Detection and Confirmation of Electricity Thefts in Advanced Metering Infrastructure by Long Short-Term Memory and Fuzzy Inference System Models

A. O. Otuoze[1,2]*, M. W. Mustafa[1], U. Sultana[3], E. A. Abiodun[4], B. Jimada-Ojuolape[5], O. Ibrahim[2], I. O. Avazi-Omeiza[2], A. I. Abdullateef[2]

[1]Department of Power Engineering, Faculty of Electrical Engineering, Universiti Teknologi Malaysia, Johor Bahru, Malaysia.

[2]Department of Electrical and Electronics Engineering, Faculty of Engineering and Technology, University of Ilorin, Ilorin, Nigeria.

[3]Department of Electrical Engineering, NED University of Engineering and Technology, Karachi, Pakistan

[4]Department of Viticulture and Enology, Fresno State University, 2415 E. San Ramon, MS AS79, Fresno, California. 93740, United States of America

[5]Department of Electrical and Computer Engineering, Faculty of Engineering and Technology, Kwara State University, Malete, Nigeria.

ABSTRACT: The successful implementation of Smart Grids heavily relies on energy efficiency, particularly through the Advanced Metering Infrastructure (AMI) and Smart Electricity Meters (SEM). However, cyber-attacks pose a threat to SEM, with electricity theft being a primary motivation. Despite the valuable data provided by SEM for analytical purposes, existing methods to identify theft involve cumbersome and costly on-site inspections. This research proposes an electricity theft detection model using the Long Short-Term Memory (LSTM) network. The model employs a collective anomaly approach, defining prediction errors through a threshold and forecast horizon. Suspicious consumption profiles are analysed, and a fuzzy inference system (FIS) implemented in MATLAB 2021b is used to model security risks based on these profiles. The study utilizes energy consumption data from four diverse consumer profiles (consumers 1, 2, 3, and 4) to develop consumer-specific LSTM models for detection and an FIS model for confirmation. Tampered consumer data is identified and confirmed based on selected AMI parameters. While all consumers exhibit suspicious profiles at times, only consumers 2 and 3 are confirmed as engaging in electricity theft. This research provides a robust approach to detecting and verifying fraudulent consumption profiles within the context of AMI, offering a more reliable dimension to theft detection and confirmation.

KEYWORDS: Advanced metering infrastructure, Anomaly detection, Confirmation model, Electricity theft detection, Fuzzy inference system, Long short-term memory.

[Received Jan. 11, 2024; Revised Feb. 1, 2024; Accepted Feb. 8, 2024] Print ISSN: 0189-9546 | Online ISSN: 2437-2110

I. INTRODUCTION

The increased complexity and dynamism of electricity theft incidences necessitate several research efforts towards providing schemes to effectively address the menace. Fortunately, the smart grid (SG) environment inherently offers enhanced systems' monitoring platform that supports the application of real-time models for various applications. While several electricity theft detection (ETD) schemes have been explored as they measure to the conventional power delivery networks, only a few works have been submitted in relation to those for applicable to the advance metering infrastructure (AMI). Moreover, the conventional power systems are being upgraded worldwide to deliver the advantages AMI offered through SG implementations. These include effective power consumption monitoring, reduced grid losses, enhanced grid operations and effective energy management (Calderaro *et al*., 2011; Clastres, 2011; El-Hawary, 2014; Moretti *et al*., 2017).

AMI enables a two-way communication between the consumers and utilities via smart electricity meters (SEM) at both ends (Fatemieh *et al*., 2010; Jiang *et al*., 2014; Jokar, 2015; Shuaib *et al*., 2015). SEM support communications and control for effective energy management, and is a key aspect of SG (Abushnaf *et al*., 2016; McLaughlin *et al*., 2009). Although the introduction of SEM has greatly curbed the incidences of electricity theft associated with conventional meters, AMI is subjected to cyber threats as adversaries continue to explore its vulnerabilities. The AMI architecture faces series of electricity thefts induced by cyber-attacks on its computational resources - devices, networks, programs, and data (Jiang *et al*., 2014; Nabil, Mahmoud, *et al*., 2019; Sharma *et al*., 2016). Electricity theft occasioned by cyber-attacks are aimed at manipulating the SEM consumption profiles, billing information, timestamp, and other possible network parameters, with the sole aim of evading bill payments.

Effectively, the adversaries' malicious manipulations cause huge losses across the globe and the perpetration trend is

*Corresponding author: Otuoze.ao@unilorin.edu.ng *doi:* http://dx.doi.org/10.4314/njtd.v21i1.2294

constantly evolving as SEM are increasingly being deployed. Moreover, electricity infrastructures are among the most common targets of attacks, physical or cyber-based. The associated large-scale losses (technical, social, and economic) make electricity theft a major concern in SG implementation (Adil *et al*., 2020; Chen *et al*., 2020; Jamil & Ahmad, 2014; Jindal *et al*., 2016). This could be worsened by poor systems planning while the system's reliability is equally threatened (Salinas & Li, 2016). Other effects of this rampaging acts include shortage of revenues for utilities, dampening investment opportunities and commitments, increased billings on honest consumers, the need for subsidy payment by the government to make up for shortfalls (Jamil & Ahmad, 2014; Mohammad *et al*., 2013; Sharma *et al*., 2016) etc.

Nigeria, India, Brazil, China, Pakistan and the US lose about 34%, 20%, 16%, 6%, 13% and 5% of their generated power, respectively, to electricity thefts (Fang *et al*., 2023; Gaur & Gupta, 2016; Krishna *et al*., 2016; Xia *et al*., 2023). US, UK, India, Russia, and Brazil lose about $6 billion, GBP 173 million, $16.2 billion, $5.1 billion, and $5 billion, respectively (Jiang *et al*., 2014; Mukhopadhyay *et al*., 2023; Sharma *et al*., 2016; Xia *et al*., 2023). The developing nations lose between 20 to 50% of their expected revenue while the developed nations record between 3.5 to 30% loss (Jiang *et al*., 2014; Musungwini, 2016). Northeast group LLC reported that worldwide, $96 billion are lost due to electricity theft yearly (Appiah *et al.*, 2023). These unfortunate losses in revenue necessitate the need for efficient detection and confirmation techniques (Delgado-Gomes *et al*., 2015; Xu *et al*., 2023; Zhao *et al*., 2023).

Electricity theft detection based on the conventional metering system data is characterized by the necessity to analyse large data collected over a long period of time and the analysis are usually offline (Haq *et al*., 2023; Sun *et al*., 2023; Xia *et al.*, 2023). In AMI, such models are not suitable as the response to fraudulent activities must be swift and timely. Although, it is difficult to compute non-technical losses (NTL), the AMI provides adequate data which are being leveraged for analysis using machine learning (ML) based techniques to detect suspicious activities. These techniques basically involve aggregating SEM energy consumption data to build a resilient defence mechanism for analysis and inferences such as firmware security, key management security, and source code development security (Goel & Hong, 2015; Gu *et al.*, 2022; Shehzad *et al.*, 2022). However, integrated energy consumption profiling of several consumers' data poses undesirable grey areas in the determination of individual consumers' contributions, highly biased, and complicated.

Moreover, reported algorithms utilizing energy consumption data are yet to substantially consider real-time monitoring suitable for AMI deployment. In addition, the use of daily, monthly, or yearly average consumption data, as obtained in most existing studies, does not correctly profile a consumer in a real-time environment as those of smart utility networks. Also, existing approaches often consider a general practice of evaluating a common threshold for determining fraudulent activity for all monitored consumers within a given network. This is also not suitable, as real-time consumer behaviour are stochastic, hence, the need for a consumer-based prediction model using a sophisticated ML technique suitable for a stochastic time-series data as those of SEM. Furthermore, existing detection techniques only aim at generating the list of suspicious consumers necessitating scheduled physical inspections of consumer premises to confirm theft cases before penalties are imposed. These procedures remain highly complicated, ineffective, and costly. Therefore, further research is required for efficient solutions to electricity thefts detection and confirmation especially as suitable for AMI deployment.

In this paper, an LSTM model is developed for energy consumption prediction and implementation on the consumption profiles of four different consumers (consumers 1, 2, 3 and 4). First, Consumers 2 and 3 data (attacked) and Consumers 1 and 4 (clean) were obtained. The model is then trained using the dataset for a short horizon forecast. A collective anomaly model is presented to determine suspected consumption profiles. To confirm fraudulent cases, the suspicious status and selected AMI parameters are modelled using fuzzy inference system (FIS). This approach presents detection and confirmation models for effectively curbing electricity thefts in AMI. Next, section 2 gives an overview of related studies while the methodology is presented in section 3. The obtained results are presented and discussed in section 4 while section 5 concludes the study.

II. RELATED STUDIES

Electricity theft detections via the AMI are generally examined using either of four basic techniques viz, the state-based, game theoretic, classification and prediction-based models (Jiang *et al.*, 2014). The state-based involves designing a device for a high monitoring and detection accuracy but it comes with high investment price. Other state-based solutions could see to the application of expert-based algorithms. A sample of a state-based technique utilising a rule-based detection which leverages AMI parameters preselected and modelled for electricity theft prevention was presented by Otuoze *et al*. (2022). Game-theoretic approaches are based on formulation of game theory between the utility and the thief. These techniques are proposed to formulate a game-theoretic model to determine the correlations between non-technical losses and consumer behaviour in order to determine abnormal consumption profiles (Cárdenas *et al*., 2012; Wang *et al*., 2020). Although game-theoretic models are of relatively low cost and suited for AMI deployments, they are optimally unreliable.

The classification-based models involve training a given customers' dataset with labels to check for suspected cases of frauds. Robust data mining and ML techniques are employed for the training and testing of the classifier before being deployed to detect fraudulent cases. Some artificial intelligence techniques such as support vector machine, decision tree, random forest, and gradient boosting have been implemented for electricity theft detection to detect non-technical losses (Ahmad *et al*., 2018; Depuru *et al*., 2011; Nagi *et al*., 2008; Tehrani *et al*., 2020; Toma *et al*., 2019). However, a fundamental issue related to ML classifiers as applicable to electricity theft detection is imbalance in the data resulting

from the difference in normal and abnormal samples. This is because theft samples are highly stochastic and do not practically exist in wholesome as they are exposed to myriads of vulnerabilities. Secondly, deploying such method means significant delays (in collecting data samples) before thefts are determined (Hu *et al*., 2019; Lu *et al*., 2019).

In prediction-based algorithms, timeseries forecasting techniques are applied to forecast future consumptions which are then used to determine the prediction errors with reference to the real time observed values. In modelling a time series data, previous observations are carefully studied to develop an intrinsic structure for generating or predicting future values (Adhikari & Agrawal, 2013; Brockwell *et al*., 2002; Karasu & Altan, 2019). Suitable models are designed and fitted in a manner that takes the time dependence of the input data into consideration. These models are relied upon when there are no adequate information as to the nature of occurrence or rather, when its stochasticity is highly random and independent of many events (Adhikari & Agrawal, 2013) such as those of SEM data.

Existing ETD techniques utilise diverse aspects of AI and ML and are mostly offline based with energy consumption data analysed as bulk sequence. These techniques are constantly enhanced based on the trend in AI and ML as they have proven to be a robust and reliable tool for data analysis. To analyse SEM data for inferences on energy theft in a SUN, recent works consider energy consumption data as a time series data. This is to enable real-time analysis of energy consumption data by predicting and comparing with observed data as required for smart grid environment, hence, making prediction accuracy a key consideration in such models. Several research foci are being directed at developing efficient models for improving forecasting or prediction accuracy, one of which is the popular autoregressive integrated moving average (ARIMA) model which is hinged on the assumption that time series data are linear and follows a normal distribution. The ARIMA model has been used in some reported researches to either predict, validate or evaluate energy consumption data for electricity theft detection (Krishna *et al*., 2015; Mashima & Cárdenas, 2012; Uparela *et al*., 2018) etc. This technique comes with the limitation of data linearization assumption which certainly does not apply to SEM data for time-series analysis. In addition, the complicated nature of energy consumption data and the need to correlate these data with other real-time parameters of the AMI makes ARIMA model unsuitable for electricity theft detection.

Artificial neural networks (ANN) have been explored given its capability of non-linearity in modelling and without any assumption on the statistical distribution of the data (Adhikari & Agrawal, 2013; Blanco *et al*., 2000; Chiappini *et al*., 2020; Tawfik, 2003). ANN has been applied for electricity theft detection as reported in some works (Costa *et al*., 2013; Guerrero *et al*., 2014; Handique *et al*., 2019). However, ANN's dependence on data for forecasting with no memory storage to help future forecasting is a significant limitation making it unsuitable for the real-time requirements of the AMI.

Recurrent neural networks (RNN) were then introduced to help solve the memory storage issues of the ANN (Aungiers; Brownlee, 2016). RNN is a sequence dependent network, designed as a powerful tool for processing large data with improved ability to feedback as input, crucial aspect of the output to provide a context of the last seen input (Brownlee, 2016). In their study, Chen *et al*. (2020) declared that most existing machine learning-based electricity detection schemes are not efficient as they mostly consider electricity consumption as static records. This is because those studies fail to capture both the internal time-series natures and external influence factors. The study then proposed an electricity theft detection using deep bidirectional RNN, which has the capability of capturing the internal characteristics and the external correlation by learning the electricity consumption data in considerations of the stochastic nature dictated by its influencing factors.

