Kalildass JANAKIRAMAN, PhD Candidate (corresponding author)
kalidass.it@gct.ac.in
Government College of Engineering, Srirangam, Trichy, Tamil Nadu, India

Purusothaman THIYAGARAJEN, PhD
purusothaman.t@gct.ac.in
Government College of Technology, Coimbatore, Tamil Nadu, India

Gowrison GENGAVEL, PhD
gowrisonirtt@gmail.com
Government College of Engineering, Erode, Tamil Nadu, India

Enhancing Cyber Resilience in Smart Meter Networks Against Resource-Stealing Attacks Using Hybrid Attack Classification

Abstract. *The Advanced Metering Infrastructure (AMI) represents the cyber backbone of the smart grid, making it highly susceptible to various cyber threats. This research addresses key challenges in AMI transmission networks, including low detection accuracy, model over fitting, and scalability limitations. To mitigate these vulnerabilities, in the proposed model analyses the information to detect and classify instances of resource stealing or anomalous behaviour. The proposed model Ensemble 1D-MN3 employs an integrated 1D CNN and MobileNetV3 architecture with hyper parameter tuning for classification task, which is particularly effective at extracting meaningful one-dimensional features and capturing complex temporal relationships in time-series data. This results in more accurate and reliable detection outcomes. Overall, the implementation of the proposed framework provides a robust and scalable solution for anomaly detection in smart metre data, making it highly suitable for real-world deployment within AMI networks.*

Keywords: *attack, one-dimensional features, classification and time-series data.*

JEL Classification: C32, C63, C83, D81.

Received: 8 August 2025	Revised: 1 March 2026	Accepted: 6 March 2026

1. Introduction

The advancement of the energy sector has driven the transition from traditional electromechanical meters to smart meters (SMs) (Rizwan et al., 2022). Conventional meters are basic mechanical devices that record total energy consumption, typically relying on manual monthly readings (Klyuev et al., 2022). These devices are limited by their inability to provide real-time data and are susceptible to human error. Due to their inefficiency and limited functionality (Rezaeimozafar et al., 2022), traditional meters have been progressively replaced by smart meters. Smart meters

DOI: 10.24818/18423264/60.1.26.14
© 2026 The Authors. Published by Editura ASE. This is an open access article under the CC BY license (http://creativecommons.org/licenses/by/4.0/).

are digital devices capable of measuring energy consumption in real time (Udo et al., 2024) and transmitting the data directly to utility companies. They facilitate demand-side management, support dynamic pricing, and enable both providers and consumers.

In Advanced Metering Infrastructure networks (Medina et al., 2024), smart meters (SMs) serve as critical components in the modernisation of power grids by enabling real-time data transmission and interaction. AMI systems provide valuable insights into energy consumption patterns (Farooq et al., 2025), thereby enhancing operational efficiency. These frameworks support two-way communication between consumers and utility providers (Hernández-Álvarez et al., 2024), facilitate remote monitoring, and eliminate the need for manual meter readings (Alam et al., 2024). Additionally, features such as demand response enable dynamic pricing models, allowing consumers to optimise their energy usage and achieve cost savings (Ajiboye et al., 2024). Given the critical importance of security in AMI, it is essential to safeguard the data exchanged among meters, communication networks, and utility companies from cyber threats. Overall, AMI plays a pivotal role in transforming traditional power grids into more efficient, intelligent, and sustainable systems (Saleem et al., 2024; Koukouvinos et al., 2025).

Despite the numerous benefits that smart meters bring to power distribution, they also introduce significant cyber security challenges. As conventional power grids evolve into smart grids, smart meters are integrated into highly digitised infrastructures, thereby increasing their exposure to cyber threats (Prabakar et al., 2022). These threats include data breaches, unauthorised access to sensitive consumer information, and large-scale system disruptions caused by attacks on communication channels between smart meters and grid control components. Their integration into broader network environments expands the attack surface, creating opportunities for malicious actors to exploit vulnerabilities – such as launching Distributed Denial of Service (DDoS) attacks (Hasan et al., 2023). Traditional cyber security mechanisms, including firewalls and Intrusion Detection Systems (IDS), which were insufficient to address the dynamic and interconnected nature of modern smart grids.

To overcome these limitations, Machine Learning (ML) and Artificial Intelligence (AI) techniques have been adopted to enhance the smart grid's capacity to detect and respond to cyber-attacks (Kotsiopoulos et al., 2021; Chen et al., 2023). These advanced methods strengthen IDS by identifying patterns based on common characteristics as well as subtle anomalies that can indicate malicious activity.

The application of AI-driven algorithms for attack classification and IDS (Chatzimiltis et al., 2024) significantly enhances the security of smart grids. Preventing disruptions within the grid infrastructure is critical to ensuring the reliability of the energy supply and safeguarding consumer data. As cyber threats continue to evolve, there is an increasing demand for more efficient and adaptive cyber security measures to maintain the resilience of smart grid systems. This study investigates advanced approaches to attack classification and IDS within the

communication framework of smart meters, leveraging innovative ML algorithms to reinforce privacy and security across the network.

