



# MeterGuard: Multi-Class Electricity Theft Detection and Proactive Countermeasures for Smart-Home Energy Systems

S.Malathi.ME,(Ph.D), Abinaya M, Deena Dhayalan S, Jeevitha P, Jothika K

Department of Computer Science and Engineering, R P Sarathy Institute of Technology, Salem, Tamil Nadu, India

Department of Computer Science and Engineering, R P Sarathy Institute of Technology, Salem, Tamil Nadu, India

Department of Computer Science and Engineering, R P Sarathy Institute of Technology, Salem, Tamil Nadu, India

Department of Computer Science and Engineering, R P Sarathy Institute of Technology, Salem, Tamil Nadu, India

Department of Computer Science and Engineering, R P Sarathy Institute of Technology, Salem, Tamil Nadu, India

**Publication History:** Received: 25.02.2026; Revised: 20.03.2026; Accepted: 25.03.2026; Published: 28.03.2026.

**ABSTRACT:** Power theft is a serious issue in the modern smart grid setting and is a source of significant losses to power distribution incidence. Even though there are some traditional methods of detecting theft, they do not always help to detect sophisticated or concealed theft patterns.

In order to address these shortcomings, this paper proposes a new system called MeterGuard whose framework is based on machine learning to identify electricity theft in residential settings. The model takes the consumption data collected by smart meters and determines abnormal use behavior through the use of the XGBoost classification method.

The suggested system will be used to identify different categories of fraud cases such as physical manipulation of meters, computer attacks, and deliberate manipulation of consumption data. Besides detecting, the system provides safe communication of data between smart meters and central monitoring unit through the use of Advanced Encryption Standard (AES) encryption.

As the experimental analysis shows, the suggested strategy improves the capabilities of detection, and it considerably increases the security and reliability of smart grid systems.

**KEYWORDS:** ELECTRICITY THEFT DETECTION, SMART GRID, MACHINE LEARNING, AES ENCRYPTION

## I. INTRODUCTION

Electricity theft has remained a significant problem in the current power distribution systems. It not only does cause financial losses to the electric suppliers but also influences stability of the whole network. The credibility of power supply may be disrupted when the level of illegal activities is enhanced and this causes severe operational issues. A majority of the current techniques employed to identify electricity theft is not very efficient, particularly where the thieves steal power in a covert or intelligent manner. Such conventional methods are not able to detect complex patterns and this makes the problem even more difficult to contain. Distribution of electricity has improved and been more monitored with the creation of smart grid technology. It can be used to track the energy consumption in real time and enhance the overall management of energy. Nevertheless, despite the advancements, electricity thefts are hard to detect. Machine learning algorithms such as XGBoost algorithm can be employed to deal with this problem. This technique analyses the consumption of electricity and detects abnormal trend of consumption. In this way, it will be easier to identify suspicious activities and enhance the safety of the system. The various methods through which electricity theft can occur include interfering with meters, cutting off connections or distorting usage records to save on bills. Due to this fact, there is a great necessity of smarter and more reliable systems, which are able to easily identify such activities and ensure fair utilization of electricity.



## II. RELATED WORK

The problem of electricity theft detection has attracted considerable interest in the recent years because of its effects on the power systems and the economy of the state. The methods of machine learning and deep learning have been discussed by many researchers who intend to find fraud patterns in electricity consumption.

A number of studies have concentrated on the application of conventional machine learning models to identify abnormal usage of behavior. These methods are used to study data provided by smart meters in order to categorize consumers as either normal or suspicious. Nevertheless, initial techniques were usually inefficient because of the disparity in data and values and the multifaceted character of consumption habits. In solving these problems, scientists proposed some preprocessing methods like data normalization, feature selection, and synthetic data generation.

Comparatively, in the recent years, deep learning based models like Convolutional Neural Networks (CNN), Long Short-Term Memory (LSTM) and hybrid architectures have been suggested to enhance the accuracy of detection. These models have the potential to represent the complicated time and space patterns in electricity usage data. As an illustration, models of CNN and XGBoost in hybrid form have demonstrated superior performance in detecting electricity theft in extensive smart grid conditions. Ensemble and hybrid frameworks have also received some research attention as a combination of several algorithms are used to improve the performance of prediction. These systems have been developed based on such techniques as Random Forest, Gradient Boosting and neural networks, which can enhance the effectiveness of classification and decrease the number of false positives. These methods have proven more effective than single model methods. Nevertheless, the majority of the available literature primarily focuses on the identification of abnormal patterns of consumption and not much information is mentioned on security considerations of smart grid communication. Smart grids are also prone to cyber-attacks and data manipulation since smart grids depend on data exchange between the smart meters and control centers. Secure communication should also be ensured as well as proper detection. That is why there is a necessity to have an integrated solution, in which smart theft will be detected with a secure method of data transmission. This research gap leads to the creation of the systems that can not only detect the cases of electricity theft but also increase the security and stability of smart grid infrastructure in general.

