Received: October 7, 2024. Revised: December 10, 2024.

INASS

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

Robust Electricity Theft Detection in Smart Grids Using Machine Learning and Secure Techniques

Ihsan H. Abdulqadder[1]* Israa T. Aziz[2] Firas M. F. Flaih[3]

[1]*Department of Computer Science, University of Kirkuk, Kirkuk, Iraq*
[2]*Computer Center, University of Mosul, Mosul, Iraq*
[3]*State Company of North Distribution Electricity, Ministry of Electricity, Iraq*
* Corresponding author's Email: ihsan.hussein@uokirkuk.edu.iq

Abstract: Theft of electricity is an increasingly common problem that has a detrimental effect on utility providers as well as power consumers. It affects consumers' high energy costs, creates electric risks, and affects the electric utility industry's capacity to grow economically. The biggest issue facing smart grids is the theft of electricity. In order to monitor loads and regulate energy usage, smart meters (SMs) are installed at the end of customers' residences and are used to periodically transmit fine-grained power consumption measurements to the supplier. Due to nonlinear correlations and missing values, existing theft detection techniques have difficulty processing large electrical usage information. An integrated system for coordinating the examination of electrical demand data is also absent. To address these limitations in this research we propose a new electricity theft detection framework to further enhance the system reliability and fault tolerance. Initially, we utilize the quantum key distribution (QKD) with the rolling optimization strategy (ROS) to reduce the computational overhead and efficiently minimize the fluctuations. After that extreme gradient boosting (EGB) and coati optimization algorithm (COA) are employed for classification. Finally, we proposed privacy functionality trade-off strategies for smart meters to improve the consumer trust and confidence in the smart grid system. Thus, the proposed new electricity theft detection framework to further enhance the system reliability and fault tolerance method's simulation in Matlab-R2023a\Simulink demonstrates superior performance compared to existing techniques. The approaches in this study to overcome the issues faced in previous technologies are tested using different metrics of authentication rate at 98(%), accuracy at 99 (%), detection rate at 98.6 (%), precision at (97%), recall at (98.6%), at F1-score (95.15%), and AUC at (0.3123).

Keywords: Smart grid, Electricity theft detection, Quantum key distribution, Rolling optimization strategy, Extreme gradient boosting, Coati optimization algorithm.

1. Introduction

Nowadays, practically everyone has access to and is impacted by electricity, making it an essential element of human life. Considering how widely it is used worldwide, there are several serious problems that need to be addressed, such as electrical loss [1, 2]. In order to increase the electricity grid's dependability, efficiency, and resilience, the smart grid vision incorporates sensing, computing, and communication into its functioning. The smart grid's advanced metering infrastructure (AMI) is a crucial component. Smart meters (SMs) are installed at the customers' locations in AMI in order to monitor and provide the system operator (SO) with precise measurements of their power use. In order to control the supply of power in real-time, these readings are utilized to estimate the future load or energy demand. In order to balance the supply and demand of energy, they are also used to support dynamic billing, in which the price of power varies throughout the day to incentivize customers to cut back on usage during peak hours [3, 4].

By incorporating novel sensing, communication, and control strategies, smart grids improve the long-term viability, dependability, and effectiveness of electrical infrastructure. They also enable renewable

energy sources and modernize demand response programs. However revolutionary benefits have new difficulties specifically in the realms of fraud detection and security [5, 6]. "Non-Technical Losses" (NTL) and "Technical Losses" (TL) are the two categories into which losses of electricity in power systems are separated [7]. NTLs are seen as a key difficulty in the smart grid and may significantly affect the extent to which power systems operate and are managed. Additionally, it raises costs, which has an impact on the utilities' financial performance [8,9]. Energy theft, out of all NTLs, has always been a major problem for utilities globally since it contributes significantly to total losses. The intentional or unauthorized consumption of electrical power through a variety of methods is referred to as energy theft [10, 11].

The quantity of energy used that is not paid to customers is known as electricity theft. Energy theft can be caused by a variety of circumstances, including high power prices and unfavourable economic conditions. Through physical or cyberattacks, malicious persons can readily corrupt smart meters in the neighbourhood. As a result, there has long been a broad understanding that AMI installations require a fraud detection approach [12, 13]. The smart grid's theft problem can potentially have a big impact on society and the economy. Customers' right to privacy can also be damaged when sensitive customer data is stolen or altered during the transit of important data across the many smart grid networks [14-16]. Other techniques have been presented in [17, 18] to overcome the issue of smart grid security.

Energy providers have historically used rule-based algorithms, physical inspections, and recurring audits to find cases of energy theft. Nevertheless, these techniques are often laborious, costly, and unproductive in detecting complex fraudulent activity. Furthermore, the sheer amount and velocity of data created by smart meters, detectors, and other network components make it harder and harder to identify and counteract fraudulent conduct using conventional methods as smart grids become more sophisticated and linked.

In this paper, we utilize the QKD with a rolling optimization strategy (ROS) to reduce the computational overhead and efficiently minimize the fluctuations. After that Extreme gradient boosting (EGB) and coati optimization algorithm (COA) are employed for classification, and then to improve consumer trust and confidentiality in the system the monitoring activities within the smart grid must maintain the balance between functionality and privacy by using smart meters provides with privacy functionality trade-off strategies.

Even though many researchers have done electricity theft and fraud detection in the grid there are still a lot of unresolved problems is existing. The primary problems are mentioned below:

Inaccurate Classification: In the existing research their model performance leads to the misclassification of electricity detection.

Lack of False Alarms*:* The previous research lacks data on the infrequent occurrence of theft in detecting energy theft (ETD) that reduces the classification accuracy and leads the false alarms.

Privacy intrusion in granularity of data: In the existing method they have challenges in data that lead the privacy intrusion and raise the ethical and regulatory concerns regarding consumer data protection.

In this paper, we develop a robust electricity theft and fraud detection system for the smart grid using machine learning techniques. The salient features of the proposed work are,

- To implement and analyze the robust techniques to minimize the sensitivity of the system fluctuation in input data that enhance the detection accuracy.
- To optimize the information sharing protocols to reduce the computational overhead associated with data transmission and processing that ensure the efficient operation of the detection system.
- To integrate the techniques to handle the infrequent instances of theft in electricity theft detection, reducing the false alarms and enhancing the overall classification accuracy.
- To design a balance between the granularity of electricity consumption and data for detection purposes while respecting consumer privacy to improve data security and user trust.

The highlights of the research work are illustrated as (1) The QKD-ROS is used to secure communication, reduce computational overhead, and minimize fluctuations within the smart grid. (2) EGB-COA is employed for high-accuracy classification of electricity theft with the generative adversarial network (GAN) to reduce false alarms and improve detection accuracy. (3) Smart meters with privacy functionality trade-off strategies balance effective monitoring with privacy intrusion prevention, ensuring consumer trust and confidentiality in the smart grid system.