1.1 Research Objectives

The major contribution of the proposed framework is listed as follows:

- The Sea Gull Optimisation Algorithm is employed for efficient feature selection, aiming to extract the most relevant features from the decrypted data to enhance model performance.
- A MobileNetV3 and 1D Convolutional Neural Network (CNN), optimised through hyper parameter tuning, is utilised to accurately detect resource theft and classify the presence or absence of attacks in smart meter readings.
- The effectiveness of the proposed approach is evaluated using standard performance metrics, including accuracy, confusion matrix, ROC curve, recall, F1-score, and precision.

1.2 Paper Organisation

This paper is organised into four sections. Section 2 provides a review of existing models that utilise various Deep Learning (DL) and Machine Learning (ML) algorithms. Section 3 describes the methodology of the proposed approach, along with the corresponding algorithms. Section 4 presents the simulation results and performance analysis of the proposed Ensemble 1D-MV3 approach. Finally, Section 5 concludes the paper and outlines potential directions for future research.

2. Literature review

Machine Learning and Deep Learning algorithms are employed to enhance the security of smart meters by detecting abnormal patterns, identifying cyber-attacks, and predicting potential real-time threats. These advanced techniques offer robust protection while maintaining the reliability and privacy of both energy consumption data and network communications.

2.1 ML in the security of smart meters

The study (Alam et al., 2024) utilised the Decision Tree (DT) algorithm for both classification and regression tasks to detect false data and monitor communication losses. This approach effectively addressed the challenges related to maintaining data consistency and ensuring privacy in smart meters, especially in the presence of cyber attacks and environmental disturbances.

In a related study (Saleem et al., 2024), Long Short-Term Memory (LSTM) networks were utilised to achieve accurate detection of electricity consumption patterns. Additionally, the AMLODA (Adversarial Machine Learning Occupancy Detection Avoidance) model was introduced to inject noise into the data, effectively obscuring usage patterns while preserving billing accuracy. This model addressed

security concerns in consumption detection using time-of-use data from smart meters and significantly reduced threat levels bringing the Matthews Correlation Coefficient (MCC) down to zero, thereby ensuring data privacy without compromising performance. Similarly, study (Ajiboye et al., 2024) proposed the use of the XGBoost algorithm for Electricity Theft Detection (ETD) by analysing customer electricity usage patterns. XGBoost outperformed traditional classifiers such as K-Nearest Neighbors (KNN), Random Forest (RF), and Support Vector Machines (SVM) by achieving higher detection accuracy and fewer false positives.

2.2 DL in the security of smart meters

Deep Learning (DL) plays a pivotal role in enhancing the security of smart meters (SMs) by identifying attack characteristics and adapting to evolving cyber threats. It enables real-time analysis of large volumes of data to detect patterns indicative of unauthorised access and data manipulation.

The study presented in (Prabhakar et al., 2022) proposed a data-driven approach for detecting non-technical losses (NTLs) using smart meter (SM) data. To address dataset imbalance, six different theft scenarios were introduced to enhance data diversity. A hybrid model combining a Multi-Layer Perceptron (MLP) with a Gated Recurrent Unit (GRU) was developed for electricity theft detection. In (Klyuev et al., 2022), a hybrid method leveraging CNN (Chatzimiltis et al., 2024) introduced to detect energy theft within smart grids (SGs). This approach integrated CNN-based feature extraction with traditional machine learning classifiers to identify instances of data tampering in SMs. Also, the CNN-based hybrid model achieved high accuracy in distinguishing between legitimate and fraudulent consumption patterns, significantly enhancing energy theft detection in smart grid environments.

A subsequent study (Kiasari et al., 2024) proposed a hybrid approach that combines Deep Learning (DL) with a Support Vector Machine (SVM) to detect electricity theft. In this method, a deep CNN was used to extract features from smart meter (SM) data collected over various time intervals, ranging from hourly to daily. These extracted features were then classified into theft and non-theft categories using the SVM. To mitigate the issue of over-fitting, a dropout layer was integrated into the CNN architecture.

3. Model specification

The proposed Ensemble 1D-MN3 aims to detect and classify the information from smart meters to the administration centre. To accomplish this, the proposed framework uses RSA and ECC algorithms for the encryption and decryption processes, the Seagull Optimisation Algorithm for feature selection, and an integrated 1D-CNN and MobileNetV3 algorithm for the classification process. The procedure for Ensemble 1D-MN3 is demonstrated in Figure 1, where the process starts by loading the AMI dataset. After loading the dataset, the smart meter information is initially encrypted and soon after decrypted by the administrator using

RSA and ECC algorithms, then transferred to the subsequent process. After decryption, the data undergoes a cleaning and normalisation process, where 80% of the dataset is allocated to the training set and the remaining 20% is used for testing. After dataset separation, feature selection employed using seagull optimisation algorithm, where the process starts by selecting the appropriate features for the model.

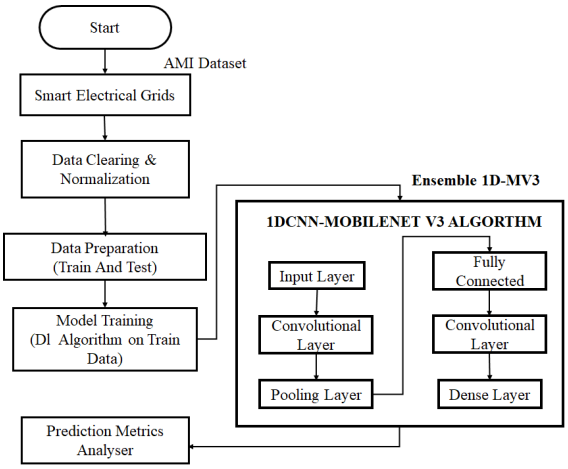

Figure 1.Overall proposed work Ensemble 1D-MN3
Source: Authors' own creation.

