a metric used for the assessment of the extent of alignment between the expected and observed accuracies, in a bid to determine the strength of classification models (Hussain et al., 2022:1268). The symbol ρ_o in Equation 2.24 represents the observed accuracy, observed agreement, or the general accuracy of the model; while ρ_e depicts the expected accuracy, expected agreement, likelihood of accurate prediction, chance agreement, random chance, or random accuracy of the model (Ghaedi et al., 2022:68). The equivalents of ρ_o and ρ_e based on the conventional 2x2 confusion matrix for a binary classifier are respectively shown in Equations 2.25 and 2.26 (Chicco et al., 2021:78371; Ghaedi et al., 2022:69). The Cohen's kappa coefficient metric is based on the customary 2x2 confusion matrix and is usually employed for evaluating two-class or binary classifiers (Chicco et al., 2021:78371).

$$kappa = \frac{\rho_o - \rho_e}{1 - \rho_e} \tag{2.24}$$

$$\rho_o = \frac{TP+TN}{TP+TN+FP+FN} \tag{2.25}$$

$$\rho_e = \left(\frac{TP+FP}{TP+TN+FP+FN} \times \frac{TP+FN}{TP+TN+FP+FN}\right) + \left(\frac{TN+FP}{TP+TN+FP+FN} \times \frac{TN+FN}{TP+TN+FP+FN}\right) \tag{2.26}$$

The observed accuracy (ρ_o) in Equation 2.25 is the proportion of correct predictions ($TP + TN$) divided by the outright number of samples ($TP + TN + FP + FN$), which is equal to the accuracy metric expressed in Equation 2.3. Equation 2.26 can be explained by considering that the columns of the confusion matrix of a binary classifier represent the predicted class while the rows represent the actual class with fraudulent predictions first before the benign predictions at the columns and rows of the confusion matrix like in Table 2.1, then the expected accuracy (ρ_e) as shown in Equation 2.26 is the sum of the fraudulent predictions of the predicted class in the first column ($TP + FP$) divided by the total number of samples

$(TP + TN + FP + FN)$, multiplied by the fraudulent predictions of the actual class in the first row $(TP + FN)$ divided by the total number of samples $(TP + TN + FP + FN)$; plus the benign predictions of the actual class in the second row $(TN + FP)$ divided by the total number of samples $(TP + TN + FP + FN)$, multiplied by the benign predictions of the predicted class in the second column $(TN + FN)$ divided by the total number of samples $(TP + TN + FP + FN)$ in the confusion matrix. Unlike the overall accuracy metric of Equation 2.3 which is biased towards the majority class and hence gives misleading results with imbalanced datasets, kappa gives reliable results with imbalanced datasets (Alkhresheh et al., 2022:808-809; Saxena, 2023). By substituting for ρ_o and ρ_e from Equations 2.25 and 2.26 into Equation 2.24, Equation 2.27 is obtained (Chicco et al., 2021:78371; Gao et al., 2022).

$$kappa = \frac{2\times(TP\times TN - FP\times FN)}{(TP+FP)\times(FP+TN)+(TP+FN)\times(FN+TN)} \quad \textbf{(2.27)}$$

Like the MCC, the Cohen's kappa coefficient ranges between -1 to 1, indicating the degree of classification agreement or accuracy (Chicco et al., 2021:78371; Ghaedi et al., 2022:69). The higher the value of the kappa coefficient, the better the predictive model, showing greater accuracy or agreement and vice versa (Ghaedi et al., 2022:69). A kappa coefficient value of -1 indicates that the classification is perfectly wrong, a coefficient value of 0 indicates no agreement, while a coefficient of 1 shows perfect agreement (Chicco et al., 2021:78371).

Area under the curve (AUC) is another performance metric used for the evaluation of ETD or NTLD models (Aslam, Javaid, et al., 2020:13; Khan et al., 2020:15; Asif et al., 2022:27469). AUC is specifically the area under the receiver operating characteristic curve (ROC) to determine the overall quality of models (Ali et al., 2023:13; Bai et al., 2023:14; Xia et al., 2023:6; Liao, Bak-Jensen, et al., 2024). The ROC curve is the plot of TPR against FPR over different classification thresholds (Ali et al., 2023:14; Xia et al., 2023:6; Iftikhar et al., 2024:10; Liao, Bak-Jensen, et al., 2024). However, AUC can be computed using the formula provided in Equation 2.28 (Huang et al., 2024:12; Liao, Bak-Jensen, et al., 2024; Liao, Zhu, et al., 2024:5080). Equation 2.28 is based on the probability that a positive sample chosen at random will rank higher than a negative sample that has also been chosen in the same randomly manner (Zheng et al., 2018:1611; Liao, Bak-Jensen, et al., 2024). The AUC metric indicate the ability of ETD models to rank fraudulent (positive) samples higher than non-fraudulent (negative) samples (W. Liao et al., 2022:3521; Liao, Bak-Jensen, et al., 2024).

$$AUC = \frac{\sum_{i \in PositiveClass} Rank_i - \frac{M(1+M)}{2}}{M \times N} \quad \textbf{(2.28)}$$

Where $i \in PositiveClass$ in Equation 2.28 depicts that the sample i being considered is a positive sample and belongs to the positive class; $Rank_i$ represents the number of samples from the n samples which the prediction value of sample i exceeds when n samples are being arranged in ascending order, in accordance with the prediction scores of the positive samples (Khan et al., 2020:15). However, M is the number of positive samples in the positive class, while N is the number of negative samples in the positive class (Bai et al., 2023:14; Khan et al., 2023:544).

The performance evaluation metrics which have so far been discussed are based on the values in the categories of TP, TN, FP, and FN from confusion matrices. TP and TN are correctly predicted, while FP or false alarm and FN are errors made by the NTLD system, as a result of wrongly predicting the given input data samples (Messinis & Hatziargyriou, 2018:259; Saeed et al., 2020:6; Mehdary et al., 2024:19). The performance scores of ETD or NTLD models normally range between 0 and 1, except for those mentioned otherwise. The higher the values of the performance metrics obtained from ETD models, the more reliable and efficient the NTLD models that produced them, except for FPR and FNR that were discussed earlier, and logarithm loss (log loss), and regression loss functions (which will be discussed in the subsequent paragraphs) are vice versa. The discussed regression loss functions are mean squared error (MSE), root mean squared error (RMSE), absolute error (AE), mean absolute error (MAE), absolute percentage error (APE), and mean absolute percentage error (MAPE). The lower the values of FPR, FNR, log loss, and the regression loss functions, the fewer the errors produced by the ETD or NTLD models that produced such scores, and hence the better and more-efficient the models. Reduced FPR scores result in lower onsite inspection costs (Messinis & Hatziargyriou, 2018:259, 264; Aldegheishem et al., 2021:25051; Pamir, Javaid, Qasim, et al., 2022:56866, 56870; Xia et al., 2023:10).

The logarithmic loss (log loss), loss function, or cross entropy performance metric is expressed in Equation 2.29 (Wang et al., 2023:12; Liao, Zhu, et al., 2024:5080). The log loss metric is also referred to as binary cross entropy because it is basically used for binary classification problems (Liao, Zhu, et al., 2024:5080).

$$Log\ loss = -\frac{1}{N}\sum_{i=1}^{N} y_i \times \log\big(P(y_i)\big) + (1 - y_i) \times \log\big(1 - P(y_i)\big) \quad \textbf{(2.29)}$$

In Equation 2.29, y_i represents the actual-class or ground-truth label of either 0 value for honest customer i or a 1 value for fraudulent customer i, $P(y_i)$ is the probability or likelihood that customer i committed ET (i.e., have a label value of 1) as predicted by the model, while N is the total samples of electricity customers in a given dataset (Wang et al., 2023:12; Liao, Zhu, et al., 2024:5080). The log loss or loss function is a metric used to evaluate the difference between the observed or predicted and the actual or expected values, to determine the extent of classification wrongness or correctness (i.e., classification error) (Coma-Puig, 2022:14; Khan et al., 2024:13). The log-loss values range between 0 and ∞ (Banga et al., 2022:9590). The greater the difference or deviation between the observed and actual values, the greater the log-loss metric values (Coma-Puig, 2022:14; Gao et al., 2022). The closer the log-loss values to 0, that is, the lower the values of log loss, the higher the accuracy of the ETD or NTLD model, and hence the better the performance of the model and vice versa (Banga et al., 2022:9590).

The following Equations 2.30 to 2.35 found in the literature are known as regression loss functions, and are also used for the purpose of evaluating ETD or NTLD models (Bian et al., 2021:47259; Ribeiro et al., 2021; Coma-Puig & Carmona, 2022:14-15; Irfan et al., 2022:2154; Velasco Rodríguez, 2022:26-27).

$$MSE = \frac{1}{n}\sum_{i=1}^{n}(y_i - \hat{y}_i)^2 \quad \textbf{(2.30)}$$

$$RMSE = \sqrt{\frac{1}{n}\sum_{i=1}^{n}(y_i - \hat{y}_i)^2} \quad \textbf{(2.31)}$$

$$AE = |y_i - \hat{y}_i| \quad \textbf{(2.32)}$$

$$MAE = \frac{1}{n}\sum_{i=1}^{n}|y_i - \hat{y}_i| \quad \textbf{(2.33)}$$

$$APE = \left|\frac{y_i - \hat{y}_i}{y_i}\right| \times 100 \quad \textbf{(2.34)}$$

$$MAPE = \frac{1}{n}\sum_{i=1}^{n}\left|\frac{y_i - \hat{y}_i}{y_i}\right| \times 100 \quad \textbf{(2.35)}$$

Regression loss functions are commonly used for evaluating regression models. The mean squared error (MSE), root mean squared error (RMSE), absolute error (AE), mean absolute error (MAE), absolute percentage error (APE), and mean absolute percentage error (MAPE) expressed in Equations 2.30, 2.31, 2.32, 2.33, 2.34, and 2.35 respectively, are used for evaluating ETD or NTLD models to determine classification errors (Badawi et al., 2022:10). In the equations, y_i represents the expected or actual value of energy consumption (using train data), $\hat{y}_i$ is the predicted value of energy consumption (using validation or test data), i is the identification number for the particular electricity consumption sample being considered, while n is the number of the total energy consumption samples (Bian et al., 2021:47259-47260; Ribeiro et al., 2021; Irfan et al., 2022:154). If the calculated errors using the regression loss functions go beyond certain set thresholds, then ET or NTL is suspected (Ford et al., 2014; Tehrani et al., 2022:2). Generally, the lower the metric values of the regression loss functions, the more reliable the models that produced them, indicating better model performances (Kawoosa et al., 2023:4807).

Another performance metric called coefficient of determination, which is otherwise referred to as R-squared and denoted as R^2 (Ribeiro et al., 2021; Farhan & Nafi, 2022; Velasco Rodríguez, 2022:26) is expressed in Equation 2.36. The R-squared metric describes how the variation of a variable affects the variation of another variable (Ribeiro et al., 2021).

$$R^2 = 1 - \frac{\sum_{i=1}^{n}(y_i - \hat{y}_i)^2}{\sum_{i=1}^{n}(y_i - \bar{y}_i)^2} \tag{2.36}$$

The variable y_i in Equation 2.36 represents each actual value or feature, $\hat{y}_i$ represents each predicted value through the regression line of best fit or through the dependent variable, while $\bar{y}$ represents the average or mean of all the actual or original values (Ribeiro et al., 2021; Farhan & Nafi, 2022). In a regression model, the coefficient of determination (R^2) refers to how well the predictor or independent variables of the model can predict the outcome or dependent variable (Ribeiro et al., 2021; Farhan & Nafi, 2022; Velasco Rodríguez, 2022:26). In the fractional part of Equation 2.36, the numerator is the sum of the squared errors between each feature and the regression line of best fit, while the denominator represents the sum of the squared errors between every feature or actual value and the mean of all the features. The regression line of best fit is drawn based on the values of the dependent and independent variables. The values of R^2 range between 0 and 1 (Farhan & Nafi, 2022). The higher the value of R^2, the more reliable the regression model is, and hence the better the explainability of the outcome variable by the predictor variables, showing the strength of the association between the dependent and the independent variables (Ribeiro et al., 2021; Farhan & Nafi, 2022).

Finally, the remaining performance metrics mentioned in the literature are support, classification time, training time, energy balance mismatch, cost of an undetected attack, inspection cost or normalized labour cost, average bill increase, anomaly coverage index, minimum detected variation, decrease in stolen electricity, and the RTU cost metrics. These performance metrics (Messinis & Hatziargyriou, 2018:253; Saeed et al., 2020:7) are described below:

(a) **Support:** In a rule-based system, support is illustrated as the sample counts upon which a rule has been applied when compared with the total number of representative data samples. It is the number of instances that are currently being considered out of the total available instances.

(b) **Classification time:** Is the time it takes an NTLD model to categorize or classify the given input data samples.

(c) **Training time:** It is the time taken to groom an NTL model before it is able to learn.

(d) **Energy balance mismatch:** Energy balance mismatch is the difference between the supplied by the energy distribution companies and the energy consumed by electricity customers.

(e) **Cost associated with undetected attack:** It is the cost connected with the impact of the worst-possible attack on the utility infrastructure.

(f) **Inspection cost or normalized labour cost:** It is the amount incurred during the inspection of electricity consumers that have been classified or predicted as fraudulent by the NTLD system.

(g) **Average bill increase:** Average bill increase is referred to as the general increase in the electricity bill of every customer due to the revenue deficits incurred by the electric utilities owing to ET.

(h) **Anomaly coverage index:** It is the ratio of the electricity thieves detected by RTUs to the total number of consumers stealing electricity.

(i) **Minimum detected variation:** Is the least possible deviation detected from a specific load profile.

(j) **Decrease in stolen electricity:** It is the drop in the electricity siphoned from the grid after the application of a particular NTLD model.

(k) **RTU cost:** This is the amount spent or incurred on acquiring and installing RTUs.

All the performance metrics mentioned should not be confused with ‘response time’, which is not an evaluation metric, but the time it takes an NTLD system to determine if an electricity customer commits theft. Response time is the time taken by the utilities to obtain the input data, which serves as input to NTLD models during ML simulations, and not the time taken for NTL algorithms to produce prediction results based on the input data (Messinis & Hatziargyriou, 2018:252, 254-257, 264-265).

2.5.3.2 Classification of non-hardware solutions

Non-hardware NTLD solutions make use of algorithms in detecting NTL. Algorithms are procedures or step-by-step methods used for NTLD in the power system (Messinis & Hatziargyriou, 2018:252, 259). NTLD algorithms form the core of the methods used for non-hardware NTLDs. Different algorithms that make up NTL models use grid data in different ways to detect NTL in the power system. To further analyse the non-hardware-based solution approach, the method is classified into three types namely: data oriented, network oriented, and the hybrid methods (Messinis & Hatziargyriou, 2018:251-252, 259; Saeed et al., 2020:8-9; Guarda et al., 2023:4-5) as shown in Figure 2.21.

❖ **Data-oriented methods**

Data-oriented, data-based, or data-driven methods for NTLD are basically the application of ML methods and data analytics (Messinis & Hatziargyriou, 2018:259; Saeed et al., 2020:9; Nayak & Jaidhar, 2023:2) on electricity consumption profiles or readings and sometimes additional data (Viegas et al., 2017:1263; Ghori et al., 2020:16035, 16037), to detect ET and eventually shortlist ET suspects for manual onsite inspections (Glauner et al., 2017:761; Messinis & Hatziargyriou, 2018:259). The advent of SG has greatly enhanced the application of data-oriented methods for ETD, owing to the huge amounts of data produced through the AMI of the intelligent grid, by employing AI-based machine learning (ML) and deep learning (DL) techniques (Gu et al., 2022:4568; Liao, Zhu, et al., 2024:5075; S. Zhu et al., 2024:15477). Data-based NTL solutions are more comprehensive, resilient, and efficient (Bai et al., 2023:2).

Some examples of additional data are temperature, environmental or geographical data, and customer information like type of house, contract type, etc., which are at times combined with the consumption data to improve NTL predictions (Viegas et al., 2017:1263; Ghori et al., 2020:16035, 16037). Some seventy-one different types of features that include consumption and additional data with their priorities and importance as determined based on F-measure are mentioned and listed in Ghori et al. (2020:16041-16041, 16045), while a couple of some other features are also mentioned in Poudel and Dhungana (2022:112) and Guarda et al. (2023:19). However, majority of data-based NTL models only make use of the energy consumption data or load data as the input data in NTL models for ETDs (Viegas et al., 2017:1263). Also, most data-oriented methods employ supervised-learning methods owing to their superior performances in terms of ETD or NTLD (Messinis & Hatziargyriou, 2018:262; Saeed et al., 2020:16; Fei et al., 2022:1, 7; Guarda et al., 2023:21; Liao, Zhu, et al., 2024:5075).

AI-based methods for the detection of ET is commonly referred to as the classification of the load data/profile or consumption profile of electricity consumers by training NTL models with the annotated data of benign or honest and malignant or fraudulent customers obtained during onsite inspections, to determine irregular consumption patterns in the load profile (Fragkioudaki et al., 2016:51). The consumption profile contains the consumption records or meter readings of the electricity customers taken hourly, daily, or monthly (Ghori et al., 2020:16035). Data-oriented methods particularly employs the use of consumer level time-series data and consumer level static data for NTLD as shown in Figure 2.22 (Messinis & Hatziargyriou, 2018:253, 258). These data are usually smart metering data of large volumes and less variety, with either medium or low resolutions for making generalized predictions (Messinis & Hatziargyriou, 2018:264). With data-oriented methods, existing infrastructure of utilities is made use of, as data-driven techniques do not require the purchase of additional equipment for the periodic gathering of voluminous data and/or labelling of the data (Messinis & Hatziargyriou, 2018:264; Osypova, 2020:45).

The various types of data-driven algorithms used for the detection of NTL by employing customers' consumption profiles fall under supervised learning, unsupervised learning, hybrid learning and semi-supervised learning (Ghori et al., 2020:16035), using AI-based ML methods (Bai et al., 2023:2). These learnings under the data-oriented method are premised on AI methods (Messinis & Hatziargyriou, 2018:259-260). The use of customers' electricity consumption data and applying the AI-based ML approach is the state-of-the-art and the most-effective approach in ETD (Glauner et al., 2017:761; Glauner, 2019:31, 110; Ghori et al., 2020:16033-16034; Saeed et al., 2020:1; Guarda et al., 2023:4; Stracqualursi et al., 2023:12, 16; Coma-Puig et al., 2024:2704). The common ML procedures used for supervised and unsupervised learnings (Messinis & Hatziargyriou, 2018:259) while deploying the consumption data of electricity customers are depicted in the flowchart shown in Figure 2.23.

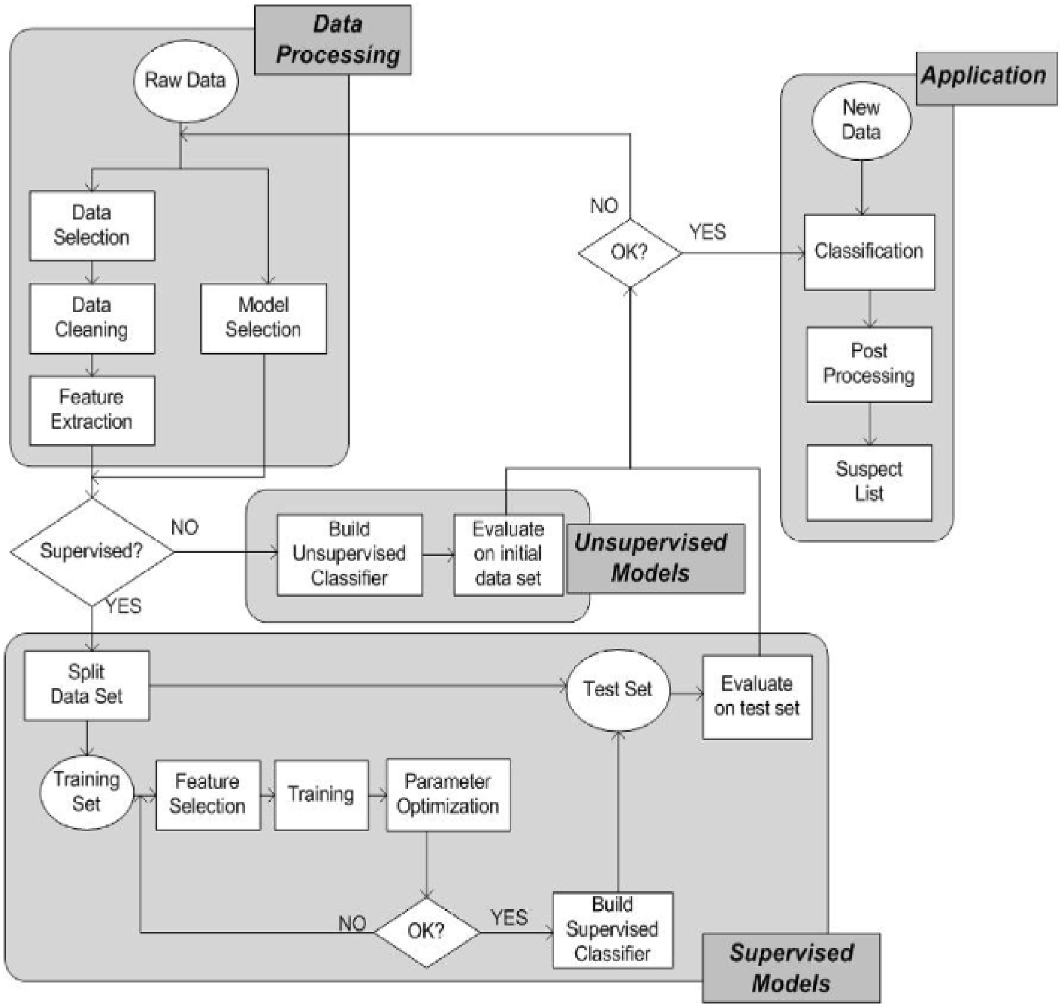


Figure 2.23: Procedures for supervised and unsupervised learnings

(Messinis & Hatziargyriou, 2018:260)

For the supervised and unsupervised learning procedures shown in Figure 2.23, the raw data is first processed, and a model for data analytics and prediction is selected. The data is processed by cleaning it and extracting the features in it. The selected model is then used for NTL prediction. During the modelling, supervised learning is used if the data is labelled, while unsupervised learning or method is used if the data is unlabelled. The quality and variety of the data employed would determine the type of algorithms or models to be used to analyse the data. For supervised methods, the input dataset is divided into training and test sets. Training sets from input data are used to tutor the model, so that the model could be able to infer meaningful patterns from the data. To verify the operation of the model and its performance, a new set of data (test set) from the samples in the dataset are used, and a suspect list is generated for customers who have the probability or propensity of engaging in ET (Messinis & Hatziargyriou, 2018:259).

- **Supervised learning**

Supervised learning is the most common and one of the widely used types of ML owing to its impressive performance (LeCun et al., 2015:436; El Bouchefry & de Souza, 2020:227; Muhammad et al., 2020:2; Hanif et al., 2021:14). Supervised learning methods for ETD or NTLD make use of positive and negative labels from the consumption profiles of consumers to train ML classifiers, such that different patterns are learnt from given historical datasets of energy consumptions (Saeed et al., 2020:9; Guarda et al., 2023:5, 21; Liao, Zhu, et al., 2024:5075). The samples that are labelled as positives are the energy consumptions of those malignant customers who steal electricity, while the negative samples represent the benign customers who do not steal electricity (Messinis & Hatziargyriou, 2018:251). In supervised learning, the labels on the datasets are the correct answers or the expected outcomes which are used for training ETD or NTLD models to accustom them to what is already being anticipated from them, and to determine the efficiency of the models in predicting ET after testing with new or test data samples (Osypova, 2020:41; Saeed et al., 2020:9).

The main demerits connected to supervised learning is the imbalanced nature of real-world datasets and the issue of data labelling or annotation which limits its usage if the expected labels are not available (Saeed et al., 2020:9; Liao, Bak-Jensen, et al., 2024). Examples of supervised learning methods are support vector machine (SVM), optimum path forest OPF), decision tree (DT), Bayesian classifiers, artificial neural network (ANN), k-nearest neighbours (KNN), rule induction methods, and generalized additive model (GAM) (Messinis & Hatziargyriou, 2018:260-261; Saeed et al., 2020::9-11; Guarda et al., 2023:5-11).

i. Support vector machine

SVM models have been frequently used as binary classifiers in NTLD problems owing to their resilience and immunity to imbalance datasets (Messinis & Hatziargyriou, 2018:260; Saeed et al., 2020:9; Guarda et al., 2023:6). SVM models use hyperplane in a high multidimensional space to maximally classify classes by drawing a wide boundary between support vectors (Pamir, Javaid, Qasim, et al., 2022:56871). SVM models have been deemed to be trusted in detecting NTL in a lot of literature, but may as well be time consuming and difficult to tune (Messinis & Hatziargyriou, 2018:260). SVM methodologies like one-class SVM (OC-SVM) and cost-sensitive SVM (CS-SVM) have been used in various SVM implementations. OC-SVM model is used for anomaly or outlier detections in an unsupervised manner because sample dataset used for its implementation is single-class (usually negative class or honest customers who do not steal electricity) labelled dataset (Messinis & Hatziargyriou, 2018:260; Saeed et al., 2020:9).

With CS-SVM, different weight values like high cost are added to classes owing to misclassifications or classification errors of different types caused mainly by minority classes to improve performance (Messinis & Hatziargyriou, 2018:260; Guarda et al., 2023:6). An example of this is the assignment of high cost to the misclassifications of minority classes in datasets to yield higher performances (Messinis & Hatziargyriou, 2018:260). Other types of SVM are linear kernel SVM (LK-SVM) and radial basis function kernel SVM (RBFK-SVM) (Messinis & Hatziargyriou, 2018:260; Saeed et al., 2020:10; Guarda et al., 2023:6). Between LK-SVM and RBFK-SVM, RBFK-SVM is more commonly used (Messinis & Hatziargyriou, 2018:260). Cost and gamma parameters are tuned for RBFK-SVM, while only cost parameter is tuned for LK-SVM. SVM could be combined with fuzzy interference system (FIS), DT, neural networks and other models to improve its performance (Messinis & Hatziargyriou, 2018:260; Saeed et al., 2020:10; Guarda et al., 2023:6).

Nagi et al. (2010) develops SVM model for ETD. Energy consumption data of customers and additional data are used to identify the irregular patterns in the electricity consumptions of the customers. These irregular patterns are highly correlated with NTL in the power grids. The energy consumption data employed was taken from three cities in Malaysia. The historical energy consumption profile of 265, 870 customers taken over 25 months were considered for the NTL simulations. The SVM model classifies the consumption data by separating the normal customers and the fraudulent customers. The model uses binary classification to try to determine sudden changes in the energy consumption data by using data mining and statistical analysis. Classification is done by finding the optimal decision function $\mathrm{f(x)}$ using the SVM classifier model in Equation 2.37. Equation 2.37 classifies test data into two classes and minimizes classification error as much as possible. The term $\mathrm{g\ (x)}$ is the decision boundary or hyperplane between the two classes of normal and fraudulent customers. The term $\mathrm{f(x)}$ minimizes classification error and improve model generalization by following the principle of structural risk minimization (SRM), as expressed in Equation 2.38 (Nagi et al., 2010:1163; Jiang et al., 2014:110; Ghori et al., 2023:15335).

$$\mathrm{f(x)} = \mathrm{sgn}\big(g(x)\big) \tag{2.37}$$

$$R < \frac{t}{n} + \sqrt{\frac{h\left(\ln\left(\frac{2n}{h}\right)+1\right)-\ln\left(\frac{\eta}{4}\right)}{n}} \tag{2.38}$$

In Equation 2.38, R is the expected error, classification-error expectation, or test-sample prediction error, t illustrates the number of training errors or errors from the training samples, n is the number of training samples, h is the dimension of the SVM set of hyperplanes, while η is a confidence measure (Nagi et al., 2010:1163; Jiang et al., 2014:110; Ghori et al., 2023:15335). The features used for the NTLD by Nagi et al. (2010) are the energy consumption data of each customer which corresponds to 24-hour daily average values of their energy consumptions, and the additional data known as the credit worthiness rating (CWR) which is automatically produced by the utility billing system for every customer who falter in paying their bills. The data were preprocessed and then later used to train and validate the SVM model. The SVM model achieved a tremendous hit rate increase from 3% to 60%. The SVM model The hit-rate increase of 57% was achieved when compared with the previous hit rate accomplished by the Tenaga Nasional Berhad electric distribution company in Peninsular Malaysia during onsite inspections.

The work of Nagi et al. (2010) reviewed above was extended and enhanced by Nagi et al. (2011), as the previous hit rate of 60% was increased to 72% by the improved model. This feat was achieved by introducing the IF-THEN rules form of FIS that involves the inclusion of human expert knowledge into the former SVM model that achieved a hit rate of 60%. The FIS produce an output that ranges from 0 and 1 for each customer. Those customers who have 0.5 outputs or higher are deemed to have higher propensity of being fraudulent.

While Nagi et al. (2010) and Nagi et al. (2011) contribute valuable insights into NTLD using SVMs and fuzzy logic, they have several limitations. The lack of comparative benchmarking, inadequate evaluation metrics, scalability concerns, and failure to address cost-sensitive learning reduce the practicality of their proposed methods.

ii. Optimum path forest

OPF conquers the challenge that AI methods require high computational overhead while training ETD models (Guarda et al., 2023:9). OPF algorithm is an algorithm that is based on graphs, and may be used for clustering or classification, but it is commonly used for classification (Messinis & Hatziargyriou, 2018:260; Saeed et al., 2020:10; Poudel & Dhungana, 2022:113). Unlike SVM and other models that uses hyperplane to distinguish two classes, the OPF algorithm does not separate two classes by finding an optimal hyperplane, but each annotated sample in a training set is regarded as a graph node that has its coordinates as its feature values (Messinis & Hatziargyriou, 2018:260).

The target of OPF is such that the graph is partitioned into two or more optimal-path trees, whereby each tree represents a class (Messinis & Hatziargyriou, 2018:260; Saeed et al., 2020:10). Each tree is attached to its prototype where it is rooted (Messinis & Hatziargyriou, 2018:260). Prototype is the root of the optimum-path trees, whereby the classification of each node is dependent on the node-prototype connection strength, resulting in optimal feature-space partitioning (Messinis & Hatziargyriou, 2018:260; Saeed et al., 2020:10; Guarda et al., 2023:9). The grouping of these trees which are connected to their various prototypes is referred to as the OPF classifier (Messinis & Hatziargyriou, 2018:260; Saeed et al., 2020:10).

Classification with OPF is interpreted as the combination of the computations of optimal-path trees or nodes based on prototypes (Guarda et al., 2023:9). During model validation, new samples being tested are assigned the labels of the prototype where they are eventually rooted, in accordance with a cost function (Messinis & Hatziargyriou, 2018:260; Saeed et al., 2020:10). OPF classifies are parameter-free and take a lower time in its training phase to train the model with train samples even with overlapped classes; hence it is well appropriate for online training of ETD system (Messinis & Hatziargyriou, 2018:260; Saeed et al., 2020:10; Guarda et al., 2023:9). OPF algorithm employs path-cost function to optimally group samples with similar characteristics (Guarda et al., 2023:9).

The authors in Ramos et al. (2011) were interested in the regions that exist between classes (overlapped regions), and addressed the path-cost function (f_{max}) for the region using Equation 2.39.

$$f_{max}(\langle s\rangle) = \begin{cases} 0, \ if \ s \in S \\ +\infty, \ otherwise \end{cases} \qquad \textbf{(2.39)}$$

$$f_{max}(\pi\langle s,t\rangle) = \max\{f_{max}(\pi), d(s,t)\}$$

Considering the neighbouring samples in π when the path of π is not trivial, the function of the path cost $f_{max}(\pi)$ in Equation 2.39 calculates the greatest distance between the adjoining samples. Whereas $d(s,t)$ represents the distance between s and t along path π. One optimum path $P^*(s)$ is assigned by the OPF algorithm from S to each sample $s \in Z_1$, to form an optimum path forest P. The optimum path forest P is a function with no cycles which assigns a marker nil or its predecessor $P(s)$ in $P^*(s)$ to every $s \in Z_1 \backslash S$ when $s \in S$. It should be noted that the train, validation, and test sets are represented as Z_1, Z_2, and Z_3. Classification is done by evaluating the optimum cost function $C(t)$ shown in Equation 2.40.

$$C(t) \ = \min\{\max\{C(s), d(s,t)\}\}, \forall s \in Z_1 \qquad \textbf{(2.40)}$$

The authors in Ramos et al. (2011) introduce an innovative application of the OPF classifier for NTLD. However, the lack of comparative benchmarking, insufficient feature analysis, imbalanced data handling, and real-world scalability concerns limit the practical impact of their findings.

iii. Decision tree

The OPF algorithm mentioned previously classifies in graph-like manner, while DT algorithm classifies its set of rules in a flowchart-like or tree-like manner when predicting new samples (Saeed et al., 2020:11; Guarda et al., 2023:9). The sets of rules of DT, which are determined by the input-output attributes relationships in data, allow for better understanding of NTL characteristics, where the algorithm split dataset into several tree-like branches according to the rules of decision (Messinis & Hatziargyriou, 2018:261; Guarda et al., 2023:9). The rules of DT algorithm has been combined with experts' rules and other classifiers to form ensemble methods (Messinis & Hatziargyriou, 2018:261). DT is able to handle non-linearity in data better than linear models, but it is sensitive to the problem of class imbalance in datasets (Messinis & Hatziargyriou, 2018:261; Saeed et al., 2020:11; Guarda et al., 2023:9).

DT is used for classification and regression problems (Saeed et al., 2020:11). DT types like C4.5, C5.0, CART, QUEST, EBT, ID3, and QUEST have been used in the literature to solve NTL-related problems (Messinis & Hatziargyriou, 2018:261; Saeed et al., 2020:11; Guarda et al., 2023:10). Divide-and-conquer methods are used to construct DT tree-based models to uncover the optimal points where the tree splits (B. Gupta et al., 2017:15; Dinov, 2018:157).

Recently a DT type known as M5P has been used by Cody et al. (2015). The M5P algorithm is a reconstruction of the M5 algorithm used in Quinlan (1992). M5P is a combination of DT and linear regression where the regression algorithm predicts future variables based on the already learned variables from data. The M5P algorithm learns the pattern of consumptions from the energy consumed by each consumer, and these learned patterns are then used to predict future patterns of energy consumptions (Guarda et al., 2023:10).

Both Quinlan (1992) and Cody et al. (2015) contribute to DT-based learning, however, Quinlan's (1992) study lacks modern evaluation metrics and comparisons with other regression models, while the work of Cody et al. (2015) did not explore alternative models, imbalanced data handling, or real-world deployment challenges.

iv. Bayesian classifiers

Bayesian classifiers are used to detect ET, NTL or intrusions in a network (Gu et al., 2022:4571). Classification using Naïve Bayes classifiers are probabilistic and require the knowledge of NTL probability which may have been previously acquired from huge national statistical energy information repository, to predict events to come (Messinis & Hatziargyriou, 2018:261; Saeed et al., 2020:11). The principle upon which this classifier operates is such that, the different features of a class could be estimated using the non-intrusive load monitoring (NILM) technique if the class of such sample is already known or determined (Guarda et al., 2023:11).

With NILM, the probability of each of the appliances used per consumer in a building and their respective probable energy consumptions learnt through the consumption pattern of every load device used by the electricity consumer are predicted in a bid to determine NTL (Saeed et al., 2020:11; Guarda et al., 2023:11). The NILM calculates the possibility of ET using NTL probability from the previously acquired information when a new device or sample is introduced (Messinis & Hatziargyriou, 2018:261; Saeed et al., 2020:11). Bayesian probability (i.e., joint probability) is a probability which conveys some set of variables graphically. The Bayesian probability is a kind of Bayesian classifier which is also known as Bayesian network (Messinis & Hatziargyriou, 2018:261).

The authors in Massaferro et al. (2020) proposed a Bayesian risk framework to detect NTL, in order to increase the income and profits of the Uruguayan electric utility, to restore its economic stability. The framework which is about obtaining the optimal subset $\widehat{X}_m$, such that $\widehat{X}_m = \{x_{i1}, \dots , x_{im}\}$, is represented by Equation 2.41, while the cost-sensitive classification loss of the framework is shown in Equation 2.42.

$$\hat{X}_m = arg\ max_{\hat{X}_m}\{\sum_{k=1}^{m} a_{ik}P(y_{ik} = 1|x_{ik}) - \sum_{k=1}^{m} c_{ik}\} \quad \textbf{(2.41)}$$

$$L(x,q) = \sum_k P(y = k|x)\mu_{qk} \quad \textbf{(2.42)}$$

The framework to optimize the revenues of the Uruguayan electric utility as proposed by Massaferro et al. (2020) is expressed in Equation 2.41; where m represents the number of inspections that the utility needs to perform, while $X_m \subset X$ represents the random subset of m samples of X. The term $P(y_i = 1|x_i)$ in the equation represents the probability that the given sample x_i is causing NTL. The monetary amount which an ith electricity customer could be siphoning from the utility owing to theft is represented by a_i, while the amount it costs the utility to inspect the ith customer is denoted by c_i. The μ_{qk} in Equation 2.42 is the cost associated with the misclassification or misprediction of a member of class k as that of class q. Experimental results have shown that the proposed NTLD method is proficient in returning the economic status quo of the electric utility.

Massaferro et al. (2020) contribute to cost-aware fraud detection but have several limitations. The study lacks generalizability, does not benchmark against other cost-sensitive methods, and overlooks key issues like model adaptability and real-world deployment challenges.

v. Artificial neural network

ANN or simply ‘neural network’ is a branch or a subcategory of ML which basically consists of three layers called input, hidden, and output layers, for the recognition or classification of patterns (Guarda et al., 2023:7). ANN can be used for forecasting energy consumptions in time series, and also for binary classifications (Saeed et al., 2020:10; Guarda et al., 2023:7). The difference or deviation between the forecasted or predicted energy consumptions and the actual or measured values of energy consumptions can be used for detecting frauds or NTL in the power grids (Messinis & Hatziargyriou, 2018:260; Saeed et al., 2020:10; Guarda et al., 2023:7). Backpropagation (BP) trained Multilayer perceptron (MLP) which is jointly termed BP-MLP is the most common type of ANN used as binary classifier for detecting NTL in distribution grids (Messinis & Hatziargyriou, 2018:260; Saeed et al., 2020:10). The cross validation process is used in ANN to ensure that the trained model generalizes well after using trial and error method to determine the optimal network structure of the model (Messinis & Hatziargyriou, 2018:260; Poudel & Dhungana, 2022:113).

Zheng et al. (2018) used wide and deep convolutional neural network (WDCNN) for ETD. The wide component of the model captures the global features of one-dimensional energy consumption data, while the deep component of the model captures the periodicity of normal electricity consumption, and also captures accurately the non-periodicity energy consumptions attributable to ET based on two-dimensional energy consumption data. Most of the previous works on ETDs were based on one-dimensional energy consumption data. The missing values in the energy consumption data used in the work are replaced by the linear interpolation method shown in Equation 2.43.

$$f(x) = \begin{cases} \frac{x_{i-1}+x_{i+1}}{2}, \; x_i \in NAN, x_{i-1} \; or \; x_{i+1} \notin NaN \\ 0, \; x_i \notin NAN, x_{i-1} \; or \; x_{i+1} \in NaN \\ x_i, \; x_i \notin NaN \end{cases} \tag{2.43}$$

Where x_i is the unit of the energy consumed over a period of time and it is represented as NaN when it is null, undefined, or missing. NaN stands for “Not a Number”. After the missing values have been replaced, the energy-consumption dataset is then normalized by setting the range of the features to values between 0 and 1 using the min-max scaling method as expressed in Equation 2.44.

$$f(x_i) = \frac{x_i - \min(x)}{\max(x) - \min(x)} \tag{2.44}$$

Where $\min(x)$ is the minimum value of the energy consumptions in x, and $\max(x)$ is the maximum value of the energy consumptions in x. Each neuron or node of the fully-connected convolutional neural network (CNN) layers calculates its own score as shown by Equation 2.45 using the one-dimensional energy consumption data.

$$y_j \coloneqq \sum_{i=1}^{n} w_{i,j} x_i + b_1 \tag{2.45}$$

From Equation 2.45, y_j is the output of the jth neuron in the fully connected layer, n is the length of the input data x which is a one-dimensional data, $w_{i,j}$ is the weight of the neuron between the input value ith and the jth neuron, while b_1 is the bias term of the neuron. After the calculation in Equation 2.45, the neuron will send the calculated value to the connected nodes in the higher layer of the network after applying Rectified Linear Unit (ReLU) activation shown in Equation 2.46, to determine how much the previous node contributed to the prediction of the next step in the network.

$$u_j \coloneqq f(y_j) = \max(0, y_j) \tag{2.46}$$

The output after calculating activation function is denoted by u_j. After the activation-function calculations, the Deep CNN processes the one-dimensional energy consumption data into a two-dimensional format according to weeks, to improve the performance of the traditional ANN. One-dimensional data could also be converted to two-dimensional format according to convinient number of days, but transforming it to two-dimensional data according to weeks has produced the best performance.

The work of Buzau et al. (2020) is an improvement on the work of Zheng et al. (2018) and other deep learning models and prominent classifiers in terms of performances. Buzau et al. (2020) have used the combination of long short-term memory (LSTM) with MLP to enhance the performance of ANN. The LSTM analyzes the consumption history of the raw data while MLP integrates the non-sequential data. LSTM uses sigmoid and hyperbolic tangent (tanh) for non-linear activations, as expressed in Equations 2.47 to 2.51.

$$i_t = \sigma(W_i x_t + U_i h_{t-1} + b_i) \tag{2.47}$$

$$f_t = \sigma(W_f x_t + U_f h_{t-1} + b_f) \tag{2.48}$$

$$o_t = \sigma(W_o x_i + U_o h_{t-1} + b_o) \tag{2.49}$$

$$C_t = f(t) \odot C_{t-1} + i_t \odot \tanh(W_c x_t + U_c h_{t-1} + b_c) \tag{2.50}$$

$$h_t = o_t \odot \tanh(C_t) \tag{2.51}$$

Where i_t represents the input gate activation, f_t represents the forget gate activation, o_t represents the output gate activation, C_t represents the cell state activation, h_t illustrates the hidden-state activation at time-step t, while h_{t-1} denotes the hidden-state activation at the previous time-step t. W_i, W_f, W_o, and W_c depict the weights of the input layer. U_i, U_f, U_o, and U_c denote the recurrent weights of LSTM, while b_i, b_f, b_o, b_c are the biases of the LSTM neural network. The x_t vector represents the input feature the time-step t.

$$z_n = W_n h_{n-1} + b_n \qquad \textbf{(2.52)}$$

In the MLP network, N which is chosen based on the validation dataset is the number of hidden layers, while every hidden layer goes through an affine transformation as expressed in Equation 2.52. The choice of N is based on the validation dataset. W_n represents weights of the n_{th} layer of the MLP network, h_{n-1} depicts the hidden state of the preceding layer, while b_n denotes the bias of the layer n of the network. For the model evaluation, the logarithmic loss function or the binary cross entropy function shown in Equation 2.53 is used to evaluate the performance of the model.

$$L = -\frac{1}{M}\sum_{i=1}^{M} -\left(y_i \log\left(P_{NTL}^{i}\right) + (1 - y_i)\log\left(1 - P_{NTL}^{i}\right)\right) \qquad \textbf{(2.53)}$$

The term M in Equation 2.53 represents the available number of customer samples, y_i represents the ground-truth or actual-class label. The computed NTL probability for the sample i of the customer using the hybrid LSTM-MLP model is represented by P_{NTL}^{i}.

Although, Zheng et al. (2018) and Buzau et al. (2020) demonstrate the effectiveness of DL models (CNN, LSTM) for ETD**,** their approaches face computational complexity, interpretability, real-time deployment considerations, and generalizability challenges.

vi. K-nearest neighbours

KNN algorithm is one of the simplest supervised ML models which uses proximity of nearest neigbours for classification and regression to detect NTL (Messinis & Hatziargyriou, 2018:261; Saeed et al., 2020:11). KNN algorithm calculates the lowest Euclidean distance between all the k-training features or new features (test data) to determine the k-training features or k-nearest neighbours and then select the class that has the highest k-nearest neighbours (majority vote) as the correct class for the test data (Messinis & Hatziargyriou, 2018:261; Ghori et al., 2020:16039). The mean values of the k-nearest neighbours is the predicted value for the test data when regression is being considered.

Pedramnia and Shojaei (2020) proposed a method that detects the injection of false data into phasor measurement units (PMUs) in SG, using a variant of the traditional KNN called decomposed k-nearest neighbours (DKNN) algorithm. These attacks on PMUs are called false data injection (FDI) attacks, which is a very critical attack in SGs. Datasets from multiple PMUs are saved in the phasor data concentrator (PDC) at the utility control centres.

DKNN is an improvement on the conventional KNN algorithm which decomposes datasets into smaller subspaces, in a bid to enhance scalability, accuracy, and efficiency. The proposed DKNN method is used by the authors on PMU measurements and tested on IEEE 14-bus system. The authors used complex optimization method in the DKNN algorithm to extract and categorize PMU data features, reduce the distances between intraclass and interclass neighbours, enhance computational efficiency by helping to reduce the time complexity associated with feature extraction and classification, and minimize errors in classification. The DKNN algorithm classifies the PMU dataset based on KNN-centroid distances after considering k-nearest neighbours from each class. The results obtained are satisfactory as the DKNN algorithm outperforms other ML algorithms used for the detection of false data injected into PMUs at utility control centres.

The authors in Pedramnia and Shojaei (2020) have made a valuable contribution to FDI detection in SGs, however, their approach is limited to cyber anomalies and overlooks physical tampering and consumption-based theft detection. A hybrid approach combining cyber anomaly detection, ML-based consumption pattern analysis, and physical tampering detection would offer a more robust NTLD solution, especially in regions where electricity thieves apply diverse theft techniques. Also, the lack of generalizability, imbalanced-data handling, scalability concerns, and absence of comparative benchmarking limit the practical applicability of this approach.

Aziz et al. (2020) also applied KNN algorithm to detect ET in electricity consumption dataset collected from AMI in SG. The authors used interpolation method to restore the missing values in the dataset, empirical mode decomposition (EMD) to break down the extracted features into intrinsic mode functions (IMFs), and adaptive synthetic (ADASYN) sampling algorithm to balance the two unequal classes in the dataset. After extracting features from the dataset, thirteen best features which give maximum classification accuracy have been chosen by the authors for the ETD experiment. The authors deployed traditional KNN variants like Fine KNN, Medium KNN, Coarse KNN, and Cosine KNN, including other ML algorithms like Fine Tree, Medium Tree, Coarse Tree, logistic regression and linear discriminant to classify the honest and fraudulent electricity customers in the employed dataset. Of all the algorithms used in the experiment, Fine KNN produced the best prediction results with classification accuracy of 91.0%.

While Aziz et al. (2020) introduce an innovative EMD-based feature extraction approach for ETD**,** the reliance of this method on KNN and offline processing limits its scalability and real-time applicability. The authors can investigate online version of EMD, and also test the method using large, diverse real-world SM datasets. The authors could evaluate alternative feature extraction methods like CNN-based methods for improved efficiency.

vii. Rule induction methods

Rule induction methods use algorithms to automatically extract set of rules in the form of “IF-THEN-ELSE” statements hidden in training data, to classify or predict the class of a new given sample or test data, in a bid to detect NTL or fraud (Nettleton, 2014:99; Messinis & Hatziargyriou, 2018:261; Saeed et al., 2020:10). This method is usually used with labelled datasets (Saeed et al., 2020:10). In the field of AI, rule induction methods are closely related to expert systems, in that, rule induction methods could be used as a tool to automatically refine or generate rules within the framework of expert systems, but in actual fact, both methods serve different purposes. Rule induction methods belong to the category of supervised learning, while expert systems belong to the category of unsupervised learning. Rule induction methods are driven by data, and involves the extraction of rules and patterns from labelled data; while expert systems are driven by human knowledge based on expertise (Saeed et al., 2020:10; Messinis & Hatziargyriou, 2018:261).

viii. Generalized additive model

The inspiration for the use of GAM model for NTL reductions came from the field of epidemiology in medicine (Messinis & Hatziargyriou, 2018:261). GAM has been used in the field of NTL to model the spatial distribution of NTL, because it is presumed that NTL the in a domain spread epidemiologically in accordance with technical and social characteristics (Messinis & Hatziargyriou, 2018:261; Saeed et al., 2020:8). The probability of NTL in an area is estimated with GAM, based on the influence of the social and technical characteristics, using Markov chain to model how the NTL may spread in the future within a given area (Faria et al., 2016:362, 364; Messinis & Hatziargyriou, 2018:261). Although, GAM algorithm does not detect NTL or fraud, but evaluates the probability or likelihood of NTL by spatial distribution (Messinis & Hatziargyriou, 2018:261).

- **Unsupervised learning**

Unsupervised learning models do not make use of labels at all in the data profiles provided to train classifiers for NTLDs or predictions (Messinis & Hatziargyriou, 2018:251; Osypova, 2020:37; Saeed et al., 2020:11; Guarda et al., 2023:11). With unsupervised learning, the relationships and patterns in a dataset are learned without any prior knowledge about the dataset or with the datasets that are being partially labelled. Unsupervised learning can also be used with methods that uses a single label, or when the labelled samples of those customers that steal electricity are very small when compared with the large numbers of labelled representative samples of those customers who did not steal electricity (Messinis & Hatziargyriou, 2018:251-252, 260, 262). The detection accuracies of supervised learning models are better than those of unsupervised learning models because supervised learning models already have deep knowledge of the datasets via their labels prior to modelling (Messinis & Hatziargyriou, 2018:262; Saeed et al., 2020:16; Liao, Zhu, et al., 2024:5075). Examples of unsupervised learning methods are self-organizing map (SOM), outlier detection methods, regression models, expert systems, clustering algorithms, statistical methods, game-theoretic methods (Messinis & Hatziargyriou, 2018:261-262; Saeed et al., 2020:12-13; Guarda et al., 2023:11-15).

i. Self-organizing map

SOM is an exclusive kind of neural network which works on training and mapping modes in an unsupervised manner (Messinis & Hatziargyriou, 2018:261; Poudel & Dhungana, 2022:114). In the training mode, the map is built using datasets while in the mapping mode, new data samples are classified automatically (Poudel & Dhungana, 2022:114). The SOM algorithm does dimensionality reduction to produce a low-dimensional equivalence of a high-dimensional data in order to convey the network distribution in a graphical map and detect features using unsupervised learning, while the topology of the original data (high-dimensional data) is still being retained (Sacco et al., 2017:68; Messinis & Hatziargyriou, 2018:261; Misra et al., 2020:146). Similar samples are mapped together using SOM (Sacco et al., 2017:68) to produce an output that depict whether NTL have occurred or not (Messinis & Hatziargyriou, 2018:261).

In Cabral et al. (2008), the authors applied SOM to detect ET among high-voltage (HV) consumers by comparing the historical energy consumption data with the present data obtained from an electric distribution company in Brazil. The energy consumption data is aggregated into weekly consumptions. Out of the 156 customers selected for ETD simulation, 30% of the customers were suspected of causing NTL by the SOM-based ETD system. Guerrero et al. (2018) developed a framework of two modules to increase the success rate of onsite inspections in the premises of electricity customers. The first module was based on text mining and ANN to filter electric customers, while the second module involved a data mining process that contained classification and regression tree (C&R), and SOM neural network.

The work of Cabral et al. (2008) lacks generalization to LV consumers and real-time fraud detection, while that of Guerrero et al. (2018) over-relies on inspection-based detection. However, both studies lack real-time ML-based detection, scalability considerations, and fully automated fraud prediction techniques.

ii. Outlier detection methods

Outliers are features that differs significantly from regular features. The concept of outlier detection methods applied for ETD involve the identification of the unusual features that behave differently in a given dataset for the purpose of detecting NTL (Messinis & Hatziargyriou, 2018:262; Guarda et al., 2023:12).

Linear programming is being employed by Yip et al. (2018) to detect NTL using the concept of outlier detection. The method is able to identify NTL and locate defective SMs in SG, in an effort to reduce revenue losses. In this method, cumulative meter readings from consumers are compared with the total readings from the distribution transformers to shortlist areas that have high probability of ET. The quantity of the electricity stolen at the point of a SM is modelled as anomaly coefficient, where a non-zero value of the anomaly coefficient indicates ET or defect in metering equipment. The NTL method also detects intermittence in the theft of electricity or in the working of faulty metering equipment.

While the authors in Yip et al. (2018) introduce an anomaly detection framework for ET and defective meters, their reliance on unsupervised learning, historical data, and lack of interpretability limits its practical usage in large-scale SGs.

Fenza et al. (2019) have been able to address the issue of context and time awareness associated with anomaly detection, the concept of drift, as well as the issue of FPR that occurs based on the changes in energy consumption habits of electricity users. To fill the gaps mentioned by the authors, the authors have employed the Long short-time memory (LSTM) model to address stated issues. The LSTM model profiled and predicted the behaviour of consumers drawing from their energy consumptions in the recent past, and was able to detect outliers at a time instance close to real time.

Inasmuch as Fenza et al. (2019) introduce a valuable drift-aware anomaly detection model, its reliance on traditional feature extraction, lack of real-time processing, and absence of explainability mechanisms limit its practical deployment in large-scale SGs.

iii. Regression models

To predict NTL using time series data, regression models such as auto-regressive moving average (ARMA) and auto-regressive integrated moving average (ARIMA) have been utilized (Messinis & Hatziargyriou, 2018:262; Saeed et al., 2020:13). If regression method is trained with energy consumption data and the distinction between the measured energy consumed and the expected or estimated energy consumption is high, then a potential likelihood of NTL or fraud is suspected (Messinis & Hatziargyriou, 2018:262; Saeed et al., 2020:13; Guarda et al., 2023:13). However, ARIMA models have proven to perform better than ARMA (Messinis & Hatziargyriou, 2018:262; Saeed et al., 2020:13).

The authors in Yip, Tan, et al. (2017) used the Linear Regression-based Scheme for Detection of Energy Theft and Defective Smart Meters (LR-ETDM) model previously developed by Yip, Wong, et al. (2017), in conjunction with a new scheme in a SG environment. For a service area that is assumed to have N consumers, the readings of the SMs in the area are registered at the time stamp of $T = t_{1,}, t_2, \dots, t_{48}$. The proposed model is represented by Equation 2.54 where $p_{t_{i,n}}$ in the model is energy consumption by consumer n at the time interval $t_i \in T$ in near real-time. a_n denotes the anomaly coefficient of every consumer n, while y_{t_i} is the disparity in the readings of the meter at the time interval of $t_i \in T$. Equation 2.54 is formulated if there is over/under-reporting by SMs and the objective of the equation is to find the values of all a_n, where the values of $n = 1,2, \dots, N$; to evaluate the reliability of the consumers' SMs or the abnormal behaviours of the consumers.

$$a_1 p_{t_{i,1}} + a_2 p_{t_{i,2}} + \cdots + a_N p_{t_{i,N}} = y_{t_i}, \ \forall t_i \in T \qquad \textbf{(2.54)}$$

The sum of all the customers' energy consumptions must be in accord with the total load consumptions measured by the collector during the time interval t_i. Yip, Tan, et al. (2017) later developed the Categorical Variable-Enhanced Linear Regression-based scheme for Detection of Energy Theft and Defective Smart Meters (CVLR-ETDM) model because the LR-ETDM algorithm designed by Yip, Wong, et al. (2017) may not be able to detect all frauds, especially when consumers only commit theft during a specific period in a day. The CVLR-ETDM algorithm uses dummy coding which introduces categorical variables x_n into the linear regression to fix time-varying or dynamic ET problem. Equation 2.55 conveys the CVLR-ETDM scheme.

$$a_1 p_{t_{i,1}} + \cdots + a_N p_{t_{i,N}} + \beta_1 p_{t_{i,1}} x_1 + \cdots + \beta_N p_{t_{i,N}} x_N = y_{t_i}, \ \forall t_i \in T \tag{2.55}$$

Considering N consumers in a service area as in Equation 2.55, and each consumer n commits ET independently, then β_n and x_n parameters are defined where $n = 1,2, \dots, N$. β_n is the detection coefficient of consumer n during the on-peak hours, while x_n is the categorical variables depicting whether the period of ET is during on-peak or off-peak hours as shown in Equation 2.56.

$$x_n = \begin{cases} 0, \ off - peak \ hours \\ 1, \ on - peak \ hours \end{cases} \tag{2.56}$$

The period of ET and the period of metering defect can be determined from Equation 2.55 by solving for the values of a_n and β_n, to discover any anomalous behaviour from the consumers and/or their faulty meters at any time of the day. The values of a_n and that of $(a_n + \beta_n)$ from Equation 2.55 represent the coefficient of anomaly for consumer n during the low-demand (off-peak) and the high-demand (on-peak) periods respectively. Results from the proposed CVLR-ETDM model shows that it is capable of detecting power pilferers as well as locating their faulty meters regardless of their mode or period of stealing.

While Yip, Tan, et al. (2017) and Yip, Wong, et al. (2017) contribute valuable insights into ET and defective meter detection using linear regression, their reliance on basic statistical models, lack of feature engineering, and absence of real-time processing limit their effectiveness in large-scale SGs.

iv. Expert systems

The decision making abilities of human experts are enhanced by expert systems (Poudel & Dhungana, 2022:114). Expert systems refers to the rules that are defined by professionals like utility-domain experts or utility technicians in a bid to detect NTL (Messinis & Hatziargyriou, 2018:261; Saeed et al., 2020:12; Poudel & Dhungana, 2022:114). This method, which although does not require learning is considered unsupervised and allows domain experts to apply their professional experience or expertise into the process of detecting NTL by introducing rules that enhance the detection of frauds in the power grids (Messinis & Hatziargyriou, 2018:261; Guarda et al., 2023:12). Expert systems may also be applied in supervised learning approaches because various models or methods can accommodate professional expertise or expert knowledge (Saeed et al., 2020:12; Guarda et al., 2023:12).

In the field of AI, expert systems are closely related to rule induction methods because expert systems accommodate rule induction algorithms as a tool to automatically refine or generate rules within their frameworks, but in actual fact, both methods serve different purposes. Expert systems belong to the category of unsupervised learning, but rule induction methods belong to the category of supervised learning. Expert systems are driven by human knowledge and are processed by inference engine, to make decision and/or proffer solutions to problems; while rule induction methods, which are driven by data, involves the extraction of rules and patterns from labelled data (Saeed et al., 2020:10; Messinis & Hatziargyriou, 2018:261).

Integrated expert system (IES) has been used by León et al. (2011) to analyse all the information of electric customers using the dataset obtained from Spain's Endesa electric utility in a bid to detect electricity fraud. The IES includes modules like data mining, text mining, and rule-based expert system. Guerrero et al. (2014) implemented an expert-system rule where a consumer is recommended for ET inspection if the reactive energy consumed is greater than or equal to the active energy consumed.

The authors in León et al. (2011) and Guerrero et al. (2014) have introduced expert system-based NTLD methods, but their reliance on static rule-based models, lack of real-time detection, interpretability, and absence of scalable ML solutions limit their effectiveness in large SGs.

v. Clustering algorithms

Clustering algorithms are used to group unlabelled energy consumption data of different consumers with similar consumption patterns together in an unsupervised manner, to assemble consumers that behave identically for the purpose of NTLD (Messinis & Hatziargyriou, 2018:261; Poudel & Dhungana, 2022:114). Baseline power profiles can also be calculated using clustering algorithms, such that fraud is suspected if new sample significantly differs from the baseline samples (Messinis & Hatziargyriou, 2018:261; Saeed et al., 2020:12). Meanwhile, fraud may also be suspected by the distance between the new sample (Messinis & Hatziargyriou, 2018:261).

Angelos et al. (2011) has employed fuzzy c-means algorithm or fuzzy clustering where every new sample is associated with fraud, and then the most probable theft case is chosen by tuning the system according to the peculiar parameters of requirements. The clustering algorithm called Density-Based Spatial Clustering of Applications with Noise (DBSCAN) with the combination of PCA have also been proposed by Krishna et al. (2015). PCA has been applied on the high-dimensional energy consumption data obtained from SMs, where each consumer is visualized in a two-dimensional space. After this, the DBSCAN is then able to cluster samples efficiently by distinguishing normal consumers from anomalous consumers.

While Angelos et al. (2011) and Krishna et al. (2015) contribute valuable statistical and PCA-based approaches for ETD, but their reliance on traditional methods, lack of real-time processing, and limited scalability reduce their effectiveness in modern SGs.

Babu et al. (2013) used fuzzy c-means cluustering algorithm to cluster or categorize consumers into classes based on their patterns of electricity usage. The clustering algorithm achieved 80% hit rate when tested with 57 customers in a particular neigbourhood in India. Determination of customers who committed theft is dependent on the application of fuzzy membership function and cluster-centre distances. The cluster-centre distances are the Euclidean distances from the centre of clusters, which are standardized and arranged using unitary index score. The fraudulent customers are those customers that have the highest unitary-index score greater than a predefined threshold of 0.7. The fuzzy c-means algorithm used the following attributes to create a general pattern of consumption for each customer over a period of 6 months: average units of energy consumption per consumer, maximum units of energy consumption per consumer, standard deviation of energy consumption of each consumer, average energy consumption in a neighbourhood or residential area, and 6-month inspection remarks.

Although, Babu et al. (2013) provide a useful rule-based method for detecting ET, their reliance on static statistical techniques, lack of feature extraction, adaptability, and absence of real-time detection limit the effectiveness of their approach in large-scale SGs.

Sharma et al. (2017) applied DBSCAN clustering to separate unusual patterns in energy consumption datasets with local outlier factor (LOF) algorithm which is used to rank the unusual energy consumptions based on the densities of the neighbours. If LOF value is higher, it shows there a significant difference between the densities of the feature under consideration and its neighbours, hence revealing such point as being suspicious. Silhouette coefficient and Davies Bouldin index have been used to validate the method. LOF is the ratio of the density of a feature in a cluster to that of the density of its KNNs (Ghori et al., 2020:16035).

While the authors in Sharma et al. (2017) provide a useful statistical framework for detecting irregular electricity consumption, their reliance on traditional methods, lack of DL integration, and the absence of real-time detection limit the effectiveness of their approach in modern SGs. The authors did not evaluate the scalability and generalizability of the model.

vi. Statistical methods

Control charts from time-series data can be used for monitoring the energy consumption of individual consumers and for defining anomalous regions in the graphs after which rules are formed to indicate which consumptions violate the rules. The customers whose consumptions violate the set rules are regarded as being fraudulent, and such suspicious customers will need to be inspected (Messinis & Hatziargyriou, 2018:262; Saeed et al., 2020:12; Guarda et al., 2023:14).

The XMR control chart in Spirić et al. (2015) monitors the X chart which represents a chart of actual individual energy consumption values and their corresponding MR chart which illustrates the chart of moving range values, to determine variations in consumptions that may be regarded as frauds based on certain set rules. Other statistical charts are the Exponentially-Weighted Moving Average (EWMA) and non-parametric cumulative sum (CUSUM) charts used by Mashima and Cárdenas (2012) to visualize data for the purpose of detecting NTL.

In the papers presented by Spirić et al. (2015) and Mashima and Cárdenas (2012), they provide valuable insights into ETD through statistical and ML approaches. However, their over-reliance on conventional methods, lack of deep learning integration, and absence of real-time detection reduce their effectiveness in large-scale SGs. The authors Mashima and Cárdenas (2012) primarily focus on data integrity attacks but do not account for other cybersecurity vulnerabilities in ETD.

Liu et al. (2015) proposed Bollinger bands which is commonly used in stock trading for NTLD. To determine NTL using the Bollinger bands, lower and upper bands are determined based on N periods of moving average and standard deviation of the time-series data, such that if the energy consumed at a specific time goes beyond the limit set for that period, then an anomaly, fraud or NTL is being suspected. However, the main disadvantage of this approach is that fraud cannot be detected if the incident had taken place of the monitoring period, since the method is basically used for detecting changes in energy consumptions.

While Liu et al. (2015) introduce a cybersecurity-based approach to ETD, their reliance on rule-based threat analysis, lack of real-time fraud monitoring, adversarial robustness, comparative evaluations, and limited scalability reduce the effectiveness of the framework in large-scale SG environments.

vii. Game-theoretic methods

Game-theoretic methods or game theory for NTLD are used to model NTL solution as a kind of game between the electricity swindlers and the electric utilities, where electricity thieves are modelled as attacker systems while the NTL solutions provided by the electric utilities are modelled as defender systems (Cardenas et al., 2012:1830; Messinis & Hatziargyriou, 2018:262; Gul et al., 2020:2). The game-theoretic approach for NTLD has been recently proposed and is still evolving as one of the major constituent of NTLD methods (Jiang et al., 2014:114-115; Messinis & Hatziargyriou, 2018:262).

ETD problem is conceived and modelled as a game between the stealing customer (attacker) and the electric utility (defender) by Cardenas et al. (2012). The electricity thief intended to steal a predefined amount of electricity and try as much as possible to avoid being detected. The attacker avoided being detected by changing the probability density function of their electric consumptions during the measurement period of the AMI. According to the authors, a probability density function called Nash equilibrium have been identified as the attacker and defender which the electric utility must select before delivering their AMI measurements, to optimize the possibility of theft detection in the game.

Cardenas et al. (2012) introduce a novel game-theoretic approach to ETD, their reliance on theoretical models, lack of real-time fraud monitoring, deficiency of explainable mechanisms, and absence of ML integration reduce the effectiveness of the framework in large-scale SG environments.

The authors in Lin et al. (2014) initiated the idea of non-cooperative game model for abnormality or NTL screening by compounding SMs with functional order self-synchronization error formulation, in a bid to distinguish between profiled consumptions and NTL-causing illegal consumptions. The authors in Amin et al. (2015) have proposed an extensive game-theoretic algorithms to model and analyse the functioning capacities of various techniques of classical statistics by using the data collected from smart meters for the purpose of ETD. This framework is motivated owing to cyber-attacks on electricity consumptions. In this work, firm preconceptions about how the fraud are being carried out are made, while estimates on precise detection capacity of the developed model under the made assumptions are provided.

The authors in Lin et al. (2014) and Amin et al. (2015) introduce innovative game-theoretic frameworks for ETD, however, their reliance on mathematical models, lack of real-time fraud monitoring, lack of cost-benefit analysis, and absence of ML integration reduce the effectiveness of the framework in large-scale SG environments.

- **Hybrid learning**

Hybrid learning is the composite or combination of supervised and unsupervised learnings (Ghori et al., 2020:16036) as depicted in Figure 2.21, and different from hybrid methods or techniques, which is the combination of both data-driven methods and network-driven methods (Messinis & Hatziargyriou, 2018:252, 263; Ghori et al., 2020:16035-16036).

In a bid to detect NTL using hybrid learning, Peng et al. (2016) used the daily energy consumption dataset of Chinese Southeast coastal city. During the initial phase of the hybrid-learning process, clusters of different consumers are being formed based on their patterns of consumptions using the k-means clustering algorithm. In the next phase of the learning process, reclassification is done by applying DT, random forest (RF), SVM and KNN to the consumers filtered initially. The classification done in the following phase using the ensemble classifiers surmounts the weakness of the clustering done in the initial phase. The authors employed the grouping of electricity consumers into classes in accordance with the patterns of their energy consumptions to assist in detecting any anomalous behaviours via their consumption patterns.

While Peng et al. (2016) present a useful two-stage pattern recognition approach for SG customer classification, their model does not explicitly address ET, lacks DL-based feature extraction, and does not support real-time fraud detection, making it less effective in practical fraud prevention scenarios.

The NTL approach proposed by Terciyanli et al. (2017) is a hybrid of fuzzy c-means clustering and fuzzy classification. In this work, clusters of consumers that have similar consumption patterns using fuzzy c-means clustering are first formed. After this, fuzzy classification with membership matrices is then performed next, which further classifies the electricity consumers. Furthermore, the deviation between the expected or target energy consumption values and the observed or predicted energy consumption values of each customer is calculated. If the deviation between the expected energy consumption values and that of the observed energy consumption values surpass a specified threshold, a potential fraud is suspected, and such customers whose energy difference passes the set threshold are shortlisted.

The authors in Terciyanli et al. (2017) introduce a rule-based score-driven approach for fraud detection, but its reliance on static scoring rules, lack of DL integration, and absence of real-time monitoring make it less effective for large-scale ETD.

- **Semi-supervised learning**

In the case of semi-supervised NTLD methods, the labelled samples (positive and negative samples) in the given dataset are too small or few with respect to the unlabelled samples, forming a borderline between supervised and unsupervised learnings (Messinis & Hatziargyriou, 2018:252; Lu et al., 2019:4; Yang, 2019:140; Osypova, 2020:40). In other words, semi-supervised learning methos make use of labelled and unlabelled samples with the proportion of the labelled-data samples being very small when compared with the unlabelled samples in the datasets (Messinis & Hatziargyriou, 2018:252; Yang, 2019:140). The primary objective of employing semi-supervised learning is to take advantage of the learning capabilities of both supervised and unsupervised learnings to produce a more-efficient ETD model (Kim et al., 2024:7).

