An Enriched RPCO-BCNN Mechanisms for Attack Detection and Classification in SCADA Systems

S. SHITHARTH1, (Member, IEEE), KANTIPUDI MVV PRASAD2, (Senior Member, IEEE), K. SANGEETHA1, PRAVIN R. KSHIRSAGAR3, THANIKANTI SUDHAKAR BABU4, (Senior Member, IEEE), AND HASSAN HAES ALHELOU5, (Senior Member, IEEE)

1Department of Computer Science and Engineering, Kebri Dehar University, Kebri Dehar 001, Somali, Ethiopia
2Department of Electronics and Telecommunication, Symbiosis Institute of Technology, Pune, Maharashtra 412115, India
3Department of Artificial Intelligence, G. H. Raisoni College of Engineering, Naggur 440016, India
4Department of Electrical and Electronics Engineering, Chaitanya Bharathi Institute of Technology, Hyderabad 500075, India
5Department of Electrical Power Engineering, Faculty of Mechanical and Electrical Engineering, Tishreen University, Latakia, Syria

Corresponding authors: Hassan Haes Alhelou (alhelou@ieee.org); Thanikanti Sudhakar Babu (sudhakarbabu66@gmail.com)

ABSTRACT Providing security to the Supervisory Control and Data Acquisition (SCADA) systems is one of the demanding and crucial tasks in recent days, due to the different types of attacks on the network. For this purpose, there are different types of attack detection and classification methodologies have been developed in the conventional works. But it limits with the issues like high complexity in design, misclassification results, increased error rate, and reduced detection efficiency. In order to solve these issues, this paper aims to develop an advanced machine learning models for improving the SCADA security. This work comprises the stages of preprocessing, clustering, feature selection, and classification. At first, the Markov Chain Clustering (MCC) model is implemented to cluster the network data by normalizing the feature values. Then, the Rapid Probabilistic Correlated Optimization (RPCO) mechanism is employed to select the optimal features by computing the matching score and likelihood of particles. Finally, the Block Correlated Neural Network (BCNN) technique is employed to classify the predicted label, where the relevancy score is computed by using the kernel function with the feature points. During experimentation, there are different performance indicators have been used to validate the results of proposed attack detection mechanisms. Also, the obtained results are compared with the RPCO-BCNN mechanism for proving the superiority of the proposed attack detection system.

INDEX TERMS Supervisory control and data acquisition (SCADA), Markov chain clustering (MCC), preprocessing, security, rapid probabilistic correlated optimization (RPCO), block correlated neural network (BCNN) and attack detection.

I. INTRODUCTION
In the recent days, the Supervisory Control and Data Acquisition (SCADA) [1], [2] is one of the widely used control systems in the industrial sectors like traffic maintenance, electric power generation, nuclear systems, water/waste water treatment oil mining, and space stations. It is highly important to secure the SCADA systems against the attacking activities of malfunctioning and threatening [3]–[5]. The present SCADA systems comprise certain security features (such as user interfaces, communication, and control logic), which helps to increase the system complexity, but maintaining those features is one the critical task [6]. Moreover, controlling the large amount of data in SCADA systems is highly difficult due to the data loss availability, which makes the architecture is more vulnerable to the attackers. The general communication structure [7] of SCADA systems is depicted in Fig 1, which contains the components of master station unit, sub-control unit, Programmable Logic Controller (PLC), Remote Terminal Unit (RTU) and Intelligent End Device (IED).

Typically, the attack detection [8]–[10] in SCADA network or mining system is performed based on the dynamic update of data obtained from the network database. In the traditional works, there are different optimization and classification methods [11]–[13] have been developed for attack prediction in SCADA systems. Also, the matching prediction
is highly complicated due to the presence of more irrelevant features in the database [14]. Thus, the existing works could use the machine learning techniques [15], [16] for selecting the best matching features between the query data and set of extracted features. The different types of machine learning [2], [17]–[20] techniques used in the conventional works are Support Vector Machine (SVM), Relevance Vector Machine (RVM), Neural Networks (NN), and other deep learning models. In which, the sequence pattern analysis and neural network techniques are widely used for identifying the attacking activities based on the relevant features. Still, it facing the challenges in predicting the accurate class of data with respect to the large amount of node characteristics. In order to solve this problem and to increase the classification accuracy, an improved feature optimization and classification methodologies are implemented in the proposed work. The major objectives behind this work are as follows:

- To pre-process the given data by eliminating the irrelevant information and to offer the normalized output data, the Markov Chain Clustering (MCC) mechanism is utilized in the attack detection system.
- To reduce the time complexity of processing the large amount of sensor data with best feature selection, a new optimization technique, named as, Rapid Probabilistic Correlated Optimization (RPCO) is developed.
- To improve the attack classification performance by identifying the best matching features, the Block Correlated Neural Network (BCNN) based classifier is implemented.