The remaining part of this research is organized as follows: Section 2 provides an explanation of the survey of current works, which includes research gaps. Section 3 outlines the primary problem with the

existing approaches. Section 4 presents the research methodology for the recommended technique together with the relevant diagrams, mathematical representation, and pseudocode. In Section 5, the experimental results are explained and the suggested and current methodologies are compared. The proposed work conclusion is presented in Section 6.

2. Literature survey

This section deals with the survey of literature on electricity theft and fraud detection in smart grid. This section additionally consists of the research gap of these previous methods.

Authors in [19] provide a hybrid deep learning model that takes into account the aforementioned issues in order to identify power thieves in smart grids with high accuracy. First, techniques for pre-processing are used to clean up the smart meter data. Subsequently, the feature extraction approach tackles the problem of dimensionality, much like AlexNet. A genuine dataset of Chinese intelligent meters is used in simulations to assess the efficacy of the suggested approach. A number of benchmark models are also used in order to do a comparison study. However, in their research, their proposed methods have challenges in long training time and computational complexity. The author of [20] presents an "ensemble model based on "convolutional neural network and extreme gradient boosting" (CNN-EGB) model". The CNN model in this framework receives input from both 1-D and 2-D power usage data. The proposed model outperformed the current approaches in detecting power theft, with a success rate of 92%. The model's capacity to identify theft is restricted as it was learning on a "small number of datasets" without the inclusion of further non-sequential parameters. "Low-sampled data" is also given, which affects the suggested model's efficiency while providing more precise information on energy theft. We will thus take into account high-sampling data as well as other non-sequential data for the trustworthy identification of energy thieves in years to come.

The resilience of power theft detectors against evasion assaults is examined in research [21]. By inserting adversarial samples, these assaults deceive the power theft detectors and lower the reported reading levels. We provide powerful evasion techniques that generate adversarial models repeatedly based on an electrical measurement and its nearby interpretations, fooling the benchmark detectors. Utilizing "white, gray, and black-box" environments, depending on the malicious awareness of the indicator's characteristics, we investigate the effects of evasion assaults. Furthermore, in their research, their detection performance is not stable due to the white box environment. The study of [22] goal is to create a model for machine learning (ML) with the understanding that the six information balancing techniques "Adaptive Synthetic Sampling" (ADASYN), SVM-"Synthetic Minority over Sampling", "Random over Sampler", "SMOTEENN", and "SMOTE Tomek Links" are used to address the issue of data imbalance. The two steps make up the intended model. Their proposed work theft detection affects the privacy of customers.

In the author of [23], a new ETD technique is used to identify power theft occurring in SGs. The methods included in the suggested methodology include "logit boosting (LogitBoost), BiLSTM, k-nearest neighbor oversampling (KNNOR), and recursive feature elimination (RFE)". Moreover, a "BiLSTM-LogitBoost stacking ensemble model" is created by combining 3 "BiLSTM networks with a LogitBoost model". The approach presented for ETD consists of four main stages: data preparation, choosing features, data balance, and categorized electricity theft. The research [24] thus suggests a technique that may be used to identify energy theft with greater accuracy while using fewer characteristics. The most effective way to choose the characteristics that are more important for detecting power theft is determined by analyzing several extractions of features and selection approaches. Selection of features and extraction techniques including Principal Component Analysis, mutual data, and low volatility filtering are used in a variety of investigations. A variety of classifiers based on ML are used. However, their proposed method becomes annotated which needs to improve the classification task.

In order to balance the dataset, research [25] presents a new technique that initially used a "time series generative adversarial network" to create synthetic data for consumers who had stolen power. After that, the characteristics of the consumers were extracted using a "hybrid multi-time-scale neural network-based model", and detection was accomplished by using a "CatBoost classifier". However, in their research, the proposed work leads an excessive learning time, increasing computation costs, and complications in the ideal decision method. The paper suggests a "deep reinforcement learning" (DRL) method as a possible remedy for the issue of electricity theft. As an environment, real dataset samples are used, and incentives are given according to how well training detects faults. Specifically, four distinct situations are described for the suggested technique. Initially, a "deep Q network" (DQN) and a "double deep Q network" (DDQN) with various

deep neural network designs are used to build a global detection model. Secondly, a customized detection model for new customers is generated by using the global detector in order to get high detection accuracy and prevent zero-day violence. Third, the third scenario takes into account altering the current clients' consumption patterns [26].

3. Problem statement

In this section, the explicit works that already exist and the solutions that correspond to them are presented in sequential order. In addition, this study also offers responses for the specific problems. The specific research works and issues are:

Article [27] proposes a multi-layer perceptron (MLP) method using gated recurrent units (GRU). The suggested hybrid system makes use of data from the Chinese national grid corporation (CNGC) for analysis and solving of power theft. First, prepare the data in the suggested hybrid system. Next, use the k-means synthetic minority oversampling technique (SMOTE) to balance the data. Finally, apply a GTU model and the MLP framework to the obtained purified data. In conclusion, assess the suggested system's achievement using various performance metrics, including visual evaluation and statistical analysis. Three distinct ratios are used for preparing and evaluating the dataset in order to confirm the reliability of our suggested hybrid method.

- The model's capacity to detect even the smallest patterns in electricity usage is limited because it can only be developed with "high-frequency data on electricity consumption". As a result, there are more instances of misclassification, and its accuracy was also decreased.

Authors of [28] suggest a new method for detecting energy theft in electric power systems using big data that is based on blurring autoencoder and metaheuristic approaches. While the latter is used for obtaining high variance characteristics from power usage data, both of them are used to identify notable features. First, eleven new features are combined based on the user's use of the past, using electrical and statistical data. Then, to identify a subset of ideal characteristics, the artificially generated features are fed into metaheuristic algorithms. The best features are ultimately fed as information into the demising autoencoder in order to gather features with a high variance. How successfully autoencoder and metaheuristic techniques select and extract features is measured using a support vector machine (SVM). The overfitting, preservation, and computing costs of ML classifiers are decreased by the suggested solution.

- However, in their research, it lacks of infrequent availability of theft in ETD that decreases the classification accuracy and false alarms.

For the purpose of ETD, a unique extreme gradient boosting (XGBoost) based model is suggested. This model analyzes the power consumption patterns of the users. Six distinct artificially generated theft assaults were used in order to eliminate the imbalance in the realm "power consumption dataset" and guarantee a fair dissemination of theft and non-theft data instances. Additionally, the use of the XGBoost algorithm for classification produced excellent accuracy rates and a low incidence of false positives, particularly in identifying purposeful cases of energy theft [29]. The suggested model uses power consumption data and other characteristics as input features to identify electricity theft that is unique to the areas.

- However, customers' privacy will be violated due to the great granularity of electricity consumption data.

Research Solution: By using QKD keys, the computational cost associated with smart grid communication authentication is decreased. Smart grid sensitivity instability is reduced with the application of ROS approach. To decrease variability and reduce computational cost, QKD-ROS integration is utilized. When classifying electricity detection, EGB is employed to increase classification accuracy. Through the use of COA, classification performance is enhanced, maximizing accuracy. To reduce false alarms and increase classification accuracy, a GAN is employed. Customers can avoid privacy invasion by using a smart meter that uses a privacy-functionality trade-off strategy.