Once the key features are selected, classification of the decrypted data is carried out using the proposed Ensemble 1D-MN3 method and effectively detects any resource stealing or attacks on the metering information, thus providing an effective AMI process. Finally, the performance of the proposed method is evaluated by comparing it against various existing methods using multiple performance metrics.

3.1 Feature selection using Seagull algorithm

While various algorithms exist for feature selection, the proposed approach utilises the Seagull Optimisation Algorithm (SGO) due to its simplicity and ease of implementation. SGO provides strong global and local search capabilities, enabling efficient exploration and exploitation of the search space. Consequently, it can produce high-quality solutions with fewer parameters compared to other optimisation techniques. The SGO performs feature selection by emulating the hunting behaviour of seagulls, navigating the search space to identify the most relevant features from a dataset. Initially, a population of candidate solutions (i.e., feature subsets) is randomly generated and evaluated using a fitness function, typically based on classification accuracy. Through an iterative process, SGO applies both local search and global exploration strategies to refine feature selection – eliminating less relevant features while retaining those that significantly enhance the

model's predictive performance. This process continues until a predefined stopping criterion is met, such as reaching a maximum number of iterations or achieving convergence. The result is an optimal subset of features that best represents the dataset and improves model performance. Furthermore, this approach not only strengthens the effectiveness of deep learning models, but also enhances the accuracy and efficiency of AMI systems, leading to more reliable monitoring and decision-making. Besides, the process involved in SGO process is expressed as follows,

a) Initialisation

The population of seagull is represented as N. Followed by, initialising the position of the seagulls randomly within the search space.

b) Fitness Evaluation

In this step, fitness value for each seagull is in the population is calculated and the fitness value of each seagull is compared to detect the global optimum value.

c) Exploration

The new position of each sea gull is calculated after migration. This process involves different steps which model the collision avoidance and movement towards the best search agent. Thus, to avoid the collision between adjacent search agents, an extra variable v is used, where it aids in estimating the new search agent location.

$$\mathrm{C_s} = \mathrm{v} \times \mathrm{post_s} \quad (1)$$

In the above equation(1), position of search agent is depicted as $\mathrm{C_s}$, which does not collide with other agents and $\mathrm{post_s}$ is denoted as the present position of search agent and x is represented as the present iteration. Eventually, v is considered as the movement behaviour of search agent in a given search space.

Then, the movement of seagull towards the best position using the below equation (2),

$$\mathrm{Mvm_s} = \mathrm{Bh} \times (\mathrm{post_{best}(t)} - \mathrm{post_s(t)}) \quad (2)$$

Here, Bh represents the random number to balance exploration, $\mathrm{Mvm_s}$ represents the population of seagulls which move towards$\mathrm{post_{best}}$. The behaviour of Bh is randomised which is responsible for balancing between exploitation and exploration properly and Bh is estimated as from below equation,

$$\mathrm{Bh} = 2 \times \mathrm{A}^2 \times \mathrm{rndm} \quad (3)$$

Where, the variable rndm is denoted as random number, which lies between the range of [0,1). Eventually, the search agent can update its position with respect to best search agent by,

$$\mathrm{Dis_s} = |\mathrm{C_s} + \mathrm{Mvm_s}| \quad (4)$$

Where, $\mathrm{Dis_S}$ is denoted as the distance between the search agent and best fit search agent. Thus, by using these mathematical equations, final position of the seagull is calculated.

d) Exploitation

The search agents utilise the history and experience of the search process. After the collision avoidance, search agents move towards the best neighbour's direction and eventually, the search agents update its position relative to the best search agent.

e) Termination Condition

At last, it is important to check if the algorithm has reached the termination condition and if the termination condition is met, output the global optimal position and fitness value, or else update the position until it reaches desired output. Eventually, the selected features are fed to 1DCNN-MobileNetV3 model for classification in order to determine the presence and absence of attack intervention.

3.2 Attack Classification using Ensemble 1D-MN3 model

MobileNetV3 is a lightweight and efficient deep learning architecture specifically designed for deployment in resource-constrained environments, such as smart meter systems. It leverages depth-wise separable convolutions to significantly reduce the number of parameters and computations while maintaining high accuracy. This makes it well-suited for real-time analysis and classification tasks in energy monitoring scenarios. Once the relevant features are selected, they are passed to a MobileNetV3-based classification model to determine the presence or absence of malicious attacks in smart meter readings. The architecture enhances efficiency by decomposing the standard convolution into two operations: Depth-wise Convolution and Point wise Convolution. This separation reduces the total number of multiplications, significantly lowering the computational cost compared to traditional convolutions. MobileNetV3 also integrates advanced design components such as Inverted Residuals, Linear Bottlenecks, the Hard-Swish activation function, and Squeeze-and-Excitation (SE) modules. Together, these innovations enable MobileNetV3 to deliver high performance with reduced computational overhead, making it a practical choice for secure and efficient attack detection in AMI systems. The mathematical equations followed for the depth-wise convolution applies a single filter per input channel and the equation is demonstrated as