The remaining sections of this paper are structuralized as follows: the conventional feature optimization and classification techniques related to the SCADA attack detection process are reviewed in Section II. Then, the detailed description about the proposed RPCO-BCNN attack detection and classification system is presented in Section III. The experimental and comparative analysis of both existing and proposed techniques are validated in Section IV. Finally, the overall paper is concluded with its future scope in Section V.

II. RELATED WORKS

This section reviews the conventional feature extraction, optimization, and classification methodologies used for improving the security of SCADA systems. Typically, the SCADA systems [21] are extensively used monitoring and controlling the distribution networks for ensuring the reliability and maintaining the operational cost consumption of network. Due to the increased utilization of SCADA systems [22], it is very challenging task for providing security to these control systems. Also, the reliability and security [23] are the major factors that must be addressed for ensuring the reliability of SCADA networks. The cyber-security [24] is one of the key issue involved in the SCADA systems, because the cyber-attacks could damage the components and performance of controlling system. So, it must be addressed by deploying the proper risk assessment and security mechanisms. This paper [25] intends to detect the malicious activities on the SCADA systems by using the temporal pattern analysis model. It finds the set of temporal patterns and used as the feature vectors for improving the attack recognition performance of classifier. A semi-supervised learning [26] methodology has been utilized to detect the anomalies by increasing the cyber-defense capabilities of SCADA systems. The cyber-physical systems [27] are monitored and controlled with the deployment of SCADA systems, which facilitates an efficient cyber-physical operations against the harmful attacks.

Ghosh and Sampalli [28] presented a comprehensive survey on various security standards and protocol layers used for establishing the secure communication in SCADA systems, where the mechanisms are reviewed under the categories of attack prevention and detection. The SCADA network could face different types of security threats such as data repudiation, loss of integrity, confidentiality, and availability. Moreover, this paper investigates the major security guidelines and crypto suits used in the recent days for SCADA systems. Based on this study, it is analyzed that providing end-to-end security and addressing the key management issues are need to be highly concentrated in the SCADA network for an efficient attack detection and prevention processes. In paper [6], the special features are illustrated for improving the security of SCADA systems. For this analysis, the gas pipeline dataset has been utilized to validate the efficiency of the decision tree mechanism. Moreover, the different types of metrics used for the implementation of IDS in SCADA systems are also discussed, which includes application logs, host logs, physical metrics and network traffic. Here, the network and payload based feature attributes are mainly considered for classification, in which the network feature set contains...
five different types of attributes, and payload set contains 12 different attributes. Based on this study, it is observed that the performance of SCADA-IDS systems are highly depends on the set of features used for classification. In paper [9], a clear survey is presented about the different types of security protocols, and threats in SCADA system. Also, it discussed about various communication protocols used in the SCADA systems with its corresponding data rates, maximum distance measures, and topologies.

Ferrag et al. [29] investigated the performance of seven different deep learning mechanisms used for developing a cyber-security IDS, where the dataset selection plays a vital role for the detection of intrusions. For this analysis, around 35 distinct datasets have been utilized for estimating the efficiency and accuracy of deep learning models. Gumaei et al. [4] developed a new security control approach for efficiently detecting the cyber-attacks by the use of correlation based feature selection mechanism. The main intention of using this technique is to improve the attack detection efficiency by removing the irrelevant features. Then, these optimal set of features are used by the Instance based Learning (IBL) classification technique for predicting the cyber-attacks from the dataset. From this work, it is studied that the accuracy and detection performance of IDS is highly depends on the optimal set of features. In work [30], an integrated framework has been developed for detecting anomalies using the cyber-physical systems with the help of Gaussian Mixture Model (GMM) and Kalman Filtering (KF) approach. For this analysis, two different public datasets such as UNSW-NB15 and power system are utilized to assess the performance of suggested framework. Based on this concept, it is analyzed that privacy preservation and anomaly detection are the most essential factors for improving the security of SCADA systems. Khan and Serpen [2] analyzed the impacts of some common threats against SCADA systems such as MPCI, MSCI, DoS, MFCI, Recon, CMRI and NMRI. Here, a binary classification technique is utilized to categorize the normal and attacking classes based on the set of patterns. To validate the performance of the technique, there are different types of datasets have been tested in this work.