The work by Nabil, Mahmoud, *et al*. (2019) presents a deep recurrent neural networks based detection scheme exploiting the time-series nature of the energy consumption data. The hyper-parameters were fine-tuned by a multi-objective evolutionary-based optimization for better performance of the detection model (Nabil, Mahmoud, *et al*., 2019). In another similar research output by the authors, a customer specific and generalized electricity theft detectors were presented based on a deep feed-forward and RNN (Nabil, Ismail, Mahmoud, Shahin, *et al.,* 2019). While SEM data analyses for ETD have been well explored using RNN and great results have been equally reported in some works (Chatterjee *et al*., 2017; Chen *et al*., 2020; Ismail *et al*., 2020), long term dependency on the models are faced with a fundamental vanishing gradient problem (Cheng *et al*., 2017; Fenza *et al*., 2019; Kim *et al*., 2018; Zhang *et al*., 2018). Hence, RNN are poorly suited for a continuous time series data as those of the SEM.

To solve the vanishing gradients, LSTM networks are developed (Haviv *et al*., 2019; Hochreiter, 1998; Kim *et al*., 2019). LSTM is also a deep neural network and a sub-class of the RNN also relying on backpropagation through time, but with the advantage of overcoming the vanishing gradient. It utilises memory blocks connected through layers rather than the neurons as used in the other architectures. Therefore, they are applied to solve difficult sequence problems for a robust and more reliable forecasting (Altan *et al*., 2019; Brownlee, 2016; Le *et al*., 2019). Figure 1 summarizes the limitation of each of the applicable techniques. As shown in Figure 1, anomaly detection models are built based on comparisons of the predictions with the true value, but with existing studies largely over-relying on Euclidean distance to determine anomalies. LSTM models or its variants have been presented for electricity theft detections in many other related studies (Hasan *et al*., 2019; Kocaman & Tümen, 2020; Madhure *et al*., 2020). For the stochastic nature of SEM data, it is not enough to base judgment of probability of deviations on energy consumption alone for anomaly detections. While some of the studies fail to consider the time series nature of typical SEM data, other parameters of the AMI critical for clericity theft detection and confirmation are equally not considered by most existing studies. In ETD, metrics such as energy consumption data, response time, pricing, time stamps, range etc. could be selectively analysed to identify anomalous trends (Siboni & Cohen, 2014).

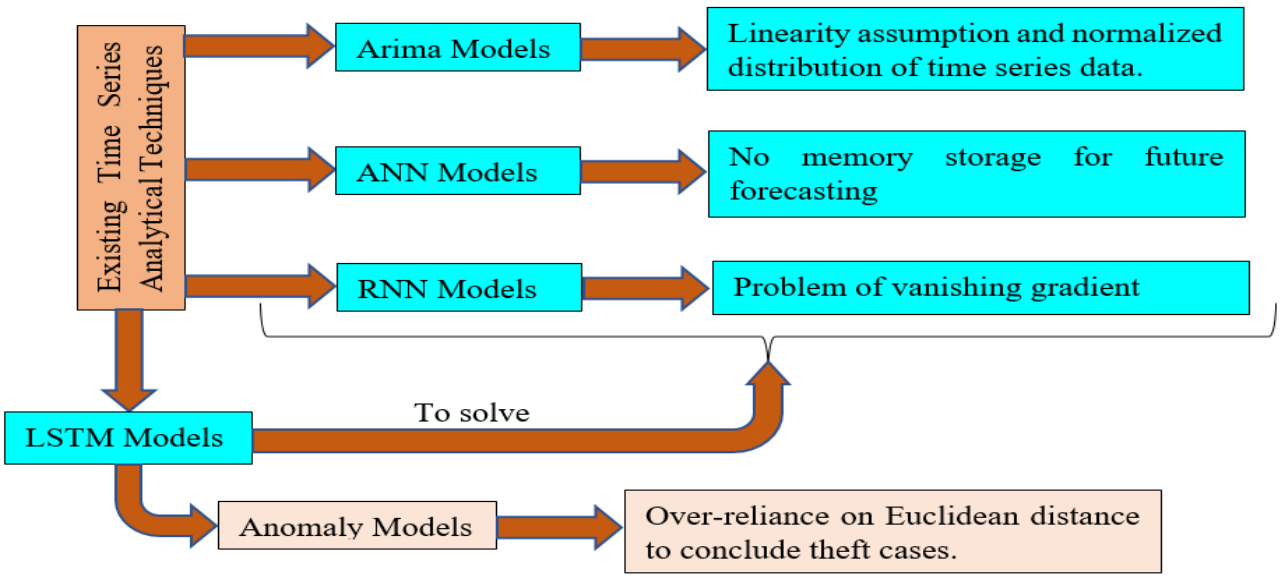


Figure 1 Limitations of time series analysis applicable to electricity theft detections

In previously reported works, various techniques deployed for ETD have focused only on identifying suspicious consumption profiles. Consequently, on-site inspection and confirmation is advised despite the huge tasks involved. To confirm if a suspicious consumption is truly fraudulent, additional steps are always required for increased reliability. This is because using only energy consumption defined by the generally stochastic consumer behaviours and activities, as well as possibilities of faults in meters and sensing devices, may cause false reflections in the readings. Table 1 gives a summary of some of the recent trends in the application of deep learning for ETD focusing on energy consumption data. The data are labelled with large, processed set of energy consumption data (ECD) in some reported studies. To solve the imbalance associated with classification algorithms and the need for confirmation of theft cases, this work contributes mainly by proposing an LSTM network for electricity theft detection and FIS model for electricity theft confirmation as suitable for AMI. We present a consumer dependent methodology with the advantages of theft confirmation which seeks to address the issues of physical on-site inspection.

III. METHODOLOGY

To examine theft cases, a prediction model is built using a deep neural LSTM network to help forecast the consumption data. The root mean square error (RMSE) plot is then used as the basis for modelling anomalies to detect suspicious consumption profiles in consideration with selected AMI parameters. Suspicious customers are defined to be those within the range of defined anomalies. A rule-based expert system model using FIS is incorporated to confirm theft cases. The FIS utilises selected parameters of the proposed AMI architecture. Four energy consumption of different profiles are selected for this study with consumers of confirmed suspicious profiles reported as fraudulent electricity consumers (FEC).

A. LSTM Architecture

In this work, an LSTM model is developed for a time series prediction of the selected households' power consumption data by exploiting its ability to automatically learn features from sequence data. Figure 2 (Hasan *et al*., 2019) gives a typical LSTM architecture. It shows how a sample time series data, X of features, C, flows through an LSTM layer to produce a regression output. The sequence input layer takes in the time series data into the network, the LSTM layer(s) learn the time dependencies of the input data, the fully connected layer defines the number of responses to the LSTM network while the regression output layer takes care of the output sequence.

B. Development of the LSTM Model for Forecasting

To develop LSTM model for forecasting, the attributes of the LSTM layer, the size of the input layers, number of features, number of hidden units and number of responses with syntax "numFeatures", "numHiddenUnits" and "numResponses" (in MATLAB) are specified. The fully connected layer has its size set to the number of responses while the output mode is set to 'last'. In this model the numFeatures is set to 1 because the model presented here is a customer dependent model. The consumers are assumably sectioned into respective protective zone, hence, every consumer within a zone is analyzed individually. Generally, to forecast future values of any given sequence where responses of the training sequence are shifted by one step and are recorded at every timestep or for a multistep, the responses are given at the defined timesteps, or they are set based on train to test ratio.

Figure 3 shows the model development and testing of the time series forecasting of the energy consumption using LSTM network. It also shows the step-by-step procedure and all the stages of the data handling by the developed model. First, the data sequence is loaded and split (for training and testing) before the train data is standardized. The predictors and the responses of the LSTM model are then prepared as the

Table 1 Recent trends in electricity theft detection techniques

S/No.	Technique Applied	Network Model	Monitored/Analysed Parameter	ECD	Confirmation of Theft cases	References
1.	Classification	CNN-LSTM	ECD (labelled)	10,000	X	(Hasan *et al*., 2019)
2.	Classification	wide and deep convolutional neural networks	ECD (labelled)	42,372	X	(Zheng *et al*., 2017)
3.	Prediction	LSTM	ECD (Unlabelled)	25	X	(Chatterjee *et al*., 2017)
4.	Game-theoretic	CNN	ECD (labelled)	NA	X	(Nabil, Ismail, Mahmoud, Alasmary, *et al*., 2019)
5.	Classification	Semi-Supervised Auto-Encoder (SSAE) – a Deep learning model	ECD (unlabelled)	5,000	X	(Lu *et al*., 2019)
6.	Classification	MFEFD	ECD (unlabelled)	N/A	X	(Lu *et al*., 2019)
7.	Classification	Convolutional Neural Networks (CNN), LSTM and Stacked Autoencoder.	ECD (labelled)	12,180	X	(Bhat *et al*., 2016)
8.	Classification	K-means and Deep Neural Network (DNN)	ECD (labelled)	535	X	(Maamar & Benahmed, 2019)
9.	Classification	LSTM	ECD (labelled)	33,979	X	(Kocaman & Tümen, 2020)
10.	Classification	LSTM and Random Under Sampling Boosting (RUSBoost)	ECD (labelled)	3,000	X	(Adil *et al*., 2020)
11.	Classification	Deep Vector Embeddings	ECD (labelled)	Consumer-dependent	X	(Takiddin *et al*., 2020)
12.	Classification & Regression	Autoencoders with LSTM-based Sequence-to-Sequence Structure	ECD (labelled & Unlabelled)	SGCC - 40,000 & ISET – 3,000	X	(Takiddin *et al*., 2022)
13.	Classification	SSA–GCAE–CSLSTM	ECD (labelled)	SGCC - 42,372	X	(Pamir *et al*., 2023)
14.	Classification	LSTM-TCN and DCNN	ECD (labelled)	SGCC - 42,372	X	(Huang *et al*., 2024)
14.	Regression & Rule-based	LSTM and Fuzzy Inference System	ECD (unlabelled), Timestamp, observer meter status, and intrusion detection status	Consumer-dependent	✓	Proposed Technique

MEED - Multitask feature extracting fraud detector. SSA - Salp Swarm Algorithm, GCAE – Gate Convolutional Autoencoder, and CSLSTM - Cost-Sensitive Learning and Long Short-Term Memory. TCN - Temporal convolutional networks; DCNN - Deep Convolutional Neural Network.