The authors, Júnior et al. (2016), have used two techniques or paradigms of semi-supervised and unsupervised learnings for NTLD. The semi-supervised learning is used for anomaly detection with the dataset which has the information of only one class, while the OPF classifier is used for the unsupervised learning. The two techniques are used with datasets which contains commercial and industrial energy consumptions from Brazilian electrical power company. The metric performances of both techniques are compared with SVM, Gaussian mixture model (GMM), OC-SVM, k-means, balanced iterative reducing and clustering using hierarchies (BIRCH), and affinity propagation (AP). The authors submitted that the two techniques or paradigms of OPF and anomaly detection outperformed the other techniques compared with them, while the results of the OPF classifier is the most accurate.

Júnior et al. (2016) introduce an OPF clustering technique for fraud detection, nonetheless, the reliance of the method on unsupervised learning, lack of real-time processing, explainability issues, and absence of deep feature extraction reduce the effectiveness of the model in large-scale SG environments.

- **Network-oriented methods**

Network-oriented or network-based methods employ the analysis of power system networks for the purpose of NTLD (Guarda et al., 2023:22). This method uses data from the sensors on the distribution grid placed on smart meters and transformers, network-related data such as the topology of the grid, loading of the distribution transformer, current flow and voltage profile data, and phase connectivity data, etc. for NTLD (Messinis & Hatziargyriou, 2018:262-263; Guarda et al., 2023:15; Liao, Bak-Jensen, et al., 2024; Liao, Zhu, et al., 2024:5075). Network-oriented methods keenly depend on the understanding of the LV and MV network topology, including the measurements obtained from devices like RTUs and observer meters. Network-based methods make use of network measurements for its NTLD by employing physical rules and network analysis like estimation, load flow and sensor network (Viegas et al., 2017:1262; Messinis & Hatziargyriou, 2018:252, 262; Guarda et al., 2023:4-5) as shown earlier in Figure 2.21.

Unlike the data-based method, network-based NTLD method requires extra electric meters and devices like RTUs, RFIDs, wireless sensors, and software tools to enhance the monitorability of the distribution grid (Jiang et al., 2014:112; Osypova, 2020:45; Ali et al., 2023:2; Nayak & Jaidhar, 2023:2; Liao, Bak-Jensen, et al., 2024; Liao, Zhu, et al., 2024:5075). These ancillary devices are in addition to the existing grid equipment used in data-oriented methods for gathering consumer-related data. The costs involved in procuring the supplementary equipment make the network-oriented methods more expensive when compared with the data-based methods; although, the method provides better accuracy in terms of measurements and performances (Messinis & Hatziargyriou, 2018:264; Osypova, 2020:45; Gu et al., 2022:4568; Nayak & Jaidhar, 2023:2; Khan et al., 2024:2). The procurement of extra equipment or devices in conjunction with the existing grid equipment for additional measurements do not change the non-hardware-method status of the network-oriented method, because it is only the data generated by the added devices that are being worked upon for the purpose of ETD, and not that the hardware devices themselves are used to detect NTL (Guarda et al., 2023:22). Unlike data-based methods, network-based methods require less-voluminous datasets, but necessitates the use of higher-resolution datasets with more variety of features (Messinis & Hatziargyriou, 2018:263; Osypova, 2020:45; Guarda et al., 2023:18, 23).

- **Estimation**

This technique of NTLD provides considerable approximation of the NTL in an area or the NTL of a particular customer under investigation. The methods to estimate NTL in the electric distribution network is subdivided into state estimation and technical loss modelling (Viegas et al., 2017:1262) as depicted in Figure 2.21. The state estimation method determines the extent of irregularities associated with the energy consumptions of the customers by checking the deviations between their billed and actual consumptions; while technical loss modelling evaluates the TL in the distribution network to assist in the direct calculation of the approximate value of NTL present in the network (Anas et al., 2012:177; Viegas et al., 2017:1262-1263).

- **State estimation**

State estimation method is premised on finding the coherence between the grid data measured from the consumers' end and that measured from the electric network (Fragkioudaki et al., 2016:45). It is used mainly in the MV networks at substations for observing the distribution grid to detect NTL in the MV/LV transformers using central observer meters, to check if the total energy distributed matches the sum of individually consumed electrical energies by the customers at the LV networks (Messinis & Hatziargyriou, 2018:263; Saeed et al., 2020:14). State estimation checks the errors and irregularities like or bad data attacks or FDI in the energy demand of consumers (Viegas et al., 2017:1262; Messinis & Hatziargyriou, 2018:263; Saeed et al., 2020:14). FDIs and/or bad data attacks are indications of the presence of NTL in the consumption data (Messinis & Hatziargyriou, 2018:263; Saeed et al., 2020:14).

Bandim et al. (2003) proposed the methodology for the detection of deviations in energy balance of a group of consumers in a secondary distribution network owing to metering problems by using a central observer meter. This method is used to observe the meters of many consumers and pinpointing those meters that show the likelihood of causing NTL in a less costly and effective manner, while preventing the possibilities of inspecting individually all the electric meters under investigation. Defective meters that cause NTL are those that have been tampered with thereby registering incorrect readings, or those meters that have been completely bypassed. To determine those customers who have problems with their respective meters, deterministic and statistics techniques are employed. At any given time, the total energy recorded by the central observer meter and those recorded by the electric meter of each customer is represented by Equation 2.57.

$$E_{total} = k_1 E_1 + k_2 E_2 + \cdots k_i E_i + \cdots + k_N E_N \tag{2.57}$$

Where E_{total} is the total energy recorded by the central observer meter, which constitutes the sum of each energy consumed by the meter of consumer i out of the total N meters being considered. k_i of the meter of consumer i is a constant that is dependent on the accuracy class of the particular meter, while E_i is the energy recorded by the electric meter of consumer i. In case the energy of each of the N meters of all the i consumers with the central observer meter are computed separately for every i consumer, matrix inversion or weighted-least squares (WLS) state estimation algorithm could be used to solve the resulting system of linearly independent N equations shown in Bandim et al. (2003:164).

Bandim et al. (2003) introduce an innovative mathematical framework for fraud detection using central observer meters. The authors only focuses on a specific type of ET (tampered meters), assumes that the central observer meter is tamper-proof, which may not always be the case, uses simulated data to test the proposed mathematical approach, but does not validate the results using real-world data. The authors did not address potential security and privacy concerns related to the use of central observer meters.

The authors in Chen et al. (2011), Lo et al. (2012), and Luan et al. (2015) have also used WLS state estimation method for the load estimation of MV/LV transformers by using the real-time three-phase measurements of current, voltage, active and reactive power measurements obtained from the MV/LV transformers as the input data to the WLS algorithm. NTL is suggested in the distribution network if the estimation done using the WLS state estimator exceeds a predefined threshold.

While Chen et al. (2011), Lo et al. (2012), and Luan et al. (2015) have introduced state estimation-based frameworks for fraud detection, but none of the authors discuss the potential security and privacy concerns related to the use of advanced measurement data, and SG technologies for ETD. The authors’ reliance on mathematical models, lack of real-time detection, and absence of ML integration reduce their effectiveness.

A statistical model known as analysis of variance (ANOVA) has been used alongside state estimation method by the authors in Huang et al. (2013) and Lu et al. (2013) to form a two-stage NTLD approach. The first stage is the state estimation of the MV level of the grid to estimate the load on the MV/LV transformer in order to identify the feeders with defective or tampered meters. The second stage involves using ANOVA to identify suspicious customers with metering issues.

Huang et al. (2013) and Lu et al. (2013) introduce state estimation and ANOVA-based techniques for NTL detection. However, their reliance on predefined statistical models, lack of real-time processing, and absence of ML integration reduce their effectiveness in large-scale SG environments. Also, the authors did not discuss practical implementation issues, such as the cost and feasibility of installing new measurement devices or their potential impact on the existing electric grid.

Salinas and Li (2016) proposed a centralized state-estimation algorithm known as Kalman filter, which utilizes the real-time energy consumptions from consumers' SMs to detect NTL in a microgrid. However, a privacy-preserving algorithm decomposes Kalman filter to estimate line currents and biases in the energy consumptions to reveal the ET culprits. The privacy-preserving algorithm protects the privacy of electricity users by hiding information on their energy consumptions from system operators and eavesdroppers. Customers whose energy biases are higher than a predetermined threshold are considered to have committed ET.

Although, Salinas & Li (2016) introduce an innovative privacy-preserving framework for fraud detection in microgrids, their reliance on predefined state estimation models, lack of real-time monitoring, and non-consideration of other theft methods reduce their effectiveness for large-scale implementations.

- **Technical loss modelling**

In this method, the technical loss of the electricity distribution network is modelled to enable the direct calculation of NTL in the network (Viegas et al., 2017:1262-1263). Most utilities already have the technical loss data of their power networks, which gives an added advantage using the direct-calculation method. A higher NTL value beyond a tolerable benchmark is an indication of probable fraud. The authors in de Oliveira et al. (2006) and de Oliveira et al. (2008) proposed statistical methods to find accurate relationships between load factors and loss factors in order to improve the calculation of TL, which are consequently used to calculate NTL. NTL could then be evaluated by direct calculation after the determination of TL in electric systems.

- **Load flow**

One of the ways to detect NTL activities in an electric distribution grid is the calculation of energy flow in that network (Saeed et al., 2020:14). Load flow analysis entails the use of an observer meter which monitors the total energy consumed from the LV terminal of the distribution transformer and compares it with the total sum of consumptions as measured from the individual meters of the electricity customers (Messinis & Hatziargyriou, 2018:262; Saeed et al., 2020:14; Guarda et al., 2023:15). If the difference between the reading on the observer meter located at the distribution transformer and those readings collated from the electric meters of individual customers is great (considering the percentage of TL), then the probability of NTL occurring in the distribution network is higher (Messinis & Hatziargyriou, 2018:262-263; Yan & Wen, 2022; Guarda et al., 2023:15). This approach used for the determination of NTL is otherwise called the energy balance method, and happens to be the most popular approach of the network-based methods used by researchers in the literature (Guarda et al., 2023:15).

Kadurek et al. (2010) have proposed smart substation method which examines the energy disparities between the smart meters of electricity consumers and the utility observer meters. If an appreciable mismatch occurs in the energy balance, this method then attempts to locate the consumer location where the fraud or NTL is actually taking place. Probabilistic power-flow approach has been used by Neto and Coelho (2013) to determine TL so as to estimate and detect NTL in a large electric distribution system in the presence of load variations. The total energy consumed by the customers as measured from the feeder using observer meter is compared with the consumers’ billed energy. With the addition of the obtained TL to the billed energy, the NTL are therefore estimated using energy balance method. In this work, the feeder is divided into subnetworks with individual observer meters, such that the estimated NTL of a particular circuit is determined with greater accuracy. However, the literature authored by Nikovski et al. (2013) and Tariq and Poor (2016) have proposed methods for the identification of network parameters and calculating TL in the distribution networks for better estimation of NTL.

While Kadurek et al. (2010) and Neto and Coelho (2013) introduce valuable discussions on smart metering practices and probabilistic NTL estimation, however, their reliance on predefined models, lack of real-time processing, and absence of ML integration reduce their effectiveness in addressing scalability and practical implementation challenges in utility settings.

The authors, Ferreira et al. (2020), modelled load buses as QV buses to identify the illegally connected loads to the distribution system. The method also requires the measurements of active (real) and reactive (imaginary) powers and the magnitude of voltage obtained from SMs. QV buses are busses in which their reactive voltage and power are specified. Buses showing a discrepancy between calculated and measured active powers suggest potential locations of non-technical losses (NTL). The core concept of this approach is to model load buses as QV buses to address a load flow problem. The basic idea of this work is to model load buses as QV buses in a bid to solve a load flow problem. The calculated active power (P_{calc}) for each QV bus are determined using the load flow method. These active-power values from the QVs are then contrasted with the measured values of the active powers (P_{meas}) obtained from SMs. If the difference between these powers for each QV bus and SM for a particular customer goes beyond the proposed threshold value which is also referred to as minimum detectable power (MDP), then such customer is suspected of causing NTL. The MDP is calculated for each bus using the submatrices $J_{P\theta}, J_{PV}, J_{Q\theta}$, and J_{QV} from the Jacobian matrix shown in Equation 2.58.

$$\begin{bmatrix} \Delta P \\ \Delta Q \end{bmatrix} = \begin{bmatrix} \frac{\partial P}{\partial \theta} & \frac{\partial P}{\partial V} \\ \frac{\partial Q}{\partial \theta} & \frac{\partial Q}{\partial V} \end{bmatrix} \begin{bmatrix} \Delta \theta \\ \Delta V \end{bmatrix} = \begin{bmatrix} J_{P\theta} & J_{PV} \\ J_{Q\theta} & J_{QV} \end{bmatrix} \begin{bmatrix} \Delta \theta \\ \Delta V \end{bmatrix} \tag{2.58}$$

Deviations in active powers are caused by the maximum voltage measurement errors (ΔV_{max}^{meas}), which correlate to the MDP index. The deviation can be determined by applying a Kron reduction which leads to Equation 2.59. The impact of voltage measurement errors on the computed active power is estimated using Equation 2.59.

$$MDP = \left(J_{PV} - J_{P\theta}.J_{Q\theta}^{-1}.J_{QV}\right).\Delta V_{max}^{meas} = J_{RPC}.\Delta V_{max}^{meas} \tag{2.59}$$

$$\Delta W_{hi} = \sum_{j\in\lambda} \Delta P_{i,j}.\Delta t_j \tag{2.60}$$

Equation 2.60 denotes the energy deviation index (ΔW_{hi}) at bus i, where those customers that have higher values of ΔW_{hi} are regarded as being suspicious of causing NTL. The term λ is the amount of time the measurement set is accessible, whereas $\Delta P_{i,j}$ is the difference between the measured and calculated active power at the bus i at time interval j (Δt_j). The unauthorized loads that are not permanently connected to the system but injected at any time are identified using the index λ, which also helps in decreasing the effect of errors owing to measurements.

Although, Ferreira et al. (2020) introduce an innovative load flow-based fraud detection method, but the reliance of their method on deterministic calculations, lack of real-time processing, and absence of consumer behavioral analysis limit its effectiveness in large-scale ETD.

- **Sensor network**

The sensor network approach aspect of the network-oriented methods for NTLD involves the use of sensors which are installed at designated points in the electric distribution network (Messinis & Hatziargyriou, 2018:263). These sensors are used to localize NTL by optimally positioning them and deploying them at lower-infrastructure cost, in order to increase the probability of NTLDs, so that they can be detected more efficiently (Messinis & Hatziargyriou, 2018:263; Saeed et al., 2020:15; Guarda et al., 2023:17). The sensor network approach requires an in-depth knowledge of the topology of the distribution grid (Messinis & Hatziargyriou, 2018:263). The implementation of this approach is closely related to the state estimation method, since the sensors increase the observability of the electric network, and also for the fact that the installed sensors alone cannot ascertain if NTL has been detected in the electric network or not (Messinis & Hatziargyriou, 2018:263; Saeed et al., 2020:15; Guarda et al., 2023:17).

The placement of redundant SMs for the purpose of detecting NTL has been proposed by Xiao et al. (2013). In this framework, an observer meter and an inspector box which contains a specified number of inspector SMs which are mounted at the secondary distribution substation before the SMs of the electricity consumers. The inspector meters engage in data exchanges between them and the SMs of the consumers to compare the energy consumptions measured by the inspector meters and those measured by the consumers' SMs. Differences in these measurements are possible indications of NTL.

Xiao et al. (2013) introduce an important security framework for identifying malicious meter inspections, but the study overlooks broader fraud detection techniques, lacks real-time monitoring capabilities, and does not empirically validate its proposed methods.

McLaughlin et al. (2013) present an AMI intrusion detection system (AMIDS) for ETD. The method uses attack graph-based information fusion technique to combine three types of information specific to the AMI which include information obtained from: anti-tampering sensors on the SMs, the cyber network and host intrusion detection systems, and anomalous power consumptions learnt via NILM. AMIDS learns the frequency of the daily usage of each appliance using the data of the appliances that the NILM provides. NILM technique leverages on the database of appliances to learn their patterns of usage over time. The anomaly or irregularity in the time series power consumption data is analysed, and the edges in the consumptions that corresponds to on/off events are logged. NILM functions by solving the binary integer programming problem shown in Equation 2.61.

$$\begin{aligned} \min \quad & B^T x \\ s.t. \quad & Q_x \leq e_{ti} + \delta \\ & -Q_x \leq -e_{ti} + \delta \\ & x \geq 0 \end{aligned} \tag{2.61}$$

Where $B = [1,1,\ldots,1]_{2.|A|\times 1}$; $Q = [Q_P; -Q_P]$, and Q_P is an $|A|$-dimensional vector of the power consumption profile of the electric appliances. The motive for solving the linear programming problem is to obtain $2 \cdot |A|$-dimensional binary vector x, where a vector element represents whether or not the appliance it depicts contributed to the edge e_{ti}. The small threshold value of δ accounts for the measured noise.

McLaughlin et al. (2013) offer a promising multi-sensor framework for ETD by leveraging diverse data sources within AMI. The approach is limited by its lack of real-time processing, challenges in scaling to large networks, and issues related to sensor data integration, cost, and privacy.

❖ Hybrid methods

Hybrid techniques have been initiated as part of the efforts to improve ETD methods, in an attempt to further increase the accuracy of NTLDs in electric grids (Messinis & Hatziargyriou, 2018:263; Guarda et al., 2023:17). The hybrid methods use a merger of the data-based and network-oriented methods (Guarda et al., 2023:4, 17, 22) as shown in Figure 2.21, in conjunction with the data types shown in Figure 2.22, for NTLDs. To achieve the hybridized NTLD solutions, energy consumption data have been combined with network data (Ghori et al., 2020:16037). This method is more efficient and reassuring (Guarda et al., 2023:4). The hybrid method involves the use of network data in order to firstly detect NTL in parts of the distribution grid, after which statistical or ML method can then be employed to further detect NTL among the electricity customers by using their energy consumption data. An example of hybrid method is the use of state estimation method at the MV level to detect NTL at the MV/LV transformer level of the grid in a bid to discover the particular section of the distribution network harbouring NTL. After this, ML classification algorithms using supervised methods could then be employed in conjunction with the energy consumption data of electricity customers to detect NTL at the consumer level (Messinis & Hatziargyriou, 2018:252).

In Guo et al. (2014), the authors used RTU measurements and consumers' SM measurements to determine the sections in the distribution network that causes NTL. Initially, subnetworks in the distribution network is created according to the number of available RTUs. TL in the network are estimated by applying distribution power flow method. If the difference or mismatch between the RTUs and SM measurements exceed a certain threshold then the presence of NTL in the distribution network is assumed. fuzzy c-means and SVM algorithms are applied to determine whether individual customers cause NTL or not. The analysis of losses has been proposed by Spirić et al. (2014) to estimate the number of consumers committing ET in the distribution network after which rough set theory is then used to calculate the boundary region of suspected electricity fraud.

Although, Guo et al. (2014) and Spirić et al. (2014) introduce innovative rule-based fraud detection techniques, however, their reliance on static models, lack of real-time fraud detection, and limited scalability assessment reduce their effectiveness for large-scale ETD. Guo et al. (2014) focuses on online data validation for distribution operations against cyber-tampering, but did not consider other types of cyber threats or attacks. Spirić et al. (2014) assumes that fraudsters will exhibit specific patterns of behaviour that can be detected using rough set theory, but did not consider that fraudsters may change their behaviour.

The authors in Jokar et al. (2016) deployed consumption pattern-based energy theft detector (CPBETD) algorithm to detect NTL using observer meters at the distribution transformers, in conjunction with SVM classifier. The output of the SVM classifier is being compared with the observer meters used to evaluate the active energy balance of the distribution network under consideration. The CPBETD algorithm is used to estimate the TL in the network and to measure the energy-balance mismatch. If the mismatch goes beyond a predetermined threshold and the SVM classifier produces a positive output or sets of positive outputs after classifying the daily energy consumptions, then the consumers under NTL investigation are classified as fraudulent and are then recommended for onsite inspections. This concept was also applied earlier by Jindal et al. (2016), but in this case, the combination of DT and SVM was proposed in addition to grid balancing at the transmission and distribution levels.

While Jokar et al. (2016) and Jindal et al. (2016) introduce innovative ETD methods using consumption patterns and ML, their lack of real-time capabilities, scalability assessment, and integration of DL techniques limit their effectiveness for large-scale SG applications. Jokar et al. (2016) and Jindal et al. (2016) assume that customers' consumption patterns are consistent and can be used to detect ET, but did not consider the potential impact of changes in customers' behaviour or lifestyle on the proposed approach.

2.6 Conclusion

Electricity must be generated before it can be transmitted and distributed to the consumers. It must also be measured to determine whether it is being stolen or not. In this chapter, the review of electricity grid led us to SG, the latest development in the electricity grid system. Similarly, the review of electricity metering led us to SM, the latest version of the electric meter. Both the SG and the SM are important components of this research project, as we will be using the smart metering data from SG for our ETD experiments. The electricity system, including its metering and its associated NTL prevention, detection, and mitigation techniques have been thoroughly reviewed in this chapter. Also, inquests have also been made into the causes and effects of ET. The next chapter is the experimental part of the thesis which discusses the methods employed in modelling the proposed NTLD model.

CHAPTER 3

METHODOLOGY

3.1 Introduction

Detection of electricity theft (ET) in power grids primarily requires the development of formidable and reliable models. This is the core and the most significant aspect of detecting and mitigating ET. Building effective electricity-theft detection (ETD) models requires developing intelligent systems to detect non-technical losses (NTL) in electric grids. Developing ETD models are inevitable as NTL cannot be determined by strictly applying the fundamental laws of electrical engineering like in the case of technical losses (TL) (Osypova, 2020:11). NTL detection (NTLD) models are constructed from algorithms that run on a given dataset through simulations to produce intelligent NTLD models or systems capable of detecting fraud in electric distribution systems. ETD models serve as the basis upon which electric utilities tackle the ET menace. The aim of this research is to build intelligent and efficient ETD model that profoundly detect ET, leading to corresponding effective mitigation of theft or fraud in the power grids.

It has earlier been asserted in Section 2.4.5 of Chapter 2 that employing artificial intelligence (AI) by implementing machine learning (ML), a subfield of AI, is the state-of-the-art method used in building efficient and cost-effective NTLD models (Glauner et al., 2017:761; Glauner, 2019:31, 110; Ghori et al., 2020:16033-16034; Saeed et al., 2020:1; Guarda et al., 2023:4; Stracqualursi et al., 2023:12, 16; Coma-Puig et al., 2024:2704). Hence, the proposed NTLD model developed in this chapter is based on ML methods. A very efficient ETD model has been built and the procedures leading to its development have also been explicitly analysed. The developed model, which is also being referred to as the proposed model, is an integration of deep convolutional neural network (CNN) and an ensemble random forest (RF) models, to form an hybrid model termed CNN-RF model. The developed NTLD system has been modelled with the intent of fulfilling the aim and objectives of the research and also to concurrently proffer answers to the research questions. The Python codes used in implementing the proposed model can be found in the Appendix. This chapter analyses the methods involved in modelling the proposed CNN-RF hybrid model.

3.2 System model

Since NTL cannot be completely eliminated in the power systems (Lewis, 2015:128-129; Kocaman & Tümen, 2020:1), the motivation behind this research project is to develop a reliable ETD model that will enhance the reduction of NTL considerably in power grids. The methodology adopted to develop the proposed ETD model in this research is the AI-based ML methods, as this approach is the latest and the most-efficient method used in developing the most-effective models for NTLDs (Glauner et al., 2017:761; Glauner, 2019:31, 110; Ghori et al., 2020:16033-16034; Saeed et al., 2020:1; Guarda et al., 2023:4; Stracqualursi et al., 2023:12, 16; Coma-Puig et al., 2024:2704). So many ML models have been experimented with the employed SGCC dataset described in Section 3.2.2, to identify the model that would give better performance results. The model development process was a rigorous and painstaking exercise with so many trials and errors before arriving at the model which produces the best results with respect to other tested models. The search for the best suited model has to be done inevitably since there is no accurate method, hard-and-fast rule, or universal best practice for finding the best model to solve any problem (Bramer, 2020:185). In the end, the NTLD model with suitable results that fulfil the aim and objectives of the research project and which also proffer answers to the research questions has been discovered and adopted as the proposed model (Poudel & Dhungana, 2022:117), while those models that did not produce satisfactory results were dropped.

The proposed ETD model is developed through the combination of convolutional neural network (CNN) model with random forest (RF) model to form a new hybrid model termed CNN-RF model. The new model involves the infusion of the features from the convolutional layer of the CNN model into RF model to increase prediction capacity. RF combines different decision trees (DTs) as against a single DT in a DT model to enhance robustness and also to prevent overfitting (Javaid, Jan, et al., 2021:50; Khan et al., 2024:14). The proposed model is a supervised NTL classification model. The model is a “supervised” model in the sense that the SGCC dataset used in training it is labelled (Appiah et al., 2023:2), in this case for honest (non-theft) and fraudulent (theft) customers.

3.2.1 Simulation tool

Python is the most popular and most pervasive simulation software and programming language used in ML and data science (Voskoglou, 2017). Python is an open-source package which is preferred over other simulation tools and programming languages like MATLAB, R, Julia, Scala, Java, Octave, SAS, JavaScript, C/C++, Ruby, etc., owing to its simplicity, flexibility, robustness, proficiency, and efficiency. Python is reinforced with comprehensive libraries, as it is an all-encompassing simulation tool deployed in carrying out any ML-related tasks. Hence, the ML simulations in this research project for the detection of suspicious customers who may have committed ET have been carried out using

Python, in a Google Colaboratory (Colab) integrated development environment (IDE). Google Colab is preferred over other conventional IDEs like Jupyter Notebook, PyCharm, Thonny, Spyder, PyScripter, Visual Studio Code, Eclipse, PyDev, and Rodeo, etc., due to its numerous advantages. Google Colab is increasingly used for executing ML projects particularly in academic settings, due to its seamless integration with GitHub by simply allowing direct import and export of notebooks.

Other justifications for choosing Google Colab IDE over other conventional IDEs are that it fully offers free and unrestricted cloud-based service, which implies that no Python installation software or setup is required on local computers, as all processing are done directly on Google servers. This thereby saves the memories and storages of personal computers. While other IDEs such as Jupyter Notebook, Visual Studio Code, and PyCharm also support version control, cloud-based execution and collaborative learning among AI enthusiasts, Google Colab combines all these functions in one platform. Google Colab connects with Google Drive for automated backups, gives free access to specialized computing resources such as hardware runtime accelerators like graphics processing units (GPUs) and tensor processing units (TPUs), to enhance computationally intensive ML simulations. Unlike other IDEs, Google Colab has higher random-access memory (RAM) runtime option and is already fortified with standard built-in libraries like NumPy, Pandas, Matplotlib, Scikit-learn, TensorFlow, OpenCV, Keras, and PyTorch, etc., which have been exclusively preinstalled for AI-based simulations. Google Colab is more powerful, more flexible, and swifter in command executions.

Simulations to implement the proposed ETD model is carried out using Python in Google Colab IDE, where the model is constructed by applying it to the SGCC dataset described in Section 3.2.2. All the Python implementation codes used for simulating the proposed model can be found in the Appendix. The local computer used in running the simulations has processor**:** Intel Core i5-10210U CPU @ 1.60GHz – 2.10GHz, RAM: 8GB, system type: 64-bit operating system, x64-based processor as specifications. Running the proposed NTLD model on Google Colab reduces computational overhead on the local computer because of some of the advantages of Google Colab mentioned in the previous paragraphs. The training time expended for developing the proposed model is around fifteen minutes using Google Colab. This could have taken up to two hours if the model had been run directly on the local computer. Memory usage during the ML simulations is about 3GB using Google Colab. This could have been up to 7GB using the local computer. The inference speed (expected prediction time) is about fifteen milliseconds using Google Colab, which could have been up to 600 milliseconds using the local computer.

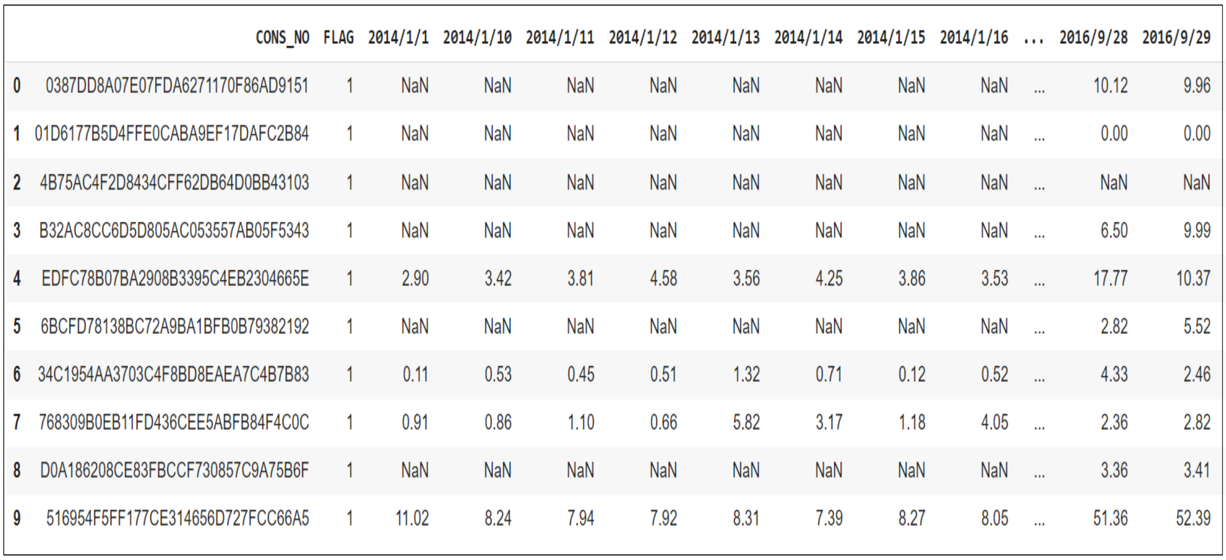
3.2.2 Dataset acquisition and description

The dataset used in this work for ML simulations in developing the proposed model, to detect NTL in power grids, is an open-source real-world large time-series electricity consumption dataset. The employed dataset which is provided by State Grid Corporation of China (SGCC) is available online and could be found in Dai (2018). SGCC is a state-owned Smart Grid (SG) electric system, and the largest electric utility company in the world (Wang et al., 2016:379; Zhou et al., 2017:73), with the domain name: (http://www.sgcc.com.cn). The dataset is widely-used and formidable, and is the most popular and one of the most-dependable datasets available for carrying out ETD experiments (Badawi et al., 2022:9; Bai et al., 2023:19; Khan et al., 2024:6; Kim et al., 2024:8; Liao, Bak-Jensen, et al., 2024). The SG dataset contains unbalanced daily electricity consumption records, or load profiles of 42,372 electricity customers in kilowatt-hour (kWh) taken for two years and ten months over 1034 days between Wednesday 01 January 2014 and Monday 31 October 2016. The daily energy consumption of every electricity consumer in the SGCC dataset represents the total units (in kWh) of electricity consumed per day by each electricity customer.

The SGCC dataset is well-known, and has been employed extensively by many prominent researchers in the field of ETD or NTLD in making their contributions to the corpus of knowledge. This is owing to its being comprehensive, standard, reliable, and effective for developing ETD or NTLD models as against other available datasets (Khan et al., 2024:6). The far-and-wide usage peculiarity of the SGCC dataset provides a good and fair ground for comparing the performance scores obtained through the ETD model developed in this work and the performance results achieved by the ETD models constructed by other researchers in the previously published research. The major contribution to knowledge of this research project is based on benchmarking the results of the proposed model with other recently developed NTL models in the existing literature. The NTL models in the benchmark literature (previous works) have also been developed using the same SGCC dataset employed in this thesis to build the proposed model.

As a typical non-synthesized real data, the consumption profile of the SGCC dataset is imbalanced (Ghori et al., 2020:16034, 16036). The dataset is in Microsoft Excel file in comma-separated values (CSV) format. Table 3.1 depicts the first ten rows of the employed SGCC dataset which is used as a prototype in describing the structure of the dataset. The figure is obtained from Google Colab IDE by invoking the Python codes in Section A.1.2.4 of the Appendix. This was done during the exploratory data analysis (EDA) stage of the ML simulations to reveal the characteristics of the dataset, after importing the SGCC dataset into Google Colab. Other vital information about the SGCC dataset could also be reaffirmed during the simulations. The first column in the data frame is the CONS_NO column denoting the consumer identity numbers, the second column is the FLAG column with labels depicting the NTL statuses of every consumer, while the remaining 1,034 columns which represent each day of the 34-month period of the load profiling consist of the daily energy consumption units per the 42,372 electricity consumers contained in the dataset.

Table 3.1: The first ten rows of the SGCC dataset



	CONS_NO	FLAG	2014/1/1	2014/1/10	2014/1/11	2014/1/12	2014/1/13	2014/1/14	2014/1/15	2014/1/16	...	2016/9/28	2016/9/29
0	0387DD8A07E07FDA6271170F86AD9151	1	NaN	NaN	NaN	NaN	NaN	NaN	NaN	NaN	...	10.12	9.96
1	01D6177B5D4FFE0CABA9EF17DAFC2B84	1	NaN	NaN	NaN	NaN	NaN	NaN	NaN	NaN	...	0.00	0.00
2	4B75AC4F2D8434CFF62DB64D0BB43103	1	NaN	NaN	NaN	NaN	NaN	NaN	NaN	NaN	...	NaN	NaN
3	B32AC8CC6D5D805AC053557AB05F5343	1	NaN	NaN	NaN	NaN	NaN	NaN	NaN	NaN	...	6.50	9.99
4	EDFC78B07BA2908B3395C4EB2304665E	1	2.90	3.42	3.81	4.58	3.56	4.25	3.86	3.53	...	17.77	10.37
5	6BCFD78138BC72A9BA1BFB0B79382192	1	NaN	NaN	NaN	NaN	NaN	NaN	NaN	NaN	...	2.82	5.52
6	34C1954AA3703C4F8BD8EAEA7C4B7B83	1	0.11	0.53	0.45	0.51	1.32	0.71	0.12	0.52	...	4.33	2.46
7	768309B0EB11FD436CEE5ABFB84F4C0C	1	0.91	0.86	1.10	0.66	5.82	3.17	1.18	4.05	...	2.36	2.82
8	D0A186208CE83FBCCF730857C9A75B6F	1	NaN	NaN	NaN	NaN	NaN	NaN	NaN	NaN	...	3.36	3.41
9	516954F5FF177CE314656D727FCC66A5	1	11.02	8.24	7.94	7.92	8.31	7.39	8.27	8.05	...	51.36	52.39

The labels in the FLAG column are binary indicators, which are also known as unique values or target variables in the dataset, to depict whether a particular consumer steals electricity or not. The consumers labelled or annotated “0” are the honest or benign customers who do not steal electricity or cause NTL, while the consumers labelled “1” are the fraudulent or malignant consumers who steal electricity and thus cause NTL in the electric grid (Glauner, 2019:48; Munawar, Javaid, et al., 2022:12; Ali et al., 2023:6, 9; Nayak & Jaidhar, 2023:4). The “0” label or annotation attributed to honest consumers is also referred to as a negative label, while the “1” label ascribed to fraudulent consumers is otherwise known as a positive label. Although, the “0” labels are not shown in the limited data distribution of the SGCC dataset shown in Table 3.1, but they are definitely in the subsequent rows of the data frame. Both the “0” and “1” labels represents the classes in the dataset.

The labels or target variables is critical for supervised learning, as it helps models to learn what constitutes typical usage (periodic usage with label “0”) and abnormal usage (non-periodic usage with label “1”). Periodicity or consistency in energy consumptions typically points to non-theft situations, while non-periodicity or inconsistency in energy consumptions potentially portends fraudulent situations, which may point to theft or illegal electricity usage (Zheng et al., 2018:1608-1609; Bai et al., 2023:13; Wang et al., 2023:5, 9, 19-20; S. Zhu et al., 2024:15477). Features like electricity consumption values, temporal attributes, and labels in the dataset help to detect anomalies in consumptions. The customer information provided helps to determine which customer is honest or fraudulent. These features enhance the training of models to allow them learn complex patterns. These patterns help to distinguish between honest and fraudulent consumptions, enables revenue recovery, reduces costly manual onsite inspections, and enhance better management of the grid.

From the dataset, 3,615 consumers committed ET, which is equivalent to about 8.5% of the total consumers, while 38,757 are consumers who did not commit ET, which constitute around 91.5% of the whole consumers. The fraudulent electricity consumers constitute the minority class, while the honest consumers comprise the majority class. The labels on the energy consumption dataset for each electricity consumer have been assigned manually by the SGCC utility stakeholders after onsite inspections were conducted by their utility technicians or inspectors to determine the honest and fraudulent consumers (Lu et al., 2019:5; Khattak et al., 2022:5). As could be seen from the data frame in Table 3.1, some spaces which are normally supposed to contain units of daily energy consumptions are rather filled with missing values or undefined values called Not a Number (NaN) (Bohani et al., 2021:3). Missing values in raw energy consumption datasets used for ETD are common issues which cause performance impairments of NTLD models (Liao, Bak-Jensen, et al., 2024). Table 3.1 shows the distribution summary of the employed SGCC dataset.

Table 3.2: Description summary of the SGCC dataset

Description	Values
Period of data collection	01 January 2014 – 31 October 2016
Number of days of data collection	1,034
Total number of electricity consumers	42,372
Total number of fraudulent consumers	3,615
Percentage of fraudulent consumers	8.5%
Total number of honest consumers	38,757
Percentage of honest consumers	91.5%

NaNs could occur as a result of faulty smart meters (SMs) or SM failures due to malfunctioning of device components and/or memory loss, errors from utility members of staff, tampering of SMs, data storage issues at the utility end, unplanned system maintenance, cyberattacks, lag or delay in data registration, corruption of data, unstable or unreliable data transmissions or fluctuations of SM network, congestion or blockage of communication, failure or malfunction of sensors and collectors, distribution-line faults, etc. (Khan et al., 2024:6; Nirmal et al., 2024:3; L. Zhu et al., 2024:259). In essence, all the cases leading to missing values in electricity consumption datasets as mentioned above are basically owing to faults that occur during data collections (Mujeeb et al., 2021:128524; Wang et al., 2023:5). Missing values during the collection of electricity consumption dataset is unavoidable in reality (W. Liao et al., 2022:3525). Figure 3.1 shows the proportion of honest and fraudulent consumers in a bar chart, while Figure 3.2 depicts the pie chart of the distribution of the honest and fraudulent electricity consumers in the SGCC dataset. The bar chart shows size of the unique values for honest and fraudulent customers, while the pie chart shows the percentage proportions of the honest and fraudulent electricity customers in the SGCC dataset.

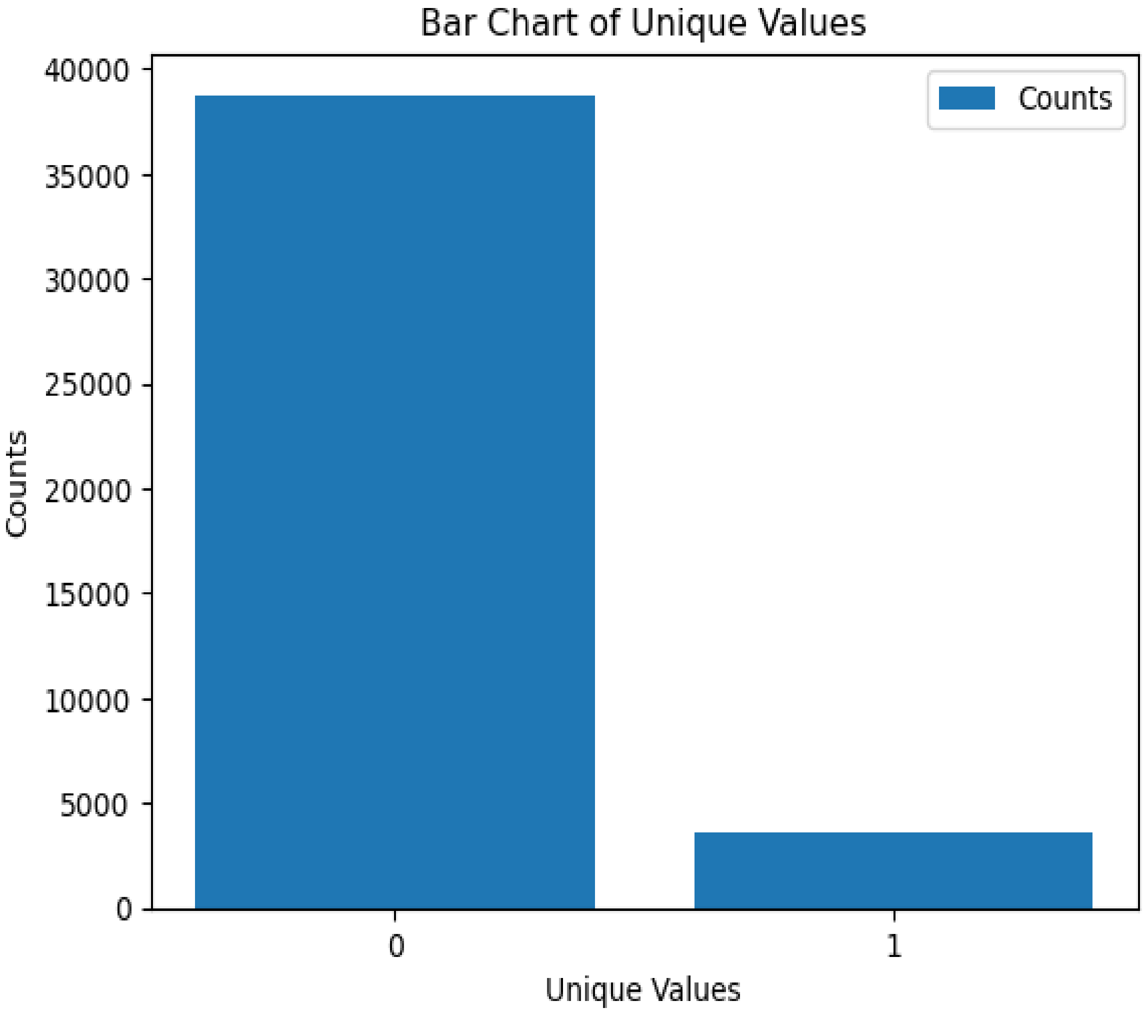


Figure 3.1: Count proportion of the unique values in the dataset

As mentioned earlier, the unique values in the SGCC dataset are the binary labels “0” and “1”, which corresponds to the labels attributed to honest electricity customers and those customers who engage in stealing electricity. The Python implementation codes used to obtain the bar chart and the pie-chart of the unique values in the dataset as shown in Figures 3.1 and 3.2 can be found in Section A.1.2.3.2 of the Appendix. In both figures, the unique values “1” and “0” respectively correspond to customers who steal electricity (flagged) and the customers who did not steal electricity (unflagged).

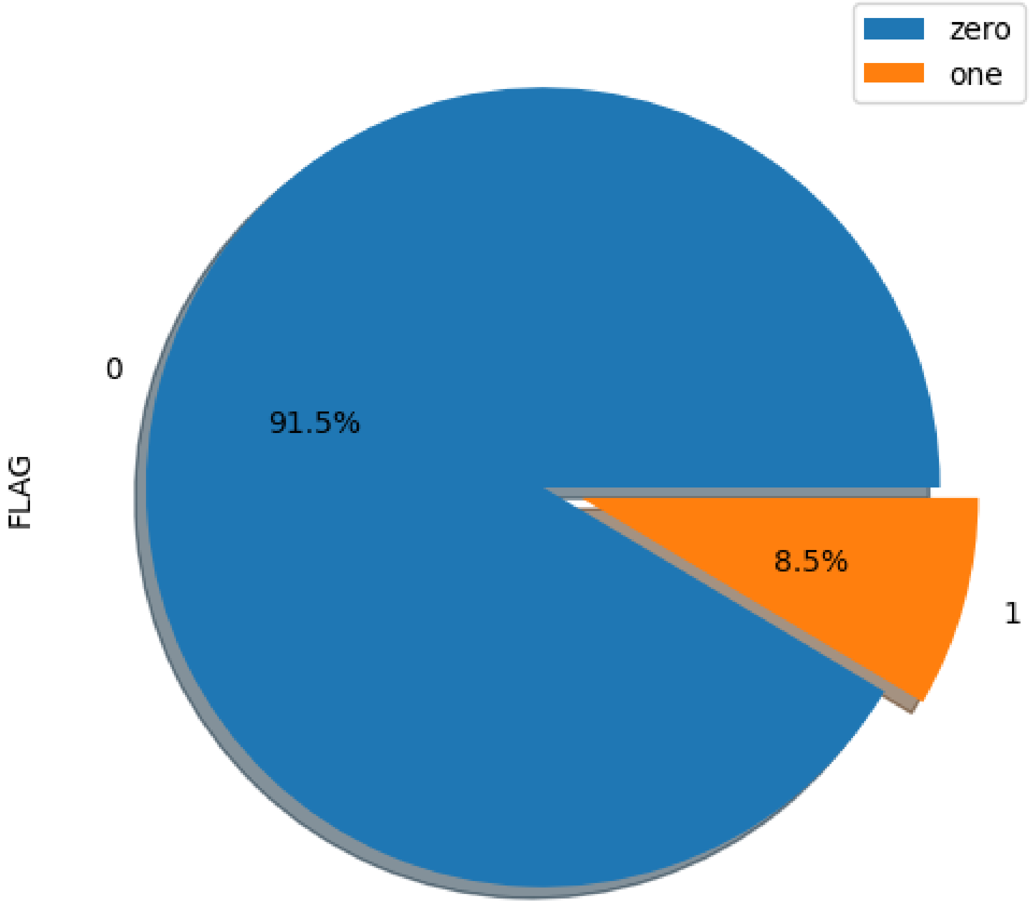


Figure 3.2: Percentage proportions of unique values in the dataset

The comparison of the results of the proposed model developed in this thesis and those of other SGCC dataset-based models in the existing literature is shown in Table 4.2 in Section 4.5.1.1 of Chapter 4. Benchmarking of the results was done with a view to validate the efficacy of the proposed model in detecting ET with respect to the previously developed NTLD models in the literature. The proposed model is superior and more potent in detecting NTLD owing to its higher performance results when compared with the performance results obtained in the previous research.

- **Justification for the choice of the employed SGCC dataset**

The selection of the SGCC dataset for the ETD experiments in this study, rather than datasets from Africa and some other developing countries, is primarily due to the fact that SG is still in the developmental phase in these regions, unlike in more developed areas such as Europe, North America, Australia, and certain parts of Asia. The SGCC dataset originates from China, a developing country, making it relevant to the context of Africa and other developing nations. Moreover, there is a general scarcity of standard and labelled datasets for NTLD in Africa and other developing regions. Despite regional differences in electricity consumptions, the patterns of ET are universally consistent across geographies. The SGCC dataset, therefore, reflects the typical patterns of ET that are common globally.

Although absolute consumption levels, such as peak load values, may vary between the SGCC dataset and those typical in Africa and other developing countries, the underlying ET patterns are comparable and transferrable. This allows the proposed model (developed using the SGCC dataset) to be adaptable and applicable for use by utilities in Africa and other developing regions. Additionally, the SGCC dataset is a widely recognized and accepted dataset within the NTLD research community, which is frequently used by prominent scholars. As such, models developed using this dataset can be easily benchmarked and validated, ensuring the reliability and robustness of the proposed model. Furthermore, the SGCC dataset is the most popular and one of the most-reliable datasets for developing NTLD models (Khan et al., 2024:6; Kim et al., 2024:8).

3.2.2.2 Mathematical representation of the dataset

Each feature in the SGCC time series dataset represents the amount of energy used at certain times by electricity customers, and can be represented as a sequence or a matrix of readings. The input dataset which is used to develop the proposed ML model for ETD consists of a sequence of energy consumption values or feature vectors in kWh at a specified time for every electricity customer represented in the SGCC dataset, as shown in Equation 3.1.

$$X_i = \left[x_{i,1}\ ,\ x_{i,2}\ , x_{i,3}\ , \dots\ , x_{i,L}\right] \tag{3.1}$$

Where X_i is the feature vector of the daily energy consumptions of an arbitrary electricity customer i, spanning through the entire time window of the dataset. Considering that L is the sequence length (i.e., the number of features, time points or time steps in the sequence) of each feature vector of an arbitrary electricity customer i in any row of the dataset, then $x_{i,j}$ is the $j-th$ feature or meter reading of a customer i at a particular time (daily in this case) in the customer's feature vector as shown in Equation 3.1. The first measured daily energy consumption feature in the feature vector of an arbitrary customer i recorded on 01 January 2014 is depicted as ($x_{i,1}$); while the last feature in the feature vector of length L corresponds to 1,034th day in the dataset, which was registered on 31 October 2016 is represented as ($x_{i,L}$) as shown in Equation 3.1. For example, $[x_{1,1}, x_{1,2}, x_{1,3}, \dots, x_{1,1034}]$ in the dataset represents the feature vector of the first electricity customer in the dataset, while $[x_{2,1}, x_{2,2}, x_{2,3}, \dots, x_{2,1034}]$ denotes the feature vector of the second electricity customer in the dataset, etc. The X_i in Equation 3.1 is such that:

$$X_i \in \mathbb{R}^L \quad \textbf{(3.2)}$$

Where X_i is a feature vector with L components of real numbers as depicted in Equation 3.1. For the binary labels attributed to the feature vectors of the energy consumptions of every electricity customer in each row of the dataset, Equation 3.3 represent the mathematical denotation of the binary labels.

$$y_i \in \{0,1\} \quad \textbf{(3.3)}$$

Where y_i represents the corresponding binary label or the expected output of the energy consumptions or feature vector of an arbitrary electricity customer i in any row of the SGCC dataset. The y_i label represents the class of each feature vector belonging of an arbitrary customer i, where customer i with 0 label (i.e., $y_i = 0$) belongs to the negative class, while another customer i with 1 label (i.e., $y_i = 1$) belongs to the positive class. The customers with 0 label represents the honest customers who do not engage in stealing electricity or causing NTL, while the customers with 1 label denotes the customers who engage in ET. The customer i in Equations 3.1, 3.2, and 3.3 respectively has the possible values $i = 1,2,3, \dots, N$; connoting the number of every sample which also corresponds to the numbers ascribed to every electricity customer i contained in the SGCC dataset.

Therefore, the equation representing the entire SGCC dataset, which consists of the X_i feature vectors of the energy consumed by electricity customers, and their corresponding

y_i binary labels for each feature vector of customer i in a particular row of the dataset is illustrated in Equation 3.4 (Li et al., 2019:7; Yan & Wen, 2021; Kawoosa et al., 2023:4805).

$$D = \{(X_i, y_i), (X_{i+1}, y_{i+1}), \ldots, (X_N, y_N) \mid i = 1,2,3, \ldots, N\} \quad \textbf{(3.4)}$$

Where D represents the entire dataset, X_i illustrates the feature vector or the meter readings of a particular customer i for the entire duration of the daily energy registrations of the customer in the dataset, y_i denotes the binary label of the particular customer i with feature vector X_i. The value of y_i indicates the class (theft or no theft) in which the particular customer i belongs, while $i = 1,2,3, \ldots, N$ indicates the number of every sample in the SGCC dataset which also corresponds to the numbers attributed to each electricity customer i contained in the dataset. The total number of samples represented as N corresponds to the total number of customers in the dataset, which is equal to 42,372, according to the total number of customers represented in the employed SGCC dataset. From Equation 3.4, the input-output pair (X_1, y_1) represents a sample or data point of electricity customer 1 with its feature vector X_1 and its corresponding label y_1, while (X_2, y_2) represents a sample or data point of electricity customer 2 with its feature vector X_2 and its corresponding label y_2, etc. A sample or a data point in the dataset represents the feature vector of a customer i with its associated label.

3.3 Development of the proposed CNN-RF model

The proposed CNN-RF model indicates that both convolutional neural network (CNN) and random forest (RF) models are dynamically integrated to form the resulting hybrid model. CNN model is hybridized with RF model because the combined model achieves better prediction results which tends to enhance detection efficiencies and ensure more profits to electric utilities. For every developed model being simulated, their classification results or test performances are generated alongside, an aspect which will be discussed explicitly in Chapter 4. The flowchart of the proposed CNN-RF model is depicted in Figure 3.3, while the block diagram of the prescribed NTLD model is illustrated in Figure 3.4.

The flowchart and the block diagram show the processes involved in the implementation of the recommended model. Combining the strengths of directly linked CNN and RF models in an hybrid layout is more advantageous because CNN models are effective in feature extraction (Ullah et al., 2020:1599; W. Liao et al., 2022:3520; Khan et al., 2024:16; Nirmal et al., 2024:1), while ensemble RF classifier model is endowed with outstanding classification accuracy as well as high efficiency and robustness (Xu et al., 2019:1, 4; Wang, 2023:505).

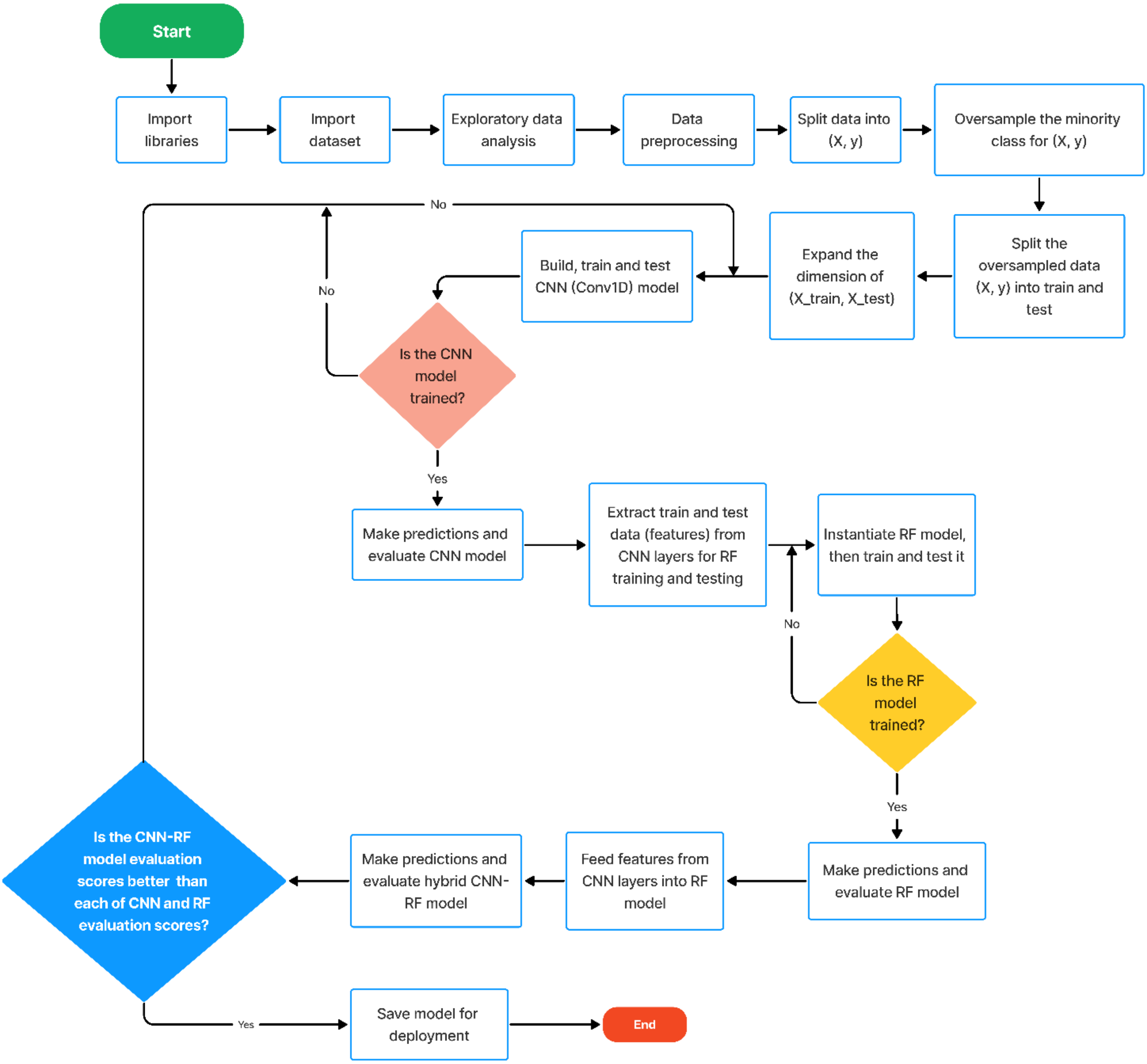

Start
Import libraries
Import dataset
Exploratory data analysis
Data preprocessing
Split data into (X, y)
Oversample the minority class for (X, y)
Split the oversampled data (X, y) into train and test
Expand the dimension of (X_train, X_test)
Build, train and test CNN (Conv1D) model
No
No
Is the CNN model trained?
Yes
Make predictions and evaluate CNN model
Extract train and test data (features) from CNN layers for RF training and testing
Instantiate RF model, then train and test it
No
Is the RF model trained?
Yes
Make predictions and evaluate RF model
Feed features from CNN layers into RF model
Make predictions and evaluate hybrid CNN-RF model
Is the CNN-RF model evaluation scores better than each of CNN and RF evaluation scores?
Yes
Save model for deployment
End

Figure 3.3: Flowchart of the proposed CNN-RF model

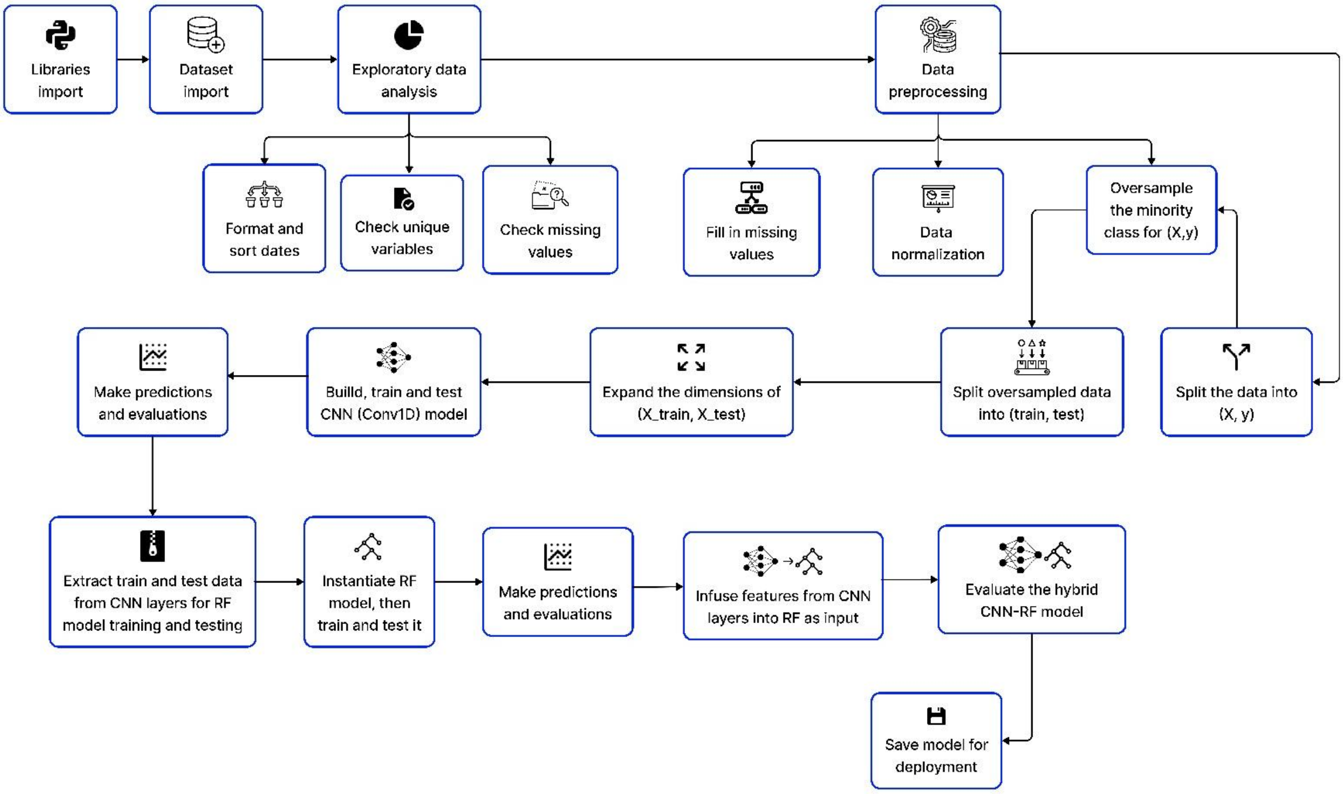

Libraries import
Dataset import
Exploratory data analysis
Data preprocessing
Format and sort dates
Check unique variables
Check missing values
Fill in missing values
Data normalization
Oversample the minority class for (X,y)
Make predictions and evaluations
Builld, train and test CNN (Conv1D) model
Expand the dimensions of (X_train, X_test)
Split oversampled data into (train, test)
Split the data into (X, y)
Extract train and test data from CNN layers for RF model training and testing
Instantiate RF model, then train and test it
Make predictions and evaluations
Infuse features from CNN layers into RF as input
Evaluate the hybrid CNN-RF model
Save model for deployment

Figure 3.4: Block diagram of the proposed CNN-RF model

To prepare the employed SGCC load profile for AI modelling and simulation, the dataset is first explored and then systematically preprocessed. The dataset is explored by launching an inquiry to seek further details about it and to verify whether it has missing values in it or not. The dataset is later preprocessed by replacing its missing values, scaling or normalizing its features, and balancing its classes.

3.3.1 Exploratory data analysis and data preprocessing

EDA is the foundation of any data analytics. Datasets must be cleaned before deploying them for ML predictions. EDA prepares the dataset for preprocessing. EDA and data preprocessing are the processes involved in cleaning up a dataset before applying any ML model to such dataset. Data cleansing is done to improve the quality of the dataset and to improve the accuracy of model predictions when an ML model is being applied to the dataset. Datasets are explored first during EDA to gain insights and uncover patterns so as to determine their characteristics. Later the explored datasets are preprocessed to enhance the training of the model applied to the datasets (Ali et al., 2023:1).

EDA is all about launching inquiry or digging deep into a dataset to reveal its true nature, gather general information about it, and then identify its characteristics that may need to be addressed during data preprocessing. EDA involves checking the shape of the dataset, checking for missing values in the dataset, and identifying relationships between variables found in the dataset, etc., to obtain valuable information or gain perception into the given dataset. EDA leads to data preprocessing after investigating what needs to be fixed in the dataset being explored.

The more the information gathered about a dataset, or how well a dataset is known during EDA determines how useful such dataset will be during analytics. Part of EDA also involves reformatting the dates in our SGCC dataset from the original DD/MM/YYYY date format to the new YYYY/MM/DD date format. This is in a bid for the date in the SGCC dataset to conform with the default date format of Google Colab, as implemented in Sections A.1.2.7 to A.1.2.11 of the Appendix. Other implementation processes which may not have been referred to in this chapter are all contained in the Appendix. Data preprocessing is done to refine the features in a raw dataset, in a bid to improve the quality of the dataset and also to enhance the performance and reliability of the ML models that are being applied to the dataset (Khan et al., 2024:6; Shahzadi et al., 2024:5-6; J. Wang et al., 2024:4; S. Zhu et al., 2024:15479).

Preprocessing of the SGCC dataset takes place before applying the model to the dataset. Although, the SGCC dataset has been examined during EDA to discover if there are missing values in it; however, the mathematical expressions which denote the process of checking and estimating the number of the missing values in the SGCC dataset is expressed in Section 3.3.1.1. The dataset is preprocessed by replacing its missing values and normalizing the features in the dataset (Arif et al., 2022:4; Mehdary et al., 2024:16; Nirmal et al., 2024:3; L. Zhu et al., 2024:259). The replacement of missing values, scaling or normalization, and resampling methods discussed in Sections 3.3.1.3, 3.3.1.4, and 3.3.1.5 respectively are all processes involved in data preprocessing for cleaning or purifying the employed dataset to remove the flaws in it (Khan et al., 2024:7).

3.3.1.1 Inspecting the dataset for missing values

The process of checking for missing features or values in the SGCC dataset can be represented mathematically below:

Let X represent the dataset features with $m \times n$ dimension as shown in Equation 3.3.

$$X = \begin{bmatrix} X_{11} & \cdots & X_{1n} \\ \vdots & \ddots & \vdots \\ X_{m1} & \cdots & X_{mn} \end{bmatrix} \quad \textbf{(3.3)}$$

Where $m =$ number of rows (samples), while $n =$ number of columns (features).

Let the feature or element in the $i - th$ row and $j - th$ column of the dataset be denoted as $X_{i,j}$. To check for the missing features in the dataset, an indicator function $I(X_{i,j})$ for each feature is defined in Equation 3.4. Indicator functions are used to check whether individual features or values are missing or not.

$$I(X_{i,j}) = \begin{cases} 1, & if\ X_{i,j}\ is\ a\ missing\ value\ or\ NaN \\ 0, & otherwise \end{cases} \quad \textbf{(3.4)}$$

Missing values or features in a specific row i and column j in the matrix of Equation 3.3 can be checked using Equations 3.5 and 3.6 respectively.

Missing values in row $i = \sum_{i=1}^{m} I(X_{i,j})$ **(3.5)**

Missing values in column $j = \sum_{i=1}^{n} I(X_{i,j})$ **(3.6)**

Where m and n are the total number of features in the $i - th$ row and $j - th$ column respectively. Equation 3.5 checks how many values are missing in row i, while Equation 3.6 checks for the number of missing values in the column j of the feature matrix of the SGCC electricity consumption dataset described in Equation 3.3. The total number of missing values or features in the entire dataset can be determined using Equation 3.7.

Total missing values $= \sum_{i=1}^{m} \sum_{j=1}^{n} I(X_{i,j})$ **(3.7)**

The total missing values in the entire dataset can be found by summing up the results of the indicator function over all elements in the feature matrix of Equation 3.3, by checking each cell individually across the rows and columns of the features, to produce a complete count of all the missing features in the entire dataset. Finding the missing features across the rows and columns separately provides the opportunity of iterating over each element or feature in the feature matrix of Equation 3.3 individually.

3.3.1.2 Interpolation method for replacing missing and undefined values

After establishing that there are missing features or values in the dataset as confirmed in Section 3.3.1.1, the next thing is to replace the missing values. Missing values in datasets lead to impairments in ML models, leading to wrong predictions (Munawar, Khan, et al., 2022:04; Appiah et al., 2023:1; Khan et al., 2024:7). To enhance the accuracy of the proposed CNN-RF model, it is essential to address the missing values. In the SGCC dataset, these missing values are replaced using linear interpolation, which assumes a linear relationship among the features in the dataset. Linear interpolation is a technique widely used in ETD literature for replacing missing values. It is a method used for determining values between two features in forward and backward directions, and enabling the connection of dots in a one-dimensional set of features (Huang, 2021:2). When a point falls between two others, linear interpolation helps estimate its value based on the surrounding points in the sequence. It is a way of smoothly filling in missing gaps in a dataset. In essence, linear interpolation fills in the missing values by utilizing the values of adjacent features. The linear interpolation function is represented by Equation 3.8 (Noor et al., 2014:279; Aldegheishem et al., 2021:25042). The linear interpolation function of Equation 3.9 is otherwise known as forward interpolation.

$$f\ (x) = f(x_0) + \frac{f(x_1) - f(x_0)}{x_1 - x_0}(x - x_0) \tag{3.8}$$

Where $(f(x_0), x_0)$ are the first coordinate features, while $(f(x_1)\ , x_1)$ are the second coordinate features. x is the point at which interpolation is to be performed, while $f\ (x)$ is the value obtained after interpolation. Generally, x is the independent variable, while x_0 and x_1 are the known values of the independent variables. $f\ (x)$ is the dependent variable which depends on independent variable x, while $f(x_0)$ and $f(x_1)$ are known values of the dependent variables. The interpolation technique expressed in Equation 3.8 involves forward and backward directions. This means that:

For forward interpolation, the condition $x_0 \leq x \leq x_1$ applies, and the estimated $f\ (x)$ at the x position within the range (x_0, x_1) based on the linear relationship between them is derived from the known values using Equation 3.8.

For backward interpolation, the condition $x_1 \leq x \leq x_0$ applies, and the estimated $f(x)$ at the x position within the range (x_0, x_1) based on the linear relationship between them is determined using Equation 3.9.

$$f\ (x) = \ f(x_1) + \frac{f(x_0) - f(x_1)}{x_0 - x_1}(x - x_1) \quad \textbf{(3.9)}$$

The conditions for forward and backward interpolations determine which method of the interpolations is to be used depending on the position of x relative to the known values. Forward interpolation is done using the values before the missing feature and works well when the missing values are closer to the starting point of the data series; while backward interpolation is done using the values after the missing feature and works well when the missing values are nearer to the end of the sample data series. Replacing missing values or features using backward or forward interpolation helps to improve the continuity and quality of the dataset. The linear interpolation approach has been considered to be easy and highly computationally efficient. Generally, the method outperforms non-linear interpolation techniques for predicting missing values with constant rates (Lepot et al., 2017:3). Essentially, the robustness and lower computational demand of linear interpolation method, owing to the regularly spaced features informed the choice of the technique.