Khan et al. [11] developed a hybrid model for automatically predicting the anomalies in SCADA systems by using the reliable feature extraction mechanism. Here, three different feature reduction mechanisms such as Independent Component Analysis (ICA), Principal Component Analysis (PCA), and Canonical Correlation Analysis (CCA) have been utilized to reduce the dimensionality of features for improving the accuracy of intrusion detection and classification. Krithivasan et al. [31] deployed a hypergraph based CNN model for the detection of cyber-attacks in an Industrial Control System (ICS) with the use of PCA based dimensionality reduction mechanism. The motive of this paper is to minimize the input feature space for eliminating the Geometrical features based on the Helly property of hypergraph, which helps to obtain a reduced false positives and increased precision values. Based on this work, it is analyzed that the uninformative features could degrade the performance of entire attack detection and classification system. For this purpose, the most set of features are selected by using the PCA model and, the optimal feature attributes are fed to the CNN model for predicting the anomalies. Lai et al. [18] intended to extract the critical features by using the CNN for improving the efficiency of attack detection in SCADA systems. Here, the strong correlation between the feature vectors are estimated for the detection of anomalies with the help of feature mapping model. The main concentrations behind this work are ensure the timely attack prediction, to obtain the reduced cost of error, and to improve the ability of imbalanced data handling. From this work, it is studied that the efficiency of attack classification is based on the feature selection and imbalance data processing models. Table 1 presents the survey on various existing techniques used attack detection and classification in SCADA systems, which also discuss about the advantages of disadvantages of each technique.

From this above survey, it is analyzed the attack detection and classification on SCADA systems is highly depends on the features of dataset, which plays a vital role in many SCADA application systems. Also, the entire performance of classification system is based on the set of attributes extracted from the input data. Moreover, the detection efficiency and accuracy are considered as the major measures and extensively used for evaluating the effectiveness of SCADA systems.

III. PROPOSED METHODOLOGY

This section presents the clear illustration about the proposed attack detection and classification mechanisms used for SCADA security. Here, a combination of RPCO-BCNN mechanisms are implemented for accurately detecting the attacks from the given dataset. The novel contribution behind this work is based on the selection of optimal parameters used for improving the security of SCADA network architecture. Here, the RPCO technique is implemented to select the most suitable parameters by reducing the set of features, which helps to reduce training time of classifier. The major parameters considered during this process are entropy, output weights of sensors, energy properties, trust ratings, Lebesgue measure, probability density of sequence, overall power, likelihood ratio, average sigma parameter, and amount of packets transmitted. Based on the optimized set of features, the BCNN classification technique accurately predicts the intrusions from the given datasets. Moreover, it separates the dataset into various blocks according to the clustered index obtained from MCC, then it finds the relevancy between the training and testing feature sets. This type of optimal clustering and classification of SCADA dataset can efficiently improves the accuracy of entire system.

The overall flow of the proposed system is depicted in Fig 2, which comprises the following working stages:

1. Preprocessing
2. Feature Selection based optimization
3. Classification
### TABLE 1. Survey on existing attack detection and classification methodologies.

