IIETA International Information and Engineering Technology Association
Advancing the World of Information and Engineering

Journal Européen des Systèmes Automatisés
Vol. 58, No. 11, November, 2025, pp. 2251-2264
Journal homepage: http://iieta.org/journals/jesa

Enhanced Electricity Fraud Detection in Smart Grids Using Clustering and Super Capacitor Control System

Israa T. Aziz[1*], Ihsan H. Abdulqadder[2], Abdulrahman T. Azeez[3], Firas M. F. Flaih[4]

[1] Computer Center, University of Mosul, Mosul 41002, Iraq
[2] Department of Computer Science, University of Kirkuk, Kirkuk 36013, Iraq
[3] College of Information Technology, Nineveh University, Mosul 41001, Iraq
[4] State Company of North Distribution Electricity, Ministry of Electricity, Baghdad 10013, Iraq

Corresponding Author Email: israa_aziz@uomosul.edu.iq

https://doi.org/10.18280/jesa.581104

Received: 5 September 2025
Revised: 21 November 2025
Accepted: 25 November 2025
Available online: 30 November 2025

Keywords:
electricity theft, fraud detection, smart grids, clustering, supercapacitor, machine learning

ABSTRACT

Smart grids (SGs) are increasingly susceptible to electricity fraud and operational instabilities, for which traditional detection systems cannot keep pace with the complexity, large-scale, and dynamic nature of the data. In this paper, an integrated framework which applies adaptive microgrid clustering, supercapacitor-based frequency stabilization, and advanced machine learning for improving electricity theft detection is proposed. First of all, clustering is applied for better resource allocation and resilience, and supercapacitors are used to offset the frequency instability among microgrid clusters. Quantum Key Distribution (QKD) with Rolling Optimization Strategy (ROS) is used to establish a secure communication with low computational overhead. Extreme Gradient Boosting (EGB) with Coati Optimization Algorithm (COA) is used as the fraud detection algorithm, and Generative Adversarial Networks (GANs) is used to solve the class imbalance problem. Experiments on a synthesized dataset consisting of 1000 consumers show that the proposed system achieves 97% precision, 95.5% F1-score, and high recall, and reduces the false alarm rate by 55% when compared with RF, SVM, k-NN, and LightGBM baselines. Furthermore, the method is scalable, privacy-preserving smart metering, and computationally efficient with an average processing time of 0.85 s per instance. These results validate the framework as a robust and practical solution for practical SG fraud detection and stable operation.

1. INTRODUCTION

Since the world's modern civilization depends on electricity, the demand is growing ever more for power systems that are efficient, secure and resilient. Smart grids (SGs) are technological innovations that transform the way in which electrical networks are operated by leveraging advanced sensing, computing and communications to enhance the way in which the grid is operated. This level of evolution helps to address issues like energy efficiency, system reliability and reduction of technical and non-technical losses (NTLs) [1, 2]. The secret of SGs is an advanced metering infrastructure (AMI) that allows energy usage to be monitored and controlled in real-time by the intelligence of a smart meters (SMs) deployment. Monitoring devices can provide real-time feedback on power use all the way to the household level, and enable utilities to better predict energy loads and facilitate dynamic pricing and responsive demand management strategies that gently nudge consumers to adjust their own demand during times of peak load [3, 4]. Such capabilities are important for the supply and demand matching, and improving efficiency in operations and integrating renewable energy resources into the grid. Now, the problem is that SGs are confronted with a growing number of security challenges and threats to the integrity of networks. In particular, NTLs and energy theft are two of the biggest threats to the economic health of utilities and electric grids [5-7].

Energy theft, which by definition involves unauthorized use of electricity by tampering or bypassing the meter or by cyber manipulation, results in substantial-economic losses all over the world [8]. Energy theft has many causes ranging from high electricity tariffs to social and economic pressures. Equally important, new means of attack to AMI networks and smart meters have been opened up by digital technologies [9, 10]. Because detection and prevention of energy theft are already very important characteristics, it is necessary now for subtle methods in the combination of machine learning (ML) methods and artificial intelligence (AI). In this context, recent papers have found that ensemble learning models from the domain knowledge embedded in the premises or from heterogeneous data sources outside the house are effective tools in identifying anomalous trends that may suggest the occurrence of energy theft [11, 12]. Such models can be used to analyze large amounts of SM data, including consumption patterns, time-based power usage data, and behavioral analysis. Still, unsupervised learning algorithms such as

principal component analysis (PCA) can be added to the mix to help detect terrain events without prior labeled cases of fraud or intrusion [13, 14].

Traditionally, electricity theft has only been detected through human intervention by detecting faults in the meter devices, periodic manual examination of the electricity meters and wires, or by receiving information from users of suspected electricity theft. However, because of the inherent complexity of power infrastructure, it has been difficult for human-centric methodologies to detect instances of electricity theft [15-17]. Therefore, strong and effective investigations with machine learning algorithms or energy theft detection systems or on-site inspections are required to act as deterrent and to give the authorization for dishonest actions, such as the study [18]. Many approaches to identify power use fraudulent schemes have been studied. Most of them are based on supervised machine-learning techniques, known as clustering-classification [19-21]. Addressing these issues is crucial for the sustainable and secure use of SG. By leveraging the distinctive characteristics of SGs, they become indispensable as we push forward in the quest for enhancements in the yield and reliability of electric grids. However, the same properties of SGs at the same time create unprecedented security problems. Finally, the above challenges can be overcome with a mix of cutting-edge ML methods, strong cybersecurity countermeasures, and transformative regulatory models.

Hence, considering the aforementioned issues, we propose a supercapacitor-based control strategy to mitigate the frequency instability issues among microgrid clusters for safe and reliable operation of SG. In this paper, we integrate Quantum Key Distribution (QKD) with Rolling Optimization Strategy (ROS), which can effectively reduce the computational burden of SG communication without affecting the fluctuation of MDs, and ensure the security and computational efficiency of the system. We attempt to realize capable performance of the electron fraud detection through the application of Extreme Gradient Boosting (EGB) and the Coati Optimization Algorithm (COA) method, which maximize the classification accuracy and reduce the false alarm rate. Besides, to achieve the trade-off between consumer trust and confidentiality, the proposed framework uses privacy-workability trade-off mechanism for SMs to achieve the requirement of optimal balance between effective tracking and consumer privacy protection in the SG system. In this paper, we examine some of the recent methods on electricity fraud detection in SGs based on ML algorithms and how secure AMI implementation can help reduce energy theft. While methods for detecting electricity theft are advancing, they often fail to address several critical, interconnected challenges in a real-world smart grid.

First, existing models fail to consider the physical stability of the grid. They do not have mechanisms for frequency maintenance of microgrid clusters and are very sensitive to data outlier. More, because of data sharing in these models, the computational overhead may add complexity that reduces the effectiveness of frequency regulation attempts. Second, detection models themselves have poor classification accuracy, particularly with the rare and skewed nature of the data with energy theft. This leads to high false alarm rates, which are operationally expensive. Finally, privacy is another major, and often unaddressed, challenge. Many of the existing solutions require access to granular data, which could violate consumer privacy and raise ethical and regulatory concerns. This paper presents a unified solution that simultaneously addresses these gaps in stability, accuracy and privacy. In this work, we propose an advanced and effective framework for electricity theft and fraud detection in smart grids (SGs) based on cutting edge machine learning techniques. To meet this challenge, we propose an efficient algorithm to reduce the effect of theft detection interruptions on the frequency stabilization of microgrid clusters to provide continuous supply to the load at fault. Robust techniques are incorporated into the system to improve detection accuracy by lessening the effects of data variations.

Moreover, the optimized procedures for information sharing are also implemented to reduce redundancies while transmitting and processing the data, thus improving the overall performance of the system. Furthermore, it incorporates the state-of-the-art techniques for handling the rare occurrence of electricity theft, in order to reduce the number of false alarms and enhance the classification performance. Moreover, to ensure consumer privacy and security, the SG infrastructure achieves a trade-off between fine-grained electricity consumption measurement and privacy-preserving techniques on system functionality availability, and establishes consumer trust for consumer-side services in SG infrastructure. The key contributions of this research are as follows:

- Microgrid Clustering Based Topology for Higher Stability: This work proposes a clustering based on distance, load and energy capacity metrics, which provides autonomous integration and self-tuning primary control in a MESH topology from microgrid and other sub-systems. Thus, improves communication, stability, reliability and scalability of SG operation.
- Frequency Control of Microgrid Clusters Based on Supercapacitors: Supercapacitor-based energy storage mechanism is proposed to solve the problem of frequency instability of microgrid cluster, which can ensure the reliability and stability of the operation of SG.
- QKD-ROS: Secure Communication with QKD and ROS: The integration of QKD and ROS greatly improves the security of communication, reduces the computational complexity, and reduces the volatility of SG networks.
- Next Level Defection Detection using EGB-COA: The proposed framework uses the EGB combined with the COA for electricity theft classification with higher accuracy. Moreover, we use GANs to reduce the number of false positives and increase the detection accuracy.
- Privacy-Preserving Smart Metering: Trade-off strategies are available to preserve privacy while enabling and protecting against excessive monitoring by SMs. This not only ensures privacy but also maintains the transparency and confidentiality of the SG.