3.3.1.3 Normalization of features

After passing through the interpolation stage to fill up the missing values, data normalization is required next to recalibrate the inconsistent independent-feature values in the dataset (Khan et al., 2024:9). Normalization is the process of scaling the independent features in the data frame to a suitable span of values to increase the rate of convergence and time of execution of ML models (Huang et al., 2024:11; Khan et al., 2024:8). With normalization, features in datasets are pegged to the same scale for numerical uniformity, such that each of the feature in the data frame is as important as another, thereby removing the weights on variables with large range, thus reducing feature dominance and ascertaining fair contributions from features, so as to alleviate the effect of outliers, and produce a restructured dataset which ML models can process more easily without any bias (Pamir, Javaid, Qasim, et al., 2022:56867; Khan et al., 2024:7). Like a typical deep learning model, CNN model is sensitive to unscaled diverse data (Pamir, Javaid, Qasim, et al., 2022:56867). Normalization of features is generally important and is required by many ML models to enhance convergence speed, to stabilize training process, and to improve performance (Liao, Zhu, et al., 2024:5077).

Minimum-maximum normalization technique also known as MinMaxScaler, which is used to transform features typically to values between 0 and 1 has been used to scale the features in the SGCC data frame (Badawi et al., 2022:5; Lepolesa et al., 2022:39647). After normalization, the independent features in the dataset are kept to a minimum and maximum threshold of 0 and 1 respectively. MinMaxScaler has been adopted for this research project as against other scaling methods like StandardScaler, RobustScaler, MaxAbsScaler, and QuantileTransformer, because it produced the best model performance when used with the employed dataset. However, MinMaxScaler is most proficient when dealing with scale-sensitive models like neural networks and algorithms which are based on gradient descent (Cheng et al., 2021:7; Guizeni, 2024).

The MinMaxScaler method for normalizing features in the data frame is expressed in Equation 3.10 (Huang et al., 2024:11; Liao, Zhu, et al., 2024:5077; Mehdary et al., 2024:16; Nirmal et al., 2024:3).

$$N(X) = \frac{X_P - \min(X)}{\max(X) - \min(X)} \quad \textbf{(3.10)}$$

Where $N(X)$ is the min-max scaling function that scales each feature in every column X of the SGCC data frame where the original input feature X_P to be scaled is located, $\min(X)$ is the original minimum value in each column X, while $\{\max(X)\}$ is the original maximum value in the particular column X. The MinMaxScaler technique substracts the original minimum value $\{\min(X)\}$ from the original value of each feature X_P to be scaled in column X, and then divides it by the range $\{\max(X) - \min(X)\}$, to give scaled evaluation value that lies between 0 and 1, providing linear transformation and keeping relationship among original data range in every column X being normalized (Patro & Sahu, 2015:20), while also preserving the shape of the original dataset (Singh & Singh, 2022:1). Range is the difference between the original maximum and the original minimum values of the features in each feature column X of the data frame for every feature X_P in a particular column that is to be scaled or normalized. All the features in all the the X columns (a total of 1,034 feature columns) of the SGCC data frame are hereby scaled accordingly using the MinMaxScaler technique, such that every input feature or independent variable in the data frame are normalized to values that range between a minimum of 0 and a maximum of 1.

3.3.1.4 Balancing the classes in the dataset

Imbalanced datasets contain uneven distribution of class labels (L'Heureux et al., 2017:7779). Without balancing the classes in the employed real dataset from SGCC, models trained using the dataset will tend to overfit and thus leading to a bias towards the majority class (Yang et al., 2023:3; S. Zhu et al., 2024:15483). Overfitting occurs when a model fails to generalize to unseen or test data, but rather learn patterns that are too specific to the training data, thus having high training accuracy but poor test accuracy. The two classes in the SGCC dataset are the theft or positive and non-theft or negative classes containing daily electricity consumption features. It is obvious from Section 3.2.2 during the description of the employed dataset that the numbers of customers who did not steal electricity (majority class) are overly more than those customers who stole electricity (minority class), giving rise to an imbalanced dataset that needs to be resampled in order to balance it.

For ML models to effectively classify labelled datasets, a more-effectual method is to oversample the under-represented samples in the dataset by generating artificial samples to supplement the minority samples to equal the size of the majority samples in order to balance the class distribution within the dataset (Ghori et al., 2021:98931). A class balancing method known as the synthetic minority oversampling technique (SMOTE) has been utilized to oversample the minority theft samples, thereby addressing the class imbalance issue in the SGCC dataset. SMOTE is a very reliable, powerful, and the most prominent oversampling technique which has been utilized by many researchers to handle imbalanced-dataset problems (Elreedy et al., 2024:4903-4904). SMOTE generates artificial samples of the minority class by interpolating the minority samples and the nearest neighbours of the minority samples in an effort to balance the distribution of classes in the dataset (Pereira & Saraiva, 2021:3).

Another means of balancing the classes in the highly imbalanced SGCC dataset is to undersample the majority class to match the size of the minority class. However, oversampling of the minority class has been considered in this research since undersampling the majority class may be counterproductive owing to the lower proportion of the available theft samples when compared with the non-theft samples (Javaid, Jan, et al., 2021:49). Since the employed dataset is severely imbalanced, reduction in the magnitude of the majority non-theft instances using undersampling technique will be sizeable, which will severely truncate more of the representations of the customer samples under the non-theft class, leading to loss of vital information (Ghori et al., 2021:98931). This will thereby reduce the quality of the employed SGCC dataset and thus increase the risk of overfitting by the model developed with such dataset which has been diminished through undersampling. Data-quality reduction will undermine the learning and performance efficacy of the ML model that would later be trained with the undersampled dataset (Javaid, Jan, et al., 2021:49).

However, ML models typically perform better when trained with big datasets (Ramezan et al., 2021:19; Ghosh, 2023), so a reduction in dataset size by undersampling may hamper the performance of the proposed model. Consequently, the employed SGCC dataset has therefore been appropriately oversampled using SMOTE to balance the dataset. In general, imbalanced datasets severely affect the performance and reliability of ML models (Pamir et al., 2023:3580; Liao, Bak-Jensen, et al., 2024).

- **Oversampling using the SMOTE algorithm**

To demonstrate the processes involved using the SMOTE algorithm, let D be the employed dataset with samples and labels, where $D = \{(X_i, y_i), \left(X_{i+1}, y_{i+1}\right), \dots, (X_N, y_N)\}$ as illustrated in Equation 3.4, and y_i is the class label of the $i - th$ customer sample X_i in the dataset. The SMOTE oversampling technique for generating synthetic samples in an imbalanced dataset is applied to the minority class and involves identifying the minority class, selecting the minority class, finding the k-nearest neighbour of the chosen sample within the minority class, generating the synthetic samples of the minority class by oversampling a subset of the minority samples, and adding the generated synthetic samples to the dataset based on the steps described in Farid et al. (2023:83) and Elreedy et al. (2024:4907), as illustrated in the subsequent paragraphs.

The SMOTE oversampling process starts with identifying the minority class in the dataset by finding the class with the minimum or fewest number of samples. This is achieved using Equation 3.11.

$$C_{min} = arg\ \min_c \ |\ \{i: y_i = c\}\ | \qquad \textbf{(3.11)}$$

Where C_{min} is the class that has the minimum number of samples in the dataset (minority class), $arg\ \min_c$ is a notation which indicates that the argument or value of a specific class (minority class) c that minimizes the given expression | $\{i: y_i = c\}$ |, while the expression

| $\{i: y_i = c\}$ | itself represents the absolute value of the minority-class samples (c) in the dataset for which the class label y_i is equal to c.

After determining the minority class samples using Equation 3.11 above, then a subset of the minority class samples which will be used to generate the synthetic data samples is chosen at random. After this, a sample instance X_i from the subset of the selected minority samples is chosen, where $y_i = C_{min}$.

The k-nearest neighbours for each sample X_i from the randomly selected subset of the minority class are determined next using Euclidean distance between the minority class samples. The Euclidean distance equation expressed in Equation 3.12 is used to determine the k-nearest neighbours between the minority sample X_i and another sample X_j from the feature space of the minority class.

$$d(X_i, X_j) = \sqrt{\sum_{m=1}^{n} (X_{i,m} - X_{j,m})^2} \tag{3.12}$$

Where $d(X_i, X_j)$ is the Euclidean distance between the two samples X_i and another sample X_j in the feature space of the minority class, m is the feature index, while n is the total number of features in the feature space of the minority class. The value of k determines the numbers of nearest neighbours that will be considered for interpolation. For the purpose of interpolation to generate synthetic samples, one of the k-nearest neighbours is chosen at random. The k-nearest neighbours of sample X_i are being determined from the set $\{X_j : y_j = C_{min}, j \neq i\}$. This set consists of all samples or feature vectors X_j that belong to the minority class ($y_i = C_{min}$) except the X_i sample which is critical for selecting the nearest neighbours. The set is used to obtain the k-nearest neighbours of the feature vector X_i within the minority class, with the goal of generating synthetic samples by interpolating between X_i and its neighbouring data points within the set.

Next is the generation of the synthetic samples. For each nearest neighbor X_j, synthetic samples are being generated along the line connecting the minority class sample X_i and one of its randomly chosen nearest neighbour X_j. This is done to keep the newly generated synthetic sample within the region of the minority class samples. The synthesized sample is generated by selecting a neighbour X_j from the previously mentioned set $\{X_j: y_j = C_{min}, j \neq i\}$. Therefore, the newly generated synthetic sample is represented in Equation 3.13.

$$X_{new} = X_i + \lambda \cdot (X_j - X_i) \quad \textbf{(3.13)}$$

Where X_{new} is the newly generated synthetic sample between a minority class sample X_i and one of its nearest neighbours X_j, while λ is a unique random number that ranges between 0 and 1 (i.e., $0 \leq \lambda \leq 1$), which is a parameter that determines the position of the newly synthesized data point between X_i and X_j. If $\Delta = X_j - X_i$, then Equation 3.13 becomes:

$$X_{new} = X_i + \lambda\Delta \quad \textbf{(3.14)}$$

Finally, all the newly generated synthetic samples are being appended or added into the default dataset**.** It should be noted that if $\lambda^* \geq 1$**,** SMOTE will allow for extrapolation beyond the standard interpolation range of the minority class samples on the line connecting the sample X_i and its randomly selected neighbour X_j. With $\lambda^* \geq 1$, SMOTE will generate more diverse minority samples outside the original range or feature space (i.e., $0 \leq \lambda \leq 1$) of the minority class samples, with greater risk of generating noisy and unrealistic samples.

3.3.2 Development of the Conv1D CNN model

After the data preprocessing stage discussed in the previous sections, the next stage of the ETD modelling is feature engineering, which involves feature selection and feature extraction (Khan et al., 2024:6). For effective ETD, selection of appropriate features is required to develop a formidable model (Khan et al., 2024:9). There are three types of CNN model namely one-dimensional CNN (Conv1D or 1D-CNN), two-dimensional CNN (Conv2D or 2D-CNN), and three-dimensional CNN (Conv3D or 3D-CNN) (Verma, 2019).

Basically, the most common type of the CNN model is Conv2D which is primarily used for the classification of images (Verma, 2019; Brownlee, 2020). Conv2D requires two-dimensional input data and a corresponding two-dimensional kernel or filter. Conv3D requires three-dimensional input data, for example, a three-dimensional image or video and a corresponding three-dimensional kernel or filter. Conv1D requires one-dimensional input data (e.g. text or time series) and a corresponding one-dimensional kernel or filter. Conv1D is primarily used with one-dimensional data like the employed SGCC time-series dataset used in developing the proposed ETD model. The Conv1D network defines the CNN architecture used to train the employed one-dimensional (1D) SGCC time-series dataset for binary classification. Conv1D model is chosen as against Conv2D or Conv3D CNN models because the electricity consumption dataset used in constructing the ETD or NTLD model is a one-dimensional dataset (Cheng et al., 2021:5; Chung & Jang, 2022:9).

The Conv1D model architecture is built and configured such that the model can accept input features and also suitable for binary classification to distinguish between the honest and fraudulent electricity customers. Using the Sequential API in a neural network framework like TensorFlow and Keras involves a series of steps. This ETD model demonstrates an example of a 1D-CNN model using Sequential API in Keras. Figure 3.5 represents the architecture of the Conv1D model. The architecture of the CNN model includes a convolutional layer (Conv1D layer), pooling layer (MaxPooling1D layer), flatten layer, fully connected (FC) layer or dense layer, dropout layer, and an output layer. The model training is monitored for accuracy and loss over epochs.

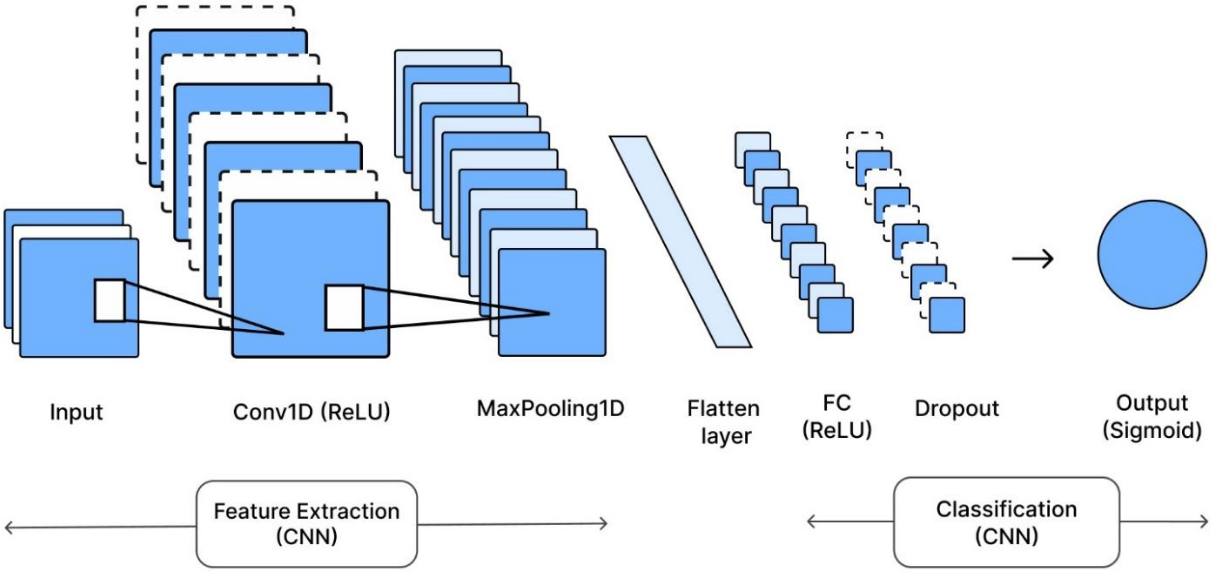


Figure 3.5: Architecture of the Conv1D CNN model

The choice of 32 neurons with kernel size of 3 for the Conv1D model is a common starting point for Conv1D layers, especially in the early layers of CNN. Size-3 kernels are noted for their high polarization exponents and have the lowest decoding complexity among larger kernels (Ardakani et al., 2021:919). These choices are often used as defaults in many architectures and have been found to work well across various tasks, and they strike a balance between computational efficiency and model complexity for capturing patterns in a sequential data. Kernel size specifies the dimension of the array of weights in the kernel. The specified array of weights determines the length of the kernel. A filter is a collection of kernels (Panchal, 2021). Other hyperparameters of the Conv1D model are 50 epochs, and 30 batch size of training samples. The input layer of 1D-CNN is denoted by the application of a Conv1D operation on the 1D input data. In this model setup, the CNN learns from the one-dimensional SGCC time-series electricity consumption data by extracting and training features from the dataset.

A kernel is a matrix of numbers or weights that convolves or slides over the input tensor to extract features and produce a feature map (Ganesh, 2019; Wen et al., 2021:1641; Panchal, 2021). During convolution to extract features, the array of input features or a local receptive field covered by the kernel window are multiplied by the kernel weights, in an elementwise manner and then later summed up to produce a feature map. A feature map is the result or output of a convolution operation by a kernel or filter over an entire dataset. A kernel size of proper length is preferred to obtain a high-quality representation to capture the salient features in a time series data. For time series classification task using 1D-CNN, the selection of kernel size is critically important to ensure the model can capture the right-scale salient features from a long time series input data. Most of the existing work on 1D-CNN treats the kernel size as a hyperparameter and tries to find the proper kernel size through a grid search which is time consuming and inefficient.

For 1D-CNN models, the selection of kernel size is essential to capture the required salient features properly. Since the employed SGCC dataset has only one feature at each time point or time step, thus each filter in the Conv1D model will also consist of one kernel. However, the 32 neurons mentioned in the previous paragraph directly relates to the number of filters in the Conv1D network. Therefore, the convolutional layer of the Conv1D model applies 32 1D convolutional filters, each of size 3 at the same time to the input data during convolution. One-dimensional kernel is typically used to process one-dimensional input data. Hence, the one-dimensional kernel size 3 or filter size 3 (3-element kernel) used in the Conv1D model is an array of weights of length size 3, capturing three consecutive adjacent features at a time from the input data, and extracting features by processing these captured sequential input data features which a kernel or filter would convolve or slide over.

Forward propagation and backward propagation or backpropagation are the two essential steps a neural network goes through during training. The first stage of training a neural network is the forward propagation phase before the later backward propagation stage (Medium, 2023). In the forward propagation phase, the input data is supplied into the network, and the output is thereby calculated by traversing the input across several layers. The observed or predicted output is then compared with the target output. The difference between the target and the observed output is used to calculate the error in the Conv1D network. In backward propagation, the calculated error at the output layer is propagated back through the network, and the neuron weights are updated iteratively to minimize the computed error (Jaokar, 2019). The architecture and backpropagation of a neural network during training is guided based on the nature of the classification task (Ali et al., 2023:12).

3.3.2.1 Forward propagation

Forward propagation in CNN is the process of passing the input feature vectors through the CNN network layer by layer, whereby the input features are being transformed before being passed from one layer to the next to produce an output at the final layer (Jaokar, 2019). Figure 3.6 depicts a simple representation of one complete-forward propagation cycle through the Conv1D architecture shown in Figure 3.5. Figure 3.6 consists of the input, hidden, and output layers made of neurons or nodes. The total losses or errors in the Conv1D network are computed during the forward pass. The input layer involves feeding the input data into the network, the hidden layer processes the input data, such that each layer in the hidden layer applies activation functions to a set of weights and biases, while the output layer produces the final predictions also known as processed data.

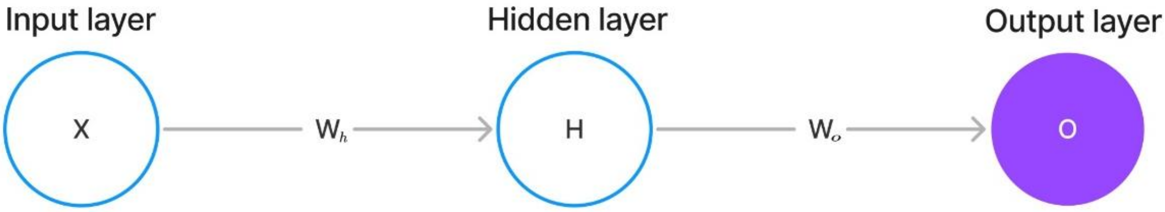


Figure 3.6: Forward propagation in the Conv1D network

The term W_h in Figure 3.6 describes the weights of all the neurons in the hidden layer, while W_o represents the weights of all the neurons in the output layer. Apart from the input layer which constitutes the customer feature vectors from the employed one-dimensional (1D) time-series electricity consumption data with their target labels, and the output layer that displays the final prediction of the binary classification, the hidden layer of a CNN model is composed of convolutional, pooling, flatten, dropout, and the FC or dense layers. At the input layer before convolution, the 1D input data which had only sequence length as its dimension is eventually transformed into a three-dimensional (3D) tensor with the shape (batch size, sequence length, and number of features or time steps), before it is being fed into the Conv1D network (MathWorks, 2021). The batch size is the number of samples or data points that will be fed into the Conv1D network at once, the sequence length is the number of features contained in each feature vector sample, while the number of features in this case correspond to the count of the type of features contained in a time step. The employed SGCC dataset contains one kind of feature (i.e., energy consumptions in kWh) per time step. Since the input data is a univariate time series data containing one kind of feature, therefore the number of features at time steps in the employed dataset is one. Conceptually, the input data is still a 1D data but which has been structured into a 3D tensor that the Conv1D network can process. This is to allow the model to process data samples in batches with multiple features at the same time.

- **Convolutional layer**

The convolutional layer is depicted as Conv1D in the Conv1D model shown in Figure 3.5. The function of the convolutional layer is to extract local features from the input data and convolve them into feature maps using kernels or filters (Yang, 2019:151-152). Convolution operation takes place in the convolutional layer of the Conv1D network using the one-dimensional electricity consumption input data and kernel weights. The convolution is carried out with the neuron of each kernel which processes the score of the convolution operation as described in Equation 3.15 (Zheng et al., 2018:1609; Bohani et al., 2021:3; Cheng et al., 2021:5; Saripuddin et al., 2021:153; Nawaz et al., 2023:5).

$$z_{j(c)} = \sum_{i=1}^{n} w_{i(i),j(c)} \circledast x_{i(i)} + b_{j(c)} \qquad \textbf{(3.15)}$$

Where:

$z_{j(c)} =$ Weighted sum processed by the $j-th$ neuron of the kernel or filter at the convolutional layer,

$w_{i(i),j(c)} =$ The weight of the $j-th$ kernel at the convolutional layer applied to the $i-th$ input feature $x_{i(i)}$ at the input layer,

$x_{i(i)} =$ The $i-th$ input feature from the input layer to the $j-th$ neuron of the kernel in the convolutional layer,

$b_{j(c)} =$ Bias term of the $j-th$ neuron at the convolutional layer,

$n =$ The total number of $i - th$ input features connected to the $j - th$ neuron.

The $w_{I(i),j(c)}$ and $b_{j(c)}$ are learnable parameters and also the stored information in the network (Ullah et al., 2021:6; Lepolesa et al., 2022:39641), while the product between $w_{i(i),j(c)}$ and $x_{i(i)}$ (i.e., $w_{i(i),j(c)} * x_{i(i)}$) is the convolution operation that took place in the convolutional layer of the Conv1D network between the input features and the kernel weights (Ullah et al., 2021:6). The sum of the convolutions as processed or computed by the $j - th$ neuron of each kernel in the convolutional layer, with the addition of the bias term of the kernel produces the weighted sum. The weighted sum is also known as linear combination of inputs. A single weighted sum as processed by the $j - th$ neuron of a kernel in the Conv1D network during convolution produces a single value in the eventual feature map that the kernel will generate across the whole dataset. Typically, a convolutional layer contains multiple kernels where each kernel matrix produces its own feature map by sliding or convolving through the entire input data.

Unlike weights which are transmitted between neurons, biases or bias terms are not transmitted. Bias terms are additional constant parameters or values which are specific to every neuron and are being added after applying the weights to the input data during convolution, to compute the weighted sum. This is done to shift or offset the output of the neuron, to enable the neuron learn patterns, and also enhance the model to fit to the input data (Ganesh, 2020; Turing, 2022). The convolution operation produces a 3D feature map (Dertat, 2017) having the shape (batch size, output length, and number of filters or depth). The batch size is the number of samples or data points fed into the Conv1D network at once, the output length or the new sequence length is the number of features in each feature vector of every input sample after the convolution operation, while number of filters which corresponds to the number of channels or number of neurons refers to the total number of convolutional filters used in the Conv1D network.

Besides convolution, another procedure that is very crucial to the convolutional layer is the activation of the weighted sums using activation functions, as both the convolution and activation processes forms a combined functionality. Activation functions decide which features are passed on to the next layer of the Conv1D network and which ones are dropped (Iftikhar et al., 2024:07). The weighted sum of each feature from the input data as processed by each $j - th$ neuron of the 32 neurons at the convolutional layer in the Conv1D network are activated using activation functions. Offsetting the convolved input by adding the bias term allows the shifting of the input to the activation function, to help in determining whether a neuron activates or not even when the input is zero. The bias term combines with the activation function to enhance nonlinearity, so that neurons can be more flexible to learn complex patterns, and thereby improve model performances (Ganesh, 2020; Turing, 2022). Equation 3.16 (Ullah et al., 2021:6; Lepolesa et al., 2022:39641; Ullah et al., 2022:18685) is the output of the $j-th$ neuron out of the 32 filter neurons after applying activation function to the weighted sum $z_{j(c)}$ of Equation 3.15:

$$u_{j(c)} = R\left(z_{j(c)}\right) \tag{3.16}$$

Where:

$u_{j(c)} =$ output of the $j-th$ neuron at the convolutional layer after the activation calculation,

$R =$ Rectified Linear Unit (ReLU) activation function.

Activation functions are transformation functions that are used to squeeze or manipulate the weighted inputs in neurons to generate outputs, by deciding whether the neurons should be fired (activated) or not (Iftikhar et al., 2024:07). The activation process is like inspecting and determining whether the provided input information into the neuron is relevant in the prediction process or should be ignored. The ReLU activation function like other nonlinear activation functions like softmax, maxout, Swish, hyperbolic tangent (tanh), sigmoid or logistic activation functions, and ReLU variants like Leaky ReLU (LReLU), Exponential Linear Unit (ELU), and Parametric ReLU (PReLU) activation functions introduce nonlinearity in the Conv1D model (Pamir et al., 2023:3581; Khan et al., 2024:10).

ReLU activation function is the state-of-the art activation function (Montesinos López et al., 2022:389), and it is chosen among other nonlinear activation functions because it allows models to learn faster (i.e., faster model training and computation), performs better than other activation functions, increases nonlinearity, favours backpropagation, and is devoid of the issues of exploding and vanishing gradients attributable to sigmoid and tanh activation functions (Saripuddin et al., 2021:153; Gao et al., 2022; Ullah et al., 2022:18686; Khan et al., 2024:10). Nonlinear activation functions are required by deep learning models to convert linear inputs to nonlinear outputs in a bid for the model to learn complex tasks and transform the input to perform better (Kiliçarslan & Celik, 2021:1). Essentially, for the given weighted input $z_{j(c)}$ from the feature map, the ReLU activation function to activate the $j-th$ neuron at the convolutional layer using the weighted sum calculated by the $j-th$ neuron in Equation 3.15 is described in Equation 3.17 (Ullah et al., 2022:18686; Nirmal et al., 2024:3), or otherwise expressed using the equivalent piecewise function given in Equation 3.18 (Lepolesa et al., 2022:39643; Huang et al., 2024:8).

$$R\left(z_{j(c)}\right) = \max\left(0, z_{j(c)}\right) \tag{3.17}$$

$$R\left(z_{j(c)}\right) = \begin{cases} 0, & z_{j(c)} \leq 0 \\ z_{j(c)}, & z_{j(c)} > 0 \end{cases} \tag{3.18}$$

Where the $z_{j(c)}$ (the weighted sum processed by the $j - th$ kernel neuron) in the ReLU activation function of Equation 3.17 or Equation 3.18 is determined using Equation 3.15 (Cheng et al., 2021:5), before applying the ReLU activation function to it as demonstrated in Equations 3.16, 3.17, or 3.18. The ReLU activation function maps the weighted sums that are equal or less than zero to zero and retains the weighted sums which are greater than zero.

- **Pooling layer**

The pooling layer is a subsampling layer in CNN used to minimize redundant features in the network (Xia et al., 2022:291). After applying activation function to the feature maps, the resulting features of the Conv1D network can further be downsampled by pooling (Ullah et al., 2021:6). Pooling is done to further transform (downsample) the kernel outputs (feature maps) after the application of activation function to the feature maps. The pooling layer is used to obtain dominant features from the local convolved features by condensing the numeric arrays generated by the kernels, and thereby reducing the dimensionality of feature maps while retaining the most important features (Kumar, 2023; Khan et al., 2024:9). Pooling reduces the dimensionality of feature maps in space, thereby reducing the number of parameters that the Conv1D model needs to learn (Kumar, 2023). This thereby controls overfitting and shortens the training time of the model (Kumar, 2023). Maximum pooling (max pooling) and average pooling are the two available types of pooling methods, but max pooling performs better than average pooling (Ullah et al., 2021:6; Ullah et al., 2022:18686). Max pooling returns the maximum values of the activations in the small windows of a feature map, while average pooling returns the average activation values in the small windows (Li et al., 2019:6; Ullah et al., 2021:6).

Max pooling is the most common type of pooling used in reducing the dimensionality of feature maps to reduce computational complexity and increase execution time (Ullah et al., 2021:6). MaxPooling1D has been adopted in the Conv1D network for pooling the features in the feature map. MaxPooling1D is used in this work for pooling because the input data is a 1D dataset. Unlike average pooling that returns average values from each pooling window, max pooling decreases feature-map dimensions by extracting or returning the maximum values or the most dominant features of the features in each pooling window of the feature map. The small window mentioned in the previous paragraph is actually a pooling window. The pooling window used for Conv1D model has a size of 2 with a stride length of 2. The size-2 pooling window considers two elements or features at a time in the feature map and selects the maximum of the two. Stride is the step size or units of the movement of the pooling window at a time across the adjacent elements in the feature vector (Kumar, 2023). Since the stride length of the pooling window is 2, it means that the pooling window moves two steps at a time across the elements in the feature vector during the pooling without overlapping. Using the employed input 1D time series data, the pooling equation after applying MaxPooling1D layer to the Conv1D network is described in Equation 3.19 (Li et al., 2019:6; Liao et al., 2022:3519-3520; Gunduz & Das, 2024:10; Liao, Zhu, et al., 2024:5080).

$$Y_l = \max_{k \in W_l} M_K \qquad \textbf{(3.19)}$$

Where:

$Y_l =$ Output of the max-pooling operation at position l in the feature map,

$W_l =$ The pooling window for the set of input features or activations around position l,

$\max =$ Max-pooling operation that takes the maximum value from the pooling window W_l,

$\mathrm{k} =$ Set of features in the pooling window W_l,

$M_k =$ The values of k input features from the feature map M within the window W_l.

Applying MaxPooling1D, the maximum value in a specified window of the feature map is selected and taken to the next layer of the Conv1D network, while the other is dropped. The pooling operation only downsampled the size of the feature map after the convolution operation, but the pooled feature map retains its 3D shape.

- **Flatten layer**

The output of the classification process is expected to be in one-dimensional (1D) binary format. Meanwhile, the shape of the pooled feature map is in a three-dimensional (3D) tensor as mentioned earlier, but the next layer after the flatten layer known as the fully connected layer requires the feature map to be in a 1D feature vector (Dertat, 2017; Yang, 2019:152), so that the FC layer can interpret the feature map correctly before the output layer finally makes the classification. Therefore, the flatten layer reshapes or rearranges the multidimensional 3D feature-map array into a 1D high-dimensional vector appropriate for the fully connected layer (Yang, 2019:155-156; Ullah et al., 2022:18686; L. Zhu et al., 2024:260). Flattening of the feature-map matrix for each filter can be done by stacking each matrix of the 3D tensor in a sequential order to form a 1D tensor (Yang, 2019:156). The flatten layer is non-parametric, that is, it does not learn any parameter but only modify tensors. The flattening of the 3D feature map from the max pooling layer into a 1D feature vector can be represented in Equation 3.20.

$$F_{fl} = \text{flatten}\ (Y_l) \tag{3.20}$$

Where:

$F_{fl} =$ Flattened feature vector,

$Y_l =$ The pooled 3D feature map from the MaxPooling1D layer,

$\text{flatten} =$ Operation that flattens the pooled 3D feature map into 1D feature vector.

It should be noted that what the flatten layer only does is structural rearrangement or reshaping of the input tensor (i.e., flattening is simply about dimension rearrangements) without any information or feature change, as the information in the feature map is retained in the transformed 1D feature map used as input to the fully connected layer in the Conv1D network.

- **Fully connected layer**

The FC layer is also known as the dense layer (Pamir, Javaid, Javaid, et al., 2022:11). This layer outputs the latent features extracted by the convolutional layer before the output layer makes the eventual classification (W. Liao et al., 2022:3520). The flattened 1D feature map from the flatten layer, which is the appropriate tensor for the final classification at the output layer, is fed into the FC layer (Yang, 2019:156). The FC layer contains the aggregate result of all the features across the entire inputs of the Conv1D network, providing a global representation of the input features and interpreting these features for the sake of final classification at the output layer (Ullah et al., 2022:18687). Each neuron in the FC layer is connected to every other neuron in the previous layer (flatten layer), that is the reason the

FC layer is referred to as being “fully connected” (Liu & Zhao, 2023:13854). In short, the FC layer combines all the features learnt in the previous layers and maps them to the output space for final classification. Equation 3.21 represents the weighted sum of a $j-th$ neuron at the FC layer (Ullah et al., 2021:6; Ullah et al., 2022:18687).

$$z_{j(fc)} = \sum_{i=1}^{n} w_{i(fl),j(fc)} \cdot z_{i(fl)} + b_{j(fc)} \tag{3.21}$$

Where:

$z_{j(fc)} =$ Weighted sum of a $j-th$ neuron at the fully connected layer,

$w_{i(fl),j(fc)} =$ Weight between the activated $i-th$ neuron at the flatten layer and the $j-th$ neuron at the fully connected layer,

$z_{i(fl)} =$ The activated $i-th$ input from the flatten layer,

$b_{j(fc)} =$ Bias term of the $j-th$ neuron at the fully connected layer,

$n =$ The total number of flattened activated $z_{i(fl)}$ inputs from the flatten layer to j neurons at the fully connected layer,

The activation of the $j-th$ the neuron at the fully connected layer is represented in Equation 3.22.

$$u_{j(fc)} = R\left(z_{j(fc)}\right) \tag{3.22}$$

Where:

$u_{j(fc)} =$ Output of the $j-th$ neuron at the fully connected layer after applying the activation function,

$R =$ ReLU activation function.

The ReLU activation function to activate the $j-th$ neuron at the fully connected layer using the calculated weighted sum by the $j-th$ neuron as described in Equation 3.21 is expressed in Equation 3.23.

$$R\left(z_{j(fc)}\right) = \max\left(0, z_{j(fc)}\right) = \begin{cases} 0, & z_{j(fc)} \leq 0 \\ z_{j(fc)}, & z_{j(fc)} > 0 \end{cases} \tag{3.23}$$

- **Dropout layer**

The dropout layer can be implemented to nodes or neurons at the input layer or nodes located anywhere within the hidden layer, except to the nodes at output layer (Dertat, 2017; Yadav, 2022; Pansambal & Nandgaokar, 2023:716, 718). However, dropout layer is usually implemented between the FC layer and the output layer, to drop or retain the activated nodes at the FC layer (Park & Kwak, 2017:189-190). The dropout layer performs better when it is positioned between the fully connected and the output layer. Dropout operation occurs at the dropout layer but it affects the neurons at the preceding FC layer. Of all the techniques used for regularizing neural networks, dropout is the most common because it performs better than other regularization techniques and it is easier to implement (Dertat, 2017; Park & Kwak, 2017:189-190). The dropout layer regularizes the model by randomly deactivating or dropping some neurons from the previous layer during training by turning off their activations to prevent overfitting (Iftikhar et al., 2024:07; Khan et al., 2024:9, 13). This layer also tends to improve the generalization of neural network models by increasing their accuracies (Dertat, 2017). The dropout equations for the Conv1D network which has been deduced from the principles described in Srivastava et al. (2014:1930-1934) and Goodfellow et al. (2016:258-262) is depicted in Equations 3.24 and 3.25. Dropout is done by retaining or dropping some of the activated neurons at the fully connected layer during the forward pass, at a particular training epoch.

$$u_{j(dr)_{[scaled]}} = \frac{1}{1-P}\left(u_{i(fc)} \odot a_{i(dr)}\right) \qquad \textbf{(3.24)}$$

Where:

$u_{j(dr)_{[scaled]}} =$ Scaled output at the dropout layer after performing dropout operation on the $i-th$ input activation $u_{i(fc)}$ from the FC layer,

$u_{i(fc)} =$ The $i-th$ input activation to the dropout layer from the FC layer before applying the binary mask to drop or retain the activation,

$a_{i(dr)} =$ The dropout mask at the dropout layer applied to the $i-th$ input activation $u_{i(fc)}$ from the FC layer to either drop or retain the activation,

$P =$ Dropout probability or dropout rate.

The element-wise multiplication between $u_{i(fc)}$ and $a_{i(dr)}$ $\left(u_{i(fc)} \odot a_{i(dr)}\right)$ as shown in Equation 3.24 is the dropout operation that took place at the dropout layer which accounts for the application of a random binary mask $a_{i(dr)}$ (where $a_{i(dr)} \in \{0,1\})$ to the activations from the FC layer during training, to determine which activation from the FC layer should be dropped or retained. The term $\left(\frac{1}{1-P}\right)$ in Equation 3.24 is the scaling factor that normalizes the output activations when the dropout mask is being applied to the activations from the FC layer during training. This is to compensate for the dropped activations, to ensure that the expected value of the output from the FC layer does not change during testing when the binary mask must have been deactivated. The binary mask $a_{i(dr)}$, which is applied to the activation $u_{i(dr)}$ at the dropout layer (from the FC layer), is generated at the dropout layer, to determine the eventual output of the activations from neurons at the FC layer. The mask keeps the activations from the neurons of the FC layer when its value is 1 and disable or drop them when its value is 0. The mask $a_{i(dr)}$ has the same shape as $u_{i(fc)}$, and it is generated randomly and multiplied elementwise with $u_{i(fc)}$. In another convention, the term $\left(\frac{1}{P}\right)$ could be used as the scaling factor. In this case, P will be called keep probability (i.e., probability of keeping an activation from a neuron active) instead of the dropout probability (or probability of dropping an activation) used in Equation 3.24. In general, scaling factor ensures that the expected values of activations remain the same during training (when the binary mask is deployed) and during testing (when the binary mask is deactivated).

The dropout rate or dropout probability of neurons at the dropout layer in the CNN model is set at 0.4, which is equivalent to a dropout rate of 40%. This signifies that 40% of the activations from the FC layer are being disabled during the forward pass to prevent overfitting, while only the remaining 60% contribute to the output. The dropout is done randomly at every epoch or iteration during training to prevent model overreliance on a few numbers of activations from the neurons at the fully connected layer (Dertat, 2017; Yadav, 2022). This in a bid to compel each node in the network to operate independently and unrestrictedly, to allow all neurons in the network contribute in generating the output, to improve the performance of the model (Dertat, 2017). Dropout is only activated during training and disabled during testing. The 1 or 0 value of the dropout mask or binary mask is determined if the random number generated by a random number generator (which uses a Bernoulli distribution) for the $i-th$ activation from a neuron at the FC layer during training is greater or lower than the dropout rate (Yadav, 2022; Pansambal & Nandgaokar, 2023:718). The value of the binary mask becomes 1 if the generated random number is greater than the dropout rate and becomes 0 if otherwise.

- **Output layer**

The last layer of the Conv1D model is the output layer, which is meant to predict theft and non-theft cases (Shahzadi et al., 2024:11). For the Conv1D model, ReLU activation function is applied to all other layers within the hidden layer of the CNN network, except the output layer where sigmoid activation function is used (Iftikhar et al., 2024:07). The prediction expected of the CNN model is a probability score that ranges between 0 and 1, indicating a no-theft or theft instance, which falls perfectly under the binary classification task. For the binary classification at the output layer, the sigmoid activation function is employed because it is the only activation function that is capable of mapping any input to values between 0 and 1, and is well-suited for tasks involving binary classifications, as against the softmax activation function which is used for multiclass classifications (Montesinos López et al., 2022:391; Ali et al., 2023:13). The weighted sum of each neuron at the output layer is represented in Equation 3.25.

$$z_{j(o)} = \sum_{i=1}^{n} w_{i(fc),j(o)} \cdot u_{i(fc)} + b_{j(o)} \tag{3.25}$$

Where:

$z_{j(o)} =$ The output or weighted sum of the $j-th$ neuron at the output layer,

$w_{i(fc),j(o)} =$ Weight between the $i-th$ input neuron at the FC layer and the $j-th$ neuron at the output layer,

$u_{i(fc)} =$ Input activation from $i-th$ neuron at the FC layer to the $j-th$ neuron at the output layer, which is equivalent to the output of the $u_{j(fc)}$ neuron from the FC layer after the dropout operation during training or without dropout during testing,

$b_{j(o)} =$ Bias term of the $j-th$ neuron at the output layer,

$n =$ The total number of activated $i-th$ inputs from the fully connected layer to the $j-th$ neuron at the output layer.

The classification output y_j (or the predicted probability $\hat{y}_i$ of the $i-th$ sample from the input layer) processed by the $j-th$ neuron at the output layer of the Conv1D model is described in Equation 3.26.

$$y_j = \hat{y}_i = S(z_{j(o)}) \tag{3.26}$$

Where the sigmoid function S with respect to $z_{j(o)}$ (i.e., $S(z_{j(o)})$, is defined in Equation 3.27 (Ali et al., 2023:12; Nawaz et al., 2023:5).

$$S(z_{j(o)}) = \hat{y}_i = \frac{1}{1+e^{-z_{j(o)}}} \qquad \textbf{(3.27)}$$

After determining the output of the classification, the loss calculation of the CNN network is computed next. Loss calculation measures the difference between the classified output and the expected output. This calculation is crucial for training the Conv1D neural network.

❖ Loss calculation

The loss or error at the output layer of the Conv1D network is being evaluated using the binary cross entropy loss function expressed in Equation 3.28 (Wang et al., 2023:12; Liao, Zhu, et al., 2024:5080). The binary cross entropy loss function is generally used for tasks involving binary classifications, to determine the losses between the observed output and the expected output (Yang, 2019:148). The primary objective of calculating loss in neural networks is to try to minimize it as much as possible, in a bid to produce a model that generalizes better. Loss is calculated based on what the model has predicted as input and what the actual input is.

$$Loss(L) = -\frac{1}{N}\sum_{i=1}^{N} y_i \times \log(\hat{y}_i) + (1-y_i) \times \log{(1-\hat{y}_i)} \qquad \textbf{(3.28)}$$

Where:

$y_i =$ True label or target output for the $i-th$ input sample,

$\hat{y}_i =$ Predicted probability for the $i-th$ sample at the output layer of the Conv1D model,

$\log =$ Natural logarithm,

$N =$ Total number of samples or data points.

The loss is computed for each sample independently using the predicted or observed output obtained during the forward propagation and the actual output or true label for each sample. Each sample or data point in the employed dataset consists of a feature vector and its associated binary label. After calculating the loss or error by applying the binary cross entropy, the next phase of the prediction training process is to backpropagate the errors into the CNN layers to update the weights and biases, in a bid to minimize the errors in the network.

3.3.2.2 Backward propagation

Backward propagation or backpropagation commences immediately when the forward pass is completed. Backward propagation is the process of distributing the total error computed during forward propagation back into the CNN network from the output layer through to the input layer. This is to determine how changes in network parameters (weights or biases) will affect model accuracy, and then these network parameters are later updated in a bid to minimize the loss function in the network to improve model performance. In other words, the total error in the CNN model are distributed back into the network during the backward pass, and the network weights and biases are adjusted and updated accordingly to minimize losses or errors in the model (Jaokar, 2019). Backpropagation is very crucial to the training and optimization of the Conv1D CNN model. Losses or errors are the disparities between the actual targets or labels and the classified outputs.

When training neural networks, gradients are used to minimize loss functions. Figure 3.7 depicts a simple representation of one complete backpropagation cycle through the Conv1D CNN architecture shown in Figure 3.5.

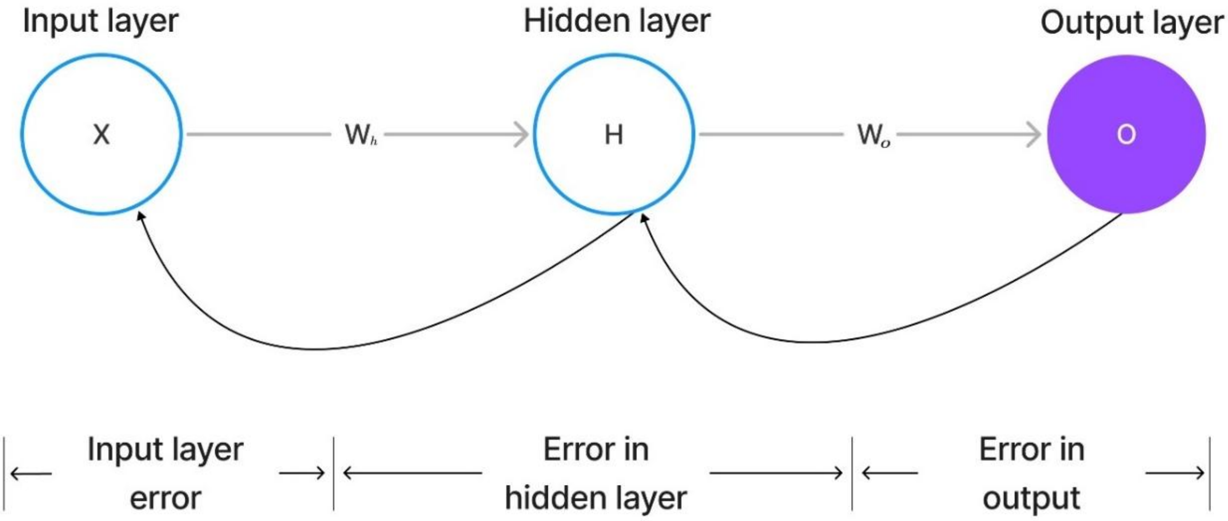


Figure 3.7: Backward propagation in the Conv1D network

Gradient points are in the direction of the steepest ascent, but since our target is to minimize losses in the network, we then have to go in the reverse direction of the gradient to ensure that the update of each model parameter reduces error in the network (Crypto, 2024). Hence, this process is referred to as backpropagation. Backpropagation involves back-passing of gradients from the output layer through to the input layer. To implement backpropagation, the derivative of the loss function with respect to the predicted output is calculated first and propagated backward through the CNN layers, followed by calculating the loss gradients for each layer of the CNN network with respect to every weight and bias in the network, using the chain rule of calculus. Once the gradients have been calculated, weights and biases are then updated accordingly using an optimizer.

The weights and biases updates are repeated for multiple epochs until the loss converges and a desired output performance is achieved by the model. The gradient of the loss function indicates how a small change in either weight or bias will affect a change in the loss function.

❖ Backpropagation through the CNN layers

The purpose of backpropagation is to compute gradients that can help update the parameters of the CNN network in a way that minimizes the loss function L of Equation 3.28. Equations 3.29 to 3.40 in this section and Equations 3.41 to 3.47 in the next section convey the processes involved in backpropagation through the CNN layers (Nielsen, 2015:39-118; Goodfellow et al., 2016:300-350; A. Zhang et al., 2021:225-296; Aggarwal, 2023:305-360). The backward-pass equations are written in accordance with the parameters in their forward-pass equations. Before calculating the gradient of each layer of the CNN model, the derivative of the loss function expressed in Equation 3.29 is calculated with respect to the predicted output $\hat{y}_i$ first, as depicted in Equation 3.29.

$$\frac{\partial L}{\partial \hat{y}_i} = \frac{\hat{y}_i - y_i}{\hat{y}_i(1-\hat{y}_i)} \qquad \textbf{(3.29)}$$

Where:

$\frac{\partial L}{\partial \hat{y}_i} =$ Gradient of the loss function L with respect to the predicted output $\hat{y}_i$,

$\hat{y}_i =$ Predicted or observed output,

$y_i =$ Target or actual output.

To reduce prediction errors through backpropagation, the gradient of the loss function of each weight and bias in the CNN network is calculated (Medium, 2023). Gradients are calculated for each layer of the Conv1D model during backpropagation to update the weights and biases in the network in order to minimize the loss function. To backpropagate through the output layer, the gradient of the loss function with respect to the weighted sum $z_{j(o)}$ at the output layer, which represent the input to the output layer from the FC layer before activation (as described in Equation 3.26) is expressed in Equation 3.30.

$$\frac{\partial L}{\partial z_{j(o)}} = \frac{\partial L}{\partial \hat{y}_i} \cdot \frac{\partial \hat{y}_i}{\partial z_{j(o)}} = \frac{\hat{y}_i - y_i}{\hat{y}_i(1-\hat{y}_i)} \cdot \hat{y}_i(1-\hat{y}_i) = \hat{y}_i - y_i \qquad \textbf{(3.30)}$$

Where:

$\frac{\partial L}{\partial z_{j(o)}}$ = Gradient of the loss function L with respect to the weighted sum at the output layer before applying the activation function,

$\frac{\partial L}{\partial \hat{y}_i}$ = Gradient of the loss function L with respect to the predicted output $\hat{y}_i$,

$\hat{y}_i$ = Predicted or observed output,

y_i = Target or actual output.

Equation 3.30 conveys the error or loss between the predicted output label and the actual input label. The calculated loss gradient is then backpropagated from the output layer into the dropout layer. Calculated gradients are passed backward through the CNN network to compute the gradients with respect to weights and biases at each layer, and thereafter the weights and biases are updated using the computed gradients (Kiliçarslan & Celik, 2021:1). The backpropagation process tend to reduce prediction errors in the CNN model. A network can be backpropagated by adjusting each weight and bias in the network according to how much they contributed to the overall error (Jaokar, 2019). The loss gradient of Equation 3.30 calculated at the output layer is backpropagated into the dropout layer as depicted in Equation 3.31.

$$\frac{\partial L}{\partial u_{i(fc)}} = \frac{\partial L}{\partial u_{j(dr)}} \odot a_{i(dr)} \qquad \textbf{(3.31)}$$

Where:

$\frac{\partial L}{\partial u_{i(fc)}}$ = Gradient of the loss function L with respect to the input activation to the dropout layer from the FC layer,

$\frac{\partial L}{\partial u_{j(dr)}}$ = Gradient of the loss function L with respect to the output of the dropout layer,

$a_{i(dr)}$ = The dropout mask.

It should be noted that the dropout mask $a_{i(dr)}$ is applied to ensure that only the activations that were not dropped during the forward pass have their gradients backpropagated into the dropout layer. After the dropout layer, the gradients are further backpropagated into the fully connected layer. For the backpropagation to the FC layer, the gradients with respect to weights, biases and input activations from the dropout layer are propagated back to the FC layer. Equations 3.32, 3.33, and 3.34 respectively represent the gradient equations with respect to weight, bias and input activation, which were backpropagated into the FC layer from the dropout layer.

$$\frac{\partial L}{\partial w_{i(fc),j(fl)}} = \frac{\partial L}{\partial z_{j(fc)}} \cdot u_{i(fl)} \tag{3.32}$$

$$\frac{\partial L}{\partial b_{j(fc)}} = \frac{\partial L}{\partial z_{j(fc)}} \cdot z_{i(fl)} \tag{3.33}$$

$$\frac{\partial L}{\partial u_{i(fl)}} = \frac{\partial L}{\partial z_{j(fc)}} \cdot w_{i(fc),j(fl)} \tag{3.34}$$

Where:

$\frac{\partial L}{\partial w_{i(fl),j(fc)}}$ = Gradient of the loss function L with respect to the weight between $i-th$ neuron at the flatten layer and $j-th$ neuron at the fully connected layer,

$\frac{\partial L}{\partial z_{j(fc)}}$ = Gradient of the loss function L with respect to the pre-activation output of the fully connected layer,

$\frac{\partial L}{\partial b_{j(fc)}}$ = Gradient of the loss function L with respect to the bias of the $j-th$ neuron at the fully connected layer,

$\frac{\partial L}{\partial u_{i(fl)}}$ $=$ Gradient of the loss function L with respect to the Input activation from the flatten layer to the fully connected layer,

$z_{j(fc)}$ $=$ Pre-activation output of the fully connected layer,

$u_{i(fl)}$ $=$ Input activation from the flatten layer to the fully connected layer,

$w_{i(fl),j(fc)}$ $=$ Weight between $i-th$ neuron at the flatten layer and $j-th$ neuron at the fully connected layer.

The gradients at the FC layer have been computed using Equations 3.32, 3.33, and 3.34. However, the gradient of the loss function L with respect to the Input activation from the flatten layer to the fully connected layer of Equation 3.34 is backpropagated to the flatten layer, providing the necessary information to adjust network parameters. Equation 3.34 helps us understand how changes in the input to the fully connected layer ($u_{i(fl)}$) would impact the overall loss L, enabling updates that would optimize the performance of the network. At the flatten layer, feature vectors are reshaped back to 3D vectors from the flattened 1D vectors as shown in Equation 3.35.

$$\frac{\partial L}{\partial Y_l} = reshape\left(\frac{\partial L}{\partial F_{fl}}\right) \quad \textbf{(3.35)}$$

Where:

$\frac{\partial L}{\partial Y_l}$ $=$ Gradient of the loss function L with respect to the activations Y_l from the pooling layer,

$\frac{\partial L}{\partial F_{fl}}$ $=$ Gradient of the loss function L with respect to the flattened activations,

$reshape =$ The reshape operation changes the shape of the gradient $\frac{\partial L}{\partial Y_l}$ to match the original shape before it was flattened.

Flatten layer is non-parametric and it simply just reshapes the incoming gradient from the FC layer back into the original shape that matches the initial output of the MaxPooling1D layer (before flattening) during the forward propagation.

Backpropagation to the MaxPooling1D layer from the flatten layer is described in Equations 3.36 and 3.37. In this process, gradients are passed back through the positions that held the maximum values during the forward pass.

$$\frac{\partial L}{\partial u_{j(c)}} = \frac{\partial L}{\partial Y_l} \tag{3.36}$$

$$\frac{\partial L}{\partial Y_l} = \begin{cases} \frac{\partial L}{\partial u_{j(c)}}, \; if \; Y_l \; was \; a \; maximum \; value \; in \; the \; pooling \; window \\ 0, \; otherwise \end{cases} \tag{3.37}$$

Where:

$\frac{\partial L}{\partial u_{j(c)}}$ = Gradient of the loss function L with respect to the output activation of $j - th$ neuron from Conv1D layer, which serves as input to the MaxPooling1D layer and corresponds to maximum value in the pooling window,

$\frac{\partial L}{\partial Y_l}$ = Gradient of the loss function L with respect to the output of the pooling operation at position l.

The gradients that belong to the non-maximum elements in the pooling window do not receive any gradient and are thereby set to zero as described in Equation 3.37. This is because those non-maximum elements or features did not contribute to the output of the pooling layer during the forward pass. Equations 3.38, 3.39, and 3.40 represent the backpropagation process to the convolutional (Conv1D) layer.

$$\frac{\partial L}{\partial w_{i(i),j(c)}} = \sum_l \frac{\partial L}{\partial z_{j(c)}} \cdot x_{i(c)} \tag{3.38}$$

$$\frac{\partial L}{\partial b_{j(c)}} = \sum_l \frac{\partial L}{\partial z_{j(c)}} \tag{3.39}$$

$$\frac{\partial L}{\partial x_{i(c)}} = \frac{\partial L}{\partial z_{j(c)}} * w_{i(i),j(c)} \tag{3.40}$$

Where:

$\frac{\partial L}{\partial w_{i(i),j(c)}} =$ Gradient of the loss function L with respect to each weight $w_{i(i),j(c)}$ between the input sequence (or feature vector) and the kernel or filter,

$\frac{\partial L}{\partial z_{j(c)}} =$ Gradient of the loss function L with respect to the $j-th$ weighted-sum output $z_{j(c)}$ of the convolutional layer,

$\frac{\partial L}{\partial b_{j(c)}} =$ Gradient of the loss function L with respect to the bias $b_{j(c)}$ of every $j-th$ kernel or filter in the convolutional layer,

$\frac{\partial L}{\partial x_{i(c)}} =$ Gradient of the loss function L with respect to the input sequence to the convolutional layer,

$x_{i(c)} =$ Input sequence from the input layer which serves as input to the convolutional layer,

$w_{i(i),j(c)} =$ Weight between the input sequence from the input layer and the kernel or filter at the convolutional layer.

In the convolutional layer, the gradients of the loss function L with respect to the input sequences, and with respect to the weights and bias of each kernel or filter are calculated. The gradients calculated in Equation 3.38 are summed over all the $l-th$ positions in the feature map where the convolutional kernel or filters are applied across the input sequence. The gradients calculated in Equation 3.39 are also summed across all the $l-th$ positions. The gradients of the loss with respect to the input sequences in Equation 3.40 are passed back to the input layer. The calculated gradients are then used to update corresponding model parameters to minimize loss L.

Finally, backpropagation to the input layer completes the backward-pass process. Although input layer does not have parameters to update, it does receive gradients from the convolutional layer, which are meant for gradient-flow purposes in the network.

- **Optimization approach for adjusting the parameters of the model**

Updating or adjusting the weights and biases of the CNN network can be done using three popular optimization algorithms like Adaptive Moment Estimation (Adam), Stochastic Gradient Descent (SGD) or Root Mean Square propagation (RMSprop) to optimize the network (Javaid, Gul, et al., 2021:98694; C. Zhang et al., 2023:1497). However, Adam optimizer has been used to update the weights and biases of the CNN network because it is deemed as the best optimization algorithm for neural networks (Javaid, Gul, et al., 2021:98685). Adam is more robust and preferred than other optimization algorithms because it is computationally less expensive and easier to implement, can adjust the learning rate of the model adaptively by reducing the time it takes to train the model with higher convergence speed, more reliable for noisy, large, and sparse datasets, can handle sparse gradient issue on noisy data, prevents local-optima trapping, reduces losses, quickly achieves optimal results with minimal memory requirements, and has the highest accuracy in terms of performance (Shehzad et al., 2021:128672; Pamir, Javaid, Qasim, et al., 2022:26864; Bai et al., 2023:12; Naeem, Javaid, et al., 2023:7; Huang et al., 2024:12). For the stated reasons, Adam optimizer is used in this work to update parameters in the CNN network.

Unlike gradient descent optimizers that use fixed learning rates, Adam combines both momentum (using the first moment estimate) and RMSprop (using the second moment estimate) to create an adaptive learning rate for each parameter (Kingma & Ba, 2015:1, 7; Goodfellow et al., 2016:294, 308). Adam uses the first and second moments of the gradient to modify the learning rate for each parameter of the model, allowing it to handle sparse gradients and noisy data more efficiently. Equations 3.41 to 3.47 illustrate the processes involved when deploying Adam optimization algorithm to update the weights and biases of the CNN network (Liu et al., 2023:6; Reyad et al., 2023:17100).

$$g_t = \frac{\partial L}{\partial W_t} \tag{3.41}$$

$$m_t = \beta_1 m_{t-1} + (1 - \beta_1) g_t \tag{3.42}$$

$$v_t = \beta_2 v_{t-1} + (1 - \beta_2) g_t^2 \tag{3.43}$$

$$\widehat{m}_t = \frac{m_t}{1-\beta_1^t} \tag{3.44}$$

$$\hat{v}_t = \frac{v_t}{1-\beta_2^t} \tag{3.45}$$

Where:

g_t = Gradient of the loss function L with respect to weights at the current timestep t,

m_t = The first moment estimate at timestep t,

m_{t-1} = The previous moment estimate at timestep $t-1$,

v_t = The second moment estimate at timestep t,

v_{t-1} = The previous moment estimate at timestep $t-1$,

$\widehat{m}_t$ = The bias-corrected first moment estimate at timestep t,

$\hat{v}_t$ = The bias-corrected second moment estimate at timestep t,

β_1 = The decay rate for the first moment,

β_2 = The decay rate for the second moment,

t = Current timestep which increases with every epoch or iteration.

The gradient g_t in Equation 3.41 gives the direction and rate of change of L with respect to each element of W_t. During the backpropagation process, the gradient g_t is used to adjust W_t in the direction that effectively reduces L, in order to effectively train the model. This is a fundamental part of the optimization process where gradients are used to update weights in every epoch. The β_1 in Equation 3.42 is the exponential decay rate for the first estimate which determines how much of the past gradients to consider, while β_2 represents the exponential decay rate of the second estimate which controls how much of the past squared gradients g_t^2 contribute to the current estimate. The default value of β_1 is 0.9, while that of β_2 is 0.999 (Kingma & Ba, 2015:2, 9; Goodfellow et al., 2016:311; Reyad et al., 2023:17100). The term $(1-\beta_1)$ in Equation 3.42 controls how much the current gradient g_t influences m_t, while the term $(1-\beta_2)$ in Equation 3.43 determines how much weight the current squared gradient g_t^2 contributes to v_t.

The first moment estimate m_t (mean of gradients or moving average of gradients) and the second moment estimate v_t (squared mean of gradients or moving average of the squared gradients) in the Adam optimizer are initialized to zero at the beginning of training. This can underestimate actual average gradient and the actual average squared gradient early in the training, which then cause them to be biased towards zero, especially when only a few gradients have been observed. Without correction, this initial zero bias could cause instability or slow convergence in the early stages. Adam optimizer corrects the zero initial bias present in m_t and v_t by applying a bias correction to m_t and v_t of Equations 3.42 and 3.43 by adjusting the initial bias in order to obtain the bias-corrected values denoted as $\widehat{m}_t$ and $\hat{v}_t$ in Equations 3.44 and 3.45 respectively (Reyad et al., 2023:17100).

The initial-zero bias correction ensures that $\widehat{m}_t$ and $\hat{v}_t$ accurately represent the true mean and the variance of the gradients throughout training. The bias-corrected first moment estimate $\widehat{m}_t$ is essentially the momentum term which is an exponentially decaying average of past gradients. The bias-corrected second moment estimate $\hat{v}_t$ controls the adaptive scaling, and it is calculated from the average of the squares of past gradients, to adjust the learning rate for each parameter. The bias corrections are done by dividing m_t by $(1-\beta_1^t)$ and dividing v_t by $(1-\beta_2^t)$ as described in Equations 3.44 and 3.45, to adjust the initial zero bias. The bias correction terms $(1-\beta_1^t)$ and $(1-\beta_2^t)$ do the adjustments to correct the initial zero bias in a bid to stabilize the optimization process. β_1^t represents decay rate β_1 raised to the power of timestep t, while β_2^t represents decay rate β_2 raised to the power of timestep t. They adjust for the exponential weightings introduced by β_1 and β_2 over multiple timesteps. Equations 3.46 and 3.47 represent the weight and bias updates using Adam optimizer.

$$W_{t+1} = w_t - \eta \frac{\widehat{m}_t}{\sqrt{\hat{v}_t} + \epsilon} \tag{3.46}$$

$$b_{t+1} = b_t - \eta \frac{\widehat{m}_t}{\sqrt{\hat{v}_t} + \epsilon} \tag{3.47}$$

Where:

$W_{t+1} =$ The updated weight at timestep $t+1$,

$W_t =$ The current weight at timestep t,

$b_{t+1} =$ The updated bias at timestep $t+1$,

$b_t =$ The current bias at timestep t

$\eta =$ Learning rate,

$\widehat{m}_t =$ The bias-corrected first moment estimate at timestep t,

$\hat{v}_t$ = The bias-corrected second moment estimate at timestep t,

$\in$= An added small constant to avoid division by zero and ensure numerical stability,

t = Current timestep which increases with every epoch.

The update of the bias term in Equation 3.47 follows the same process as the weight update in Equation 3.46. The updates are done by combining moment and adaptive learning rate components. Each weight w and bias b are updated using both first moment $\widehat{m}_t$ and second moment $\hat{v}_t$ to achieve adaptive learning rate for each parameter. Dividing by $\sqrt{\hat{v}_t}+\in$ scales the learning rate η of each parameter based on the magnitude of recent gradients and helps the algorithm to converge quickly. The constant $\in$ has a default value of 10^{-8}, while the learning rate η has a default value of 0.001 (Kingma & Ba, 2015:2; Goodfellow et al., 2016:311).

After the weights and biases have been updated through the backward pass, the next forward pass would utilize the updated weights and biases to reduce the total error in the network, and the process would be repeated iteratively until the error is reduced to a minima (Jaokar, 2019). Eventually, a set of weights and biases that yield accurate predictions can be obtained once the error of each weight and bias in the network are minimized by decreasing them repeatedly over time. After successfully developing the Conv1D CNN model, attempt was also made to further improve the model. In doing this, features from CNN layers were used to train and test random forest (RF) model in a standalone and hybrid arrangements.

3.3.3 Random forest

Random forest (RF) is an ensemble learning model, which is developed from a large number of randomly-constructed decision trees (DTs) called forest, and is trained on different subsets of training data to make predictions (Xu et al., 2019:4; Wang, 2023:507). RF is a typical supervised learning algorithm which predicts by collective learning, and is known for high efficiency, robustness, and outstanding classification accuracy (Wang, 2023:505). Random forests are quick and simple to implement, deliver highly accurate predictions, and can manage a large number of input variables without the risk of overfitting (Fawagreh et al., 2014:605).

RF model uses a bagging (bootstrap aggregating) technique by training multiple DTs on different random subsets of the training data, creating a wide array of decorrelated trees, in a bid to reduce variance in the model and increase robustness and accuracy (Breiman, 2001:5). The random feature selection at each split within a tree adds an additional layer of randomness, making RF even more diverse and less likely to overfit when compared with simple bagging methods.

RF model will randomly sample subsets of the training data to build each of the fifty DTs (as used in this project) in the forest. Once all the trees in the model have been trained, RF combines the predictions from each of these trees to make the final prediction. For classification tasks, the final prediction of the RF model is determined by selecting the most common class out of the predicted class among the DTs in a process called majority voting; while for regression tasks, the final output of RF model is determined by the prediction average from of all the DTs in the model (Fawagreh et al., 2014:604; Wang, 2023:507). The equation of the RF model for classification is depicted in Equation 3.48, while the equation of the RF model for regression is expressed in Equation 3.49 (Wang, 2023:507).

$$\hat{y}_i = mode\big(T_1(X_i), T_2(X_i), \dots, T_K(X_i)\big) \quad \textbf{(3.48)}$$

$$\hat{y}_i = \frac{1}{K}\sum_{K=1}^{K} T_K\,(X_i) \quad \textbf{(3.49)}$$

Where:

$\hat{y}_i =$ The final predicted class,

$K =$ The total number of decision trees in the random forest,

$T_k(X_i) =$ The prediction made by the $k-th$ decision tree for the input feature vector X_i,

$mode =$ The most common class label predicted by the K trees.

While the trees in the RF grows to its full depth, the total number of K trees in the forest of the RF model is set at 50, while the random state which indirectly controls randomness in the model to ensure reproducibility is set at 42. It is important to mention that aside the thorough and excellent data preprocessing carried out on the employed SGCC dataset used in developing the proposed model, the train-validation-test split of the large dataset, applying dropout regularization to the CNN model, and the deployment of ensemble RF as final classifier are enough to mitigate any potential overfitting issues that may arise within the proposed model. The hyperparameters of the CNN and RF models are summarized in Table 3.3.

Table 3.3: Hyperparameters for the CNN and RF models

CNN	RF
Kernel or filter size = 3	Number of trees = 50
Stride of kernel or filter = 1	Maximum depth = default
Batch size = 30	Minimum samples split = 2
Number of kernels or filters = 32	Maximum terminal nodes = default
Padding = 0	Minimum samples leaf = 1
Size of pooling window = 2	Maximum samples: default
Stride of pooling window = 2	Maximum features = default
Optimizer = Adam	
Activation functions = ReLU, Sigmoid	
Dropout rate = 0.4	
Learning rate = 0.001	
Number of epochs = 50	

3.3.4 Leveraging the combined strengths of CNN and RF models

When the strengths of deep CNN and ensemble RF models are being combined, the deep feature extraction capability of CNN and the robust classification ability of RF are being leveraged. The resulting composite CNN-RF model which is derived from infusing features from CNN layers to train RF classifier model operates in two stages. In the first stage, the CNN performs feature extraction, while the RF makes the final classification in the second stage based on the extracted features. CNNs are effective for feature extraction (Ullah et al., 2020:1599; W. Liao et al., 2022:3520; Khan et al., 2024:16; Nirmal et al., 2024:1), while RF is excellent in classification (Xu et al., 2019:1, 4; Wang, 2023:505) and avoids the overfitting problem peculiar to imbalanced datasets (Ghori et al., 2023:15335). Hence, this research project explores the individual strength of each model to improve ETD. In real-world scenarios, datasets can be noisy and contain outliers. RF is robust to noisy data, and is also known for its ability to handle missing values, outliers, and still provide accurate predictions (Fawagreh et al., 2014:602; Xu et al., 2019:1, 4). The stated characteristics of the RF classifier make it a good fit for ETD in classifying honest and fraudulent electricity customers. A blend of CNN and RF synergize efficiently and effectively in producing a composite ETD model, which is more robust than individual CNN and/or RF models.

The convolutional (Conv1D) layer of the CNN network performs convolution operation on the input data to extract structured convolved features from it. The extracted features (high-dimensional feature maps) from the convolutional layer then serves as input into the RF classifier. RF models work better with more structured convolved features like the Conv1D layer-extracted features instead of raw input data. To ensure compatibility with RF format, the extracted three-dimensional (3D) feature maps from the Conv1D layer are reshaped into two-dimensional (2D) feature maps for RF training and testing, as implemented in Section A.1.4.4 of the Appendix. In this work, three instances of model developments were carried out. In the first instance, Conv1D model was trained as tested separately as previously discussed in Sections 3.3.2, 3.3.2.1, and 3.3.2.2. In the second instance, RF model was trained and tested as a standalone model with static pre-extracted features from the Conv1D layer of the separately pretrained CNN model. In the third instance, features were extracted dynamically from the Conv1D layer of the CNN model into an RF model, in an adaptive joint arrangement as shown in Figure 3.8, to form the hybrid CNN-RF model. The three instances of model developments were carried out to check which of the models would performs best. Eventually, the integrated model proves to be more efficient than the standalone CNN and RF models in terms of its performance results.