4. Proposed method

A The research goal is to develop a robust electricity theft and fraud detection system for the smart grid using machine learning techniques. Fig. 1 depicts the whole structure of the suggested approach. The key aspects of the proposed model are

- Secure smart grid fluctuation
- Electricity theft and Fraud detection
- Monitoring

4.1 Secure smart grid fluctuation

To overcome the fluctuations and prevent unauthorized access. The QKD keys are employed to improve the authentication security while minimizing computational overhead. The security measures are accompanied by ROS to design to minimize the

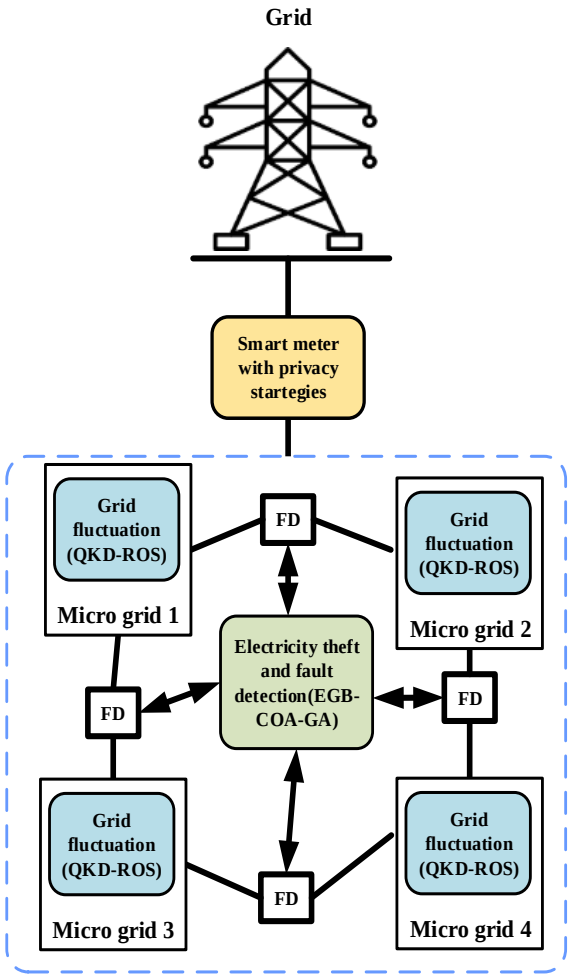

Figure. 1 Overall architecture of the proposed work

sensitive fluctuation within the smart grid further improving the stability and reliability.

4.1.1. Quantum key distribution

For every pair of nodes connected by QKD connections, we believe that paired secret keys are constantly created. Decentralized QKD provides a powerful solution to enhance the security of communications in smart grids by providing a secure value exchange and authentication mechanism. QKD is a technology that uses the principles of quantum mechanics to securely distribute encryption keys between parties. QKD's security is based on quantum physics principles such as the Heisenberg Uncertainty Principle and quantum entanglement to ensure that any eavesdropping attempts are testable.

4.1.2. Rolling optimization strategy

Initially, a methodical description of the energy trigger mechanism for *sc* is provided. Subsequently, the microgrid operation optimization concept is completely introduced. Ultimately, a thorough four-part description of a unique ROS algorithm is provided.

Energy trigger mechanism for sc: In a typical microgrid ($\mathfrak{MG}$), three uncertainties are taken into account: load demand ($\mathcal{L}_d$), wind turbine ($\mathcal{W}t$), and photovoltaic cell ($\mathcal{P}\mathbb{v}$) output. Eq. (1), which defines the low-frequency component of the conventional net load $\mathfrak{F}_{net}^{\mathcal{T}}$, must be anticipated prior to initiating dispatch optimization.

$$\begin{cases} \mathfrak{F}_{\mathcal{L}_d}^{\mathcal{T}} = \mathfrak{F}_{\mathcal{CL}_d}^{\mathcal{T}} + \mathfrak{F}_{\mathcal{Q}}^{\mathcal{T}} \\ \mathfrak{F}_{net}^{\mathcal{T}} = \mathfrak{F}_{\mathcal{CL}_d}^{\mathcal{T}} - \left(\mathfrak{F}_{\mathcal{P}\mathbb{v}}^{\mathcal{T}} + \mathfrak{F}_{\mathcal{W}t}^{\mathcal{T}}\right) = \\ \mathfrak{F}_{net,\mathfrak{p}}^{\mathcal{T}} - \mathfrak{F}_{net,\mathcal{E}}^{\mathcal{T}} \end{cases} \quad (1)$$

$\mathfrak{F}_{net,\mathfrak{p}}^{\mathcal{T}}$ represents the customer nominal load (CNL)'s point prediction result, while $\mathfrak{F}_{net,\mathcal{E}}^{\mathcal{T}}$ is the power error brought on by computation discretization and forecast mistake. The prediction intervals approach is used to anticipate a spectrum of uncertainties, whereas point prediction is often used to predict the stable value of the CNL. The range of uncertainties is often predicted using the prediction intervals approach, whereas the stable value of the CNL is typically predicted using point prediction. The normalized root-mean-square width and the coverage probability are used to assess how well prediction intervals work. The coverage probability for a particular time is $\mathfrak{F}\left(L^{\mathcal{T}} \leq \mathfrak{F}_{net}^{\mathcal{K}} \leq U^{\mathcal{T}}\right)$, indicating that the forecast range (between the lower bound $L^{\mathcal{T}}$ and upper bound $U^{\mathcal{T}}$) covers the target values. This work focuses on optimization strategy research due to space constraints.

4.2 Electricity theft and fraud detection

Once the grid is secure, the attention shifts to detecting electricity theft and fraud. EGB-COA is employed for classification. EGB is used to classify the instance of electricity theft with high accuracy while COA optimizes the classification performance that enhances the overall accuracy.

4.2.1. Extreme grading boosting

A potent technique for effectively training machine learning models is XGBoost. By combining predictions from several weak models, its ensemble learning approach creates a stronger and more accurate forecast. Additionally, as XGBoost natively supports machine learning, it is feasible to train algorithms on big datasets in an acceptable amount of time. Large dataset management is one of its strong points, and it routinely produces excellent results in tasks like regression and classification, setting the

standard for cutting-edge outcomes. In algorithm 1, XGBoost pseudo code is displayed. XGBoost's general goal function combines standardization terms with a loss effect for every sample of training and tree within the groups:

$$\sum_{\mathfrak{a}=1}^{O}\left[loss_f(z_{\mathfrak{a}},\widehat{z_{\mathfrak{a}}})+\sum_{J=1}^{J}\Omega(Q_J)\right] \quad (2)$$

Where O is the number of training examples. For the $\mathfrak{a}^{th}$ training sample, $z_{\mathfrak{a}}$ and $\widehat{z_{\mathfrak{a}}}$ indicate the real label and predicted value, respectively. The ensemble's tree count is denoted by J. The tree is represented by Q_J, and the "loss function" $loss_f$ measures the distinctions among them $z_{\mathfrak{a}}$ and $\widehat{z_{\mathfrak{a}}}$. The term of normalization is J^{th} tree is Ω, while the number of classes is denoted by (cls).