| Author & Year          | Methodology                                                                 | Advantages/Disadvantages                  |
|------------------------|-----------------------------------------------------------------------------|-------------------------------------------|
| Ghosh and Sampali [28] | Various security standards and protocols for establishing secure communication n in SCADA systems. | 1. Increased end-to-end security.         |
|                        |                                                                             | 2. Crypto-suitability.                    |
|                        |                                                                             | 3. Inefficient attack detection.          |
|                        |                                                                             | 4. Reduced performance outcomes.          |
| Al-Asiri [6]           | Cyberphysical IDS for SCADA systems.                                        | 1. Average performance metrics.           |
|                        |                                                                             | 2. Increased accuracy.                    |
|                        |                                                                             | 3. High false positive rate.              |
|                        |                                                                             | 4. It does not have the ability to handle large dimensional data. |
| Gumaci, et al [4]      | Correlation based Feature Selection (CFS) with Instance based Learning (IBL) mechanism for developing an efficient IDS. | 1. Reduced overhead.                      |
|                        |                                                                             | 2. High accuracy.                         |
|                        |                                                                             | 3. Reduced computational efficiency.      |
|                        |                                                                             | 4. Not having the ability to process the large data with varying size. |
| Keshk, et al [30]      | GMM-KF based anomaly detection framework for SCADA systems.                 | 1. Better feature mapping.                |
|                        |                                                                             | 2. Consumes the minimized amount of time for processing the transformed data. |
|                        |                                                                             | 3. It does not the space to transform the high dimensional data into a low dimensional data. |
| Khan and Serpan [2]    | Three stage classification system for intrusion detection in SCADA systems.  | 1. It is capable of handling of different datasets. |
|                        |                                                                             | 2. Still, it limits with the problems of reduced accuracy and detection efficiency. |
| Khan, et al [11]       | Hybrid Multi-Level (HML) IDS for predicting anomalies in SCADA systems.      | 1. Minimized false acceptance rate.       |
|                        |                                                                             | 2. Simple training process.               |
|                        |                                                                             | 3. High complexity in algorithm design.   |
|                        |                                                                             | 4. Reduced detection efficiency.          |
| Kirthivasan, et al [31]| Hypergraph based CNN model is developed for predicting anomalies in ICS.    | 1. High accuracy.                         |
|                        |                                                                             | 2. It restricts the presence uninformative feature attributes.               |
|                        |                                                                             | 3. Minimal time requirement for processing. |
|                        |                                                                             | 4. It failed to analyze the inconsistent data during the prediction.         |
|                        |                                                                             | 5. Reduced efficiency.                   |
| Lai, et al [18]        | Deep neural network based classification model is utilized to predict the anomalies in ICS. | 1. Efficient feature representation.      |
|                        |                                                                             | 2. Reduced time consumption.              |
|                        |                                                                             | 3. Imbalanced data processing.            |
|                        |                                                                             | 4. Reduced efficiency of attacking classification.                            |
|                        |                                                                             | 5. High computational complexity.         |

### FIGURE 2. Overall flow of the proposed attack prediction system.

At first, the given input dataset is preprocessed for eliminating the irrelevant information and to perform the attribute labeling process. Then, the cluster points are initialized from the preprocessed dataset for organizing the feature sets. During the dataset training, the RPCO technique is implemented to perform the relevancy mapping between the query data and entire dataset. Based on the relevancy level, the best optimal features are selected and are given to the input of BCNN classification technique. Then, it predicts the output label as whether normal or abnormal by estimating the matching score of the correlated blocks. The major benefits of the proposed RPCO-BCNN techniques are reduced time complexity, accurate detection, ability of handling large datasets, and improved classification performance.

### A. PREPROCESSING

Typically, the value of the raw dataset should be improved because that has the strong influence on determining the overall performance of the SCADA systems. At first, the original SCADA network input dataset is preprocessed for manipulating the data based on the concepts of normalization, balancing, segmentation, and removal of irrelevant information. For this purpose, the Markov Chain Clustering (MCC) model is implemented in this work, which performs both the data preprocessing and clustering for improving the quality of data. After loading the dataset, the attribute labeling, initialization of cluster index, and segmentation can be performed for arranging the feature values. In this algorithm, the original network data HDSs taken as the input and the clustered network data is obtained as the output. At first, the feature values of the given data can be normalized with respect to the minimum
and maximum values as shown in below:

\[
H_N = \left[ \frac{(H_D - H_{D_{\text{min}}})}{(H_{D_{\text{max}}} - H_{D_{\text{min}}})} \right] \quad H_N = \left[ \frac{(H_D - H_{D_{\text{min}}})}{(H_{D_{\text{max}}} - H_{D_{\text{min}}})} \right] \tag{1}
\]

where, \(H_N\) is the normalized dataset, \(H_{D_{\text{min}}}\) indicates the minimum value and \(H_{D_{\text{max}}}\) represents the maximum value. Then, the features in the normalized data can be arranged based on the number of number of rows and columns in the dataset, which is represented as follows:

\[
H_N = \begin{bmatrix}
f_{11} & f_{12} & \cdots & f_{1m} \\
f_{21} & f_{22} & \cdots & f_{2m} \\
\vdots & \vdots & \ddots & \vdots \\
 f_{n1} & f_{n2} & \cdots & f_{nm}
\end{bmatrix} \tag{2}
\]

where, \(m\) and \(n\) represents the row and column size of feature set respectively. Consequently, the distance \(D_i\) between the particles \(F_i\) computed as shown in below:

\[
D_i = K [F_i] [H_N (f_i) - H_N (f_j)] \quad \forall i, 1, 2, \ldots m & j, 1, 2, \ldots n \tag{3}
\]