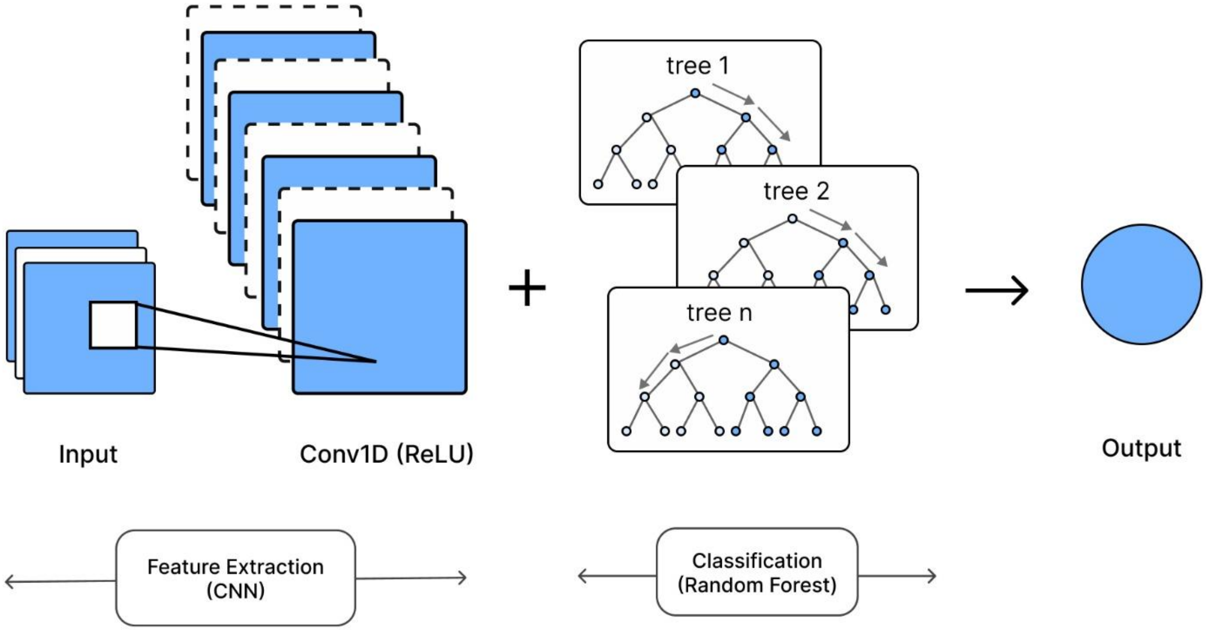


Figure 3.8: Architecture of the proposed CNN-RF model

In the eventual architecture of the proposed hybrid model shown in Figure 3.8, CNN and RF are trained together as a single model by combining the strengths of CNN and RF. Instead of using FC layer for classification in a conventional CNN architecture shown in

Figure 3.5, RF is used instead, in a hybrid CNN-RF network displayed in Figure 3.8. In the CNN-RF hybrid model, CNN adjusts and dynamically updates and adapts the extracted features used to train the RF (based on the feedback from RF), in a bid to improve RF classification. Empirical studies have shown that connecting the RF model to the Conv1D layer (Layer 1 of the CNN network in this case) is often optimal and preferable for producing superior results (Munawar, Khan, et al., 2022; Gunduz & Das, 2024). This is because the convolved features retain rich spatial patterns in a compact form while reducing noise and dimensionality in the data to enhance classifier performance. Features extracted from Conv1D layer also preserves low-level and mid-level representations before excessive transformation. These characteristics make the Conv1D layer-extracted features more suitable for a traditional ML classifier like the RF ensemble model.

The CNN features imputed into the RF classifier from the Conv1D layer is expressed in Equation 3.16, while the RF model which ultimately does the classification to predict the honest and fraudulent electricity customers is described in Equation 3.48. Extraction of features from the Conv1D layer to train RF model can be implemented by running the codes in Section A.1.4.2 of the Appendix. The combination of CNN and RF leverages the strengths of the deep learning (CNN) model for feature extraction, and the ensemble (RF) model reduces overfitting and improves generalization. The results of the CNN-RF model shows that the performance of the proposed model is comparatively better than the individual performances of either the CNN or RF model, and also better than the results of all the previous SGCC dataset-based ETD models developed in the existing literature, as explained in Sections 4.2.1 and 4.2.3 of Chapter 4, and as also shown in Table 4.2 of the same chapter.

In a bid to check whether the efficiency of the proposed model could further be improved or not, concatenation of the Conv1D and MaxPooling1D layers of the CNN network is done as shown in Figure 3.9, to better enrich the features used to train and test the RF model. To achieve this, a variant of the proposed CNN-RF model termed CNN-RF (concatenation) model is developed, to explore whether or not the enriched features may further improve the efficiency of the proposed CNN-RF model. Concatenating features from multiple pairs of convolutional and max pooling layers before feeding them into RF model can enrich and improve the feature set for RF training (Yu et al., 2022).

The CNN-RF (concatenation) model is built when the output features of the concatenation of three pairs of Conv1D and MaxPooling1D layers are fed from the last MaxPooling1D layer (Layer 6 of the CNN network in this case) into the RF model to train and test it. The

Python codes which show the implementations of the proposed CNN-RF model are presented in Sections A.1.1 to A.1.8 of the Appendix, while the codes used to implement the variant CNN-RF (concatenation) model can be found in Section A.1.9 of the Appendix. The performance scores of the proposed model are marginally greater than the performance scores of the variant model, as revealed in Table 4.1 in Chapter 4. Since the proposed CNN-RF model proves to be a bit more efficient than the CNN-RF (concatenation) model, the proposed CNN-RF model is thus preferred.

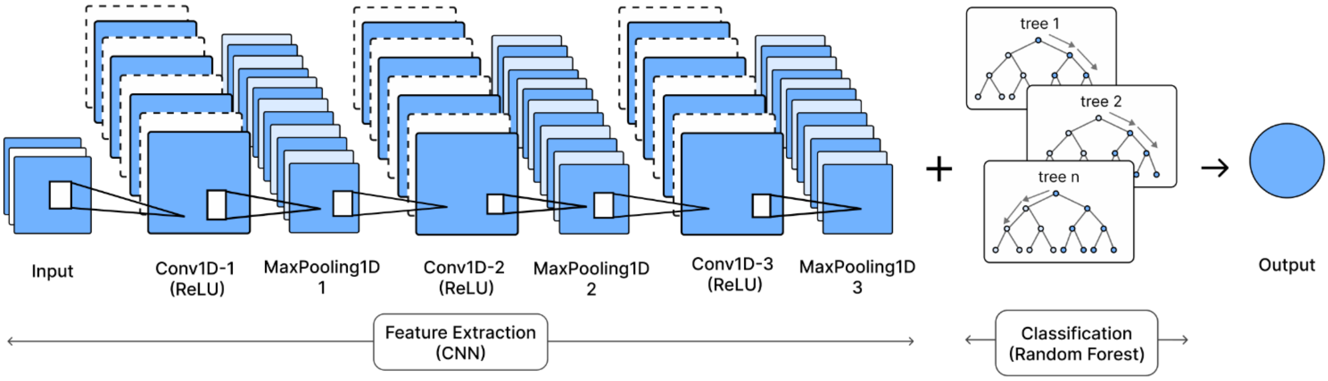


Figure 3.9: Architecture of CNN-RF model with concatenation of layers

The proposed CNN-RF hybrid model is a promising solution for ETD, especially in developing regions. However, its real-world effectiveness depends on overcoming data limitations, computational constraints, and the need for periodic model updates. Obtaining standard and labelled dataset especially in Africa and other developing countries can be very challenging. The constituent CNN model of the hybrid model introduces computational overhead when using local computers with limited computational resources especially during training. The proposed model requires continuous monitoring and periodic retraining to maintain detection accuracy.

3.4 Performance metrics used in evaluating the developed models

It is necessary to choose the performance metrics that suits the goal of this research project in a bid to determine the efficiency and reliability of the obtained results (Poudel & Dhungana, 2022:117). The aim of the research project is to reliably detect electricity thieves by profoundly reducing false positives (FPs), and to lessen the high operational cost incurred by the electric utilities with respect to FPs (Messinis & Hatziargyriou, 2018:259, 264; Saeed et al., 2020:6). While high FPs accrue huge cost to the utilities in terms of onsite-inspection costs during NTL mitigation efforts (Aldegheishem et al., 2021:25051; Pamir, Javaid, Qasim, et al., 2022:56866, 56870), reduction of false negatives also translates to corresponding increase in NTL detection (true positives), which allows for the apprehension of more electricity thieves. Apprehension and prosecution of electricity thieves reduce NTL, and assist in generating more revenues for the utilities. Selecting appropriate performance evaluation metrics for ETD models is crucial for assessing the effectiveness of the developed model. The choice of performance metrics for the evaluation of the developed ETD models is based on those metrics that can give reliable results even with imbalanced datasets, and are also able to better predict those customers who steal electricity. Reliable performance results prevent unnecessary and costly onsite inspections which spike huge revenue losses to the utilities (Ghori et al., 2020:16034:16041). Traditional NTL method involves general inspections of all electricity consumers; a measure which is very expensive and inefficient (Zheng et al., 2018:1606; Liao, Zhu, et al., 2024:5075).

When dealing with class-imbalanced datasets, It is imperative to use different types of metrics to ascertain reliable results (Messinis & Hatziargyriou, 2018:259; Saeed et al., 2020:6; Poudel & Dhungana, 2022:115). However, the use of different performance metrics ascertains the reliability of classifiers (Ali et al., 2023:14). Therefore, the performance metrics used for the evaluation of the developed ETD models are precision, recall, and F1 score, accuracy, Matthews correlation coefficient (MCC), area under receiver operating characteristic curve (AUC), and area under precision-recall curve (PR-AUC). Other metrics also being considered are true negative rate (TNR), false positive rate (FPR), and false negative rate (FNR). The prediction values of all the other performance assessment metrics range between 0 and 1, except for MCC which ranges between -1 and 1. In general, the closer the prediction values of an ETD model to 1, the better the performance of such model, indicating that the model is good and generalizing well, except for FPR and FNR which is vice versa. The closer the values of FPR and FNR to zero, the better the performance of such ETD model.

However, It is very vital to note that the choice of evaluation metrics should align with the specific goals and constraints of the ETD problem, as their applications may vary from one use case to another. Therefore, it is crucial to understand the trade-offs and choose the metrics that corroborate best to the business objectives and priorities of the electricity providers. Ultimately, detection of ET done in a bid to considerably purge the grid of NTL is the main priority of all electric utilities. The evaluation measures used for the assessment of the developed ETD models have been carefully chosen to align with this objective.

3.4.1 Confusion matrix

Confusion matrix is a performance indicator table that contains the result summary or the performance breakdown of a binary classifier using machine learning (ML) (Xia et al., 2023:6; Mehdary et al., 2024:19). It is used primarily for evaluating the performances of classifier models (Hussain et al., 2022:1269; Farid et al., 2023:84). Performance metrics of ETD models are being determined from the confusion matrix (Gul et al., 2020:13; Khan et al., 2020:15; Kawoosa et al., 2023:4807).

Confusion matrix contains the actual class and the predicted class from the test samples as predicted by ML models. ML models produce four possible prediction results in a confusion matrix that include true positive (TP), true negative (TN), false positive (FP), and false negative (FN) (Pamir et al., 2023:3586; Khan et al., 2024:12). A typical 2x2 confusion matrix which gives the summary of ETD or NTLD binary classification results is shown in Table 3.4 (S. Zhu et al., 2024:15487).

Table 3.4: Confusion matrix

Predicted class	**Actual class**	
	Negative (0)	Positive (1)
Negative (0)	True negative (TN)	False negative (FN)
Positive (1)	False positive (FP)	True positive (TP)

In Table 3.4, honest or benign electricity customers are referred to as ‘negative’ and can also be depicted by “0” label, while electricity thieves or fraudulent customers are denoted as ‘positive’ and can also be labelled as “1” (Ali et al., 2023:6, 9; Nayak & Jaidhar, 2023:4). The TN, FN, and FP, TP in the columns under the predicted class represent the outcome of ML predictors, while the TN, FP, and FP, TP in the columns of the actual class show the NTL statuses of electricity customers given by utility technicians after onsite inspections (Lu et al., 2019:5; Khattak et al., 2022:5). TPs are the actual values of positive samples (electricity thieves) which the NTLD classifier has correctly predicted as positives, TNs are the actual values of the negative samples (honest electricity consumers) which the ETD model has correctly predicted as negatives, FP is a type of classification error made by ML classifiers where actual negative values have been misclassified or mispredicted as positive values, FN is another type of classification error made by ML classifiers in which actual positive values have been misclassified as negative values (Khan et al., 2024:12; Mehdary et al., 2024:19).

In summary, TPs are actual electricity thieves or fraudulent consumers who cause NTL, while TNs are honest electricity consumers who neither engage in theft nor cause NTL. FPs and FNs are errors made while classifying into TPs and TNs (Messinis & Hatziargyriou, 2018:259; Saeed et al., 2020:6; Mehdary et al., 2024:19).

3.4.1.1 Precision

The precision metric or positive predictive value (PPV) measures the proportion of correctly predicted positive or theft cases among all the instances the NTLD model has predicted as positives (Lepolesa et al., 2022:29647; Ghori et al., 2023:15336). In the context of ET, precision is important to minimize false alarms or FPs, and reduce the effect of unnecessary inspections in order to lessen the consequences of high operational costs attributable to FPs (Aldegheishem et al., 2021:25051; Pamir, Javaid, Qasim, et al., 2022:56866, 56870). High precision ensures that positively flagged cases are more likely to be actual thefts indicating low FPs (Ali et al., 2023:14). In simpler terms, precision is a measure of how accurately the ETD model predicts the positive samples. The precision evaluation metric is the ratio of the predicted TPs to that of the total number of predicted positives (TP + FP) as expressed in Equation 3.50 (Huang et al., 2024:12; Iftikhar et al., 2024:10).

$$Precision = \frac{TP}{TP+FP} \tag{3.50}$$

In a binary classification problem, the precision evaluation metric is useful when the focus of the prediction is to minimize FPs. Higher precision values indicates that the models that produce such performance results have low FPs (Ali et al., 2023:14), signifying that positive samples are accurately identified. Precision is the ability of a model to avoid or ignore irrelevant data, that is, the ability of the model to minimize the incorrect classification of negatives as positives.

3.4.1.2 Recall

Recall or true positive rate (TPR) or sensitivity is the measure of the proportion of the actual positive samples (or actual number of electricity thieves or fraudulent consumers) that have been correctly identified or predicted by the model as positives out all the available actual positive samples (Khan et al., 2023:544). Higher recall values depict low false negatives (FNs) (Ali et al., 2023:14), indicating that the model is good at identifying large proportion of positive or fraudulent cases. The recall metric is shown in Equation 3.51 (Khan et al., 2023:544; Iftikhar et al., 2024:10).

$$Recall = \frac{TP}{TP+FN} \tag{3.51}$$

Recall is the ability of a model to identify the relevant data, that is, the ability of the model to minimize the incorrect classification of positives as negatives.

3.4.1.3 F1 score

The performance metric called the F1 score or F-measure aggregates recall and precision into a single value called harmonic mean or weighted average, to maximize precision and recall, and provide a balance between them (Bohani et al., 2021:5; Xia et al., 2023:6). This metric is particularly important when a balance between precision and recall is intended, especially when evaluating models with imbalanced datasets or datasets with uneven distribution of class (Khan et al., 2020:15; Saripuddin et al., 2021:154; Mehdary et al., 2024:19). Higher F1 score values indicate that there is a strong balance between precision and recall suggesting that the model is reliable and performing well. F1 score can be evaluated using Equation 3.52 (Fei et al., 2022:4).

$$F1\ score = \frac{2TP}{2TP+FP+FN} \tag{3.52}$$

Precision, recall, and F1 score are commonly used evaluation metrics in the ML community. Using these metrics makes it easier to compare the performances of models being considered with other similar models or benchmarks.

3.4.1.4 Accuracy

Although, accuracy is the most popular and most-frequently used performance assessment metrics used in the world of ML, but it is very susceptible to class imbalance, cause overfitting of the majority class, and hence convey misleading or unreliable results (Khattak et al., 2022:11; Ghori et al., 2023:15336). Based on class imbalance or imbalanced dataset problem, a model may have a higher accuracy, but the model may still not be viable or useful owing to unequal label distribution in the dataset. The accuracy metric is eventually considered for the evaluation of the NTLD models in this research project because the SGCC dataset used in developing the models has been oversampled and balanced. Equation 3.53 depicts the mathematical expression of the accuracy metric (Fei et al., 2023:5; Iftikhar et al., 2024:10).

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \quad \textbf{(3.53)}$$

Accuracy, as defined in Equation 3.53, represents the proportion of correct predictions out of the total number of predictions. In general, higher accuracy indicates a better-performing model, except in cases of imbalanced data. Accuracy is a good metric in evaluating classification models when the datasets used in developing the models are balanced.

Real-world datasets used for ETDs or NTLDs often suffer from class imbalance, where the number of non-theft instances significantly outweighs the theft instances (Ghori et al., 2020:16034, 16036). In such cases, adopting accuracy as a performance metric could be misleading. In ETD experiments, imbalanced datasets are capable of causing overfitting if the dataset is not well balanced using appropriate class-balancing techniques. Therefore, a model predicting all instances of non-theft with an imbalanced dataset could still achieve a high accuracy because the accuracy metric is naturally biased towards the majority class (Aslam, Javaid, et al., 2020:4; Khan et al., 2020:9).

3.4.1.5 True negative rate

TNR or specificity is the measure of the proportion of actual negative samples (or actual number of honest electricity consumers) which have been correctly predicted as negatives out of all the available negative samples (Khan et al., 2020:15; Ghori et al., 2023:15336). Equation 3.54 shows the mathematical expression of TNR (Gunduz & Das, 2024:14).

$$TNR = \frac{TN}{TN+FP} \quad \textbf{(3.54)}$$

The greater the value of TNR, the better the ETD or NTLD model that produced such score.

3.4.1.6 False positive rate

The FPR metric is the measure of the true negative samples that have been misclassified or predicted wrongly as positive by the ML model out of all the available instances of negative samples (Ghori et al., 2023:15336; Khan et al., 2023:544). FPR can be calculated using Equation 3.55 (Huang et al., 2024:11).

$$FPR = \frac{FP}{FP+TN} \quad \textbf{(3.55)}$$

FPR needs to very low to ensure an efficiently working ETD model and to enhance lower onsite inspection costs (Pamir, Javaid, Qasim, et al., 2022:56870; Xia et al., 2023:10).

3.4.1.7 False negative rate

The FNR metric is the measure or ratio of actual positives samples which have been misclassified or mispredicted as negatives by the classifier out of all the available instances of positive samples (Hussain et al., 2021:4431; Ghori et al., 2023:15336). FNR is expressed in Equation 3.56.

$$FNR = \frac{FN}{FN+TP} \qquad \textbf{(3.56)}$$

The lower the value of FNR becomes, the better and more reliable the ETD or NTLD models producing such desired scores.

3.4.1.8 Matthews correlation coefficient

The Matthews correlation coefficient (MCC) is the most reliable metric used to determine the performance of models developed with datasets of imbalanced classes (Kulkarni et al., 2021:534), as the metric is insensitive to class imbalance (Glauner, 2019:90), and is very reliable to check quality of predictions. MCC can be evaluated using Equation 3.57 (Khalid et al., 2024:11; X. Wang et al., 2024;2186).

$$MCC = \frac{TP \times TN - FP \times FN}{\sqrt{(TP+FP)(TP+FN)(TN+FP)(TN+FN)}} \qquad \textbf{(3.57)}$$

The prediction values of MCC ranges between -1 to 1 (Ghaedi et al., 2022:68; Khalid et al., 2024:11). MCC value or score of -1 indicates incorrect prediction, MCC value of 0 indicates no prediction, MCC score close to 1 is a good prediction indicating that the model producing such prediction is working well and that all the categories of the confusion matrix (TP, TN, FP, and FN) produce good prediction results, while MCC value equals to 1 indicates a perfect model producing a perfect prediction, which is rare and unrealistic (Ghaedi et al., 2022:68; Khalid et al., 2024:12).

3.4.1.9 Area under receiver operating characteristic curve

Area under the curve (AUC) is the area covered by the receiver operating characteristic curve (ROC) (Ali et al., 2023:13; Xia et al., 2023:6; Liao, Bak-Jensen, et al., 2024). The

ROC curve is a graph generated by plotting the TPR against the FPR (Ali et al., 2023:14; Xia et al., 2023:6; Iftikhar et al., 2024:10; Liao, Bak-Jensen, et al., 2024). It is a useful metric to assess the overall discriminative power or performance of a model (Pamir, Javaid, Qasim, et al., 2022:56873). AUC evaluates the capacity of a model to discriminate between theft (positive) and non-theft (negative) instances. AUC is a summary of the trade-off between precision and recall values of a model (Khan et al., 2020:15), and gives a reliable model assessment when dealing with highly imbalanced datasets (Khan et al., 2023:544; Iftikhar et al., 2024:10). A higher AUC closer to 1 indicates a better ability in ranking randomly-chosen fraudulent or positive samples higher than negative samples, therefore indicating better ETD performance (W. Liao et al., 2022:3521; Liao, Bak-Jensen, et al., 2024).

Several confusion matrices are created under varying classification thresholds. Separate values of TPR and FPR are also calculated and obtained through the several confusion matrices. The ROC curve can be generated by plotting the different values of TPRs against the varying values of FPRs obtained under different classification thresholds that range between 0 and 1, showing trade-off between TPR and FPR (Xia et al., 2023:6; Liao, Bak-Jensen, et al., 2024). The implementation of AUC in Python for the individual CNN, RF, and the combine CNN-RF models are depicted respectively in Sections A.1.3.6, A.1.5.6, and A.1.6.4 of the Appendix. The AUC result of the NTLD models obtained through simulation has been presented as the AUC value.

The AUC performance score is realised in Python by implementing Equation 3.58 (Huang et al., 2024:12; Liao, Zhu, et al., 2024:5080). The AUC performance metric demonstrate that positive samples are rated higher than negative samples (W. Liao et al., 2022:3521; Liao, Bak-Jensen, et al., 2024)

$$AUC = \frac{\sum_{i \in PositiveClass} Rank_i - \frac{M(1+M)}{2}}{M \times N} \tag{3.58}$$

The term $i \in PositiveClass$ as shown in Equation 3.58 represents that sample i is a positive sample and therefore belongs to the positive class; $Rank_i$ is the number of samples which the prediction value of sample i exceeds when the samples are being arranged in ascending order according to the prediction scores of the positive samples (Zheng et al., 2018:1611; Khan et al., 2020:15). The terms M and N are the number of positive and negative samples found in the positive class (Bai et al., 2023:14; Khan et al., 2023:544).

3.4.1.10 Area under precision-recall curve

The area under the precision-recall curve (PR-AUC) is the area under the plot of precision against recall at varying thresholds (Kulkarni et al., 2021:533; Ali et al., 2023:14; Khan et al., 2024:12). PR-AUC is more reliable and appropriate when evaluating models with imbalanced datasets (Khan et al., 2020:15; Gao et al., 2024:16). Several confusion matrices are created under varying classification thresholds. Separate values of precision and recall are also obtained through the several confusion matrices.

The precision-recall curve is a plot that shows the trade-off between precision and recall, and is drawn by plotting the varying values of precisions against the different values of recalls obtained under varying classification thresholds (Calvo et al., 2020:7; Khan et al., 2024:12). The classification thresholds range between 0 and 1 (Sun et al., 2023:15; Khan et al., 2024:12). The area under the precision-recall curve is known as PR-AUC. The implementations of the values of PR-AUC in Python for CNN, RF, and CNN-RF models are depicted respectively in Sections A.1.3.6, A.1.5.6, and A.1.6.4 of the Appendix. The PR-AUC results of the developed models obtained through simulation has been presented as the PR-AUC value. The Python program executed the PR-AUC scores using Equation 3.59 (Gao et al., 2024:16).

$$PR - AUC = \sum_{I=1}^{m} (Recall_i - Recall_{i-1}) \times Precision_i \tag{3.59}$$

Where m depicts the total number of thresholds contained within the precision-recall curve, $Recall_i$ and $Precision_i$ are the precision and recall scores at $i - th$ threshold, while $Recall_{i-1}$ is the recall score of the previous threshold.

3.5 Conclusion

The proposed NTLD model developed in this thesis is a hybrid model termed CNN-RF model. The methods employed in developing the proposed ETD model have been explicitly discussed in this chapter. After rigorous trial of several ML models in a bid to achieve better NTLD results, the proposed model has been discovered to give the best performance results when compared with several other ETD models which have earlier been developed in the existing literature using same SGCC dataset employed in constructing the proposed model, as extensively explored in Section 4.5.1.1 of the next chapter (Chapter 4). Therefore, the proposed model becomes the choice model for this research project. The performance metrics used in evaluating the proposed model, to determine its efficiencies and efficacies, have also been explicitly explored in this chapter. The next chapter is an extension of this chapter, as it discusses the performance results of the developed models, to validate the essence of the research.

CHAPTER 4

RESULTS AND DISCUSSION

4.1 Introduction

This chapter gives insights into the electricity-theft detection (ETD) model developed in this thesis. The modelling approach leading to the ETD model has been presented in Chapter 3, while the implementation codes for the developed models are also presented in the Appendix. The proposed model is a hybrid of convolutional neural network (CNN) and random forest (RF) models which is otherwise referred to as CNN-RF. The dataset issued by the State Grid Corporation of China (SGCC), as discussed in Section 3.2.1 of Chapter 3, has been used as the input data to train, validate and test the developed ETD models. After the analysis of the methods used in arriving at the detection models for electricity theft (ET) or non-technical losses (NTL) in Chapter 3, this chapter analyses the results obtained through the modelled NTL detection (NTLD) systems and also discusses the interpretation of the attained results.

The results of the developed models are determined through the performance assessment metrics. These results show the efficacy or the predictive power of the built model. Just as the model is developed using Python in a Google Colaboratory (Colab) Integrated Development Environment (IDE), the simulation results can also be assessed within the confines of the IDE. The proposed CNN-RF model has been developed such that the results obtained through it are able to accomplish the aim and objectives of the research, while at the same time proffering answers to the research questions.

4.2 Results analysis of the CNN, RF, and CNN-RF models

The analysis of the results of the convolutional neural network (CNN), random forest (RF), and the hybrid CNN-RF models will be done separately in the subsequent sections under this section. Precision, recall, F1 score, accuracy, true negative rate (TNR), false positive rate (FPR), false negative rate (FNR), Matthews correlation coefficient (MCC), area under receiver operating characteristic curve (AUC), and area under the precision-recall curve (PR-AUC) have been used to check how the CNN, RF, and CNN-RF models have fared. These performance assessment metrics used to evaluate the models in Sections 4.2.1, 4.2.2, and 4.2.3 have been sufficiently described in Chapter 3 from Sections 3.4.1.1 to 3.4.1.10. The accuracy metric has however been eventually considered for evaluation since the dataset employed has been balanced using appropriate data balancing technique during the ETD simulations.

4.2.1 Results analysis of the CNN model

After training, validating and testing the CNN model as implemented in Sections A.1.3.1 and A.1.3.2 of the Appendix, the classification results depicted by the confusion matrix in Figure 4.1 is obtained. The confusion matrix is obtained by implementing the code in Section A.1.3.3 of the Appendix.

From the confusion matrix in Figure 4.1, True positive (TP) = 1.1e+04 = 1.1×10^4 = 11000, True negative (TN) = 1.2e+04 = 1.2×10^4 = 12000, False positive (FP) = 5,
False negative (FN) = 1.7e+02 = 1.7×10^2 = 170.

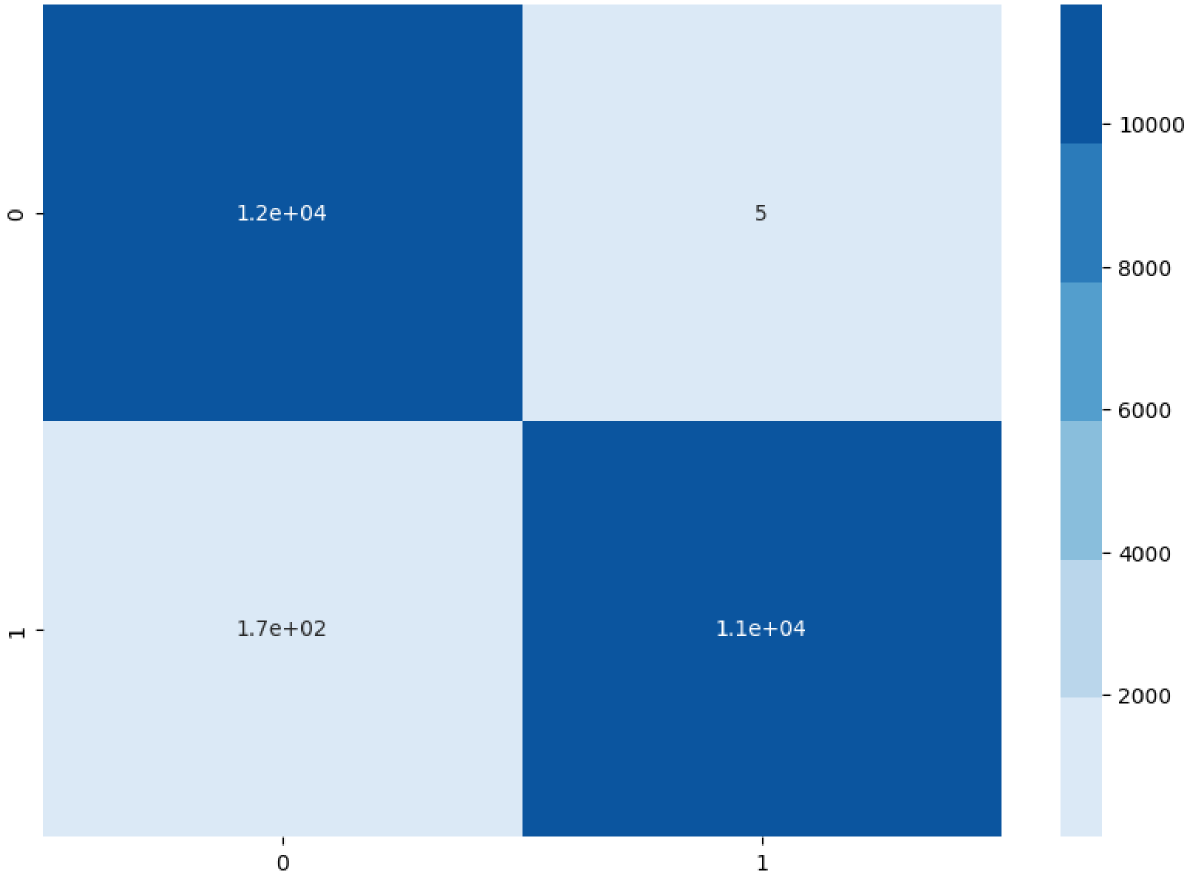


Figure 4.1: Confusion matrix of the CNN model

Based on the confusion matrix presented in Figure 4.1, the performance scores of the CNN model are thus calculated through the following evaluation metrics:

$$\text{Precision}=\frac{\text{TP}}{\text{TP+FP}}=\frac{11000}{11000+5}=0.9995=99.95\%$$

$$\text{Recall}=\frac{\text{TP}}{\text{TP+FN}}=\frac{11000}{11000+170}=0.9848=98.48\%$$

$$\text{F1 score}=\frac{2\text{TP}}{2\text{TP+FP+FN}}=\frac{2\times 11000}{(2\times 11000)+5+170}=0.9921=99.21\%$$

$$\text{Accuracy}=\frac{\text{TP+TN}}{\text{TP+TN+FP+FN}}=\frac{11000+12000}{11000+12000+5+170}=0.9925=99.25\%$$

$$\text{TNR}=\frac{\text{TN}}{\text{TN+FP}}=\frac{12000}{12000+5}=0.9996=99.96\%$$

$$\text{MCC}=\frac{\text{TP}\times\text{TN}-\text{FP}\times\text{FN}}{\sqrt{(\text{TP+FP})(\text{TP+FN})(\text{TN+FP})(\text{TN+FN})}}$$

$$\therefore \text{MCC}=\frac{(11000\times 12000)-(5\times 170)}{\sqrt{(11000+5)\times(11000+170)\times(12000+5)\times(12000+170)}}=0.9850=98.50\%$$

$$\text{FPR}=\frac{\text{FP}}{\text{FP+TN}}=\frac{5}{5+12000}=0.0004=0.04\%$$

$$\text{FNR}=\frac{\text{FN}}{\text{FN+TP}}=\frac{170}{170+11000}=0.0152=1.52\%$$

For the CNN model, AUC score of 0.9994 (99.94%) and the PR-AUC value of 0.9995 (99.95%) at 0.5 detection threshold were obtained by implementing the codes in Section A.1.3.6 of the Appendix. The performance scores from precision, recall, F1 score, accuracy, TNR, and the MCC metrics show that the CNN model performs well in terms of the classification or prediction of the honest and fraudulent electricity customers, while the FPR and FNR scores show that little errors were made in the classification process.

The precision-recall curve shown in Figure 4.2 is obtained by implementing the code in Section A.1.3.4 of the Appendix. The precision-recall curve, which is a plot of the precision values against the recall values at different exploratory thresholds between 0 and 1, is a useful visualization tool to illustrate the performance of ML models. Figure 4.2 depicts that the CNN model is performing well since the PR-AUC score (0.9995) of the curve which summarizes the performance of the CNN classifier is closer to 1, indicating that the model is distinguishing between honest and fraudulent electricity customers very satisfactorily.

From the precision-recall curve, the values of the precision and recall scores are also closer to 1, showing that the model achieves high precision and high recall values. If precision decreases significantly as recall increases, it means that the model is struggling to maintain accuracy while trying to capture more positive instances. Lowering the threshold for the precision-recall curve increases recall and decreases precision, and vice versa.

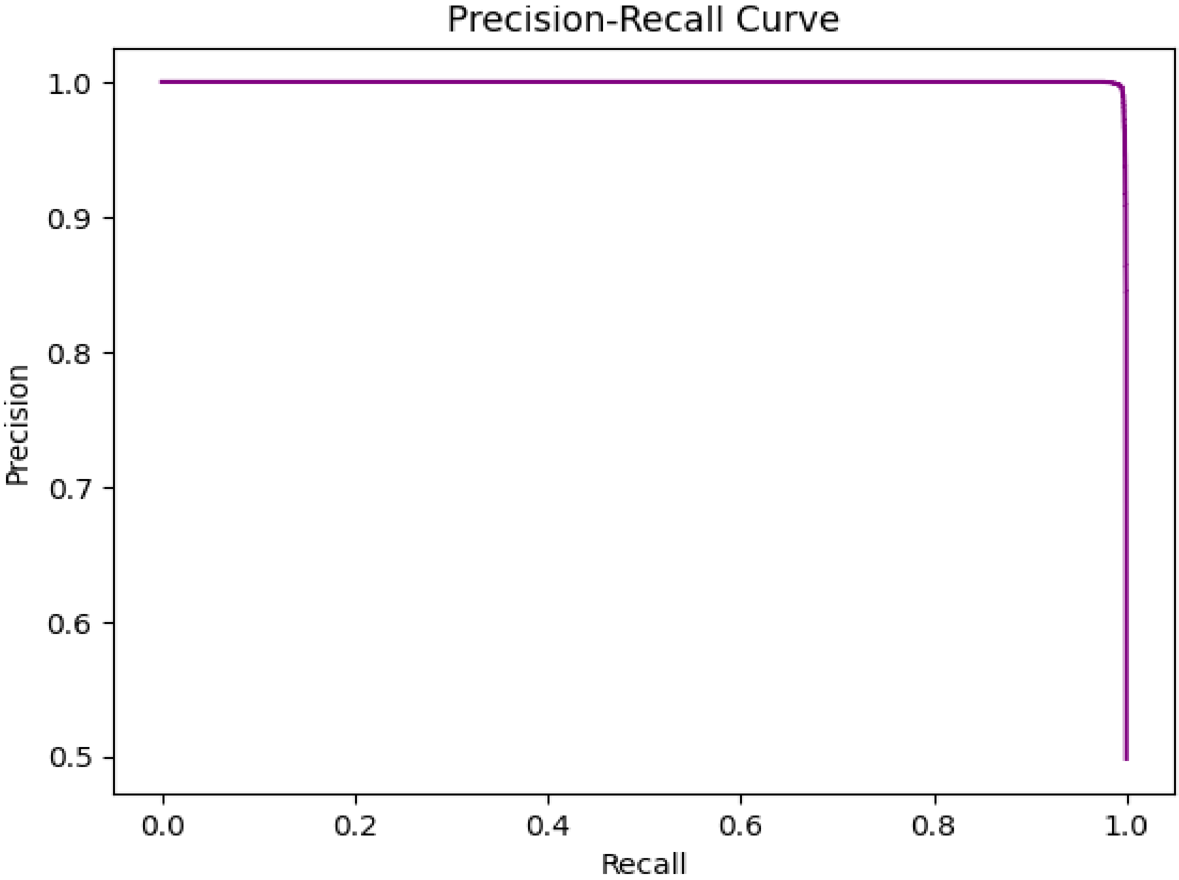


Figure 4.2: The precision-recall curve of the CNN model

The high precision and high recall values achieved by the CNN model indicates that the model predicts very few false positives and successfully identifies most true positives. The curve being closer to the top-right corner of the plot also indicates a better performing CNN model. Figure 4.3 shows the ROC curve of the CNN model, which is a plot of the TPR values against the FPR values at different exploratory thesholds. Infact, precision-recall curves summarize the trade-off between precision and recall, while ROC curves summarize the trade-off between TPR and FPR at different exploratory thresholds (Brownlee, 2023). The ROC curve has a broken red diagonal line that indicates a fixed final decision threshold or final classification threshold of 0.5. The threshold for making the final classification is a standard decision point for random guessing of the prediction class, and a common choice for interpreting binary probabilities. The final prediction threshold of 0.5 assumes balanced classes and equal costs for false positives and false negatives. The final classification threshold is applied to performance score and is compared to it to determine the prediction class of the model. With a final decision threshold of 0.5, it means that if the performance score of the model is greater than or equal to 0.5, the predicted electricity customer is fraudulent, and also indicates that the predicted electricity customer is honest if the performance score of the model is less than 0.5.

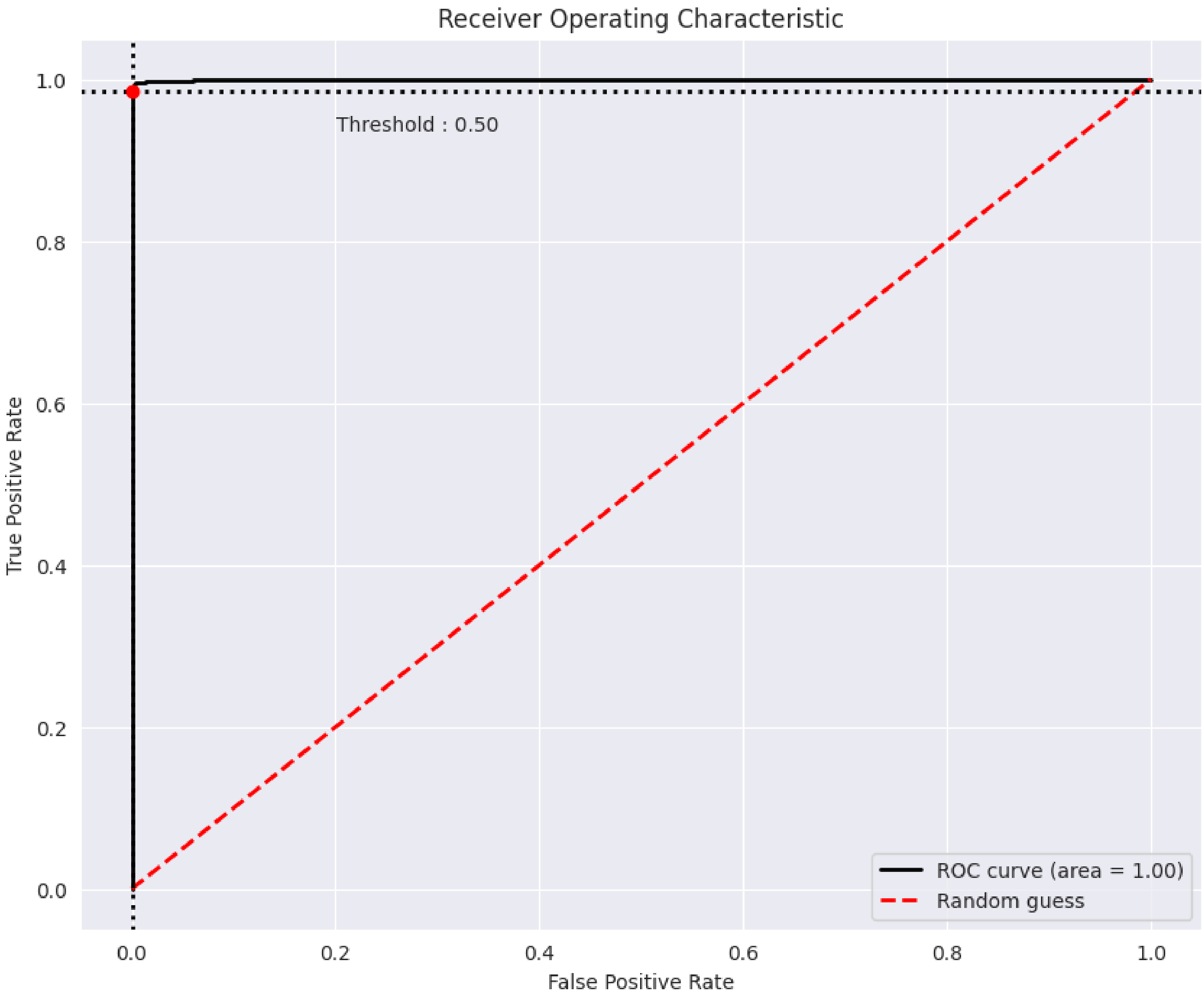


Figure 4.3: The ROC curve of the CNN model

The AUC score (0.9994) of the ROC curve of the CNN model is closer to 1, showing higher generalization ability by the model in terms of distinguishing between honest and fraudulent electricity customers. Also, the fact that the curve is closer to the top-left corner of the plot indicates that the CNN model is showing a better model performance. The ROC curve demonstrates the predictive proficiency of the CNN model as its exploratory threshold is being varied. Varying the threshold affects the trade-off between TPR and FPR. Lowering the threshold increases TPR and also increases FPR, and vice versa. Both precision-recall and ROC curves are generated by varying the exploratory thresholds of the model and recalculating the performances (true positives, true negatives, false positives and false negatives) of the model at each threshold. As the threshold changes, it affects both the precision and recall values of the precision-recall curve, and the TPR and FPR values of the ROC curve. Figure 4.4 shows the accuracy of the CNN model on training and validation data. It is implemented in Python using the codes in Section A.1.3.8 of the Appendix.

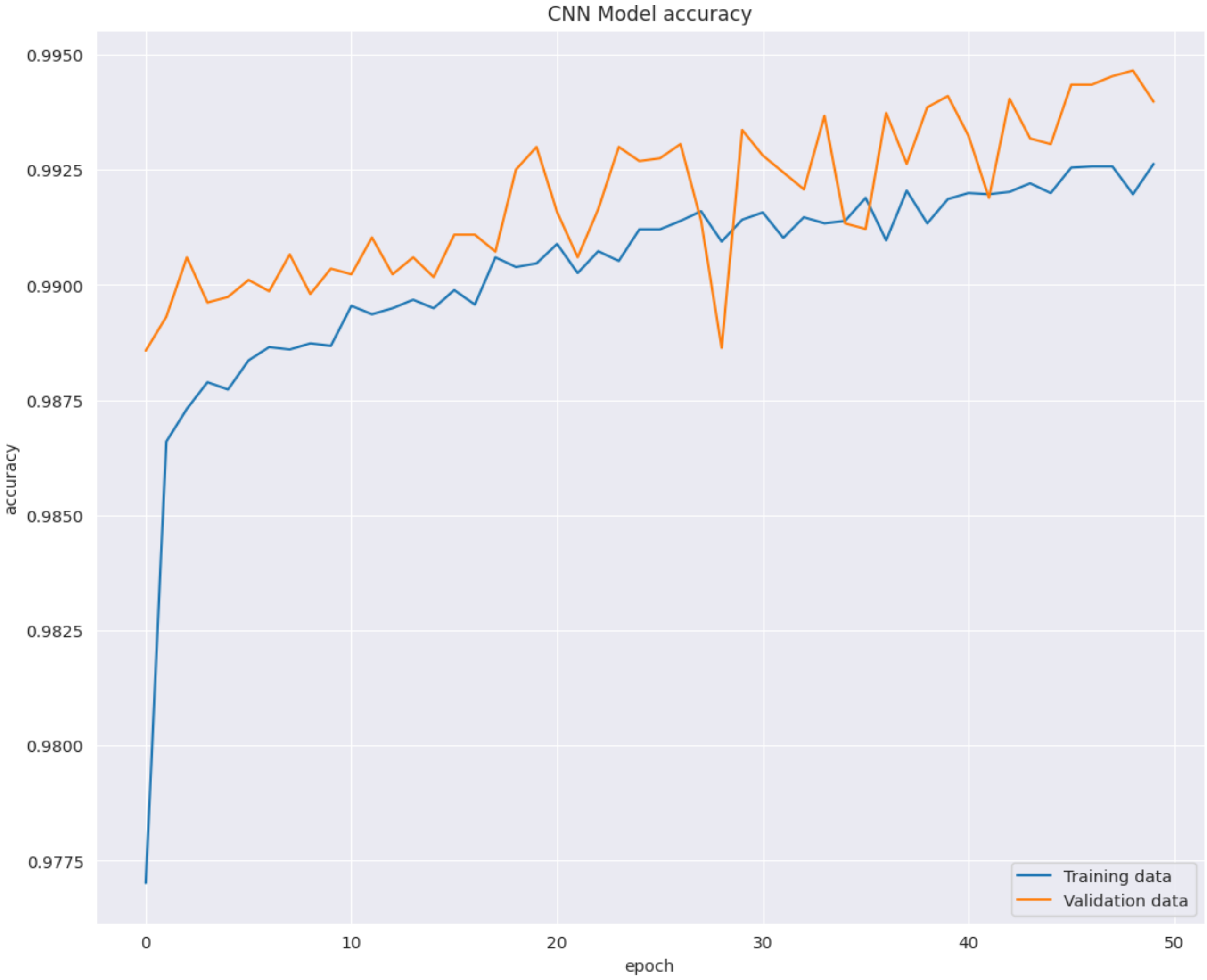


Figure 4.4: Accuracy of the training and validation data of the CNN model

Visualizing the accuracy of the training and validation data shown in Figure 4.4 is meant to test whether the CNN model is overfitting or not. This is to determine the accuracy of the

CNN model from the start of the training and validation processes till the end. From Figure 4.4, the training-data curve (blue curve) depicts the accuracy of the training data while the validation-data curve (orange curve) shows the accuracy of the validation data at different epochs. Looking at the training-data curve, it can be seen that around 1 epoch when we started training the CNN model that the accuracy of the model is close to around 0.9775 (97.75%), and kept on increasing to about 0.9925 (99.25%) at around 50 epochs or iterations. It is obvious from the validation-data curve that the accuracy of the validation data is greater than that of the training data. The accuracy of the validation data started around greater than 0.9875 (98.75%) at about 1 epoch to close to about 0.9950 (99.50%) at around 50 epochs, showing that the validation data performs better than the training data. The pattern of the curves shows that accuracy increases with increase in epoch for the training and validation data (Nirmal et al., 2024:5). Since the performance of the model using the validation data is better than that of training data, it clearly shows that the model is generalizing well and not overfitting (Aldegheishem et al., 2021:25052).

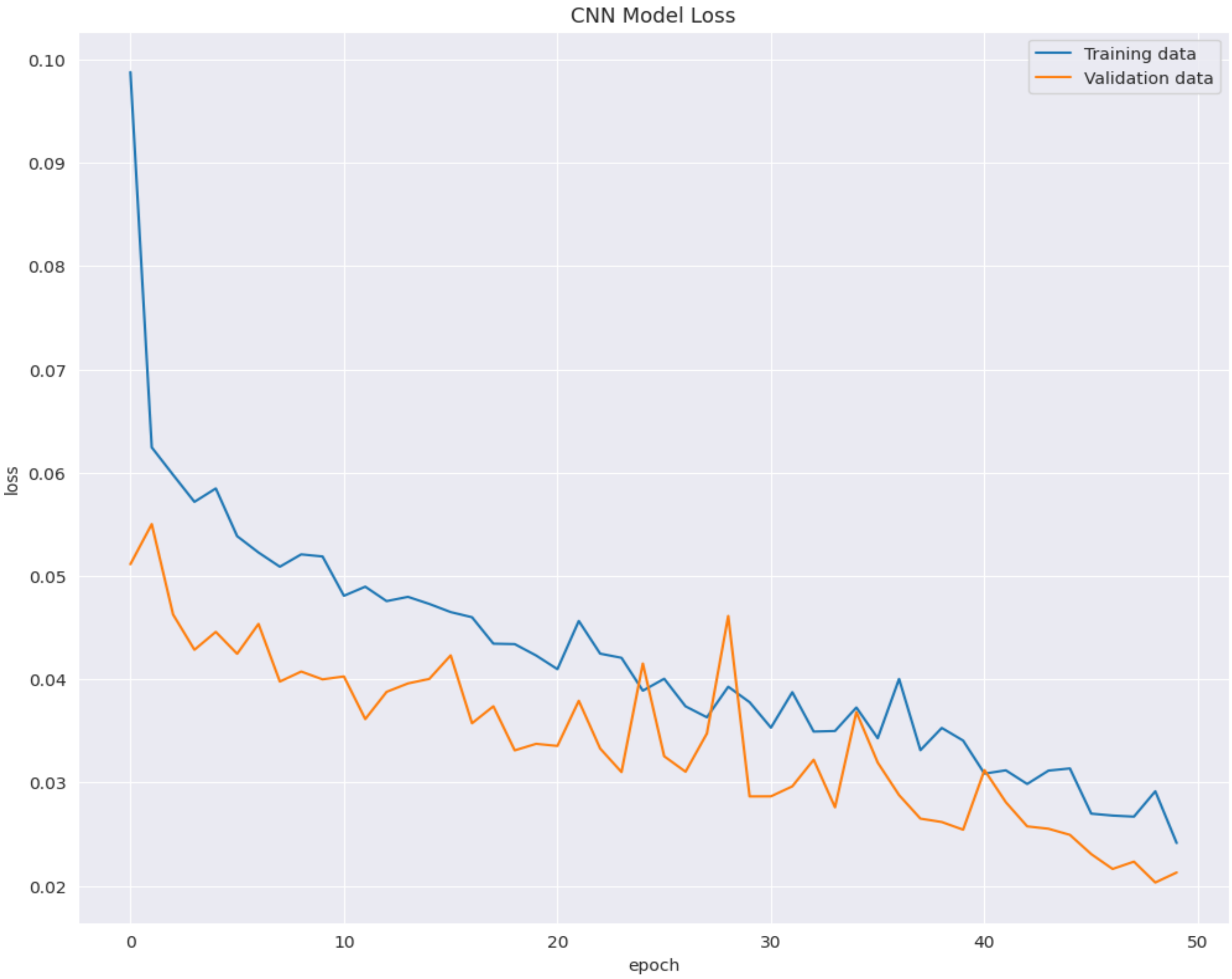


Figure 4.5: Training and validation data losses of the CNN model

Figure 4.5 shows the losses experienced during training and validation processes using the CNN model. The figure is the output of the Python codes implemented in Section A.1.3.9 of the Appendix. The Figure 4.5 show the level of losses when the CNN model was tested with the validation data. The validation-data curve (orange curve) shows more reduction in loss in the validation data when compared with the training data as conveyed through the training-data curve (blue curve). According to the training-data curve, the loss in the training data started with about 0.10 (10%) at around 1 epoch and continued to decrease gradually up to around 0.025 (2.5%) at around 50 epochs. The loss in the validation data as shown by the validation-data curve started with around 0.05 (5%) at about 1 epoch to about 0.02 (2%) at around 50 epochs. The pattern of the curves indicates that loss decreases with increase in epoch. The loss graph as shown in Figure 4.5 indicates the changes that occurs in the loss function during training and validation processes, showing differences or disagreements between the output predictions of the CNN model and the target values (Khan et al., 2024:13-14). The decreasing trend in losses as shown in the loss graph is a pointer to the fact that the CNN model is learning and predicting well (Aldegheishem et al., 2021:25052; Khan et al., 2024:13; Nirmal et al., 2024:5).

A likely question that might arise owing to the performance results obtained through the CNN model is that: since the CNN model has performed considerably well in terms of prediction results, would there then be any need to further extend the ETD process by building the RF model and subsequently the CNN-RF model? The answer to this probable question is that we are trying to get the best possible prediction results by reducing false positives (FPs) to the lowest minimum as much as possible in the proposed CNN-RF model because of the higher costs associated with FPs. The justification for the RF model as shown from its prediction results in Section 4.2.2 is that it perfectly predicts positive samples without any error (i.e. without any FP) in its positive-sample predictions as against the CNN model.

FP is very crucial to electric utilities because of the high cost associated with it. Predicting zero FP by RF and CNN-RF as shown in their confusion matrices, and revealed in their performance scores for the precision metric (100.00%) and the FPR metric (0.00%), as described in subsequent Sections 4.2.2 and 4.2.3, indicate that the utilities would not have to border to waste their scarce resources to inspect customers who do not engage in stealing electricity during the process of electricity mitigation (Messinis & Hatziargyriou, 2018:259, 264; Saeed et al., 2020:6; Aldegheishem et al., 2021:25051; Pamir, Javaid, Qasim, et al., 2022:56870). High values of FPR lead to increase in onsite inspection costs of electric customers (Messinis & Hatziargyriou, 2018:259, 264; Aldegheishem et al., 2021:25051; Pamir, Javaid, Qasim, et al., 2022:56866, 56870; Xia et al., 2023:10). Electric utilities have limited resources to execute onsite inspections, hence they cannot condone high FPRs (Khattak et al., 2022:7).

Precision score is specifically very significant when considering the consequence of FP in ML predictions (Mehdary et al., 2024:19), because high precision scores indicate low values of FPs (Ali et al., 2023:14). High values of precision indicate that the ML models or classifiers that produces such performance scores have correctly predicted majority of the customers who steal electricity as fraudulent customers (Messinis & Hatziargyriou, 2018:259; Saeed et al., 2020:6). Lower values of FPs prevent unnecessary and expensive onsite inspections during mitigation of ET and also ensure more profits to the electric utilities (Messinis & Hatziargyriou, 2018:259, 264; Aldegheishem et al., 2021:25051; Pamir, Javaid, Qasim, et al., 2022:56866, 56870; Xia et al., 2023:10). The RF and CNN-RF models produced results that show that FPs are totally eliminated in the performance results of the models. However, aside from the perfect precision score of 100.00%, the CNN-RF model improved better in other performance metric scores than the RF model. The proposed CNN-RF model is better than each of the standalone CNN and RF models in terms of comparative advantage.

4.2.2 Results analysis of the RF model

The RF model is trained and tested with the output features from the convolutional (Conv1D) layer of the CNN network in a standalone layout, as implemented in Sections A.1.5 and A.1.5.1 of the Appendix. The confusion matrix provided in Figure 4.6 displays the predictions of the standalone RF model. The confusion matrix is obtained by implementing the code in Section A.1.5.2 of the Appendix.

From the confusion matrix in Figure 4.6, True positive (TP) = 7.2e+02 = 7.2×10^2 = 720, True negative (TN) = 7.6e+02 = 7.6×10^2 = 760, False positive (FP) = 0,
False negative (FN) = 13.

Based on the confusion matrix in Figure 4.6, the following performance metrics are used to calculate the evaluation scores of the RF model:

$$\text{Precision} = \frac{\text{TP}}{\text{TP+FP}} = \frac{720}{720+0} = 1.0000 = 100.00\%$$

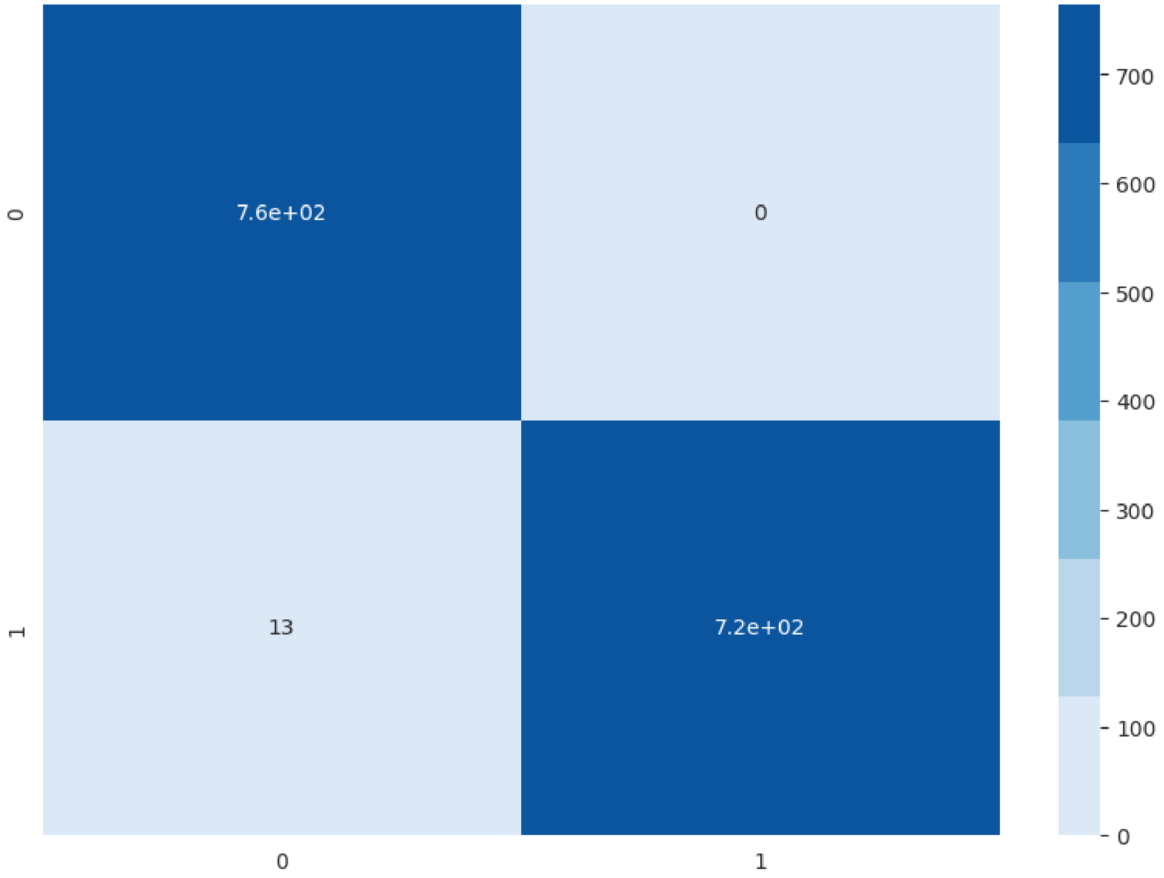


Figure 4.6: Confusion matrix of the RF model

$$\text{Recall} = \frac{TP}{TP+FN} = \frac{720}{720+13} = 0.9823 = 98.23\%$$

$$\text{F1 score} = \frac{2TP}{2TP+FP+FN} = \frac{2\times720}{2\times720+0+13} = 0.9911 = 99.11\%$$

$$\text{Accuracy} = \frac{TP+TN}{TP+TN+FP+FN} = \frac{720+760}{720+760+0+13} = 0.9913 = 99.13\%$$

$$\text{TNR} = \frac{TN}{TN+FP} = \frac{760}{760+0} = 1.0000 = 100.00\%$$

$$\text{MCC} = \frac{TP\times TN\text{-}FP\times FN}{\sqrt{(TP+FP)(TP+FN)(TN+FP)(TN+FN)}}$$

$$\therefore \text{MCC} = \frac{(720\times760)\text{-}(0\times13)}{\sqrt{(720+0)\times(720+13)\times(760+0)\times(760+13)}} = 0.9827 = 98.27\%$$

$$\text{FPR} = \frac{\text{FP}}{\text{FP+TN}} = \frac{0}{0+760} = 0.0000 = 0.00\%$$

$$\text{FNR} = \frac{\text{FN}}{\text{FN+TP}} = \frac{13}{13+720} = 0.0177 = 1.77\%$$

For the RF model, AUC score of 0.9912 (99.12%) and the PR-AUC value of 0.9955 (99.55%) at 0.5 decision threshold were obtained by implementing the codes in Section A.1.5.6 of the Appendix. Figure 4.7 shows the precision-recall curve of the RF model.

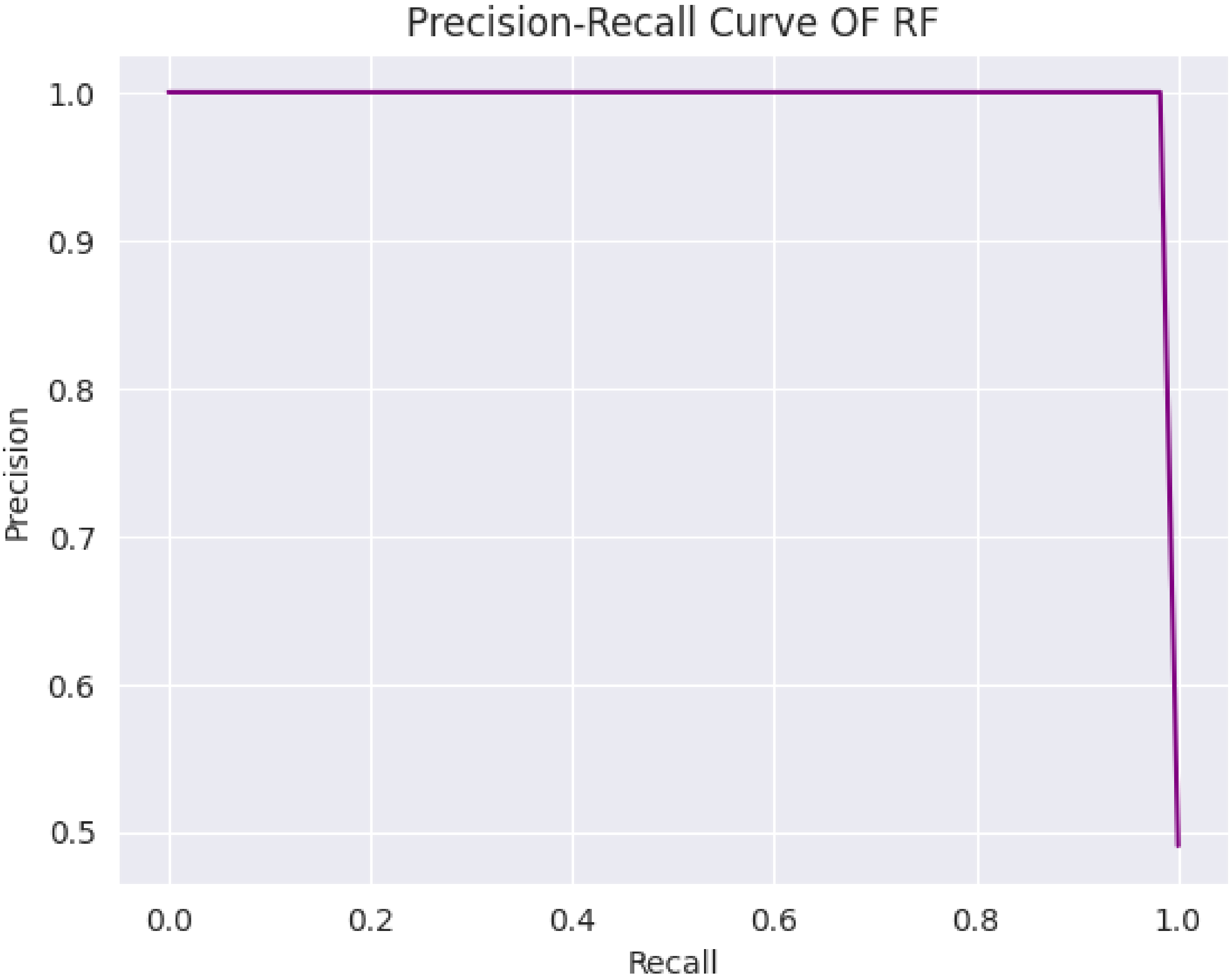


Figure 4.7: Precision-recall curve of the RF model

Much has been explained previously about the precision-recall curve and the ROC curve in Section 4.2.1. The explanations for the precision-recall and the ROC curves of the RF model and the subsequent CNN-RF hybrid model also follow the same principle. Figure 4.7 shows that the RF model achieves high precision and high recall values, with its PR-AUC score (0.9955) closer to 1, showing that the classification ability of the RF model is higher.

However, the AUC score (0.9912) of the RF model is also closer to 1, showing greater classification ability by the model in distinguishing between the benign and malignant electricity customers. The precision-recall curve is also closer to the top-right corner of the plot, indicating a better performing model. Figure 4.8 shows the ROC curve of the RF model. The ROC curve is plotted using TPR and FPR values at different exploratory thresholds ranging between 0 and 1.

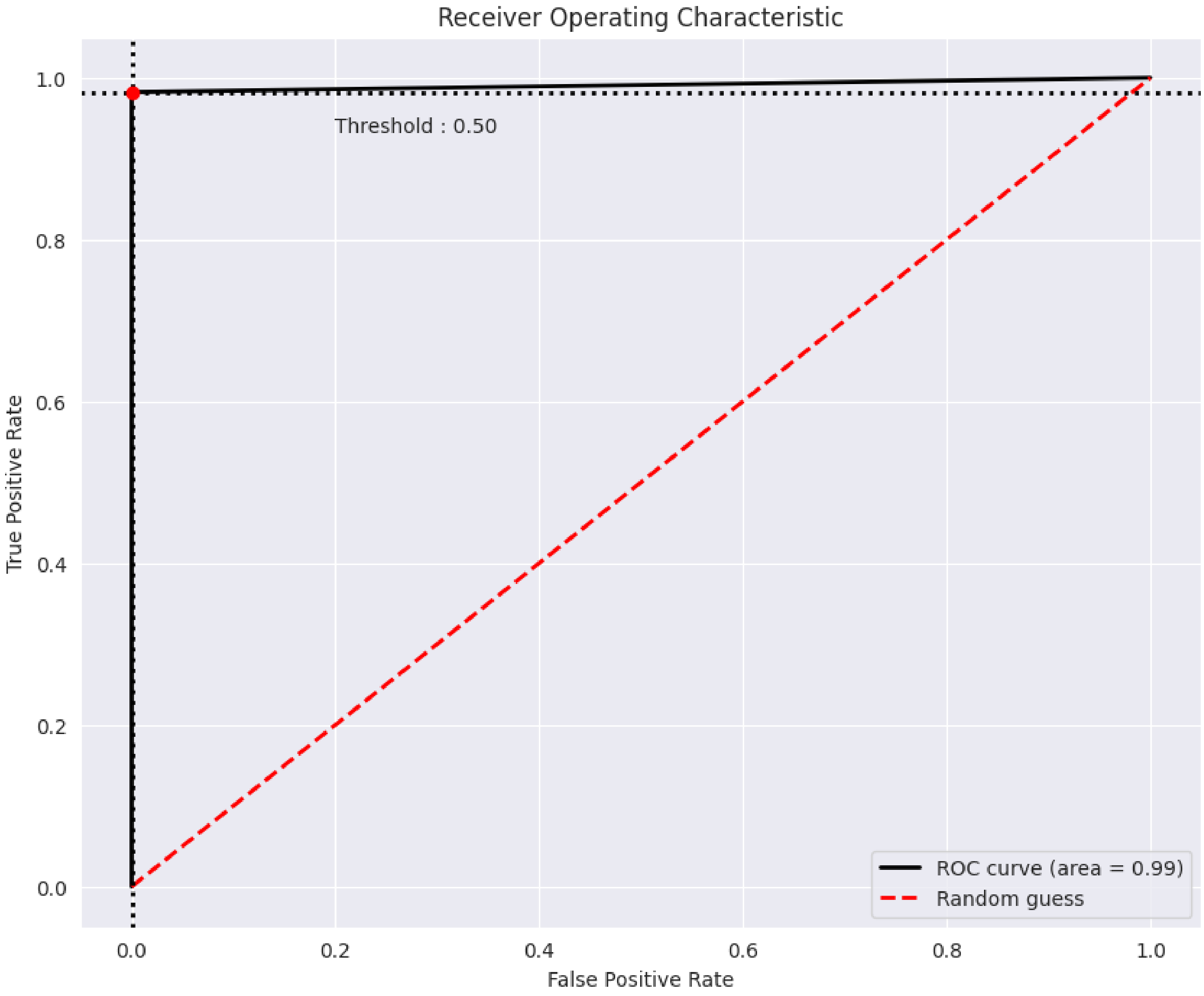


Figure 4.8: The ROC curve of the RF model

The decision threshold for final classification is set to 0.5 as depicted by the broken red line in the ROC curve. The decision threshold of 0.5 means that If the prediction score is equal to or greater than 0.5, the electricity customer is regarded as fraudulent, and the electricity customer is considered as honest or benign if the prediction score is less than 0.5. Varying exploratory thresholds when plotting the ROC curve shows the trade-off between TPR and FPR. Lowering the exploratory threshold leads to increase in TPR and FPR, and vice versa.