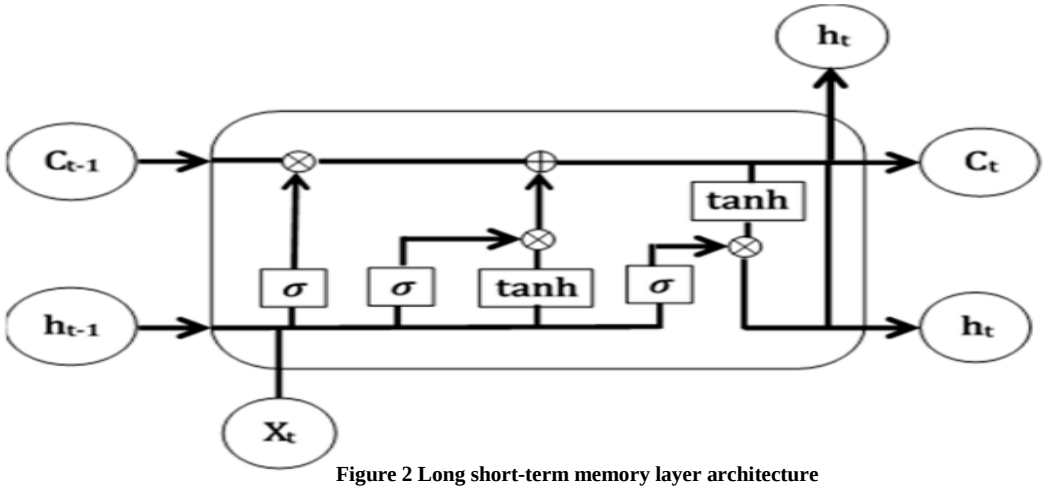


Figure 2 Long short-term memory layer architecture

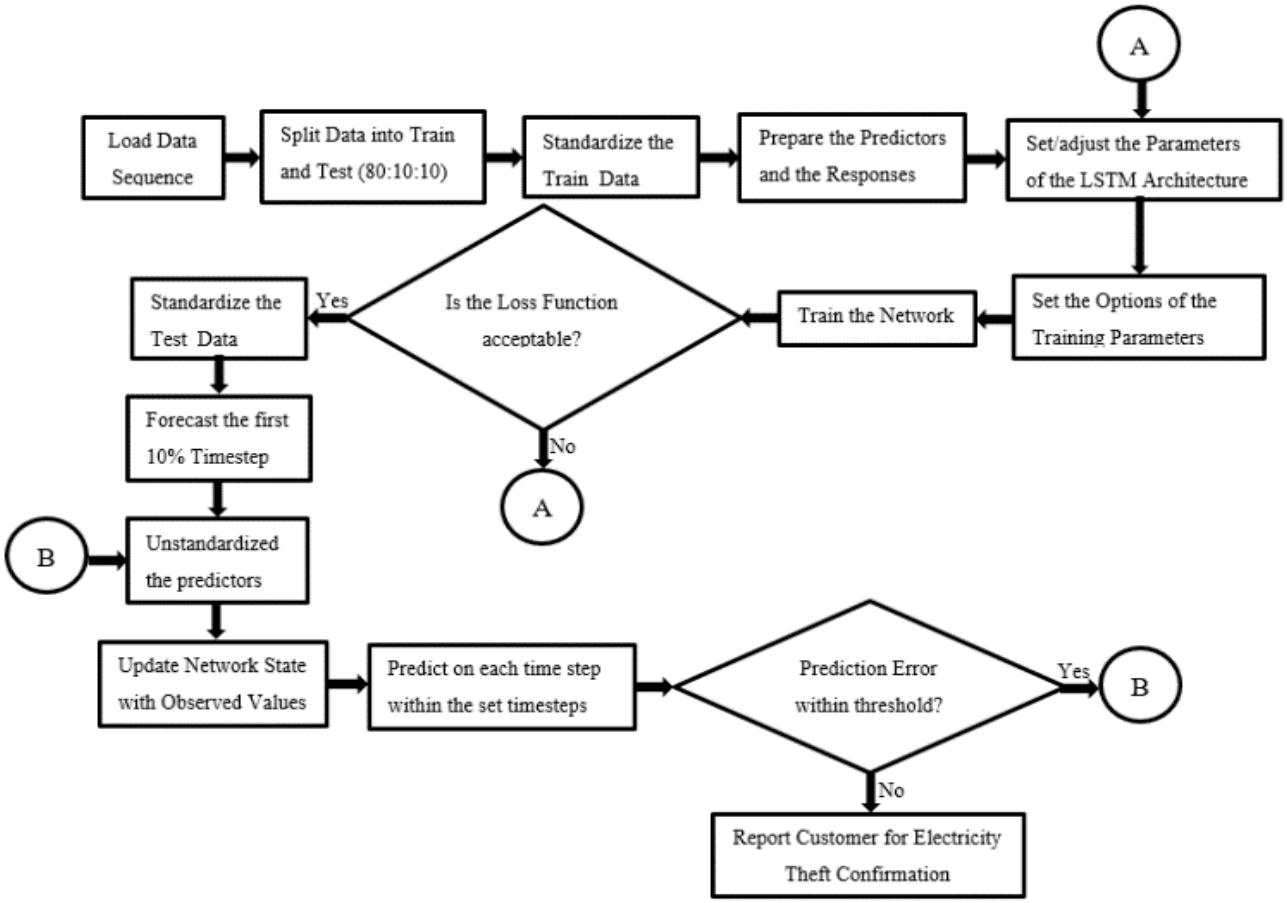


Figure 3 Model development and testing of the developed long short-term memory network for a time series forecasting of the energy consumption data.

parameters are adjusted for training the network. The training parameters are adjusted until an acceptable loss function is achieved and deemed suitable for optimal results. When the forecasts are made, the prediction errors are then checked based on the developed anomaly detection model and the need for theft confirmation.

C. Data Collection and Analysis

This study requires collection of energy consumption data obtained from SEM. The energy consumption data is a typically continuous and highly stochastic time series data. Unlike in many related studies where lengthy consumption data may be needed, exploring the advantage of the LSTM network, only four consumers with different profiles were selected for this study and each datapoint was recorded every 30 minutes. Three months data of 4,320 data points were collected and analysed for each of the four selected consumers. The energy consumption data used in this model is an extract of the data available via LondonDataStore (2015) which were reportedly recorded at every half-hour and refined as is. The selection of the energy consumption data was random and of different profiles. First, the energy consumption data obtained contained no anomaly, but it was strategically introduced at some timesteps for those of Consumers 2 and 3 data. Consumers 1 and 4 were left as obtained.

The step-by-step procedure of how the collected data were prepared and processed is as presented in Figure 4. The selected consumers' profiles largely vary from one to the other which makes them perfect fit for this study. By physical inspections, it may be inferred which set of the data contains anomaly but may not necessarily reflect true assertions. This is due to the highly stochastic nature of consumers' consumption behaviours. However, with the developed model, further analysis is carried out to determine anomalies. Consumers 1, 2, 3 and 4 are then subjected to training and testing using the developed LSTM model to forecast and study the behaviour of the profiles.

D. Training and Testing of the Developed Long Short-Term Memory Model

The energy consumption data of the selected profiles were split into 80% for training and from the remaining dataset, the first 10% was used for the first test forecast and the next 10% for updated forecasting. Therefore, the test data were equally standardized for prediction using the same parameters as those of the training data. The gradient threshold is set to 1 to make sure it does not explode. Depending on the nature of the data, the RMSE and the loss function are examined to determine the fitness of the model. In this work, after several trial and errors, the best training parameters fit for the model is as shown in Table 2. Typically, the loss function must be close to zero at the set epoch. To set an optimal value for the epoch, the training time as well as its performance are critical parameters which are carefully examined too. For a well-

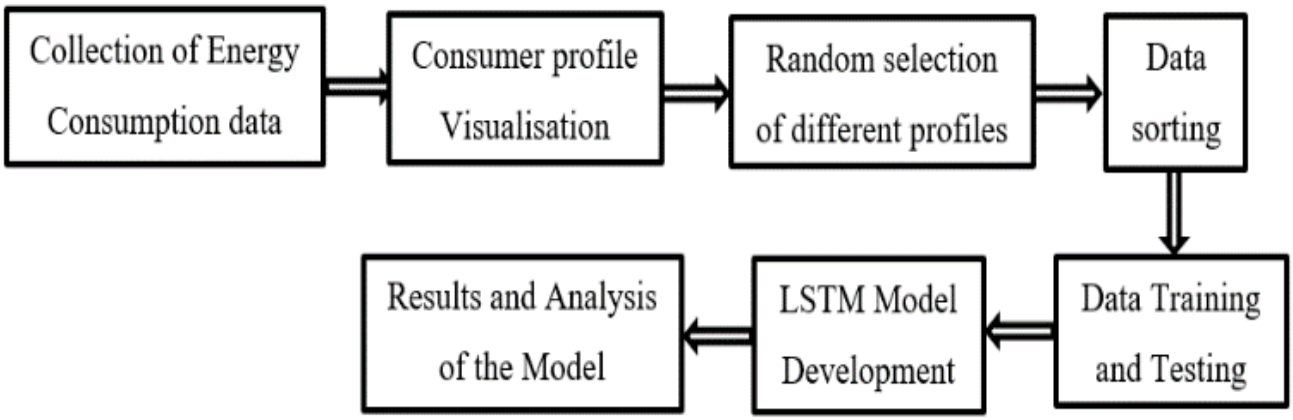


Figure 4 Data preparation and processing for long short-term memory forecasting

Table 2: Set training parameters for the developed long short-term memory model

Model Training Parameters	Values
Solver	Adam
Maximum number of epochs	500
Gradient threshold	1
Initial learn rate	0.005
Learn rate schedule	piecewise
Learn rate drop period	125
Learn rate drop factor	0.25
Verbose	0
Number of features	1
Number of responses	1
Number of hidden units	250

trained model, the loss function of the loss model settles at values lying below 0.1 for the maximum number of set iterations for all the selected data.

E. Development of the Anomaly Detection Model

In time series data as those of SEM, the presence of anomalies must be carefully defined by putting several situational inferences related to energy consumption behaviour into considerations. Given the stochastic nature of a typical energy consumption profile, point anomalies are not applicable. Using the technique of collective anomaly is most suitable in this study and fortunately, the LSTM network makes this easier with its predictive power. First, the energy consumption data is forecast for some time steps ahead. In this study, the error plot is relied upon to make decision on whether anomalous consumption is suspected or not based on the following:

i.The set threshold of prediction errors.

ii.Threshold for collective anomaly.

iii.The number of timesteps defining collective anomaly.

1) The Set Threshold for Prediction Errors

To determine the prediction errors, P_{Er}, each of the point forecast of the consumption value is compared with the observed or recorded value such that at every point in the forecast data, prediction errors are marked as anomaly based on Eqn. (1). This equation depicts the fact that if the forecast value, E_F is less than the observed value, E_O, at a given timestep, there is no suspected anomaly, and this is captured in the equation as 'P_{Er} is negative' meaning no cause for alarm. However, anomaly is suspected if the forecast value is greater than the observed value by a set threshold. This model provides for a threshold of $1.2E_O$ as contained in Eqn. (1). This means only 20% deviation from the observed values is allowed. This allowance for prediction error is based on the observed RMSE whose profile lies within 20% deviation of the error plots for the forecast as observed for the non-fraudulent consumption profiles.

$$P_{Er} = \begin{cases} \text{Negative}, & E_F < E_O \\ \text{Positive}, & E_F > 1.2E_O \end{cases} \quad (1)$$

2) Threshold for collective anomaly

Having set $E_F > 1.2E_O$ for a possible anomalous state, it is crucial to set a limit of collective anomaly to suspect such consumption values. For classification problems, the labelled normal and anomalous records of a validation set is used to determine this threshold but in a smart utility network-based analysis relying on real-time predictions and comparisons, this study models that a suspicious consumption be flagged if the status of the central observed meter, $\delta = 1$, and P_{Er} is positive at the same timesteps of the anomalous states. Summarily, suspicious consumption,E_S, combines these formulations as given in Eqn. (2).

$$E_S = \begin{cases} 1, & \delta = 1, P_{Er} \text{ is positive} \\ 0, & \text{Otherwise} \end{cases} \quad (2)$$

3) The Number of Timesteps Defining Collective Anomaly

While the computational model of Eqn. (2) gives a valid base to suspect anomalous consumption, it is not enough to conclude theft activity. This is because energy consumption profile is one that can vary so randomly as the activities of the user. Therefore, collection of points of continuous anomalies for a set timesteps known as collective anomalies must be defined to make this decision. However, shortest possible timesteps must be set such that in cases of thefts, only bearable losses are incurred. This arbitrary period of timesteps depends

on the convenience determined by the utility operator. Note that anomalies are not tolerated for significant timesteps before an inference is made for possible halt of services and/or imposition of penalty on the FEC to avoid significant losses. In this model, 24 timesteps is suggested which is equivalent to half of a day since our datapoints are recorded at 30 minutes interval. Consequently, for a theft activity to be suspected, Eqn. (2) must hold for a set period, T before such consumers are flagged. Eqn. (3) defines the collective anomalous consumption, E_{CA} when suspicious consumption is flagged. However, there is still need for further analysis since these customers are merely suspected, hence, the need for a confirmation model.

$$E_{CA} = \begin{cases} 1, \ E_S = 1, \ 0 < \tau \geq T \\ 0, \ \text{Otherwise} \end{cases} \quad (3)$$

where τ is the period indicative of how long a suspicious consumption is recorded.

F. Designing the Electricity Theft Confirmation Model

The proposed electricity theft confirmation model (ETCM) is aimed at ensuring suspected fraudulent consumers are rightly adjudged before applying sanctions or any other correctional operations. To achieve this, three key parameters of the AMI are selected, the status of the intrusion detection, α, observer meter status, δ, and the collective anomaly, E_{CA}. In basic AMI architecture, constant monitoring for possible intrusions is ensured due to its susceptibility to cyber-attacks. This study has selected the status of this important parameter, α, as it helps corroborate fraud detection inferences. Also, central observer meters are included for monitoring in AMI architecture. The status of the central observer meter, δ, is considered as a primary indication of fraud or technical losses. In this study, we assume the technical losses are accounted for and hence, all flagged cases by δ signifies theft cases.

For all the selected parameters (α, δ, and E_{CA}) for this model, a state "1' signifies compromised state while state "0" signifies uncompromised or normal state. To normalize this scenario, Table 3 is developed with each of the parameters acting as a check on the other. This study models that electricity theft is confirmed True (state "1"), only when two of the parameters are true, otherwise, its false. Table 3 can be implemented by any of the rule-based techniques. This study proposes a FIS model for the implementation. The input and output layout of the developed FIS model utilising the popular Mamdani model is as shown in Figure 5. Table 4 shows the fuzzy sets defined for the input and output with "Low" and 'High" representing the "0" and "1" states, respectively. The developed membership functions for the input and output are as shown in Figures 6 and 7, respectively. The membership functions defined for input "Low" and "High" representing "0" and "1" are Triangular and Trapezoidal and were set at equal margins for all inputs. Although, no specific membership function is defined for any event, every human-expert system as this requires a fundamental understanding and possibly some trial-and-error approach, as was followed in this model. The triangular membership function set for the low is to ensure the state is not allowed to last for too long before any form of breach is detected while the trapezoidal input is to ensure higher chances of detecting intrusion. Based on the rules implemented in this model, confirmed electricity thieves are generated and are subsequently listed for possible automated penalty.

Table 3 Developed truth table for electricity theft confirmation

S/No.	α	δ	E_{CA}	Electricity Theft Confirmation
1	0	0	0	False
2	0	0	1	False
3	0	1	0	False
4	0	1	1	True
5	1	0	0	False
6	1	0	1	True
7	1	1	0	True
8	1	1	1	True

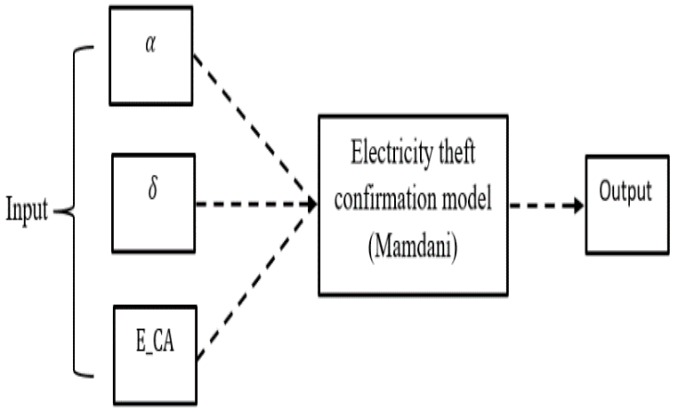


Figure 5 Input-output model of the developed FIS for electricity theft confirmation.