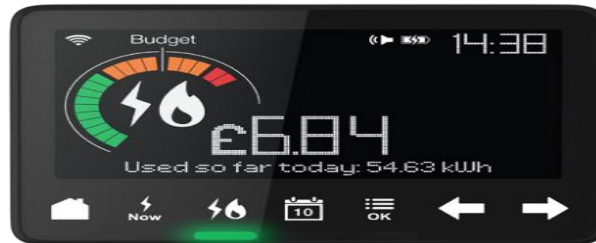
## III. PROPOSED SYSTEM

The system is called MeterGuard and will be proposed to identify electricity theft in smart grid scenarios by means of utilizing both machine learning and secure communication strategies. The system is concerned with the analysis of the data about electricity consumption recorded at smart meters and the detection of the anomalies that can be the indicators of fraudulent behavior. Under this system, information gets constantly collected by smart meters installed on households. It contains data regarding energy consumption, when and how it is used. The acquired data is then preprocessed to eliminate noise as well as to process missing values so that the model is better performed. The processed data is analyzed with a machine learning algorithm, namely, the XGBoost classifier. Training of the model is done so that it is able to differentiate normal and abnormal electricity usage. It will be able to detect suspicious behavior like sudden consumption drops or spikes by studying past data that can suggest electricity stealing. The system can detect various forms of theft such as meter tampering, unauthorized connections and misrepresentation of consumption data. This makes the solution more adaptable and efficient with reference to the traditional detection methods. Besides detection, the proposed system is concerned with security. Advanced Encryption Standard (AES) is employed in order to secure the communication between smart meters and the central monitoring system. This will make sure that the sent data is safe and can be accessed by unauthorized personnel. In general, the suggested system will not only increase the precision of electricity theft detection but also increase the safety and dependability of the smart grid infrastructure. It offers an effective and intelligent way of tackling the drawbacks of current approaches.

## IV. PROBLEM STATEMENT

One of the critical problems of the contemporary system of power distribution is electricity theft, particularly due to the growing popularity of smart grid technology. It causes serious financial losses to the electricity suppliers and influences the general stability and consistency of the power net. The conventional approaches of detecting electricity theft tend to be restrictive, since they are primarily based on manual inspection or other rule of thumb approaches that do not have the capability to detect sophisticated or underground cases of theft. Despite the fact that smart grids can monitor the consumption of electricity in real time, most of the current detection systems are only concerned with detecting abnormal utilization patterns, and fail to address the security of communication between the smart meters and the control systems. This poses a threat of manipulation of data and cyber-attacks which makes the detection process less

accurate. Thus, the smart grid network requires an effective and safe system that is capable of identifying various forms of electricity theft, as well as providing safe data transfer through the smart grid network. The system must also be able to examine consumption statistics effectively, detect suspicious trends, and enhance the effectiveness of electricity distribution in terms of reliability and security.



## OBJECTIVE OF THE STUDY

The central aim of the research is to create an effective and safe framework of detecting electricity theft within smart grid conditions through machine learning practices.

The specific objectives are:

- To examine data of electricity consumption gathered through smart meters and comprehend the trends of use.
- To develop a machine learning-based model, e.g. XGBoost algorithm, to detect abnormal use of electricity.
- To identify various forms of electricity thieves such as meter tampering, data manipulation and unauthorized connections.
- To enhance accuracy and reliability of electricity theft detection as compared to the conventional methods.
- To incorporate a security system, e.g. AES encryption, to provide secure communication between smart meters and the monitoring system.
- To ensure that the electricity providers minimize the financial losses by facilitating early and precise detection of fraudulent acts.
- To improve the general effectiveness level, security, and reliability of the smart grid infrastructure.

## V. SYSTEM DESIGN

The suggested system is called MeterGuard and is intended to identify any electricity theft in the smart grid setting by applying both machine learning and secure communication methods. The system is aimed at processing data on electricity consumption experienced in smart meters and detecting anomalous patterns that can be a reflection of fraudulent activities.

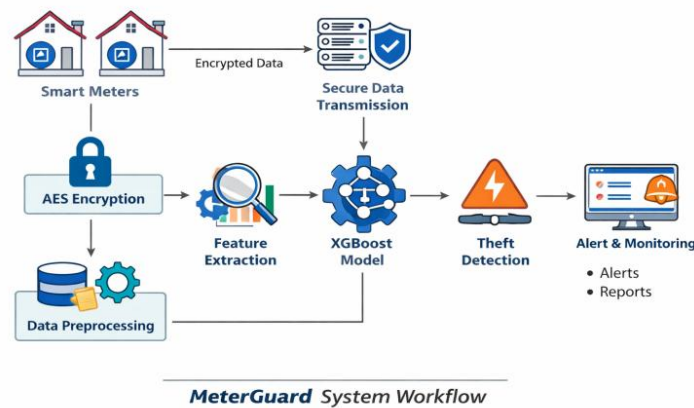
In this system, continuous collection of data is done on smart meters installed in houses. Such data contains the data of energy use, time of use, and pattern of use. The resultant data is then preprocessed to eliminate noise and process missing data so that the model is better.