That the ROC curve is closer to the top-left corner of the plot indicates that the model is satisfactory with better classification performance.

4.2.3 Results analysis of the proposed CNN-RF model

The infusion of features from the convolutional (Conv1D) layer (Layer 1) of the CNN network into the RF model for final classification in a hybrid layout produce the proposed CNN-RF model. This is implemented using the codes in Section A.1.6 of the Appendix. The final classification of the Conv1D layer features by the RF model produced the confusion matrix shown in Figure 4.9. The confusion matrix is obtained by implementing the code in Section A.1.6.1 of the Appendix.

From the confusion matrix in Figure 4.9, True positive (TP) = 7.2e+02 =7.2×10^2 = 720, True negative (TN) = 7.6e+02 = 7.6×10^2 = 760, False positive (FP) = 0,
False negative (FN) = 12.

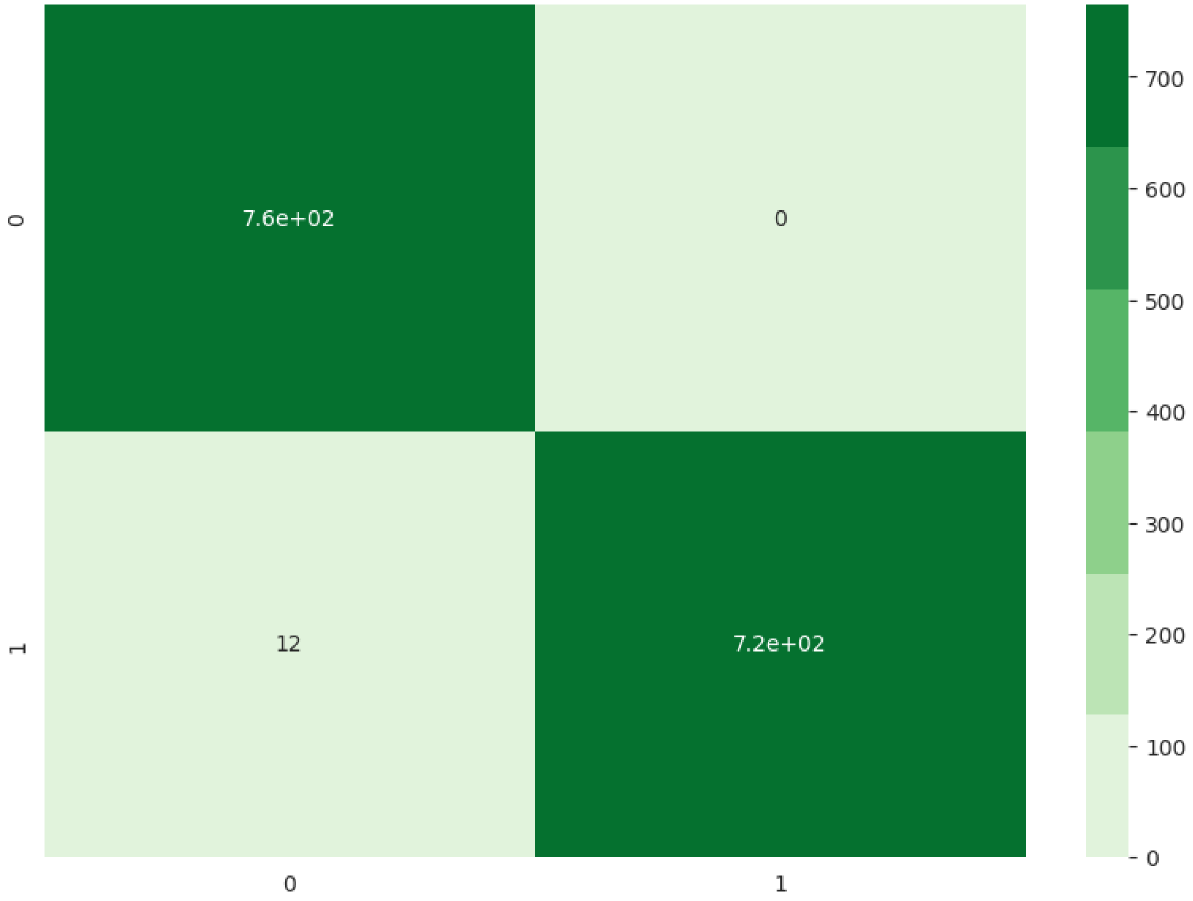


Figure 4.9: Confusion matrix of the proposed CNN-RF model

Based on the confusion matrix in Figure 4.9 above, the following performance metrics are calculated:

$$\text{Precision} = \frac{TP}{TP+FP} = \frac{720}{720+0} = 1.0000 = 100.00\%$$

$$\text{Recall} = \frac{TP}{TP+FN} = \frac{720}{720+12} = 0.9836 = 98.36\%$$

$$\text{F1 score} = \frac{2TP}{2TP+FP+FN} = \frac{2\times720}{(2\times720)+0+12} = 0.9917 = 99.17\%$$

$$\text{Accuracy} = \frac{TP+TN}{TP+TN+FP+FN} = \frac{720+760}{720+760+0+12} = 0.9920 = 99.20\%$$

$$\text{TNR} = \frac{TN}{TN+FP} = \frac{760}{760+0} = 1.0000 = 100.00\%$$

$$\text{MCC} = \frac{TP\times TN-FP\times FN}{\sqrt{(TP+FP)(TP+FN)(TN+FP)(TN+FN)}}$$

$$\therefore \text{MCC} = \frac{(720\times760)-(0\times12)}{\sqrt{(720+0)\times(720+13)\times(760+0)\times(760+12)}} = 0.9840 = 98.40\%$$

$$\text{FPR} = \frac{FP}{FP+TN} = \frac{0}{0+760} = 0.0000 = 0.00\%$$

$$\text{FNR} = \frac{FN}{FN+TP} = \frac{12}{12+720} = 0.0164 = 1.64\%$$

For the CNN-RF model, AUC score of 0.9913 (99.13%) and the PR-AUC value of 0.9955 (99.55%) at 0.5 decision threshold were obtained by implementing the Python codes in Section A.1.6.4 of the Appendix.

So far, the CNN-RF model has produced the best results because apart from achieving a precision score of 100.00% and FPR score of 0.00% like the RF model, indicating that the model is devoid of FPs, the CNN-RF model also achieved better prediction scores with other evaluation metrics than the RF model. Since mitigation of ET is the primary aim of detecting it, the results of the hybrid CNN-RF model will enhance the mitigation of ET better because it will afford the utilities more economic strength as they will not bother to waste resources inspecting customers who do not engage in stealing electricity (Khattak et al., 2022:7). Reducing FPs to the lowest minimum, or eliminating them completely is a critical issue to be considered when developing models for the detection and later mitigation of ET, and is one of the main targets in this research project.

Another question that may easily come to mind after checking out the performance scores of the CNN-RF model is that: why did we go further to implement the CNN-RF model since RF model has already afforded us a perfect precision score of 100.00% and an FPR score of 0.00%, which indicated that the model is already devoid of any FP? The answer to this probable question is that it could be observed that after outrightly eliminating FPs by the RF and CNN-RF models, the performance scores of other evaluation metrics like recall, F1 score, accuracy, MCC, FNR, and AUC obtained from CNN-RF model have shown better prediction scores than the RF model, spurring better detection of ET. In essence, the CNN-RF model achieved better results than the RF model, while also completely eliminating FPs in the model like the RF model. The precision-recall curve of the proposed CNN-RF hybrid model is shown in Figure 4.10.

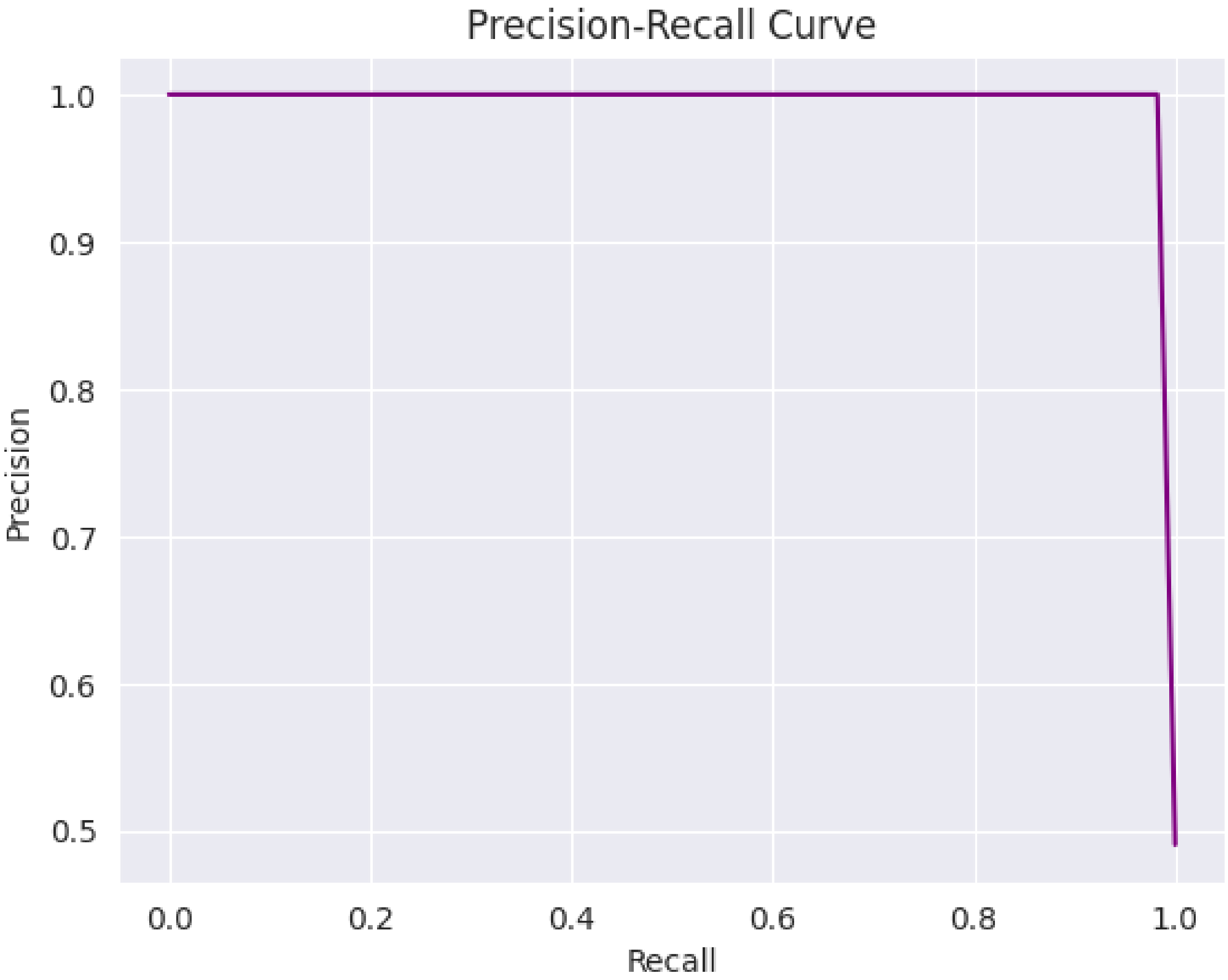


Figure 4.10: The precision-recall curve of the CNN-RF model

The Figure 4.10 shows that the CNN-RF model achieves high precision and high recall values, with its PR-AUC score (0.9955) closer to 1, showing that the classification ability of the CNN-RF model is higher. However, the AUC score (0.9913) of the CNN-RF model is also closer to 1, showing greater classification ability by the proposed model in distinguishing honest and fraudulent electricity customers. The precision-recall curve is also closer to the top-right corner of the plot, depicting a better performing model. Figure 4.11 shows the ROC curve of the RF model. The ROC curve is plotted using TPR and FPR values at different exploratory thresholds ranging between 0 and 1.

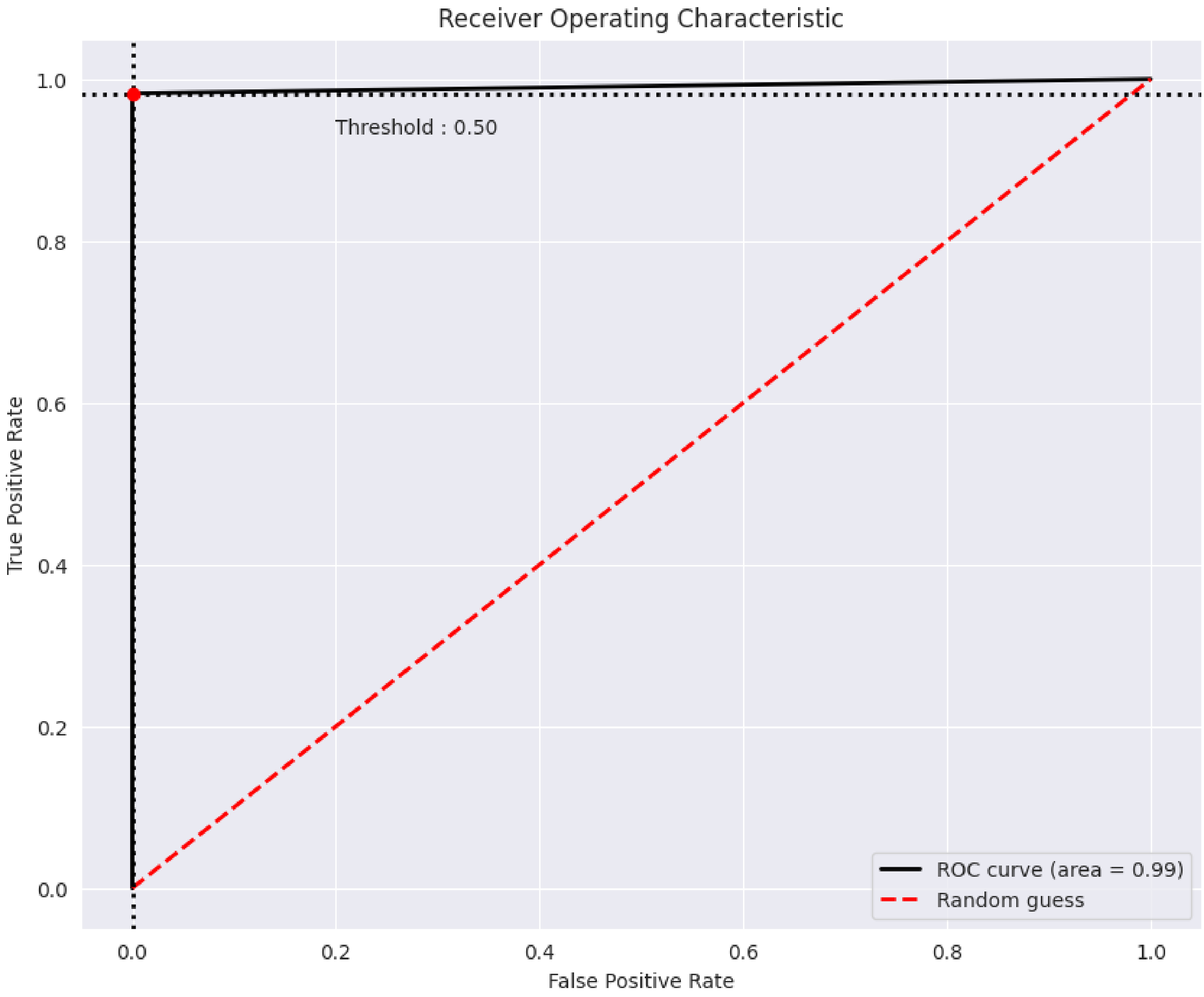


Figure 4.11: The ROC curve of the CNN-RF model

As was done for CNN and RF models, the decision threshold for final classification for the proposed CNN-RF model is set to 0.5 as depicted by the broken red line in the ROC curve of Figure 4.11. With the 0.5 decision threshold, the CNN-RF model will predict an electricity customer as fraudulent if the prediction score of the proposed model is greater than or equal to 0.5, and will predict an electricity customer as honest if the prediction score is less than 0.5. Exploratory thresholds are varied when plotting the ROC curve showing the trade-off between TPR and FPR. Lowering the exploratory threshold leads to increase in TPR and FPR, and vice versa. The fact that the ROC curve is closer to the top-left corner of the plot indicates that the model demonstrates greater classification performance. In summary, the proposed CNN-RF model provides a more cost-effective, versatile and robust approach to ETD, which is comparatively better than the individual CNN and RF models and will be preferred by utility stakeholders in the task of ETD.

However, an inquiry was carried out to check whether the results of the proposed CNN-RF model could further be improved. This was done by taking features from the last MaxPooling1D layer (layer 6) of a three-pair of concatenated Conv1D and MaxPooling1D layers as depicted in Figure 3.9 of Chapter 3. This new variant of the proposed CNN-RF model is referred to as CNN-RF (concatenation) model as implemented in Section A.1.9 of the Appendix. In general terms, any undistinguished CNN-RF model mentioned in this thesis refers to the proposed CNN-RF model.

From the confusion matrix in Figure 4.12, True positive (TP) = 7.2e+02 = 7.2×10^2 = 720, True negative (TN) = 7.6e+02 = 7.6×10^2 = 760, False positive (FP) = 0.0e+00 = 0,
False negative (FN) = 1.3e+01 = 1.3×10^1 = 13.

Based on the confusion matrix presented in Figure 4.12, the performance scores of the CNN-RF (concatenation) model are thus calculated through the following evaluation metrics:

$$\text{Precision}=\frac{\text{TP}}{\text{TP+FP}}=\frac{720}{720+5} = 1.0000 = 100.00\%$$

$$\text{Recall} = \frac{\text{TP}}{\text{TP+FN}} = \frac{720}{720+13} = 0.9823 = 98.23\%$$

$$\text{F1 score} = \frac{\text{2TP}}{\text{2TP+FP+FN}} = \frac{2\times720}{(2\times720)+0+13} = 0.9911 = 99.11\%$$

$$\text{Accuracy} = \frac{\text{TP+TN}}{\text{TP+TN+FP+FN}} = \frac{720+760}{720+760+0+13} = 0.9913 = 99.13\%$$

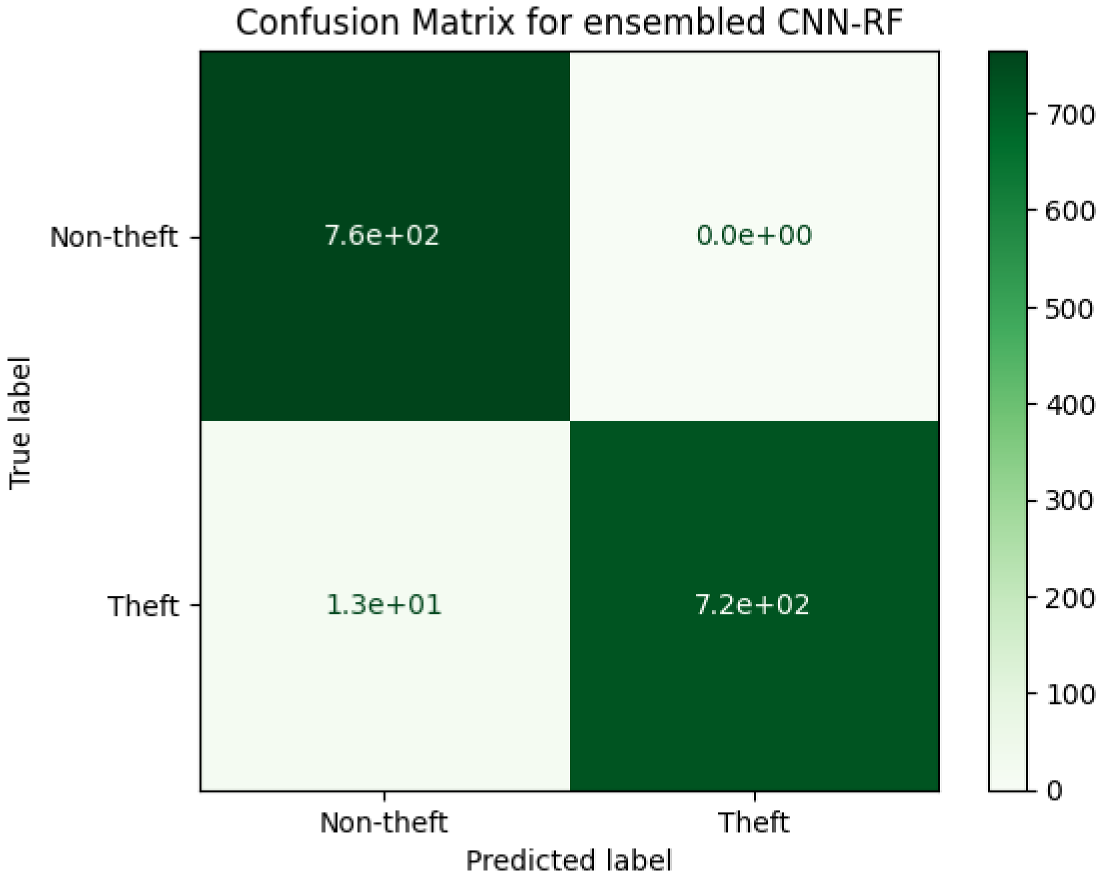


Figure 4.12: Confusion matrix of the CNN-RF (concatenation) model

$$\text{TNR} = \frac{\text{TN}}{\text{TN+FP}} = \frac{760}{760+0} = 1.0000 = 100.00\%$$

$$\text{MCC}=\frac{\text{TP}\times\text{TN-FP}\times\text{FN}}{\sqrt{(\text{TP+FP})(\text{TP+FN})(\text{TN+FP})(\text{TN+FN})}}$$

$$\therefore \text{MCC} = \frac{(720\times760)\text{-}(0\times13)}{\sqrt{(720+0)\times(720+13)\times(760+0)\times(760+13)}} = 0.9827 = 98.27\%$$

$$\text{FPR} = \frac{\text{FP}}{\text{FP+TN}} = \frac{0}{0+760} = 0.0000 = 0.00\%$$

$$\text{FNR} = \frac{\text{FN}}{\text{FN+TP}} = \frac{13}{13+720} = 0.0177 = 1.77\%$$

For the CNN-RF (concatenation) model, AUC score of 0.9912 (99.12%) and the PR-AUC value of 0.9955 (99.55%) at 0.5 decision threshold were obtained from the IDE. The summary of results for the CNN, RF, and CNN-RF (concatenation), and the proposed CNN-RF models are shown in Table 4.1.

Table 4.1: Summary of the performance scores

Model	Precision	Recall	F1 score	Accuracy	TNR	FPR	FNR	MCC	AUC	PR-AUC
CNN	0.9995	0.9848	0.9921	0.9925	0.9996	0.0004	0.0152	0.9850	0.9994	0.9995
RF	1.0000	0.9823	0.9911	0.9913	1.0000	0.0000	0.0177	0.9827	0.9912	0.9955
CNN-RF (Concatenation)	1.0000	0.9823	0.9911	0.9913	1.0000	0.0000	0.0177	0.9827	0.9912	0.9955
Proposed CNN-RF	**1.0000**	**0.9836**	**0.9917**	**0.9920**	**1.0000**	**0.0000**	**0.0164**	**0.9840**	**0.9913**	**0.9955**

Results have shown that there is really no significant difference between the performance results of the proposed CNN-RF model and that of the CNN-RF (concatenation) model. Hence, the proposed CNN-RF model constructed by simply taking features from the Conv1D layer (Layer 1) of the CNN network to train the RF model, as shown in Figure 3.8 of Chapter 3, is preferred. In fact, the proposed CNN-RF model fared a bit better than the CNN-RF (concatenation) model in terms of performance results, as evident in Table 4.1. The proposed CNN-RF model is hereby adopted, while the CNN-RF (concatenation) model is thus dropped. Figure 4.13 shows the comparison of all the developed ETD models in a bar chart.

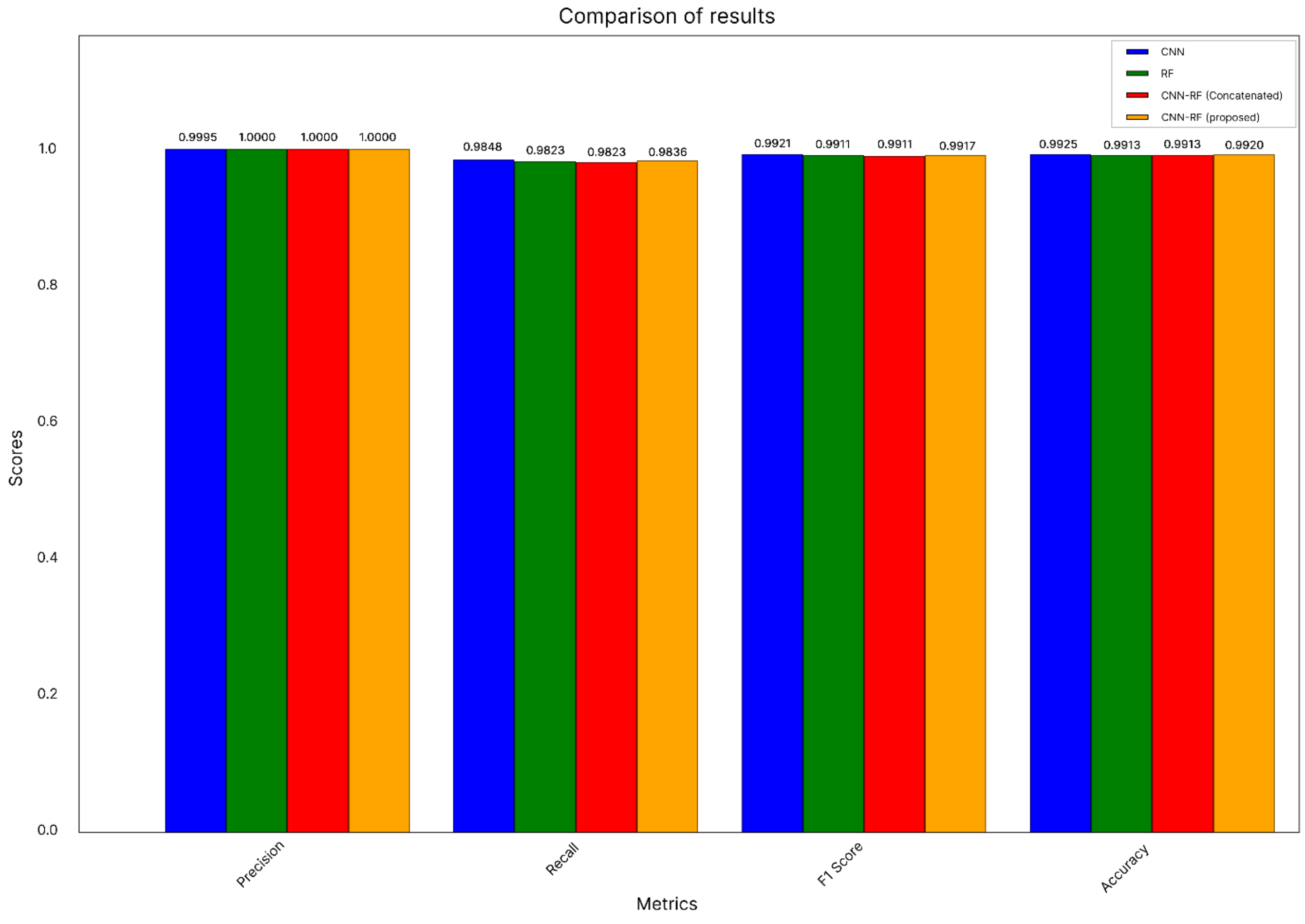


Figure 4.13: Bar chart showing comparison of performance results

The bar chart in Figure 4.13 shows the result comparisons of the models using precision, recall, F1 score, and accuracy metrics. Only four metrics vis-à-vis their performance scores are used in evaluating the developed models as shown on the bar chart. This is owing to economy of space, so that the bar chart could be more visible. Other scores of the performance metrics used in assessing the developed models are presented in Table 4.1. It is clear from the table and the bar chart that the proposed CNN-RF model performs best.

4.3 Pilot operation

Pilot operation in NTLD systems refers to the generation of customers' suspect list, and the manual field-operation exercise which serves as a follow-up process during NTL mitigation efforts (Messinis & Hatziargyriou, 2018:259). After the NTLD simulations, suspected electricity consumers are shortlisted. The suspect list contains those customers who may be engaging in ET after the theft suspects have been identified through the developed NTLD model. After collating the suspect list, a manual onsite inspection by the utility technicians or inspectors is next, to affirm or establish the ET culprits (Glauner et al., 2017:761; Messinis & Hatziargyriou, 2018:259). The proposed ETD model developed in this thesis provide utility domain experts with definitive and dependable identification of the suspected electricity thieves for reliable onsite inspections (Pamir, Javaid, Qasim, et al., 2022:56865).

The final verification of the suspect list is paramount, since the electric utilities cannot afford to inspect all their customers; as such adventure is very expensive, unaffordable, and practically infeasible (Yip, Wong, et al., 2017:230; Zheng et al., 2018:1606; Liao, Zhu, et al., 2024:5075). Suspect list is a list of electricity thieves as classified by the proposed ETD model. The suspect list for the CNN, RF, and the proposed CNN-RF models can be generated by implementing the Python codes in Section A.1.7 of the Appendix.

4.4 Implications of the model results

The relevance of this research extends to Africa, other developing nations, and the global electricity sector. The enhanced performance achieved through the proposed CNN-RF hybrid model has direct and far-reaching implications for improving ETD, optimizing grid operational efficiency, and promoting customer satisfaction. These improvements collectively result in significant cost savings for electric utilities, enhanced operational performance, and protection of consumer interests.

The cost-saving potential of the proposed model is particularly notable, as it reduces the need for frequent onsite inspections and minimizes the associated labour costs. By effectively identifying ET, the model also aids in revenue recovery by mitigating the financial losses traditionally incurred by electric utilities due to NTL. This recovered revenue contributes to the stabilization and growth of national economies, particularly in regions severely impacted by ET.

Furthermore, the proposed hybrid model enhances operational efficiency through its automated, real-time detection capabilities. This allows utility providers to swiftly address theft incidents, reducing response times and improving overall grid management. The robust performance of the proposed model which completely eliminates FPs, also reduces the likelihood of errors associated with manual inspections. Consequently, utility operators can leverage the insights generated by the CNN-RF hybrid model to better regulate electricity demand and supply, thereby facilitating more effective load management and ensuring stable service delivery.

In addition, the ability of the proposed model to detect irregular electricity consumption patterns fosters fair billing practices, which is crucial in protecting customers from being charged for electricity they did not consume. This, in turn, strengthens customer trust and confidence in utility providers. By promoting accurate billing and reducing theft-induced power disruptions, the proposed model supports the minimization of supply interruptions and contributes to overall power reliability. Ultimately, the proposed CNN-RF hybrid model serves as a vital tool for enhancing grid performance, improving financial stability within the electricity sector, and fostering sustainable electricity management, particularly in developing regions.

4.5 Comparison of results

To determine the efficiency of the proposed ETD model, there is a need to compare the performance or prediction results of the proposed model with the performance results of other scholars. This is done by comparing the results obtained through the proposed model and the results previously obtained in the existing literature by other researchers who have also built their various ETD models using the same SGCC dataset employed in developing the proposed model. The benchmarking is based on same dataset to ensure fair comparison of results. The SGCC dataset is a standardized popular electricity consumption dataset which is available online (Dai, 2018), and has been used by many prominent researchers in recent high-profile ETD literature for NTLDs. Hence, the comparison is done to determine the model that have fared much better (Janiesch et al., 2021:690). The employed SGCC dataset has been described in detail in Section 3.2.2 of Chapter 3.

The performance evaluation metrics such as precision, recall, F1 score, accuracy, MCC, AUC, and PR-AUC obtained through the proposed model have been compared with matching metrics presented in previous research. It should be noted that accuracy as a performance metric is not a reliable metric because it is always biased by default towards the majority class when using imbalanced datasets (Khan et al., 2020:15), unless the datasets are properly balanced using appropriate class-balancing techniques. However, since the SGCC dataset used in this research, as well as by other researchers in the selected literature have been balanced appropriately using various resampling techniques, the accuracy metric has however been considered for comparison.

4.5.1 Selected literature for comparison

Performance or prediction results in fifty-four (54) highly-rated journal articles published in IEEE, IET, MDPI, Elsevier, Springer, etc., between the years 2020 and 2024 have been selected as benchmarks for comparison with the prediction results of the proposed model. This is to establish the superiority, veracity, and potency of the proposed model in detecting NTL. To allow for unprejudiced comparison, the proposed model developed in this thesis and the ETD or NTLD benchmark models built in the selected literature have been developed using same dataset, as mentioned earlier in Section 4.5. The results of the performance assessment metrics like precision, recall, F1 score, accuracy, MCC, AUC, and PR-AUC of the proposed model and those of the ETD models in the selected literature are being compared.

Performance results are the predictions derived from ETD models using test sets from the given dataset. The various ETD models used in arriving at the performance results, the different data resampling techniques used in balancing the dataset, and other parameters used to enhance the predictions of the ETD models in the existing literature have also been mentioned in the SGCC dataset-based literature synopses in Section 4.5.1.1. Also, if the model performance scores in the literature have been presented originally in decimal, they are being converted to their percentage equivalents (to two decimal places) for comparison as shown in Table 4.2.

Performance metric results for precision, recall, F1 score, accuracy, MCC, AUC and PR-AUC metrics obtained from the proposed model has been used for comparison with the performance results from ETD models from the selected literature shown in Table 4.2. Any metric space in Table 4.2 which is filled with dash (–) shows that the value of such metric is not given in the referenced journal article. All the parameters attributable to the proposed model in Table 4.2 have been written in bold texts, while not applicable (N/A) appears in the reference space of the proposed model in the table. This is because the supposed reference of the proposed model with their performance results is this thesis. For authors who have developed more than one ETD model in the selected literature, only the results of the best performing models appear for comparisons in Table 4.2.

4.5.1.1 Synopses on the literature selected for comparison

This section gives the overview of each of the 54-selected journal articles in which the performance results of the ETD model in each article are being compared with the performance results of the proposed ETD model developed in this thesis. The performance results attained by the various benchmark ETD models in the selected literature and that of the proposed model have been realized using same SGCC dataset. The prediction results in the selected literature and that of the proposed model have been summarized in Table 4.2. Each of the following paragraphs is a rundown of every piece of literature selected for comparison.

Relational denoising autoencoder attention guided triple generative adversarial network (RDAE-AG-TripleGAN) model has been proposed by the authors in Aslam, Ahmed, et al. (2020) for ETD. The authors replaced the missing values in the SGCC dataset using linear interpolation, and also used the generator and classifier submodels of AG-TripleGAN to solve the class imbalance issue associated with the dataset. The missing values in the SGCC dataset are represented as not a number (NaN) and zero (0). The model results of 98.70% precision, 95.60% recall, 96.70% F1 score, 94.30% MCC, 95.20% AUC, and 95.80% PR-AUC have been obtained using the proposed ETD model.

The authors in Aslam, Javaid, et al. (2020) used a combination of long short-term memory (LSTM), UNet, and adaptive boosting (Adaboost) termed LSTM-UNet-Adaboost as ETD model. Interquartile minority oversampling technique (IQMOT) was used by the authors as class-balancing technique, and linear interpolation method to replace the missing values in the SGCC dataset. The model acheived prediction scores of 99.80% precision, 92.90% recall, 95.40% F1 score, 97.20% accuracy, 90.20% MCC, 94.80% AUC, and 95.80% PR-AUC.

Adaptive synthetic (ADASYN) sampling algorithm has been used by Khan et al. (2020) to address the class imbalanced problem and also deployed linear interpolation method to replace the missing values in the SGCC dataset. The balanced dataset is then fed into

Visual Geometry Group with 16 deep layers (VGG-16) module to detect anomalous patterns and to extract relevant features from the electricity consumption dataset. Firefly algorithm-based extreme gradient boosting (FA-XGBoost) is then used as the classifier or ETD model. The model achieved performances of 93.00% precision, 97.00% recall, 93.70% F1 score, 95.00% accuracy, 85.60% MCC, and 95.90% AUC.

Aldegheishem et al. (2021) presented two models for ETD. The first model has been termed SMOTEENN-AlexNet-LGB (SALM) model, while the second model is called generative adversarial network GoogLeNet adaptive boosting (GAN-NETBoost). The SMOTEENN in the first model is known as synthetic minority oversampling technique and edited nearest neighbour (ENN), while LGB is light gradient boosting. In the first model, SMOTEENN algorithm was employed to balance the dataset, Alexnet for feature extraction and dimensionality reduction, while LGB was used for the classification of benign and malignant customers. In the second model, conditional Wasserstein generative adversarial network gradient penalty (CWGAN-GP) was used for dataset balancing, GoogLeNet used for feature extraction and dimensionality reduction, while adaptive boosting (AdaBoost) was used for the classification of honest and fraudulent electricity consumers. The authors used linear interpolation method to replace the missing values in the SGCC dataset. The SALM model achieves 95.5% precision, 91.80% recall, 93.90% F1 score, Matthews correlation coefficient (MCC) of 87.60%, AUC of 90.60%, and accuracy of 91.00%; while the GAN-NETBoost achieves precision of 96.80%, recall of 94.00%, F1 score of 95.00%, MCC of 91.00%, AUC of 96.00%, and accuracy of 95.00%. Performance results have shown that the second model (GAN-NETBoost) performs better than the first model (SALM).

Arif et al. (2021) have suggested the use of three tree-based classifiers to predict ET using the SGCC dataset after using residual network (ResNet) to extract the hidden features in the dataset. The deployed tree-based classifiers for ETD are decision tree (DT), random forest (RF), and AdaBoost. The hybrid of synthetic minority oversampling technique with near miss (SMOTE-NM) has been used as the data balancing technique, linear interpolation method used to fill in the missing values, while Bayesian optimizer method has been deployed for hyperparameter tuning to facilitate the model optimization process. The results of the three tree-based classifiers with support vector machine (SVM) and linear regression (LR) are compared with or without feature extraction and resampling techniques, and hyperparameter tunings. From the results of all the mentioned ML models, RF produced the best prediction results of 99.17% precision, 94.92% recall, 96.93% F1 score, 99.10% accuracy, and 99.68% AUC after applying data balancing, ResNet, and hyperparameter tuning.

The deep artificial neural network (DANN) model proposed by Bohani et al. (2021) achieves the best performance results when the train and test data were split into 60:40 ratio. The authors ran the ETD simulations without balancing the SGCC dataset, and then used the mean of each customer's energy consumption on a particular row of the dataset to fill in the missing energy values of that particular customer. The proposed DANN model at the said 60:40 split ratio achieves precision of 48.24%, recall of 61.03%, F1 score of 53.89%, accuracy of 91.29%, and area under receiver operating characteristic curve (AUC) of 77.54% as the best performance sores when compared with other classifiers.

The hybrid model of day, week, and month convolutional neural network and random forest (DWMCNN-RF) has been used as a classifier by Cheng et al. (2021) for ETD. Dimensionality reduction of the dataset and increase in computation speed have been achieved by K-means clustering. To deal with the missing values in the dataset, the authors removed the missing values and also removed the zero values in the dataset. From the confusion matrix derived through the predictions of the DWMCNN-RF model, 97.70% of precision, 87.47% of recall, 92.30% of F1 score, 99.00% of AUC, and 90.65% of accuracy have been achieved by the ETD classifier.

Hussain et al. (2021) uses categorical boosting (CatBoost) algorithm as ETD model to predict consumers who steal electricity and the honest consumers who do not engage in electricity theft. K-nearest neighours (KNN) technique using the mean of selected nearest neighbours has been used to replace the missing values of the dataset used in developing the ETD model. Synthetic minority oversampling technique-and Tomek link (SMOTE-Tomek) algorithm has been used as resampling technique to balance the dataset, feature extraction and scalable hypothesis (FRESH) algorithm has been used as feature extraction, while tree-SHapley Additive exPlanation (tree-SHAP) algorithm has been used to interpret the decision of the ETD model. The model achieved an average precision, recall, F1 score, and accuracy metrics of 95.08%, 92.37%, 93.71%, and 93.38% respectively.

Javaid (2021) developed AlexNet and peephole long short-term memory echo state neural network (APLSTM-ESNN) model for ETD. SMOTE-Tomek or ST-Links was used by the authors for data balancing, APLSTM used as feature extractor from the dataset, grey wolf optimization (GWO) technique used for hyperparameter tuning to improve the performance of the model, ESNN as the classifier, and a paired t-test has been applied on the classification results of the model to ensure reliable assessment. The author used data interpolation method to handle the missing values in the SGCC dataset. The ETD model precision of 90.00%, recall of 92.10%, F1 score of 92.00%, accuracy of 96.30%, MCC of 84.00%, AUC of 96.40%, and PR-AUC of 97.30% as performance results.

The authors in Javaid, Gul, et al. (2021) proposed two ETD solutions. The authors proposed GANCNN model in the first ETD solution. GANCNN is the combination of self-attention generative adversarial network (SAGAN) and wide and deep convolutional neural network (WDCNN). The first ETD solution involved using adaptive synthetic edited nearest neighbour (ADASYNENN) as class balancing technique and locally linear embedding (LLE) technique for feature extraction. The authors also proposed ERNET model as the second ETD solution. ERNET is the hybrid of EfficientNet, ResNet, and gated recurrent unit (GRU). The second ETD model involved using sparse auto encoder (SAE) for feature extraction and a robust optimizer known as root mean square propagation (RMSProp) was used to improve the rate of learning of the model and SMOTEENN as class balancing technique. Imputation method has been used to replace the missing values in the SGCC dataset when applying GANCNN model, while linear interpolation method has been used to replace the missing values in the SGCC dataset when applying ERNET model to the dataset. Both GANCNN and ERNET were used for the classification of honest and fraudulent electricity consumers. The GANCNN model achieved the precision of 95.00%, recall of 99.00%, F1 score of 90.00%, accuracy of 95.00%, AUC of 98.50%, and FPR of 5.00% as performance values, while ERNET model achieved 94.00% precision, 93.00% recall, 89.00% F1 score, 98.00% accuracy, 98.80% AUC, and 2.00% FPR as prediction results. From the results, the GANCNN model has superior scores in terms of precision, recall, and F1 score metrics and hence adjudged to perform better than the ERNET model.

In Javaid, Jan, et al. (2021), the authors proposed an integrated deep siamese network (DSN) model for ETD. The DSN is a hybrid of CNN and LSTM. The authors also used ADASYN as class balancing technique. In the DSN, CNN actually performed feature extraction, while LSTM performed the classification of benign and malignant electricity customers. The authors replaced the missing values in the SGCC dataset using linear interpolation method. The effectiveness of the proposed model has been conveyed through the 91.20% precision, 92.30% recall, 92.80% F1 score, 95.30% accuracy, 93.40% AUC, and 90.00% MAP scores achieved as the best performance results at 80% training ratio.

The authors in Mujeeb et al. (2021) proposed differential evolution random undersampling boosting (DE-RUSBoost) as first classifier and Jaya random undersampling boosting (Jaya-RUSBoost) as second classifier for ETD. Also, the authors used reconstruction independent component analysis-based sparse autoencoder (RICASAE) feature extractor to extract relevant features from the given datasets. The authors used linear interpolation method to fill in the missing values in the dataset. Using the SGCC dataset, DE-RUSBoost classifier achieved precision of 90.20%, recall of 73.50%, accuracy of 95.60%, AUC of 89.60%, and specificity or TNR of 99.60%, while the Jaya-RUSBoost classifier achieved precision of 57.20%, recall of 100.00%, accuracy of 96.40%, AUC of 95.70%, and specificity (TNR) of 96.20% as performance evaluation scores. The Jaya-RUSBoost model obviously achieved better prediction results.

Pereira and Saraiva (2021) submitted that data balancing is most critical to achieving better prediction outcomes in terms of ETD, and hence used data-balancing techniques to improve NTLD. The authors used CNN as the ETD model and experimented with cost-sensitive learning (weighting), random undersampling (RUS), random oversampling (ROS), k-medoids based undersampling, synthetic minority oversampling technique (SMOTE), and cluster-based oversampling (CBOS) as class-balancing techniques to handle the imbalanced SGCC dataset used in constructing the ETD model. The authors also used linear interpolation method to fill in the missing values in the dataset. At the end of the ETD experiment, CBOS data-balancing technique achieved the overall-best prediction results of 68.33% accuracy and 80.84% AUC with the CNN model.

The authors, Shehzad et al. (2021), achieved AUC of 96.00% and PR-AUC of 97.00% as performance results using hybrid GoogLeNet and GRU as ETD model at 80% training ratio proportion. Time least square generative adversarial network (TLSGAN) has been used by the authors to solve the class imbalance problem, while also using linear interpolation method to replace the missing values in the SGCC dataset.

Arif et al. (2022) employed temporal convolutional network with enhanced multilayer perceptron (TCN-EMLP) as ETD model to classify honest and fraudulent electricity customers. The authors also applied Tomek link borderline synthetic minority oversampling technique with support vector machine (TBSSVM) as resampling technique to equalize the imbalanced dataset in order to achieve the most-reliable prediction results, while also deploying linear interpolation method to replace the missing values in the SGCC dataset. The proposed TCN-EMLP classifier model achieved the greatest AUC of 84.00% as performance measure using the SGCC dataset.

The NTLD model developed by Asif et al. (2022) involves combining two-dimensional convolutional neural network (2D-CNN) and bidirectional long short-term memory (Bi-LSTM) network. The authors employed bidirectional Wassertein generative adversarial network (Bi-WGAN) as data balancing technique, and linear interpolation method to fill in the missing values in the SGCC dataset. The proposed model achieved precision of 97.00%, recall of 92.00%, F1 score of 94.00%, accuracy of 95.00%, MCC of 93.00%, AUC of 97.00%, and PR-AUC of 98.00% as performance results.

Badawi et al. (2022) have proposed a two-stage ETD processes. The first stage involved the extraction of new features from the SGCC dataset. Extraction of new features from the default SGCC electricity consumption dataset involved sudden-change detection method which detected sudden jump or unusual change in electricity consumptions. The newly extracted features from the sudden-jump (fraudulent) patterns in energy consumptions were moving average measures like auto-regressive integrated moving average (ARIMA), Holt-Winters, seasonality, etc. The new features included smart meter features and other mentioned statistical features, and were used in conjunction with electricity consumption data. In the second stage, distributed random forest (DRF) was used as ETD classifier and also handled the missing values in the SGCC dataset. DRF used the features in stage one for the classification of honest and fradulent consumers. In this ETD experiment, the authors took 7,000 samples (520 fraudulent, 6,480 honest) from the dataset out of the total available 42,372 samples (3,615 fraudulent, 39,757 honest). The ETD model achieved precision of 99.00%, recall of 98.00%, F1 score of 98.00%, accuracy of 98.00%, MCC of 97.00%, AUC of 98.33%, specificity (TNR) of 99.00%, mean squared error (MSE) of 0.14%, root mean squared error (RMSE) of 2.00%, log loss or cross entropy of 3.13%, and R-squared (R^2) or coefficient of determination of 99.46% as performance measures.

The authors in Fei et al. (2022) proposed a self-supervised method for ETD to cater for situations where fully labelled data may not always be available. The authors implemented this method by using NTL detection contrastive prediction coding (ND-CP) model. The ND-CP model was used to extract long-term consumption patterns from the SGCC dataset to detect NTL, but not short-term features which was determined using Pruned Exact Linear Time (PELT) method. PELT was able to detect sudden or unexpected consumption changes in the dataset and provided evidences for using long-term consumption patterns in detecting NTL better than short-term consumption patterns. ND-CP involved using 1D-CNN to encode a sequence of the SGCC dataset into a matrix, and then employing GRU compact to summarize the matrix and make it compact . The authors removed customer samples with up to 100 missing values and systematically splited the aftermath data into unlabelled pretrain, and labelled train and test sets to balance and handle the missing values in the dataset. The proposed method leveraged on the unlabelled data to improve ETD rates. Although, the SGCC dataset is already labelled from source, but the larger part of the labelled samples were ignored by the authors to satisfy the proposed method, in an attempt to accomplish better ETD than most supervised models. To achieve the self-supervised method, the authors pretrained the ND-CP model with large unlabelled samples from the dataset to extract long-term consumption-pattern features, and then trained a single-layer neural network with the extracted long-term features and tested it using the remaining fewer labelled data samples to classify or predict the honest and faudulent customers. The proposed ETD model achieved F1 score of 78.90%, accuracy of 77.00%, and AUC of 83.20% as evaluation scores.

Gao et al. (2022a) used hybrid convolutional long short-term memory (ConvLSTM) classifier which supports default or raw format of the SGCC consumption dataset as input into NTLD model with a batch normalization meant to improve training and testing efficiencies. Borderline-synthetic minority oversampling technique (borderline-SMOTE) was employed for class balancing, and KNN technique to handle the missing values in the dataset. The NTLD model with tenfold cross validation achieves the better performance results of 98.40% precision, 94.80% recall, 96.60% F1 score, 96.60% accuracy, 97.70% AUC, and 98.00% PR-AUC.

A combined Kernel and Tree Boosting (KTBoost) classifier, an ensemble-based classifier, which used Jaya algorithm to optimize its hyperparameters (Jaya-optimized combined KTBoost) has been deployed by Hussain et al. (2022) for NTLD. The classifier used Robust-SMOTE as class balancing technique and also used the intelligence of extreme gradient boosting (XGBoost) algorithm to estimate and fix the missing values in the SGCC dataset. This ETD method achieved the precision of 95.08%, recall of 93.18%, F1 score of 93.71%, accuracy of 93.38%, and MCC of 90.77% as performance results.

Khan et al. (2022) developed a multi-model that is based on combination of ML and deep learning (DL) algorithms called data preparations, first and second-order classification (PFSC) to detect abnormality in electricity consumption patterns. The first-order classifier is based on SVM, RF and gradient boosting decision tree (GBDT) machine learning (ML) methods, while the second-order classifier uses a temporal convolutional network (TCN). The data preparation aspect of PFSC involves interpolation, outlier detections, normalization, and balancing (IONB). The authors used linear interpolation method to replace the missing values in the SGCC dataset. The highest performance results achieved by the multi-model (PFSC) at 80% train proportion are 96.40%, 95.40%, 95.90%, 98.50% for precision, recall, F1 score, and AUC respectively. The proposed PFSC framework performed better than the benchmarked individual ML and DL models.

Khattak et al. (2022) proposed a hybrid of GRU and CNN models termed HGC for ETD. GRU was used to extract temporal patterns, while CNN was used to extract hidden or latent patterns from the SGCC dataset. ADASYN and Tomek links were used to resample and balance the dataset, while linear interpolation method was used to handle the missing values in the dataset. The better performance results of the HGC model achieved at 60% training data are 92.10% recall, 94.8% F1 score, 94.70% accuracy, 98.70% AUC, and 98.50% PR-AUC.

In the journal article written by Lepolesa et al. (2022), a fully connected feed-forward deep neural network (DNN) classifier was deployed as the ETD model, principal component analysis (PCA) was used to reduce the feature size, Bayesian classifier was utilized to optimize hyperparameter tuning, while minimum redundancy maximum relevance (mRMR) has also been used to validate the most essential features for ETD. The features used for the classification were time and frequency domains which have been manually extracted from the raw time-series SGCC dataset. The classification done with the frequency-domain features outperforms that done with time-domain features, and also outperforms that done when both domains are combined. The mRMR scheme was also used to ratify and consolidate the significance of frequency-domain features for ETD over the features in their time domains. The authors used Piecewise Cubic Hermite Interpolating Polynomial (PCHIP) technique to replace the missing values in the SGCC dataset. The prediction results of the proposed classifier achieve accuracy of 91.80% and AUC of 97.00% as performance measures.

The authors in Liao et al. (2022) achieved highest performance scores of 78.70% AUC, and 98.10% MAP@100, and 95.40% MAP@200 at 70% training ratio using the proposed GCN-CNN hybrid model. GCN is graph convolutional neural network which perform graph convolutional procedures by depicting temporal correlation or time dependency and periodicity of consumer load curve from the perspective of graph, as captured through the adjacency matrix. Meanwhile, CNN captured the latent features in the load curve using Euclidean convolutional processes. Latent features were modelled from load curves at different fraudulent ratios. The proposed model performed better than the benchmark models at various training and fraudulent ratios or data imbalances. The higher metrics (AUC and MAP) obtained at different fraudulent ratios indicated that the proposed model is more robust and adaptable to model latent features from the load curves. The effect of class imbalance was being suppressed by randomly selecting samples from the raw dataset to form new dataset and then varying the fraudulent ratios of the train and test sets. Linear interpolation method was deployed to fill in the missing values in the SGCC dataset.

Munawar, Javaid, et al. (2022) used the hybrid of Bi-GRU and Bi-LSTM as a classifier to predict benign and malignant electricity consumers. The authors also deployed Tomek links to address the issue of misclassification of defused data, abstract features were extracted using stochastic feature engineering to enhance classification, K-means SMOTE technique was used to balance the SGCC dataset, while mean-based was deployed to replace the missing values in the dataset. The hybrid ETD model achieved performance scores of 80.60% precision, 80.90% recall, 80.70% F1 score, 95.00% accuracy, and 95.00% AUC. The performance of the classifier was eventually verified using an attack vector.

Munawar, Khan, et al. (2022) deployed an effective hybrid classification architecture which consists of attention layers, LSTM, and inception modules termed AttenLSTMInception as the proposed model to detect ET using the SGCC dataset. In this approach, the authors only considered six months of data of 1500 honest customers from the SGCC dataset owing to their limited computing resources. In these selected 1500 honest customers, the authors used six false data injections (FDIs) to manipulate each honest customer sample, such that, six new variants of fraudulent samples are synthesized for a single honest sample. This then disrupts the class balancing in the dataset creating more fraudulent samples. The novel FDI techniques were compared with the six theft attack cases used in Pamir, Javaid, Javaid, et al. (2022). The complexity and variance introduced into the data distribution by the FDI techniques and the six theft cases were determined via kurtosis and skewness analysis. The complexity and skewness introduced into the data by the FDI techniques are minimal when compared with that of the six theft attacks. Simple imputer method was employed to replace missing values and remove outliers in the data. Data inconsistency after the data synthesis was eventually tackled by balancing the dataset using a novel resampling technique called Proximity Weighted Synthetic Oversampling (ProWsyn). The proposed model achieved precision of 97.00%, recall of 94.00%, F1 score of 96.00%, accuracy of 95.00%, and AUC of 98.00% as performance measures.

The authors in Pamir, Javaid, Javaid, et al. (2022) explored the combination of LSTM and GRU to form an ETD model called theft attacks-based LSTM and GRU (TLGRU). This work is an extension of the work in Pamir et al. (2021). Technically, the LSTM performed feature extraction, while GRU did the classification. Simple imputer technique was used to replace the missing values in the SGCC dataset, while artificial theft attacks that produced synthetic theft samples were used to balance the dataset. The TLGRU model achieved 97.96%, 86.59%, 91.92%, 91.56%, 91.68%, and 1.00% for precision, recall, F1 score, accuracy, AUC, and FPR respectively as prediction results.

Meanwhile, the authors in Pamir, Javaid, Qasim, et al. (2022) used autoencoder and bidirectional gated recurrent unit (AE-BiGRU) model for ETD. Six artificial theft attacks that generated synthetic theft samples were used to balance the imbalanced SGCC dataset, while simple imputer method was used to replace the missing values in the dataset. The bidirectional gated recurrent unit (BiGRU) was used for identifying patterns in the consumption data. The results obtained from the AE-BiGRU ETD classifier are 91.30% precision, 88.60% recall, 89.90% F1 score, 90.10% accuracy, 90.10% AUC, and 10.20% FPR.

In the ETD experiments performed by Ullah et al. (2022), AdaBoost model has been used as the classifier, AlexNet used to handle dimensionality reduction, near miss used as the class-balancing technique for the imbalanced SGCC dataset, while linear interpolation method was used to fill in the missing values in the given dataset. The hyperparameters of Adaboost and AlexNet have also been tuned using bee colony optimization algorithm, otherwise known as artificial bee colony (ABC). The following performance results were obtained owing to the ETD experiments are: 86.00% precision, 84.00% recall, 85.00% F1 score, 88.00% accuracy, 78.00% MCC, and 91.00% AUC.

The authors in Ali et al. (2023) proposed a stacking model for ETD. The stacking model involved the combination of the prediction outputs of LGB, extra trees, XGBoost, and RF ensemble models with an MLP deep learning model which served as a meta-classifier. The combined prediction outputs of the ensemble models served as input features to the MLP model. The MLP model was used to improve the predictions of the ensemble models. The predictions of the MLP model or meta-classifier served as the final predictions of the stacking model. The authors also used PCA technique for feature extraction and data reduction, while SVM-SMOTE was being used as the class-balancing technique. To balance the dataset, SVM was first used to separate the theft and honest samples, while SMOTE was later used to oversample the theft samples to balance the SGCC dataset. The authors deployed simple imputer technique to reinstate the missing values in the SGCC dataset. The stacking model achieved F1 score of 97.66%, accuracy of 97.69%, AUC of 97.69%, PR-AUC of 96.55%, FPR of 0.72%, and FNR of 2.05% as performance results at 80% training and 20% testing ratios.

Appiah et al. (2023) applied SMOTE-Tomek to balance the imbalanced SGCC dataset, extremely randomized trees classifier as the proposed model to detect ET, and grid search optimization technique to optimize the proposed model. The authors also deployed linear interpolation technique to fill in the missing values in the dataset. The proposed model produced precision of 97.00%, detection rate (recall) of 98.00%, F1 score of 98.00%, accuracy of 98.00%, MCC of 95.06%, and AUC of 99.65% as ETD performance scores.

In the journal article written by Bai et al. (2023), the authors deployed a CNN model which constitutes a dual-scale and a dual-branch (DSDB) structure with periodic intra and inter convolutional blocks, and a transformer network called Gaussian weighting (GWT) network, to form a novel hybrid neural network termed DSDBGWT. The novel hybrid ETD model was able to effectively discover anomalies in the electricity consumption dataset. The CNN-based DSDB structure enabled comprehensive feature extraction from the SGCC dataset during the process of shallow feature extraction, decreased parameter usage, and increased efficiency. The transformer network-based GWT module was able to augment the feature-extracting ability of DSDB by extracting characteristic features from extended-distance sequences or dependences of longer duration in a more logical manner, allowing the attention mechanism to further be rationally allocated. The authors addressed the missing values in the dataset using zero replacement and binary mask approach. The hybrid DSDBGWT model has proven to be more efficient in extracting anomalies in electricity consumption dataset with increased F1 score, AUC, and MAP@ALL metric values of 62.90%, 92.30%, and 82.30% respectively as performance evaluation scores.

Kawoosa et al. (2023) used XGBoost ensemble algorithm as ETD model, trained and tested the model using energy consumption data from the SGCC dataset, in conjunction with additional features like location, seasonality, weekends, weekdays, regional festivals, and high-demand power curtailments taken from auxiliary databases as input data to train and test the XGBoost classifier. According to the authors, the additional data improved the capacity of the model in detecting NTL by reducing false positives. Six artificial theft attacks which generated synthetic fraudulent samples have been used to balance the dataset, while the dimension of the dataset was reduced using PCA. The missing values in the given dataset have been replaced using the forward filling method. The performance results obtained were 98.00% precision, 98.00% recall, 97.00% F1 score, and 3.00% FPR.

The authors in Khan et al. (2023) used sequential preprocessing, resampling, and classification (SPRC) as ETD framework. The sequential preprocessing aspect of the framework involves interpolation, outliers handling, and standardization (IOS), hybrid data resampler (HDR) was used for resampling to balance the dataset, and classification was done with improved artificial neural network (iANN). Linear interpolation method was deployed to inpute the missing values in the SGCC dataset. The authors achieved the best results through iANN using parallel sequential topology at 80% training ratio. The SPRC framework achieves 99.60% precision, 98.70% recall, 99.10% F1 score, 99.70% accuracy, and 98.70% AUC.

The ETD model termed DenseNet-GRU-LightGBM has been used in Naeem, Aslam, et al. (2023). DenseNet-GRU-LightGBM model is a hybrid of densenet-fully convolutional network (DenseNet-FCN) and gated recurrent unit (GRU) with a light gradient boosting machine (LightGBM). Random oversampling using both classes (ROBC) sampling technique has been used by the authors to balance the imbalance real-world SGCC dataset used in developing the proposed model. The authors also used linear interpolation method to fill in the missing values in the SGCC dataset. The proposed ETD model achieved precision of 92.00%, recall of 96.00%, AUC of 92.00%, and PR-AUC of 87.00%.

In Naeem, Javaid, et al. (2023), the authors proposed the application of seasonal and trend decomposition using loess (STL), fractal network (FractalNet), and LightGBM as ETD model. STL was used to transform the pattern of electricity consumption in the SGCC dataset into seasonality and trend, FractalNet was used to learn the seasonality and trend of benign and malignant customers, while LightGBM was employed to improve on the learning capacity of FractalNet and to classify both the benign and malignant customers in the dataset. A novel hybrid oversampling and undersampling using both classes (HOUBC) was used as the class balancing technique by performing undersampling from the majority class first, before oversampling both from the majority and minority classes. The two classes mentioned in HOUBC are the honest and fraudulent labels or classes in the electricity consumption dataset. However, linear interpolation method was utilized to handle the missing values in the SGCC dataset. LightGBM model was used for the classification of honest and fraudulent customers, and hence achieved the following performance results: 94.20% precision, 96.10% recall, 93.30% F1 score, 96.20% accuracy, 94.20% MCC, 92.10% AUC, and 90.40% PR-AUC.

The precision, recall, F1 score, accuracy, and AUC values of 92.00%, 54.00%, 15.00%, 92.00%, and 54.00% respectively have been obtained by Nawaz et al. (2023) in their SGCC dataset-based ETD experiments. The mentioned performance metrics have been realized through the proposed hybrid convolutional neural network and extreme gradient boosting (CNN-XGB) ETD model developed by the authors. The proposed CNN-XGB model also achieved a PR-AUC value close to 1. The authors used linear interpolation method to replace the missing values in the given dataset.

In the journal publication authored by Nayak and Jaidhar (2023), the authors intended to achieve higher ETD prediction results by using fewer features from the SGCC dataset. To address the class imbalance issue of the SGCC dataset, the number of benign samples were made equal to the number of fraudulent samples by random selection. Each missing value (NaN or 0) in the given dataset were imputed separately with random values that lie between the minimum and maximum values of the features in the missing-value column. Experiments were carried out using mutual information, low variance filtering, and PCA as feature selection and extraction techniques to optimize the classification processes. RF, SVM, KNN, Naïve Bayes, and DT were used as ETD classifiers to determine which model would perform best after the various feature selections and extractions from the dataset. Experimental results revealed that RF classifier with 30 PCA components or features (PCA-30) performed best and achieved 98.60%, 93.80%, 95.82%, and 98.90% as precision, recall, accuracy, and AUC scores respectively.

Pamir et al. (2023) presented the combination of SSA, GCAE, and CSLSTM termed SSA-GCAE-CSLSTM as ETD model. SSA is salp swarm algorithm, GCAE is a combination of GRU and convolutional encoder known as gate convolutional autoencoder, while CSLSTM is a combination of cost-sensitive learning and LSTM. The authors handled the missing values in the SGCC dataset using linear interpolation method. The presented ETD model achieved precision of 99.45%, recall of 92.66%, F1 score of 95.93%, accuracy of 92.25%, and AUC of 71.13% as performance results.

The authors in Wang et al. (2023) proposed an NTLD model that is based on convolution-non-convolution parallel deep network (CNCP). In this method, the output of two fused deep heterogenous neural networks have been used for ETD. The CNCP-based two deep neural networks captured the features in the load time-series of the SGCC dataset at different time scales before fusing their outputs to produce the NTLD results. However, the load time series data of the benign electricity customers have obvious periodicity in different time frames when compared with the load time series data of the customers who stole electricity. To cater for the missing values in the SGCC dataset, the load profile of a customer is discarded if the missing-value ratio of the customer to the whole dataset is greater than 30%. After that, weighted interpolation is then used to correct the remaining missing values. The CNCP-based method achieved precision of 95.08%, recall of 98.70%, and F1 score of 96.85% at 80% training sets of the dataset.

The improved hybrid WDCNN model developed by Xia et al. (2023) achieved F1 score value of 53.72%, AUC of 83.61%, and mean average precision (MAP@100) of 97.08% as highest performance assessment scores at 70% train ratio. MAP@100 means MAP among top 100 electricity users. The authors used focal loss to solve the data imbalance problem and also used Lagrange interpolation method to replace the missing values in the employed SGCC dataset.

The authors in Yang et al. (2023) made use of broad learning system-based (BLS-based) multi-view rotation model to improve ETD performances. The proposed ETD method is termed rotation_dwbls and involved the design of rotational subspaces which maps the raw samples in the SGCC dataset into distinct sub-views to remove the negative impacts of redundant features in the dataset, and mitigate the effect of the characteristic class-imbalance distribution nature of the dataset using a weighting mechanism and a weighted broad learning system (BLS). Transformation of dual space or rotation of features was meant to generate more accurate and robust ensemble classifier, weighting strategy was based on regional distribution of the data and took into cognizance the distribution of the data and class imbalance, and thirdly the selection of progressive ensemble model after BLS-based models have been trained from various views are the cores of the rotation_dwbls approach. The proposed ETD model achieved AUC of 83.41% and geometric mean (G-mean) of 83.90% as prediction results, achieving the best performance when the authors compared it with existing ML models.

The authors, Yao et al. (2023), deployed an ETD scheme called multiscale convolutional neural network-bidirectional gate recurrent unit (MCNN-BiGRU) to classify the honest and fraudulent electricity consumers. The authors used convolutional transformer-Wasserstein generative adversarial network (CT-WGAN) as the class balancing technique to augment and equalize the SGCC dataset. To handle the missing values in the given dataset, the authors applied linear interpolation method for consecutive missing values less than three days, and assigned zero if otherwise. The ETD scheme achieved precision of 95.67%, recall of 91.48%, F1 score of 93.53%, accuracy of 91.10%, and AUC of 93.00% as the best performance results at different training ratios using the SGCC dataset.

Huang et al. (2024) leveraged on the weekly periodic consumption and weekly anomalous consumption patterns attributable to normal and fraudulent customers in the SGCC dataset to enhance ETD. The features of these weekly-scale electricity consumption features were integrated with the default daily-scale consumption features of the dataset to form dual-time features. The hybrid of TCN with LSTM multi-level feature extraction module termed LSTM-TCN, and deep convolutional neural network (DCNN) were used to extract the dual-time features from the SGCC dataset. Meanwhile, SMOTE-Tomek links was used as class balancing technique to equalize the imbalanced dataset. Linear interpolation method was used to replace the missing values in the given dataset. The novel strategy proposed by the authors to enhance ETD was based on the use of LSTM-TCN and DCNN in extracting dual-time features from the dataset. The extracted features were then fused into a fully connected layer as input features for classification to validate the novel NTLD framework. ETD classification as processed by the fully connected layer achieved 93.20% precision, 96.40% recall, 94.80% F1 score, 94.70% accuracy, and 98.60% AUC as performance measures.

In another quest to improve the accuracy and efficiency of ETD models using the SGCC dataset, Iftikhar et al. (2024) proposed a hybrid ETD model of MLP and GRU (MLP-GRU), and used k-means SMOTE as a class-equalizing technique to balance the dataset. The authors used simple imputer method to replace the missing values in the given dataset. The hybrid MLP-GRU model achieved precision of 97.50%, recall of 95.00%, F1 score of 94.00%, accuracy of 93.33%, MCC of 85.00%, AUC of 100%, PR-AUC of 95.00%, and test loss of 20.00% as metric performances at 90% and 10% train and test ratios respectively. Khan et al. (2024) used RUS technique to balance the imbalanced SGCC dataset during data preprocessing, and then also applied AlexNet for reducing the dimension of the SGCC dataset and for feature extraction to enhance ETD. After these, a CNN model was deployed for ETD. The authors used data interpolation technique to replace the missing values in the given dataset. The CNN model achieved precision of 89.00%, recall of 86.00%, F1 score of 84.00%, and accuracy of 86.00% as ETD results. The authors also experimented with unpreprocessed SGCC dataset using fully connected neural network as the ETD model, but the preprocessed dataset expectedly achieved better ETD results.