Table 4 Defined fuzzy sets of the input and output membership function for the confirmation models.

	Defined Signal Sates	Membership Function	Defined Fuzzy Sets
	Low	Triangular	[0 0.3 0.5]
	High	Triangular	[0.4 0.7 1]
	False	Trapezoidal	[0 0.2 0.4 0.6]
	True	Trapezoidal	[0.5 0.7 0.9 1]

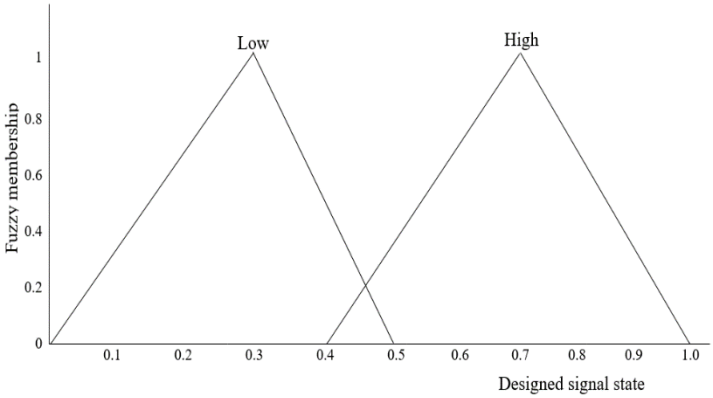


Figure 6 Input membership function for the confirmation model.

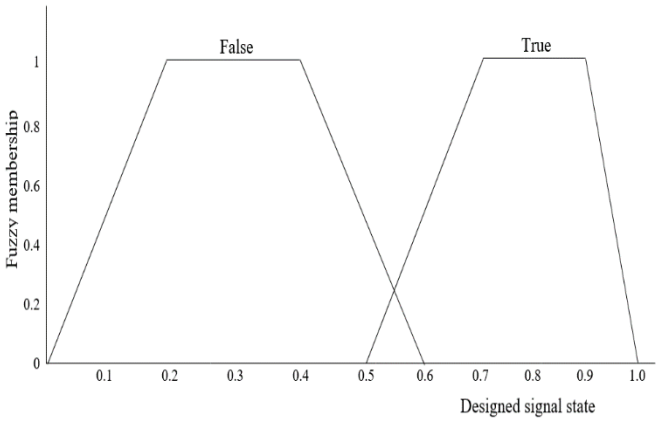


Figure 7 Output membership function for the confirmation model.

IV. RESULTS AND DISCUSSION

The developed models for electricity theft detection and confirmation were implemented on the selected consumer profiles using MATLAB 2021b. The forecast was made on the first 10% of the test data for each of the studied consumption profiles as shown in Figure 8 (a to d). By physical inspection, the forecast values of Consumer 1 (Figure 8a) show suspicious trend from the 3500th to 3800th while those of other consumers show otherwise (Figures 8b to d). To analyse theft cases, consumption patterns have to be subjected to further analysis to determine suspicious cases and possibly be able to conclude whether a theft has been committed. Figures 8 (a to d) are referred in this research for the analysis of suspicious and confirmation status on possible theft cases.

These forecast profiles are subsequently compared with the corresponding observed profiles (Figures 9a through d). The comparisons of the forecast with the observed test values of Consumer 1 during the first 10% (Figure 9a) shows that largely, there may be no theft cases until about 450th timestep as shown. From this region till the last shown timestep, Consumer 1's profile seems suspicious by physical inspections. It is not enough however, to conclude a theft case. Consumer 2 profile (Figure 9b) shows significant deviation from the observed values and proves a significant reason to suspect theft. Recall that the forecast of Consumer 2 shown in Figure 8b gives no sign of suspicious consumption. As for Consumer 3 (Figure 9c), some random abnormality is observed and could be interpreted as suspicious consumption while Consumer 4 (Figure 9d) shows no sign of suspicion.

The studied profiles have given random reasons to suspect electricity thefts. With reference to various studies relying only on Euclidean distance, Consumers 1, 2 and 3 would be reported as suspicious while Consumer 4 may not be examined further. In this study, further analysis is made before drawing conclusions. Consequently, forecast is made on the next 10% of the test data with the observed values updated using the observed values of the previous 10%. This is because predictions given in the updated forecast are more accurate since the network was updated with the observed values of the previous test data rather than the predicted values. For more timesteps, forecasts are made based on the previously updated observed values. Figure 10 (a through d) gives the updated forecast for all the consumers. To ascertain the suspicious status of each of the consumer profiles, the results of the anomaly detection models of Eqns. (1) to (3) are examined.

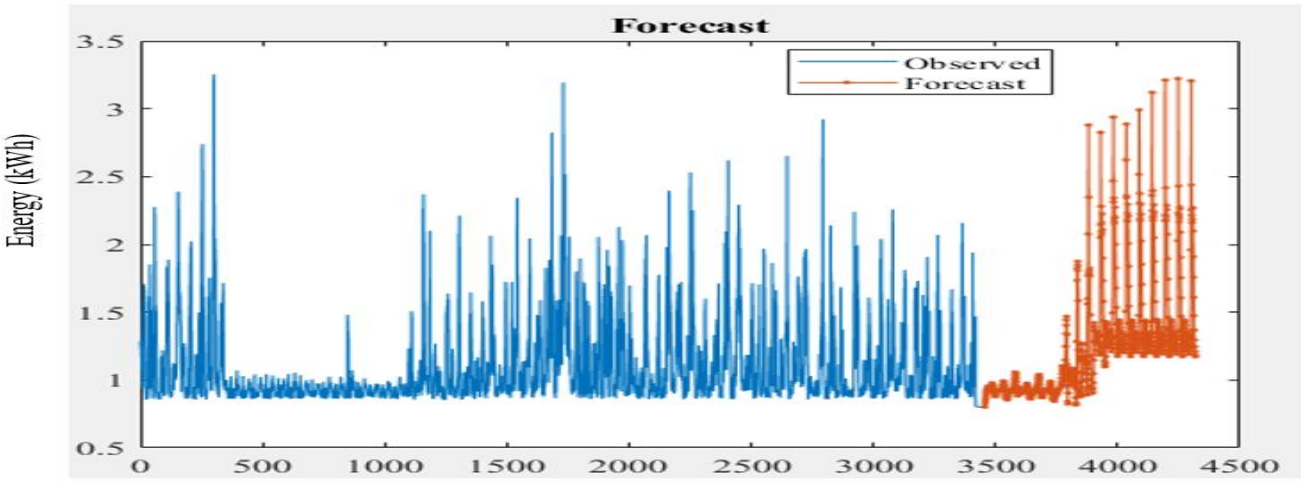
A. Determining the Suspicious Consumption Profiles

To detect suspicious consumption, the anomaly detection model given in Eqns. (1) to (3) were implemented to observe the first and updated forecast. During the first forecast (Figures 9a through d), anomalous behaviours are observed for Consumer 1 from the 450th timestep (Figure 9a), Consumer 2 from the 55th timestep (Figure 9b) and for Consumer 3 from the 95th timestep (Figure 9c). Consumer 4 showed no suspicious sign (Figure 9d). In the updated forecast (Figures 10a through d), Consumer 1 showed no sign of anomaly (Figure 10a) while Consumer 2 shows huge sign of anomalies from the 80th timestep (Figure 10b). Consumer 3 only shows a very slight deviation as observed from the error plot (Figure 10c) and Consumer 4 again, shows no sign of anomaly (Figure 10d). Tables 5 and 6 give the suspicious status of the consumers with each consumer identification (CID) during the first and updated forecast based on the anomaly detection models as given in Eqns. (1) to (3). In summary, Consumers 1, 2 and 3 showed suspicious status while only consumers 2 and 3 are suspected during the updated forecast. Notwithstanding, the confirmation status needs to be ascertained before final decision is made on the fraudulent status of the suspected consumption profiles.

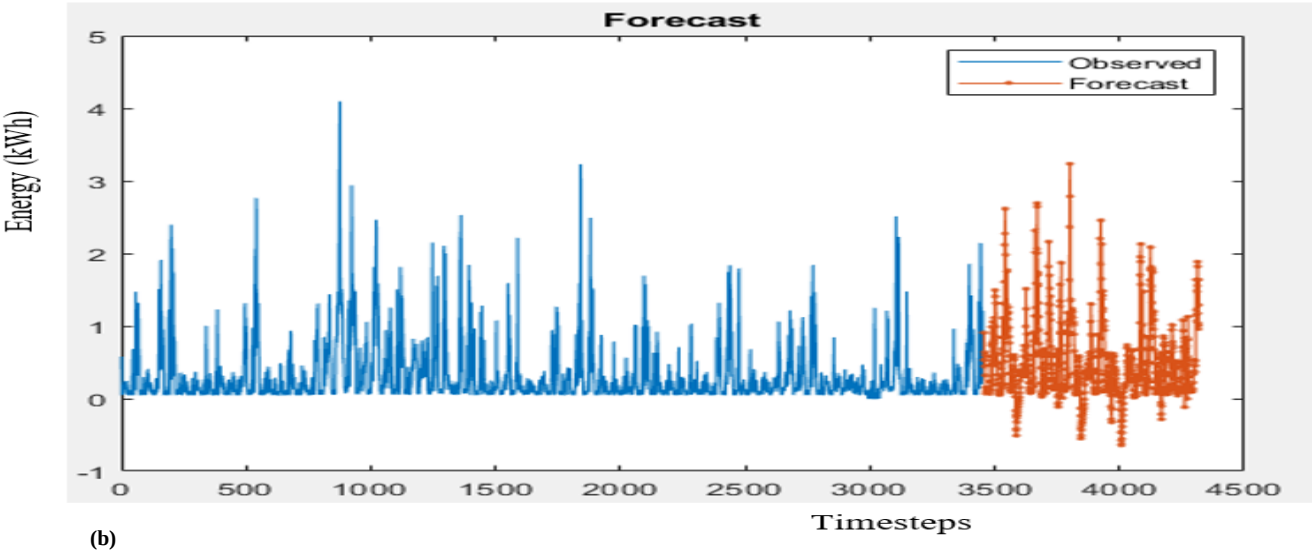
B. Confirming Fraudulent Consumption Profiles

Having provided for anomaly detection upon which the suspicious status of possible fraudulent status was determined, the results are further subjected to the rule-based model presented in subsection 3.F. The results of the ETCM is as given in Figure 11 at 0.5 weight for each of the modelled parameters by implementing the rules presented in Table 7 where E_{CA} is denoted by E_CA. Figure 11 clearly shows that theft is confirmed when at least two of the parameters are significant above the 0.5 weight. At this state, the confirmation is as weighty as 0.7 showing a high confidence level of theft confirmation. The interdependencies of the modelled parameters given as velocity vectors of Figures 12 to 14 indicate the direction of the densities of the states. All the interdependencies as shown clearly hints that before the 0.5 weight, the parameters do not signal theft confirmation while from 0.5 weight and above, all the modelled parameters as shown, tend to confirm possible theft cases. Although, other possible translation could be achieved depending on the variation of each of the parameters, the model presented in Figure 13 is an integral sum of the state of the parameters at 0.5 weight. This can be tuned for other weights between 0 and 1 to determine the status but significance is obtained from the 0.5 weight and above.