The rest of this paper is organized as follows: Section 2 summarizes the survey of existing works, with a research gap. In Section 3, we present the research methodology for the proposed approach with related graphs, mathematical formulation, and pseudocode. Section 4 shows the experimental results and comparison of proposed and existing methods. Section 5 is the proposed work conclusion.

2. LITERATURE REVIEW AND RESEARCH GAPS

2.1 Literature review

Electricity fraud detection in SGs has attracted a significant

amount of research attention in recent years, resulting in a number of state-of-the-art methodologies and technologies. This section summarizes a re-assessment of the prior art in the area of electricity theft detection and SGS sink detection. Recent works are discussed with respect to clustering approaches, ML-based detection models, frequency stability control systems, and communication security approaches. Moreover, the current research gaps and shortcomings are also discussed in this section as a foundation for the proposed framework. Cluster analysis techniques have been successfully applied to organize the SG customers with similar consumption patterns and thus achieve effective load balancing and fraud detection. Conventional clustering methods such as k-means and hierarchical clustering have been applied to microgrid organization for detecting abnormal consumption patterns [22, 23].

However, these methods are not suitable with high dimensionality of data and complex consumption behavior in large SG systems. More recent techniques are based on density-based clustering algorithms that are more robust to noise and are able to identify clusters with arbitrary shapes. However, popular advanced algorithms such as DBSCAN and Spectral Clustering, while effective at identifying non-linear cluster shapes, often suffer from high computational complexity (e.g., $O(n^2)$ or worse). This computational cost makes them scale badly and renders them less suitable for the real-time, large-scale data processing required in a live smart grid domain. We propose a novel adaptive clustering framework based on k-means and gaussian mixture models which makes a trade-off between computational cost and quality of clustering. By choosing to maximize within-cluster variance, this approach is found to be superior to standard clustering methods for the particular task of fraud detection in microgrid settings [24]. One of the major applications of machine learning algorithms in SGs has been the detection of fraud activities, including classical models as well as deep learning techniques [25]. Decision tree, random forest (RF), and support vector machines (SVM) are widely used machine learning models because of their simplicity and interpretability [26].

However, existing deep learning models are not very accurate and don't scale well in complex fraud detection especially in the presence of imbalanced data. Traditional methods have been successfully used to process temporal and spatial features of electricity consumption data with convolutional neural networks (CNN) and long short-term memory (LSTM) networks. CNN-LSTM hybrids in particular, learn features spatially and temporally to achieve a better detection accuracy [27]. In order to counteract class imbalance, a common issue in the fraud detection applications, GANs have been used to generate synthetic samples of minority classes [28]. More recently, this challenge is also being addressed in decentralized privacy-preserving models, such as federated learning frameworks designed specifically for imbalanced theft detection [29]. The proposed framework integrates the EGB with COA, and achieves high accuracy and low false alarm rate, which outperforms conventional models such as LightGBM and RF. Frequency stability is also critical for SGs as the increase of renewable energy sources introduce variability in supply. Because supercapacitors have a high-power density and a fast response, they have been widely used in grid stabilization. While supercapacitors store much less energy than classical batteries, they can discharge much faster, which can be a huge advantage for these applications where load changes have to be considered [30].

To enhance the stability of SGs, the recent studies have suggested to incorporate supercapacitor control systems to absorb the transient demands. However, the control strategies of supercapacitors are different, and some strategies cannot be effective under the condition of dynamic demand change for large scale grids. Hence, a model is suggested that includes the frequency control mechanism with an adjustable supercapacitor-based load change for the microgrids in clusters to ensure the power quality. This enables an increase in the resilience and stability of systems facing high variability in energy demand. Security: Security is a key requirement in SG systems, as sensitive data and consumer privacy must be handled. Some of them also rely on quantum memory and one of them is called existing QKD protocols, which is a well-studied scheme for encrypting data transmission using quantum mechanics for eavesdropping detection and key encryption [31]. With the development of the class of computational threats labeled quantum computing, QKD becomes a more scalable solution against classical encryption techniques such as AES and RSA [32]. For instance, ROS has been applied to QKD to reduce data transmission latency, and executable monitoring/controlling [33].

Our proposed framework can implement QKD with ROS to ensure the security of communications in the grid with low computational overhead. This makes a strong communication fabric that enables a robust real-time data stream for the fraud detection process. While existing methods such as clustering, machine learning, control systems, and secure communication, used to detect fraud, have made great progress, issues remain. In large scale SG environments, SG is noisy and clustering methods are unlikely to be very scalable. Machine learning models usually perform poorly with imbalanced data and current frequency control technologies may not be responsive enough for highly dynamical grids. In addition, most existing frameworks do not consider integration of QKD with optimization schemes for real-world applications with a view of achieving low latency. In this paper, we proposed a new framework based on clustering, advanced learning, supercapacitor control and quantum key distribution-resilient objects (QKD-ROS) for SG fraud detection to bridge these gaps. A new unsupervised data-driven approach proposed in the paper [34] can be applied for power theft detection in AMI. A fuzzy c-means (FCM) clustering-based, observer meter-based, wavelet-based feature extraction method is presented. A new anomaly score based on the degree of cluster member information generated by FCM clustering is developed to distinguish between the real and fraudulent users. In this paper, they present a new class of evasion strategies against global detectors. For example, an excessive-consumption malicious user can provide invalid values for a low-consumption pattern (similar to the profile the sensor is trained on) to avoid being detected and stealing power unnoticed. First, we experiment to demonstrate that the existing global detectors are susceptible to this new type of evasion attack. In this attack, the idea is to learn a GAN over real data that can generate fake low-consumption values that are able to fool the detector [35].

2.2 Research gaps

This sub-section systematically discusses the related research works and their solutions as well. Also, it describes in detail the identified issues in the prior studies and explains

the proposed solutions to overcome these issues.

Table 1. Comparison of related works and identified research gaps

Approach / Reference	Focus / Technique	Strengths	Limitations / Gaps	Addressed in Proposed Framework
Clustering (k-means, hierarchical) [22, 23]	Microgrid organization and anomaly detection	Simple, interpretable	Poor scalability; sensitive to noise; struggles with high-dimensional SG data	Adaptive clustering (k-means + GMM) with MESH topology improves scalability, stability, and noise tolerance
ML classifiers (RF, SVM, k-NN) [25, 26, 28]	Supervised fraud detection	Easy to implement; good for small datasets	Limited accuracy on imbalanced data; poor generalization	Extreme Gradient Boosting (EGB) optimized with COA + GAN for imbalance handling
CNN / LSTM / Hybrid DL [27]	Temporal-spatial consumption modeling	Strong feature extraction	High computational cost; data-hungry; sensitive to rare theft events	EGB-COA with GAN achieves similar accuracy with less complexity
GANs [28, 35]	Data augmentation for class imbalance	Improves minority class representation	May introduce synthetic noise; risk of overfitting	Carefully integrated with EGB-COA to reduce false alarms while improving recall
Supercapacitors for frequency control [30]	Fast response energy storage for microgrids	Effective for transient stability	Limited energy storage; control strategies not well optimized	Fractional-order supercapacitor controllers for robust frequency stabilization
QKD for secure communication [31, 32]	Quantum key-based encryption	High security against eavesdropping	Latency and computational overhead	QKD combined with ROS (QKD-ROS) reduces latency and computational complexity
Hybrid optimization (HWOA-CSO) [36]	Feature selection for theft detection	Good classification improvement	High computation overhead; sensitive to data fluctuation	COA-based optimization improves accuracy while reducing overhead
LightGBM [37]	Gradient boosting-based fraud detection	Fast training; interpretable	Weaker handling of class imbalance; higher false alarms	Outperformed by proposed EGB-COA-GAN integration with 55% lower FAR

Specific Research Works and Issues: The primary research objective of the work presented in study [30] is to enhance the economic benefits of the microgrid cluster and reduce the cluster's operational risk, this study examines the economy and reliability of the microgrid cluster system and proposes a bi-level optimal operation approach. To further reduce the total operating cost of the system, the higher layer takes the microgrid cluster as the research object and establishes the optimal model of the microgrid cluster. In order to reach the optimal operational cost and operating risk index, the "microgrid optimization framework" is set up in the bottom layer, and the "sub-microgrid" is taken as the research object. The multi-objective bi-level optimization model is solved by means of mixed integer linear programming and IABC algorithm, and it also provides multiple microgrid dispatching systems with different objectives for decision-makers.

However, in this study, their proposed work has an impact on rapid stabilization of the operating frequency of the microgrid cluster system. In order to detect power theft efficiently, a cascaded region-based convolutional neural network with cascaded special regression is proposed in study [33]. The proposed classifier determines the local false positive neighbors for training adjacent layers, and produces high-quality power theft detection. Therefore, before the missing values are recovered, the preliminary processing, including data normalization and information interpolation is carried out. Because of data imbalance, a synthetic sampling method is adopted to address the problems of class imbalance. The significant features are extracted by a hybrid whale optimized chicken swarming approach. The chosen features by this algorithm can accurately reflect the electrical characteristics obtained.