$$loss_f(z_{\mathfrak{a}},\widehat{z_{\mathfrak{a}}})=-\sum_{\mathfrak{b}=1}^{cls}z_{\mathfrak{a}\mathfrak{b}}\log\left(\frac{e^{\widehat{z_{\mathfrak{a}\mathfrak{b}}}}}{\sum_{J=1}^{cls}e^{\widehat{z_{\mathfrak{a}J}}}}\right) \quad (3)$$

We employ the SoftMax activation function for multi-class classification. Each tree's structure has a definition of regularization that includes penalties for the square of the leaf weights and the number of terminated nodes.

$$\Omega_{\mathrm{Tree}}(Q_J)= \alpha\Re+\frac{1}{2}\alpha\sum_{\mathfrak{b}=1}^{\Re}\mathbb{W}_{\mathfrak{b}}^2+\beta\sum_{\mathfrak{b}=1}^{\Re}|\mathbb{W}_{\mathfrak{b}}| \quad (4)$$

In the above tree, $\Re$ represents the total number of terminal nodes. A terminal node's weight is represented by $\mathbb{W}_{\mathfrak{b}}$. The minimal infant weight, or minimum increase needed to create a second division, is α. The regularization term that regulates the total complexity is called β. The parameter that governs $loss_f$ regularization on leaf weights is called α. The leaf weights' absolute value is penalized in the regularization term as follows:

$$\Omega_{Leaf}(Q_J)=\eta\sum_{\mathfrak{b}=1}^{\Re}|\mathbb{W}_{\mathfrak{b}}| \quad (5)$$

The shrinkage parameter η regulates how much each tree contributes. For every training sample, the "Gradient" ($\mathbb{G}_{\mathfrak{a}}$) and "Hessian" ($\mathcal{H}_{\mathfrak{a}}$) with regard to the anticipated standards are calculated throughout the optimization process:

$$\mathbb{G}_{\mathfrak{a}}=\frac{d}{d\widehat{z_{\mathfrak{a}}}}\left[loss_f(z_{\mathfrak{a}},\widehat{z_{\mathfrak{a}}})+\sum_{J=1}^{J}\Omega(Q_J)\right] \quad (6)$$

$$\mathcal{H}_{\mathfrak{a}}=\frac{d^2}{d\widehat{z_{\mathfrak{a}}^2}}\left[loss_f(z_{\mathfrak{a}},\widehat{z_{\mathfrak{a}}})+\sum_{J=1}^{J}\Omega(Q_J)\right] \quad (7)$$

The rule that updates the terminal nodes' weights ($\mathbb{W}_{\mathfrak{b}}$) after every boosting round.

$$\mathbb{W}_{\mathfrak{b}}=-\frac{\mathbb{G}_{\mathfrak{a}}}{\mathcal{H}_{\mathfrak{a}}+\beta} \quad (8)$$

All trees contribute in proportion to the learning rate. The subsequent boosting round's update rule for the anticipated values is as follows:

$$\widehat{z_{\mathfrak{a}}}^{(BR+1)}=\widehat{z_{\mathfrak{a}}}^{(BR)}+\eta Q_J(q_{\mathfrak{a}}) \quad (9)$$

The boosting round is denoted by BR, and $Q_J(q_{\mathfrak{a}})$ is the predicted tree for the J^{th} sample. The approach aims to obtain high percentages of real favorable and true adverse outcomes while maintaining low percentages of results that are not real.

Algorithm 1: Extreme Grading Boosting

Input: $(q_{\mathfrak{a}},z_{\mathfrak{a}})$

1. η: Rate of learning
2. $loss_f(z_{\mathfrak{a}},\widehat{z_{\mathfrak{a}}})$: An alternative loss function
3. β : Coefficient of Regularization
4. **For** $\mathfrak{a}=1$ to N **do**
5. $\quad\mathbb{G}_{\mathfrak{a}}=\frac{d}{d\widehat{z_{\mathfrak{a}}}}\left[loss_f(z_{\mathfrak{a}},\widehat{z_{\mathfrak{a}}})+\sum_{J=1}^{J}\Omega(Q_J)\right]$
6. $\quad\mathcal{H}_{\mathfrak{a}}=\frac{d^2}{d\widehat{z_{\mathfrak{a}}^2}}\left[loss_f(z_{\mathfrak{a}},\widehat{z_{\mathfrak{a}}})+\sum_{J=1}^{J}\Omega(Q_J)\right]$
7. Leaf weight $\mathbb{W}_{\mathfrak{b}}=-\frac{\mathbb{G}_{\mathfrak{a}}}{\mathcal{H}_{\mathfrak{a}}+\beta}$
8. $\widehat{z_{\mathfrak{a}}}^{(BR+1)}=\widehat{z_{\mathfrak{a}}}^{(BR)}+\eta Q_J(q_{\mathfrak{a}})$
9. **End for**
10. For the $\mathfrak{a}^{th}$ sample, the predicted J^{th} tree is $Q_J(q_{\mathfrak{a}})$.

4.2.2. Coati optimization algorithm

The COA is used in the suggested work as an optimization method for effective power and energy management. Coatis, which are regarded as algorithm population members, are involved in the optimization process. Every coat essentially represents a possible solution to the problem since its location in the search space corresponds to values for the decision variable. To ensure a varied exploration of the solution space, the coatis beginning position in the search space is randomly initialized in the COA implementation. This methodology allows the COA algorithm to include parameters such as energy availability, energy demand, economic limitations, and power variations, hence addressing issues associated with microgrid failures and changing energy requirements.

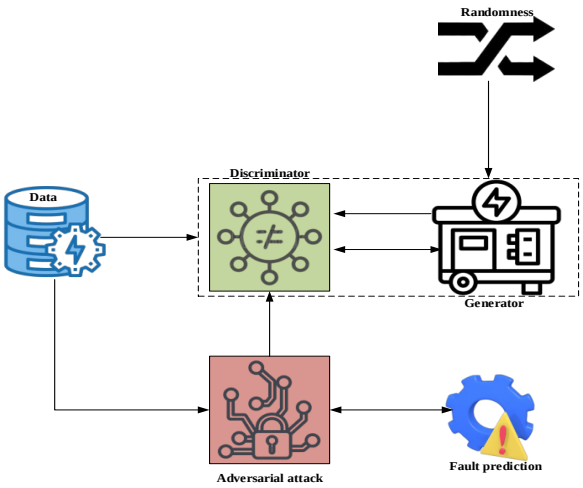

Figure. 2 Architecture of generative adversarial network

4.2.3. Coati optimization algorithm

The attacker creates harmful data by synthesizing instances that closely resemble real ones using GAN. A type of artificial intelligence algorithm known as GAN is made up of two neural networks a discriminator and a generator that have been trained in tandem to produce data that is realistic. The attacker can guide the fault prediction model to identify a particular fault type or zone in this way. By using real data to train a GAN model, this evasion technique creates synthetic data that mimics actual smart grid data. The adversary gains a potent tool (the trained generator) by effectively training the GAN, whereby the generated data may subsequently be incorporated within the smart energy system. We incorporate an additional training layer into the conventional GAN training procedure since we recognize the significance it is to strengthen the discriminator's skills. Fig. 2 depicts this procedure in brief.