$$Y_d^{(c)} = X^{(c)} * W_d^{(c)} + b_d^{(c)} \quad (5)$$

Here, $Y_d^{(c)}$ is expressed as the depthwise convolution for channel (c), $X^{(c)}$ is denoted as the input feature map for channel (c), $W_d^{(c)}$ and $b_d^{(c)}$ is represented as the depthwise filter for channel and bias term for channel (c). The below equation shows the point wise convolution, where the point wise convolution is a 1x1 convolution that combine the outputs of the depth wise convolution across channels,

$$Y_p = Y_d * W_p + b_p \quad (6)$$

Where, y_p is denoted as the point wise convolution, Y_d is defined as the depthwise convolution, W_p represents the point wise filter and b_p is defined as the bias term for the point wise layer. The swish activation function MobileNetv3 is defined as,

$f(x) = x.\sigma(x)$, where $\sigma(x) = \frac{1}{1+e^{-x}}$ is the sigmoid function.

Likewise, One-Dimensional Convolutional Neural Network (1D-CNN) is designed to operate on sequential data such as time-series signals, text, or any data organised in a 1D format. The architecture typically comprises Convolutional layers, pooling layers, flattening layers, and fully connected (dense) layers, working together to extract and classify meaningful patterns from the input data. The input layer accepts one-dimensional sequential data such as time-series, sensor readings, or textual input which were arranged in a 1D structure suitable for processing. Convolutional layers apply a 1D Convolutional filter (also known as kernels) to the input data to extract features. As the filters slide along the sequence, they compute dot products between the filter weights and segments of the input data. This operation generates feature maps that emphasise important patterns, such as trends, peaks, or recurring sequences. The pooling layers are responsible for reducing the dimensionality of the feature maps, thus lowering the computational load and helping the model become more resilient to small variations in the input. Common types include max pooling and average pooling.

After convolution and pooling, the resulting multi-dimensional output is flattened into a 1D vector. This transformation prepares the data for processing by the dense (fully connected) layers. Fully Connected Layers (Dense Layers) layers perform the final classification or regression task. They apply learned weights to the flattened feature vector and output the final prediction. The network learns these weights during training to optimise performance based on the task at hand. This layered structure allows 1D-CNNs effectively learn and classify patterns in sequential data, and making them highly suitable for applications in time-series forecasting, anomaly detection, and natural language processing. Therefore, mathematical equations involved in hybrid 1D-CNN-MobileNetv3 is given as follows, Where, the convolution operation in a 1D-CNN is mathematically expressed as,

$$Y = X * W + b \tag{7}$$

Here, Y is the output feature map, X is defined as input feature map, W is convolutional filter and b is defined as bias term.

Eventually, the outputs from MobileNetv3 and 1D-CNN is integrated using concatenation and depicted follows,

$$Z = [Y_{MBNet}, Y_{spacnn}) \tag{8}$$

This equation describes the concatenation process by joining the feature vectors from the two models into a single, longer feature vector. Y_{MBNet} is represented as the output feature vector from the MobileNetv3 model and , Y_{spacnn} denotes the output feature vector from the 1D-CNN by representing the features that capture the 1Drelationships and patterns and z denotes the resulting combined feature vector after concatenation. Hence, the final classification layer is defined in the following equation,

$$P(y|Z) = \frac{e^{ZW}+b}{\sum_j e^{ZW_j}+b_j} \tag{9}$$

The above equation represents the softmax function, which is employed for converting the combined functions into probabilities for each class. Z denotes the combined feature vector from the concatenation step and this is the input to the final classification layer. W is depicted as the weight matrix of the FCL and b represents the bias vector of the FCL. $e^{ZW} + b$ represents the linear transformation of the combined features and $e^{ZW_j} + b_j$ highlights the sum of the exponential scores overall classes j.

```
Input: Smart meter dataset D, maximum iterations T, population size N, learning rate α, number of epochs E
Output: Predicted class label (Normal / Attack)

 Begin
   // ------------------------- Data Preprocessing -------------------------
   Load raw AMI dataset D
   Decrypt smart meter readings using E3S scheme
   Clean and normalize numerical attributes
   Convert time series values into fixed length input sequences

   // ------------------------- SGO Initialization -------------------------
   Initialize seagull population S = {s1, s2, …, sN}
   For each seagull si in S do
      Randomly generate binary feature vector Fsi
   End For

  // ------------------------- Fitness Evaluation -------------------------
  For each seagull si do
     Train Ensemble 1D-MN3 using selected features Fsi
     Compute fitness as:
     Fitness(si) = λ × Accuracy - (1 − λ) × |Fsi| / Ftotal
  End For

  // ------------------------- SGO Iterative Optimization ------------------
  For iteration t = 1 to T do
     Identify best seagull sbest with maximum fitness
     For each seagull si do
        // Migration (Exploration)
        Update position of si using collision avoidance and movement rules
        // Attack behavior (Exploitation)
        Move si towards sbest using spiral and attraction functions
        Recompute fitness(si)
     End For
```

```
    End For

    Select final best feature subset Fbest = F(sbest)
    // ------------------------- Model Construction -------------------------
    Build MobileNetV3 module:
        Apply depthwise convolution:
            Yd(c) = X(c) * Wd(c) + bd(c)
        Apply pointwise convolution:
            Yp = Yd * Wp + bp
        Apply Hard-Swish activation
    Build 1D-CNN module:
        Apply 1D convolution:
            Ycnn = X * W + b
        Apply pooling, flatten output

    // ------------------------- Feature Fusion -----------------------------
    Concatenate features:
        Z = [YMobileNetV3 , Ycnn]

    // ------------------------- Classification Layer -----------------------
    Apply softmax:
        P(y|Z) = exp(ZW + b) / Σj exp(ZWj + bj)

    // ------------------------- Training Phase -----------------------------
    For epoch e = 1 to E do
        Forward propagate training data through MobileNetV3 and 1D-CNN
        Compute loss using cross entropy
        Backpropagate and update weights using Adam optimiser
    End For

    // ------------------------- Prediction and Evaluation ------------------
    For each test instance xi do
        Compute class probability P(y|xi)
        Assign label with highest probability
    End For

    Compute evaluation metrics: Accuracy, Precision, Recall, F1-score
    Return predicted labels and performance metrics
End
```