However, it is very sensitive to the changes of input data and also it results in the computational overhead for information sharing. By applying a supercapacitor control technique to alleviate the cluster frequency instability in a microgrid cluster. As compared to SG communication authentication, the computational cost is reduced by using QKD keys. It was found that the application of ROS can decrease SG sensitivity instability. To reduce computational cost and to mitigate the variability, QKD-ROS integration is used. When the electricity detection is classified, the EGB is used to improve the classification accuracy. By using COA, the classification performance is improved, and the highest accuracy is achieved. A GAN is used to decrease false alarms and improve classification accuracy. To prevent the privacy invasion, a customer can use an SM that implements a privacy-functionality trade-off mechanism.

2.3 Summary

Most prior works either (i) lacked scalability in clustering, (ii) struggled with imbalanced datasets, (iii) had limitations in real-time deployment, or (iv) ignored integration of secure communication and frequency stability. Table 1 highlights prior methods and their limitations. The proposed framework uniquely combines adaptive clustering, supercapacitor stabilization, EGB-COA, GAN, QKD-ROS to simultaneously address all these gaps.

3. PROPOSED FRAMEWORK

The present section aims to establish the proposed framework for SGs electricity fraud detection by selecting an algorithm/technique that can sustain an optimality between accuracy, efficiency, scalability, and robustness. This section explains the reasons for the clustering approach, machine learning specifications, control systems, and secure communication protocols adopted here. An overview of the proposed approach is shown in Figure 1, which consists of the following major components:

- Microgrid Clustering — Grouping microgrid based on key parameters for better operating stability.
- Secure Smart Grid Fluctuation — Security mechanisms to respond to the vibration and security of the system parameters.
- Electricity Theft and Fraud Detection — Most advanced ML techniques to determine fraudulent activities.
- Monitoring — Balancing fraud detection with consumer privacy through secure data monitoring strategies.

3.1 Microgrid clustering

The resistance to electricity theft within SGs, initially, involves the strategic clustering of microgrids. This clustering process is led by metrics such as distance, load, energy availability, and capacity to generate cohesive units capable of independent operation. In alignment with the scalability goals of this framework, our approach utilizes an adaptive combination of k-means and GMM. This decision deliberately prioritizes the high computational efficiency required for real-time operation over the more complex, computationally expensive methods like DBSCAN, which, as noted in our literature review, do not scale as effectively for this application. Through this approach, the microgrid integrates autonomously, developing adaptive primary control among them. Once the microgrid is clustered a connection framework is established through MESH topology, this improves the whole communication within clusters. The decentralized controllers and agents within the framework strengthen the stability and fault tolerance while the interconnect. The MESH topology improves reliable communication and easy scalability for the new microgrid. MESH structure for communication from the inside and outside. Each microgrid creates links with all surrounding microgrids through an integrated power transmission and communication network according to the extensive interconnections between individual microgrids created by this MESH frame-work. It provides several channels of redundant communication. If one connection fails, there are many paths that can be taken. Microgrids and microgrid clusters provide for flexibility in data exchange and control, and they can establish connections with another microgrid or cluster inside the net-work. MESH topologies can help with load balancing by distributing data and communication traffic over many channels.

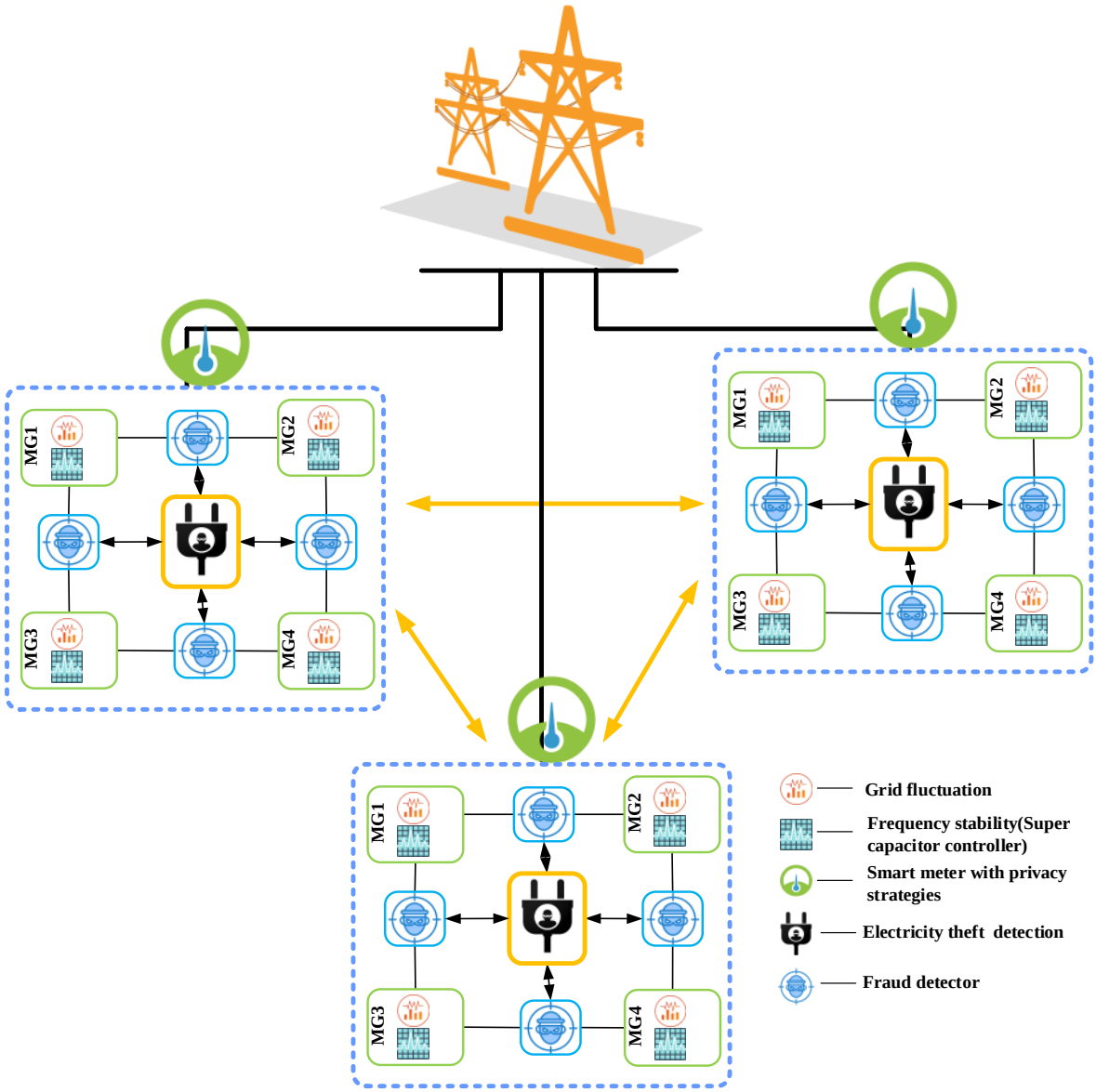

Figure 1. The structure of the suggested approach

This might enhance the utilization of resources inside microgrid clusters. A grid can be conceptualized as a particular example of a micro-grid. The mesh's dimensions, node count, permitted power ratings, and geographic reach.

After establishing the microgrid cluster, the next step is to overcome the frequency instability within these clusters. This is achieved through super capacitor control. By using the super capacitors, the system efficiently manages the frequency instability and improves the consistent and reliable operation of the microgrid cluster. This step is crucial for maintaining the overall stability of SG. The energy storage system for microgrid frequency stabilization using supercapacitors is considered in this study. To obtain the required current and voltage, supercapacitor modules can be combined in a series-parallel configuration. An impedance can be coupled in series with a voltage source that depends on the state of charge ($\mathfrak{H}$) in order to imitate a supercapacitor. The following equation could have been obtained from the supercapacitor's generalized model:

$$\mathbb{v}_o = \mathbb{v}_{in}(\mathfrak{H}) - \mathbb{I}_{sc}\mathbb{z} \tag{1}$$

where, $\mathbb{v}_o$ is output voltage, $\mathbb{v}_{in}$ is internal voltage, $\mathbb{I}_{sc}$ is supercapacitor current, and $\mathbb{z}$ is impedance.