The authors in Liao, Bak-Jensen, et al. (2024) explored optimal sample selection of dataset features as a proposed strategy to reduce dataset annotation efforts within a limited budget in a bid to maximize ETD prediction performances. Although the employed SGCC dataset is already annotated or labelled by default but the comprised annotations were not considered by the authors. This approach tends to improve ETD from the perspective of data by selecting the most useful samples instead of the conventional approach of improving model performances through enhancing the structure of the ETD model. The authors proposed uncertainty-based sample (UBS) annotation, fraud class-based sample (FBS) annotation, and distance-based sample (DBS) annotation as the three innovative strategies for the selection of the optimal samples for annotation in the SGCC dataset for ETD. Linear interpolation was employed to impute the missing values in the given dataset, while part of the functions of the FBS strategy was to handle the class-imbalance problem. The SGCC dataset was divided into three different sizes of datasets (dataset 1, dataset 2, and dataset 3) before applying the novel strategies. Dataset 1 was referred to as small dataset, dataset 2 as medium dataset, and dataset 3 as large dataset in accordance with the sizes of their training samples. Simulations were carried out separately on each of the three datasets with sample annotations of 500, 1500, 3000, and 4500 on each of the three datasets at different fraudulent ratios and different ETD classifiers. The results of baseline or traditional strategies like random sampling (RS), clustering-based sampling (CS), and density estimation-based sampling (DES), including when the datasets were without any annotation have also been compared with the novel strategies. Simulation results showed that the results of the novel strategies were better than the baseline strategies. MLP, CNN, RF, XGBoost, and LightGBM were used as ETD classifiers. Overall, the FBS strategy produced the best results of 90.20% F1 score, 77.80% AUC, 95.90% MAP@100, and 93.00% MAP@200, at 1500 sample annotations using dataset 2 and XGBoost as classifier. The proposed novel strategies are capable of improving ETD better across range of ML classifiers when compared with the traditional ML strategies.

Also, the authors in Liao, Zhu, et al. (2024) have proposed DetectGAT model for ETD. DetectGAT is a modified graph attention network (GAT), a new neural network model which captures the periodicity and latent features of electricity consumption data through dynamic graphs, for the purpose of ETD. DetectGAT refers to using GAT in dynamic-graph domain for ETD after initially converting the electricity consumption data into a graph. This is done by migrating GAT from conventional static graph inferences to ETD-based dynamic graph inferences. Dynamic graphs allow necessary structural adjustments in order to capture periodicity and latent features from the SGCC dataset. The authors used linear interpolation method to replace the missing values in the given dataset. The DetectGAT model achieved AUC of 78.90%, MAP@100 of 98.10%, and MAP@200 of 95.60% as the best performance results during group 3 experiment when the ETD model proposed by the authors (DetectGAT) was applied to the SGCC dataset.

Mehdary et al. (2024) employed XGBoost model for ETD and a metaheuristic algorithm called genetic algorithm (GA) to enhance the performance of the model. The GA was used to finetune the hyperparameters of XGBoost model to optimize the ETD metric performances. The authors utilized linear interpolation method to replace the missing data in the SGCC dataset, and also used SMOTE and ensemble methods to balance the dataset. The performance metrics like precision, recall, accuracy, and the AUC of the ETD model improved significantly after tuning hyperparameters using GA to optimize the XGBoost model. After hyperparameter tunings, the performance metric value of precision increased from 75.00% to 92.00%, recall increased from 68.00% to 89.00%, accuracy increased from 82.00% to 97.80%, while AUC also increased from 78.00% to 96.00%.

The authors in Nirmal et al. (2024) proposed the hybrid of CNN and AdaBoost as ETD model. The CNN extracts important features from the preprocessed SGCC dataset, while AdaBoost classifies the benign and fraudulent electricity customers. Meanwhile the authors used SMOTE as the class balancing technique to equalize the benign and fraudulent consumer samples in the SGCC dataset. Also, linear interpolation method was used to fill in the missing values in the dataset. The proposed model eventually achieved 94.07% precision, 95.73% recall, 95.60% F1 score, 96.35% accuracy, 57.00% AUC, 28.80% RMSE, and 8.29% mean absolute error (MAE) as evaluation scores to determine the model performances.

In another attempt to develop an efficient NTLD model using the SGCC dataset, Shahzadi et al. (2024) proposed Time Series Lag Embedded Network (TLENET) as ETD model to classify honest and fraudulent electricity customers. The authors used Wavelet Transform, Fastfood Transform, and Nyström Transform as dimensionality reduction methods. They also used Localized Random Affine Shadowsampling (LoRAS) as a class-balancing technique, and a game theory-based SHapley Additive exPlanation (SHAP) method to interpret the output of the proposed DNN model. Aside LoRAS, other class-balancing techniques like Adaptive Oversampling Minority Samples (ADOMS), Synthetic Minority Oversampling Borderline-Data (SMOBD), Minority Cloning Technique (MCT), Random Oversampling Examples (ROSE), and Proximity Weighted Synthetic Oversampling (ProWSyn) were also experimented, but LoRAS proved to be a better technique in terms solving overfitting problem, and producing low variance with respect to the classifier output. The authors deployed simple imputation method to fill in the missing values in the SGCC dataset. The TLENET model achieved 92.00% F1 score, 94.00% accuracy, 93.00% AUC, and 87.00% MCC as performance scores using LoRAS class-balancing technique, and Wavelet Transform for dimensionality reduction. The Wavelet Transform produced better prediction scores with the TLENET classifier and LoRAS class-balancing technique than other experimented dimensionality reduction methods.

Wang et al. (2024) deployed multi-step model based on LSTM to fill in the missing data in the SGCC dataset, and hybrid federated learning-based stacking ensemble gate recurrent unit (FL-SE-GRU) algorithm which utilized the optimal features from the dataset as the ETD model. The authors introduced artificial theft attacks from nine cyberattack models which produced nine different types of data attacks on the SGCC dataset in order to balance the dataset. The model achieved 96.6% precision, 93.8% sensitivity or recall, 95.1% F1 score, and 95.0% accuracy as ETD performance results.

The authors in L. Zhu et al. (2024) proposed a model that significantly reduced the inherent high costs associated with the manual labelling of electricity consumption datasets used in developing ETD or NTLD models. This is in addition to the authors' fundamental objective of achieving desirable performance scores to ensuring significant ET or NTL reduction in electric grids. These objectives were accomplished by developing an intelligent and cost-effective ETD model which is an incorporation of deep learning (DL) and active learning (AL) termed deep active learning (DAL). DAL involved splitting the default annotated dataset into labelled and unlabelled sets. The DAL scheme constitute the combination of CNN with Bayesian AL or Bayesian active query that is based on Monte Carlo dropout. The CNN algorithm dealt with the ETD aspect, while the Bayesian AL tackled the data annotation aspect of the scheme. The Bayesian AL assisted in deriving a discriminative CNN model that require minimum data annotations without compromising the detection reliability of the proposed DAL model. Class-balancing of the SGCC dataset was not considered by the authors, but forward interpolation method was used to replace the missing values in the dataset. The proposed model achieved 93.02% accuracy, 81.91% AUC, 91.67% MAP@100, and 87.89% MAP@200. The DAL model enhanced cost-effective data annotation with reliable performance scores. The DAL scheme culminates in about 66.7% reduction in manual data annotation costs.

Finally, S. Zhu et al. (2024) presented a combination of Omni-Scale CNN (OS-CNN) and AutoXGB models termed OS-CNN-AutoXGB as the proposed model for ETD. The OS-CNN was used for feature extraction, while AutoXGB was utilized for hyperparameter optimization and classification of benign and malignant electricity consumers. The authors deployed SMOTEENN as the class-balancing technique, and Piecewise Cubic Hermite Interpolating Polynomial (PCHIP) method to replace the missing values in the SGCC dataset. The OS-CNN-AutoXGB model achieved 97.50% precision, 94.10% recall, 95.50% F1 score, 99.20% accuracy, and 98.40% AUC as experimental assessment results showing the predictive powers of the model.

Table 4.2: Performance comparison of the proposed ETD model and other SGCC dataset-based models presented in the literature

S/No.	Model	Precision (%)	Recall (%)	F1 Score (%)	Accuracy (%)	MCC (%)	AUC (%)	PR-AUC (%)	Reference
1.	RDAE-AG-TripleGAN	98.70	95.60	96.70	–	94.30	95.20	95.80	(Aslam, Ahmed, et al., 2020)
2.	LSTM-Unet-Adaboost	99.80	92.90	95.40	97.20	90.20	94.80	95.80	(Aslam, Javaid, et al., 2020)
3.	(FA-XGBoost)	93.00	97.00	93.70	95.00	85.60	95.90	–	(Khan et al., 2020)
4.	GAN-NETBoost	96.80	94.00	95.00	95.00	91.00	96.00	–	(Aldegheishem et al., 2021)
5.	ResNet+RF	99.17	94.92	96.93	99.10	–	99.68	–	(Arif et al., 2021)
6.	DANN	48.24	61.03	53.89	91.29	–	77.54		(Bohani et al., 2021)
7.	K-means+DWMCNN-RF	97.70	87.47	92.30	90.65	–	99.00	–	(Cheng et al., 2021)
8.	FRESH+treeSHAP+CatBoost	95.08	92.37	93.71	93.38	–	–	–	(Hussain et al., 2021)
9.	AlexNet+APLSTM-ESNN	90.00	92.10	92.00	96.30	84.00	96.40	97.30	(Javaid, 2021)
10.	LLE+GANCNN	95.00	99.00	90.00	95.00	–	98.5	–	(Javaid, Gul, et al., 2021)
11.	DSN	91.20	92.30	92.80	95.30	–	93.40	–	(Javaid, Jan, et al., 2021)
12.	RICASAE+Jaya-RUSBoost	57.20	100.00	–	96.40	–	95.70	–	(Mujeeb et al., 2021)
13.	CBOS+CNN	–	–	–	68.33	–	80.84	–	(Pereira & Saraiva, 2021)
14.	GoogLeNet+GRU	–	–	–	–	–	96.00	97.00	(Shehzad et al., 2021)
15.	TCN-EMLP	–	–	–	–	–	84.00	–	(Arif et al., 2022)
16.	2D-CNN+Bi-LSTM	97.00	92.00	94.00	95.00	93.00	97.00	98.00	(Asif et al., 2022)
17.	Default and generated statistical features+DRF	99.00	98.00	98.00	98.00	97.00	98.33	–	(Badawi et al., 2022)

18.	ND-CP+single-layer neural network	–	–	78.90	77.00	–	83.20	–	(Fei et al., 2022)
19.	ConvLSTM	98.40	94.80	96.60	96.60	–	97.70	98.00	(Gao et al., 2022)
20.	Jaya algorithm+KTBoost	95.08	93.18	93.71	93.38	90.77	–	–	(Hussain et al., 2022)
21.	PFSC	96.40	95.40	95.90	–	–	98.50	–	(Khan et al., 2022)
22.	HGC	–	92.10	94.80	94.70	–	98.70	98.50	(Khattak et al., 2022)
23.	PCA+Bayesian classifier+Mrmr+DNN	–	–	–	91.80	–	97.00	–	(Lepolesa et al., 2022)
24.	GCN-CNN	–	–	–	–	–	78.70	–	(Liao et al., 2022)
25.	Tomek links+BiGRU-BiLSTM)	80.60	80.90	80.70	95.00	–	95.00	–	(Munawar, Javaid, et al., 2022)
26.	AttenLSTMInception	97.00	94.00	96.00	95.00	–	98.00	–	(Munawar, Khan, et al., 2022)
27.	TLGRU	97.96	86.59	91.92	91.56	–	91.68	–	(Pamir, Javaid, Javaid, et al., 2022)
28.	AE-BiGRU	91.30	88.60	89.90	90.10	–	90.10	–	(Pamir, Javaid, Qasim, et al., 2022)
29.	ABC+AlexNet+AdaBoost	86.00	84.00	85.00	88.00	78.00	91.00	–	(Ullah et al., 2022)
30.	PCA+stacking model	–	–	97.66	97.69	–	97.69	96.55	(Ali et al., 2023)
31.	Grid search optimization technique+extremely randomized trees	97.00	98.00	98.00	98.00	95.06	99.65	–	(Appiah et al., 2023)
32.	DSDBGWT	–	–	62.90	–	–	92.30	–	(Bai et al., 2023)
33.	PCA+XGBoost	98.00	98.00	97.00	–	–	–	–	(Kawoosa et al., 2023)
34.	SPRC	99.60	98.70	99.10	99.70	–	98.70	–	(Khan et al., 2023)

35.	DenseNet-GRU-LightGBM	92.00	96.00	–	–	–	92.00	87.00	(Naeem, Aslam, et al., 2023)
36.	STL-FractalNet-LightGBM	94.20	96.10	93.30	96.20	94.20	92.10	90.40	(Naeem, Javaid, et al., 2023)
37.	CNN-XGB	92.00	54.00	15.00	92.00	–	54.00	–	(Nawaz et al., 2023)
38.	PCA+RF	98.60	93.80	–	95.82	–	98.90	–	(Nayak & Jaidhar, 2023)
39.	SSA-GCAE-CSLSTM	99.45	92.66	95.93	92.25	–	71.13	–	(Pamir et al., 2023)
40.	CNCP	95.08	98.70	96.85	–	–	–	–	(Wang et al., 2023)
41.	WDCNN	–	–	53.72	–	–	83.61	–	(Xia et al., 2023)
42.	rotation_dwbls	–	–	–	–	–	83.41	–	(Yang et al., 2023)
43.	MCNN-BiGRU	95.67	91.48	93.53	91.10	–	93.00	–	(Yao et al., 2023)
44.	LSTM-TCN+DCNN	93.20	96.40	94.80	94.70	–	98.60	–	(Huang et al., 2024)
45.	MLP-GRU	97.50	95.00	94.00	93.33	85.00	100.00	95.00	(Iftikhar et al., 2024)
46.	AlexNet+CNN	89.00	86.00	84.00	86.00	–	–	–	(Khan et al., 2024)
47.	FBS+XGBoost	–	–	90.20	–	–	77.80	–	(Liao, Bak-Jensen, et al., 2024)
48.	DetectGAT	–	–	–	–	–	78.90	–	(Liao, Zhu, et al., 2024)
49.	GA+XGBoost	92.00	89.00	–	97.80	–	96.00	–	(Mehdary et al., 2024)
50.	CNN-AdaBoost	94.07	95.73	95.60	96.35	–	57.00	–	(Nirmal et al., 2024)
51.	Wavelet Transform+LoRAS+TLENET	–	–	92.00	94.00	87.00	93.00	–	(Shahzadi et al., 2024)
52.	FL-SE-GRU	96.6	93.8	95.1	95.0	–	–	–	(J. Wang et al., 2024)
53.	DAL	–	–	–	93.02	–	81.91	–	(L. Zhu et al., 2024)

54.	OS-CNN-AutoXGB	97.50	94.10	95.50	99.20	–	98.40	–	(S. Zhu et al., 2024)
55.	**Proposed CNN-RF**	**100.00**	**98.36**	**99.17**	**99.20**	**98.40**	**99.13**	**99.55**	**N/A**

The result comparisons in Table 4.2 have shown that the proposed CNN-RF model outperformed all other SGCC dataset-based ETD models presented in the existing literature. The higher performance-metric values obtained through the proposed CNN-RF model have shown that the proposed model generalizes better (Khan et al., 2020:22) and is more reliable and accurate than all other SGCC dataset-based ETD classifiers which have been presented in the literature. The comparison has solidly established the superiority of the proposed model in ETD. As previously mentioned, the SGCC dataset-based NTLD models presented in the benchmark journal articles have been trained on same SGCC dataset which have also been used in training the proposed model, to ensure fair comparisons. Again, the referenced SGCC dataset-based ETD models and their prediction results in the existing literature were published between the years 2020 and 2024, and have been used as benchmarks to determine the effectiveness of the proposed model in detecting ET, as shown in Table 4.2. The superiority of the proposed model over the benchmark models represents a huge contribution and advancement to the field of NTLD, for the detection of NTL in Smart Grids.

4.6 Discussion

The first point of departure in the process of detection and mitigation of ET or NTL is to develop a formidable model to do so. In a bid to significantly contribute to knowledge in this research project, the aim of the thesis has been to build a formidable NTLD model that will profoundly detect ET better with greater mitigation prospects than the previously developed NTLD models in the existing literature. The CNN, RF, and the proposed CNN-RF hybrid models developed in this research have separately shown superior and impressive prediction results, but the classification results of the proposed CNN-RF model have shown better ETD predictions when compared exclusively with the results of either the standalone CNN model or the RF model. The proposed model has performed better than all the previously developed NTLD models in the existing literature. Those previously developed benchmark NTLD models in the previous research have also been constructed by employing the same SGCC dataset used in developing the proposed model. It is noteworthy to mention that the higher the detection capacity of an ETD model, the better its onsite mitigation prospects.

Fifty-four (54) recent NTLD models developed in the existing literature between the years 2020 and 2024 have been benchmarked with the proposed model, and the results obtained through the models have shown that the proposed model produces the best results as presented in Table 4.2, showing enhanced detection performances which will eventually spur greater mitigation of NTL in electric grids. The higher predictive power obtained vis-à-vis the proposed model is a fulfilment of the aim and objectives of the research, and is also a means of proffering answers to the research questions. NTLD models with greater prediction results promote healthier electric grids with enhanced electricity availability, help the electric utilities to generate more profits, stimulate economic growths and foster sustainable economies, aid security of citizens, and bolster technological advancements since most inventions and innovations in modern societies largely dependent on the availability of electricity.

4.7 Conclusion

The proposed CNN-RF model shows very excellent and interesting results. Overall, the proposed model has performed better than all the previously presented ETD models in the selected literature. The ETD models presented in the previous research, which are compared or benchmarked with the proposed model, have all been developed using same SGCC dataset. It is reasonable to compare different types of NTLD models to be able to ascertain the models with the best predictive powers (Janiesch et al., 2021:690). The comparison of the performance results of the proposed CNN-RF model developed in this thesis with the performance results of the recently developed SGCC dataset-based ETD models presented in the existing literature is the benchmark used in rating the efficacies and efficiencies of the proposed model with respect to other NTLD models.

The performance results achieved by the proposed model are superior and constitute the major contribution of this research project. The increased performance scores obtained from the proposed model indicates better NTLD. Better NTLD would further spur more-reliable and more-efficient onsite inspections for better mitigations of ET in the power grids. Onsite mitigation efficiency is premised on the detection capacities of ETD models. The higher NTL detections achieved in this research, as indicated by the performance results of the proposed model through the performance assessment metrics, have seamlessly proffered answers to the research questions, while also simultaneously fulfilling the aim and objectives of the research project. Better mitigations of ET enhance grid stability and reliability, ensure more revenues and profits to the electric utilities, and also help in improving the economies of nations worldwide. These are feats which the proposed model is poised to achieve based on its higher prediction scores. Without reducing NTL significantly in the power grids, the United Nations' vision of "electricity for all" by the year 2030 (Javaid, Jan, et al., 2021:44) would definitely be unrealized.

CHAPTER 5

CONCLUSIONS AND RECOMMENDATIONS

5.1 Introduction

Additional electricity generation to cater for extrinsically-induced energy losses is not sustainable without drastically curtailing electricity theft (ET) or non-technical losses (NTL) in the power grids. ET has triggered dire economic consequences as it has caused financial losses close to US$100 billion per year to electric utilities all over the world (Coma-Puig et al., 2024:2705; Kim et al., 2024:2; Shahzadi et al., 2024:2; L. Zhu et al., 2024:256). Since it is impossible to completely eliminate ET in the power systems, the motivation for this research is premised on the quest to further prune ET in the distribution networks to the barest minimum, using the state-of-the-art artificial intelligence-based (AI-based) machine learning (ML) methods. This is done by improving the existing electricity-theft detection (ETD) methods, which is necessary to obtain more robust, effective, efficient, and reliable models for better NTL detections (NTLDs).

The effort of this research project is primarily geared towards detecting and mitigating ET better in Smart Grid (SG) using real-world dataset. The proposed ETD model is basically developed to further increase NTLD performances, in order to achieve a more satisfactory mitigations of ET in the power grids. This chapter concludes the research by summarizing all the previous chapters of the thesis, recapping the performance results of the developed model, while also highlighting the essence and contributions of the research. Lastly, this chapter gives other supplementary suggestions and prospects that could further assist in the future detections and mitigations of NTL.

5.2 Conclusions

Chapter 1 of this thesis underscores the importance of electricity to humanity and also establishes the concept of ET including its historical background, forms, causes, effects, and its detection and mitigation approaches. The statement of the research, the salient research questions, the aim and objectives of the research, its delineation, significance, research contributions as well as the organization of the thesis have also been discussed in the introductory chapter. Chapter 2 is a review of the literature. The review centres on the evolution of the electricity grids and the electricity meters. Various NTL prevention, detection and mitigation techniques which form the core of this research have also been reviewed in the chapter. Chapters 3 and 4 are the experimental part of the thesis. Chapter 3 dealt with the methodology employed in modelling the ETD systems, while Chapter 4 explicates the experimental results and their interpretations. This chapter (Chapter 5) is the final chapter of the thesis and thus summarizes the research project as a whole and recommends possible future directions that would tend to supplement the existing ETD and ET mitigation efforts in a bid to further stem the spate of NTL in the electricity grids.

We have been able to establish earlier in the previous chapters that AI-based NTLD methods are the predominant, cost-effective, and the most reliable techniques for predicting customers who may likely steal electricity or cause NTL. Using the AI-based methods, electricity consumers with suspicious or irregular consumptions are then shortlisted for onsite inspections. Using AI methods reduce unnecessary, unilateral, and costlier onsite inspections associated with the traditional NTLD methods, thereby lessening the cost of NTL mitigations in electricity systems.

The ETD model developed in this thesis is more reliable and efficient, and are even of greater importance and benefits, especially now that the spate of ET has increased geometrically in the developing countries, while also considerably rising in the developed countries. The proposed CNN-RF model is therefore recommended for use by electric utilities to reduce NTL in their various distribution networks (Iftikhar et al., 2024:02). NTL must be significantly reduced to enhance healthy, reliable, and sustainable electric grids. Apart from reducing energy poverty, a thriving electricity grid with low NTL achieves economy of scale, which proportionally translates into increase in utility revenues that ensure profits to the power supply companies, and improves national economies.

Countries in the modern world depend on reliable electricity as a major economic driver because there is hardly a sector in any progressive economy that do not require electricity to function. A reliable electricity supply translates into economic prosperity, creates more job opportunities, and helps to improve the social well-beings among citizens (Wabukala et al., 2023:1, 3). Therefore, developing formidable ETD models with high-predictive powers, which will assist in reducing NTL significantly in the electric grids is of greater economic value. Reducing ET in the power grids to a bearable minimum is a serious task that must be accomplished. The proposed CNN-RF model developed in this research project achieved unprecedented increase in performance results, and such improvement will pave way for significant NTL reduction in power grids.

5.2.1 Summary of results

To address our research questions in a bid to fulfill the aim and objectives of this study, there is a need to develop an ETD model that would be more efficient (i.e., produce higher metric performances) with very-low false positives (FPs) or false alarms. We have been able to develop such model to fulfill the veracity of the research project. The NTLD simulations were carried out using Python in a Google Colab Integrated Development Environment (IDE), using the real-world dataset released by the State Grid Corporation of China (SGCC). The SGCC dataset used in constructing the proposed model has also been used in several existing high-profile literature for developing several ETD models. This provides a good ground for comparing the performance results of the proposed model with the performance results of other ETD models in the previous research. The proposed ETD model developed in this research project with the dataset provided by SGCC performed better than all the previous ETD or NTLD models that have been developed in the existing literature using the same dataset.

The NTLD simulation started with the modelling of convolutional neural network (CNN) model, after which the random forest (RF) model was instantiated, and the two models were later combined by feeding features from the MaxPooling1D layer of the CNN model into RF model to form a hybrid model termed CNN-RF. The hybridization is done in a bid to obtain optimal results. Combination of models and hyperparameter tunings of models have been formidable means of optimizing models in order to achieve better prediction performances (Poudel & Dhungana, 2022:117; Vincent & Jidesh, 2023). The detailed Python codes used in implementing the proposed ETD model can be found in the Appendix.

The proposed CNN-RF model achieved precision of 100.00%, recall of 98.36%, F1 score of 99.17%, accuracy of 99.20%, Matthews correlation coefficient (MCC) of 98.40%, area under the receiver operating characteristic curve (AUC) of 99.13%, area under precision-recall curve (PR-AUC) of 99.55%, true negative rate (TNR) of 100.00%, false positive rate (FPR) of 0.00%, and false negative rate (FNR) of 1.64% as prediction scores. However, before the hybridization of CNN and RF models to form the proposed model, CNN model achieved 99.95 % precision, 98.48% recall, 99.21 F1 score, 99.25% accuracy, 98.50% MCC, 99.94% AUC, 99.95% PR-AUC, 99.96% TNR, 0.04% FPR, 1.52% FNR, while RF model achieved precision of 100.00%, recall of 98.23%, F1 score of 99.11%, accuracy of 99.13%, MCC of 98.27%, AUC of 99.12%, PR-AUC of 99.55%, TNR of 100.00%, FPR of 0.00%, and FNR of 1.77% individually as performance results. We have so far been able to obtain the highest and superior ET prediction results with the proposed CNN-RF model when compared with the previous models presented in previous research which have also employed same SGCC dataset used in this work. The table that compares and summarizes the results of the proposed model and other SGCC dataset-based ETD models (presented in the existing literature) can be found in Table 4.2 in Section 4.5.1.1 of Chapter 4.

5.2.1.1 Contributions to knowledge

Building reliable, efficient, and formidable NTLD model is the core of any realistic and cost-effective effort towards ET detection and mitigation. Hence, the development of such model is the basis of the contribution of this research project. The mitigation efficiency of ET after building an ETD model is a function of the predictive or detection power of the developed model. The classification efficiency of the proposed model is directly proportional to their performance scores. The greater the performance scores, the higher the predictive power of the model. Utility technicians will achieve very efficient and cost-effective onsite mitigations of ET if the model upon which they have premised their mitigation efforts achieves higher performance scores (Messinis & Hatziargyriou, 2018:259). Higher performance scores indicate higher model efficiency, signifying low false positives and low false negatives. The construction of more accurate and more efficient ETD model can significantly contribute to the field of energy management to enhance energy security. The proposed model can help utility companies to reduce revenue losses and improve the overall reliability of electricity in distribution systems. The developed NTLD model is robust, efficient, and reliable. The success achievable by utility inspectors during onsite NTL mitigation efforts is directly correlated with the performance of the built model.

It is clear from the comparison of results shown in Table 4.2 in Section 4.5.1.1 of Chapter 4 that the proposed CNN-RF model outperforms all the existing models that were previously developed using the same SGCC dataset employed in this research. The performance results of the recent SGCC dataset-based ETD models presented in the existing literature never surpassed the performance results of the proposed model. We have been able to improve on the efficiency status quos of the previous NTLD models presented in the previous research. The detection performance comparisons are based on the employment of same SGCC dataset for the model developments, but with different methods of model implementations. This is in a bid to reveal the ETD models that have achieved better performance results.

Based on the information available to us, the performance results obtained through the proposed ETD model developed in this research project are unprecedentedly better when compared with the results of other previously developed NTLD models in the previous research. Those previously developed models in the literature have also been constructed using the same SGCC dataset employed in developing the proposed model. The proposed model is characterized with excellent NTLD results based on the increased predictive power of the model as revealed via their performance results. The higher performance scores achieved by the proposed model have seamlessly proffered answers to the research questions, and have also simultaneously provided the premise for fulfilling the aim and objectives of the research.

Apart from the obtained performance results with their excellent predictive powers which shows the efficacy of the proposed model in mitigating ET, the discovery of the proposed CNN-RF model itself (which serves as a means to achieving the ends) is also a huge contribution to the research. Based on the information available to us, no previous work has explored the combined strengths of CNN and RF in developing ETD model by applying the employed SGCC dataset. The results of the proposed model have revealed that integration of models by leveraging on their combined strengths could generate a more robust, accurate, and cost-effective ETD model. The summary of the key contributions of the research, which has been categorized into theoretical, methodological, and practical aspects, is presented in Table 5.1.

Table 5. 1: Summary of the key contributions of the research

Type of contribution	Impact
Theoretical	**i.** The proposed hybrid model bridges deep learning (CNN) with ensemble learning (RF). **ii.** It enhances generalization on small datasets. **iii**. Replacement of fully connected layers that do classification in CNN with RF for better efficiency. **iv.** Interpretability of deep learning improves with the feature importance analysis of RF, which allows insights into the extracted CNN features to determine those that contributed most to classification.
Methodological	**i.** RF model is trained on the hierarchical features extracted from CNN layers instead of training it on raw data. **ii.** The hybrid model reduces the computational cost that may arise when only CNN model is deployed. **iii**. RF model handles noisy and imbalanced data better than CNN.

	iv. The hybrid model works well across different data types, like the time series data used in developing the proposed ETD model. It also generalizes well with image data and tabular data.
Practical	**i.** The hybrid model achieves higher performance results when handling real-world tasks than when either CNN or RF model is implemented individually. **ii.** It enables efficient deployment of edge computing. **iii**. The model fosters better generalization to tasks. **iv.** The hybridization of the deep and ensemble models enhances the interpretability of the new composite model and make it suitable and applicable for better decision making in real-life situations.

5.3 Recommendations for future work

To further improve the detection and mitigation of ET or prevent it in the future, the following recommendations are made:

(a) Design of stronger firewalls as a formidable cybersecurity system for the Smart Grid (SG) system, to ensure that the advanced metering infrastructures (AMIs) and their smart meters (SMs) are more secured in order to prevent probable cyber-physical attacks. The envisioned intelligent cybersecurity framework should be able to automatically preempt and keep track of the latest probable AMI and SM hacking techniques and keep updating its database in a bid to always anticipate, stem, and be a step ahead of potential attackers of the AMIs and SMs. It is only when the SGs are secured against cyber-physical attacks that any NTLD system developed using data from SGs could become effective and reliable. Interdisciplinary collaboration among experts in fields like data science, cybersecurity, and energy management can bring diverse perspectives and expertise to the development of more robust ETD models.

(b) Building explainable ML models for ETD can enhance more transparency and trust in NTL predictions, and counter the black-box issues associated with ML (Coma-Puig et al., 2024). Explainable ML models would fortify algorithms with augmented reality or cognition that would allow domain experts to decipher the underlying reasons behind the predictions or decisions made by NTLD models. For example, an explainable ML model for NTLD would be able to interpret the reasons why a particular customer steals electricity. The intuitive nature of explainable ML would further enhance the protection of the grid against NTL and tremendously increase the efficiency of physical onsite inspections. Electric utilities need explainable ML models to justify theft classification decisions before taking legal actions against customers. Explainable ML should be explored to build ETD models that will further reduce NTL in the electric power systems to promote healthier grids.

(c) Exploring ways to integrate ETD models with several other grid management systems that forecast energy consumptions. Such integrated system can provide domain experts with firm and holistic control of the grids.

(d) Developing novel feature engineering methods specific to ETD can improve model performances and help in better extraction of more meaningful insights from raw datasets.

(e) Utility technicians should improve the inspection accuracies of their onsite surveillances by avoiding false positives (false alarms) and false negatives. This would ensure correct labelling of input dataset which would then be used to develop reliable NTLD systems or models to enhance better ET predictions (Messinis & Hatziargyriou, 2018:262; Saeed et al., 2020:16; Liao, Zhu, et al., 2024:5075).

(f) AI-based automated NTLD models could only reliably predict those consumers who steal electricity and those who do not, but would not be able to inspect the premises of the customers to confirm NTL or enforce the law to mitigate ET after the theft may have been confirmed. However, to enhance reduction of NTL, the criminal law of every country must include ET which should be enforced against the culprits. Governments of various countries should revise their electricity acts and include ET among major crimes that should attract stringent penalties.

Any crime like ET which culminates in bringing the economic activities of any country down should be given priority attention, and must be tackled with utmost seriousness and sincerity. Governments of various realms should reform and empower the law enforcement agents and make them available to the utilities for immediate arrest of confirmed electricity thieves. The role of the law enforcement agents in the fight against ET is very significant, as six electricity thieves including a teacher were recently caught by the utility inspectors and arrested by the law enforcement agents in a joint operation in Osogbo, Osun State, Nigeria for stealing electricity via tampering their meters (Ezediuno, 2023). The functionality of security agents in the fight against ET cannot be overemphasized. Also, special or dedicated courts should be established in all realms to enhance speedy hearing, trial, and prosecution of ET offenders. The Jamaican electric utility, Jamaica Public Service Company (JPS), is clamouring through the Government for the establishment of special utility courts in the country in order to quickly bring electricity thieves to book (Campbell, 2021). However, the governments of Sierra Leone (Sesay, 2021) and Pakistan (Dawn, 2023) have already considered the concept of special courts to try ET offenders, while the Nigerian authority (Aduloju, 2024) is also currently considering this important measure to hasten the prosecution of ET culprits in a bid to specially curb the theft of electricity. Special courts will enhance quick prosecution of electricity thieves, and such will debar future reoccurrences of the crime.

(g) Raising public awareness about ET to sensitize citizens that stealing electricity is an illegal act, including rolling out its legal implications under the law and encouraging customers to report suspected consumers who engage in theft. Erasing through publicities the dubious notions among some citizens who think electricity should be a social service (Onat, 2018:166; Ojoye, 2019; Shokoya & Raji, 2019b:469), and also obliterate such among those who believe that electricity should be given for free by right or by entitlement (Robinson, 2014), are also very important steps in stemming the acts of stealing electricity.

(h) NTL prohibitive measure like publicizing the names and other particulars of stealing consumers in the available media, including launching whistleblowing platforms in a bid to “name and shame” the theft culprits has been used in some realms as mentioned in Section 2.4.4 of Chapter 2 to avert ET. Such prohibitive measure has proven to be very effective (Antmann, 2009:24), and should be sustained as a veritable tool to further prevent NTL in the power grids. This method is very potent as many electricity consumers are media-shy and are always keen to protect their names and those of their families, especially for the negative reasons. This method is recommended to those electric utilities around the world that have not yet adopted it.

(i) Researchers, especially those in the field of economics, social sciences, and humanities should do more innovative works on theoretical NTL mitigation-based studies and promulgate new economic and scientific theories that will make the payment of bills attractive to electricity customers, and enhance customer-utility relational engagements that will further strengthen the interrelationships between the utilities and their customers, in a bid to prevent or prohibit ET.

(j) The proposed NTLD solution could be potentially servitized (Janiesch et al., 2021:692-693) for future use in real-world applications by transferring its detection prowess to other utility domains across the world in the form of commercial NTLD software for optimal detection of ET (Iftikhar et al., 2024:02). Such software should be integrated with the AMI to enhance real-time monitoring of electricity customers for NTLD. This would then provide utilities with timely information to be able to take immediate action against electricity thieves, thus reducing NTL drastically. Using different or non-SGCC datasets from other utilities with the proposed model will also help to further establish its efficiency and effectiveness.

(k) The NTLD experiment in this research project and the majority of works on NTLD in the previous research mainly focus on detecting NTL in the low-voltage (LV) secondary distribution networks of the power grids because most dubious actions that cause NTL take place at this level of the grid (Kim et al., 2024:11). Future efforts should also be made to check NTL in the medium-voltage (MV) primary distribution networks and the high-voltage (HV) transmission networks. Although, majority of electricity thieves do not venture into theft at MV and HV network levels of the grid due to the intricacies and greater risks involved, but some sophisticated electricity thieves, powerful ET syndicates or mafia might perhaps be exploring the MV and HV network levels of the electric grid in a bid to steal electricity and later sell at cheaper rates (Depuru et al., 2011a:1010). Grid stakeholders or domain experts should be proactive and keep surveillance on the entire grid system to achieve optimal results in terms of NTLDs and NTL mitigations.

(l) Electric utilities, especially those in Africa, should upgrade to the next-generation grid otherwise known as SG, to enhance the efficiency and security of their electricity grids and to prevent ET by using the intelligent SMs with end-to-end real-time monitoring of energy consumptions through the AMIs. Additionally, with SMs more data will be available to diagnose the grid of NTL using the state-of-the-art AI-based ML methods (Gu et al., 2022:4568; Liao, Zhu, et al., 2024:5075).

(m) Open-access and anonymized real-world electricity consumption datasets should be made available by the utilities to advance the course of research in NTLDs. Big datasets that would reveal consumers' geographical spread and seasonal consumption changes over the years are recommended. This is necessary to capture the actual electricity consumption patterns of different electricity consumers, showing reasons behind diversity in their consumptions.

(n) Finally, future efforts should also be geared towards modifying and utilizing the proposed model to detect theft or fraud in non-electricity sectors like banking, insurance, capital markets, and accounting, etc.

REFERENCES

Abaide, A.R., Canha, L.N., Barin, A. & Cassel, G. 2010. Assessment of the smart grids applied in reducing the cost of distribution system losses. In *2010 7th International Conference on the European Energy Market*. IEEE: 1–6. http://ieeexplore.ieee.org/document/5558678/.

Abdul-Aziz, A., Amirrudin, S.A.-H. & Raya, L. 2023. Analysis and Monitoring Energy Consumption in Basic Electric Bills. In *2023 19th IEEE International Colloquium on Signal Processing & Its Applications (CSPA)*. IEEE: 248–251. https://ieeexplore.ieee.org/document/10087759/.

Abdullateef, A.I., Salami, M.J.E., Musse, M.A., Aibinu, A.M. & Onasanya, M.A. 2012. Electricity Theft Prediction on Low Voltage Distribution System Using Autoregressive Technique. *International Journal of Research in Engineering and Technology*, 1(5): 250–254. http://repository.elizadeuniversity.edu.ng/jspui/handle/20.500.12398/564.

Adam, A.A., Doud, K.R. & Boshara, M.M.K. 2021. Reduction of Basher City's Distribution Losses using Medium Voltage Network. In *2020 International Conference on Computer, Control, Electrical, and Electronics Engineering (ICCCEEE)*. IEEE: 1–3. https://ieeexplore.ieee.org/document/9429562/.

Aduloju, B. 2024. FG to set up tribunal for prosecution of electricity theft cases. *The Cable*. https://www.thecable.ng/fg-to-set-up-tribunal-for-prosecution-of-electricity-theft-cases/ 23 June 2024.

Afridi, A., Wahab, A., Khan, Shamsher, Ullah, W., Khan, Sheharyar, Ul Islam, S.Z. & Hussain, K. 2021. An efficient and improved model for power theft detection in Pakistan. *Bulletin of Electrical Engineering and Informatics*, 10(4): 1828–1837. https://beei.org/index.php/EEI/article/view/3014.

Aggarwal, C.C. 2023. *Neural Networks and Deep Learning*. Cham: Springer International Publishing. https://link.springer.com/10.1007/978-3-031-29642-0.

Aggarwal, S. & Kumar, N. 2021. Smart grid. In *Advances in Computers*. Elsevier Inc.: 455–481. http://dx.doi.org/10.1016/bs.adcom.2020.08.023.

Ahmad, M.W., Mourshed, M., Mundow, D., Sisinni, M. & Rezgui, Y. 2016. Building energy metering and environmental monitoring – A state-of-the-art review and directions for future research. *Energy and Buildings*, 120: 85–102. http://dx.doi.org/10.1016/j.enbuild.2016.03.059.

Ahmad, T., Chen, H., Wang, J. & Guo, Y. 2018. Review of various modeling techniques for the detection of electricity theft in smart grid environment. *Renewable and Sustainable Energy Reviews*, 82(August): 2916–2933. http://dx.doi.org/10.1016/j.rser.2017.10.040.

Ahmed, Mohsin, Khan, A., Ahmed, Mansoor, Tahir, M., Jeon, G., Fortino, G. & Piccialli, F. 2022. Energy Theft Detection in Smart Grids: Taxonomy, Comparative Analysis, Challenges, and Future Research Directions. *IEEE/CAA Journal of Automatica Sinica*, 9(4): 578–600. https://ieeexplore.ieee.org/document/9696293/.

AIEE. 1941. Progress in the art of metering electric energy I — Origins. *American Institute of Electrical Engineers (AIEE) - Electrical Engineering*, 60(9): 421–427.

http://ieeexplore.ieee.org/document/6432357/.

Ajenikoko, G.A. & Adelusi, L.O. 2015. Impact of Prepaid Energy Metering System on the Electricity Consumption in Ogbomoso South Local Government Area of Oyo State. *Computer Engineering and Intelligent Systems*, 6(5): 99–105. https://iiste.org/Journals/index.php/CEIS/article/view/22711/22612.

Aldegheishem, A., Anwar, M., Javaid, N., Alrajeh, N., Shafiq, M. & Ahmed, H. 2021. Towards Sustainable Energy Efficiency With Intelligent Electricity Theft Detection in Smart Grids Emphasising Enhanced Neural Networks. *IEEE Access*, 9: 25036–25061. https://ieeexplore.ieee.org/document/9344652/.

Alhelou, H.H. 2019. Under Frequency Load Shedding Techniques for Future Smart Power Systems. In *Handbook of Research on Smart Power System Operation and Control*. IGI Global: 188–202. http://services.igi-global.com/resolvedoi/resolve.aspx?doi=10.4018/978-1-5225-8030-0.ch007.

Ali, A., Khan, L., Javaid, N., Bouk, S.H., Aldegheishem, A. & Alrajeh, N. 2023. Mitigating anomalous electricity consumption in smart cities using an AI-based stacked-generalization technique. *IET Renewable Power Generation*: 1–14. https://doi.org/10.1049/rpg2.12785.

Aliyu, A.S., Ramli, A.T. & Saleh, M.A. 2013. Nigeria electricity crisis: Power generation capacity expansion and environmental ramifications. *Energy*, 61: 354–367. http://dx.doi.org/10.1016/j.energy.2013.09.011.

Alkhresheh, A., Al-Tarawneh, M.A.B. & Alnawayseh, M. 2022. Evaluation of Online Machine Learning Algorithms for Electricity Theft Detection in Smart Grids. *International Journal of Advanced Computer Science and Applications*, 13(10): 805–813. http://thesai.org/Publications/ViewPaper?Volume=13&Issue=10&Code=IJACSA&SerialNo=96.

Althobaiti, A., Jindal, A., Marnerides, A.K. & Roedig, U. 2021. Energy Theft in Smart Grids: A Survey on Data-Driven Attack Strategies and Detection Methods. *IEEE Access*, 9: 159291–159312. https://ieeexplore.ieee.org/document/9627910/.

Amadala, V. 2021. Kenya Power loses Sh18bn yearly in power theft. *The Star*. https://www.the-star.co.ke/business/kenya/2021-08-26-kenya-power-loses-sh18bn-yearly-in-power-theft/ 20 January 2022.

Amin, S., Schwartz, G.A., Cardenas, A.A. & Shankar Sastry, S. 2015. Game-Theoretic Models of Electricity Theft Detection in Smart Utility Networks: Providing New Capabilities with Advanced Metering Infrastructure. *IEEE Control Systems*, 35(1): 66–81. https://ieeexplore.ieee.org/document/7011178/.

Amisha, Malik, P., Pathania, M. & Rathaur, V. 2019. Overview of artificial intelligence in medicine. *Journal of Family Medicine and Primary Care*, 8(7): 2328–2331. https://journals.lww.com/jfmpc/Fulltext/2019/08070/Overview_of_artificial_intelligence_in_medicine.27.aspx.

Anas, M., Javaid, N., Mahmood, A., Raza, S.M., Qasim, U. & Khan, Z.A. 2012. Minimizing Electricity Theft Using Smart Meters in AMI. In *2012 Seventh International Conference on P2P, Parallel, Grid, Cloud and Internet Computing*. IEEE: 176–182. http://ieeexplore.ieee.org/document/6362966/.

Angelos, E.W.S., Saavedra, O.R., Cortés, O.A.C. & de Souza, A.N. 2011. Detection and Identification of Abnormalities in Customer Consumptions in Power Distribution Systems. *IEEE Transactions on Power Delivery*, 26(4): 2436–2442. https://ieeexplore.ieee.org/document/5989884/.

Antmann, P. 2009. *Reducing Technical and Non-Technical Losses in the Power Sector*. Washington DC. http://hdl.handle.net/10986/20786.

Anwar, M., Javaid, N., Khalid, A., Imran, M. & Shoaib, M. 2020. Electricity Theft Detection using Pipeline in Machine Learning. In *2020 International Wireless Communications and Mobile Computing (IWCMC)*. IEEE: 2138–2142. https://ieeexplore.ieee.org/document/9148453/.

Apogee. 2001. Fundamentals of Electricity. *Apogee Interactive Inc.* https://c03.apogee.net/mvc/home/hes/land/el?utilityname=citizenselectric&spc=foe&id=4593 18 September 2021.

Appiah, S.Y., Akowuah, E.K., Ikpo, V.C. & Dede, A. 2023. Extremely randomised trees machine learning model for electricity theft detection. *Machine Learning with Applications*, 12(March): 1–6. https://doi.org/10.1016/j.mlwa.2023.100458.

Arango, L.G., Deccache, E., Bonatto, B.D., Arango, H. & Pamplona, E.O. 2017. Study of Electricity Theft Impact on the Economy of a Regulated Electricity Company. *Journal of Control, Automation and Electrical Systems*, 28(4): 567–575.

Ardakani, M.H., Hanif, M., Ardakani, M. & Tellambura, C. 2021. Modified REP Pattern for 3×3 Kernel Polar Codes. *IEEE Wireless Communications Letters*, 10(5): 919–923. https://ieeexplore.ieee.org/document/9310295/.

Arief, A., Nappu, M.B. & Sultan, A. 2020. Frequency stability and under frequency load shedding of the Southern Sulawesi power system with integration of wind power plants. *IOP Conference Series: Earth and Environmental Science*, 473(1): 012105. https://iopscience.iop.org/article/10.1088/1755-1315/473/1/012105.

Arif, A., Alghamdi, T.A., Khan, Z.A. & Javaid, N. 2022. Towards Efficient Energy Utilization Using Big Data Analytics in Smart Cities for Electricity Theft Detection. *Big Data Research*, 27: 1–12. https://doi.org/10.1016/j.bdr.2021.100285.

Arif, A., Javaid, N., Aldegheishem, A. & Alrajeh, N. 2021. Big data analytics for identifying electricity theft using machine learning approaches in microgrids for smart communities. *Concurrency and Computation: Practice and Experience*, 33(17): 1–21. https://onlinelibrary.wiley.com/doi/10.1002/cpe.6316.

Asif, M., Nazeer, O., Javaid, N., Alkhammash, E.H. & Hadjouni, M. 2022. Data Augmentation Using BiWGAN, Feature Extraction and Classification by Hybrid 2DCNN and BiLSTM to Detect Non-Technical Losses in Smart Grids. *IEEE Access*, 10: 27467–27483. https://ieeexplore.ieee.org/document/9707774/.

Aslam, Z., Ahmed, F., Almogren, A., Shafiq, M., Zuair, M. & Javaid, N. 2020. An Attention Guided Semi-Supervised Learning Mechanism to Detect Electricity Frauds in the Distribution Systems. *IEEE Access*, 8: 221767–221782. https://ieeexplore.ieee.org/document/9281043/.

Aslam, Z., Javaid, N., Ahmad, A., Ahmed, A. & Gulfam, S.M. 2020. A Combined Deep Learning and Ensemble Learning Methodology to Avoid Electricity Theft in Smart Grids. *Energies*, 13(21): 1–24. https://www.mdpi.com/1996-1073/13/21/5599.

Astronomo, J., Dayrit, M.D., Edjic, C. & Regidor, E.R.T. 2020. Development of Electricity Theft Detector with GSM Module and Alarm System. In *2020 IEEE 12th International Conference on Humanoid, Nanotechnology, Information Technology, Communication and Control, Environment, and Management (HNICEM)*. IEEE: 1–5. https://ieeexplore.ieee.org/document/9400128/.

Aurilio, G., Gallo, D., Landi, C., Luiso, M., Cigolotti, V. & Graditi, G. 2014. Low cost combined voltage and current transducer for Smart Meters. In *2014 IEEE International Instrumentation and Measurement Technology Conference (I2MTC) Proceedings*. IEEE: 1459–1464. https://ieeexplore.ieee.org/document/6860987.

Avancini, D.B., Rodrigues, J.J.P.C., Martins, S.G.B., Rabêlo, R.A.L., Al-Muhtadi, J. & Solic, P. 2019. Energy meters evolution in smart grids: A review. *Journal of Cleaner Production*, 217: 702–715. https://linkinghub.elsevier.com/retrieve/pii/S0959652619302501.

Aziz, S., Hassan Naqvi, S.Z., Khan, M.U. & Aslam, T. 2020. Electricity Theft Detection using Empirical Mode Decomposition and K-Nearest Neighbors. In *2020 International Conference on Emerging Trends in Smart Technologies (ICETST)*. IEEE: 1–5. https://ieeexplore.ieee.org/document/9080727/.

Babu, T.V., Murthy, T.S. & Sivaiah, B. 2013. Detecting unusual customer consumption profiles in power distribution systems - APSPDCL. In *2013 IEEE International Conference on Computational Intelligence and Computing Research*. IEEE: 1–5. http://ieeexplore.ieee.org/document/6724264/.

Babuta, A., Gupta, B., Kumar, A. & Ganguli, S. 2021. Power and energy measurement devices: A review, comparison, discussion, and the future of research. *Measurement*, 172(December 2020): 1–11. https://doi.org/10.1016/j.measurement.2020.108961.

Badawi, S.A., Guessoum, D., Elbadawi, I. & Albadawi, A. 2022. A Novel Time-Series Transformation and Machine-Learning-Based Method for NTL Fraud Detection in Utility Companies. *Mathematics*, 10(11): 1–16. https://www.mdpi.com/2227-7390/10/11/1878.

Bai, Y., Sun, H., Zhang, L. & Wu, H. 2023. Hybrid CNN–Transformer Network for Electricity Theft Detection in Smart Grids. *Sensors*, 23(20): 1–21. https://www.mdpi.com/1424-8220/23/20/8405.

Bajpai, M. & Reddy, A.V.S. eds. 2021. *Emerging Trends in Engineering and Technology (Volume - 1)*. Integrated Publications. https://www.integratedpublications.in/books/1620716658-emerging-trends-in-engineering-and-technology-volume-1.

Bandim, C.J., Alves, J.E.R., Pinto, A.V., Souza, F.C., Loureiro, M.R.B., Magalhaes, C.A. & Galvez-Durand, F. 2003. Identification of energy theft and tampered meters using a central observer meter: a mathematical approach. In *2003 IEEE PES Transmission and Distribution Conference and Exposition (IEEE Cat. No.03CH37495)*. IEEE: 163–168. http://ieeexplore.ieee.org/document/1335175/.

Banga, A., Ahuja, R. & Sharma, S.C. 2022. Accurate Detection of Electricity Theft Using Classification Algorithms and Internet of Things in Smart Grid. *Arabian Journal for Science* *and Engineering*, 47(8): 9583–9599. https://doi.org/10.1007/s13369-021-06313-z.

Bansal, P. & Singh, A. 2016. Smart metering in smart grid framework: A review. In *2016 Fourth International Conference on Parallel, Distributed and Grid Computing (PDGC)*. IEEE: 174–176. http://ieeexplore.ieee.org/document/7913139/.

Barros, R.M.R., da Costa, E.G. & Araujo, J.F. 2021. Evaluation of classifiers for non-technical loss identification in electric power systems. *International Journal of Electrical Power & Energy Systems*, 132(April): 107173. https://doi.org/10.1016/j.ijepes.2021.107173.

El Bassam, N., Maegaard, P. & Schlichting, M.L. 2013. Energy Storage, Smart Grids and Electric Vehicles. In *Distributed Renewable Energies for Off-Grid Communities*. Elsevier: 193–213. https://linkinghub.elsevier.com/retrieve/pii/B9780123971784000050.

Bevrani, H., Golpîra, H., Messina, A.R., Hatziargyriou, N., Milano, F. & Ise, T. 2021. Power system frequency control: An updated review of current solutions and new challenges. *Electric Power Systems Research*, 194: 107114. https://linkinghub.elsevier.com/retrieve/pii/S037877962100095X.

Bian, J., Wang, L., Scherer, R., Wozniak, M., Zhang, P. & Wei, W. 2021. Abnormal Detection of Electricity Consumption of User Based on Particle Swarm Optimization and Long Short Term Memory With the Attention Mechanism. *IEEE Access*, 9: 47252–47265. https://ieeexplore.ieee.org/document/9366425/.

Bihl, T.J. & Hajjar, S. 2017. Electricity theft concerns within advanced energy technologies. In *2017 IEEE National Aerospace and Electronics Conference (NAECON)*. IEEE: 271–278. http://ieeexplore.ieee.org/document/8268784/.

Bîrleanu, F.G., Anghelescu, P., Bizon, N. & Pricop, E. 2019. Cyber Security Objectives and Requirements for Smart Grid. In *Smart Grids and Their Communication Systems*. Springer Singapore: 607–634. http://dx.doi.org/10.1007/978-981-13-1768-2_17.

Boayue, F.G. 2022. Liberia Electricity Corporation Launches National Campaign to Eradicate Power Theft; Assures Stable Electricity Beginning December 1st. *Front Page Africa (FPA)*. https://frontpageafricaonline.com/front-slider/liberia-electricity-corporation-launches-national-campaign-to-eradicate-power-theft-assures-stable-electricity-beginning-december-1st/ 12 April 2023.

Bohani, F.A., Suliman, A., Saripuddin, M., Sameon, S.S., Md Salleh, N.S. & Nazeri, S. 2021. A Comprehensive Analysis of Supervised Learning Techniques for Electricity Theft Detection J. S. Mandeep, ed. *Journal of Electrical and Computer Engineering*, 2021: 1–10. https://www.hindawi.com/journals/jece/2021/9136206/.

Bolaji, E. 2020. Energy Theft: PHED Sets to Name and Shame Offenders. *Brand Spur*. https://brandspurng.com/2020/10/12/energy-theft-phed-sets-to-name-and-shame-offenders/ 25 December 2021.

El Bouchefry, K. & de Souza, R.S. 2020. Learning in Big Data: Introduction to Machine Learning. In *Knowledge Discovery in Big Data from Astronomy and Earth Observation*. Elsevier: 225–249. https://doi.org/10.1016/B978-0-12-819154-5.00023-0.

Bramer, M. 2020. Measuring the Performance of a Classifier. In *Principles of Data Mining*. Springer, London: 175–187. http://link.springer.com/10.1007/978-1-4471-7493-6_12.

Breeze, P. 2014. An Introduction to Electricity Generation. In *Power Generation Technologies*. Elsevier: 1–13. http://dx.doi.org/10.1016/B978-0-08-098330-1.00001-6.

Breiman, L. 2001. Random Forests. *Machine Learning*, 45: 5–32. https://doi.org/10.1023/A:1010933404324.

Brown, J. 2013. Power and Grounding for Audio and Video Systems: A White Paper for the Real World - International Edition. *White Paper*: 1–43. https://www.fast-and-wide.com/more/white-papers/4380-power-and-grounding-for-audio-and-video-systems-a-white-paper-for-the-real-world.

Brown, S. 2021. Machine learning, explained. *MIT Sloan*. https://mitsloan.mit.edu/ideas-made-to-matter/machine-learning-explained 24 October 2021.

Brownlee, J. 2020. How Do Convolutional Layers Work in Deep Learning Neural Networks? *Machine Learning Mastery*. https://machinelearningmastery.com/convolutional-layers-for-deep-learning-neural-networks/ 29 July 2024.

Brownlee, J. 2023. How to Use ROC Curves and Precision-Recall Curves for Classification in Python. *Machine Learning Mastery*. https://machinelearningmastery.com/roc-curves-and-precision-recall-curves-for-classification-in-python/ 27 October 2024.

BSE. 2021. Four Key Benefits of Smart Meters to Electric Utilities. *Border States Electric*. https://solutions.borderstates.com/benefits-of-smart-meters/ 25 September 2021.

Buzau, M., Tejedor-Aguilera, J., Cruz-Romero, P. & Gomez-Exposito, A. 2020. Hybrid Deep Neural Networks for Detection of Non-Technical Losses in Electricity Smart Meters. *IEEE Transactions on Power Systems*, 35(2): 1254–1263. https://ieeexplore.ieee.org/document/8846082/.

Cabral, J.E., Pinto, J.O.P., Martins, E.M. & Pinto, A.M.A.C. 2008. Fraud detection in high voltage electricity consumers using data mining. In *2008 IEEE/PES Transmission and Distribution Conference and Exposition*. IEEE: 1–5. http://ieeexplore.ieee.org/document/4517232/.

Calvo, A., Coma-Puig, B., Carmona, J. & Arias, M. 2020. Knowledge-Based Segmentation to Improve Accuracy and Explainability in Non-Technical Losses Detection. *Energies*, 13(21): 1–15. https://www.mdpi.com/1996-1073/13/21/5674.

Campbell, E. 2021. JPS wants special court for electricity thieves. *The Gleaner*. https://jamaica-gleaner.com/article/lead-stories/20210702/jps-wants-special-court-electricity-thieves 30 June 2024.

Cao, L. 2022. AI Science and Engineering: A New Field. *IEEE Intelligent Systems*, 37(1): 3–13. https://ieeexplore.ieee.org/document/9756274/.

Cardenas, A.A., Amin, S., Schwartz, G., Dong, R. & Sastry, S. 2012. A game theory model for electricity theft detection and privacy-aware control in AMI systems. In *2012 50th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*. IEEE: 1830–1837. http://ieeexplore.ieee.org/document/6483444/.

Casey, J.A., Fukurai, M., Hernández, D., Balsari, S. & Kiang, M. V. 2020. Power Outages and

Community Health: a Narrative Review. *Current Environmental Health Reports*, 7(4): 371–383.

Chandrashekar, G. & Sahin, F. 2014. A survey on feature selection methods. *Computers and Electrical Engineering*, 40(1): 16–28. http://dx.doi.org/10.1016/j.compeleceng.2013.11.024.

Chen, L., Xu, X. & Wang, C. 2011. Research on anti-electricity stealing method base on state estimation. In *2011 IEEE Power Engineering and Automation Conference*. IEEE: 413–416. http://ieeexplore.ieee.org/document/6134972/.

Chen, X., Qiu, X., Ma, Y., Wang, L. & Fang, L. 2022. Boruta-XGBoost Electricity Theft Detection Based on Features of Electric Energy Parameters. *Journal of Physics: Conference Series*, 2290(1): 1–9. https://iopscience.iop.org/article/10.1088/1742-6596/2290/1/012121.

Cheng, G., Zhang, Z., Li, Q., Li, Y. & Jin, W. 2021. Energy Theft Detection in an Edge Data Center Using Deep Learning J. Huang, ed. *Mathematical Problems in Engineering*, 2021(1): 1–12. https://www.hindawi.com/journals/mpe/2021/9938475/.

Chicco, D., Warrens, M.J. & Jurman, G. 2021. The Matthews Correlation Coefficient (MCC) is More Informative Than Cohen’s Kappa and Brier Score in Binary Classification Assessment. *IEEE Access*, 9: 78368–78381. https://ieeexplore.ieee.org/document/9440903/.

Choi, R.Y., Coyner, A.S., Kalpathy-Cramer, J., Chiang, M.F. & Peter Campbell, J. 2020. Introduction to machine learning, neural networks, and deep learning. *Translational Vision Science and Technology*, 9(2): 1–12. https://tvst.arvojournals.org/article.aspx?articleid=2762344.

Christopher, A.V., Swaminathan, G., Subramanian, M. & Thangaraj, P. 2014. Distribution line monitoring system for the detection of power theft using power line communication. In *2014 IEEE Conference on Energy Conversion (CENCON)*. IEEE: 55–60. http://ieeexplore.ieee.org/document/6967476/.

Chung, J. & Jang, B. 2022. Accurate prediction of electricity consumption using a hybrid CNN-LSTM model based on multivariable data Y. Arya, ed. *PLOS ONE*, 17(11): 1–16. http://dx.doi.org/10.1371/journal.pone.0278071.

Cody, C., Ford, V. & Siraj, A. 2015. Decision Tree Learning for Fraud Detection in Consumer Energy Consumption. In *2015 IEEE 14th International Conference on Machine Learning and Applications (ICMLA)*. IEEE: 1175–1179. http://ieeexplore.ieee.org/document/7424479/.

Coelho, P., Gomes, M. & Moreira, C. 2019. Smart Metering Technology. In A. C. Zambroni de Souza & M. Castilla, eds. *Microgrids Design and Implementation*. Cham: Springer International Publishing: 97–137. http://link.springer.com/10.1007/978-3-319-98687-6_4.

Cole, B.M. & Chandler, D. 2019. A Model of Competitive Impression Management: Edison versus Westinghouse in the War of the Currents. *Administrative Science Quarterly*, 64(4): 1020–1063. http://journals.sagepub.com/doi/10.1177/0001839218821439.

Coltman, J.W. 1988. The Transformer. *Scientific American*, 258(1): 86–95. https://www.scientificamerican.com/article/the-transformer.

Coma-Puig, B. 2022. *Human-aware application of data science techniques*. Universitat Politècnica de Catalunya. http://hdl.handle.net/2117/365522.

Coma-Puig, B., Calvo, A., Carmona, J. & Gavaldà, R. 2024. A case study of improving a non-technical losses detection system through explainability. *Data Mining and Knowledge Discovery*, 38(5): 2704–2732. https://doi.org/10.1007/s10618-023-00927-7.

Coma-Puig, B. & Carmona, J. 2022. Non-technical losses detection in energy consumption focusing on energy recovery and explainability. *Machine Learning*, 111(2): 487–517. https://doi.org/10.1007/s10994-021-06051-1.

Conceição, P. & UNDP. 2019. *Human development report 2019 : beyond income, beyond averages, beyond today: inequalities in human development in the 21st century*. https://digitallibrary.un.org/record/3846848#record-files-collapse-header.

Cowdrey, J. 2006. The War of the Currents. *Home Power*, (111): 88–92. https://h2oradio.org/PDF/WaroftheCurrents_Cowdrey.pdf.

Crawford, J. 2019. Why AC won the Electricity Wars. *The Roots of Progress*. https://rootsofprogress.org/why-ac-won 25 July 2023.

Crypto. 2024. Gradient Descent Algorithm: How Does it Work in Machine Learning? *Analytics Vidhya*. https://www.analyticsvidhya.com/blog/2020/10/how-does-the-gradient-descent-algorithm-work-in-machine-learning/ 30 October 2024.

Dai, H.-N. 2018. Electricity Theft Detection. *Github (henryRDlab)*. https://github.com/henryRDlab/ElectricityTheftDetection 7 June 2021.

Daily Yellowstone Journal. 1886. People who steal Edison's electricity. *The Daily Yellowstone Journal*, 4(167): 1–4. https://chroniclingamerica.loc.gov/lccn/sn86075021/1886-03-27/ed-1/seq-2/ 21 July 2021.

David, A.P. 2017. Electro-Magnetic Induction: Free Electricity Generator. *SSRN Electronic Journal*: 1–15. https://www.ssrn.com/abstract=3486740.

Dawn. 2009. KARACHI: KESC to launch `name and shame` drive against power thieves. *Dawn Group of Newspapers*. https://www.dawn.com/news/975415/karachi-kesc-to- launch-name-and-shame-drive-against-power-thieves 13 April 2023.

Dawn. 2023. Special courts demanded for power thieves. *Dawn Group of Newspapers*. https://www.dawn.com/news/1776946 29 June 2024.

DeBoer, C. 2021. Smart Electricity Power Meters - Everything You Need to Know. *Protool Reviews*. https://www.protoolreviews.com/smart-electricity-power-meters/ 15 December 2021.

Depuru, S.S.S.R., Wang, L. & Devabhaktuni, V. 2011a. Electricity theft: Overview, issues, prevention and a smart meter based approach to control theft. *Energy Policy*, 39(2): 1007–1015. http://dx.doi.org/10.1016/j.enpol.2010.11.037.

Depuru, S.S.S.R., Wang, L. & Devabhaktuni, V. 2011b. Smart meters for power grid: Challenges, issues, advantages and status. *Renewable and Sustainable Energy Reviews*, 15(6): 2736–2742. https://linkinghub.elsevier.com/retrieve/pii/S1364032111000876.

Depuru, S.S.S.R., Wang, L. & Devabhaktuni, V. 2011c. Support vector machine based data classification for detection of electricity theft. In *2011 IEEE/PES Power Systems Conference and Exposition*. IEEE: 1–8. http://ieeexplore.ieee.org/document/5772466/.

Dertat, A. 2017. Applied Deep Learning - Part 4: Convolutional Neural Networks. *Towards Data Science*. https://towardsdatascience.com/applied-deep-learning-part-4-convolutional-neural-networks-584bc134c1e2 27 September 2024.

Dick, A.J. 1995. Theft of electricity - how UK electricity companies detect and deter. In *European Convention on Security and Detection*. IEE: 90–95. https://digital-library.theiet.org/content/conferences/10.1049/cp_19950476.

Dike, D.O., Obiora, U.A., Nwokorie, E.C. & Dike, B.C. 2015. Minimizing Household Electricity Theft in Nigeria Using GSM Based Prepaid Meter. *American Journal of Engineering Research (AJER)*, 4(1): 59–69. https://www.ajer.org/papers/v4(01)/I0401059069.pdf.

Dimf, G.P., Kumar, P. & Manju, V.N. 2023. An Efficient Power Theft Detection Using Modified Deep Artificial Neural Network (MDANN). *International Journal of Intelligent Systems and Applications in Engineering*, 11(1): 1–11. https://www.ijisae.org/index.php/IJISAE/article/view/2437.

Dimkpa, V.C., Agba, J.C. & Ogu, V.U. 2023. Design and Construction of a GSM Based Energy Meter Reader and Load Control System. *International Journal for Research in Applied Science and Engineering Technology (IJRASET)*, 11(6): 2636–2667. https://www.ijraset.com/best-journal/design-and-construction-of-a-gsm-based-energy-meter-reader-and-load-control-system.

Dindar, B. & Gül, Ö. 2021. The detection of illicit cryptocurrency mining farms with innovative approaches for the prevention of electricity theft. *Energy & Environment*: 1–16. http://journals.sagepub.com/doi/10.1177/0958305X211045066.

Dineshkumar, K., Ramanathan, P. & Ramasamy, S. 2015. Development of ARM processor based electricity theft control system using GSM network. In *2015 International Conference on Circuits, Power and Computing Technologies [ICCPCT-2015]*. IEEE: 1–6. http://ieeexplore.ieee.org/document/7159401/.

Dinov, I.D. 2018. Decision Tree Divide and Conquer Classification. In *Data Science and Predictive Analytics*. Cham: Springer International Publishing: 307–343. http://link.springer.com/10.1007/978-3-319-72347-1_9.

Dlodlo, N., Mudumbe, J.M. & Ndwe, T.J. 2014. The internet of things for a smart South African grid architecture. *Proceedings of the 8th International Development Informatics Association Conference*, (2014): 95–107. http://researchspace.csir.co.za/dspace/handle/10204/7914.

Dodoo, L. 2022. Liberia: The Power Theft Act, Has It Helped? *Front Page Africa (FPA)*. https://frontpageafricaonline.com/opinion/liberia-the-power-theft-act-has-it-helped/ 12 April 2023.

Dyer, S.A. 2001. *Wiley Survey of Instrumentation and Measurement*. New York: John Wlley & Sons.

Edris, A.A. & D’Andrade, B.W. 2017. *Transmission Grid Smart Technologies*. Elsevier Ltd. http://dx.doi.org/10.1016/B978-0-12-805321-8.00002-1.

Ekanayake, J., Liyanage, K., Wu, J., Yokoyama, A. & Jenkins, N. 2012. Smart Metering and Demand-Side Integration. In *Smart Grid*. Wiley: 81–112. https://onlinelibrary.wiley.com/doi/10.1002/9781119968696.ch5.

Elreedy, D., Atiya, A.F. & Kamalov, F. 2024. A theoretical distribution analysis of synthetic minority oversampling technique (SMOTE) for imbalanced learning. *Machine Learning*, 113(7): 4903–4923. https://doi.org/10.1007/s10994-022-06296-4.

Energy Central. 2019. A sustainable approach in curbing electricity theft. *Energy Central News*. https://energycentral.com/news/sustainable-approach-curbing-electricity-theft 8 February 2021.

Erenoğlu, A.K., Erdinç, O. & Taşcıkaraoğlu, A. 2019. History of Electricity. In *Pathways to a Smarter Power System*. Elsevier: 1–27. https://linkinghub.elsevier.com/retrieve/pii/B9780081025925000016.

ESI Africa. 2019. The Big Question: Is Nigeria embracing the 4IR? *Electricity Supply International (ESI) Africa*. https://www.esi-africa.com/industry-sectors/future-energy/the-big-question-is-nigeria-embracing-the-4ir/ 4 January 2022.

Eskom. 2013. Eskom load shedding. https://loadshedding.eskom.co.za/loadshedding/description 19 June 2021.

Essig, M. 2009. *Edison and the Electric Chair: A Story of Light and Death*. Bloomsbury Publishing.

Express Tribune. 2016. Amended law: Power thieves to face up to 7-year imprisonment. *The Express Tribune*. https://tribune.com.pk/story/1048302/amended-law-power-thieves-to-face-up-to-7-year-imprisonment 11 January 2021.

Ezediuno, F. 2023. NSCDC parades teacher, five others for metre tampering, energy theft in Osun. *Daily Post Nigeria*. https://dailypost.ng/2023/10/17/nscdc-parades-teacher-five-others-for-metre-tampering-energy-theft-in-osun/ 17 October 2023.