Consequently, the weight value \(\omega\) of the MARKOV model is estimated for the normalized data based on the distance computation.

\[
\omega = - \sum_{j=1}^{M} H_N (i) \cdot \log (D_j) \tag{4}
\]

If the present weight value is greater than the previous one, the grouping can be performed. The algorithmic steps involved in the MCC clustering technique are illustrated as follows:

**B. RPCO OPTIMIZATION**

Typically, the data points of the feature vectors are not in a complete form, which leads to a misclassified results at the time of classification. So, it must be solved by implementing an optimization technique for selecting the most suitable features. Thus, the RPCO mechanism is designed in this work, which helps to improve the classification accuracy by selecting the best feature attributes from the input set of input feature vectors. The main motive of using this technique is to extract the optimal set of features from the preprocessed data based on the best parameter selection process. The different types of parameters considered in this work are

1. Entropy
2. Output weight of sensors
3. Energy properties
4. Trust ratings
5. Lebesgue measure
6. Probability density of sequence
7. Overall power
8. Average sigma
9. Amount of packets transmission
10. Likelihood ratio

In this mechanism, different parameters have been optimally selected and its fitness functions are computed for improving the convergence speed of each and every iteration. These attributes are used to simplify the process of classifier and training and testing with reduced computational complexity. Also, it helps to obtain an improved accuracy by integrating the objective functions with the selected feature attributes.

After pre-processing, the optimal set of features are selected from the training dataset by using the RPCO mechanism. The intention of implementing this optimization technique is to reduce the number of input features based on the fitness function. In which, the learning features have been computed with respect to the weight and distance values. The major benefit of using this technique is, it evaluates the separate data features that are related to each class. The clustered network data \(TD\) is given as the input for this technique, and it provides the optimal selection of attributes \(TD\) \((s)\) the output. Here, the \(m\) number of particles \(x\) are initialized with the weight value of \(\omega_i\) which is computed as follows:

\[
\omega_i (n) = \left( \frac{P_i^m (x (n))}{\sum_{l=1}^{N} P_l^m (x (n))} \right) \quad \forall n = 1, 2, \ldots, m \tag{5}
\]

where, \(\omega_i (n)\) represents the weight value of particles for \(i^{th}\) iteration, and \(P_i^m\) indicates the potential of particle as represented as below:

\[
P_i^m = e^{- \sum_{y \in TD} f_i (y)} \tag{6}
\]

After finding the potential, the likelihood of the particles \(L_i^m\), re estimated by using the following equation:

\[
L_{i-1}^m = L_{i-1}^m \times L_i^m \quad \forall n = 1, 2, \ldots, m \tag{7}
\]

\[
L_i^m = \frac{1}{N} \sum_{l=1}^{N} P_i^m (x (n)) \tag{8}
\]

Algorithm I – MCC Clustering

**Input:** Network Data \(H_D\)

**Output:** Clustered Network Data \(TD\)

**Step 1:** Normalize the feature value of input network data by using equation (1).

**Step 2:** The features in the normalized data can be arranged by using equation (2).

**Step 3:** Estimate the distance between particles as shown in equation (3).

**Step 4:** Calculate weight value of Markov model using equation (4).

For \(i = 1\) to \(N\)

If \(\omega (i) < \omega (i + 1)\) then

\[
N_i = \begin{cases} 
  k, & \text{if } (1 + e^{\omega (i)}) < 0 \\
  0, & \text{otherwise}
\end{cases}
\]

\(k = k + 1\)

End if

End loop
Consequently, the weight value of each particle is updated based on the following:

$$\omega_i (n + 1) = \sum_{l=1}^{N} \omega_i (n) \delta (x_n)$$

(9)

Then, the particle updating is performed as follows:

$$x (n + 1) = \frac{1}{N} \sum_{l=1}^{N} \delta (x_n)$$

(10)

After that, the maximum likelihood \(m^*_n\) and fitness values \(\omega^*_n\) re-computed for the updated particles with respect to the weight value, which are represented as follows:

$$m^*_n = \max (L_{1:d}^m)$$

(11)

$$\omega^*_n (n) = \max \{ P_i^n (x (n)) \omega_i (n) \}$$

(12)

Based the maximum likelihood, the coordinates particles are updated with the best fitness value.