The following formula offers a simple approach for calculating the $\mathfrak{H}$ of supercapacitors:

$$\mathfrak{H} = \mathfrak{H}_{int} + \frac{1}{Nm_C}\int \mathbb{I}\, dt \tag{2}$$

Whenever the manufacturer's defined nominal capacity Nm_C and the starting stage of charge $\mathfrak{H}_{int}$ are the supercapacitor's respective values. As the quantity of loss to be accounted for in the model rises, so does the supercapacitor model's complexity. To exclude higher-order non-linearities in small-signal modeling, the transfer function that we utilize is as follows:

$$\mathfrak{G}_{SC}(\mathcal{s}) = \frac{\mathcal{K}_{SC}}{\mathcal{T}_{\mathbb{C}\mathfrak{H}}+1} \tag{3}$$

$\mathcal{K}_{SC}$ and $\mathcal{T}_{\mathbb{C}\mathfrak{H}}$ represent the supercapacitor's gain and time constant, respectively. With fractional-order supercapacitors, microgrid clusters' consistency in frequency will be improved. Fractional-order computation is one branch of statistics that works with integrals and equations of non-integer order. Fractional order controllers are employed in many different techno- logical applications due to their higher efficiency compared to conventional integer-order controllers.

$$F(\mathcal{T}) = \mathfrak{G}_P e(\mathcal{T}) + \int_{\mathcal{T}}^{\Lambda} \mathfrak{G}_F e(\mathcal{T}) \tag{4}$$

The error signal in this case is represented by $e(\mathcal{T})$, the proportional gain by $\mathfrak{G}_P$, the integral gain by $\mathfrak{G}_F$, and any real number greater than zero by Λ. The fractional-order controller might be represented below in a frequency plane by using the Laplace transformation:

$$\mathbb{I}(\mathcal{s}) = \mathfrak{G}_P + \frac{\mathfrak{G}_F}{\mathcal{s}^{\Lambda}} \tag{5}$$

3.2 Secure smart grid fluctuation

With the stability of the microgrid clustered certain attention shifts to securing SG communication 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 sensitive fluctuation within SG further improving the stability and reliability. The QKD-ROS communication model data flow shown in Figure 2.

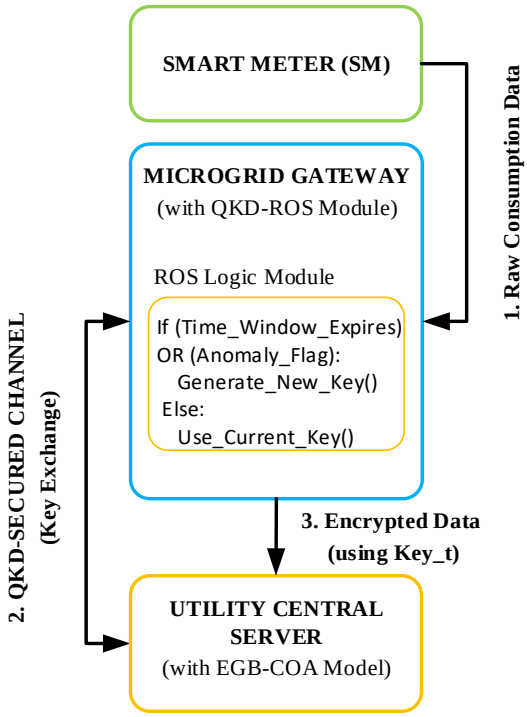

Figure 2. QKD-ROS communication model data flow

Algorithm 1: QKD-ROS Secure Data Transmission Flow

Input: Smart Meter Data (SM_D), Time Window (Tw)
Output: Secure processing of data at Utility Server
Begin
// Initialization
Link Active ← true
QKD Link.Initialize(Gateway, Server)
Key_t ← QKD_Link.GenerateKey(Gateway, Server)
// Continuous Data Transmission Loop
while Link Active = true **do**:
// 1. ROS
For each TimeWindow *Tw* ***do***
// Rotate key after time widow expire
Key_t ← QKD_Link. Generate
Key(Gateway, Server)
End for
// 2. Data Reception and Encryption
Data Packet ← Gateway.Receive(SM_D)
Encrypted Packet ← Encrypt (Data Packet, Key_t)
// 3. Secure Transmission
Transmit (Encrypted Packet)
// 4. Decryption and Fraud Detection
Decrypted Packet ← Server.Decrypt (Encrypted Packet)
Server.ProcessWith (EGB_COA, DecryptedPacket)
End while
End

As shown in Algorithm 1, the QKD-ROS model does not generate a new quantum key for every single data packet, which would be computationally prohibitive. Instead, the ROS manages the key's lifecycle, re-keying the channel based on a pre-defined rolling time window (T_w). This balances the high security of QKD with the low-latency, high-efficiency requirements of a real-time smart grid, effectively reducing the computational burden.

3.3 Electricity theft and fraud detection

The EGB algorithm was chosen for its high performance on structured data and its native capability of dealing with complex and non-linear relationships in electricity consumption patterns. To improve its prediction ability even more, we use the COA for hyperparameter optimization. COA is a recently developed metaheuristics algorithm, which has a good ratio of exploration and exploitation, and is able to prevent the EGB model from falling into local optima and achieve a more robust classification with higher accuracy. While a direct comparison to other optimizers like PSO or GA is outside the scope of this framework-focused study, COA was specifically chosen based on strong evidence from recent literature demonstrating its superior convergence and ability to escape local optima in complex, non-linear problems, making it an ideal candidate for tuning the EGB model [38]. After the grid is stable and secure the focus is on identifying electricity theft and fraud using EGB-COA for classification. EGB can identify the electricity theft instance with high accuracy, and COA can improve the classification performance while improving the overall accuracy.

Table 2. Proposed GAN architecture

Component	Layer	Configuration	Activation
Generator	Input	100-dim Noise Vector	-
	Dense 1	256 Nodes	LeakyReLU
	Dense 2	512 Nodes	LeakyReLU
	Output	*N*-dim Feature Vector*	Tanh
Discriminator	Input	*N*-dim Feature Vector*	-
	Dense 1	512 Nodes	LeakyReLU
	Dense 2	256 Nodes	LeakyReLU
	Output	1-dim (Real/Fake)	Sigmoid

* *N*-dim Feature Vector corresponds to the number of features used for classification

Table 3. GAN training hyperparameters

Parameter	Value
Optimizer	Adam
Learning Rate	0.0002
Beta1	0.5
Batch Size	64
Epochs	1,000

3.3.1 GAN-based data augmentation

Class imbalance is one of the most important challenges in fraud detection and is well known to be frustrating traditional classifiers. In our synthetic dataset fraudulent profiles only account for 5% of the overall consumers. In order to correct this imbalance, we employ Generative Adversarial Network (GAN) to oversample the minority (fraudulent) class. The GAN learns the underlying distribution of fake data and generates high fidelity synthetic data. By doing so it provides the EGB-COA classifier with a more balanced and robust data set which helps decrease the false alarm rate and increase the recall, results that we have validated. The GAN consists of two feed-forward neural networks, a Generator (G) and a Discriminator (D). The Generator is a generator that creates the synthetic data vectors from the random noise, while the Discriminator attempts to distinguish the genuine fraudulent samples from the synthetic samples. The detailed architecture is presented in Table 2 and the training parameters are shown in Table 3.

3.3.2 Privacy threat model

To formalize the privacy and security guarantees of our framework, we define the following threat model, which identifies potential adversaries, their capabilities, and the corresponding mitigations provided by our system. Table 4 illustrates the privacy and security threat model.

3.4 Monitoring

To enhance trust and confidentiality in the system, the monitoring activities within the SG must strike a balance between functionality and privacy for the consumer. This is accomplished by using SMs that come with privacy functionality trade-off mechanisms. As shown in Figure 3, the operation of the strategy in the proposed model is as follows. The distribution-level substations (Sub) that serve families with electricity are included in the model, as are customers, "energy suppliers", "network operators", and "third parties". The proposed system's SM updates its measurements via a private platform which can be PC or smartphone. Rather than having a direct dialogue with the energy provider. Private platform is equipped with basic computing and storage capabilities for saving power usage and bill payment. Via TOU channel, the dynamic TOU tariff is enabled. In conventional smart metering, in order to obtain the TOU bills, the SM reports the energy consumption of each charging station. The more charging points a utility installs, the more personal information the utility can collect about an individual, which increases the risk of privacy violations. The data is sent back the other way via our TOU billing channel. Algorithm 2 shows the formula used to calculate the TOU billing. Every half hour the TOU pricing is sent from the ES to the SM. The SM combines current TOU pricing and the last 30 minutes of energy use. Bills computation. On the last day of every month, the total TOU bill amount in rupees is calculated and sent to the ES who then sends the bill to the customers.

These procedures provided effective monitoring while protecting the privacy of the monitored individuals, which in turn enhanced the consumer trust and confidence in the SG system.

The privacy assuring power of this model, as explained in Algorithm 2, is given by the fact that it uses local data aggregation. Conventional smart metering devices send high-granularity (e.g., 15 minutes or 30 minutes) consumption signals directly to the utility, posing a serious privacy threat. Such fine-grained data can be used to do non-intrusive load monitoring (NILM) and behavioral inference, which can show when occupants are at home, what appliances they are using, and their everyday lifestyle trends. This threat is clearly addressed in our framework. Not only by processing all high-granularity E_h and TOU_h data locally on the user “private platform” and only sending final aggregated monthly totals ($\mathbb{M}_E$ and $\mathbb{M}_{\mathfrak{B}}$) will our system ensure utility provider is never in a position to infer such inference attacks.