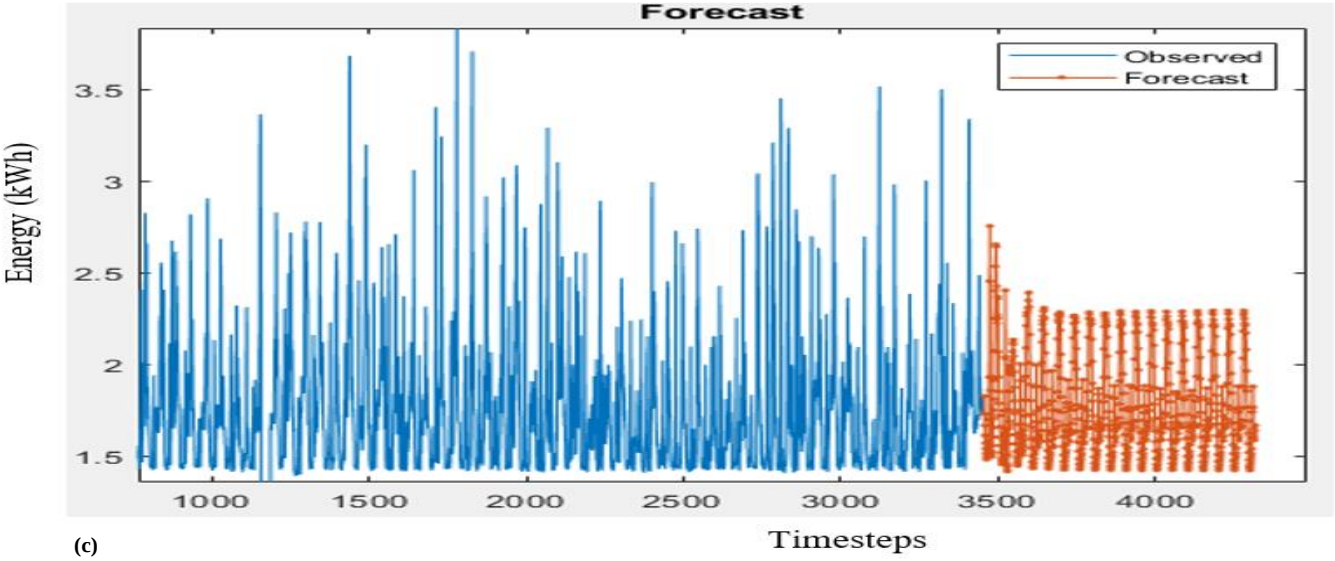
During the confirmation status, customers' consumption whose profile flags the status "True" at the set timesteps and for all instances from τ are reported to have committed fraud. The results of the confirmation status for each of the consumers are as given in Tables 8 and 9 for the first forecast at negative and positive intrusion status, respectively. Tables 10 and 11 give the confirmation status for the updated forecast at the


Forecast
Observed
Forecast
Energy (kWh)
Timesteps
3.5
3
2.5
2
1.5
1
0.5
0
500
1000
1500
2000
2500
3000
3500
4000
4500

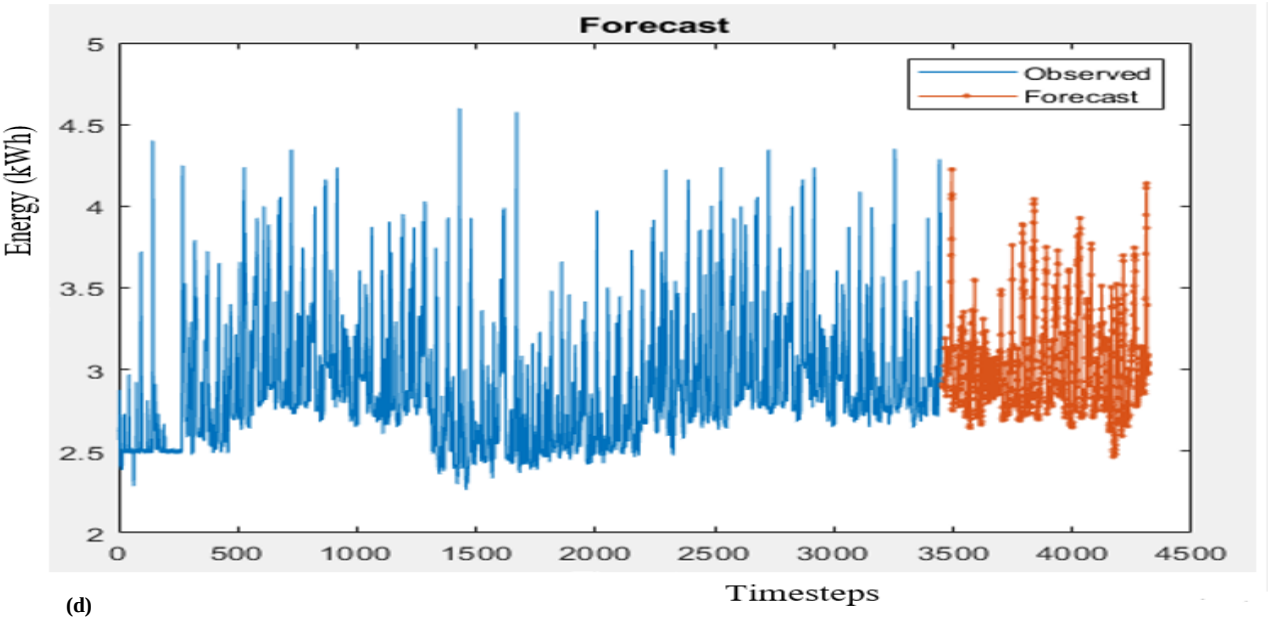
(a)


Forecast
Observed
Forecast
Energy (kWh)
Timesteps
5
4
3
2
1
0
-1
0
500
1000
1500
2000
2500
3000
3500
4000
4500

(b)

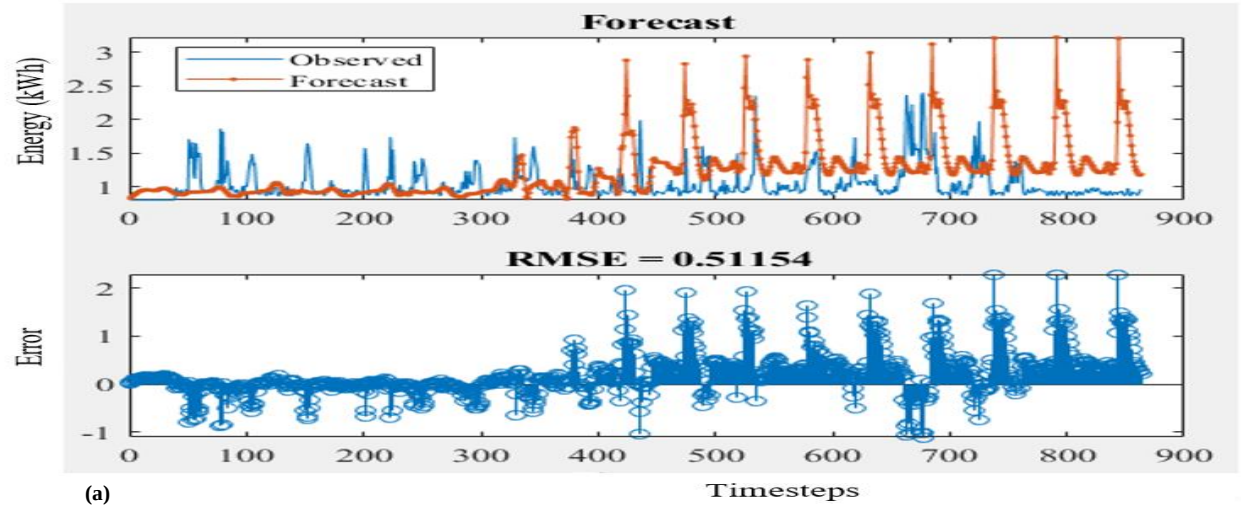

Forecast
Observed
Forecast
Energy (kWh)
Timesteps
3.5
3
2.5
2
1.5
1000
1500
2000
2500
3000
3500
4000

(c)

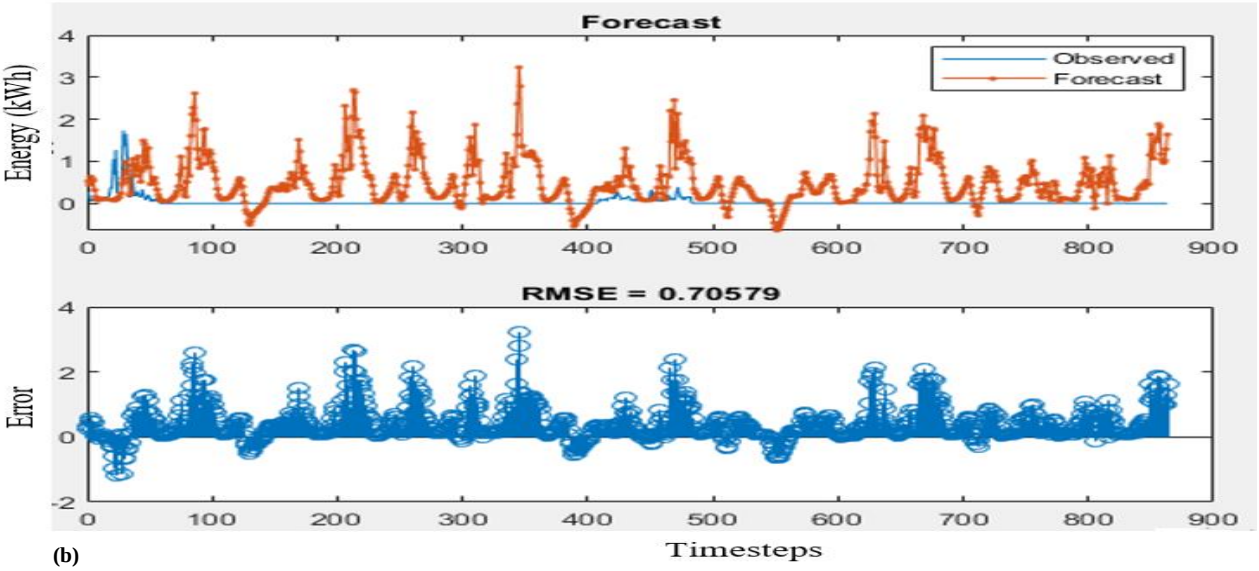


(d)

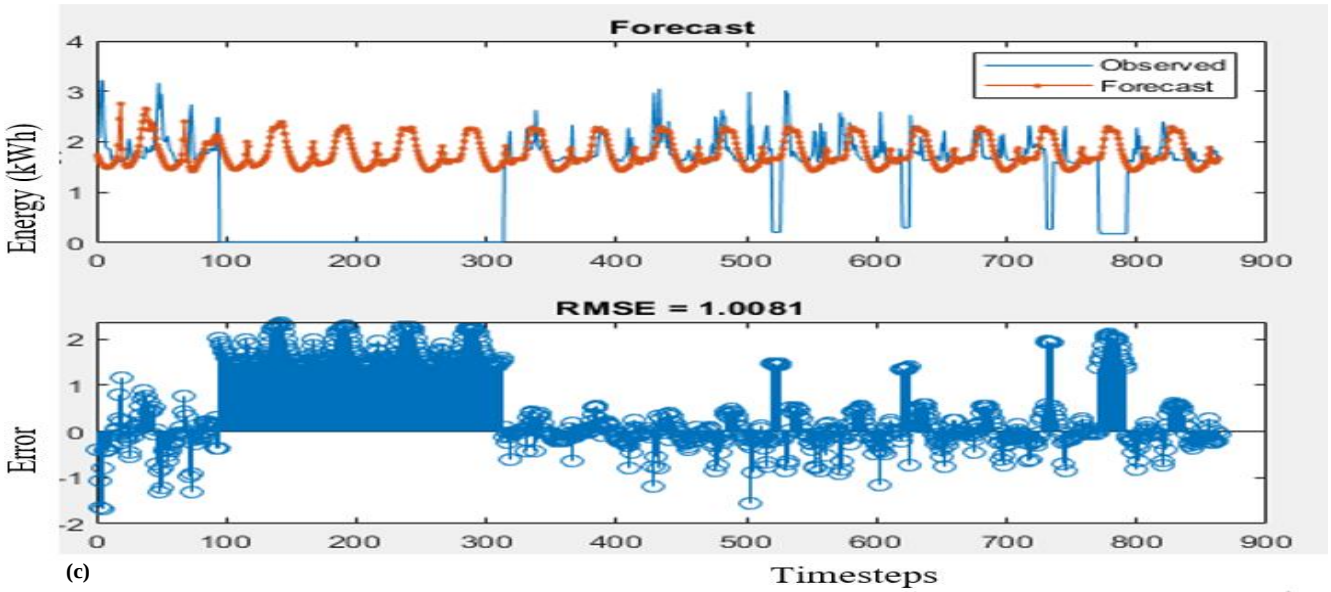
Figure 8 Forecast of the first 10% for (a) consumer 1 (b) Consumer 2 (c) Consumer 3 and (d) Consumer 4.