Figure 2. Pseudo code for Ensemble classification of Ensemble 1D-MV3 method
Source: Authors' own creation.

Thus, incorporation of the MobileNetv3- 1D-CNN has showcased the effectiveness performance in terms of detecting and classifying the presence of attacks or electricity theft from the smart meter readings. The pseudocode of the proposed method Ensemble 1D-MV3 is shown in Figure 2. In this method, MobileNetV3 serves as the primary feature extractor, capturing high-level abstract features from the input data. To further enhance classification capability, additional processing layers are appended to the MobileNetV3 architecture to refine these extracted features. Simultaneously, 1D-CNN layers are integrated into the model to effectively capture one-dimensional temporal or sequential patterns inherent in smart meter readings. The hybrid model is trained on a labelled dataset containing smart meter data associated with different categories of cyber attacks. Through supervised learning, it learns to distinguish between normal operational behaviour and malicious activity.

4. Results and discussion

The performance results of the proposed model are test out using the benchmark dataset which is available in www.kaggle.com/datasets/eyabaklouti/smartmeter-energy-consumption-data.

Besides, Table-1 shows the hyper parameter tuning employed in the proposed model. The Table 1 outlines the key parameters used in a machine learning model. The model employs a learning rate of 0.00001, a batch size of 64, and is trained over 10 epochs.

Table 1. Hyperparameter values

Parameters	Learning Rate	Batch Size	Epochs	Dropout Rate	Weight Decay	Optimizer	Momentum	Activation Function
Values	0.00001	64	10	0.2	1.00E-04	Adam	0.9	ReLu

Source: Authors' processing.

To mitigate overfitting, a dropout rate of 0.2 is applied, alongside a weight decay (L2 regularisation) of 1.00E-04. The Adam optimiser is used for training, with a momentum of 0.9. Finally, the ReLU (Rectified Linear Unit) activation function is used within the model's architecture.

The model's performance is then evaluated using standard classification metrics such as accuracy, precision, recall, and F1-score, to assess its effectiveness in detecting and classifying smart meter attacks.

4.1 Performance Analysis

The performance of the Ensemble 1D-MN3 in detecting resource stealing and cyber-attacks on smart meters is demonstrated through a series of steps. Initially, meter data is collected from Host 1. A secure connection is established between Host 1 and Host 7 using a secure communication protocol. During this process, cryptographic keys are exchanged to ensure a secured communication channel,

verifying successful authentication, and confirming that the correct hosts are involved in the data exchange. Following the secure handshake, the meter data from Host 1 is encrypted and securely transmitted to Host 7. Upon receipt, Host 7 decrypts the data, recovering the original information without any loss or tampering. This successful round of encryption and decryption confirms the reliability and security of the communication process. The authentication sequence between Host 1 and Host 7 is illustrated in Figure 3.

Figure 4 presents a histogram of predicted probabilities for the "natural" (non-attack) class. The x-axis represents the prediction probability values, while the y-axis shows the frequency of predictions at each probability level. The red dashed line indicates the mean predicted probability, which is close to 1. This clustering near 1 suggests that the model confidently classifies most instances as natural. The slightly lower mean value implies that the model maintains high and average confidence in all predictions.

Figure 5 illustrates the topology of the AMI network. In the diagram, red lines represent connections between controllers, blue lines indicate switch connections, and green lines correspond to host connections. The two red-highlighted nodes function as controllers, acting as the central management units of the network. Four switches, depicted as blue nodes, facilitate communication among devices, while various hosts, shown as green nodes, represent endpoint devices within the network.

Figure 3. Switch Authentication of Host 1 to Host 7
Source: Obtained by Authors' work.

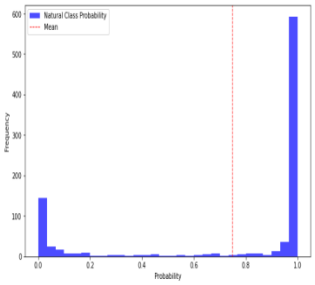

Figure 4. Distribution of predicted probabilities for natural class
Source: Obtained by Authors' work.