Fig 3 shows the convergence plot of RPCO based feature selection process, where the fitness is evaluated with respect to different iterations.

**C. BCNN CLASSIFIER**

During the attack classification process, the optimally selected features are given to both the training and testing dataset. For this purpose, the BCNN technique is designed in this work, which works based on the concept of NN algorithm. Also, this technique contains three operating layers such as input layer, hidden layer, and output layer. In which, the input layer accepts the selected features as the input data, and the classification processes are carried out in the hidden layer. Finally, the predicted class of label is produced as the result in the output layer. Based on the parameters of RPCO mechanism, the feature attributes are obtained and integrated as an objective function of optimization, which is used to improve the overall efficiency of classification. The novelty of this technique is, it separates the blocks of information for processing the given datasets, which is highly related to the parallel processing structure. So, it has the ability to process the large dimensional datasets in the form of correlated blocks by estimating the maximum correlation efficiency. Due to this process, the accuracy of classification has been increased with reduced number of features. Then, the BCNN technique utilize these optimally selected feature attributes for classifying the intrusions from the given datasets with high accuracy and efficiency. Also, it provided the benefits of high reliability, reduced computational complexity, and improved detection performance. After selecting the most suited features, the training set \(T_D (s)\) can be given as the input for classification, and the classified result \(V (k)\) is obtained as the output. In this stage, the feature properties can be initialized based on the sequential order as shown in below:

$$T_D (s) = \{ T_{D1} (s), T_{D2} (s), \ldots, T_{Dm} (s) \}$$

(13)

Then, the input data sequences are arranged in the matrix format at the input layer of the network for separating the blocks, which is represented as follows:

$$X_D (s) = \begin{bmatrix} T_{D1} (s) \\ T_{D2} (s) \\ \ldots \\ T_{Dm} (s) \end{bmatrix}$$

(14)

Sequentially, the correlation features of each block are computed in order to arrange the matrix as represented...
as follows:
\[ F(X_D(s), X_D^*(s)) = X_D^*e^{T - T_m} \quad (15) \]

where, ‘T’ and ‘T_m’ represents the attribute values of matrix \( X_D(s) \). Then, the kernel model of classifier is constructed with respect to the range of feature distance \( r \) and length of feature vector \( l \) which is illustrated as follows on the following model:
\[ K_m = \frac{1}{2^{q-1}} \left( \frac{\sqrt{2q}}{l} \right)^q k_q \left( \frac{\sqrt{2q}r}{l} \right) \quad \forall q = 1, 2, \ldots, N \quad (16) \]

Then, the relevancy level is estimated based on the kernel function with its corresponding feature points as shown in below:
\[ t_n = F^T \omega_n \quad (17) \]
\[ u_m = F^T \omega_m \quad (18) \]

where, \( \omega_n \) indicates the weight value of attributes and \( F^T \) is the feature points. Then, the network is constructed by extracting the training features, which is illustrated as follows:
\[ T_r = \{t_1, t_2, \ldots, t_n\} \quad (19) \]
\[ X_b = \bar{X}_b + \sum_{i=1}^{N} t_i (d)p^i \quad (20) \]

Based on the relevancy level, the matching score is computed for the correlated blocks by using the following model:
\[ \hat{S} = \left( (X_b^d - \bar{X}_b^d)^T (p^f) \right)^T \quad (21) \]

where, the relevance factor \( X_b^d \in R^{(T - T_p)M} \) is indicated by,
\[ R^{(T - T_p)M} = T_s^T Q^T + \pi_d \quad (22) \]

where, \( P \) and \( Q^T \) are the predicted components. Finally, the output predicted label can be represented with the help of distance matrix \( d_{ij} \) and relevance matrix \( R \) values.
\[ V(k) = \frac{d_{ij}}{R_j - R_i} \quad (23) \]

Fig 4 shows the prediction chart of BCNN based attack classification system, where the colored plots indicate the class of attack in the SCADA network data.