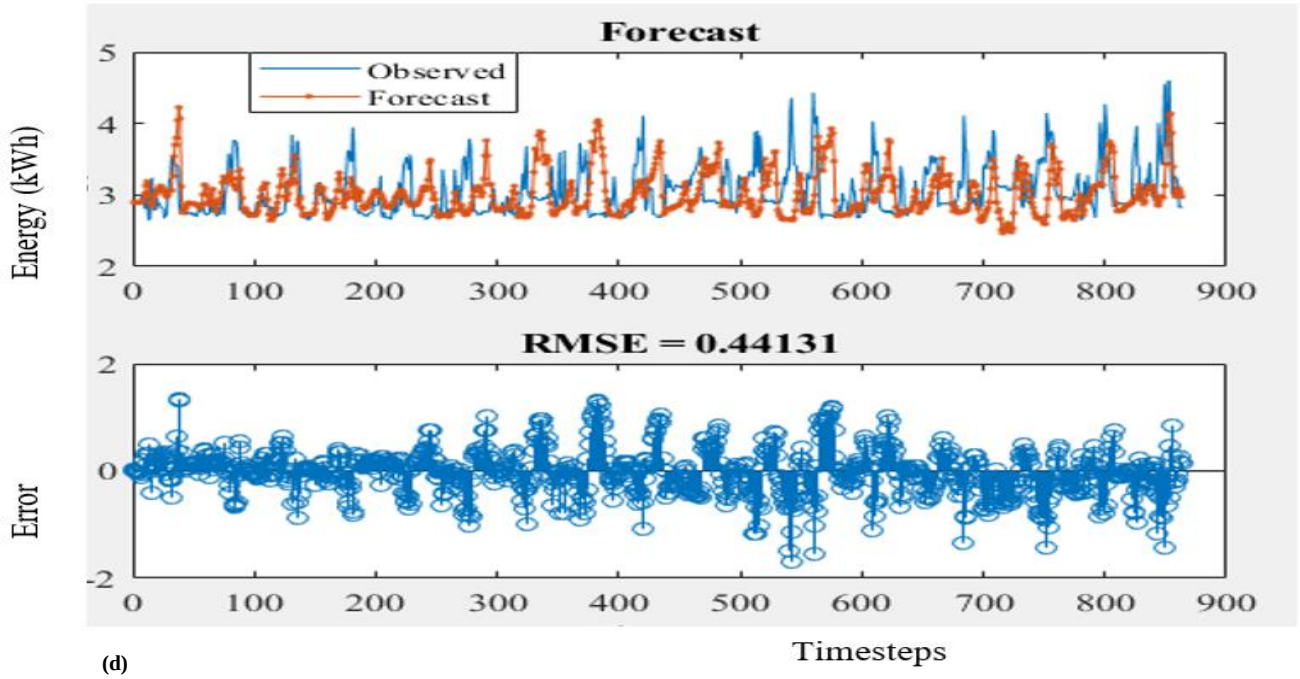
(a)



(b)

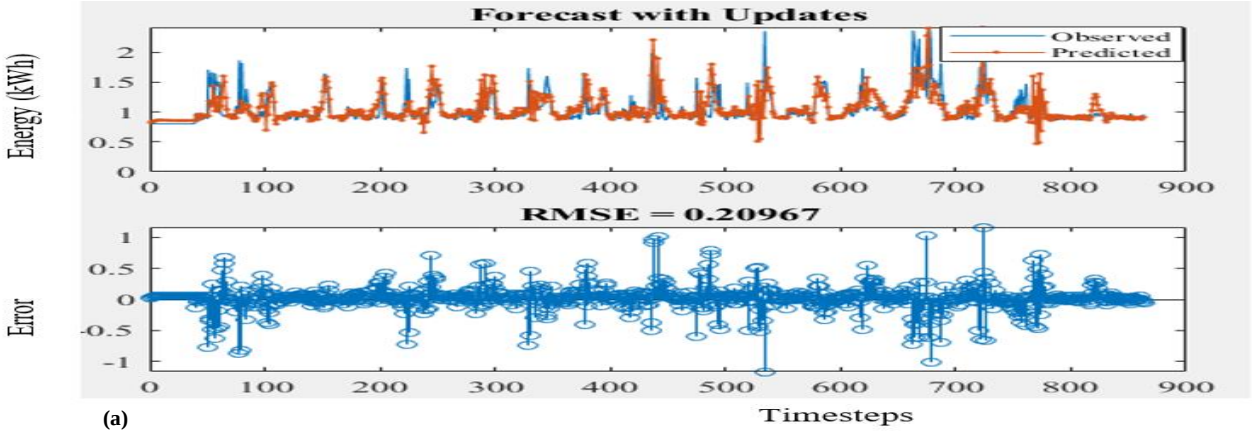


(c)



(d)

Figure 9 Comparisons of the first 10% forecast with the observed test values of (a) Consumer 1 (b) Consumer 2 (c) Consumer 3 and (d) Consumer 4



(a)

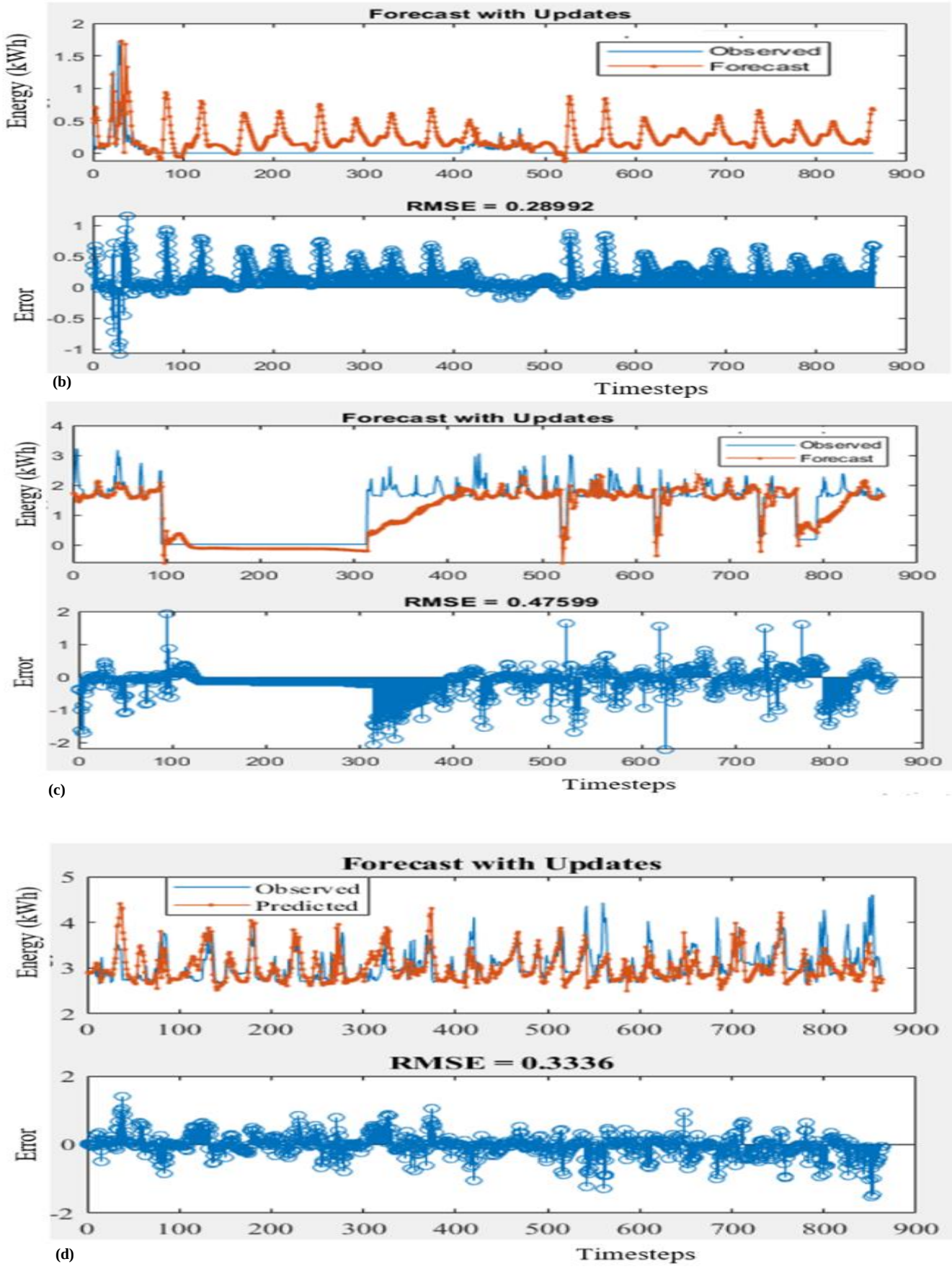


Figure 10 Updated forecast compared with the observed test profiles of (a) Consumer 1 (b) Consumer 2 (c) Consumer 3 (d) Consumer 4.

Table 5 Suspicious fraudulent consumption status during the first forecast

CID	Reported Timesteps	P_{Er}	E_S	E_{CA}	Suspicious status
1	> 450th	Positive	1	1	True
2	> 55th	Positive	1	1	True
3	> 95	Positive	1	1	True
4	None	Negative	0	0	False

Table 6 Suspicious fraudulent consumption status during the updated forecast

CID	Reported Timesteps	P_{Er}	E_S	E_{CA}	Suspicious status
1	None	Negative	0	0	False
2	> 80th	Positive	1	1	True
3	320th to 400th	Positive	1	1	True
4	None	Negative	0	0	False

Table 7 The implemented set rules for the developed fuzzy inference system model for electricity theft confirmation

S/No.	Defined Rules for the Model			
	If			Then
	α	δ	E_CA	ETCM Output
1	Low	Low	Low	False
2	Low	Low	High	False
3	Low	High	Low	False
4	Low	High	High	True
5	High	Low	Low	False
6	High	Low	High	True
7	High	High	Low	True
8	High	High	High	True

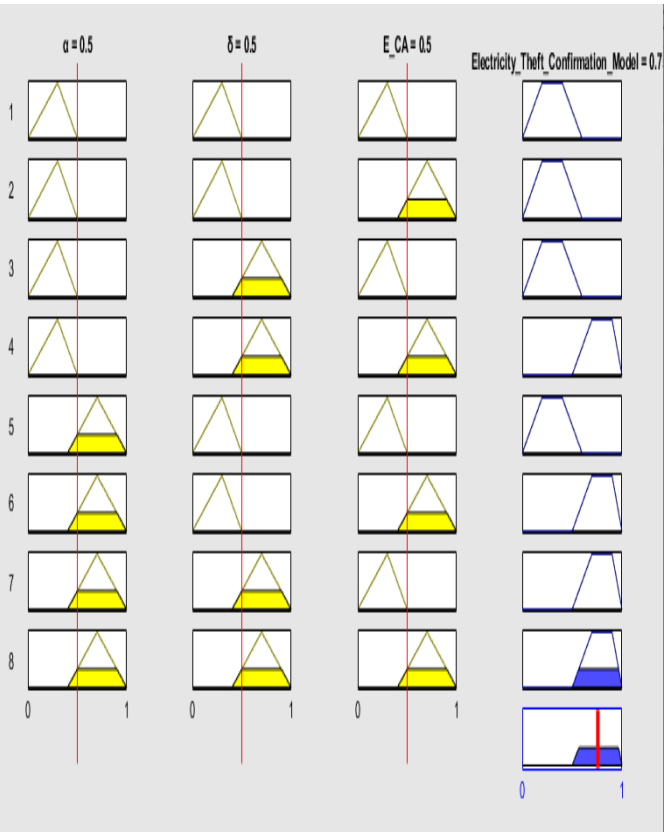


Figure 11 Rules implementation of the fuzzy inferences system-based electricity theft confirmation model

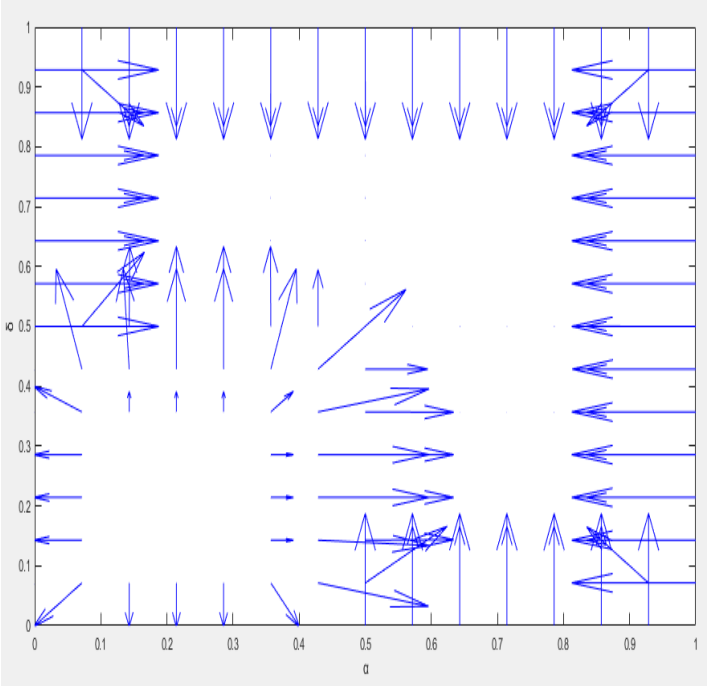


Figure 12 Model dependency of the intrusion and observer meter status error on electricity theft confirmation model

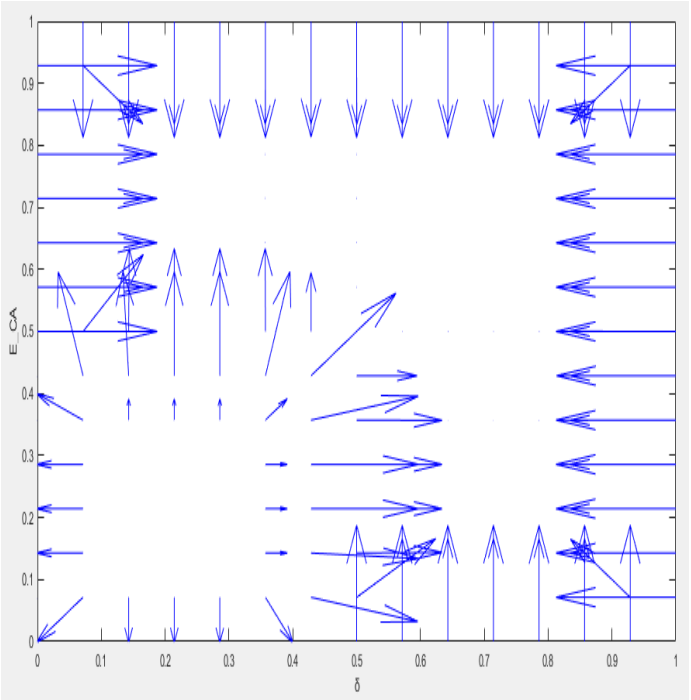


Figure 13 Model dependency of the observer meter status error and anomaly detection status on electricity theft confirmation model