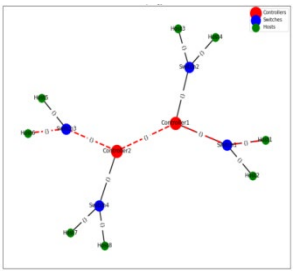

Figure 5. Smart Meter AMI Network topology with Attack Detection
Source: Obtained by Authors' work.

Dashed red lines between the controllers represent communication paths specifically related to attack detection, whereas solid lines connecting hosts, switches, and controllers indicate standard operational communication. In this centralised architecture, the controllers play a critical role in managing the flow of data between switches and hosts, ensuring secure and efficient network operation.

4.2 Evaluation Metrics and Model Performance Analysis

Confusion matrix is shown in Figure 6 presents the predicted labels with the actual labels of the model. The terms TP, TN, FP, and FN represent true positives, true negatives, false positives, and false negatives, respectively.

Specifically, 670 instances are correctly predicted as class 0 (true negatives), and 31 instances are false positives, where the model incorrectly predicted class 1 while the actual label was 0. Additionally, 21 instances are false negatives, where the model predicted class 0 but the true label was 1, and 200 instances are true positives, where the model correctly predicted class 1.

Figure 7 shows the accuracy of the model across training epochs. The x-axis represents the number of epochs, while the y-axis displays accuracy values ranging from approximately 0.75 to 1.0. The blue line indicates training accuracy, which steadily increases and approaches nearly 100%. The orange line represents validation accuracy, which also improves and stabilises slightly below the training accuracy. This trend suggests that the model is learning effectively from the training data without showing signs of severe over fitting.

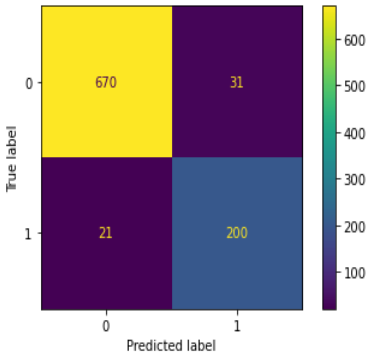

Figure 6. Confusion Matrix
Source: Authors' processing.

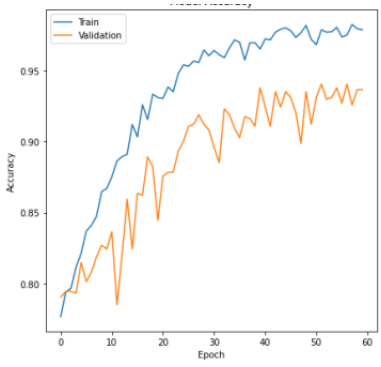

Figure 7. Model Accuracy
Source: Authors' processing.

Figure 8 illustrates the training and validation loss over epochs. The x-axis indicates the number of epochs, and the y-axis shows loss values ranging from 0 to approximately 0.5. The training loss (blue line) consistently decreases toward zero, indicating that the model is successfully minimising prediction errors on the training set. The validation loss (orange line) shows some fluctuations, indicating variability in generalisation, but it does not increase significantly, suggesting that the model maintains stable performance on unseen data.

The Receiver Operating Characteristic (ROC) curve of the proposed model is shown in Figure 9.

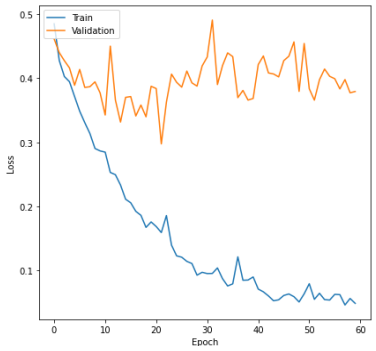

Figure 8. Model Loss
Source: Authors' processing.

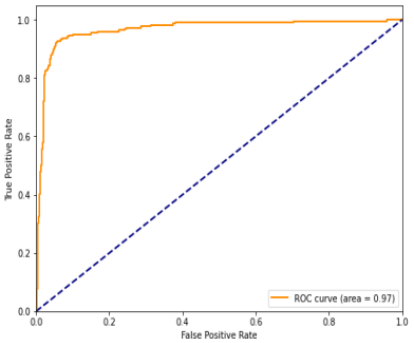

Figure 9. ROC curve
Source: Authors' processing.

The x-axis represents the False Positive Rate (FPR), and the y-axis represents the True Positive Rate (TPR). The ROC curve illustrates the trade-off between sensitivity and specificity as the classification threshold varies. The model achieves an Area Under the Curve (AUC) of 0.97, indicating excellent performance. A curve closer to the top-left corner reflects a better ability of the model to distinguish between positive and negative instances while minimising false positives.

4.3 Comparative Analysis

Though the performance of the proposed model is known to be superior to the existing RF, DT and KNN, it is very much substantial to compare the efficacy of the proposed work with other existing approaches, and it is deliberated in the present section. Overall, the data emphasises that the Ensemble 1D-MN3 offers a significant improvement in detection accuracy compared to both traditional and ensemble-based methods.