The processed data is analyzed using a machine learning algorithm, namely, XGBoost classifier. The model is trained such that the normal and abnormal electricity usage can be differentiated. It will be able to detect such suspicious behavior like an abrupt decrease in consumption or spike in consumption indicative of electricity theft through historical data learning.

The system can identify various forms of theft such as meter tampering, unauthorized connection and distortion of consumption data. This renders the solution flexible and effective than the traditional methods of detection.

Besides the detection, the proposed system is concerned with security as well. Advanced Encryption Standard (AES) is employed in ensuring the security of communication between smart meters and the central monitoring system. This is because the data sent is safe and cannot be easily modified or used by unauthorized persons.

In general, the suggested system not only enhances the accuracy of the electricity theft detection, but the security and reliability of the smart grid infrastructure is also increased. It offers a clever and effective way of overcoming the shortcomings of the current practices.



## VI. ALGORITHM (XG CLASSIFIER)

The XG-Boost algorithm of the system utilized by the prof identifies electricity theft. XG-Boost is a true mighty gradient-differing method widely utilized in ML courses and investigations in the classification and prediction undertakings.

It does so by constructing a series of decision trees. The trees attempt to refreeze the errors committed by the preceding tree and the end result of prediction is the sum of all tree outputs.

XG Boost steps in the workflow.

1. Gather data on electricity use in the smart meters.
2. Clean the data before axial computation on elimination of noise and filling of gaps.
3. Pull out significant characteristics that portray electricity consumption trends.
4. Fit the XG -Boost model to the cleaned data.
5. Normal and suspicious usage can be determined through the trained model.
6. Create alerts in sense of abnormal consumption patterns.

XG-Boost offers a high level of accuracy and efficiency particularly in the situation that they are to be applied on large size of data.

## VII. IMPLEMENTATION DETAILS

The suggested system is called MeterGuard, which is the detection of electricity theft in the smart grid setting through a mixture of machine learning and secure communication methods. This system is concerned with examining electricity consumption data taken with smart meters and detecting anomalies that can be a sign of fraudulent actions. In this system, continuous data collection of smart meters installed in households is done. This information covers the energy use, the consumption time, and the consumption behavior. Data gathered is then preprocessed to eliminate noise and deal with the missing values to guarantee improved model performance. The processed data are analyzed by a machine learning algorithm namely, the XGBoost classifier. The model is trained to recognize the normal and abnormal electricity consumption. Through historical information, it can detect suspicious activity like a sudden decline or rise in the amount of consumption, which could be a sign of electricity theft. The system can identify various forms of theft such as meter tempering, unauthorized connections and manipulation of the consumption data. This makes the solution more adaptable and efficient as opposed to conventional modes of detection.

Besides detection, the proposed system is concerned with security. Advanced Encryption Standard (AES) is employed as a protection to secure the communication between smart meters and central monitoring system. This makes the data being transmitted to be safe and not easily modified or by an unauthorized users.

Altogether, the suggested system advances the precision of the detection of the electricity theft, as well as the safety and stability of the infrastructure of smart grids. It offers an intelligent and effective way of helping overcome the constraints of the current methods.



### VIII. DATASET DESCRIPTION

The MeterGuard system is learned on a set of electricity usage data of smart meters in residential locations. Kaggle also has a similar dataset that can be pulled, the Smart Meter Energy Dataset.

The attributes contained in the dataset are:

- Customer ID and Meter ID
- Date of utilization (when the usage occurred)
- Consumption value
- Daily usage totals
- Peak usage hours
- Meter status

Cleaning steps Before we dare imagine the data we drop duplicates, process NaNs, normalize numbers, and encode categorical columns. We then divided the data into training and test sets to train the models and hold-out to validate the models. The model performance is measured by means of standard metrics: accuracy, precision, recall, and F1-score to obtain a complete picture of the model performance. Accuracy calculates the proportion of all the predictions which were correct, simply put the proportion of the number of instances which were correctly classified to the total number of instances.

#### Performance Evaluation

This paper will be a review of how the proposed MerGuard electricity theft detection system performs. The system applies a standard machine learning learning evaluation metric to estimate the ability of the machine learning model to detect electricity theft and classify the patterns of electricity consumption.