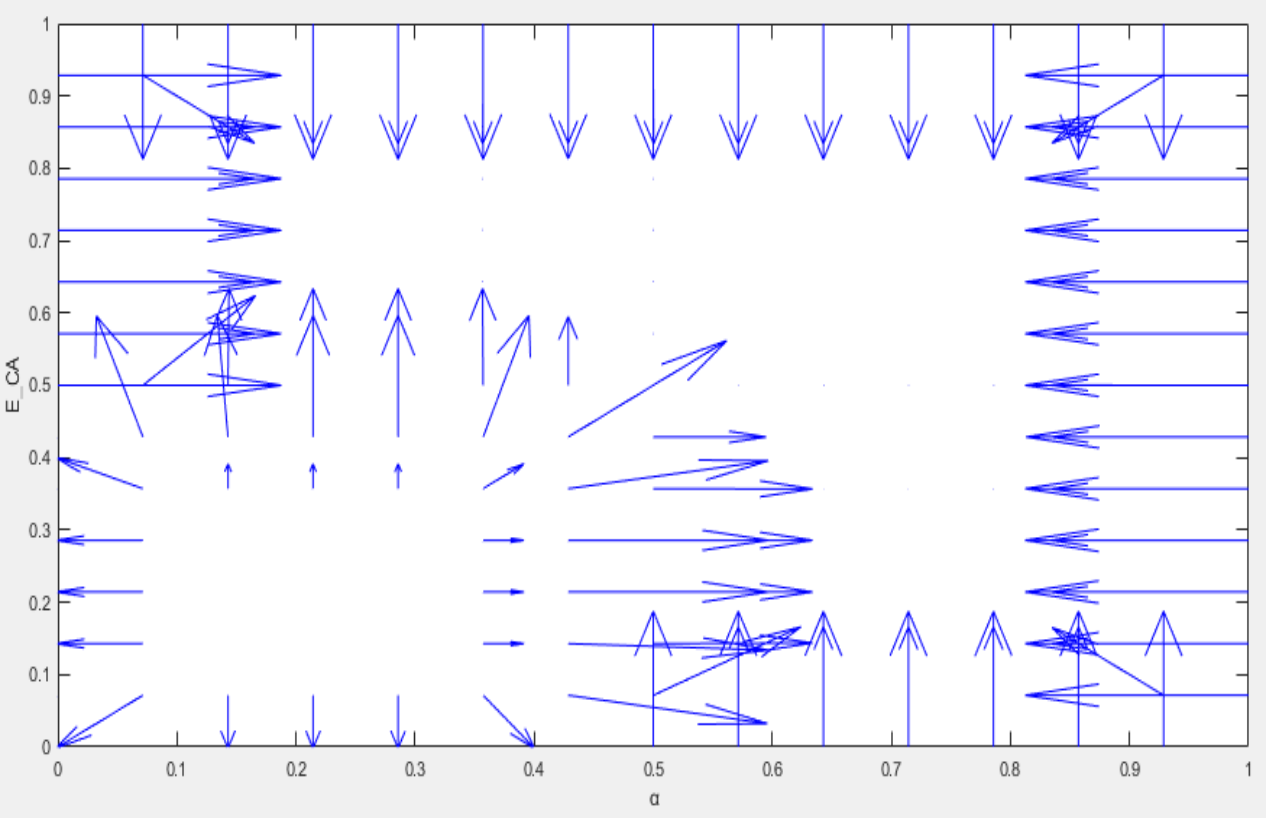


Figure 14 Model dependency of the intrusion and observer meter status error on electricity theft confirmation model.

respective intrusion status. During the first forecast, Consumers 1 and 4 were not confirmed fraudulent while consumers 2 and 3 were confirmed fraudulent when there is no intrusion reported (Table 8). At reported intrusions (Table 9), only Consumer 4 was free from fraud. At no intrusion, Consumers 1 and 4 were not confirmed fraudulent irrespective of the observer meter status while Consumers 2 and 3 posed mixed status depending on the observer meter status (Table 10). Meanwhile, during the updated forecast, Consumers 1 and 4 were confirmed depending on the observer meter status but Consumers 2 and 3 remain confirmed fraudulent irrespective of the observer meter status for all positive intrusion status (Table 11).

Table 8 Confirmed fraudulent consumers during the first forecast (with α = Negative for all instances)

CID	Reported Timesteps	Λ	E_{CA}	Confirmed status
1	> 450th	0	1	False
2	> 55th	1	1	True
3	> 95th	1	1	True
4	None	0	0	False

Table 9 Confirmed FEC during the first forecast (with α = Positive for all instances)

CID	Reported Timesteps	δ	E_{CA}	Confirmed status
1	> 450th	0	1	True
2	> 55th	1	1	True
3	> 95th	1	1	True
4	None	0	0	False

Table 10 Confirmed status of FEC during the updated Forecast (with α = Negative for all instances)

CID	Reported Timesteps	Λ	E_{CA}	Suspicious status
1	None	0	0	False
1	None	1	0	False
2	> 80th	0	1	False
2	> 80th	1	1	True
3	320th to 400th	0	1	False
3	320th to 400th	1	1	True
4	None	0	0	False
4	None	1	0	False

Table 11 Confirmed status of FEC during the updated forecast (with α = Positive for all instances)

CID	Reported Timesteps	Λ	E_{CA}	Suspicious status
1	None	0	0	False
1	None	1	0	True
2	> 80th	0	1	True
2	> 80th	1	1	True
3	320th to 400th	0	1	True
3	320th to 400th	1	1	True
4	None	0	0	False
4	None	1	0	True

In all cases, Consumer 4 consistently exhibits honest behaviour, whereas Consumer 1's honesty depends on factors beyond energy consumption data. Consumers 2 and 3 present heightened threats to the system, being implicated in nearly all modelled parameter statuses. Since tampered data for Consumers 2 and 3 were successfully detected, the effectiveness of the developed models in identifying suspicious and confirmed profiles is validated. Consequently,

based on reported instances, implementing forced correction is recommended for a potential automated penalization as presented in the study by Otuoze *et al*. (2020). In summary, the study presented in this study contributes to knowledge by: (1) Reducing reliance on prediction errors for concluding theft cases; (2) Introducing a confirmation model, an advancement compared to recent studies focused solely on the detection phase; (3) Proposing a unique collective anomaly model that explores AMI monitoring parameters for anomaly detection in electricity theft; and (4) Eliminating the need for labour-intensive on-site confirmation of electricity theft. The obtained results offer a novel direction in the study of electricity theft detection, particularly in the context of AMI.

V. CONCLUSION

This study has contributed to the field by introducing effective models for detecting and confirming electricity theft within the context of Advanced Metering Infrastructure (AMI). The detection model utilized a deep Recurrent Neural Network with Long Short-Term Memory (RNN-LSTM), while a rule-based technique, Fuzzy Inference System (FIS), was employed for confirmation. The LSTM model was specifically tailored for energy consumption prediction and was applied to the energy profiles of four distinct consumers (Consumers 1, 2, 3, and 4). An anomaly detection mechanism was then devised to identify suspicious profiles by comparing the prediction error against a predefined threshold and a collectively defined anomaly. For confirmation, a model was developed to assess security risks based on the status of selected monitoring parameters inherent to the foundational AMI architecture. These parameters were meticulously modelled using FIS.

Implementing these models on the selected consumers effectively detected tampered profiles by considering the status of the modelled AMI parameters. This study contributes to the existing works on electricity theft detection in AMI by surpassing the reliance solely on prediction errors to determine instances of thefts. It also addresses the challenges associated with the impracticality of physical on-site inspections for theft confirmation within the AMI framework. In essence, our approach provides a definitive and more reliable framework for detecting and confirming fraudulent profiles within the AMI. The insights from this study will aid utility operators in more effective planning for combating electricity theft related to AMI. The results not only advance the current understanding of electricity theft detection but also open new dimensions for future research, suggesting possibilities for incorporating other expert-based systems to enhance monitoring and evaluation.

ACKNOWLEDGMENT

The Lead author appreciates the financial supports offered by the CEOs of Golden Consults Info. Tech. Company Ltd., Alh. Hamza Usman (The Talba of Ebiraland) and Smile Image Media Ltd., Alh. S. S. Asuku during the course of the study leading to this research output.

AUTHOR CONTRIBUTIONS

A. O. Otuoze: Conceptualization; Formal analysis; Funding acquisition; Investigation; Methodology; Visualization; Writing - original draft; Writing - review & editing. **M. W. Mustafa**: Conceptualization; Project administration; Resources; Supervision; Review & Editing. **U. Sultana:** Data curation; Formal analysis; Investigation; Validation; Visualization; Writing - original draft; Writing - review & editing. **E. A. Abiodun**: Data curation; Investigation; Methodology; Validation; Visualization; Writing - original draft; Writing - review & editing. **B. Jimada-Ojuolape:** Formal analysis; Investigation; Project administration; Writing - review & editing. **O. Ibrahim:** Formal analysis; Investigation; Methodology; Validation; Visualization; Writing - original draft; Writing - review & editing. **I. O. Omeiza:** Investigation; Validation; Writing - review & editing. **A. I. Abdullateef:** Investigation; Validation; Writing - review & editing.

REFERENCES

Abushnaf, J.; A. Rassau and W. Górnisiewicz. (2016). Impact on electricity use of introducing time-of-use pricing to a multi-user home energy management system. *International Transactions on Electrical Energy Systems*, *26*(5), 993-1005.

Adhikari, R. and Agrawal, R. K. (2013). An introductory study on time series modeling and forecasting. *arXiv preprint arXiv:1302.6613*.

Adil, M.; N. Javaid; Z. Ullah; M. Maqsood; S. Ali and M. A. Daud. (2020). Electricity Theft Detection Using Machine Learning Techniques to Secure Smart Grid. Conference on Complex, Intelligent, and Software Intensive Systems,

Ahmad, T.; H. Chen; J. Wang and Y. Guo. (2018). Review of various modeling techniques for the detection of electricity theft in smart grid environment. *Renewable and Sustainable Energy Reviews*, *82*, 2916-2933.

Altan, A.; S. Karasu and S. Bekiros. (2019). Digital currency forecasting with chaotic meta-heuristic bio-inspired signal processing techniques. *Chaos, Solitons & Fractals*, *126*, 325-336.

Appiah, S. Y.; E. K.kowuah; V. C. Ikpo and A. Dede. (2023). Extremely randomised trees machine learning model for electricity theft detection. *Machine Learning with Applications*, 100458.

Aungiers, J. TIME SERIES PREDICTION USING LSTM DEEP NEURAL NETWORKS. Accessed [Online] on 10th June 2019 via https://www.altumintelligence.com/articles/a/Time-Series-Prediction-Using-LSTM-Deep-Neural-Networks.

Bhat, R. R.; R. D. Trevizan; R. Sengupta; X. Li and A. Bretas. (2016). Identifying nontechnical power loss via spatial and temporal deep learning. 2016 15th IEEE International Conference on Machine Learning and Applications (ICMLA),

Blanco, M.; J. Coello; H. Iturriaga; S. Maspoch and J. Pages. (2000). NIR calibration in non-linear systems: different PLS approaches and artificial neural networks. *Chemometrics and Intelligent Laboratory Systems*, *50*(1), 75-82.

Brockwell, P. J.; R. A. Davis and M. V. Calder. (2002). *Introduction to time series and forecasting* (Vol. 2). Springer.

Brownlee, J. (2016). Time Series Prediction with LSTM Recurrent Neural Networks in Python with Keras. Accessed via https://machinelearningmastery.com/time-series-

prediction-lstm-recurrent-neural-networks-python-keras/ on 3rd March 2019.

Calderaro, V.; C. N. Hadjicostis; A. Piccolo and P. Siano. (2011). Failure identification in smart grids based on petri net modeling. *IEEE Transactions on Industrial Electronics*, *58*(10), 4613-4623.

Cárdenas, A. A.; S. Amin; G. Schwartz; R. Dong and S. Sastry. (2012). A game theory model for electricity theft detection and privacy-aware control in AMI systems. 2012 50th Annual Allerton Conference on Communication, Control, and Computing (Allerton),

Chatterjee, S.; V. Archana; K. Suresh; R. Saha; R. Gupta and F. Doshi. (2017). Detection of non-technical losses using advanced metering infrastructure and deep recurrent neural networks. 2017 IEEE International Conference on Environment and Electrical Engineering and 2017 IEEE Industrial and Commercial Power Systems Europe (EEEIC/I&CPS Europe),

Chen, Z.; D. Meng; Y. Zhang; T. Xin and D. Xiao. (2020). Electricity Theft Detection Using Deep Bidirectional Recurrent Neural Network. 2020 22nd International Conference on Advanced Communication Technology (ICACT),

Cheng, Y.; C. Xu; D. Mashima; V. L. Thing and Y. Wu. (2017). PowerLSTM: Power demand forecasting using long short-term memory neural network. International Conference on Advanced Data Mining and Applications,

Chiappini, F. A.; C. M. Teglia; Á. G. Forno and H. C. Goicoechea. (2020). Modelling of bioprocess non-linear fluorescence data for at-line prediction of etanercept based on artificial neural networks optimized by response surface methodology. *Talanta*, *210*, 120664.

Clastres, C. (2011). Smart grids: Another step towards competition, energy security and climate change objectives. *Energy policy*, *39*(9), 5399-5408.

Costa, B. C.; B. L. Alberto; A. M. Portela; W. Maduro and Eler, E. O. (2013). Fraud detection in electric power distribution networks using an ann-based knowledge-discovery process. *International Journal of Artificial Intelligence & Applications*, *4*(6), 17.