The discriminator is trained using real data in the first training phases, which follow the conventional protocol. Once backpropagation of the discriminator's damage has occurred, the generator is employed to produce false information. In order to do this, we start by creating a random vector of hidden components, which the generator model then creates the fake inputs.

We use the discriminator to analyze these samples, and then we backpropagate the loss. Initially apply our unique layer of training before continuing with the generator's training.

4.3 Monitoring

To improve consumer trust and confidentiality in the system the monitoring activities within the smart grid must maintain the balance among functionality and privacy. This is achieved through the use of SMs provided with privacy functionality trade-off strategies. In the suggested model, the strategy's functioning is depicted as follows. The distribution-level substations (Sub) that provide families with power are part of the model, along with customers, "energy suppliers", "network operators", and "third parties". The suggested system's SM updates its measurements through a private platform, which can be a PC or smartphone. Instead of communicating directly with the energy supplier. Basic computing and storage capabilities are available on the private platform to save power usage and bill payment.

Assume that a smart meter group $smart_{\mathcal{M}} = \{smart_{\mathcal{M}1}, \ldots\ smart_{\mathcal{M}i}, \ldots\ smart_{\mathcal{M}n}\}\ (i \in [1, n])$ is present in the neighborhood. Power consumption at interval $\mathcal{T}$ (often 15 minutes), denoted as $I\mathbb{P}_c$, can be measured by the smart meter.

To stop users from altering the data on power use, the smart meter data is encrypted. Encrypting the data from smart meters stops users from changing the information about how much power they use. All data communication between customers and the utility is regulated by the data communications company, and as the SM is constructed without a backdoor, neither energy providers nor manufacturers are able to obtain the data from the device unlawfully. The SM in the suggested system reports monthly billing ($\mathbb{M}_{\mathcal{B}}$) and monthly energy usage ($\mathbb{M}_E$).

The dynamic time-of-use (TOU) tariff has been enabled through the TOU channel. To get TOU bills under the conventional SM method, the SM has to report the energy usage at each charging station. A utility's ability to gather comprehensive personal information about a person increases with the number of charging points it installs, raising the risk of privacy violations. The information is transmitted in the opposite methods using our TOU billing channel.

Every thirty minutes, the SM receives the TOU pricing from the energy supplier (ES). The SM couples the current TOU pricing with the energy use of the last 30 minutes. Bills computation. On the last day of every month, the total TOU bills in money are computed and forwarded to the ES, which subsequently issues invoices to the customers. Verification of billing accuracy. These strategies secured against privacy intrusion while improving effective monitoring thereby improving the consumer trust and confidence in the smart grid system**.** These strategies secured against privacy intrusion while improving effective monitoring thereby improving consumer trust and confidence in the smart grid system**.**

Table 1. System specification

Hardware specifications	Hard disk	512GB
	RAM	8GB
	Processor	Intel(R) Core™ i5-4200U CPU @ 2.30 GHz
Software specifications	Simulation tools	Matlab-R2023a\Simulink
	OS	Windows 10 (64-bit)

5. Experimental results

The experimental analysis of the proposed work is to enhance the effectiveness of the machine learning method to detect electricity theft and fraud within the smart grid environment. The study summary and comparative analysis are included in this subsection.

5.1 Simulation setup

The simulation environment and setup for the machine learning-based electricity theft and fraud detection in a smart grid environment are described in this subsection. The Simulink model, which acts as the implementation environment and data generator, is the sole foundation upon which the simulation scenario is built. No external datasets were imported or used for this project; instead, the dataset was produced directly from the behavior of the Simulink model itself. The dynamic functioning of a smart grid system, including, load variations, and energy consumption patterns, is simulated by the Simulink model. As a result, data reflecting the interactions and events inside the model might be generated in real time. A thorough dataset customized to the project's goals was produced by simulating variables such as load demand, power generation from renewable sources, frequency stability, and electricity theft detection. The setup of the system is shown in Table 1.

5.2 Comparative analysis

The suggested method's efficacy is assessed by comparing it with other techniques that are currently in use across a number of important performance indicators. These consist of accuracy, detection rate, and authentication rate. Visual representations of the comparison study, such as graphs, clearly demonstrate the benefits of the suggested technique over the alternative.

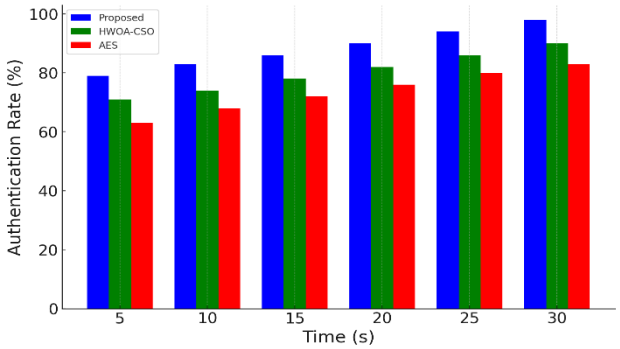

Figure. 3 Time (s) vs. authentication rate (%)

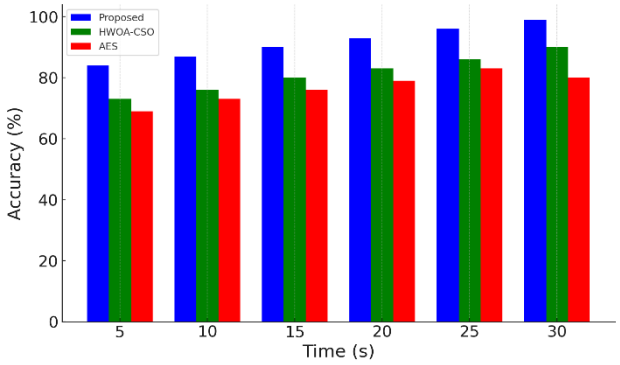

Figure. 4 Time (s) vs. accuracy (%)

5.2.1. Time (s) vs. authentication rate (%)

The graphical representation of Time (s) vs. Authentication accuracy (%) shows that the relationship between the system authentication users in the smart grid and similar recognition results. This is an important method to evaluate the effectiveness and security of the power theft and fraud detection system. Eq. (10) shows that the relationship between the time and authentication rate.

$$\Re(\mathcal{T}) = \Re_m \times \left(1 - e^{-k\mathcal{T}}\right) \tag{10}$$

Where $\Re(\mathcal{T})$ is the authentication rate at time $(\mathcal{T})$, the maximum authentication rate is denoted by $\Re_m$, and k is the constant value.

5.2.2. Time(s) vs. accuracy (%)

The connection between the system processing time and classification is shown in the time vs. accuracy graph. Regarding smart grids, the accuracy of properly detected incidents of theft and non-theft out of all instances that were examined.