The major advantages of the proposed RPCO-BCNN based IDS are listed as follows:

1. It provides an increased attack detection efficiency and accuracy by extracting the most suited feature attributes based on the optimal selection of parameters.
2. It increases the convergence speed of optimization by evaluating the fitness function for the specified attributes.
3. It has the ability to handle large dimensional datasets by splitting it into different types of blocks. Then, it parallelly processing these blocks based on the maximum correlation estimation.

Algorithm III– BCNN Classification

**Input:** Training set \( T_D(s) \)

**Output:** Classified Result \( V(k) \)

**Step 1:** The input series are arranged in the sequential as shown in equation (13)

**Step 2:** In the input layer of neural network, the data sequence can be formed as the matrix based on equation (14)

**Step 3:** Form the matrix arrangement, the block correlation feature can be estimated by \( F(X_D(s), X_D^*(s)) \) which is represented in equation (15).

**Step 4:** Estimate the kernel model of classifier by using equation (16).

**Step 5:** Estimate the relevancy using kernel function with feature points based on equations (17) and (18).

**Step 6:** Extract the training features and form the network by using equations (19) and (20).

**Step 7:** Estimate the matching score for the correlated blocks by using equations (21) and (22).

**Step 8:** The predicted label can be provided as the output shown in equation (23).

**IV. RESULTS AND DISCUSSION**

This section evaluates the performance and analysis of both existing and proposed attack detection mechanisms by using various performance measures. It includes ROC analysis, False Negative Rate (FNR), Error Rate (ER), precision, recall, and F1-measure. Table 2 describes the different types of datasets used in this work for evaluating the performance of proposed system.

Here, the real time dataset, named as, Cyber-Physical Model is taken for evaluating the performance of the proposed mechanism. This dataset details are presented in

**FIGURE 4. Classification prediction chart.**

4. It obtains high accuracy in attack detection by utilizing the optimal features for classification.
5. It consumes reduced amount of time due to the parallel processing of blocks.
TABLE 2. Different types of datasets used in this analysis.

| Datasets                          | Description                                                                                                                                      | Pros and Cons |
|-----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|---------------|
| Cyber-Physical Model [32]         | It is a real time dataset contains the different types of attacks like moving files, uploading executable files, Modbus conversion, and creating Modbus traffic. |               |
| ICS network traffic dataset [33]  | It is a kind of publicly available dataset and extensively used for assessing the performance of various security mechanisms.                     |               |
| Real vehicle dataset [34]         | It is publicly available that contains the information related to network traffic and other fabricated messages.                                 |               |
| CSE-CIC-IDS 2018 [29]             | It contains the attacking information related to DoS, DDoS, Bruteforce, and web attack.                                                           |               |
| Bot-IoT dataset [29]              | It is a type of IoT traffic based dataset, which contains more than 72,000 records related to the different types of attacks.                 |               |

TABLE 3. Attacking information of cyber physical model for scada systems.

| Name and Notation          | Depiction                                                                                     | Number of Samples | Number of Attacking Samples |
|-----------------------------|------------------------------------------------------------------------------------------------|-------------------|-----------------------------|
| 6RTU_with_operate (Attack 1) | It uses some Metasploit information from one compromised RTU to another RTU.                  | 1856              | 1200                        |
| CnC_uploading_exe (Attack 2) | It shares the executable files from RTU to another.                                             | 1426              | 121                         |
| Moving_two_files (Attack 3) | Sharing of two files from one RTU to other.                                                     | 3319              | 75                          |
| Characterization (Attack 4) | It categorize the available registers by transmitting the series of Modbus commands.           | 12296             | 6719                        |
| Send_a_fake_command (Attack 5)| It uses both the proxychains tool and Metasploit proxy functions for Modbus writing operation.| 11166             | 10                          |
| Channel_4d_12s (Attack 6)   | It makes use of Modbus covert channel.                                                          | 44977             | 44977                       |
| Modbus_polling_only (Attack 7)| Creates the Modbus traffic with polling.                                                        | 58325             | 0                           |

Table 3 with the information of different attacks, description, number of samples, and number of attacking samples. It contains the information related to the series of real world attacks on SCADA system like cyber-attack against the Ukrainian power grid. In addition to that, some other existing datasets such as ICS network traffic dataset [33], real vehicle dataset [34], CSE-CIC-IDS 2018, and Bot-IoT [29] are also used to test and compare the performance of the proposed technique.