Ezhilarasi, P. & Ramesh, L. 2019. Review on Smart Energy Meter for low cost design. In *2019 5th International Conference On Computing, Communication, Control And Automation (ICCUBEA)*. IEEE: 1–8. https://ieeexplore.ieee.org/document/9128805/.

Fang, X., Misra, S., Xue, G. & Yang, D. 2012. Smart Grid — The New and Improved Power Grid: A Survey. *IEEE Communications Surveys & Tutorials*, 14(4): 944–980. http://ieeexplore.ieee.org/document/6099519/.

Farhan, F. & Nafi, T.I. 2022. ANN based approach to predict criminal trends in Bangladesh. In *2022 2nd International Conference on Artificial Intelligence and Signal Processing (AISP)*. IEEE: 1–7. https://ieeexplore.ieee.org/document/9760684/.

Faria, L.T., Melo, J.D. & Padilha-Feltrin, A. 2016. Spatial-Temporal Estimation for Nontechnical Losses. *IEEE Transactions on Power Delivery*, 31(1): 362–369. http://ieeexplore.ieee.org/document/7279178/.

Farid, S., Iltaf, N. & Afzal, H. 2023. Electricity Theft Detection Via Deep Learning. In *2023 International Conference on Communication Technologies (ComTech)*. IEEE: 79–86. https://ieeexplore.ieee.org/document/10164983/.

Fawagreh, K., Gaber, M.M. & Elyan, E. 2014. Random forests: from early developments to recent advancements. *Systems Science & Control Engineering*, 2(1): 602–609. http://www.tandfonline.com/doi/abs/10.1080/21642583.2014.956265.

Fei, K., Li, Q., Ma, Z., Gryazina, E. & Terzija, V. 2023. Non-technical losses detection employing adversarial domain adaptation. *International Journal of Electrical Power & Energy Systems*, 150(January): 1–8. https://linkinghub.elsevier.com/retrieve/pii/S0142061523001163.

Fei, K., Li, Q., Zhu, C., Dong, M. & Li, Y. 2022. Electricity frauds detection in Low-voltage networks with contrastive predictive coding. *International Journal of Electrical Power & Energy Systems*, 137(November 2021): 1–8. https://linkinghub.elsevier.com/retrieve/pii/S0142061521009418.

Fenza, G., Gallo, M. & Loia, V. 2019. Drift-Aware Methodology for Anomaly Detection in Smart Grid. *IEEE Access*, 7: 9645–9657. https://ieeexplore.ieee.org/document/8604042/.

Ferreira, T.S.D., Trindade, F.C.L. & Vieira, J.C.M. 2020. Load Flow-Based Method for Nontechnical Electrical Loss Detection and Location in Distribution Systems Using Smart Meters. *IEEE Transactions on Power Systems*, 35(5): 3671–3681. https://ieeexplore.ieee.org/document/9040643/.

Ford, V., Siraj, A. & Eberle, W. 2014. Smart grid energy fraud detection using artificial neural networks. In *2014 IEEE Symposium on Computational Intelligence Applications in Smart Grid (CIASG)*. IEEE: 1–6. http://ieeexplore.ieee.org/document/7011557/.

Fragkioudaki, A., Cruz-Romero, P., Gómez-Expósito, A., Biscarri, J., de Tellechea, M.J. & Arcos, Á. 2016. Detection of Non-technical Losses in Smart Distribution Networks: A Review. In *International Conference on Practical Applications of Agents and Multi-Agent Systems*. Springer: 43–54. http://link.springer.com/10.1007/978-3-319-40159-1_4.

French, D. 2017. *When They Hid the Fire: A History of Electricity and Invisible Energy in America*. University of Pittsburgh Press. https://www.jstor.org/stable/10.2307/j.ctt1mtz5d6.

Ganesh, K.S. 2020. What's The Role Of Weights And Bias In a Neural Network? *Towards Data Science*. https://towardsdatascience.com/whats-the-role-of-weights-and-bias-in-a-neural-network-4cf7e9888a0f 17 September 2024.

Ganesh, P. 2019. Types of Convolution Kernels : Simplified. *Towards Data Science*. https://towardsdatascience.com/types-of-convolution-kernels-simplified-f040cb307c37 1 August 2024.

Gao, A., Mei, F., Zheng, J., Sha, H., Guo, M. & Xie, Y. 2023. Electricity Theft Detection Based on Contrastive Learning and Non-Intrusive Load Monitoring. *IEEE Transactions on Smart Grid*, 14(6): 4565–4580. https://ieeexplore.ieee.org/document/10089187/.

Gao, B., Kong, X., Li, S., Chen, Y., Zhang, X., Liu, Z. & Lv, W. 2024. Enhancing anomaly detection accuracy and interpretability in low-quality and class imbalanced data: A comprehensive approach. *Applied Energy*, 353(PB): 1–23.

https://doi.org/10.1016/j.apenergy.2023.122157.

Gao, H.-X., Kuenzel, S. & Zhang, X.-Y. 2022. A Hybrid ConvLSTM-Based Anomaly Detection Approach for Combating Energy Theft. *IEEE Transactions on Instrumentation and Measurement*, 71: 1–10. https://ieeexplore.ieee.org/document/9866709/.

García, V., Mollineda, R.A. & Sánchez, J.S. 2008. A New Performance Evaluation Method for Two-Class Imbalanced Problems. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. 917–925. http://link.springer.com/10.1007/978-3-540-89689-0_95.

Gaur, V. & Gupta, E. 2016. The determinants of electricity theft: An empirical analysis of Indian states. *Energy Policy*, 93: 127–136. http://www.sciencedirect.com/science/article/pii/S0301421516300878.

Ghaedi, H., Kamel Tabbakh, S.R. & Ghaemi, R. 2022. A Novel Meta-heuristic Framework for Solving Power Theft Detection Problem: Cheetah Optimization Algorithm. *International Journal of Industrial Electronics, Control and Optimization*, 5(1): 63–76. https://ieco.usb.ac.ir/article_6688.html.

GhanaWeb. 2018. ECG to name and shame ‘power thieves’. *General News*. https://www.ghanaweb.com/GhanaHomePage/NewsArchive/ECG-to-name-and-shame-power-thieves-632491 11 April 2023.

Ghori, K.M., Abbasi, R.A., Awais, M., Imran, M., Ullah, A. & Szathmary, L. 2020. Performance Analysis of Different Types of Machine Learning Classifiers for Non-Technical Loss Detection. *IEEE Access*, 8: 16033–16048. https://ieeexplore.ieee.org/document/8943419/.

Ghori, K.M., Awais, M., Khattak, A.S., Imran, M., Fazal-E-Amin & Szathmary, L. 2021. Treating Class Imbalance in Non-Technical Loss Detection: An Exploratory Analysis of a Real Dataset. *IEEE Access*, 9: 98928–98938. https://ieeexplore.ieee.org/document/9475464/.

Ghori, K.M., Imran, M., Nawaz, A., Abbasi, R.A., Ullah, A. & Szathmary, L. 2023. Performance analysis of machine learning classifiers for non-technical loss detection. *Journal of Ambient Intelligence and Humanized Computing*, 14(11): 15327–15342. https://doi.org/10.1007/s12652-019-01649-9.

Ghosal, S., Banerjee, S., Kundu, S. & Yadav, S. 2022. IOT-BASED ENERGY METER FOR DISPLAYING CONSUMPTION STATISTIC. *International Journal of Engineering Applied Sciences and Technology*, 6(11): 160–164. https://www.ijeast.com/papers/160-164, Tesma611,IJEAST.pdf.

Ghosh, B. 2023. What Matters More — Data Size or Model Size. *Medium*. https://medium.com/@bijit211987/what-matters-more-data-size-or-model-size-31cb004d7209#:~:text=Generalization%3A Larger datasets often lead,perform well on unseen examples. 25 July 2024.

Glauner, P. 2019. *Artificial Intelligence for the Detection of Electricity Theft and Irregular Power Usage in Emerging Markets*. University of Luxembourg. http://hdl.handle.net/10993/38544.

Glauner, P., Meira, J.A., Dolberg, L., State, R., Bettinger, F. & Rangoni, Y. 2016. Neighborhood features help detecting non-technical losses in big data sets. In *Proceedings of the 3rd IEEE/ACM International Conference on Big Data Computing, Applications and*

Technologies. New York, NY, USA: ACM: 253–261. https://dl.acm.org/doi/10.1145/3006299.3006310.

Glauner, P., Meira, J.A., Valtchev, P., State, R. & Bettinger, F. 2017. The Challenge of Non-Technical Loss Detection Using Artificial Intelligence: A Survey. *International Journal of Computational Intelligence Systems*, 10(1): 760–775. http://dx.doi.org/10.2991/ijcis.2017.10.1.51.

Goodfellow, I., Bengio, Y. & Courville, A. 2016. *Deep Learning*. The MIT Press.

Gopinath, S., Suresh, R., Devika, T., Divya, N. & Vanitha, N.S. 2013. Embedded Based Digital Energy Measurement for Improved Metering and Billing System. *International Journal of Innovative Research in Science, Engineering and Technology*, 1(9): 428–432. www.ijireeice.com.

Grochocki, D., Huh, J.H., Berthier, R., Bobba, R., Sanders, W.H., Cardenas, A.A. & Jetcheva, J.G. 2012. AMI threats, intrusion detection requirements and deployment recommendations. In *2012 IEEE Third International Conference on Smart Grid Communications (SmartGridComm)*. IEEE: 395–400. http://ieeexplore.ieee.org/document/6486016/.

Grootes, S. 2019. Twelve years of load shedding – written, starring & directed by the ANC. *Daily Maverick*. https://www.dailymaverick.co.za/article/2019-12-09-twelve-years-of-load-shedding-written-starring-directed-by-the-anc/?__cf_chl_captcha_tk__=f30d8132f78d8c753debb5dd5d45aca09f47bea4-1624105459-0-ARlMTeioDG9Xs1YjNV1XLSA6Y1FAUnYcY16NqSQrPUpOm-lOVc3tjqwx8au5 19 June 2021.

Gu, D., Gao, Y., Chen, K., Shi, J., Li, Y. & Cao, Y. 2022. Electricity Theft Detection in AMI With Low False Positive Rate Based on Deep Learning and Evolutionary Algorithm. *IEEE Transactions on Power Systems*, 37(6): 4568–4578. https://ieeexplore.ieee.org/document/9709670/.

Guarda, F.G.K., Hammerschmitt, B.K., Capeletti, M.B., Neto, N.K., dos Santos, L.L.C., Prade, L.R. & Abaide, A. 2023. Non-Hardware-Based Non-Technical Losses Detection Methods: A Review. *Energies*, 16(4): 1–27. https://www.mdpi.com/1996-1073/16/4/2054.

Guarnieri, M. 2013. The Beginning of Electric Energy Transmission: Part Two. *IEEE Industrial Electronics Magazine*, 7(2): 52–59. http://ieeexplore.ieee.org/document/6532479/.

Guerrero, J.I., León, C., Monedero, I., Biscarri, F. & Biscarri, J. 2014. Improving Knowledge-Based Systems with statistical techniques, text mining, and neural networks for non-technical loss detection. *Knowledge-Based Systems*, 71: 376–388. https://linkinghub.elsevier.com/retrieve/pii/S0950705114003025.

Guerrero, J.I., Monedero, I., Biscarri, F., Biscarri, J., Millan, R. & Leon, C. 2018. Non-Technical Losses Reduction by Improving the Inspections Accuracy in a Power Utility. *IEEE Transactions on Power Systems*, 33(2): 1209–1218. http://ieeexplore.ieee.org/document/7962285/.

Guizeni, S. 2024. Is Min-Max Scaler the Key to Optimal Data Normalization? Unveiling the Pros, Cons, and Best Practices. *Seifeur*. https://seifeur.com/min-max-scaler/ 22 July 2024.

Gul, H., Javaid, N., Ullah, I., Qamar, A.M., Afzal, M.K. & Joshi, G.P. 2020. Detection of Non-Technical Losses Using SOSTLink and Bidirectional Gated Recurrent Unit to Secure Smart Meters. *Applied Sciences*, 10(9): 1–21. https://www.mdpi.com/2076-3417/10/9/3151.

Gunduz, M.Z. & Das, R. 2024. Smart Grid Security: An Effective Hybrid CNN-Based Approach for Detecting Energy Theft Using Consumption Patterns. *Sensors*, 24(4): 1–21. https://www.mdpi.com/1424-8220/24/4/1148.

Guo, Y., Ten, C.W. & Jirutitijaroen, P. 2014. Online data validation for distribution operations against cybertampering. *IEEE Transactions on Power Systems*, 29(2): 550–560.

Gupta, A.K., Routray, A. & Naikan, V.A. 2022. Detection of Power Theft in Low Voltage Distribution Systems: A Review from the Indian Perspective. *IETE Journal of Research*, 68(6): 4180–4197. https://doi.org/03772063.2020.1787881.

Gupta, B., Rawat, A., Jain, A., Arora, A. & Dhami, N. 2017. Analysis of Various Decision Tree Algorithms for Classification in Data Mining. *International Journal of Computer Applications*, 163(8): 15–19. http://www.ijcaonline.org/archives/volume163/number8/gupta-2017-ijca-913660.pdf.

Hall, J. 2015. Shocking moment passers-by refused to help fatally injured South African man who burst into flames while stealing copper wires from an electricity substation. *Daily Mail Online*. https://www.dailymail.co.uk/news/article-3004108/Shocking-moment-passers-refused-help-fatally-injured-South-African-man-burst-flames-stealing-copper-wires-electricity-substation.html 4 March 2021.

Hamet, P. & Tremblay, J. 2017. Artificial intelligence in medicine. *Metabolism*, 69: S36–S40. http://dx.doi.org/10.1016/j.metabol.2017.01.011.

Hammerstrom, D.J. 2007. AC Versus DC Distribution SystemsDid We Get it Right? In *2007 IEEE Power Engineering Society General Meeting*. IEEE: 1–5. http://ieeexplore.ieee.org/document/4275896/.

Hanif, H., Md Nasir, M.H.N., Ab Razak, M.F., Firdaus, A. & Anuar, N.B. 2021. The rise of software vulnerability: Taxonomy of software vulnerabilities detection and machine learning approaches. *Journal of Network and Computer Applications*, 179(February): 1–24. https://doi.org/10.1016/j.jnca.2021.103009.

Hashmi, M.U. & Priolkar, J.G. 2015. Anti-theft energy metering for smart electrical distribution system. In *2015 International Conference on Industrial Instrumentation and Control (ICIC)*. IEEE: 1424–1428. http://ieeexplore.ieee.org/document/7150972/.

Hassan, A., Afrouzi, H.N., Siang, C.H., Ahmed, J., Mehranzamir, K. & Wooi, C.-L. 2022. Simulation of GSM Based Smart Energy Meter Presenting Electric Theft Detection and Prevention Mechanism by Using Arduino. In Z. Zakaria & S. S. Emamian, eds. *Recent Advances in Electrical and Electronic Engineering and Computer Science*. Springer, Singapore: 1–9. https://link.springer.com/10.1007/978-981-16-9781-4_1.

Henriques, H.O., Barbero, A.P.L., Ribeiro, R.M., Fortes, M.Z., Zanco, W., Xavier, O.S. & Amorim, R.M. 2014. Development of adapted ammeter for fraud detection in low-voltage installations. *Measurement*, 56: 1–7. https://linkinghub.elsevier.com/retrieve/pii/S0263224114002760.

Van Hertem, D. & Delimar, M. 2013. High Voltage Direct Current (HVDC) electric power transmission systems. In *Electricity Transmission, Distribution and Storage Systems*. Elsevier: 143–173. http://dx.doi.org/10.1533/9780857097378.2.143.

Huang, G. 2021. Missing data filling method based on linear interpolation and lightgbm. *Journal of Physics: Conference Series*, 1754(1): 012187. https://iopscience.iop.org/article/10.1088/1742-6596/1754/1/012187.

Huang, Q., Tang, Z., Weng, X., He, M., Liu, F., Yang, M. & Jin, T. 2024. A Novel Electricity Theft Detection Strategy Based on Dual-Time Feature Fusion and Deep Learning Methods. *Energies*, 17(2): 1–18. https://www.mdpi.com/1996-1073/17/2/275.

Huang, S.-C., Lo, Y.-L. & Lu, C.-N. 2013. Non-Technical Loss Detection Using State Estimation and Analysis of Variance. *IEEE Transactions on Power Systems*, 28(3): 2959–2966. https://ieeexplore.ieee.org/document/6490071/.

Hughes, T.P. 1958. Harold P. Brown and the Executioner's Current: an Incident in the AC-DC Controversy. *Business History Review*, 32(2): 143–165. https://www.cambridge.org/core/product/identifier/S0007680500011028/type/journal_article.

Hussain, S., Mustafa, M.W., Ateyeh Al-Shqeerat, K.H., Saleh Al-rimy, B.A. & Saeed, F. 2022. Electric theft detection in advanced metering infrastructure using Jaya optimized combined Kernel-Tree boosting classifier—A novel sequentially executed supervised machine learning approach. *IET Generation, Transmission & Distribution*, 16(6): 1257–1275. https://onlinelibrary.wiley.com/doi/10.1049/gtd2.12386.

Hussain, S., Mustafa, M.W., Jumani, T.A., Baloch, S.K., Alotaibi, H., Khan, I. & Khan, A. 2021. A novel feature engineered-CatBoost-based supervised machine learning framework for electricity theft detection. *Energy Reports*, 7: 4425–4436. https://doi.org/10.1016/j.egyr.2021.07.008.

Iftikhar, H., Khan, N., Raza, M.A., Abbas, G., Khan, M., Aoudia, M., Touti, E. & Emara, A. 2024. Electricity theft detection in smart grid using machine learning. *Frontiers in Energy Research*, 12(March): 01–18. https://doi.org/10.3389/fenrg.2024.1383090.

Irfan, M., Ayub, N., Althobiani, F., Ali, Z., Idrees, M., Ullah, S., Rahman, S., Saeed Alwadie, A., Mohammed Ghonaim, S., Abdushkour, H., Salem Alkahtani, F., Alqhtani, S. & Gas, P. 2022. Energy Theft Identification Using Adaboost Ensembler in the Smart Grids. *Computers, Materials & Continua*, 72(1): 2141–2158. https://www.techscience.com/cmc/v72n1/46936.

Iribagiza, G. 2020. REG to install smart metres after Rwf19bn electricity theft. *The New Times*. https://www.newtimes.co.rw/news/reg-install-smart-metres-curb-electricity-theft 8 January 2022.

Islam, M., Chen, G. & Jin, S. 2019. An Overview of Neural Network. *American Journal of Neural Networks and Applications*, 5(1): 7–11. http://www.sciencepublishinggroup.com/journal/paperinfo?journalid=339&doi=10.11648/j.ajnna.20190501.12.

Jamil, F. & Ahmad, E. 2019. Policy considerations for limiting electricity theft in the developing countries. *Energy Policy*, 129(July 2018): 452–458.

https://doi.org/10.1016/j.enpol.2019.02.035.

Janiesch, C., Zschech, P. & Heinrich, K. 2021. Machine learning and deep learning. *Electronic Markets*, 31(3): 685–695. https://link.springer.com/10.1007/s12525-021-00475-2.

Jaokar, A. 2019. The Mathematics of Forward and Back Propagation. *Data Science Central*. https://www.datasciencecentral.com/the-mathematics-of-forward-and-back-propagation/ 25 August 2024.

Javaid, N. 2021. A PLSTM, AlexNet and ESNN Based Ensemble Learning Model for Detecting Electricity Theft in Smart Grids. *IEEE Access*, 9: 162935–162950. https://ieeexplore.ieee.org/document/9646878/.

Javaid, N., Gul, H., Baig, S., Shehzad, F., Xia, C., Guan, L. & Sultana, T. 2021. Using GANCNN and ERNET for Detection of Non Technical Losses to Secure Smart Grids. *IEEE Access*, 9: 98679–98700. https://ieeexplore.ieee.org/document/9465107/.

Javaid, N., Jan, N. & Javed, M.U. 2021. An adaptive synthesis to handle imbalanced big data with deep siamese network for electricity theft detection in smart grids. *Journal of Parallel and Distributed Computing*, 153: 44–52. https://doi.org/10.1016/j.jpdc.2021.03.002.

Jiang, R., Lu, R., Wang, Y., Luo, J., Shen, C. & Shen, X. 2014. Energy-theft detection issues for advanced metering infrastructure in smart grid. *Tsinghua Science and Technology*, 19(2): 105–120. https://ieeexplore.ieee.org/document/6787363/.

Jindal, A., Member, S., Dua, A., Member, S., Kaur, K., Member, S. & Singh, M. 2016. Decision Tree and SVM-Based Data Analytics for Theft Detection in Smart Grid. *IEEE Transactions on Industrial Informatics*, 12(3): 1005–1016.

Jokar, P., Arianpoo, N. & Leung, V.C.M. 2016. Electricity Theft Detection in AMI Using Customers' Consumption Patterns. *IEEE Transactions on Smart Grid*, 7(1): 216–226. http://ieeexplore.ieee.org/document/7108042/.

Jones, J.S. 2021. Hydro-Québec uses smart meters to shut down electricity theft network. *Smart Energy International (SEI)*. https://www.smart-energy.com/industry-sectors/smart-meters/hydro-quebec-uses-smart-meters-to-shut-down-electricity-theft-network/ 30 December 2021.

Jones, M.P. 1982. Looking back. *IEEE Potentials*, 1(Spring): 30–30. http://ieeexplore.ieee.org/document/6499513/.

Jordan, M.I. & Mitchell, T.M. 2015. Machine learning: Trends, perspectives, and prospects. *Science*, 349(6245): 255–260. https://www.science.org/doi/10.1126/science.aaa8415.

Júnior, L.A.P., Ramos, C.C.O., Rodrigues, D., Pereira, D.R., de Souza, A.N., Pontara da Costa, K.A. & Papa, J.P. 2016. Unsupervised non-technical losses identification through optimum-path forest. *Electric Power Systems Research*, 140: 413–423. https://linkinghub.elsevier.com/retrieve/pii/S0378779616302085.

Kabalci, E. & Kabalci, Y. 2019. Introduction to smart grid and internet of energy systems. In *From Smart Grid to Internet of Energy*. Elsevier: 1–62. https://linkinghub.elsevier.com/retrieve/pii/B9780128197103000016.

Kabalci, Y. 2016. A survey on smart metering and smart grid communication. *Renewable and Sustainable Energy Reviews*, 57: 302–318. http://www.sciencedirect.com/science/article/pii/S1364032115014975.

Kadurek, P., Blom, J., Cobben, J.F.G. & Kling, W.L. 2010. Theft detection and smart metering practices and expectations in the Netherlands. In *2010 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT Europe)*. IEEE: 1–6. http://ieeexplore.ieee.org/document/5638852/.

Kambule, N. & Nwulu, N. 2021. Rationale Part II: A Misdiagnosis of Non-payment and Electricity Theft. In *The Deployment of Prepaid Electricity Meters in Sub-Saharan Africa. Lecture Notes in Electrical Engineering*. Springer, Cham: 33–53. https://link.springer.com/10.1007/978-3-030-71217-4_3.

Karimi, M., Atashbar, M. & Najafi Ravadanegh, S. 2020. Risk-based modelling of simultaneous reconfiguration of power distribution networks and allocation of distributed generations. *International Journal of Ambient Energy*, 41(2): 169–178. https://doi.org/10.1080/01430750.2018.1451372.

Kathiresh, M. & Subahani, A.M. 2020. Smart Meter: A Key Component for Industry 4.0 in Power Sector. In *Internet of Things for Industry 4.0 Design, Challenges and Solutions*. 177–196. http://link.springer.com/10.1007/978-3-030-32530-5_12.

Kawoosa, A.I., Prashar, D., Faheem, M., Jha, N. & Khan, A.A. 2023. Using machine learning ensemble method for detection of energy theft in smart meters. *IET Generation, Transmission & Distribution*, 17(21): 4794–4809. https://ietresearch.onlinelibrary.wiley.com/doi/10.1049/gtd2.12997.

Kelly-Detwiler, P. 2013. Electricity Theft: A Bigger Issue Than You Think. *Forbes*. https://www.forbes.com/sites/peterdetwiler/2013/04/23/electricity-theft-a-bigger-issue-than-you-think/?sh=30b947f45ed7 11 February 2021.

Kgaphola, P.M., Marebane, S.M. & Hans, R.T. 2024. Electricity Theft Detection and Prevention Using Technology-Based Models: A Systematic Literature Review. *Electricity*, 5(2): 334–350. https://www.mdpi.com/2673-4826/5/2/17.

Khalid, A., Mustafa, G., Rana, M.R.R., Alshahrani, S.M. & Alymani, M. 2024. RNN-BiLSTM-CRF based amalgamated deep learning model for electricity theft detection to secure smart grids. *PeerJ Computer Science*, 10: 1–18. https://peerj.com/articles/cs-1872.

Khalid, S., Khalil, T. & Nasreen, S. 2014. A survey of feature selection and feature extraction techniques in machine learning. In *2014 Science and Information Conference*. IEEE: 372–378. https://ieeexplore.ieee.org/document/6918213.

Khan, I.U., Javaid, N., Taylor, C.J. & Ma, X. 2023. Robust Data Driven Analysis for Electricity Theft Attack-Resilient Power Grid. *IEEE Transactions on Power Systems*, 38(1): 537–548. https://ieeexplore.ieee.org/document/9743316/.

Khan, I.U., Javeid, N., Taylor, C.J., Gamage, K.A.A. & Ma, X. 2022. A Stacked Machine and Deep Learning-Based Approach for Analysing Electricity Theft in Smart Grids. *IEEE Transactions on Smart Grid*, 13(2): 1633–1644. https://ieeexplore.ieee.org/document/9644473/.

Khan, N., Shahid, Z., Alam, M.M., Sajak, A.A.B., Nazar, M. & Mazliham, M.S. 2024. A novel deep learning technique to detect electricity theft in smart grids using AlexNet. *IET Renewable Power Generation*, 11(August 2023): 1–18. https://ietresearch.onlinelibrary.wiley.com/doi/10.1049/rpg2.12846.

Khan, Z.A., Adil, M., Javaid, N., Saqib, M.N., Shafiq, M. & Choi, J. 2020. Electricity Theft Detection Using Supervised Learning Techniques on Smart Meter Data. *Sustainability*, 12(19): 1–25. https://www.mdpi.com/2071-1050/12/19/8023.

Khattak, A., Bukhsh, R., Aslam, S., Yafoz, A., Alghushairy, O. & Alsini, R. 2022. A Hybrid Deep Learning-Based Model for Detection of Electricity Losses Using Big Data in Power Systems. *Sustainability*, 14(20): 1–20. https://www.mdpi.com/2071-1050/14/20/13627.

Khoo, B. & Cheng, Y. 2011. Using RFID for anti-theft in a Chinese electrical supply company: A cost-benefit analysis. In *2011 Wireless Telecommunications Symposium (WTS)*. IEEE: 1–6. http://ieeexplore.ieee.org/document/5960892/.

Khoussi, S. & Mattas, A. 2017. A Brief Introduction to Smart Grid Safety and Security. In *Handbook of System Safety and Security*. Elsevier: 225–252. http://dx.doi.org/10.1016/B978-0-12-803773-7.00011-5.

Kiliçarslan, S. & Celik, M. 2021. RSigELU: A nonlinear activation function for deep neural networks. *Expert Systems with Applications*, 174(December 2020): 1–12. https://doi.org/10.1016/j.eswa.2021.114805.

Kim, S., Sun, Y., Lee, S., Seon, J., Hwang, B., Kim, Jeongho, Kim, Jinwook, Kim, K. & Kim, Jinyoung. 2024. Data-Driven Approaches for Energy Theft Detection: A Comprehensive Review. *Energies*, 17(12): 1–22. https://www.mdpi.com/1996-1073/17/12/3057.

King, G. 2011. Edison vs. Westinghouse: A Shocking Rivalry. *Smithsonian Magazine*. https://www.smithsonianmag.com/history/edison-vs-westinghouse-a-shocking-rivalry-102146036/ 8 September 2021.

King, G. 2013. The Rise and Fall of Nikola Tesla and His Tower. *Smithsonian Magazine*. https://www.smithsonianmag.com/history/the-rise-and-fall-of-nikola-tesla-and-his-tower-11074324/ 29 November 2021.

Kingma, D.P. & Ba, J.L. 2015. Adam: A method for stochastic optimization. In *3rd International Conference on Learning Representations (ICLR), San Diego, 2015*. 1–15. https://doi.org/10.48550/arXiv.1412.6980.

Knapp, E.D. & Samani, R. 2013. Smart Grid Network Architecture. In *Applied Cyber Security and the Smart Grid*. Elsevier: 17–56. https://linkinghub.elsevier.com/retrieve/pii/B9781597499989000025.

Kocaman, B. & Tümen, V. 2020. Detection of electricity theft using data processing and LSTM method in distribution systems. *Sādhanā*, 45(1): 286. http://link.springer.com/10.1007/s12046-020-01512-0.

Kommajosyula, K.M. 2017. Light on Electric Light! *Science Reporter*, 54(04): 37–43. http://nopr.niscair.res.in/handle/123456789/40965.

Krishna, V.B., Weaver, G.A. & Sanders, W.H. 2015. PCA-Based Method for Detecting Integrity Attacks on Advanced Metering Infrastructure. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. 70–85. https://link.springer.com/10.1007/978-3-319-22264-6_5.

Kruse, J., Schäfer, B. & Witthaut, D. 2021. Revealing drivers and risks for power grid frequency stability with explainable AI. *Patterns*, 2(11): 100365. https://linkinghub.elsevier.com/retrieve/pii/S2666389921002270.

Kularatna, N. & Gunawardane, K. 2021. Modern electrical power system and the role of distributed generation. In *Energy Storage Devices for Renewable Energy-Based Systems: Rechargeable Batteries and Supercapacitors*. Elsevier: 1–35. https://linkinghub.elsevier.com/retrieve/pii/B9780128207789000024.

Kulkarni, Y., Z, S.H., Ramamritham, K. & Somu, N. 2021. EnsembleNTLDetect: An Intelligent Framework for Electricity Theft Detection in Smart Grid. In *2021 International Conference on Data Mining Workshops (ICDMW)*. IEEE: 527–536. https://ieeexplore.ieee.org/document/9679840/.

Kumar, D. 2023. MAX POOLING. *Medium*. https://medium.com/@danushidk507/max-pooling-ef545993b6e4 21 September 2024.

Kwarteng, M.Y., Effah, F.B., Kwegyir, D. & Frimpong, E.A. 2023. ANN-Based Electricity Theft Classification Technique for Limited Data Distribution Systems. *Jurnal Nasional Teknik Elektro*, 12(1): 7–15. http://jnte.ft.unand.ac.id/index.php/jnte/article/view/1072.

L'Heureux, A., Grolinger, K., Elyamany, H.F. & Capretz, M.A.M. 2017. Machine Learning With Big Data: Challenges and Approaches. *IEEE Access*, 5: 7776–7797. https://ieeexplore.ieee.org/document/7906512/.

Lantero, A. 2014. The War of the Currents: AC vs. DC Power. https://www.energy.gov/articles/war-currents-ac-vs-dc-power 2 September 2021.

LeCun, Y., Bengio, Y. & Hinton, G. 2015. Deep learning. *Nature*, 521(7553): 436–444. https://doi.org/10.1038/nature14539.

León, C., Biscarri, F., Monedero, I., Guerrero, J.I., Biscarri, J. & Millán, R. 2011. Integrated expert system applied to the analysis of non-technical losses in power utilities. *Expert Systems with Applications*, 38(8): 10274–10285. https://linkinghub.elsevier.com/retrieve/pii/S0957417411002685.

Lepolesa, L.J., Achari, S. & Cheng, L. 2022. Electricity Theft Detection in Smart Grids Based on Deep Neural Network. *IEEE Access*, 10: 39638–39655. https://ieeexplore.ieee.org/document/9754513/.

Lepot, M., Aubin, J.-B. & Clemens, F. 2017. Interpolation in Time Series: An Introductive Overview of Existing Methods, Their Performance Criteria and Uncertainty Assessment. *Water*, 9(10): 1–20. https://www.mdpi.com/2073-4441/9/10/796.

Lewis, F.B. 2015. Costly 'Throw-Ups': Electricity Theft and Power Disruptions. *The Electricity Journal*, 28(7): 118–135. http://dx.doi.org/10.1016/j.tej.2015.07.009.

Li, S., Han, Y., Yao, X., Yingchen, S., Wang, J. & Zhao, Q. 2019. Electricity Theft Detection in Power Grids with Deep Learning and Random Forests. *Journal of Electrical and Computer Engineering*, 2019: 1–12. https://www.hindawi.com/journals/jece/2019/4136874/.

Liao, W., Bak-Jensen, B., Pillai, J.R., Xia, X., Ruan, G. & Yang, Z. 2024. Reducing Annotation Efforts in Electricity Theft Detection Through Optimal Sample Selection. *IEEE Transactions on Instrumentation and Measurement*, 73: 1–11. https://ieeexplore.ieee.org/document/10409125/.

Liao, W., Yang, Z., Liu, K., Zhang, B., Chen, X. & Song, R. 2022. Electricity Theft Detection Using Euclidean and Graph Convolutional Neural Networks. *IEEE Transactions on Power Systems*, 38(4): 3514–3527. https://ieeexplore.ieee.org/document/9852006/.

Liao, W., Zhu, R., Yang, Z., Liu, K., Zhang, B., Zhu, S. & Feng, B. 2024. Electricity Theft Detection Using Dynamic Graph Construction and Graph Attention Network. *IEEE Transactions on Industrial Informatics*, 20(4): 5074–5086. https://ieeexplore.ieee.org/document/10323252/.

Lin, C.-H., Chen, S.-J., Kuo, C.-L. & Chen, J.-L. 2014. Non-Cooperative Game Model Applied to an Advanced Metering Infrastructure for Non-Technical Loss Screening in Micro-Distribution Systems. *IEEE Transactions on Smart Grid*, 5(5): 2468–2469. https://ieeexplore.ieee.org/document/6880425.

Liu, J. & Zhao, Y. 2023. Improved generalization performance of convolutional neural networks with LossDA. *Applied Intelligence*, 53(11): 13852–13866. https://link.springer.com/10.1007/s10489-022-04208-6.

Liu, M., Yao, D., Liu, Z., Guo, J. & Chen, J. 2023. An Improved Adam Optimization Algorithm Combining Adaptive Coefficients and Composite Gradients Based on Randomized Block Coordinate Descent U. Rathnayake, ed. *Computational Intelligence and Neuroscience*, 2023(1–14). https://onlinelibrary.wiley.com/doi/10.1155/2023/4765891.

Liu, Y., Hu, S. & Member, S. 2015. Cyberthreat Analysis and Detection for Energy Theft in Social Networking of Smart Homes. *IEEE Transactions on Computational Social Systems*, 2(4): 148–158.

Lo, Y.-L., Huang, S.-C. & Lu, C.-N. 2012. Non-technical loss detection using smart distribution network measurement data. In *IEEE PES Innovative Smart Grid Technologies*. IEEE: 1–5. http://ieeexplore.ieee.org/document/6303316/.

Lobenstein, R. & Sulzberger, C. 2008. Eyewitness to dc history. *IEEE Power and Energy Magazine*, 6(3): 84–90. http://ieeexplore.ieee.org/document/4505831/.

Lovett, R. 2013. Maxwell’s Equations. *Topics in Quantum Mechanics*: 1–8. https://openscholarship.wustl.edu/chem_papers/12/.

Lu, C.-N., Huang, S.-C. & Lo, Y.-L. 2013. Non-technical loss detection using state estimation and analysis of variance. In *2013 IEEE Power & Energy Society General Meeting*. IEEE: 1–1. http://ieeexplore.ieee.org/document/6672128/.

Lu, X., Zhou, Y., Wang, Z., Yi, Y., Feng, L. & Wang, F. 2019. Knowledge Embedded Semi-Supervised Deep Learning for Detecting Non-Technical Losses in the Smart Grid. *Energies*, 12(18): 1–18. https://www.mdpi.com/1996-1073/12/18/3452.

Luan, W., Wang, G., Yu, Y., Lin, J., Zhang, W. & Liu, Q. 2015. Energy theft detection via integrated distribution state estimation based on AMI and SCADA measurements. In *2015 5th International Conference on Electric Utility Deregulation and Restructuring and Power Technologies (DRPT)*. IEEE: 751–756. http://ieeexplore.ieee.org/document/7432350/.

Ma, R., Chen, H.-H., Huang, Y.-R. & Meng, W. 2013. Smart Grid Communication: Its Challenges and Opportunities. *IEEE Transactions on Smart Grid*, 4(1): 36–46. http://ieeexplore.ieee.org/document/6451177/.

Malik, O.P. 2013. Evolution of Power Systems into Smarter Networks. *Journal of Control, Automation and Electrical Systems*, 24(1–2): 139–147. http://link.springer.com/10.1007/s40313-013-0005-6.

Martins, J.F., Pronto, A.G., Delgado-Gomes, V. & Sanduleac, M. 2019. Smart Meters and Advanced Metering Infrastructure. In *Pathways to a Smarter Power System*. Elsevier: 89–114. https://linkinghub.elsevier.com/retrieve/pii/B9780081025925000041.

Mashima, D. & Cárdenas, A.A. 2012. Evaluating Electricity Theft Detectors in Smart Grid Networks. In *International Workshop on Recent Advances in Intrusion Detection*. Springer: 210–229. http://link.springer.com/10.1007/978-3-642-33338-5_11.

Masnicki, R. & Mindykowski, J. 2018. What Should Be Measured Using Static Energy Meters. In *2018 International Conference and Exposition on Electrical And Power Engineering (EPE)*. IEEE: 0183–0188. https://ieeexplore.ieee.org/document/8559757/.

Massaferro, P., Martino, J.M. Di & Fernandez, A. 2020. Fraud Detection in Electric Power Distribution: An Approach That Maximizes the Economic Return. *IEEE Transactions on Power Systems*, 35(1): 703–710. https://ieeexplore.ieee.org/document/8760388/.

MathWorks. 2021. Convolution 1D Layer. *MathWorks*. https://www.mathworks.com/help/deeplearning/ref/nnet.cnn.layer.convolution1dlayer.html 25 September 2024.

McLaughlin, S., Holbert, B., Fawaz, A., Berthier, R. & Zonouz, S. 2013. A Multi-Sensor Energy Theft Detection Framework for Advanced Metering Infrastructures. *IEEE Journal on Selected Areas in Communications*, 31(7): 1319–1330. http://ieeexplore.ieee.org/document/6547839/.

Mebtoul, T. 2020. Energy Minister: Electricity Theft Costs Morocco $131 Million Annually. *Morocco World News*. https://www.moroccoworldnews.com/2020/11/326524/energy-minister-electricity-theft-costs-morocco-131-million-annually 9 January 2022.

Medium. 2023. Deep Learning Course — Lesson 5: Forward and Backward Propagation. *Machine Learning in Plain English - Medium*. https://medium.com/@nerdjock/deep-learning-course-lesson-5-forward-and-backward-propagation-ec8e4e6a8b92 25 August 2024.

Megger. 2020. Colombian utility identifies a way to reduce energy theft. *Electricity Supply International (ESI) Africa*. https://www.esi-africa.com/industry-sectors/transmission-and-distribution/colombian-utility-identifies-a-way-to-reduce-energy-theft/ 11 June 2021.

Mehdary, A., Chehri, A., Jakimi, A. & Saadane, R. 2024. Hyperparameter Optimization with Genetic Algorithms and XGBoost: A Step Forward in Smart Grid Fraud Detection. *Sensors*, 24(4): 1–24. https://www.mdpi.com/1424-8220/24/4/1230.

Messinis, G.M. & Hatziargyriou, N.D. 2018. Review of non-technical loss detection methods. *Electric Power Systems Research*, 158: 250–266. https://linkinghub.elsevier.com/retrieve/pii/S0378779618300051.

Meuse, M. 2016. BC Hydro uses new technology to stop theft, spot grow-ops. *Canadian Broadcasting Corporation (CBC) News*. https://www.cbc.ca/news/canada/british-columbia/hydro-grid-meters-1.3837496 26 December 2021.

Miao, J. & Niu, L. 2016. A Survey on Feature Selection. *Procedia Computer Science*, 91(Itqm): 919–926. http://dx.doi.org/10.1016/j.procs.2016.07.111.

Micheli, G., Soda, E., Vespucci, M.T., Gobbi, M. & Bertani, A. 2019. Big data analytics: an aid to detection of non-technical losses in power utilities. *Computational Management Science*, 16(1–2): 329–343. http://link.springer.com/10.1007/s10287-018-0325-x.

Mirza, F. & Hashmi, M. 2015. Long Run Determinants of Electricity Theft in Pakistan: An Empirical Analysis. *Pakistan Journal of Social Sciences (PJSS)*, 35(2): 599–608. http://pjss.bzu.edu.pk/index.php/pjss/article/view/337.

Misra, S., Li, H. & He, J. 2020. Robust geomechanical characterization by analyzing the performance of shallow-learning regression methods using unsupervised clustering methods. In *Machine Learning for Subsurface Characterization*. Elsevier: 129–155. http://dx.doi.org/10.1016/B978-0-12-817736-5.00005-3.

Mohammad, F., Saleem, K. & Al-Muhtadi, J. 2023. Ensemble-Learning-Based Decision Support System for Energy-Theft Detection in Smart-Grid Environment. *Energies*, 16(4): 1–16. https://www.mdpi.com/1996-1073/16/4/1907.

Montesinos López, O.A., Montesinos López, A. & Crossa, J. 2022. Fundamentals of Artificial Neural Networks and Deep Learning. In *Multivariate Statistical Machine Learning Methods for Genomic Prediction*. Cham: Springer International Publishing: 379–425. https://link.springer.com/10.1007/978-3-030-89010-0_10.

Mostafa, B., El-Attar, N., Abd-Elhafeez, S. & Awad, W. 2020. Machine and Deep Learning Approaches in Genome: Review Article. *Alfarama Journal of Basic & Applied Sciences*, 2(1): 105–113. https://ajbas.journals.ekb.eg/article_109144.html.

Muhammad, L.J., Algehyne, E.A. & Usman, S.S. 2020. Predictive Supervised Machine Learning Models for Diabetes Mellitus. *SN Computer Science*, 1(5): 1–10. https://doi.org/10.1007/s42979-020-00250-8.

Mujeeb, S., Javaid, N., Ahmed, A., Gulfam, S.M., Qasim, U., Shafiq, M. & Choi, J.-G. 2021. Electricity Theft Detection With Automatic Labeling and Enhanced RUSBoost Classification Using Differential Evolution and Jaya Algorithm. *IEEE Access*, 9: 128521–128539. https://ieeexplore.ieee.org/document/9507434/.

Mujeeb, S., Javaid, N., Khalid, R., Imran, M. & Naseer, N. 2020. DE-RUSBoost: An Efficient Electricity Theft Detection Scheme with Additive Communication Layer. In *ICC 2020 - 2020 IEEE International Conference on Communications (ICC)*. IEEE: 1–6. https://ieeexplore.ieee.org/document/9149315/.

Mujuzi, J.D. 2020. Electricity Theft in South Africa: Examining the Need to Clarify the Offence and Pursue Private Prosecution? *Obiter*, 41(1): 78–87. https://obiter.mandela.ac.za/article/view/10549.

Munawar, S., Javaid, N., Khan, Z.A., Chaudhary, N.I., Raja, M.A.Z., Milyani, A.H. & Ahmed Azhari, A. 2022. Electricity Theft Detection in Smart Grids Using a Hybrid BiGRU–BiLSTM Model with Feature Engineering-Based Preprocessing. *Sensors*, 22(20): 1–19. https://www.mdpi.com/1424-8220/22/20/7818.

Munawar, S., Khan, Z.A., Chaudhary, N.I., Javaid, N., Raja, M.A.Z., Milyani, A.H. & Azhari, A.A. 2022. Novel FDIs-based data manipulation and its detection in smart meters' electricity theft scenarios. *Frontiers in Energy Research*, 10(December): 1–13. https://www.frontiersin.org/articles/10.3389/fenrg.2022.1043593/full.

MyBroadband. 2015. Electricity theft in South Africa is out of control. https://mybroadband.co.za/news/energy/127894-electricity-theft-in-south-africa-is-out-of-control.html 31 January 2021.

Naeem, A., Aslam, Z., Shloul, T. Al, Naz, A., Nadeem, M.I., Al-Adhaileh, M.H., Ghadi, Y.Y. & Mohamed, H.G. 2023. A Novel Combined DenseNet and Gated Recurrent Unit Approach to Detect Energy Thefts in Smart Grids. *IEEE Access*, 11(May): 59496–59510. https://ieeexplore.ieee.org/document/10149326/.

Naeem, A., Javaid, N., Aslam, Z., Nadeem, M.I., Ahmed, K., Ghadi, Y.Y., Alahmadi, T.J., Ghamry, N.A. & Eldin, S.M. 2023. A novel data balancing approach and a deep fractal network with light gradient boosting approach for theft detection in smart grids. *Heliyon*, 9(9): 1–11. https://doi.org/10.1016/j.heliyon.2023.e18928.

Nagi, J., Keem Siah Yap, Sieh Kiong Tiong, Ahmed, S.K. & Nagi, F. 2011. Improving SVM-Based Nontechnical Loss Detection in Power Utility Using the Fuzzy Inference System. *IEEE Transactions on Power Delivery*, 26(2): 1284–1285. http://ieeexplore.ieee.org/document/5738432/.

Nagi, J., Yap, K.S., Tiong, S.K., Ahmed, S.K. & Mohamad, M. 2010. Nontechnical Loss Detection for Metered Customers in Power Utility Using Support Vector Machines. *IEEE Transactions on Power Delivery*, 25(2): 1162–1171. http://ieeexplore.ieee.org/document/5286297/.

Nawaz, A., Ali, T., Mustafa, G., Rehman, S.U. & Rashid, M.R. 2023. A novel technique for detecting electricity theft in secure smart grids using CNN and XG-boost. *Intelligent Systems with Applications*, 17(November 2022): 1–8. https://doi.org/10.1016/j.iswa.2022.200168.

Nayak, R. & Jaidhar, C.D. 2023. Employing Feature Extraction, Feature Selection, and Machine Learning to Classify Electricity Consumption as Normal or Electricity Theft. *SN Computer Science*, 4(5): 1–15. https://doi.org/10.1007/s42979-023-01911-0.

Nduhuura, P., Garschagen, M. & Zerga, A. 2021. Impacts of Electricity Outages in Urban Households in Developing Countries: A Case of Accra, Ghana. *Energies*, 14(12): 3676. https://www.mdpi.com/1996-1073/14/12/3676.

Nduhuura, P., Garschagen, M. & Zerga, A. 2020. Mapping and spatial analysis of electricity load shedding experiences: A case study of communities in accra, ghana. *Energies*, 13(17): 1–26.

Neto, E.A.C.A. & Coelho, J. 2013. Probabilistic methodology for Technical and Non-Technical Losses estimation in distribution system. *Electric Power Systems Research*, 97: 93–99. http://dx.doi.org/10.1016/j.epsr.2012.12.008.

Nettleton, D. 2014. Selection of Variables and Factor Derivation. In *Commercial Data Mining*. Elsevier: 79–104. https://linkinghub.elsevier.com/retrieve/pii/B9780124166028000066.

Ngamchuen, S. & Pirak, C. 2013. Smart anti-tampering algorithm design for single phase smart meter applied to AMI systems. In *2013 10th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology*. IEEE: 1–6. http://ieeexplore.ieee.org/document/6559617/.

Nielsen, M. 2015. *Neural networks and deep learning*. http://neuralnetworksanddeeplearning.com/.

Nikovski, D.N., Wang, Z., Esenther, A., Sun, H., Sugiura, K., Muso, T. & Tsuru, K. 2013. Smart Meter Data Analysis for Power Theft Detection. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. 379–389. http://link.springer.com/10.1007/978-3-642-39712-7_29.

Nilsson, N.J. 2013. *The Quest for Artificial Intelligence*. Cambridge University Press. https://www.cambridge.org/core/product/identifier/9780511819346/type/book.

Nirmal, S., Patil, P. & Kumar, J.R.R. 2024. CNN-AdaBoost based hybrid model for electricity theft detection in smart grid. *e-Prime - Advances in Electrical Engineering, Electronics and Energy*, 7(January): 1–8. https://doi.org/10.1016/j.prime.2024.100452.

Noor, N.M., Al Bakri Abdullah, M.M., Yahaya, A.S. & Ramli, N.A. 2014. Comparison of Linear Interpolation Method and Mean Method to Replace the Missing Values in Environmental Data Set. *Materials Science Forum*, 803: 278–281. https://www.scientific.net/MSF.803.278.

North Africa Post. 2021. Illegal power connections: Tunisia loses over $106m a year. *The North Africa Post*. https://northafricapost.com/48683-illegal-power-connections-tunisia-loses-over-106m-a-year.html 9 January 2022.

OBAID, Z.A., CIPCIGAN, L.M., ABRAHIM, L. & MUHSSIN, M.T. 2019. Frequency control of future power systems: reviewing and evaluating challenges and new control methods. *Journal of Modern Power Systems and Clean Energy*, 7(1): 9–25. https://doi.org/10.1007/s40565-018-0441-1.

Observer. 2017. JPS ready to name, shame and prosecute electricity thieves. *Antigua Observer Newspaper*. https://antiguaobserver.com/jps-ready-to-name-shame-and-prosecute-electricity-thieves/ 11 April 2023.

Ojoye, T. 2019. Nigerians see power supply as social service. *The Punch*. https://punchng.com/nigerians-see-power-supply-as-social-service-nextier-boss/ 26 May 2021.

Okwumbu-Imafidon, R. 2020. Discos call for sanctions on perpetrators of electricity theft. *Nairametrics (Energy)*. https://nairametrics.com/2020/06/26/discos-call-for-sanctions-on-perpetrators-of-electricity-theft/ 6 January 2022.

Oladokun, V.O. & Asemota, O.C. 2015. Unit cost of electricity in Nigeria: A cost model for captive diesel powered generating system. *Renewable and Sustainable Energy Reviews*, 52: 35–40. http://dx.doi.org/10.1016/j.rser.2015.07.028.

de Oliveira, M.E., Boson, D.F.A. & Padilha-Feltrin, A. 2008. A statistical analysis of loss factor to determine the energy losses. In *2008 IEEE/PES Transmission and Distribution Conference and Exposition: Latin America*. IEEE: 1–6. http://ieeexplore.ieee.org/document/4641691/.

de Oliveira, M.E., Padilha-Feltrin, A. & Candian, F.J. 2006. Investigation of the Relationship between Load and Loss Factors for a Brazilian Electric Utility. In *2006 IEEE/PES Transmission & Distribution Conference and Exposition: Latin America*. IEEE: 1–6. http://ieeexplore.ieee.org/document/4104638/.

Oloruntoba, D.O. & Komolafe, O.A. 2018. Development Of A Smart Electrical Energy Meter For Controlling Power Consumption. *Ife Journal of Technology*, 25(1): 15–19. http://ijt.oauife.edu.ng/index.php/ijt/article/view/132.

Oluwasuji, O.I., Malik, O., Zhang, J. & Ramchurn, S.D. 2018. Algorithms for Fair Load Shedding in Developing Countries. In *Proceedings of the Twenty-Seventh International Joint Conference on Artificial Intelligence*. California: International Joint Conferences on Artificial Intelligence Organization: 1590–1596. https://www.ijcai.org/proceedings/2018/220.

Oluwasuji, O.I., Malik, O., Zhang, J. & Ramchurn, S.D. 2020. Solving the fair electric load shedding problem in developing countries. *Autonomous Agents and Multi-Agent Systems*, 34(1): 12. https://doi.org/10.1007/s10458-019-09428-8.

Onat, N. 2018. Electricity Theft Problem and Effects of Privatization Policies on Distribution Losses of Turkey. *Celal Bayar Üniversitesi Fen Bilimleri Dergisi*, 14(2): 163–176. https://dergipark.org.tr/en/doi/10.18466/cbayarfbe.387054.

Osmanski, S. 2020. How Do Carbon Emissions Affect the Environment? *Green Matters*. https://www.greenmatters.com/p/how-do-carbon-emissions-affect-environment 21 June 2021.

Osypova, S. 2020. *Consumption Pattern Detection Through the Use of Machine Learning: Clustering Techniques for Non-Technical Losses Detection RERORT*. Universitat Politècnica de Catalunya (UPC). http://hdl.handle.net/2117/332789.

Otcenasova, A., Bolf, A., Altus, J. & Regula, M. 2019. The Influence of Power Quality Indices on Active Power Losses in a Local Distribution Grid. *Energies*, 12(7): 1–31. https://www.mdpi.com/1996-1073/12/7/1389.

Otchere-Appiah, G., Takahashi, S., Yeboah, M.S. & Yoshida, Y. 2021. The Impact of Smart Prepaid Metering on Non-Technical Losses in Ghana. *Energies*, 14(7): 2–16. https://www.mdpi.com/1996-1073/14/7/1852.

Owens, B.N. 2019. *The Wind Power Story: A Century of Innovation That Reshaped the Global Energy Landscape*. Wiley-IEEE Press.

Pamir, Javaid, N., Javaid, S., Asif, M., Javed, M.U., Yahaya, A.S. & Aslam, S. 2022. Synthetic

Theft Attacks and Long Short Term Memory-Based Preprocessing for Electricity Theft Detection Using Gated Recurrent Unit. *Energies*, 15(8): 1–20. https://www.mdpi.com/1996-1073/15/8/2778.

Pamir, Javaid, N., Javed, M.U., Houran, M.A., Almasoud, A.M. & Imran, M. 2023. Electricity theft detection for energy optimization using deep learning models. *Energy Science & Engineering*, 11(10): 3575–3596. https://onlinelibrary.wiley.com/doi/10.1002/ese3.1541.

Pamir, Javaid, N., Qasim, U., Yahaya, A.S., Alkhammash, E.H. & Hadjouni, M. 2022. Non-Technical Losses Detection Using Autoencoder and Bidirectional Gated Recurrent Unit to Secure Smart Grids. *IEEE Access*, 10: 56863–56875. https://ieeexplore.ieee.org/document/9765457/.

Pamir, Ullah, A., Munawar, S., Asif, M., Kabir, B. & Javaid, N. 2021. Synthetic Theft Attacks Implementation for Data Balancing and a Gated Recurrent Unit Based Electricity Theft Detection in Smart Grids. In *Complex, Intelligent and Software Intensive Systems. CISIS 2021*. 395–405. https://link.springer.com/10.1007/978-3-030-79725-6_39.

Panchal, S. 2021. No, Kernels & Filters Are Not The Same. *Towards Data Science*. https://towardsdatascience.com/no-kernels-filters-are-not-the-same-b230ec192ac9 31 July 2024.

Pansambal, B.H. & Nandgaokar, A.B. 2023. Integrating Dropout Regularization Technique at Different Layers to Improve the Performance of Neural Networks. *International Journal of Advanced Computer Science and Applications (IJACSA)*, 14(4): 716–722. http://thesai.org/Publications/ViewPaper?Volume=14&Issue=4&Code=IJACSA&SerialNo=78.

Papalexopoulos, A. 2013. Transmission Grid Fundamentals. In *Climate Vulnerability*. Elsevier: 217–230. http://dx.doi.org/10.1016/B978-0-12-384703-4.00327-0.

Park, S. & Kwak, N. 2017. Analysis on the Dropout Effect in Convolutional Neural Networks. In S.-H. Lai, V. Lepetit, K. Nishino, & Y. Sato, eds. *Computer Vision – ACCV 2016*. Lecture Notes in Computer Science. Cham: Springer International Publishing: 189–204. http://link.springer.com/10.1007/978-3-319-54184-6.

Paruchuri, V. & Dubey, S. 2012. An approach to determine non-technical energy losses in India. *International Conference on Advanced Communication Technology, ICACT*: 111–115. https://ieeexplore.ieee.org/abstract/document/6174622.

Pasdar, A. & Mirzakuchaki, S. 2007. A Solution to Remote Detecting of Illegal Electricity Usage Based on Smart Metering. In *2007 2nd International Workshop on Soft Computing Applications*. IEEE: 163–167. http://ieeexplore.ieee.org/document/4318322/.

Patro, S.G.K. & Sahu, K.K. 2015. Normalization: A Preprocessing Stage. *International Advanced Research Journal in Science, Engineering and Technology (IARJSET)*, 2(3): 20–22. http://www.iarjset.com/upload/2015/march-15/IARJSET 5.pdf.

Pedramnia, K. & Shojaei, S. 2020. Detection of False Data Injection Attack in Smart Grid Using Decomposed Nearest Neighbor Techniques. In *2020 10th Smart Grid Conference (SGC)*. IEEE: 1–6. https://ieeexplore.ieee.org/document/9335732/.

Peng, B., Wan, C., Dong, S., Lin, J., Song, Y., Zhang, Y. & Xiong, J. 2016. A two-stage pattern recognition method for electric customer classification in smart grid. In *2016 IEEE International Conference on Smart Grid Communications (SmartGridComm)*. IEEE: 758–763. http://ieeexplore.ieee.org/document/7778853/.

Pereira, J. & Saraiva, F. 2021. Convolutional neural network applied to detect electricity theft: A comparative study on unbalanced data handling techniques. *International Journal of Electrical Power & Energy Systems*, 131(March): 1–7. https://doi.org/10.1016/j.ijepes.2021.107085.

Peters, M., Ketter, W., Saar-Tsechansky, M. & Collins, J. 2013. A reinforcement learning approach to autonomous decision-making in smart electricity markets. *Machine Learning*, 92(1): 5–39. http://link.springer.com/10.1007/s10994-013-5340-0.

Petrlik, I., Lezama, P., Rodriguez, C., Inquilla, R., Reyna-González, J.E. & Esparza, R. 2022. Electricity Theft Detection using Machine Learning. *International Journal of Advanced Computer Science and Applications*, 13(12): 420–425. http://thesai.org/Publications/ViewPaper?Volume=13&Issue=12&Code=IJACSA&SerialNo=51.

Pickering, P. 2016. E-Meters Offer Multiple Ways to Combat Electricity Theft and Tampering. *Electronic Design*. https://www.electronicdesign.com/technologies/meters/article/21802049/emeters-offer-multiple-ways-to-combat-electricity-theft-and-tampering 19 December 2021.

Porcu, D., Chochliouros, I.P., Castro, S., Fiorentino, G., Costa, R., Nodaros, D., Koumaras, V., Brasca, F., di Pietro, N., Papaioannou, G., Ciornei, I., Sarigiannidis, A., Palov, N., Bobochikov, T., Zarakovitis, C. & Spiliopoulou, A.S. 2021. 5G Communications as "Enabler" for Smart Power Grids: The Case of the Smart5Grid Project. In *IFIP Advances in Information and Communication Technology*. Springer, Cham: 7–20. https://link.springer.com/10.1007/978-3-030-79157-5.

Poudel, S. & Dhungana, U.R. 2022. Artificial intelligence for energy fraud detection: a review. *International Journal of Applied Power Engineering (IJAPE)*, 11(2): 109–119. https://ijape.iaescore.com/index.php/IJAPE/article/view/20383.

Primicanta, A.H. 2013. *The Prototype of Low Power Zigbee-GSM Based Automatic Meter Reading System*. Universiti Technologi Petronas. http://utpedia.utp.edu.my/id/eprint/22695/.

Qazi, S. 2017. Photovoltaics for Disaster Relief and Remote Areas. In *Standalone Photovoltaic (PV) Systems for Disaster Relief and Remote Areas*. Elsevier: 1–30. https://linkinghub.elsevier.com/retrieve/pii/B9780128030226000010.

Quinlan, J.R. 1992. Learning with continuous classes. In *Australian Joint Conference on Artificial Intelligence*. 343–348. https://doi.org/10.1142/9789814536271.

Ramchurn, S.D., Vytelingum, P., Rogers, A. & Jennings, N.R. 2012. Putting the 'Smarts' into the Smart Grid: A Grand Challenge for Artificial Intelligence. *Communications of the ACM*, 55(4): 86–97. https://dl.acm.org/doi/10.1145/2133806.2133825.

Ramezan, C.A., Warner, T.A., Maxwell, A.E. & Price, B.S. 2021. Effects of Training Set Size on Supervised Machine-Learning Land-Cover Classification of Large-Area High-Resolution Remotely Sensed Data. *Remote Sensing*, 13(3): 1–27. https://www.mdpi.com/2072-

4292/13/3/368.

Ramos, C.C.O., Papa, J.P., Sousa, A.N., Chiachia, G. & Falcao, A.X. 2011. A New Approach for Nontechnical Losses Detection Based on Optimum-Path Forest. *IEEE Transactions on Power Systems*, 26(1): 181–189. http://ieeexplore.ieee.org/document/5530391/.

Ramos, C.C.O., Rodrigues, D., de Souza, A.N. & Papa, J.P. 2018. On the Study of Commercial Losses in Brazil: A Binary Black Hole Algorithm for Theft Characterization. *IEEE Transactions on Smart Grid*, 9(2): 676–683. http://ieeexplore.ieee.org/document/7463030/.

Rapp, D.N. & Mensink, M.C. 2011. Focusing Effects from Online and Offline Reading Tasks. In M. T. McCrudden, J. P. Magliano, & G. Schraw, eds. *Text Relevance and Learning from Text*. Greenwich, CT: Information Age Publishing: 141–164.

Raschka, S., Patterson, J. & Nolet, C. 2020. Machine Learning in Python: Main Developments and Technology Trends in Data Science, Machine Learning, and Artificial Intelligence. *Information*, 11(4): 1–44. https://www.mdpi.com/2078-2489/11/4/193.

Rastogi, S., Sharma, M. & Varshney, P. 2016. Internet of Things based Smart Electricity Meters. *International Journal of Computer Applications*, 133(8): 13–16. http://www.ijcaonline.org/research/volume133/number8/rastogi-2016-ijca-907903.pdf.

Reinhardt, A. & Pereira, L. 2021. Special Issue: “Energy Data Analytics for Smart Meter Data”. *Energies*, 14(17): 1–3. https://www.mdpi.com/1996-1073/14/17/5376.

Rendroyoko, I., Setiawan, A.D. & Suhardi. 2021. Development of Meter Data Management System Based-on Event-Driven Streaming Architecture for IoT-based AMI Implementation. In *2021 3rd International Conference on High Voltage Engineering and Power Systems (ICHVEPS)*. IEEE: 403–407. https://ieeexplore.ieee.org/document/9601104/.

Reuters. 2009. Clerics condemn theft of electricity. https://www.reuters.com/article/us-power-decree/clerics-condemn-theft-of-electricity-idUSTRE56C4RL20090713?feedType=RSS&feedName=oddlyEnoughNews 1 February 2021.

Reyad, M., Sarhan, A.M. & Arafa, M. 2023. A modified Adam algorithm for deep neural network optimization. *Neural Computing and Applications*, 35(23): 17095–17112. https://doi.org/10.1007/s00521-023-08568-z.

Ribeiro, G., Maione, C., Goncalves, C., de Castro Rodrigues, D. & Barbosa, R.M. 2021. Recent advances in detection and prediction of customers energy consumption patterns through the use of machine learning techniques. In *2021 International Conference on Engineering and Emerging Technologies (ICEET)*. IEEE: 1–8. https://ieeexplore.ieee.org/document/9659738/.

Ricks, G.W.D. 1896. Eelectricity supply meters. *Journal of the Institution of Electrical Engineers*, 25(120): 57–77. https://digital-library.theiet.org/content/journals/10.1049/jiee-1.1896.0005.

Robinson, C. 2014. Electricity theft and the politics of entitlement. *Jamaica Observer*. https://www.jamaicaobserver.com/columns/electricity-theft-and-the-politics-of-entitlement/ 13 April 2023.

Ruch, C. 1984. George Westinghouse-Engineer and DOER!!! *IEEE Transactions on Industry Applications*, IA-20(6): 1395–1402. http://ieeexplore.ieee.org/document/4504619/.

Russel, S.J. & Norvig, P. 2021. *Artificial intelligence: A modern approach*. 4th ed. New York: Pearson.

Rutgers. 1882. Pearl street central station. *Rutgers School of Arts and Sciences (Thomas A. Edison Papers)*, (March): 423–428. http://edison.rutgers.edu/yearofinno/EL/PearlStreetHeadnote.pdf.

Sacco, D., Motta, G., You, L. -l., Bertolazzo, N., Carini, F. & Ma, T. -y. 2017. Smart cities, urban sensing, and big data: mining geo-location in social networks. In *Big Data and Smart Service Systems*. Elsevier: 59–84. https://linkinghub.elsevier.com/retrieve/pii/B9780128120132000058.

Saeed, M.S., Mustafa, M.W., Hamadneh, N.N., Alshammari, N.A., Sheikh, U.U., Jumani, T.A., Khalid, S.B.A. & Khan, I. 2020. Detection of Non-Technical Losses in Power Utilities—A Comprehensive Systematic Review. *Energies*, 13(18): 1–25. https://www.mdpi.com/1996-1073/13/18/4727.

Sainworla, F. 2021. Higher-ups, Others Involved In Power Theft To Be Named And Shamed. *News Public Trust*. https://newspublictrust.com/higher-ups-others-involved-in-power-theft-to-be-named-and-shamed/ 12 April 2023.

Salinas, S.A. & Li, P. 2016. Privacy-Preserving Energy Theft Detection in Microgrids: A State Estimation Approach. *IEEE Transactions on Power Systems*, 31(2): 883–894. https://ieeexplore.ieee.org/document/7087399/.

Salman Saeed, M., Mustafa, M.W., Sheikh, U.U., Jumani, T.A., Khan, I., Atawneh, S. & Hamadneh, N.N. 2020. An Efficient Boosted C5.0 Decision-Tree-Based Classification Approach for Detecting Non-Technical Losses in Power Utilities. *Energies*, 13(12): 1–19. https://www.mdpi.com/1996-1073/13/12/3242.

SAP. 2021. The smart grid: How AI is powering today’s energy technologies. *SAP Insights*. https://www.sap.com/insights/smart-grid-ai-in-energy-technologies.html 25 June 2023.

Saponara, S. & Bacchillone, T. 2012. Network Architecture, Security Issues, and Hardware Implementation of a Home Area Network for Smart Grid. *Journal of Computer Networks and Communications*, 2012: 1–19. http://www.hindawi.com/journals/jcnc/2012/534512/.

Saripuddin, M., Suliman, A., Syarmila Sameon, S. & Jorgensen, B.N. 2021. Random Undersampling on Imbalance Time Series Data for Anomaly Detection. In *2021 The 4th International Conference on Machine Learning and Machine Intelligence*. New York, NY, USA: ACM: 151–156. https://dl.acm.org/doi/10.1145/3490725.3490748.

Savian, F. de S., Siluk, J.C.M., Garlet, T.B., do Nascimento, F.M., Pinheiro, J.R. & Vale, Z. 2021. Non-technical losses: A systematic contemporary article review. *Renewable and Sustainable Energy Reviews*, 147(April): 111205. https://linkinghub.elsevier.com/retrieve/pii/S1364032121004937.

Saxena, P. 2023. Evaluation Metrics for Classification Models in Machine Learning (Part 2). *comet ML*. https://www.comet.com/site/blog/evaluation-metrics-for-classification-models-in-machine-learning-part-2/ 16 February 2024.

Schuster, E.J. 1901. German Legislation in 1900. *Journal of the Society of Comparative Legislation*, 3(1): 119–125. https://www.jstor.org/stable/752029.

SEI. 2006. The history of the electricity meter. *Smart Energy International (SEI)*. https://www.smart-energy.com/features-analysis/the-history-of-the-electricity-meter/ 13 August 2021.

Serrano, N.C. 2019. CFE reports MXN$60 billion loss due to power theft. *El Universal*. https://www.eluniversal.com.mx/english/cfe-reports-mxn60-billion-loss-due-power-theft 31 May 2021.

Sesay, I. 2021. Six Special Electricity Crimes Court for Electricity Theft. *Sierra Leone News Agency (SLENA)*. https://slena.gov.sl/News/six-special-electricity-crimes-court-for-electricity-theft 29 June 2024.

Shahzadi, N., Javaid, N., Akbar, M., Aldegheishem, A., Alrajeh, N. & Bouk, S.H. 2024. A novel data driven approach for combating energy theft in urbanized smart grids using artificial intelligence. *Expert Systems with Applications*, 253(July 2023): 1–21. https://doi.org/10.1016/j.eswa.2024.124182.

Sharma, D.D., Singh, S.N., Lin, J. & Foruzan, E. 2017. Identification and characterization of irregular consumptions of load data. *Journal of Modern Power Systems and Clean Energy*, 5(3): 465–477. http://link.springer.com/10.1007/s40565-017-0268-1.

Sharma, T., Pandey, K.K., Punia, D.K. & Rao, J. 2016. Of pilferers and poachers: Combating electricity theft in India. *Energy Research & Social Science*, 11: 40–52. https://linkinghub.elsevier.com/retrieve/pii/S2214629615300293.

Shehzad, F., Javaid, N., Almogren, A., Ahmed, A., Gulfam, S.M. & Radwan, A. 2021. A Robust Hybrid Deep Learning Model for Detection of Non-Technical Losses to Secure Smart Grids. *IEEE Access*, 9: 128663–128678. https://ieeexplore.ieee.org/document/9540700/.