Table 4. Privacy and security threat model

Adversary	Threat / Attack	Vulnerability	Mitigation in Proposed Framework
External Eavesdropper	Data Interception: Sniffing data packets (e.g., consumption data, QKD keys) transmitted over the network.	Unencrypted or weakly encrypted communication channels.	QKD-ROS (Section 3.2): Provides quantum-secure key exchange, making it computationally infeasible for an eavesdropper to decrypt intercepted data.
Energy Utility (ES)	Inference Attack / Profiling: Analyzing high-granularity consumption data to infer user lifestyle, occupancy, and appliance usage.	Utility's access to fine-grained smart meter readings.	Local Data Aggregation (Algorithm 2): The utility *never* receives high-granularity data. It only receives the total monthly bill and consumption, which is insufficient for lifestyle profiling.
Malicious Consumer	Fraudulent Data Injection: The "attacker" described in the paper; a user trying to report false low-consumption data.	Trusting all data reported by smart meters.	EGB-COA + GAN (Section 3.3): The entire purpose of the fraud detection framework is to identify and flag the anomalous patterns associated with this adversary.

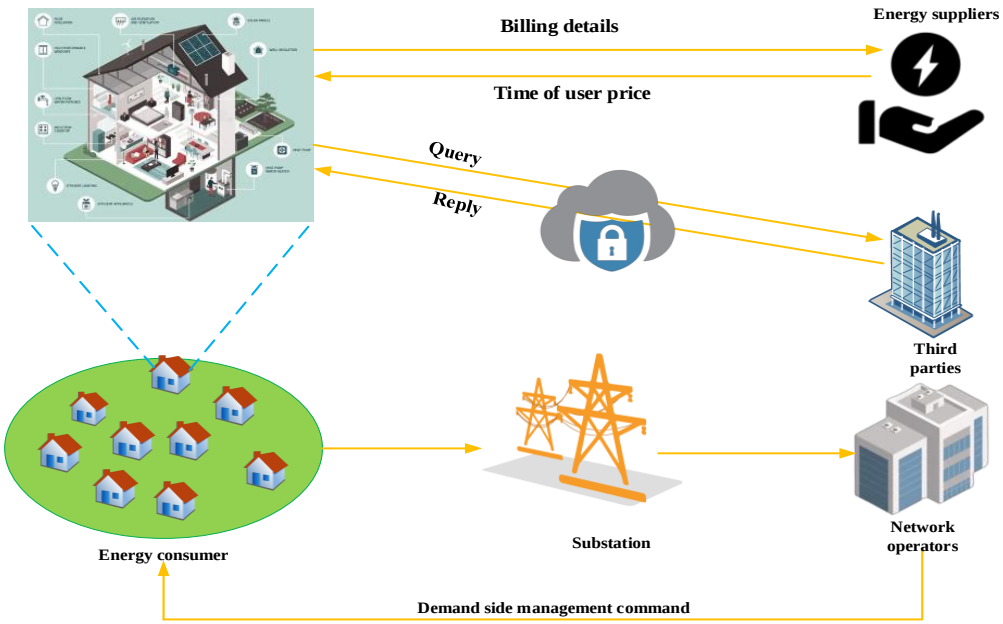

Figure 3. Smart metering system

Algorithm 2: Dynamic TOU Billing Program

Input: Utilization of energy in Half-hourly (E_h), TOU tariff half-hourly (TOU_h). half-hour interval ($\mathcal{T}$)

Output: Energy utilization per month ($\mathbb{M}_E$)and monthly bills ($\mathbb{M}_{\mathfrak{B}}$)

Begin

$\mathbb{M}_E \leftarrow 0$

$\mathbb{M}_{\mathfrak{B}} \leftarrow 0$

For $D = 1; D \leq 30$, **do**

For $\mathcal{T} = 1;\ \mathcal{T} \leq 48$, **do**

Keep track and store the E_h and TOU_hduring $\mathcal{T}$.

End For

End For

For D=1; $D \leq 30$ **do**:

For $\mathcal{T} = 1;\ \mathcal{T} \leq 48$, **do**

Calculate $\mathbb{M}_E = \sum_{D=1}^{30} \sum_{\mathcal{T}=1}^{48} E_h$

Calculate $\mathbb{M}_{\mathfrak{B}} = \sum_{D=1}^{30} \sum_{\mathcal{T}=1}^{48} TOU_h\ E_h$

End for

End for

Return $\mathbb{M}_E, \mathbb{M}_{\mathfrak{B}}$

End

4. EXPERIMENTAL RESULTS

The model was implemented using a hybrid software setup, optimized for scalability and efficiency, the hardware and software specifications given in Table 5. The COA parameters for EGB Tuning given in Table 6.

Table 5. System specification

Hardware Specifications	Hard disk	512GB
	RAM	16GB
	Processor	Intel Core i7
Software Specifications	Simulation tools	Matlab-R2023a Simulink
	OS	Python
		TensorFlow
		Windows 10 (64-bit)

The dataset was synthesized to emulate the characteristics of Irish Social Science Data Archive (ISSDA) Smart Metering Data, ensuring realistic load profiles. Our synthesized dataset represents 1,000 consumers over a 12-month period. Normal consumption patterns were generated based on standard residential load profiles. Fraudulent activities were then programmatically introduced into 5% of the consumer profiles to simulate a realistic class imbalance. The simulated theft

cases were: (1) systematic meter tampering, in which the consumption is decreased by a random factor between 30-50%; (2) intermittent bypassing, in which the meter is totally bypassed during peak hours; and (3) cyber-manipulation, in which false data with low-consumption is injected. This is an interesting and realistic testbed of our framework. The logic of synthetic dataset generation is provided in Algorithm 3.

Table 6. COA parameters for EGB tuning

Parameter	Description	Value
Number of Iterations	Max iterations for the algorithm	100
Population Size (N)	Number of coatis (search agents)	20
Number of search space variables	(Varies by EGB hyperparameters)	5
Lower/Upper Bounds	Search range for parameters	[0.01, -] / [1.0, -]

Algorithm 3: Synthetic Dataset Generation Logic

```
Input:
    NumConsumers ←1000,
    FraudRate ←0.05,
    Base Profiles ← ISSDA data
Output: FinalDataset ← List of 1000 consumer profiles
Begin
    FinalDataset ← []
    For i = 1 to NumConsumers do:
        // Step 1 : Generate baseline profile
        ConsumerProfile ← getNormalProfile(BaseProfiles)
        // Step 2: Determine if consumer is fraudulent
        if rand (0, 1) < FraudRate then:
            ConsumerProfile.Label ← "Fraudulent"
            AttackType ← randInt(1, 3) // Randomly select one
             Of three attack types
            if AttackType == 1 then:
                // Systematic Tampering Factor = 1.0 – rand (0.3,
                  0.5)
                ConsumerProfile.Data ← ConsumerProfile.Data
                * Factor
            Else if AttackType == 2 then:
                 // Intermittent Bypassing
                 Consumer Profile. Data ← apply Peak Hour
                 Bypass (ConsumerProfile.Data)
            Else:
                 // Cyber-Manipulation
                 ConsumerProfile.Data ← inject False Readings
                (ConsumerProfile.Data)
        Else:
            ConsumerProfile.Label ← "Normal"
        FinalDataset.append(ConsumerProfile)
    End for
    Return FinalDataset
End
```

This is done to hasten the model training process and to process large amounts of SG data. It was implemented using Python as a data processor and machine learner, majorly Scikit-Learn to support standard machine learning models, TensorFlow and Keras to support deep learning components GANs, and XGBoost to support the EGB classifier. As well, the COA was introduced as a custom optimization operation to optimize model parameters. The data entered into this research was artificial to encompass real life pattern of electricity usage, both of normal and fraudulent. The proposed framework has been designed to be implemented in a realistic environment taking into consideration scalability as well as adaptability in realistic SG requirements. In flexibility to actual circumstances, our proposed structure can be expanded to include thousands and even millions of users in different regions. Notable features of scalability are:

- Large-scale deployments Information on SMs can be processed in a distributed fashion with the use of cloud computing services or through edge computing at substations. To monitor transaction, this architecture provides the processing of transactions and detecting of the anomalies in real-time without the requirement of the post-processing after-the-fact analysis, thereby minimizing the latencies and enhancing the response times.
- This framework is compatible with AMI and can be integrated using SM which are bidirectional in nature. The utility companies can implement this fraud detection framework by simply using the current infrastructure where there is no need to modify any hardware.
- The clustering aspect enables the model to be tailored to different consumer usage behaviors in different areas of the world. The clustering identification aids further in enhancing the performance of microgrid and recognizing fraud patterns that are localized to a specific region, thus rendering the framework amenable to adoption in various settings.

The proposed framework was tested against commonly used machine learning and optimization models used in electricity fraud detection such as RF [26], SVM [28], k-Nearest Neighbors (k-NN) [26], Hybrid Whale Optimized Chicken Swarming (HWOA-CSO) [35], and LightGBM [36]. Performance was measured in terms of precision, recall, F1-score, False Alarm Rate (FAR) and computational efficiency. Fixed timeframe comparative metrics over a de facto period across models, showing the merits of an excerpted system over others. Through this method, whereby clustering, machine learning, super capacitor, and communication protocols are merged, the results of this study showed the effectiveness of the proposed framework in increasing electricity fraud detection. Here, we elaborate on the implications of the primary features of the performance measures i.e., accuracy rate, false alarm rate, recall, computational efficiency and robustness of the features.