Fig. 4 show the accuracy percentages that the suggested model attained at various time intervals in comparison to the AES and the HWOA-CSO techniques. suggested technique displays a sharp rise in accuracy, achieving 99% in less than 30 seconds,

demonstrating exceptional ability in promptly and precisely identifying occurrences.

The result shows a consistent increase, reaching 90% accuracy after 30 seconds, but it is still somewhat less effective than the suggested model. demonstrates a slower rate of growth than the other two approaches, attaining 80% accuracy after 30 seconds.

5.2.3. Time(s) vs. detection rate (%)

In the context of using machine learning for electricity theft and fraud detection, the relationship between the detection time and detection rate is an important metric. This connection is often evaluated to understand the effectiveness of the fraud detection model over time.

$$\mathcal{DR}(\mathcal{T}) = \frac{\mathcal{N}_{cor}(\mathcal{T})}{\mathcal{N}_{Total}} \times 100 \quad (11)$$

In Eq. (11) $\mathcal{DR}$ is the detection rate, $\mathcal{N}_{cor}(\mathcal{T})$is the total number of fraud instances that have been successfully identified by time, and $\mathcal{N}_{Total}$ is the total number of fraud cases.

The output of time vs detection rate is shown in Fig. 5. In terms of detection rate, the proposed method outperforms HWOA-CSO and AES algorithms throughout the all-time duration. Initially, at 5 seconds, the proposed method achieves an 80% detection rate, which is 6.4% higher than the HWOA-CSO and 13.5% higher than the AES. At 30 seconds, the scheme shows a significant difference with a detection rate of 98.6%, which is 7.2% better than HWOA-CSO and 15.1% better than AES. This model shows that the scheme not only provides good initial performance but also shows significant improvement over time, making it the best way to protect against theft and fraud.

5.2.4. Time(s) vs. precision (%)

This metric indicates the accuracy of positive predictions by each method over the time. The following equation calculate this metric,

$$Precision = \frac{True\ Positives}{True\ Positives + False\ Positives} \times 100 \quad (12)$$

Fig. 6 shows the precision of the proposed method starts at 80% at 5 seconds and steadily increases to 97% at 30 seconds. Also, the proposed method improves its ability to avoid false positives over time, likely due to better classification or decision-making at later stages. The precision of HWOA-CSO begins at 73% at 5 seconds and rises to 91% by 30 seconds. While showing consistent

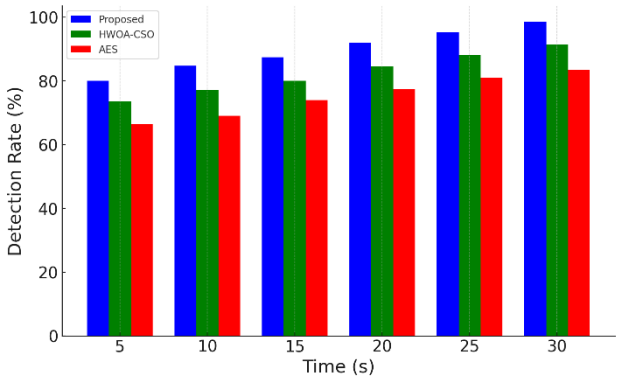

Figure. 5 Time(s) vs. Detection rate (%)

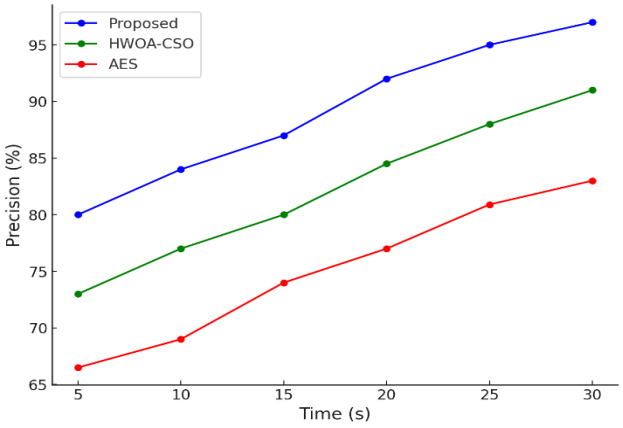

Figure. 6 Time(s) vs. Precision (%)

improvement, the precision of HWOA-CSO lags behind the Proposed Method at all time intervals. AES starting at 66.5% at 5 seconds, it reaches 83% by 30 seconds. AES demonstrates the slowest improvement in precision over time, with a noticeable gap compared to the proposed method.

5.2.5. Time(s) vs. recall (%)

This metric measures the ability of the model to correctly identify all the positive samples also known as sensitivity or true positive rate as the following equation,

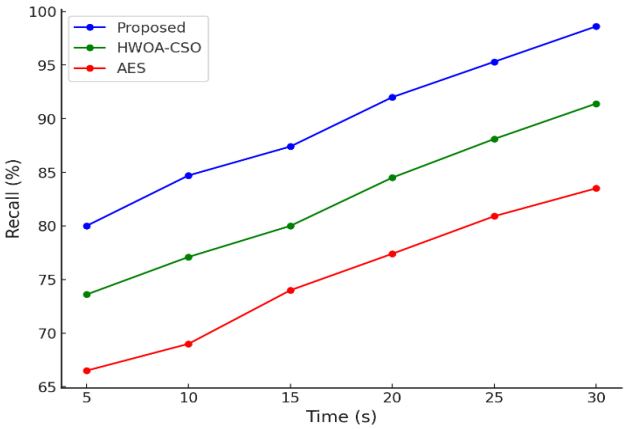

Figure. 7 Time(s) vs Recall (%)

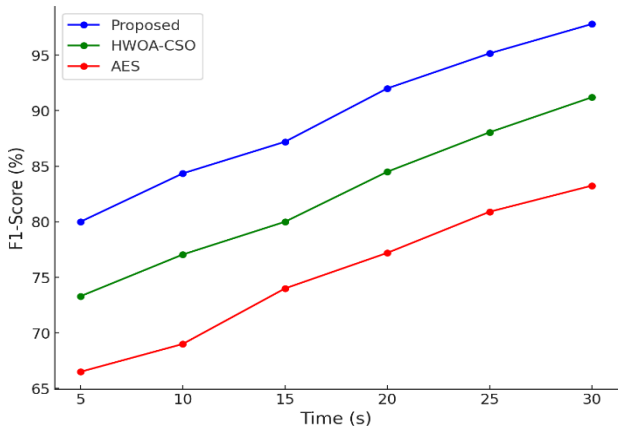

Figure. 8 Time(s) vs F1-score (%)