(Naeem et al., 2025) compared previous models and the Table-2 depicts the performance of several algorithms with proposed algorithm in terms of TPR and TNR. The algorithms analysed include "Con.", FedAvg, P-Trusted, P-Untrusted, Malicious SPSs, and a proposed algorithm. The proposed model algorithm generally demonstrates competitive performance, achieving a TPR of 87.3% and a TNR of 83.6%. In comparison, FedAvg shows significantly lower TPR (28.2%) and TNR (25.1%). The P-Trusted algorithm reaches a TPR of 86% and a TNR of 86.2%, while P-Untrusted has a TPR of 23.8% and a TNR of 37.4%. Malicious SPSs achieves the highest TPR at 92.7%, but its TNR is 85.3%. The "Con." algorithm shows a TPR of 81.2% and a TNR of 63.1%. Overall, the proposed algorithm offers a balanced performance with reasonably high TPR and TNR values, demonstrating its potential effectiveness for smart meter attack detection process.

Table 2. TPR and TNR Comparative Analysis

Algorithms	Con.	FedAvg	P – Trusted	P – Untrusted	Malicious SPSs	Ensemble 1D-MN3
TP Rate (%)	81.2	28.2	86	23.8	92.7	87.3
TNR (%)	63.1	25.1	86.2	37.4	85.3	83.6

Source: Authors' processing.

Likewise, the performance comparison in (Anin et al., 2024), the Table-3 provides a comprehensive performance comparison of several models and proposed Ensemble 1D-MV3 for a detection task, evaluating them across key metrics: Detection Rate, False Alarm Rate, Highest Difference (between Detection and False Alarm Rates), Accuracy, Precision-Recall, and AUC.

The existing model also demonstrates strong performance, with a balanced Detection Rate of 92.95% and a low FAR of 3.68%, yielding an Accuracy of 94.65%. It achieves a Precision-Recall score of 98.8 and an AUC of 98.5, indicating robust classification capabilities. Among alternative approaches, the ConvLSTM model offers a favourable trade-off, maintaining a relatively low FAR of 4.06% and a high Accuracy of 92.39%, supported by competitive Precision-Recall and AUC scores of 97.9 each.

Table 3. Performance metrics of Ensemble 1D-MV3

Model Structure	Detection Rate (%)	False Alarm Rate (%)	Highest Difference (%)	Accuracy (%)	Precision-Recall	Area Under the Curve
FFN	91.3	6.83	84.47	92.21	98	97.1
2-D CNN	90.66	12.32	78.34	89.02	96.9	96
CONVLSTM	89.22	4.06	85.16	92.39	97.9	97.9
2D-Conv LSTM	92.95	3.68	89.27	94.65	98.8	98.5
Ensemble 1D-MN3	99.22	1.06	95.16	99	98.9	99

Source: Authors' processing.

In contrast, the FFN and 2D-CNN models exhibit higher false alarm rates, which negatively impact their overall accuracy despite achieving reasonable detection rates. The graphical representation of Ensemble 1D-MV3 in terms of accuracy, false alarm rate, and detection rate is shown in Figure 10.

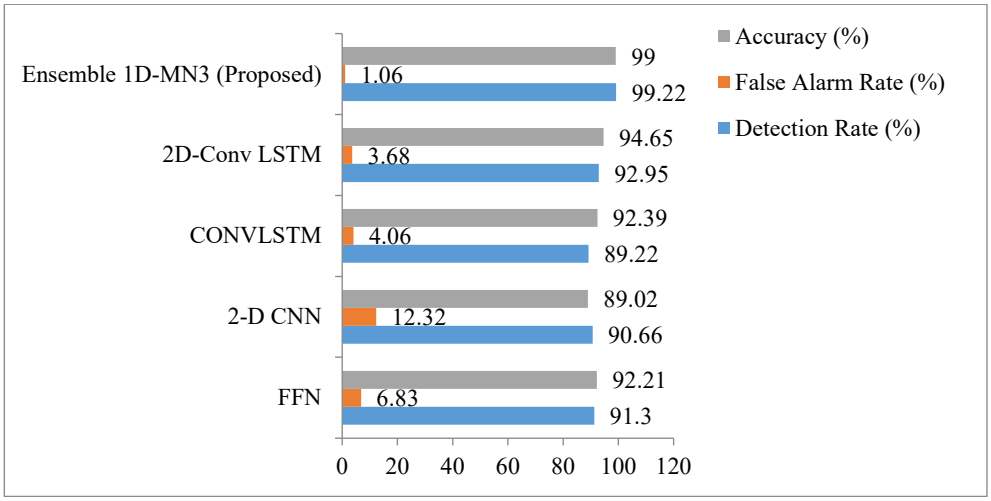

Figure 10.Graphical Representation of Ensemble 1D-MV3
Source: Authors' processing.

The proposed model outperforms nearly all existing approaches, achieving an exceptional Detection Rate of 99.22% and a very low FAR of 1.06% and highest Difference Metric of 95.16%, along with excellent overall performance metrics, in Accuracy of 99%, a Precision-Recall score of 98.9, and an AUC of 99. Overall, the proposed model represents a significant advancement for cyber-attack detection in smart meter systems, offering superior reliability, precision, and robustness.