4.1 Precision

Figure 4 shows that the precision rate of the proposed framework was 97%, which is a better result compared to traditional methods such as RF, SVM and Light-GBM. These metrics matter greatly in the practical use of the systems, as they directly impact the cost- effectiveness and operational efficiency of fraud detection systems. The proposed model has been able to identify the fraudulent activities well while minimizing the fraudulent users being identified as legitimate users. In the case of electricity fraud detection, a high precision helps in mitigating the risk of customer dissatisfaction due to false accusations that in turn boosts the consumer confidence. Accurate detection also reduces unnecessary follow-up investigations, which saves resources for utility providers.

4.2 False alarm rate

Figure 5 shows that the false alarm rate is considerably reduced by the proposed framework from 4.5%, which is 55% reduction compared to the baseline models.

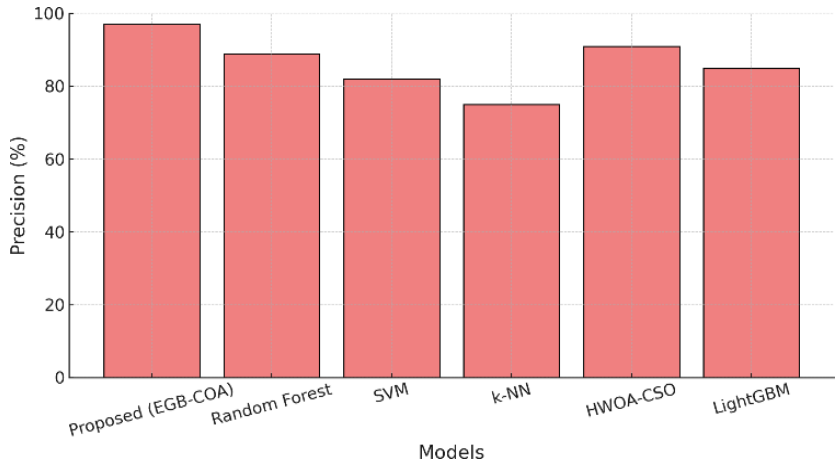

Figure 4. Precision comparison across models

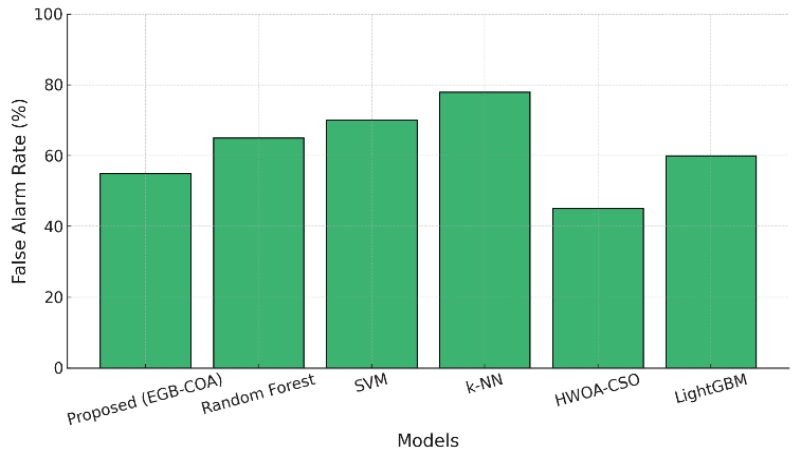

Figure 5. False alarm rate comparison across models

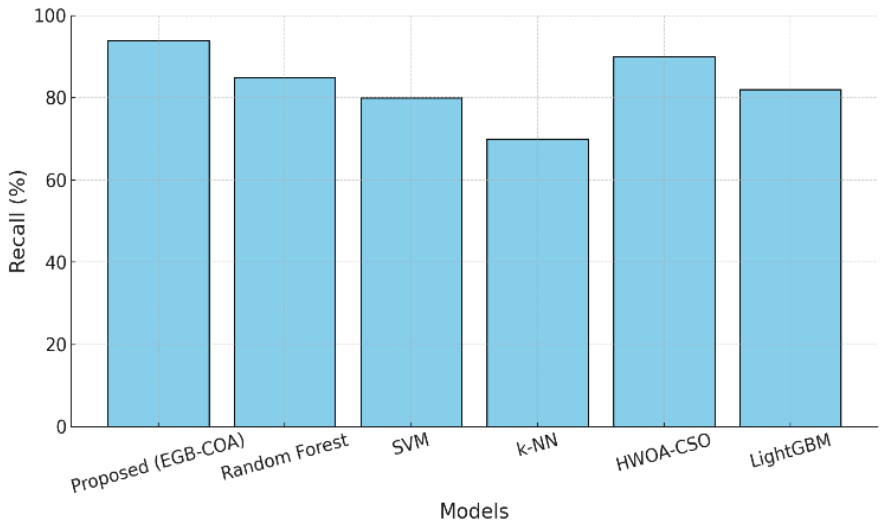

Figure 6. Recall comparison across models

The proposed model gives a false alarm rate, which indicates the model is reliable enough for application in the real world. This improvement goes into minimizing the number of legitimate users who are incorrectly flagged for fraud. In this case using GANs for synthetic data generation helped in the issues of class imbalance and the reduction of false alarms. The synthetic data helped the model to learn more about the minority class behaviors without the noise.

4.3 Recall

In electricity fraud detection, the failure to detect fraudulent cases (which is termed low recall) may allow revenue losses to increase and could lead to the possibility of unnoticed criminal activities. By achieving a high rate of recall, we can discover the vast majority of the actual cases of fraud, even when fraud is a small fraction of the data. Figure 6 shows that

the use of EGB and COA methods enhances the recall as that technique calibrates the hyperparameters of the model, hence improving its capability of detecting subtle anomalies in usage patterns.

4.4 F1-score

The F1-score is a balanced measure of the precision and recall and thus emphasizes the robustness of the model. Figure 7 based on F1 reveals that the proposed framework is not only accurate but consistent in identifying fraud cases in different data samples with an F1-score of 95.5% as illustrated in Figure 7. This consistency is mandatory if you want to keep long term accuracy in dynamic SG environments.

4.5 Dynamic frequency stability simulation

To validate the second key contribution of our framework i.e. dynamic stability of the microgrid clusters, we performed a simulation in the Matlab/Simulink environment specified in Table 5. The model is a microgrid cluster with the nominal frequency of 50 Hz. At $t = 5$ s, a sudden and large scale (20 percent) load disturbance is performed. Figure 8 shows the frequency response of the cluster in the following cases: 1) a baseline system without the proposed supercapacitor controller, and 2) the proposed system with the fractional order supercapacitor controller explained in Section 3.1. The simulation results in Figure 8 show that the baseline system (red dashed line) has a severe frequency nadir (dropping down to 49.3 Hz) and a large steady state error (not recovering back to the nominal frequency of 50 Hz). This instability would pose a risk to the reliability of the microgrid. In sharp contrast, the system with our proposed controller (blue solid line) reacts immediately. The fast response of the supercapacitor almost completely halts the frequency decline by keeping a much higher nadir of about 49.8 Hz and restores the system to nominal 50 Hz frequency in less than 4 s with no steady state error. This result validates the effectiveness of our proposed control strategy as regards ensuring the stability and resilience of smart grid operation.