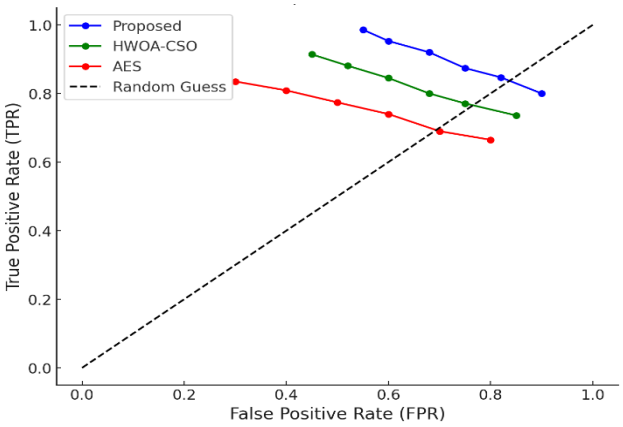

Figure. 9 ROC Curves

$$Recall = \frac{True\ Positives}{True\ Positives + False\ \ Negatives} \times 100 \qquad (13)$$

Fig. 7 shows the recall of the proposed method starts at 80% at 5 seconds and increases steadily to 98.6% at 30 seconds. This indicates that the proposed method is highly effective in identifying true positives over time, showing a steady improvement as processing time increases. HWOA-CSO begins at 73.6% at 5 seconds and rises to 91.4% by 30 seconds. While it improves consistently, it remains behind the proposed method throughout all time intervals, reflecting a less effective ability to capture all true positives. AES starts at 66.5% at 5 seconds and reaches 83.5% at 30 seconds. The AES method demonstrates the lowest recall performance, with a relatively slower rate of improvement over time compared to the other methods.

5.2.6. Time(s) vs. F1-score (%)

This metric combines precision and recall into a single metric to show the balance of accuracy and sensitivity. The F1-score is the harmonic mean of precision and recall, offering a single metric that balances both. The following equation show the evaluation of this metric,

$$F1 = \frac{Precision \cdot Recall}{Precision + Recall} \times 100 \qquad (14)$$

Fig. 8 shows the F1-score of the proposed method which starts at 80% at 5 seconds and increases steadily to 95.15% by 30 seconds. This indicates that the proposed method achieves a balanced and consistently improving performance in terms of both precision and recall over time. The proposed method maintains the highest F1-score across all time intervals, highlighting its effectiveness in minimizing both false positives and false negatives. While HWOA-CSO begins at 73.30% at 5 seconds and reaches 88.05% at 30 seconds. This shows steady improvement over time but consistently lags behind the proposed method, reflecting slightly lower precision and recall balance**.** AES starts at 66.50% at 5 seconds and climbs to 80.90% by 30 seconds. The AES method demonstrates the slowest improvement, reflecting its relatively poorer performance in balancing precision and recall compared to the other methods.

5.2.7. ROC-AUC

ROC-AUC stands for receiver operating characteristic - area under the curve. It is a performance metric used to evaluate the classification ability of a model, especially for binary classification tasks. The resulted values of ROC-AUC are as follows, the proposed is 0.3123, HWOA-CSO is 0.3280 and AES is 0.3763 provide insight into the performance of each method in terms of the trade-off between true positive rate and false positive rate.

Fig. 9 shows the ROC curve for the proposed method is below the diagonal reference line ($y=x$), indicating the performance across thresholds. The AUC value **(**0.3123**)** suggests that the model fights to decide between positive and negative classes effectively. Despite high recall and F1-score at specific thresholds, the curve indicates varying performance across the entire range of thresholds.

5.3 Research summary

First, we implement QKD with a ROS for secure authentication, aiming to reduce fluctuations within the microgrid. Following this, we employ EGB combined with the COA to be (EGB-COA) and GANs for accurate classification of data. Finally, we deploy SMs equipped with privacy functionality trade-off strategies to efficiently monitor and mitigate intrusions in the microgrids, ensuring both security and data privacy. Finally, we plot the graph for the following metrics: Time(s) vs.

(Authentication rate (%), vs. Accuracy (%), vs. Detection rate (%), vs. Precision (%), vs. Recall (%), vs. F1-score (%)) and ROC-AUC.

6. Conclusion

Our research aims to develop a robust electricity theft and fraud detection system using machine learning techniques. Traditional fraud detection techniques like management control and location verification are no longer adequate as the smart grid advancements. To overcome this issue, we propose using QKD with a continuous optimization strategy to reduce the overhead and reduce the efficiency changes. The integration of Extreme Gradient Boosting (EGB) and Coati Optimization Algorithm (COA) algorithm are used for accurate classification. Finally, to increase the customer's trust in the system and privacy, a balance should be established between business and privacy in the monitoring activities in the smart plan using a secret trading strategy broadcast by smart meters. The proposed model was verified with the help of the simulation tool Matlab-R2023a\Simulink. Additionally, a comparison study with the existing approaches was done to evaluate the current methodology. Numerical analysis is used to assess an approach's performance. Based on this study, it is feasible to show that our method outperforms all other presently available methodologies across all measures and highlight how well the suggested smart grid power theft detection system works. When compared to current methods, the system that incorporates machine learning approaches performs better on several parameters. In particular, our findings show a high authentication rate (98%), accuracy (99%), detection rate (98.6%), precision (97%), recall (98.6%), F1-score (95.15%), and AUC. In the future, as smart grids develop, the main focus will be on improving the suggested detection models to handle increasingly sophisticated fraudulent activities. To increase accuracy, real-time data analytics and deep learning will be investigated. We'll keep improving the privacy-preserving methods used in smart meters and look at the possibility of using blockchain technology to secure data. The main contributions of this paper are:

Effective Authentication*:* To provide secure communication while reducing computing cost, Quantum Key Distribution (QKD) with a Rolling Optimization Strategy (ROS) was introduced.

High-Accuracy Classification*:* Extreme Gradient Boosting (EGB) in conjunction with the Coati Optimization Algorithm (COA) for classification optimization, together with Generative Adversarial Networks (GANs) to reduce false alarms, allowing for the achievement of high accuracy in the detection of energy theft.

Enhancement of Privacy*:* Smart meters with privacy-functionality trade-off solutions that balance privacy with system monitoring capabilities have increased consumer confidence.

Conflicts of Interest

The authors declare no conflict of interest.

Author Contributions

Ihsan H. Abdulqadder was responsible for gathering needed the data, conceptual and methodology conducting the formal analysis, implementation the code, validation and writing the first draft of the article. Israa T. Aziz handled code validation, editing and supervising. Visualization project and supervision were done by Firas M. F. Flaih.

References

[1] S. O. Tehrani, A. Shahrestani, and M. H. Yaghmaee, "Online electricity theft detection framework for large-scale smart grid data", *Electr. Power Syst. Res.*, Vol. 208, p. 107895, 2022.

[2] M. K. Hasan, A. A. Habib, S. Islam, M. Balfaqih, K. M. Alfawaz, and D. Singh, "Smart grid communication networks for electric vehicles empowering distributed energy generation: Constraints, challenges, and recommendations", *Energies*, Vol. 16, No. 3, p. 1140, 2023.

[3] M. J. Abdulaal, M. I. Ibrahem, M. M. Mahmoud, J. Khalid, A. J. Aljohani, A. H. Milyani, and A. M. Abusorrah, "Real-time detection of false readings in smart grid AMI using deep and ensemble learning", *IEEE Access*, Vol. 10, pp. 47541-47556, 2022.