Delgado-Gomes, V.; J. F. Martins; C. Lima and P. N. Borza. (2015). Smart grid security issues. 2015 9th International Conference on Compatibility and Power Electronics (CPE),

Depuru, S. S. S. R.; L. Wang and V. Devabhaktuni. (2011). Support vector machine based data classification for detection of electricity theft. 2011 IEEE/PES Power Systems Conference and Exposition,

El-Hawary, M. E. (2014). The smart grid—state-of-the-art and future trends. *Electric Power Components and Systems*, *42*(3-4), 239-250.

Fang, H.; J.-W. Xiao and Y.-W. Wang. (2023). A machine learning-based detection framework against intermittent electricity theft attack. *International Journal of Electrical Power & Energy Systems*, *150*, 109075.

Fatemieh, O.; R. Chandra and C. A. Gunter. (2010). Low cost and secure smart meter communications using the tv white spaces. Resilient Control Systems (ISRCS), 2010 3rd International Symposium on,

Fenza, G.; M. Gallo and V. Loia. (2019). Drift-aware methodology for anomaly detection in smart grid. *IEEE Access*, *7*, 9645-9657.

Gaur, V. and Gupta, E. (2016). The determinants of electricity theft: An empirical analysis of Indian states. *Energy policy*, *93*, 127-136.

Goel, S. and Hong, Y. (2015). Security Challenges in Smart Grid Implementation. In *Smart Grid Security* (pp. 1-39). Springer.

Gu, D.; Y. Gao; K. Chen; J. Shi; Y. Li and Y. Cao. (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.

Guerrero, J. I.; C. León; I. Monedero; F. Biscarri and J. Biscarri. (2014). Improving knowledge-based systems with statistical techniques, text mining, and neural networks for non-technical loss detection. *Knowledge-Based Systems*, *71*, 376-388.

Handique, M. L.; Q. Kalita. and G. Das. (2019). Design and Simulation of Electricity Theft Detection in Radial Distribution System. *ADBU Journal of Electrical and Electronics Engineering (AJEEE)*, *3*(2), 44-49.

Haq, E. U.; C. Pei; R. Zhang; H. Jianjun and F. Ahmad. (2023). Electricity-theft detection for smart grid security using smart meter data: A deep-CNN based approach. *Energy Reports*, *9*, 634-643.

Hasan, M.; R. N. Toma; A.-A. Nahid; M. Islam and J.-M. Kim. (2019). Electricity Theft Detection in Smart Grid Systems: A CNN-LSTM Based Approach. *Energies*, *12*(17), 3310.

Haviv, D.; A. Rivkind and O. Barak. (2019). Understanding and Controlling Memory in Recurrent Neural Networks. *arXiv preprint arXiv:1902.07275*.

Hochreiter, S. (1998). The vanishing gradient problem during learning recurrent neural nets and problem solutions. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, *6*(02), 107-116.

Hu, T.; Q. Guo; X. Shen; H. Sun; R. Wu and H. Xi. (2019). Utilizing Unlabeled Data to Detect Electricity Fraud in AMI: A Semisupervised Deep Learning Approach. *IEEE transactions on neural networks and learning systems*.

Huang, Q., Tang, Z., Weng, X., He, M., Liu, F., Yang, M. and Jin, T. (2024). A Novel Electricity Theft Detection Strategy Based on Dual-Time Feature Fusion and Deep Learning Methods. *Energies*, *17*(2), 275.

Ismail, M., Shaaban, M. F., Naidu, M. and Serpedin, E. (2020). Deep Learning Detection of Electricity Theft Cyber-attacks in Renewable Distributed Generation. *IEEE Transactions on Smart Grid*.

Jamil, F. and Ahmad, E. (2014). An empirical study of electricity theft from electricity distribution companies in Pakistan. *The Pakistan Development Review*, 239-254.

Jiang, R.; R. Lu; Y. Wang; J. Luo; C. Shen and X. S. Shen. (2014). Energy-theft detection issues for advanced metering infrastructure in smart grid. *Tsinghua Science and Technology*, *19*(2), 105-120.

Jindal, A.; A. Dua; K. Kaur; M. Singh; N. Kumar and S. Mishra. (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. (2015). *Detection of malicious activities against advanced metering infrastructure in smart grid* University of British Columbia].

Karasu, S. and Altan, A. (2019). Recognition Model for Solar Radiation Time Series based on Random Forest with Feature Selection Approach. 2019 11th International Conference on Electrical and Electronics Engineering (ELECO),

Kim, J.; I. Kang; M. El-Khamy and J. Lee. (2019). System and method for higher order long short-term memory (LSTM) network. In: Google Patents.

Kim, S.; G. Lee; G.-Y. Kwon; D.-I. Kim and Y.-J. Shin. (2018). Deep Learning Based on Multi-Decomposition for Short-Term Load Forecasting. *Energies*, *11*(12), 3433.

Kocaman, B. and Tümen, V. (2020). Detection of electricity theft using data processing and LSTM method in distribution systems. *Sādhanā*, *45*(1), 1-10.

Krishna, V. B.; R. K. Iyer and W. H. Sanders. (2015). ARIMA-based modeling and validation of consumption readings in power grids. International Conference on Critical Information Infrastructures Security.

Krishna, V. B.; K. Lee; G. A. Weaver; R. K. Iyer and W. H. Sanders. (2016). F-DETA: A framework for detecting electricity theft attacks in smart grids. Dependable Systems and Networks (DSN), 2016 46th Annual IEEE/IFIP International Conference on,

Le, X.-H.; H. V. Ho; G. Lee. and S. Jung. (2019). Application of Long Short-Term Memory (LSTM) Neural Network for Flood Forecasting. *Water*, *11*(7), 1387.

LondonDataStore. (2015). SmartMeter Energy Consumption Data in London Households. accessed [Online] on 20 July 2018 via https://data.london.gov.uk/dataset/smartmeter-energy-use-data-in-london-households.

Lu, X.; Y. Zhou; Z. Wang; Y. Yi; L. Feng and F. Wang. (2019). Knowledge Embedded Semi-Supervised Deep Learning for Detecting Non-Technical Losses in the Smart Grid. *Energies*, *12*(18), 3452.

Maamar, A. and Benahmed, K. (2019). A Hybrid Model for Anomalies Detection in AMI System Combining K-means Clustering and Deep Neural Network.

Madhure, R. U.; R. Raman and S. K. Singh. (2020). CNN-LSTM based Electricity Theft Detector in Advanced Metering Infrastructure. 2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT),

Mashima, D. and Cárdenas, A. A. (2012). Evaluating electricity theft detectors in smart grid networks. International Workshop on Recent Advances in Intrusion Detection,

McLaughlin, S.; D. Podkuiko and P. McDaniel. (2009). Energy theft in the advanced metering infrastructure. International Workshop on Critical Information Infrastructures Security,

Mohammad, N.; A. Barua and M. A. Arafat. (2013). A smart prepaid energy metering system to control electricity theft. International Conference on Power, Energy and Control (ICPEC), 2013. 562-565,

Moretti, M.; S. N. Djomo; H. Azadi; K. May; K. De Vos; S. Van Passel and N. Witters. (2017). A systematic review of environmental and economic impacts of smart grids. *Renewable and Sustainable Energy Reviews*, *68*, 888-898.

Mukhopadhyay, S.; M. Sahni; A. Chauhan; N. Kumari; R. C. Singh; M. Kumar; Alheety M. A. and Aldbea, F. W. (2023). An Optimized Method for Detecting Unauthorized Power Consumption. Macromolecular Symposia,

Musungwini, S. (2016). A framework for monitoring electricity theft in Zimbabwe using mobile technologies. *Journal of Systems Integration*, *7*(3), 54.

Nabil, M.; M. Ismail; M. Mahmoud; M. Shahin; K. Qaraqe and E. Serpedin. (2019). Deep learning-based detection of electricity theft cyber-attacks in smart grid AMI networks. In *Deep Learning Applications for Cyber Security* (pp. 73-102). Springer.

Nabil, M.; M. Ismail; M. M. Mahmoud; W. Alasmary and E. Serpedin. (2019). PPETD: Privacy-Preserving Electricity Theft Detection Scheme With Load Monitoring and Billing for AMI Networks. *IEEE Access*, *7*, 96334-96348.

Nabil, M.; M. Mahmoud; M. Ismail and E. Serpedin. (2019). Deep Recurrent Electricity Theft Detection in AMI Networks with Evolutionary Hyper-Parameter Tuning. 2019 International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData),

Nagi, J.; K. S. Yap; S. K. Tiong; S. K. Ahmed and A. Mohammad. (2008). Detection of abnormalities and electricity theft using genetic support vector machines. TENCON 2008-2008 IEEE Region 10 Conference,

Otuoze, A. O.; M. W. Mustafa; A. T. Abdulrahman; O. O. Mohammed and S. Salisu. (2020). Penalization of electricity thefts in smart utility networks by a cost estimation-based forced corrective measure. *Energy policy*, *143*, 111553.

Otuoze, A. O.; M. W. Mustafa; A. E. Abioye; U. Sultana; A. M. Usman; O. Ibrahim; I. O. A. Omeiza and A. Abu-Saeed. (2022). A rule-based model for electricity theft prevention in advanced metering infrastructure. *Journal of Electrical Systems and Information Technology*, *9*(1), 1-17.

Pamir; N. Javaid; M. U. Javed; M. A. Houran; A. M. Almasoud and M. Imran. (2023). Electricity theft detection for energy optimization using deep learning models. *Energy Science & Engineering*, *11*(10), 3575-3596.

Salinas, S. A. and Li, P. (2016). Privacy-preserving energy theft detection in microgrids: A state estimation approach. *IEEE Transactions on Power Systems*, *31*(2), 883-894.

Sharma, T.; K. Pandey; D. Punia and J. Rao. (2016). Of pilferers and poachers: Combating electricity theft in India. *Energy Research & Social Science*, *11*, 40-52.

Shehzad, F.; N. Javaid; S. Aslam and M. U. Javaid. (2022). Electricity theft detection using big data and genetic algorithm in electric power systems. *Electric Power Systems Research*, *209*, 107975.

Shuaib, K.; Z. Trabelsi; M. Abed-Hafez; A. Gaouda and Alahmad, M. (2015). Resiliency of Smart Power Meters

to Common Security Attacks. *Procedia Computer Science*, *52*, 145-152.

Siboni, S. and Cohen, A. (2014). Botnet identification via universal anomaly detection. Information Forensics and Security (WIFS), 2014 IEEE International Workshop on,

Sun, Y.; J. Lee; S. Kim; J. Seon; S. Lee; C. Kyeong and J. Kim. (2023). Energy Theft Detection Model Based on VAE-GAN for Imbalanced Dataset. *Energies*, *16*(3), 1109.

Takiddin, A.; M. Ismail; M. Nabil; M. M. Mahmoud and E. Serpedin. (2020). Detecting Electricity Theft Cyber-Attacks in AMI Networks Using Deep Vector Embeddings. *IEEE Systems Journal*.

Takiddin, A.; M. Ismail; U. Zafar and E. Serpedin. (2022). Deep autoencoder-based anomaly detection of electricity theft cyberattacks in smart grids. *IEEE Systems Journal*, *16*(3), 4106-4117.

Tawfik, M. (2003). Linearity versus non-linearity in forecasting Nile River flows. *Advances in Engineering Software*, *34*(8), 515-524.

Tehrani, S. O.; M. H. Y. Moghaddam and M. Asadi. (2020). Decision Tree based Electricity Theft Detection in Smart Grid. 2020 4th International Conference on Smart City, Internet of Things and Applications (SCIOT),

Toma, R. N.; M. N. Hasan; A.-A. Nahid and B. Li. (2019). Electricity theft detection to reduce non-technical loss using support vector machine in smart grid. 2019 1st International Conference on Advances in Science, Engineering and Robotics Technology (ICASERT),

Uparela, M. A.; M. Gonzalez; J. R. Jimenez and C. G. Quintero. (2018). Intelligent system for non-technical losses management in residential users of the electricity sector. *Ingeniería e Investigación*, *38*(2), 52-60.

Wang, Y.; Q. Chen and C. Kang. (2020). Electricity Theft Detection. In *Smart Meter Data Analytics* (pp. 79-98). Springer.

Xia, R.; Y. Gao; Y. Zhu; D. Gu and J. Wang. (2023). An attention-based wide and deep CNN with dilated convolutions for detecting electricity theft considering imbalanced data. *Electric Power Systems Research*, *214*, 108886.

Xu, L.; Z. Shao and F. Chen. (2023). A combined unsupervised learning approach for electricity theft detection and loss estimation. *IET Energy Systems Integration*.

Zhang, D.; X. Han and C. Deng. (2018). Review on the research and practice of deep learning and reinforcement learning in smart grids. *CSEE Journal of Power and Energy Systems*, *4*(3), 362-370.

Zhao, Z.; Y. Liu; Z. Zeng; Z. Chen and H. Zhou. (2023). Privacy-Preserving Electricity Theft Detection based on Blockchain. *IEEE Transactions on Smart Grid*.

Zheng, Z.; Y. Yang; X. Niu; H.-N. Dai and Y. Zhou. (2017). Wide and deep convolutional neural networks for electricity-theft detection to secure smart grids. *IEEE Transactions on Industrial Informatics*, *14*(4), 1606-1615.