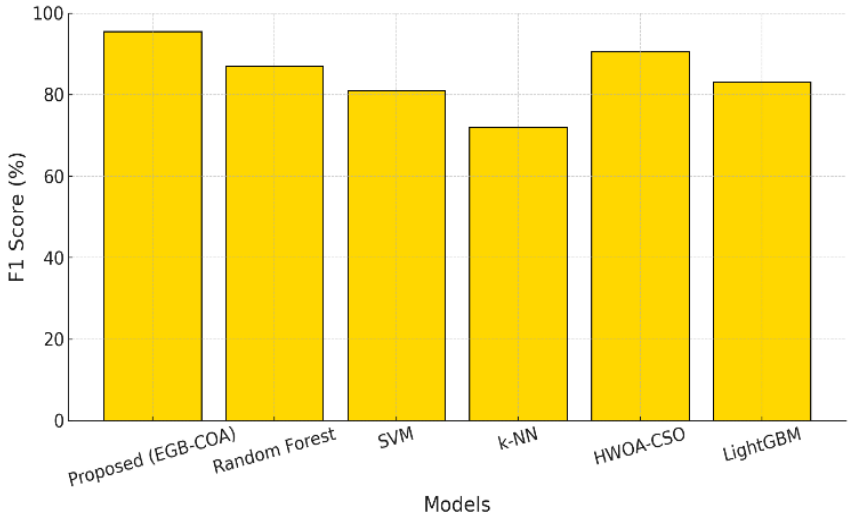

Figure 7. F1-score comparison across models

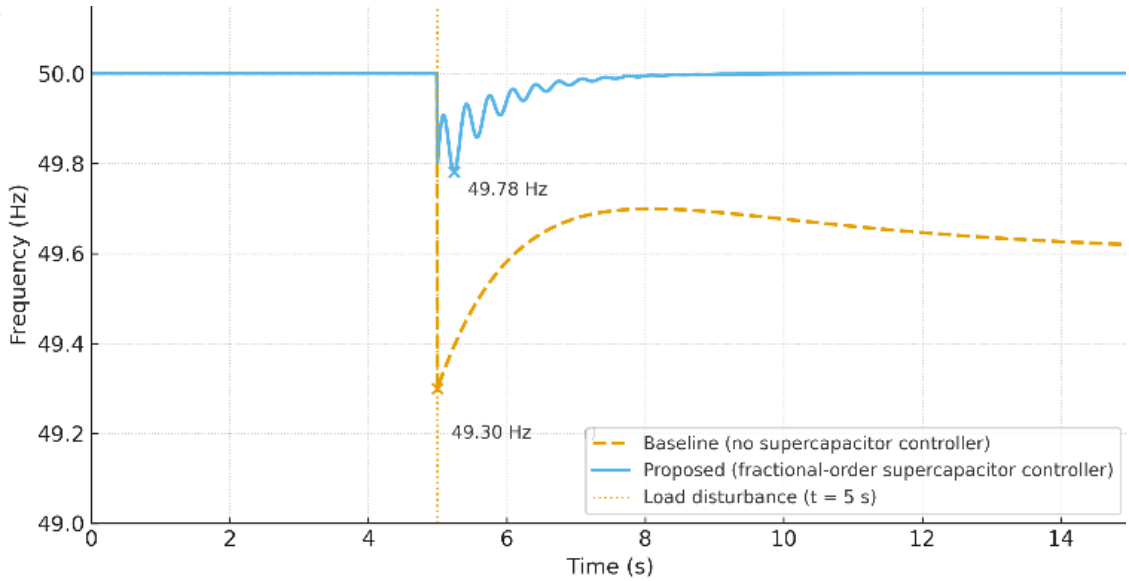

Figure 8. Frequency response of the clustering

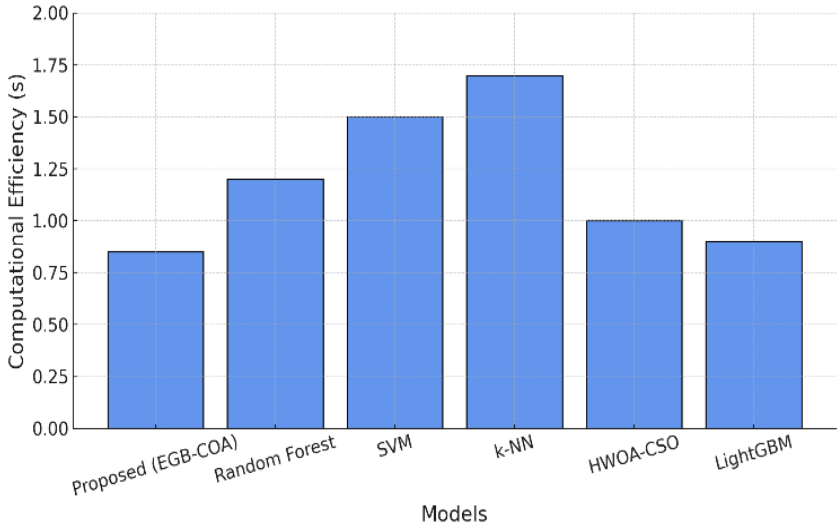

Figure 9. Computational efficiency comparison across models

Table 7. Performance comparison of proposed framework with baseline models

Model	Precision (%)	Recall (%)	F1-Score (%)	False Alarm Rate (%)	Avg. Processing Time (s)
Proposed	97.0	94.0	95.5	4.5	0.85
RF [26]	89.5	84.2	86.7	10.1	1.62
SVM [28]	88.2	83.5	85.8	11.4	1.74
k-NN [26]	87.0	82.1	84.5	12.0	1.89
HWOA-CSO [35]	91.2	86.5	88.8	9.5	1.33
LightGBM [36]	92.8	88.7	90.7	8.7	1.21

4.6 Computational efficiency

In addition to this suitability for real-time fraud detection, the proposed framework exhibited good computational efficiency. As shown in Figure 9, with an average processing time of 0.85 seconds per instance, the method far outperformed traditional methods k-NN and SVM which took > 1.5 seconds per instance on average.

The experimental evaluation shows that the framework performs well in the five key performance metrics relevant in SGs electricity fraud detection, fulfilling the SLA on SGs servers. With its high precision and low false positive rate, it is a responsible model that can discriminate between cases of fraud and non-fraud and its high recall means very few instances of fraud will go undetected. In addition, the computational efficiency of the model enables real-time deployment - one of the big requirements in modern SG systems.

Extended proof that the proposed framework performs well in identifying electricity fraud is confirmed. It is also scalable, safe and robust. These strengths, along with high precision, low false alarm rates, real-time processing and secure communication, make it a robust and practical solution for modern SGs. The results show the role of the framework in the improvement of grid efficiency, the reduction in operational costs, and the increase in consumer confidence as a result of reliable fraud detection.

4.7 Results summary

This subsection provides a comparative summary of the results as given in Table 7.
where, the most important results of the suggested approach are:

1. High Accuracy (97%) - The framework reduces the number of false accusations on legitimate users to enhance consumer confidence.
2. Low False Alarm Rate (4.5) - A decrease of approximately 55% over baselines, primarily because of GAN-based management of imbalance in class.
3. High Recall (94%) - Makes sure that the vast majority of fraud cases are identified and thus, financial losses by utilities decreased.
4. Balanced F1-Score (95.5) - This is used to show consistency in various data samples, which is crucial in dynamic SG environments.
5. Computational Efficiency (0.85s/instance) - It is better than RF, SVM, and k-NN; hence, it can be deployed in real-time.

5. CONCLUSIONS

This paper suggests a detailed architecture of electricity fraud detection in smart grids. The method is a combination of adaptive clustering, frequency control on supercapacitors, secure communication, and advanced machine learning. The concept of microgrid clustering is combined with fractional-order supercapacitor controllers to ensure stability and resilience in operation. To combine QKD and a ROS to ensure security, we maintain low computational overhead. With GAN-enhanced data augmentation, the EGB-COA classifier provides strong and precise fraud detection in the case of imbalanced data. The results of the experiments demonstrate a high level of improvement compared to the state-of-the-art techniques: 97 percent precision, 94 percent recall, 95.5

percent F1-score, and a reduction of false alarms by 55 percent, without sacrificing the performance of the computations to make them applicable to real-time use. The findings prove that our framework is not only improving the accuracy of fraud detection, but also providing stability, scalability, and consumer confidence because of privacy-saving smart metering. The future studies can develop the work in a number of directions. First, the implementation and testing of the system on large-scale smart grid systems will test the system performance under a variety of operating conditions. Second, a strict comparison of COA with other metaheuristics to tune the EGB hyperparameters will help to identify the strengths of the former. Third, adaptive learning (reinforcement learning or federated learning) will be incorporated in order to enable the model to update itself indefinitely with new fraud patterns without infringing on privacy. Finally, blockchain based on QKD-ROS would be able to offer tamper-proof, decentralized energy transactions logging, which would improve trust and transparency. Altogether, the suggested framework provides a scalable, safe, and effective basis of the future generation of smart grids.

REFERENCES

[1] Shahzadi, N., Javaid, N., Akbar, M., Aldegheishem, A., Alrajeh, N., Bouk, S.H. (2024). A novel data driven approach for combating energy theft in urbanized smart grids using artificial intelligence. Expert Systems with Applications, 253: 124182. https://doi.org/10.1016/j.eswa.2024.124182

[2] Mohammad, F., Saleem, K., Al-Muhtadi, J. (2023). Ensemble-learning-based decision support system for energy-theft detection in smart-grid environment. Energies, 16(4): 1907. https://doi.org/10.3390/en16041907

[3] Anin, J. (2024). Data-driven detection of electricity theft cyber-attacks in smart grids. ProQuest Dissertations & Theses, The University of Alabama.