[4] E. J. Salazar, M. E. Samper, and H. D. Patiño, "Dynamic customer demand management: A reinforcement learning model based on real-time pricing and incentives", *Renew. Energy Focus*, Vol. 46, pp. 39-56, 2023.

[5] M. Shaaban, U. Tariq, M. Ismail, N. A. Almadani, and M. Mokhtar, "Data-driven detection of electricity theft cyberattacks in PV generation", *IEEE Syst. J.*, Vol. 16, No. 2, pp. 3349-3359, 2021.

[6] H. Jain, M. Kumar, and A. M. Joshi, "Intelligent energy cyber-physical systems (iECPS) for reliable smart grid against energy theft and false data injection", *Electr. Eng.*, Vol. 104, No. 1, pp. 331-346, 2022.

[7] Y. Yang, R. Song, Y. Xue, P. Zhang, Y. Xu, J. Kang, and H. Zhao, "A detection method for group fixed ratio electricity thieves based on correlation analysis of non-technical loss", *IEEE Access*, Vol. 10, pp. 5608-5619, 2022.

[8] R. K. Ahir and B. Chakraborty, "Pattern-based and context-aware electricity theft detection in smart grid", *Sustain. Energy Grids Netw.*, Vol. 32, p. 100833, 2022.

[9] I. T. Aziz, I. H. Abdulqadder, S. M. Alturfi, R. M. Imran, and F. M. Flaih, "A secured and authenticated state estimation approach to protect measurements in smart grids", In: *Proc. of Int. Conf. Innov. Intell. Informat.*, *Comput. Technol*., pp. 1-5, 2020.

[10] S. K. Gunturi and D. Sarkar, "Ensemble machine learning models for the detection of energy theft", *Electr. Power Syst. Res.*, Vol. 192, p. 106904, 2021.

[11] E. Stracqualursi, A. Rosato, G. Di Lorenzo, M. Panella, and R. Araneo, "Systematic review of energy theft practices and autonomous detection through artificial intelligence methods", *Renew. Sustain. Energy Rev.*, Vol. 184, p. 113544, 2023.

[12] L. Cui, L. Guo, L. Gao, B. Cai, Y. Qu, Y. Zhou, and S. Yu, "A covert electricity-theft cyberattack against machine learning-based detection models", *IEEE Trans. Ind. Informat.*, Vol. 18, No. 11, pp. 7824-7833, 2021.

[13] M. Emadaleslami, M. R. Haghifam, and M. Zangiabadi, "A two-stage approach to electricity theft detection in AMI using deep learning", *Int. J. Electr. Power Energy Syst.*, Vol. 150, p. 109088, 2023.

[14] R. Sharma, A. M. Joshi, C. Sahu, and S. J. Nanda, "Detection of false data injection in smart grid using PCA-based unsupervised learning", *Electr. Eng.*, Vol. 105, No. 4, pp. 2383-2396, 2023.

[15] P. Massaferro, J. M. Di Martino, and A. Fernández, "Fraud detection on power grids while transitioning to smart meters by leveraging multi-resolution consumption data", *IEEE Trans. Smart Grid*, Vol. 13, No. 3, pp. 2381-2389, 2022.

[16] Chaithra, L. G. Malleshappa, and J. Sreenivasaiah, "Classification of web pages using the machine learning algorithms with web page recommendations", *Int. J. Intell. Eng. Syst.*, Vol. 15, No. 4, 2022, doi: 10.22266/ijies2022.0831.57.

[17] I. O. Lopes, D. Zou, I. H. Abdulqadder, S. Akbar, Z. Li, F. Ruambo, and W. Pereira, "Network intrusion detection based on the temporal convolutional model", *Comput. Secur.*, Vol. 135, p. 103465, 2023.

[18] I. H. Abdulqadder, I. T. Aziz, and D. Zou, "DT-Block: Adaptive vertical federated reinforcement learning scheme for secure and efficient communication in 6G", *Comput. Netw.*, Vol. 254, p. 110841, 2024.

[19] N. Khan, M. Amir Raza, D. Ara, S. Mirsaeidi, A. Ali, G. Abbas, and M. Bouzguenda, "A deep learning technique AlexNet to detect electricity theft in smart grids", *Front. Energy Res.*, Vol. 11, p. 1287413, 2023.

[20] A. Nawaz, T. Ali, G. Mustafa, S. U. Rehman, and M. R. Rashid, "A novel technique for detecting electricity theft in secure smart grids using CNN and XG-boost", *Intell. Syst. Appl.*, Vol. 17, p. 200168, 2023.

[21] A. Takiddin, M. Ismail, and E. Serpedin, "Robust data-driven detection of electricity theft adversarial evasion attacks in smart grids", *IEEE Trans. Smart Grid*, Vol. 14, No. 1, pp. 663-676, 2022.

[22] A. Banga, R. Ahuja, and S. C. Sharma, "Accurate detection of electricity theft using classification algorithms and Internet of Things in smart grid", *Arab. J. Sci. Eng.*, Vol. 47, No. 8, pp. 9583-9599, 2022.

[23] N. Javaid, A. Almogren, M. Adil, M. U. Javed, and M. Zuair, "RFE-based feature selection and KNNOR-based data balancing for electricity theft detection using BiLSTM-LogitBoost stacking ensemble model", *IEEE Access*, Vol. 10, pp. 112948-112963, 2022.

[24] R. Nayak and C. D. Jaidhar, "Employing feature extraction, feature selection, and machine learning to classify electricity consumption as normal or electricity theft", *SN Comput. Sci.*, Vol. 4, No. 5, p. 483, 2023.

[25] Y. Sun, X. Sun, T. Hu, and L. Zhu, "Smart grid theft detection based on hybrid multi-time scale neural network", *Appl. Sci.*, Vol. 13, No. 9, p. 5710, 2023.

[26] A. T. El-Toukhy et al., "Electricity theft detection using deep reinforcement learning in smart power grids", *IEEE Access*, Vol. 11, pp. 59558-59574, 2023.

[27] H. Iftikhar et al., "Electricity theft detection in smart grid using machine learning", *Front. Energy Res.*, Vol. 12, p. 1383090, 2024.

[28] F. Shehzad, N. Javaid, S. Aslam, and M. U. Javed, "Electricity theft detection using big data and genetic algorithm in electric power systems", *Electr. Power Syst. Res.*, Vol. 209, p. 107975, 2022.

[29] A. I. Kawoosa, D. Prashar, M. Faheem, N. Jha, and A. A. Khan, "Using machine learning ensemble method for detection of energy theft in smart meters", *IET Gener. Transm. Distrib.*, Vol. 17, No. 21, pp. 4794-4809, 2023.

[30] A. Muzumdar, C. Modi, and C. Vyjayanthi, "Designing a blockchain-enabled privacy-preserving energy theft detection system for smart grid neighborhood area network", *Electr. Power Syst. Res.*, Vol. 207, p. 107884, 2022.