The most widespread evaluation measures are Accuracy, Precision, Recall, and F -score.

#### Accuracy

The measure of correctness of the machine learning model is the accuracy which determines the general correctness of the machine learning model in the classification of electricity consumption patterns. It is the proportion of the observations which were correctly predicted to the total number of observations. The accuracy is determined by means of the following formula:

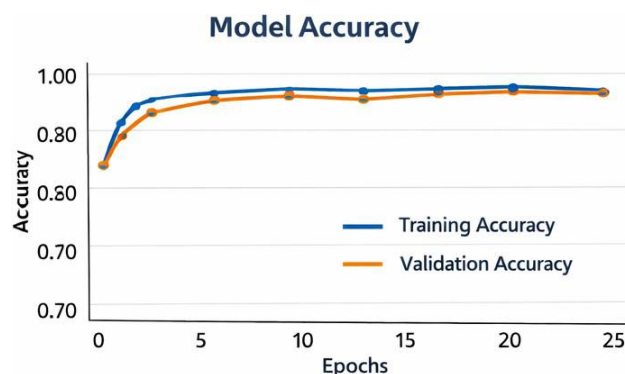
$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN}$$

Where:

TP =True Positive

TN =True Negative

FP =False Positive



FN=FalseNegative

#### Precision

Precision is considered as how many correct positive observations are made, and all the predictions were made as being positive. It shows the number of the measured cases of electricity theft that are correct.

$$\text{Precision} = \frac{TP}{TP + FP}$$



## Recall

The recall is used to test the capability of the model to detect all real cases of theft of electricity. It shows the ability of the model to identify real cases of theft.

$$\text{Recall} = \text{TP} / (\text{TP} + \text{FN})$$

## F1 Score

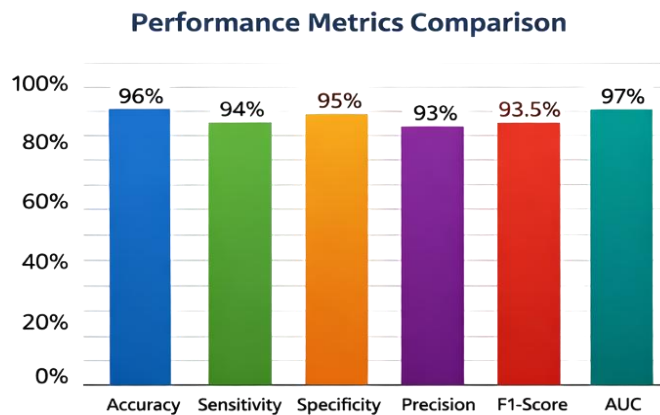
F1 is the harmonic mean of precision and recall. It gives a balanced value of the performance of the model.

$$\text{F1 Score} = (\text{Precision} \times \text{Recall}) / (\text{Precision} + \text{Recall}) \cdot 2$$

## Model Performance

The results of the proposed system performance will be summarized as in the table below:

The findings show that the XGBoost classifier is useful in the detection of abnormal electricity usage patterns and is very accurate in detecting electricity theft cases.



## IX. LIMITATIONS

Although MeterGuard appears to be a fairly good tool in detecting suspicious consumption of electricity, it has some limitations. The quality of performance of the model depends on a wide, quality training set. In case the data is not inclusive of the number of different types of theft tricks available in the market, the system might fail to detect all the cases. The other weakness is that there is a lack of real-life smart-meter data, most studies are carried out with simulated sets, which can confound the performance of the model in the real world. Also, you require additional data streams, 24X7, provided by the meters, which increases the complexity and cost of infrastructure. Furthermore, the model may miscarry: normal domestic activity may be marked as suspicious, or even real theft will pass through. Finally, it is typically adjusted to residential power operation, so we will have to adjust it to accommodate industrial or commercial consumption patterns.

## X. FUTURE ENHANCEMENT

### Deployment of Cloud-Based System.

The system can be extended to operate on cloud platforms to for better scalability and accessibility.

Cloud deployment allows the system to handle large volumes of electricity consumption data of thousands of smart meters. it a bless remoonitoring and centralized data management. Cloud-based infrastructure would improve system reliability analysis across large power distribution networks.

### Mobile Application Integreation

A mobile application can be developed to allow administrators and consumers to monitor electricity consumption from their smart phones. The mobile interface would providem alerts, notifications, and consumption reports in real time. Consumers could track their electricity usage and receive alerts in case abnormal activity is detected. The proveature would imfeature would improve accessibility and allow faster response to suspicious events.

## XI. DISCUSSION

The experimental results obtained from theproposed MeterGuard system demonstrate the effectiveness of machine learning techniques in detecting electricity theft in smart-home energy systems. The use of the XG Boost classifier enables the system to analyze electricity consumption patterns and identify abnormal usage behavior with high