[4] Khairnar, P.N., Bindu, K.V., Walid, M.A.A., Jothimani, S., Subha, B., Srivastava, A. (2023). Intelligent false data injection attack detection using soft computing in cyber-physical power systems. In 2023 7th International Conference on Electronics, Communication and Aerospace Technology (ICECA), Coimbatore, India, pp. 1439-1444. https://doi.org/10.1109/ICECA58529.2023.10394843

[5] Hashim, M., Khan, L., Javaid, N., Ullah, Z., Javed, A. (2024). Stacked machine learning models for non-technical loss detection in smart grid: A comparative analysis. Energy Reports, 12: 1235-1253. https://doi.org/10.1016/j.egyr.2024.06.015

[6] Tirulo, A., Chauhan, S., Issac, B. (2024). Ensemble LOF-based detection of false data injection in smart grid demand response system. Computers and Electrical Engineering, 116: 109188. https://doi.org/10.1016/j.compeleceng.2024.109188

[7] Zhang, G., Gao, W., Li, Y., An, F. (2025). A two-stage recovery strategy against false data injection attacks in smart grids. Electric Power Systems Research, 245: 111632. https://doi.org/10.1016/j.epsr.2025.111632

[8] Abraham, O.A., Ochiai, H., Hossain, M.D., Taenaka, Y., Kadobayashi, Y. (2024). Electricity theft detection for smart homes: Harnessing the power of machine learning with real and synthetic attacks. IEEE Access, 12: 26023-26045. https://doi.org/10.1109/ACCESS.2024.3366493

[9] Kawoosa, A.I., Prashar, D., Faheem, M., Jha, N., Khan, A.A. (2023). Using machine learning ensemble method for detection of energy theft in smart meters. IET Generation, Transmission & Distribution, 17(21): 4794-4809. https://doi.org/10.1049/gtd2.12997

[10] Mahapatra, U., Rahman, M.A., Islam, M.R., Hossain, M.A., Sheikh, M.R.I., Hossain, M.J. (2025). Adversarial training-based robust model for transmission line's insulator defect classification against cyber-attacks. Electric Power Systems Research, 245: 111585. https://doi.org/10.1016/j.epsr.2025.111585

[11] Fang, H., Xiao, J.W., Wang, Y.W. (2023). A machine learning-based detection framework against intermittent electricity theft attack. International Journal of Electrical Power & Energy Systems, 150: 109075. https://doi.org/10.1016/j.ijepes.2023.109075

[12] Sharma, R., Joshi, A.M., Sahu, C., Nanda, S.J. (2023). Detection of false data injection in smart grid using PCA based unsupervised learning. Electrical Engineering, 105(4): 2383-2396. https://doi.org/10.1007/s00202-023-01809-3

[13] Yadav, P.K., Biswal, M., Vemuganti, H. (2024). Smart meter data management challenges. In Smart Metering, pp. 221-256. https://doi.org/10.1016/B978-0-443-15317-4.00002-6

[14] Kapadiya, K., Ramoliya, F., Gohil, K., Patel, U., Gupta, R., Tanwar, S., Rodrigues, J.J.P.C., Alqahtani, F., Tolba, A. (2025). Blockchain-assisted healthcare insurance fraud detection framework using ensemble learning. Computers and Electrical Engineering, 122: 109898. https://doi.org/10.1016/j.compeleceng.2024.109898

[15] Khan, N., Amir Raza, M., Ara, D., Mirsaeidi, S., Ali, A., Abbas, G., Shahid, M., Touti, E., Yousef, A., Bouzguenda, M. (2023). A deep learning technique Alexnet to detect electricity theft in smart grids. Frontiers in Energy Research, 11: 1287413. https://doi.org/10.3389/fenrg.2023.1287413

[16] Ahmad, H., Gulzar, M.M., Mustafa, G., Habib, S. (2025). AI-based approach for detecting FDI attacks in load frequency control for centralized multi-area power systems. Computers and Electrical Engineering, 123: 110060. https://doi.org/10.1016/j.compeleceng.2025.110060

[17] Abdulqadder, I.H., Aziz, I.T., Zou, D. (2024). DT-Block: Adaptive vertical federated reinforcement learning scheme for secure and efficient communication in 6G. Computer Networks, 254: 110841. https://doi.org/10.1016/j.comnet.2024.110841

[18] Tayebi, M., El Kafhali, S. (2025). A novel approach based on XGBoost classifier and Bayesian optimization for credit card fraud detection. Cyber Security and Applications, 3: 100093. https://doi.org/10.1016/j.csa.2025.100093

[19] Kong, J., Jiang, W., Tian, Q., Jiang, M., Liu, T. (2023). Anomaly detection based on joint spatio-temporal learning for building electricity consumption. Applied Energy, 334: 120635. https://doi.org/10.1016/j.apenergy.2022.120635

[20] Abdulkareem, O.A., Kontham, R.K., Mahmood, F.E. (2024). Securing smart grids: Machine learning-driven ensemble intrusion detection for IoT RPL networks. International Journal of Safety and Security Engineering,

14(5): 1517-1525. https://doi.org/10.18280/ijsse.140519
[21] Tripathi, A.K., Pandey, A.C., Sharma, N. (2024). A new electricity theft detection method using hybrid adaptive sampling and pipeline machine learning. Multimedia Tools and Applications, 83(18): 54521-54544. https://doi.org/10.1007/s11042-023-17730-7
[22] Mohamed, M., Mahmood, F.E., Abd, M.A., Rezkallah, M., Hamadi, A., Chandra, A. (2023). Load demand forecasting using eXtreme gradient boosting (XGboost). In 2023 IEEE Industry Applications Society Annual Meeting (IAS), Nashville, TN, USA, pp. 1-7. https://doi.org/10.1109/IAS54024.2023.10406613
[23] Abbas, S., Bouazzi, I., Ojo, S., Sampedro, G.A., Almadhor, A.S., Al Hejaili, A., Stolicna, Z. (2023). Improving smart grids security: An active learning approach for smart grid-based energy theft detection. IEEE Access, 12: 1706-1717. https://doi.org/10.1109/ACCESS.2023.3346327
[24] Nawaz, A., Ali, T., Mustafa, G., Rehman, S.U., Rashid, M.R. (2023). A novel technique for detecting electricity theft in secure smart grids using CNN and XG-boost. Intelligent Systems with Applications, 17: 200168. https://doi.org/10.1016/j.iswa.2022.200168
[25] Kritika, E. (2025). A comprehensive literature review on ransomware detection using deep learning. Cyber Security and Applications, 3: 100078. https://doi.org/10.1016/j.csa.2024.100078
[26] Nayak, R., Jaidhar, C.D. (2023). Employing feature extraction, feature selection, and machine learning to classify electricity consumption as normal or electricity theft. SN Computer Science, 4(5): 483. https://doi.org/10.1007/s42979-023-01911-0
[27] Iftikhar, H., Khan, N., Raza, M.A., Abbas, G., Khan, M., Aoudia, M., Touti, E., Emara, A. (2024). Electricity theft detection in smart grid using machine learning. Frontiers in Energy Research, 12: 1383090. https://doi.org/10.3389/fenrg.2024.1383090
[28] Sun, Y., Sun, X., Hu, T., Zhu, L. (2023). Smart grid theft detection based on hybrid multi-time scale neural network. Applied Sciences, 13(9): 5710. https://doi.org/10.3390/app13095710
[29] Wen, H., Liu, X., Lei, B., Yang, M., Cheng, X., Chen, Z. (2025). A privacy-preserving heterogeneous federated learning framework with class imbalance learning for electricity theft detection. Applied Energy, 378: 124789. https://doi.org/10.1016/j.apenergy.2024.124789
[30] Shakerinia, S., Meyabadi, A.F., Vahedi, M., Salehi, N., Moghaddam, M.S. (2023). Optimal operation of microgrids with worst-case renewable energy outage: A mixed-integer bi-level model. IEEE Access, 11: 59804-59815. https://doi.org/10.1109/ACCESS.2023.3285480
[31] Din, J., Su, H., Ali, S., Salman, M. (2024). Research on blockchain-enabled smart grid for anti-theft electricity securing peer-to-peer transactions in modern grids. Sensors, 24(5): 1668. https://doi.org/10.3390/s24051668
[32] Zhu, S., Xue, Z., Li, Y. (2024). Electricity theft detection in smart grids based on omni-scale CNN and AutoXGB. IEEE Access, 12: 15477-15492. https://doi.org/10.1109/ACCESS.2024.3358683
[33] Sulaiman, A., Mahmood, F.E., Majeed, S.A. (2023). Long-term solar irradiance forecasting using multilinear predictors. International Journal of Electrical and Electronic Engineering & Telecommunications, 12(2): 134-141. https://doi.org/10.18178/ijeetc.12.2.134-141
[34] Qi, R., Zheng, J., Luo, Z., Li, Q. (2022). A novel unsupervised data-driven method for electricity theft detection in AMI using observer meters. IEEE Transactions on Instrumentation and Measurement, 71: 1-10. https://doi.org/10.1109/TIM.2022.3189748
[35] Badr, M.M., Mahmoud, M.M., Abdulaal, M., Aljohani, A.J., Alsolami, F., Balamsh, A. (2023). A novel evasion attack against global electricity theft detectors and a countermeasure. IEEE Internet of Things Journal, 10(12): 11038-11053. https://doi.org/10.1109/JIOT.2023.3243086
[36] Abdulqadder, I.H., Aziz, I.T., Flaih, F.M. (2025). Robust electricity theft detection in smart grids using machine learning and secure techniques. International Journal of Intelligent Engineering & Systems, 18(1): 1021-1033. https://doi.org/10.22266/ijies2025.0229.73
[37] Du, H., Lv, L., Guo, A., Wang, H. (2023). AutoEncoder and LightGBM for credit card fraud detection problems. Symmetry, 15(4): 870. https://doi.org/10.3390/sym15040870
[38] Aggarwal, S., Kaddoum, G. (2024). Authentication of smart grid by integrating QKD and blockchain in SCADA systems. IEEE Transactions on Network and Service Management, 21(5): 5768-5780. https://doi.org/10.1109/TNSM.2024.3423762