5. Conclusions

The proposed work focuses on a smart meter attack detection system by integrating various algorithms and techniques. Initially, RSA and ECC algorithms are employed for data encryption and decryption to ensure secure communication. Once the data is decrypted using the corresponding public and private keys, the SGO are applied for feature selection to identify the most relevant attributes. Subsequently, the Ensemble 1D-MN3 model is utilised to detect and classify the decrypted data, distinguishing between normal readings and instances of electricity theft or cyber-attacks. The proposed model delivers promising results, achieving an accuracy of 99%, a recall of 98.6%, a precision of 98.12%, and an F1-score of 99.32%. Compared to both internal benchmarks and existing external methods, the model demonstrates superior performance. Despite these encouraging outcomes, future work will explore the integration of federated learning techniques to further improve detection accuracy while enhancing data privacy.

References

[1] Ajiboye, P.O., Agyekum, K.O.B.O., Frimpong, E.A. (2024), *Privacy and security of advanced metering infrastructure (AMI) data and network: a comprehensive review. Journal of Engineering and Applied Science,* 71(1), 91.

[2] Alam, M.U., Ali, B., Ullah, S., Hafeez, M.H. (2024), *Intelligent Fault Detection and Diagnostic System for Smart Meter. Power System Technology,* 48(1), 2223-2238.

[3] Anin, J., Khan, M.J., Abdelsalam, O., Nabil, M., Hu, F., Alsharif, A. (2024), *Efficient and Privacy-Preserving ConvLSTM-based Detection of Electricity Theft Cyber-Attacks in Smart Grids. IEEE Access*, 12, 153089-153104.

[4] Chatzimiltis, S., Shojafar, M., Mashhadi, M.B., Tafazolli, R. (2024), *A Collaborative Software Defined Network-Based Smart Grid Intrusion Detection System. IEEE Open Journal of the Communications Society*, 1, 700-711.

[5] Chen, Z., Li, J., Cheng, L., Liu, X. (2023), *Federated-WDCGAN: A federated smart meter data sharing framework for privacy preservation. Applied Energy,* 334, 120711.

[6] Farooq, A., Shahid, K., Olsen, R.L. (2025), *Prioritization of smart meters based on data monitoring for enhanced grid resilience. Computer Communications,* 234, 108082.

[7] Hasan, M.K., Habib, A.A., Islam, S., Safie, N., Abdullah, S.N.H.S., Pandey, B. (2023), *DDoS: Distributed denial of service attack in communication standard vulnerabilities in smart grid applications and cyber security with recent developments. Energy Reports,* (9), 1318-1326.

[8] Hernández-Álvarez, L., Bullón Pérez, J.J., Queiruga-Dios, A. (2024), *Security in advanced metering infrastructures: Lightweight cryptography*. *Logic Journal of the IGPL,* p. jzae074.

[9] Kiasari, M., Ghaffari, M., Aly, H.H. (2024), *A comprehensive review of the current status of smart grid technologies for renewable energies integration and future trends: The role of machine learning and energy storage systems. Energies,* (16), 4128.

[10] Klyuev, R.V., Morgoev, I.D., Morgoeva, A.D., Gavrina, O.A., Martyushev, N.V., Efremenkov, E.A., Mengxu, Q. (2022), *Methods of forecasting electric energy consumption: A literature review. Energies,* 15(23), 8919.

[11] Kotsiopoulos, T., Sarigiannidis, P., Ioannidis, D., Tzovaras, D.J. (2021), *Machine learning and deep learning in smart manufacturing: The smart grid paradigm. Computer Science Review,* 40, 100341.

[12] Koukouvinos, K.G., Koukouvinos, G.K., Chalkiadakis, P., Kaminaris, S.D., Orfanos, V.A., Rimpas, D. (2025), *Evaluating the Performance of Smart Meters: Insights into Energy Management, Dynamic Pricing and Consumer Behaviour*. *Applied Sciences,* 15(2), 960.

[13] Medina, J., Rojas-Cessa, R. (2024), *AMI-Chain: a scalable power-metering blockchain with IPFS storage for smart cities. Internet of Things,* 25, 101097.

[14] Naeem, H., Ullah, F., Srivastava, G. (2025), *Classification of intrusion cyber-attacks in smart power grids using deep ensemble learning with metaheuristic-based optimization*. *Expert Systems,* 42(1), e13556.

[15] Prabhakar, P., Arora, S., Khosla, A., Beniwal, R.K., Arthur, M.N., Arias-Gonzáles, J.L., Areche, F.O. (2022), *Cyber security of smart metering infrastructure using median absolute deviation methodology. Security Communication Networks,* 1, 6200121.

[16] Rezaeimozafar, M., Monaghan, R.F., Barrett, E., Duffy, M. (2022), *A review of behind-the-meter energy storage systems in smart grids. Renewable Sustainable Energy Reviews,* 164, 112573.

[17] Rizwan, A., Rasheed, R., Javed, H., Farid, Q., Ahmad, S.R. (2022), *Environmental sustainability and life cycle cost analysis of smart versus conventional energy meters in developing countries*. *Sustainable Materials Technologies,* 33, e00464.

[18] Saleem, M.U., Usman, M.R., Yaqub, M.A., Liotta, A., Asim, A. (2024), *Smarter Grid in the 5G Era: Integrating the Internet of Things with a Cyber-Physical System*. *IEEE Access,* 12, 34002-34018.

[19] Udo, W.S., Kwakye, J.M., Ekechukwu, D.E., Ogundipe, O.B. (2024), *Smart grid innovation: machine learning for real-time energy management and load balancing. International Journal of Smart Grid Applications,* 22(4), 405-423.