Shokoya, N.O. & Raji, A.K. 2019a. Electricity theft: A reason to deploy smart grid in South Africa. In *Proceedings of the 27th International Conference on the Domestic Use of Energy, DUE 2019*. 96–101. https://ieeexplore.ieee.org/abstract/document/8734431.

Shokoya, N.O. & Raji, A.K. 2019b. Electricity theft mitigation in the Nigerian power sector. *International Journal of Engineering & Technology*, 8(4): 467–472. https://doi.org/10.14419/ijet.v8i4.29391.

Silver, D., Hubert, T., Schrittwieser, J., Antonoglou, I., Lai, M., Guez, A., Lanctot, M., Sifre, L., Kumaran, D., Graepel, T., Lillicrap, T., Simonyan, K. & Hassabis, D. 2018. A general reinforcement learning algorithm that masters chess, shogi, and Go through self-play. *Science*, 362(6419): 1140–1144. https://www.science.org/doi/10.1126/science.aar6404.

Singh, B., Kumar, R. & Singh, V.P. 2022. Reinforcement learning in robotic applications: a comprehensive survey. *Artificial Intelligence Review*, 55(2): 945–990. https://doi.org/10.1007/s10462-021-09997-9.

Singh, D. & Singh, B. 2022. Feature wise normalization: An effective way of normalizing data. *Pattern Recognition*, 122: 1–14. https://doi.org/10.1016/j.patcog.2021.108307.

Smith, T.B. 2004. Electricity theft: a comparative analysis. *Energy Policy*, 32(18): 2067–2076. https://linkinghub.elsevier.com/retrieve/pii/S0301421503001824.

Smithsonian. 2001. Lighting A Revolution: 19th Century Preconditions. *Smithsonian National Museum of American History*. https://americanhistory.si.edu/lighting/19thcent/prec19.htm 6 July 2023.

Smithsonian. 2019. Samuel Gardiner, Jr. Electro-Magnetic Meter. *Smithsonian National Museum of American History*. https://americanhistory.si.edu/collections/search/object/nmah_703350 9 April 2023.

Soliman, M.H., Talaat, H.E.A. & Attia, M.A. 2021. Power system frequency control enhancement by optimization of wind energy control system. *Ain Shams Engineering Journal*, 12(4): 3711–3723. https://doi.org/10.1016/j.asej.2021.03.027.

Sowmya, B., Kumar, B.S. & Gangadhar, V.V.R.L.S. 2016. Wireless ARM-Based Automatic Meter Reading & Control System (WAMRCS). *International Journal of Advanced Technology and Innovative Research*, 8(22): 4366–4370. http://www.ijatir.org/uploads/253416IJATIR13020-694.pdf.

Soyemi, A.O., Samuel, I.A., Ayobami, A.A.O. & Akinmeji, A. 2021. The Challenges of Estimated Billing on Electricity Consumers in Nigeria: A Review. *IOP Conference Series: Earth and Environmental Science*, 730(1): 012025. https://iopscience.iop.org/article/10.1088/1755-1315/730/1/012025.

Spark Media. 2016. Seminar on Electricity Theft: PHED CEO. *Spark Ltd for Port Harcourt Electricity Distribution Company (PHED), Nigeria*. https://www.youtube.com/watch?v=7wUo7Uq7RSo 22 December 2021.

Spirić, J. V., Dočić, M.B. & Stanković, S.S. 2015. Fraud detection in registered electricity time series. *International Journal of Electrical Power & Energy Systems*, 71: 42–50. https://linkinghub.elsevier.com/retrieve/pii/S0142061515001209.

Spirić, J. V., Stanković, S.S., Dočić, M.B. & Popović, T.D. 2014. Using the rough set theory to detect fraud committed by electricity customers. *International Journal of Electrical Power and Energy Systems*, 62: 727–734.

Srivastava, N., Hinton, G., Krizhevsky, A., Sutskever, I. & Salakhutdinov, R. 2014. Dropout : A Simple Way to Prevent Neural Networks from Overfitting. *Journal of Machine Learning Research (JMLR)*, 15(56): 1929–1958. http://jmlr.org/papers/v15/srivastava14a.html.

Stracqualursi, E., Rosato, A., Di Lorenzo, G., Panella, M. & Araneo, R. 2023. Systematic review of energy theft practices and autonomous detection through artificial intelligence methods. *Renewable and Sustainable Energy Reviews*, 184(June): 1–19. https://doi.org/10.1016/j.rser.2023.113544.

Su, C.-L., Lee, W.-H. & Wen, C.-K. 2016. Electricity theft detection in low voltage networks with smart meters using state estimation. In *2016 IEEE International Conference on Industrial Technology (ICIT)*. IEEE: 493–498. http://ieeexplore.ieee.org/document/7474800/.

Sulzberger, C. 2013. Pearl Street in Miniature: Models of the Electric Generating Station. *IEEE Power and Energy Magazine*, 11(2): 76–85. http://ieeexplore.ieee.org/document/6466478/.

Sulzberger, C.L. 2003a. Triumph of AC. 2. The battle of the currents. *IEEE Power and Energy Magazine*, 1(4): 70–73. https://ieeexplore.ieee.org/document/1213534/.

Sulzberger, C.L. 2003b. Triumph of AC - from Pearl Street to Niagara. *IEEE Power and Energy Magazine*, 1(3): 64–67. https://ieeexplore.ieee.org/document/1213534/.

Sun, Y., Sun, X., Hu, T. & Zhu, L. 2023. Smart Grid Theft Detection Based on Hybrid Multi-Time Scale Neural Network. *Applied Sciences*, 13(9): 1–22. https://www.mdpi.com/2076-3417/13/9/5710.

Sun, Z. & Liang, W. 2016. A Survey of Communication Technologies for the Energy Local Area Network in the Energy Internet. In *Proceedings of the 2016 6th International Conference on Advanced Design and Manufacturing Engineering (ICADME 2016)*. Paris, France: Atlantis Press: 900–903. http://www.atlantis-press.com/php/paper-details.php?id=25862879.

Tariq, M. & Poor, H.V. 2016. Electricity Theft Detection and Localization in Grid-tied Microgrids. *IEEE Transactions on Smart Grid*, 9(3): 1–1. http://ieeexplore.ieee.org/document/7552555/.

Tatte, R., Chaudhari, M., Khrabe, M., Lokhnade, P., Muneshwar, P. & Yenorkar, D. 2019. Power Theft and Fault Detection using IoT Technology. *International Research Journal of Engineering and Technology (IRJET)*, 6(3): 175–178. https://www.irjet.net/archives/V6/i3/IRJET-V6I332.pdf.

TBY. 2014. Pylon the Power. *The Business Year (TBY)*. https://www.thebusinessyear.com/article/pylon-the-power/ 6 September 2022.

Tehrani, S.O., Shahrestani, A. & Yaghmaee, M.H. 2022. Online electricity theft detection framework for large-scale smart grid data. *Electric Power Systems Research*, 208(March): 1–10. https://doi.org/10.1016/j.epsr.2022.107895.

Terciyanli, E., Eryigit, E., Emre, T. & Caliskan, S. 2017. Score based non-technical loss detection algorithm for electricity distribution networks. In *2017 5th International Istanbul Smart Grid and Cities Congress and Fair (ICSG)*. IEEE: 180–184. http://ieeexplore.ieee.org/document/7947629/.

Trace, S. 2020. South Africa’s crippling electricity problem. *Oxford Policy Management*. https://www.opml.co.uk/blog/south-africa-s-crippling-electricity-problem 3 October 2021.

Tsiatsis, V., Karnouskos, S., Höller, J., Boyle, D. & Mulligan, C. 2019. Smart Grid. In *Internet of Things*. Elsevier: 257–268. https://linkinghub.elsevier.com/retrieve/pii/B9780128144350000250.

Tuballa, M.L. & Abundo, M.L. 2016. A review of the development of Smart Grid technologies. *Renewable and Sustainable Energy Reviews*, 59: 710–725. http://dx.doi.org/10.1016/j.rser.2016.01.011.

Turing. 2022. What Is the Necessity of Bias in Neural Networks? *Artificial Neural Networks*. https://www.turing.com/kb/necessity-of-bias-in-neural-networks 18 September 2024.

Tweed, K. 2013. Pot Growers Costing Canada $500 Million in Power Theft. *Greentech Media*. https://www.greentechmedia.com/articles/read/pot-growers-costing-canada-500-million-in-power-theft 30 December 2021.

Ullah, A., Javaid, N., Asif, M., Javed, M.U. & Yahaya, A.S. 2022. AlexNet, AdaBoost and Artificial Bee Colony Based Hybrid Model for Electricity Theft Detection in Smart Grids. *IEEE Access*, 10: 18681–18694. https://ieeexplore.ieee.org/document/9707814/.

Ullah, A., Javaid, N., Samuel, O., Imran, M. & Shoaib, M. 2020. CNN and GRU based Deep Neural Network for Electricity Theft Detection to Secure Smart Grid. In *2020 International Wireless Communications and Mobile Computing (IWCMC)*. IEEE: 1598–1602. https://ieeexplore.ieee.org/document/9148314/.

Ullah, A., Javaid, N., Yahaya, A.S., Sultana, T., Al-Zahrani, F.A. & Zaman, F. 2021. A Hybrid Deep Neural Network for Electricity Theft Detection Using Intelligent Antenna-Based Smart Meters D. Pinchera, ed. *Wireless Communications and Mobile Computing*, 2021(1): 1–19. https://onlinelibrary.wiley.com/doi/10.1155/2021/9933111.

Upadhyay, R. 2018. UT to name, shame power defaulters. *The Tribune India*. https://www.tribuneindia.com/news/archive/chandigarh/ut-to-name-shame-power-defaulters-535883 11 April 2023.

USDOE. 2008. Grid Modernization and the Smart Grid. *United States Department of Energy (USDOE)*. https://www.energy.gov/oe/activities/technology-development/grid-modernization-and-smart-grid 23 May 2021.

Vanguard. 2021. Energy Theft: Ikeja Electric introduces incentive for whistleblowers. *Vanguard Media Limited*. https://www.vanguardngr.com/2021/02/energy-theft-ikeja-electric-introduces-incentive-for-whistleblowers/ 25 December 2021.

Velasco Rodríguez, J.Á. 2022. *Power Losses Estimation in Low Voltage Smart Grids*. Universidad Carlos III de Madrid. https://e-archivo.uc3m.es/handle/10016/35860.

Verma, S. 2019. Understanding 1D and 3D Convolution Neural Network | Keras. *Towards Data Science*. https://towardsdatascience.com/understanding-1d-and-3d-convolution-neural-network-keras-9d8f76e29610 29 July 2024.

Viegas, J.L., Esteves, P.R., Melício, R., Mendes, V.M.F. & Vieira, S.M. 2017. Solutions for detection of non-technical losses in the electricity grid: A review. *Renewable and Sustainable Energy Reviews*, 80: 1256–1268. https://linkinghub.elsevier.com/retrieve/pii/S1364032117308328.

Vincent, A.M. & Jidesh, P. 2023. An improved hyperparameter optimization framework for AutoML systems using evolutionary algorithms. *Scientific Reports*, 13(1): 4737. https://doi.org/10.1038/s41598-023-32027-3.

Voskoglou, C. 2017. What is the best programming language for Machine Learning? https://towardsdatascience.com/what-is-the-best-programming-language-for-machine-learning-a745c156d6b7 15 October 2023.

Wabukala, B.M., Mukisa, N., Watundu, S., Bergland, O., Rudaheranwa, N. & Adaramola, M.S. 2023. Impact of household electricity theft and unaffordability on electricity security: A case of Uganda. *Energy Policy*, 173(January): 1–16. https://doi.org/10.1016/j.enpol.2022.113411.

Wang, H. 2023. Research on the Application of Random Forest-based Feature Selection Algorithm in Data Mining Experiments. *International Journal of Advanced Computer*

Science and Applications, 14(10): 505–518. http://thesai.org/Publications/ViewPaper?Volume=14&Issue=10&Code=IJACSA&SerialNo=54.

Wang, J., Si, Y., Zhu, Y., Zhang, K., Yin, S. & Liu, B. 2024. Cyberattack detection for electricity theft in smart grids via stacking ensemble GRU optimization algorithm using federated learning framework. *International Journal of Electrical Power & Energy Systems*, 157(December 2023): 1–16. https://doi.org/10.1016/j.ijepes.2024.109848.

Wang, X., Xie, H., Tang, L., Chen, C. & Bie, Z. 2024. Decentralized Privacy-Preserving Electricity Theft Detection for Distribution System Operators. *IEEE Transactions on Smart Grid*, 15(2): 2179–2190. https://ieeexplore.ieee.org/document/10246323/.

Wang, Y., Jin, S. & Cheng, M. 2023. A Convolution–Non-Convolution Parallel Deep Network for Electricity Theft Detection. *Sustainability*, 15(13): 1–22. https://www.mdpi.com/2071-1050/15/13/10127.

Wang, Y., Wang, J., Dong, X., Du, P., Ni, M., Wang, C., Yao, L., Zhang, B. & Chen, C. 2016. Guest Editorial Smart Grid Technologies and Development in China. *IEEE Transactions on Smart Grid*, 7(1): 379–380. http://ieeexplore.ieee.org/document/7361698/.

Wen, S., Chen, J., Wu, Y., Yan, Z., Cao, Y., Yang, Y. & Huang, T. 2021. CKFO: Convolution Kernel First Operated Algorithm With Applications in Memristor-Based Convolutional Neural Network. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 40(8): 1640–1647. https://ieeexplore.ieee.org/document/9186619/.

Weranga, K., Kumarawadu, S. & Chandima, D.P. 2014. Evolution of Electricity Meters. In *Smart Metering Design and Applications*. SpringerBriefs in Applied Sciences and Technology. Singapore: Springer, Singapore: 17–38. https://link.springer.com/10.1007/978-981-4451-82-6.

Winther, T. 2012. Electricity theft as a relational issue: A comparative look at Zanzibar, Tanzania, and the Sunderban Islands, India. *Energy for Sustainable Development*, 16(1): 111–119. http://dx.doi.org/10.1016/j.esd.2011.11.002.

Wu, R., Wang, L. & Hu, T. 2018. AdaBoost-SVM for Electrical Theft Detection and GRNN for Stealing Time Periods Identification. In *IECON 2018 - 44th Annual Conference of the IEEE Industrial Electronics Society*. IEEE: 3073–3078. https://ieeexplore.ieee.org/document/8591459/.

Xia, R., Gao, Y., Zhu, Y., Gu, D. & Wang, J. 2023. An attention-based wide and deep CNN with dilated convolutions for detecting electricity theft considering imbalanced data. *Electric Power Systems Research*, 214(PA): 1–10. https://doi.org/10.1016/j.epsr.2022.108886.

Xia, X., Xiao, Y., Liang, W. & Cui, J. 2022. Detection Methods in Smart Meters for Electricity Thefts: A Survey. *Proceedings of the IEEE*, 110(2): 273–319. https://ieeexplore.ieee.org/document/9686052/.

Xiao, Z., Xiao, Y. & Du, D.H.-C. 2013. Exploring Malicious Meter Inspection in Neighborhood Area Smart Grids. *IEEE Transactions on Smart Grid*, 4(1): 214–226. http://ieeexplore.ieee.org/document/6397580/.

Xu, G., Liu, M., Jiang, Z., Söffker, D. & Shen, W. 2019. Bearing Fault Diagnosis Method Based on Deep Convolutional Neural Network and Random Forest Ensemble Learning. *Sensors*, 19(5): 1–21. https://www.mdpi.com/1424-8220/19/5/1088.

Yadav, H. 2022. Dropout in Neural Networks. *Towards Data Science*. https://towardsdatascience.com/dropout-in-neural-networks-47a162d621d9 2 October 2024.

Yakubu, O., Babu C., N. & Adjei, O. 2018. Electricity theft: Analysis of the underlying contributory factors in Ghana. *Energy Policy*, 123: 611–618. http://www.sciencedirect.com/science/article/pii/S0301421518306232.

Yan, Z. & Wen, H. 2021. Electricity Theft Detection Base on Extreme Gradient Boosting in AMI. *IEEE Transactions on Instrumentation and Measurement*, 70: 1–9. https://ieeexplore.ieee.org/document/9312127/.

Yan, Z. & Wen, H. 2022. Performance Analysis of Electricity Theft Detection for the Smart Grid: An Overview. *IEEE Transactions on Instrumentation and Measurement*, 71: 1–28. https://ieeexplore.ieee.org/document/9612408/.

Yang, K., Chen, W., Bi, J., Wang, M. & Luo, F. 2023. Multi-view broad learning system for electricity theft detection. *Applied Energy*, 352(September): 1–9. https://doi.org/10.1016/j.apenergy.2023.121914.

Yang, X.-S. 2019. Neural networks and deep learning. In *Introduction to Algorithms for Data Mining and Machine Learning*. Elsevier: 139–161. https://linkinghub.elsevier.com/retrieve/pii/B9780128172162000156.

Yao, R., Wang, N., Ke, W., Chen, P. & Sheng, X. 2023. Electricity theft detection in unbalanced sample distribution: a novel approach including a mechanism of sample augmentation. *Applied Intelligence*, 53(9): 11162–11181. https://link.springer.com/10.1007/s10489-022-04069-z.

Yip, S.-C., Tan, C.-K., Tan, W.-N., Gan, M.-T. & Bakar, A.-H.A. 2017. Energy theft and defective meters detection in AMI using linear regression. In *2017 IEEE International Conference on Environment and Electrical Engineering and 2017 IEEE Industrial and Commercial Power Systems Europe (EEEIC / I&CPS Europe)*. IEEE: 1–6. http://ieeexplore.ieee.org/document/7977752/.

Yip, S.-C., Tan, W.-N., Tan, C., Gan, M.-T. & Wong, K. 2018. An anomaly detection framework for identifying energy theft and defective meters in smart grids. *International Journal of Electrical Power & Energy Systems*, 101(July 2017): 189–203. https://doi.org/10.1016/j.ijepes.2018.03.025.

Yip, S.-C., Wong, K., Hew, W.-P., Gan, M.-T., Phan, R.C.W. & Tan, S.-W. 2017. Detection of energy theft and defective smart meters in smart grids using linear regression. *International Journal of Electrical Power & Energy Systems*, 91: 230–240. http://dx.doi.org/10.1016/j.ijepes.2017.04.005.

Bin Yousuf, S., Jamil, M., Zia ur Rehman, M., Hassan, A. & Gilani, S.O. 2016. Prototype Development to Detect Electric Theft using PIC18F452 Microcontroller. *Indian Journal of Science and Technology*, 9(46): 1–5. https://indjst.org/articles/prototype-development-to-detect-electric-theft-using-pic18f452-microcontroller.

Yu, Y., Qiu, Z., Liao, H., Wei, Z., Zhu, X. & Zhou, Z. 2022. A Method Based on Multi-Network Feature Fusion and Random Forest for Foreign Objects Detection on Transmission Lines. *Applied Sciences*, 12(10): 4982. https://www.mdpi.com/2076-3417/12/10/4982.

Yurtseven, Ç. 2015. The causes of electricity theft: An econometric analysis of the case of Turkey. *Utilities Policy*, 37(2): 70–78. https://linkinghub.elsevier.com/retrieve/pii/S0957178715000429.

Zaitsu, T., Tran, N.H., Kawanishi, M. & Narikiyo, T. 2018. Advanced SVR control by PSO to handle over-voltage. In *The 61st Joint Conference on Automatic Control*. Nagoya: 352–355. https://doi.org/10.11511/jacc.61.0_352.

Zhang, A., Lipton, Z.C., Li, M. & Smola, A.J. 2021. *Dive into Deep Learning*.

Zhang, C., Wang, Z., Liu, L., Li, G. & Li, H. 2023. Electricity-Theft Detection Based on Optimized Deep Learning Model in Smart Grid. In *2023 6th International Conference on Energy, Electrical and Power Engineering (CEEPE)*. IEEE: 1494–1499. https://ieeexplore.ieee.org/document/10166884/.

Zhang, Q., Dong, Y., Hao, M., Yang, Y., Wang, X., Bao, Y. & Sun, J. 2023. Self-attentive mechanism model-based anomaly detectionmethodforbig data of electricity users. In S. Patnaik & T. Shen, eds. *Seventh International Conference on Mechatronics and Intelligent Robotics (ICMIR 2023)*. SPIE: 1–9. https://www.spiedigitallibrary.org/conference-proceedings-of-spie/12779/2689888/Self-attentive-mechanism-model-based-anomaly-detectionmethodforbig-data-of-electricity/10.1117/12.2689888.full.

Zheng, Z., Yang, Y., Niu, X., Dai, H.-N. & Zhou, Y. 2018. Wide and Deep Convolutional Neural Networks for Electricity-Theft Detection to Secure Smart Grids. *IEEE Transactions on Industrial Informatics*, 14(4): 1606–1615. https://ieeexplore.ieee.org/document/8233155/.

Zhou, K., Yang, C. & Shen, J. 2017. Discovering residential electricity consumption patterns through smart-meter data mining: A case study from China. *Utilities Policy*, 44: 73–84. http://dx.doi.org/10.1016/j.jup.2017.01.004.

Zhu, L., Wen, W., Li, J., Zhang, C., Zhou, B. & Shuai, Z. 2024. Deep Active Learning-Enabled Cost-Effective Electricity Theft Detection in Smart Grids. *IEEE Transactions on Industrial Informatics*, 20(1): 256–268. https://ieeexplore.ieee.org/document/10080868/.

Zhu, S., Xue, Z. & Li, Y. 2024. Electricity Theft Detection in Smart Grids Based on Omni-Scale CNN and AutoXGB. *IEEE Access*, 12(January): 15477–15492. https://ieeexplore.ieee.org/document/10414103/.

Zhu, Y., Wang, M., Yin, X., Zhang, J., Meijering, E. & Hu, J. 2022. Deep Learning in Diverse Intelligent Sensor Based Systems. *Sensors*, 23(1): 1–86. https://www.mdpi.com/1424-8220/23/1/62.

APPENDIX

The Appendix contains the codes used in the implementation of the algorithms to develop the proposed electricity-theft (ET) or non-technical losses (NTL) detection model which its theoretical modelling approach has already been presented in Chapter 3. The artificial intelligence-based (AI-based) machine learning (ML) simulations for the NTL detection (NTLD) model is carried out using Python in Google Colaboratory (Colab) Integrated Development Environment (IDE). Only the implementation codes used in developing the proposed model has been explicitly presented here, but the code outputs or results have not been presented. The Python implementation codes could then be run (by anyone who intends to authenticate the veracity of this work) on any Python IDE to obtain their corresponding outputs. The dataset used in the development of the NTLD model is from the State Grid Corporation of China (SGCC). SGCC is a Smart Grid (SG) electric system, while the dataset used in building the proposed model is thus a SG data which has been obtained from the smart meters (SMs) of the represented electric customers.

The hybrid of CNN and RF models termed as CNN-RF has been proposed in this thesis to enhance or optimize electricity-theft detection (ETD). The model hybridization combines the strengths of both convolutional neural network (CNN) and random forest (RF) models, in a bid to improve the individual performances of the constituting models. Model performance improvement tends to increase the efficacy and efficiency of utility onsite mitigation efforts, which further reduces NTL in the power grids to the barest minimum. Although CNN-RF is the proposed model, the constituent models (CNN and RF) that make up the hybrid model have also been tested individually to determine their viabilities before later combining them to get better results.

The Python codes used in executing the CNN, RF, and the proposed CNN-RF models are contained from Sections A.1.1 to A.1.8 of the implementation codes. The comprehensive implementation codes reveal details of the ML algorithms executed to construct the ETD-based ML models. Comments are added to the codes, while some other explanations are also infused within the codes to shed more light on the functions of the Python codes. Also, the codes have been broken into several sections to aid easier understanding of the different steps taken to arrive at the developed models. The inclusion of the implementation codes used in constructing the models is important to convey the originality of the research.

Python implementation codes

A.1.1 Libraries import

```
import pandas as pd
import numpy as np
import seaborn as sns
import matplotlib.pyplot as plt
import math
import statistics
import imblearn
import plotly.express as px
from imblearn.over_sampling import SMOTE
from sklearn.preprocessing import StandardScaler, MinMaxScaler
from sklearn.ensemble import RandomForestClassifier
from sklearn.model_selection import train_test_split
from sklearn.metrics import classification_report, accuracy_score
from sklearn.metrics import confusion_matrix
from sklearn.metrics import f1_score
from sklearn.metrics import (auc, confusion_matrix,
precision_recall_curve, precision_score, recall_score, roc_auc_score,
roc_curve)
!pip install plot-metric
from plot_metric.functions import BinaryClassification

from sklearn.model_selection import train_test_split
from sklearn.metrics import accuracy_score
from matplotlib import pyplot
import matplotlib.pyplot as plt
import matplotlib.pyplot as plot
import pandas as pd
import numpy as np

from keras.models import Sequential
from keras.layers import Dense
from keras.layers import Dropout
from keras.layers import Conv1D
from keras.layers import Flatten
import tensorflow as tf
import tensorflow.compat.v1 as tf
tf.disable_v2_behavior()
from numpy import loadtxt
import keras
from tensorflow.keras import Sequential
from tensorflow.keras.layers import Conv2D, MaxPooling2D, Dense,
Activation, Dropout, Flatten, BatchNormalization
from tensorflow.keras.optimizers import Adam, RMSprop, SGD
from tensorflow.keras import Model
from tensorflow.keras.callbacks import
ModelCheckpoint,EarlyStopping,CSVLogger,
LearningRateScheduler,ReduceLROnPlateau
from tensorflow.keras.metrics import binary_crossentropy, TruePositives,
TrueNegatives, FalsePositives, FalseNegatives, BinaryAccuracy, Precision,
Recall, AUC
from tensorflow. keras.utils import plot_model
from tabulate import tabulate
```

There are several modules in Python from which libraries are imported to the IDE. To start a machine learning project, a good grasp of the model or algorithms remains a vital source to getting better predictions or decisions. Some libraries are a straight-away picks from the Python IDE for any researcher starting a new project. However, choosing the correct set of algorithms for the new project may be quite tasking. The libraries that are imported is divided into the following categories: model creation (TensorFlow, Keras and PyTorch), data preprocessing (pandas, NumPy, SimplerImputer, SMOTE, etc.), hyperparameter tuning (RandomSearchCV, GridSearchCV), experiment tracking (weight, biases), problem specific (OpenCV, Geopandas, imutils), and utils (matplotlib, seaborn).

Pandas is a Python package that is used mainly for DataFrame manipulations. NumPy is a Python package mainly used for mathematical operations like reshaping of array, expansion of the dimensions of array, etc. Seaborn is a package that is built on top of matplotlib module, and is mainly used for better data visualizations. Matplotlib is a visualization module like seaborn, but its output is not as appealing as that of seaborn. Math module is used for mathematical functions. Imblearn is a Python module where undersampling and oversampling techniques like SMOTE reside. SimpleInputer is a library that resides in sklearn which is used mainly for replacing missing values in DataFrame with either mean, median or the most frequent values, etc. StandardScaler is used to scale DataFrame down to values between -1 and 1, while MinMaxScaler scales DataFrame down to values between 0 and 1.

The command `train_test_split` is used to split data into train and test data. Test data is kept aside and unexposed during training for effective modelling. `classification_report` is used to give detailed report of performance metrics like precision, recall, F1 score and accuracy of the train data. `accuracy_score` also resides in the `classification_report` and gives how accurately our model performs. `Confusion_matrix` summarizes true positive (TP), true negative (TN), false positive (FP), and false negative (FN) in a graphical form. It states how many of the responses that our model classifies accurately as positives and negatives, and how many are misclassified as positives and negatives.

As the name implies, `Sequential` model consists of sequence of layers one after the other. `Dense` layer is a neural network that is deeply connected, meaning that each neuron in the dense layer is connected to more than one neuron in the preceding layer. `Dropout` is easily implemented by randomly selecting nodes to be dropped out with a given probability (e.g., 20%) in each weight update cycle.

This function `import tensorflow.compat.v1 as tf tf.disable_v2_behavior()` can be called at the beginning of the program (before creating Tensors, Graphs, or other structures and before devices are being initialized. It switches all global behaviours that are different between TensorFlow 1.x and 2.x to behave as intended for 1.x. The `Conv1D` is used to create convolutional layer. It is used to apply 1D convolution to the input data. `Flatten` layer in Keras reshapes the tensor to have a shape that is equal to the number of elements contained in the tensor. `Adam, RMSprop` and `SGD` are optimizers to reduce loss and improve training speeds. The `Model` provides a straightforward, user-friendly method for defining a neural network, which TensorFlow will subsequently construct.

A.1.2 Exploratory data analysis and data preprocessing

A.1.2.1 Importing dataset from Google Drive to Google Colab IDE

```
from google.colab import drive #Import
drive.mount('/content/gdrive')
```

A.1.2.2 Link the dataset residing in Google Drive to Google Colab

```
!gdown  --id 1pTpBfO1CwStFodOtIn_uzzNOWpAmQn_8
```

Downloading the SGCC dataset residing in the Google Drive to Google Colab using the above Google-Drive link attributed to the dataset. The link is automatically generated in Google Drive and other Google users could also be given authorized access to the dataset via the link.

A.1.2.3 Reading in the dataset into Google Colab using pandas read_csv

```
df = pd.read_csv('data.csv')
```

With the aid of pandas and its method like `read_csv(), read_sql()`,and `read_json()` any data of these extensions can be read and displayed. Since the dataset used in this research is a CSV type, `read_csv()` has been used to read this file. This module allows researchers to retrieve data in the form of a DataFrame.

A.1.2.3.1 Determining the proportion of unique values in the dataset

```
num_Flagged = df[df['FLAG'] == 1].shape[0]
num_unflagged = df[df['FLAG'] == 0].shape[0]
```

```
num_Flagged
```

```
num_unflagged
```

```
#Print % proportion of flagged and unflagged customers in the whole data
print(num_Flagged / (num_Flagged + num_unflagged) * 100, '% of customers flagged.')

print(num_unflagged / (num_Flagged + num_unflagged) * 100, '% of customers unflagged.')
```

```
#Print proportion of flagged and unflagged customers in the whole dataset
print(f'{num_Flagged} customers flagged.')

print(f'{num_unflagged} customers unflagged.')
```

A.1.2.3.2 Visualizing the proportion of unique values in a bar and a pie chart

```
#Count proportion of unique values (flagged and unflagged customers) in the whole dataset in a bar chart
```

```
import numpy as np
import matplotlib.pyplot as plt

y = df['FLAG']
unique, counts = np.unique(y, return_counts=True)
positions = np.arange(len(unique))

# Create the bar chart with labels
plt.bar(positions, counts, label='Counts')
plt.xticks(positions, unique)
plt.xlabel('Unique Values')
plt.ylabel('Counts')
plt.title('Bar Chart of Unique Values')


# Create a legend

plt.legend()
plt.show()
```

```
#Percentage proportion of the flagged and unflagged customers in the whole dataset in a pie chart

df["FLAG"].value_counts().plot(kind = 'pie',explode=[0, 0.1],figsize=(6, 6),autopct='%1.1f%%',shadow=True)
```

```
plt.title("Fraudulent and Non-Fraudulent Distribution",fontsize=20)
plt.legend(["unflagged", "Flagged"])
plt.show()
```

`value_counts()` method of pandas is used to check how many unique values (0 and 1) in the column of FLAG in the DataFrame. `explode=[0, 0.1]` allows the pie chart to be sliced into appropriate portions, `autopct='%1.1f%%` allows display of percentage (%) which is rounded off to one decimal place in the pie chart. `shadow=True` allows graphic shadow in the pie chart.

A.1.2.4 Checking the first ten rows of the DataFrame (df)

```
df.head(10)
```

A.1.2.5 Build a function that checks for the missing values in the DataFrame (df)

```
def missing_data_all(df): #This function is to find missing data in the DataFrame
    total = df.isnull().sum().sort_values(ascending=False) #sums any field whose data is missing to arrive at their total
    percent = 
(df.isnull().sum()/df.isnull().count()).sort_values(ascending=False) #to determine the percentage of the missing or null values in each column
    missing_data = pd.concat([total, percent], axis=1, keys=['Total', 'Percent']) #Create a DataFrame to put side by side the total missing values and the percentage of missing values for each column
    return missing_data #Return the result as the DataFrame created in missing data above
```

```
#Checking the missing data

missing_data_all(df)
```

A.1.2.6 Append other columns except for “CONS_NO”, and “FLAG” columns into lb list

```
l=df.columns # Check all columns in df and store them in l
la=['CONS_NO','FLAG'] # Store subsets of the columns, ‘CONS_NO’, ‘FLAG’ as a list in la
lb=[]  # Create an empty list called lb
for i in l: # Loop through every member of l above
    if i not in la: # Check if those elements in df are not in la
```

```
        lb.append(i) # Put those elements not in la in the empty list lb,
meaning that all dates in the df will be stored in lb except ‘CONS_NO’ and
‘FLAG’
```

A.1.2.6.1 Checking if the values in the rows and columns are still intact

```
#Check if item in row 0 and column 2 is having a null value

math.isnan(df.iloc[0][2])
```

A.1.2.7 Format date in year/month/day for all columns and store in fdatesdates list

```
import datetime #Import datetime module to modify dates
dates = [datetime.datetime.strptime(ts, "%Y/%m/%d") for ts in lb]
#Convert string date to datetime format and then store results in dates
#dates.sort()
fdatesdates = [datetime.datetime.strftime(ts, "%Y/%m/%d") for ts in dates]
#Using list comprehension, loop through the lb list created above to
modify date to the format of year/month/day and store results in
fdatesdates
```

A.1.2.8 Insert “0” in all rows of the columns CONS_NO and FLAG

```
fdatesdates.insert(0,"CONS_NO") #In fdatesdates, insert CONS_NO into
position 0
fdatesdates.insert(0,"FLAG")#In fdatesdates, insert FLAG into position 0
df.columns=fdatesdates #Replace all coulumns in df with new formatted
columns called fdatesdates
```

A.1.2.9 Sort dates in ascending order

```
import datetime
dates = [datetime.datetime.strptime(ts, "%Y/%m/%d") for ts in lb]
dates.sort()
sorteddates = [datetime.datetime.strftime(ts, "%Y/%m/%d") for ts in dates]
#Change fdatesdates to sorteddates for easy identification of variable name
```

A.1.2.10 Concatenate sorted dates and the columns CONS_NO and FLAG

```
cols=df.columns.tolist()[0:2]+sorteddates #Join columns 0 and 1 to
sorteddates. df.columns.tolist()[0:2] means columns located in position 0
and 1, i.e., columns CONS_NO and FLAG. sorteddates are the dates on the df
columns

df=df[cols] #Create a formatted DataFrame still named df with sorted dates
```

A.1.2.11 Fill all columns with their respective observations

```
train_df=df #Create a version of df named train_df
l=train_df["2014/01/01"] #Subset “2014/01/01” column of the df and save in
l
l1=train_df["2014/01/01"] #Subset “2014/01/01” column of the df and save
in l1
l=np.asarray(l).tolist()#Convert the l into NumPy array and then to a list
l1=np.asarray(l1).tolist #Convert the l1 into NumPy array and then to a
list
l2=[] #Create an empty list and name it l2
for i in range(len(l)): () #Loop through the length of l list

    if math.isnan(l[i]): #Is there any missing member in l list?
        if math.isnan(l1[i]): #Is there any missing member in l1 list?
            l2.append(0) #Insert 0 if there is a missing number
        else:
            l2.append(l1[i]/2) #If there is no missing number insert
number /2
    else:
        l2.append(l[i]) #Insert number available in the field
train_df["2014/01/01"]=l2  #Subset “2014/01/01” column of the train_df and
save in l2

train_df.head() #Display the first five rows of the new train_df
l=train_df["2016/10/31"]
l1=train_df["2016/10/31"]
l=np.asarray(l).tolist()
l1=np.asarray(l1).tolist()

l2=[]
for i in range(len(l)):
    if math.isnan(l[i]):
        if math.isnan(l1[i]):
            l2.append(0)
        else:
            l2.append(l1[i]/2)
    else:
        l2.append(l[i])
train_df["2016/10/31"]=l2
l=train_df.columns
la=['CONS_NO','FLAG']
lbx=[]
for i in l:
    if i not in la:
        lbx.append(i)
```

A.1.2.12 Using interpolation method to replace NaNs or missing values

```
df_1=df.interpolate(method ='linear', limit_direction ='forward') #Use
interpolation method of pandas to fill up NaN using two previous non-
missing values in a row in a forward direction
```

```
df_1=df.interpolate(method ='linear', limit_direction ='backward') #Use
interpolation method of pandas to fill up NaN using two previous non-
missing values in a row in a backward direction
```

NaN is an abbreviation for “not a number”, which is also known as a missing value. Note that if two previous values in a row in either forward or backward direction are not available, NaN will still be inserted in the field.

A.1.2.12.1 Checking the values replaced by interpolation

```
df_1.head()
```

A.1.2.12.2 Checking if there are still missing values in the DataFrame after interpolation

```
def missing_data_all(df):
    overall = df.isnull().sum().sort_values(ascending=False)
    percentage =
(df.isnull().sum()/df.isnull().count()).sort_values(ascending=False)
    missing_data = pd.concat([overall, percentage], axis=1,
keys=['Overall', 'Percentage'])
    return missing_data
missing_data_all(df_1)
```

Like the function used for missing values in Section A.1.2.5, this function determines the overall number of missing values and the percentage of missing values in `df_1`

A.1.2.12.3 Checking the independent features for missing values

```
X = df_1.drop(['CONS_NO', 'FLAG'], axis = 1) #Filter features or
predictors for all rows and columns for all dates but drop CONS_NO and
FLAG columns
```

```
Y = df_1.iloc[:, 1]#Select only FLAG as the target. FLAG is in column 1

pd.DataFrame(X)
```

A.1.2.13 Checking the dependent (target) features (FLAG column) for missing values

```
Y
```

A.1.2.14 Using MinMaxScaler to scale down the independent features from 0 to 1

```
scaler = MinMaxScaler()#Create an instance of MinMaxScaler called scaler
X = scaler.fit_transform(X) #Fit, train and transform the features and
store transformed X in X
print(X)  #Print all scaled features
```

A.1.2.14.1 Checking if the independent features have been scaled

```
pd.DataFrame(X)
```

A.1.2.14.2 Checking the first-row array of the scaled independent features

```
print(X[0,:1034])
```

A.1.2.15 Using SMOTE technique to oversample the minority class

```
ros = SMOTE(random_state= 42) #Create an instance of SMOTE to resample the
training data. Random_state can be any integer that functions for
reproducibility of resampled data.
X, Y = ros.fit_resample(X, Y.ravel()) #Resample X and y using SMOTE object
created above
```

A.1.2.15.1 Splitting the oversampled data into train data and test data

```
x_train, x_test, y_train, y_test=train_test_split(X, Y, test_size=0.3,
random_state = 42) #Split the resampled features and target using
train_test_split module to split data features X and target Y into
x_train, x_test, y_train, y_test using 30% of X as test data
```

The command `train_test_split` is used to split the SGCC dataset into train and test sets. Firstly, the dataset is separated into features `(X)` and labels (`y)`. The DataFrame gets divided into `x_train, x_test, y_train, y_test.` The `x_train, y_train` sets which are used for training and fitting the model.

A.1.2.15.2 Convert oversampled y_train any y_test into numpy array

```
#Convert y_train and y_test into NumPy array
y_train = np.array(y_train)
y_test = np.array(y_test)
```

A.1.2.15.3 Expand the dimension of X_train, X_test

```
#Expand the dimensions of x_train, x_test and insert the extended
dimension in the axis =2, i.e., adding 1 to the third position of both
x_train and x_test shapes
```

```
x_train = np.expand_dims(x_train, axis=2)
x_test = np.expand_dims(x_test, axis=2)
input_shape=x_train.shape[1] #input_shape takes the value of the column of
x_train for CNN model
```

```
x_train.shape[1] #to extract column array but x_train.shape[0] is to
extract the row array
```

```
x_train.shape
```

A.1.3 Development of the Conv1D model with 32 neurons at the input layer

```
model_cnn= Sequential() #Create a sequential array named model_cnn
```

```

model_cnn.add(Conv1D(32, kernel_size=(3), activation='relu',
padding='same' ,input_shape=(x_train.shape[1],1))) #Add Conv1D layer with
32 neurons, filter or kernel size of 3, activation function of relu which
converts weight<= 0 to 0 and weight > 0 to 1

model_cnn.add(MaxPooling1D(pool_size= 2, strides=2) #To reduce the
dimension of the feature maps

model_cnn.add(Flatten())#Convert the Conv1D layer into a single vector
array – 1 Dimension

m = model_cnn.output #Store output of the model in m

m = Dense(64, activation = 'relu', kernel_initializer = 'he_uniform')(m)
#Create a dense layer with 64 neurons
m = Dropout(0.4)(m) #Apply Dropout

prediction_layer = Dense(1,activation= 'sigmoid')(m) #The final prediction
layer or output layer with one neuron that displays classification between
fraudulent and non-fraudulent electricity customer

model_cnn_1 = Model(outputs = prediction_layer, inputs = model_cnn.input)
#Using keras model that enshrouds both outputs and inputs of the model
#model_cnn.add(Dense(1,activation= 'sigmoid'))
model_cnn_1.compile(optimizer = 'adam', loss='binary_crossentropy',
metrics=['accuracy']) #Compile model using optimizer adam for easy
convergence; binary_crossentropy as loss metric because we have binary
classification problem to predict.
```

```
model_cnn_1.summary() #Displays both number of trainable and non-trainable
parameters of the network.
```

input_shape is (1034,1), 40% of the neurons are dropped (dropout), hidden layer has a dense layer of 64 neurons.

A.1.3.1 Training the CNN model with 70% train data and 30% validation data

```
history = model_cnn_1.fit(x_train, y_train, epochs=50, batch_size=30,
verbose=0,validation_split=0.3) #Train the model with 70% of X and y with
backward and forward propagations of 50 times. Each batch of the training
data =30, and validate the model with 30% of the data
```

A.1.3.2 Make prediction using X_test

```
cnn_prediction=model_cnn_1.predict(x_test); #Making prediction with test
data that has been kept aside
```

```
resampled_prediction = cnn_prediction #Save the prediction list in a
variable name resampled_prediction
```

```
resampled_prediction.shape #Check the shape of the resampled_prediction.
```

A.1.3.3 Plot confusion matrix for the CNN model

```
labels = sorted(list(set(y_test))) #Create a sorted list of y_test and
name it labels.
cmx_data = confusion_matrix(y_test, resampled_prediction.round(),
labels=labels) #Compare y_test and CNN predicted values list using
confusion matrix package of sklearn.
df_cmx = pd.DataFrame(cmx_data, index=labels, columns=labels) #Create a
DataFrame of the result of the the confusion matrix using index as labels
(0,1) and columns (0,1) as labels as well in both x and y axes.
plt.figure(figsize = (10,7)) #Size of the plot: x-axis = 10, y-axis =.7
colormap = sns.color_palette("Blues")#Using seaborn colour blue.
sns.heatmap(df_cmx, annot=True, cmap = colormap) #Using seaborn to plot
heatmap of the DataFrame of the confusion matrix. annot=True is to insert
integers into the four cells of the confusion matrix. Colormap as
arguments
plt.show() #Display the plot
```

A.1.3.4 Determining precision and recall values for CNN model and plotting PRC

```
thresholds = 0.5
#calculate precision and recall
```

```
precision, recall, thresholds = precision_recall_curve(y_test,
resampled_prediction)
print(f'Precision: {precision}\nRecall: {recall}\nThresholds:
{thresholds}')

auc_precision_recall = auc(recall, precision)
print(auc_precision_recall)

#create precision-recall curve (PRC)
fig, ax = plt.subplots()
ax.plot(recall, precision, color='purple')

#add axis labels to plot
ax.set_title('Precision-Recall Curve')
ax.set_ylabel('Precision')
ax.set_xlabel('Recall')

#display plot
plt.show()
```

A.1.3.5 Plotting the receiver operating characteristic (ROC) curve

```
fpr, tpr, _ = roc_curve(y_test,  resampled_prediction)
```

```
#create ROC curve
plt.plot(fpr,tpr)
plt.ylabel('True Positive Rate')
plt.xlabel('False Positive Rate')
plt.title('Receiver operating characteristic curve')
plt.show()
```

A.1.3.6 Determining the values of TPR and FPR and visualizing their ROC plot

```
#Determining the values of true positive rate (TPR) and false positive
rate (FPR)
```

```
from scipy import interpolate
```

```
fpr, tpr, thresholds = roc_curve(y_test, resampled_prediction)
tpr_intrp = interpolate.interp1d(thresholds, tpr)
fpr_intrp= interpolate.interp1d(thresholds, fpr)

print(f'TPR of CNN model : {tpr_intrp(0.5)}')
print(f'FPR of CNN model : {fpr_intrp(0.5)}')

# Visualisation with plot_metric
fpr, tpr, thresholds = roc_curve(y_test, resampled_prediction)
#print(f'CNN FPR: {fpr}\nTPR:{tpr}\nThresholds:{thresholds}')
auc_value = auc(fpr,tpr)
```

```
print(f'AUC score for CNN is:   {auc_value}')

bc = BinaryClassification(y_test, resampled_prediction, labels=[1, 0])

# Figures
plt.figure(figsize=(10,8))
bc.plot_roc_curve()
plt.show()
```

A.1.3.7 Printing classification report

```
threshold=0.5
for i in range(0,len(resampled_prediction)):

    if  resampled_prediction[i] > threshold:
        resampled_prediction[i] = 1
    else:
        resampled_prediction[i] = 0
print(classification_report(y_test, resampled_prediction))
```

A.1.3.8 Visualize accuracy in the training data

```
#Visualize accuracy in training data
plt.figure(figsize = (12, 10)) #Creating size of the figure to plot x-axis =12, y-axis = 10
plt.plot(history.history['acc']) #Subset accuracy (acc) from history in Section 1.3.1 above
plt.plot(history.history['val_acc']) #Subset validation accuracy (val_acc) from history in Section 1.3.1 above
plt.title('CNN Model accuracy')
plt.ylabel('accuracy')
plt.xlabel('epoch')
plt.legend(['Training data', 'Validation data'], loc = 'lower right')
```

A.1.3.9 Visualize loss in the training data

```
#Visualize loss in training data
plt.figure(figsize = (12, 10))
plt.plot(history.history['loss'])
plt.plot(history.history['val_loss'])
plt.title('CNN Model Loss')
plt.ylabel('loss')
plt.xlabel('epoch')
plt.legend(['Training data', 'Validation data'], loc = 'upper right')
```

A.1.4 Using backend package from Keras to extract some training data from CNN layers

```
from keras import backend as K
```

```
for l in range(len(model_cnn_1.layers)):
    print(l, model_cnn_1.layers[l])
```

A.1.4.1 Check features in the first (input) layer of CNN network

```
model_cnn_1.layers[0].input
```

A.1.4.2 Find features from Conv1D layer to later use to train the standalone random forest (RF) model

```
#Using backend to find features from CNN model to train RF model
```

```
findFeature = K.function([model_cnn.layers[0].input, K.learning_phase()],
[model_cnn.layers[1].output])
```

A.1.4.3 Extract samples as train and test data from CNN layers

```
train_example4000 = findFeature([x_train[:4000], 0])[0] #Extract 4000
samples as train data
```

```

test_example1500 = findFeature([x_test[:1500], 0])[0] #Extract 1500
samples as test data
```

A.1.4.4 Convert 3-D array for CNN model back to 2-D for RF model

```
y_train4000 = y_train[:4000].reshape(y_train[:4000].shape[0],)#Reshape y
as a vector of only 1 column
```

```
y_test1500 = y_test[:1500]
#Using reshape function, 3-D has changed to 2-D
```

```
train_example4000.shape #Check number of rows and columns in
train_example4000
```

A.1.4.5 Check shapes of all train and test data extracted from CNN layers

```
print(train_example4000.shape, test_example1500.shape, y_train4000.shape,
y_test1500.shape) #Check the rows and columns in the train and test data.
```

A.1.5 Instantiate RF model and train with features from CNN layers

```
from sklearn.ensemble import RandomForestClassifier
```

```
rf = RandomForestClassifier(n_estimators= 50, random_state= 42)
#Instantiate RF with the number of estimators, random_state or seed for
reproducibility as arguments.
rf.fit(train_example4000, y_train4000) #Train the data on the object of RF
```

A.1.5.1 Check the performance of standalone RF model using test data from CNN layers

```
y_test_rf = rf.predict(test_example1500) #Making prediction with the test
data kept aside
```

```
from sklearn.metrics import confusion_matrix, classification_report,
accuracy_score #Import evaluation metrics to observe performance of the RF
model

print(classification_report(y_test1500, y_test_rf)) #Print classification
report
print("Accuracy: {0}".format(accuracy_score(y_test1500, y_test_rf)))
#Print the accuracy score of the RF model
```

A.1.5.2 Plot the confusion matrix for the RF model

```
labels = sorted(list(set(y_test)))
```

```
cmx_data = confusion_matrix(y_test1500, y_test_rf, labels=labels)

df_cmx = pd.DataFrame(cmx_data, index=labels, columns=labels)
plt.figure(figsize = (10,7))
colormap = sns.color_palette("Blues")
sns.heatmap(df_cmx, annot=True, cmap = colormap)
plt.show()
```

A.1.5.3 Determine the values of TPR and FPR for RF model

```
from scipy import interpolate
```

```
fpr, tpr, thresholds = roc_curve(y_test1500, y_test_rf)
tpr_intrp = interpolate.interp1d(thresholds, tpr)
fpr_intrp= interpolate.interp1d(thresholds, fpr)

print(f'TPR of RF model : {tpr_intrp(0.5)}')
print(f'FPR of RF model : {fpr_intrp(0.5)}')
```

A.,1.5.4 Plot the precision-recall curve (PRC) for RF model

```
thresholds = 0.5
```

```
#calculate precision and recall
precision, recall, thresholds = precision_recall_curve(y_test1500,
y_test_rf)
```

```
print(f'Precision: {precision}\nRecall: {recall}\nThresholds:
{thresholds}')

#create precision recall curve
fig, ax = plt.subplots()
ax.plot(recall, precision, color='purple')
#add axis labels to plot
ax.set_title('Precision-Recall Curve OF RF')
ax.set_ylabel('Precision')
ax.set_xlabel('Recall')

plt.show()#display plot
```

A.1.5.5 Plot the receiver operating characteristic curve (ROC) for the RF model

```
# Visualisation with plot_metric
```

```
false_positive_rate, true_positive_rate, _ = roc_curve(y_test1500,
y_test_rf)
print(f'false_positive_rate: {false_positive_rate}\ntrue_positive_rate:
{true_positive_rate}')

pr, tpr, thresholds = roc_curve(y_test1500, y_test_rf)
tpr_intrp = interpolate.interp1d(thresholds, tpr)
fpr_intrp= interpolate.interp1d(thresholds, fpr)
print(f'TPR of RF model : {tpr_intrp(0.5)}')
print(f'FPR of RF model : {fpr_intrp(0.5)}')

bc = BinaryClassification(y_test1500, y_test_rf, labels=[1, 0])

# Figures
plt.figure(figsize=(10,8))
bc.plot_roc_curve()
plt.show()
```

A.1.5.6 Printing performance scores for the RF model

```
from sklearn.metrics import auc
```

```
print("roc_auc score is :  ",roc_auc_score(y_test1500, y_test_rf))

f1 = f1_score(y_test1500, y_test_rf)
print("f1 score is :  ",f1)

precision, recall, thresholds = precision_recall_curve(y_test1500,
y_test_rf)
print("precision-recall curve array is :  ",
precision_recall_curve(y_test1500, y_test_rf))
auc = auc(recall, precision)
```

```
print("precision-recall AUC score of RF is :  ", auc)
```

A.1.5.7 Checking the shape of the test set for the RF model

```
y_test_rf.shape #Checking the shape of the RF model prediction
```

A.1.6 Infusion of the extracted CNN features into RF model to form hybrid CNN-RF model

```
#Using y_test extracted from the flatten layer of the CNN model to train
and test the RF model to form the hybrid CNN-RF model.

y_test=y_test1500 #Using 1500 data samples for testing
```

```
resampled_prediction=y_test_rf #Let the resampled prediction equal
predictions from RF model
```

A.1.6.1 Plot the confusion matrix of the new hybrid CNN-RF model

```
labels = sorted(list(set(y_test)))
```

```
cmx_data = confusion_matrix(y_test, resampled_prediction, labels=labels)
df_cmx = pd.DataFrame(cmx_data, index=labels, columns=labels)
plt.figure(figsize = (10,7))
colormap = sns.color_palette("Greens")
sns.heatmap(df_cmx, annot=True, cmap = colormap)
plt.show()
```

```
y_test=y_test1500

resampled_prediction=y_test_rf
```

```
resampled_prediction[:10]
```

A.1.6.2 Plotting the ROC curve for the CNN-RF model

```
# Visualisation with plot_metric
```

```
false_positive_rate, true_positive_rate, _ = roc_curve(y_test,
resampled_prediction)
print(f'false_positive_rate: {false_positive_rate}\ntrue_positive_rate:
{true_positive_rate}')

pr, tpr, thresholds = roc_curve(y_test, resampled_prediction)
tpr_intrp = interpolate.interp1d(thresholds, tpr)
fpr_intrp= interpolate.interp1d(thresholds, fpr)

print(f'TPR of CNN-RF model : {tpr_intrp(0.3)}')
print(f'FPR of CNN-RF model : {fpr_intrp(0.3)}')
bc = BinaryClassification(y_test, resampled_prediction, labels=[1, 0])
```

```
# Figures
plt.figure(figsize=(10,8))
bc.plot_roc_curve()
plt.show()
```

A.1.6.3 Checking the precision, recall and PRC curve for the CNN-RF model

```
matrix = confusion_matrix(y_test, resampled_prediction)
```

```
matrix = pd.DataFrame(matrix, index=["Actual Positive", "Actual
Negative"], columns = ["Predicted Positive", "Predicted Negative"])
print(tabulate(matrix, tablefmt="orgtbl", headers="keys"))
print()
#calculate precision and recall
precision, recall, thresholds = precision_recall_curve(y_test,
resampled_prediction)
print(f'Precision: {precision}\nRecall: {recall}\nThresholds:
{thresholds}') #Print precision and recall scores for the CNN-RF model

#create precision recall curve
fig, ax = plt.subplots()
ax.plot(recall, precision, color='purple')

#add axis labels to plot
ax.set_title('Precision-Recall Curve')
ax.set_ylabel('Precision')
ax.set_xlabel('Recall')

#display plot
plt.show()
```

```
#With threshold of 0.5, precision and recall are 1.0 and 0.98 respectively
for the positive class
threshold=0.5
for i in range(0,len(resampled_prediction)):

    if  resampled_prediction[i] > threshold:
        resampled_prediction[i] = 1
    else:
        resampled_prediction[i] = 0
print(classification_report(y_test, resampled_prediction))
```

A.1.6.4 More metric results for the CNN-RF model

```
from sklearn.metrics import confusion_matrix
```

```
from sklearn import metrics
cnn_prediction=resampled_prediction;
cm1 = confusion_matrix(y_test, cnn_prediction)
```

```
print('Confusion Matrix : \n', cm1)

total1=sum(sum(cm1))

accuracy1=(cm1[0,0]+cm1[1,1])/total1
print ('Accuracy : ', accuracy1)

sensitivity1 = cm1[0,0]/(cm1[0,0]+cm1[0,1])
print('Sensitivity : ', sensitivity1 )
specificity1 = cm1[1,1]/(cm1[1,0]+cm1[1,1])
print('Specificity : ', specificity1)
fpr, tpr, thresholds = metrics.roc_curve(y_test, cnn_prediction)
print("AUC",metrics.auc(fpr, tpr))
#More metric results
```

```
from sklearn.metrics import auc
print("roc_auc score is :  ",roc_auc_score(y_test, cnn_prediction))

f1 = f1_score(y_test, cnn_prediction)
print("f1 score is :  ",f1)

precision, recall, thresholds = precision_recall_curve(y_test,
cnn_prediction)

print("precision-recall curve array is :  ",
precision_recall_curve(y_test, cnn_prediction))

auc = auc(recall, precision)

print("precision-recall AUC score is :  ", auc)
```

A.1.7 Creation of a suspect list of fraudulent customers for the developed models

Creation of suspect list for the CNN model:

```
#Suspect list for CNN model
```

```
# Create a list of customers predicted to commit energy theft (CNN model)
cnn_theft_customers = np.where(resampled_prediction[:1500] == 1)[0]

# Retrieve the original customer IDs of the CNN theft customers
cnn_theft_customers_ids = df.iloc[cnn_theft_customers]['CONS_NO'].values

# Create a DataFrame from the list of CNN theft customer IDs
cnn_theft_customers_df = pd.DataFrame({
    'Customer_ID': cnn_theft_customers_ids,
    'Predicted_Theft': 1
})
```

```
# Display the DataFrame
print("Energy theft customers (CNN):")
print(cnn_theft_customers_df)
```

Creation of suspect list for the RF model:

```
#Suspect list for RF model
```

```
# Train and predict with the RF model
rf_model = RandomForestClassifier(n_estimators=50, random_state=42)
rf_model.fit(test_example1500, y_test[:1500])

rf_predictions = rf_model.predict(test_example1500)

# Create a list of customers predicted to commit energy theft (RF model)
rf_theft_customers = np.where(rf_predictions == 1)[0]

# Retrieve the original customer IDs of the RF theft customers
rf_theft_customers_ids = df.iloc[rf_theft_customers]['CONS_NO'].values

# Create a DataFrame from the list of RF theft customer IDs
rf_theft_customers_df = pd.DataFrame({
    'Customer_ID': rf_theft_customers_ids,
    'Predicted_Theft': 1
})

# Display the DataFrame
print("Energy theft customers (RF):")
print(rf_theft_customers_df)
```

Creation of suspect list for the CNN-RF model:

```
#Suspect list for CNN-RF model
```

```
import numpy as np
import pandas as pd
import joblib
# Load the combined CNN-RF model
cnn_rf_combined_model = joblib.load('models/cnn_rf_combined_model.pkl')

# Extract the RandomForest model from the combined model if necessary
# For standalone RandomForestClassifier
rf_model = cnn_rf_combined_model  # If it is just a RandomForestClassifier

# Number of features the model expects
n_features_rf = rf_model.n_features_in_
print("Number of features the model expects:", n_features_rf)
```

```
# Sample 800 rows from test_example1500
sampled_test_data =
test_example1500[np.random.choice(test_example1500.shape[0], 800,
replace=False)]

# Check the number of features in sampled_test_data
print("Number of features in sampled test data:",
sampled_test_data.shape[1])

# Adjust features if necessary
if sampled_test_data.shape[1] != n_features_rf:
    # Example: If the model expects 33121 features, you may need to adjust
the test data
    # This may involve adding or removing a feature
    # For example, if you need to add a feature, you could add a dummy
column
    # Assuming you need to add one feature:
    if sampled_test_data.shape[1] < n_features_rf:
        # Add dummy feature column (fill with zeros)
        additional_features = np.zeros((sampled_test_data.shape[0],
n_features_rf - sampled_test_data.shape[1]))
        sampled_test_data = np.hstack([sampled_test_data,
additional_features])
    else:
        raise ValueError(f"Test data has more features
({sampled_test_data.shape[1]}) than expected ({n_features_rf}).")

# Predict using the RandomForest model
rf_predictions = rf_model.predict(sampled_test_data)

# Create a DataFrame for the theft customers
theft_customers_indices = np.where(rf_predictions == 1)[0]

# Assuming df_1 has the Customer_ID column and is related to the test data
# Adjust indices according to actual data
CNN_RF_theft_customers_df = pd.DataFrame({
    'Customer_ID': df_1.iloc[np.random.choice(df_1.shape[0], 800,
replace=False)]['CONS_NO'].values[theft_customers_indices],
    'Predicted_Theft': 1
})
# Save the list as a CSV file
CNN_RF_theft_customers_df.to_csv('models/cnn_rf_theft_customers.csv',
index=False)

print("Energy theft customers predicted by the RF model:")
print(CNN_RF_theft_customers_df)
```

A.1.8 Saving the models using save function in Keras

```
import os
import joblib
from tensorflow.keras.models import save_model

# Create the 'model' directory if it doesn't exist
os.makedirs('model', exist_ok=True)

# Save model_cnn_1 (Keras model)
save_model(model_cnn_1, 'model/model_cnn_1.h5')

# Save RF (Random Forest model)
joblib.dump(rf, 'model/rf.pkl')

# Save the combined CNN-RF model
joblib.dump(cnn_rf_combined_model, 'models/cnn_rf_combined_model.pkl')

print("All models have been saved successfully!")
```

A.1.9 Creating a variant of the CNN-RF model using features from concatenated layers

Instead of taking features from the Conv1D layer (Layer 1) of the CNN network to train and test the RF model to form the proposed CNN-RF model, features are otherwise taken from the last MaxPooling1D layer (Layer 6) where three pairs of Conv1D and MaxPooling1D layers (3-layer CNN) are concatenated in a bid to enrich the extracted features used to train and test RF. This process leads to the development of the variant CNN-RF (concatenation) model.

The implementation codes to develop the variant CNN-RF (concatenation) model are thus:

```
# DEVELOPING THE VARIANT CNN-RF (CONCATENATION) MODEL
```

```
def build_3layer_cnn(input_shape):
    """
    Builds a 3-layer CNN with MaxPooling model using Functional API.
    """
    inputs = Input(shape=input_shape)
    # 1st Conv + MaxPool
    x = Conv1D(32, kernel_size=3, activation='relu',
padding='same')(inputs)
    x = MaxPooling1D(pool_size=2)(x)

    # 2nd Conv + MaxPool
    x = Conv1D(64, kernel_size=3, activation='relu', padding='same')(x)
    x = MaxPooling1D(pool_size=2)(x)
    # 3rd Conv + MaxPool
    x = Conv1D(128, kernel_size=3, activation='relu', padding='same')(x)
    x = MaxPooling1D(pool_size=2)(x)

    x = Flatten()(x)
    x = Dense(128, activation='relu', kernel_initializer=HeUniform())(x)
    x = Dropout(0.4)(x)
    outputs = Dense(1, activation='sigmoid')(x)

    model = Model(inputs, outputs, name="3LayerCNN")
    return model
```

```
# Build, compile, and train
model_cnn_3 = build_3layer_cnn((x_train.shape[1], 1))
model_cnn_3.compile(optimizer=Adam(), loss='binary_crossentropy',
metrics=['accuracy'])
model_cnn_3.summary()
```

```
history_3 = model_cnn_3.fit(
    x_train, y_train,
    epochs=50,
    batch_size=30,
    validation_split=0.3,
    verbose=1
```

```
# Predict probabilities on the test set
y_pred_prob = model_cnn_3.predict(x_test)

# Convert probabilities to binary class labels (using 0.5 as threshold)
y_pred = (y_pred_prob > 0.5).astype(int)

# Compute the confusion matrix
cm = confusion_matrix(y_test, y_pred)

# Create a ConfusionMatrixDisplay with custom labels
disp = ConfusionMatrixDisplay(confusion_matrix=cm, display_labels=['Non-
theft', 'Theft'])

# Plot the confusion matrix with a custom values format (.1e for
scientific notation)
disp.plot(cmap=plt.cm.Greens, values_format='.1e')
plt.title("Confusion Matrix for 3-layer CNN model")
plt.show()
```

```
# Predict
cnn_3_proba = model_cnn_3.predict(x_test).ravel()
```

```
cnn_3_pred = (cnn_3_proba > 0.5).astype(int)

# Evaluate
cnn_3_metrics = calculate_metrics(y_test, cnn_3_pred, cnn_3_proba)
print("\n=== 3-Layer CNN Metrics ===")
for k, v in cnn_3_metrics.items():
    if v is None:
        print(f"{k}: None")
    else:
        print(f"{k}: {v:.4f}")
```

```
# Define a feature extractor model that outputs the features from the last
Conv1D layer at the MaxPooling1D layer
feature_extractor = Model(inputs=model_cnn_3.input,
outputs=model_cnn_3.layers[6].output)  # Layer 6 is the last MaxPooling1D
layer in the concatenated network of three pairs of Conv1D and
MaxPooling1D layers.

# Get feature maps for training and testing data
train_features = feature_extractor.predict(x_train[:4000])
test_features = feature_extractor.predict(x_test[:1500])

# Reshape features for Random Forest
train_features = train_features.reshape(train_features.shape[0], -1)
test_features = test_features.reshape(test_features.shape[0], -1)

# Train Random Forest Model
rf = RandomForestClassifier(n_estimators=50, random_state=42)
rf.fit(train_features, y_train[:4000])

# Evaluate Random Forest model
rf_predictions = rf.predict_proba(test_features)[:, 1]
rf_label_predictions = rf.predict(test_features)
```

```
# Evaluate
rf_metrics = calculate_metrics(y_test[:1500], rf_label_predictions,
rf_predictions)
print("\n=== Random Forest Metrics ===")
for k, v in rf_metrics.items():
    print(f"{k}: {v:.4f}" if v is not None else f"{k}: None")
# Compute the confusion matrix
cm = confusion_matrix(y_test[:1500], rf_label_predictions)

# Create a ConfusionMatrixDisplay with custom labels
disp = ConfusionMatrixDisplay(confusion_matrix=cm, display_labels=['Non-
theft', 'Theft'])
```

```
# Plot the confusion matrix with a custom values format (.1e for
scientific notation)
disp.plot(cmap=plt.cm.Greens, values_format='.1e')
plt.title("Confusion Matrix RF 3-Layer CNN")
plt.show()
```

```
# Combine CNN and RF Predictions for 3-layer CNN
cnn_weight = 0.3
rf_weight = 0.7

# Combine predictions using weighted averaging
cnn_rf_predictions = (cnn_weight * cnn_3_pred[:1500].flatten() + rf_weight
* rf_predictions)

# Convert probabilities to binary class labels (using 0.5 as threshold)
cnn_rf_predictions = (cnn_rf_predictions > 0.5).astype(int)

# Evaluate combined model
cnn_rf_3_metrics = calculate_metrics(y_test[:1500], (cnn_rf_predictions >
0.5).astype(int), cnn_rf_predictions)
print("\n=== 3-Layer CNN-RF Ensemble Metrics ===")
for k, v in cnn_rf_3_metrics.items():
    print(f"{k}: {v:.4f}" if v is not None else f"{k}: None")
```

```
# Compute the confusion matrix
cm = confusion_matrix(y_test[:1500], cnn_rf_predictions)

# Create a ConfusionMatrixDisplay with custom labels
disp = ConfusionMatrixDisplay(confusion_matrix=cm, display_labels=['Non-
theft', 'Theft'])

# Plot the confusion matrix with a custom values format (.1e for
scientific notation)
disp.plot(cmap=plt.cm.Greens, values_format='.1e')
plt.title("Confusion Matrix for ensembled CNN-RF")
plt.show()
```

```
# PLOT METRIC COMPARISON BAR CHART FOR ALL MODELS
```

```
# Find common metrics across all models
common_keys = set(cnn_3_metrics.keys()) & set(rf_metrics.keys()) &
set(cnn_rf_3_metrics.keys()) & set(cnn_rf_1_metrics.keys())

# Preferred order of metrics
preferred_order = [
   "Precision", "Recall", "F1 Score", "Accuracy",
]
```

```
metric_order = [m for m in preferred_order if m in common_keys]

# Extract scores for each model
cnn3_scores = [cnn_3_metrics[m] for m in metric_order]
rf3_scores = [rf_metrics[m] for m in metric_order]
cnnrf3_scores = [cnn_rf_3_metrics[m] for m in metric_order]
cnnrf1_scores = [cnn_rf_1_metrics[m] for m in metric_order]

# Plot settings
plt.figure(figsize=(20, 15))
x = np.arange(len(metric_order))
width = 0.2  # Adjusted for four bars

# Create bars
bars_cnn3 = plt.bar(x - 1.5*width, cnn3_scores, width, label='CNN', color='blue', edgecolor='black')
bars_rf3 = plt.bar(x - 0.5*width, rf3_scores, width, label='RF', color='green', edgecolor='black')
bars_cnnrf3 = plt.bar(x + 0.5*width, cnnrf3_scores, width, label='CNN-RF (Concatenated)', color='red', edgecolor='black')
bars_cnnrf1 = plt.bar(x + 1.5*width, cnnrf1_scores, width, label='CNN-RF (proposed)', color='orange', edgecolor='black')

# Labels and titles
plt.xlabel('Metrics', fontsize=14)
plt.ylabel('Scores', fontsize=14)
plt.title('Comparison of results', fontsize=16)
plt.xticks(x, metric_order, rotation=45, ha='right')
plt.legend()

# Annotate bars with values
def autolabel(rects):
    for rect in rects:
        height = rect.get_height()
        plt.annotate(f'{height:.4f}',
                     xy=(rect.get_x() + rect.get_width()/2, height),
                     xytext=(0, 3),
                     textcoords="offset points",
                     ha='center', va='bottom', fontsize=12)

autolabel(bars_cnn3)
autolabel(bars_rf3)
autolabel(bars_cnnrf3)
autolabel(bars_cnnrf1)

plt.ylim(0, max(cnn3_scores + rf3_scores + cnnrf3_scores + cnnrf1_scores) + 0.1)
plt.tight_layout()
plt.show()
```