For the Cyber Physical model dataset, the confusion matrix has been defined for both existing and proposed techniques with respect to the different types of attacks as shown in Table 4 and Table 5. From the analysis, it is clear that the proposed RPCO-BCNN technique provides the reduced FPs and FNs by accurately predicting the attacks from the real time dataset. The values are comparatively improved than the existing method, because the optimal parameter selection based feature attributes extraction helps to improve the accuracy of classification approach.

Then, the real vehicle dataset contains the logging information of network traffic and injected fabricated messages. Table 6 presents the total number of normal and injected messages with respect to different types of attacks such as DoS attack, fuzzy attack, gear spoofing and RPM. Typically, the DoS attack intends to damage the availability of normal
TABLE 4. Confusion matrix of existing mechanism (risk assessment model).

| Attack   | TP   | TN   | FP  | FN  |
|----------|------|------|-----|-----|
| Attack 1 | 1200 | 656  | 0   | 0   |
| Attack 2 | 120  | 1305 | 0   | 1   |
| Attack 3 | 73   | 3244 | 0   | 2   |
| Attack 4 | 6719 | 5385 | 192 | 0   |
| Attack 5 | 10   | 11122| 34  | 0   |
| Attack 6 | 44977| 0    | 0   | 0   |
| Normal Data | 0    | 58142| 183 | 0   |

TABLE 5. Confusion matrix of proposed mechanism (RPCO-BCNN).

| Attack   | TP   | TN   | FP  | FN  |
|----------|------|------|-----|-----|
| Attack 1 | 1200 | 656  | 0   | 0   |
| Attack 2 | 120  | 1306 | 0   | 0   |
| Attack 3 | 73   | 3245 | 0   | 1   |
| Attack 4 | 6771 | 5385 | 140 | 0   |
| Attack 5 | 17   | 11122| 27  | 0   |
| Attack 6 | 44977| 0    | 0   | 0   |
| Normal Data | 67   | 58142| 116 | 0   |

TABLE 6. Attacking information of real vehicle dataset.

| Attack type         | Normal messages | Injected messages |
|---------------------|-----------------|-------------------|
| DoS Attack          | 30,78,250       | 5,87,521          |
| Fuzzy Attack        | 33,47,013       | 4,91,847          |
| Gear Spoofing       | 27,66,522       | 5,97,252          |
| RPM Spoofing        | 22,90,185       | 6,54,897          |

A. CONFUSION MATRIX

Table 7 and 8 depict the confusion matrix of both existing DCNN and proposed RPCO-BCNN techniques with respect to five different types of attacks represented in Dataset 2. Here, the confusion matrix is formed to analyze the accuracy of classifier based on the differential ratio of the sum of values mentioned in the diagonal matrix with respect to the values in other side. Moreover, the overall efficiency and accuracy of the attack detection system can be determined based on the confusion matrix. Here, the matrix is constructed for both existing and proposed techniques based on the detection of number of attacks in the entire dataset 2. From the evaluation, it is evident that the RPCO-BCNN technique exactly detects the types of attacks from the dataset, when compared to the conventional DCNN technique.

B. ROC ANALYSIS

Fig 5 to Fig 8 shows the ROC analysis of the existing DNN and proposed RPCO-BCNN techniques with respect to varying TPR and FPR values. Here, the ROC is evaluated for each attack mentioned in the vehicle dataset. Generally, the ROC can be estimated to validate the performance of classification technique with respect to varying threshold values. From the results, it is analyzed that the RPCO-BCNN technique outperforms the DNN technique by providing an improved results for all types of attacks.

C. OVERALL PERFORMANCE EVALUATION

Table 4 and Fig 9 compares the existing and proposed attack detection methodologies based on the measures of sensitivity, specificity, precision, F1-measure, and Matthews Correlation Coefficient (MCC). Typically, the sensitivity is defined based on the ratio of the number of TP rate and the value of TP with FN. Similarly, the specificity is defined by the ratio of network operations. Then, the fuzzy attack is more similar to the DoS attack, but it performs malfunctioning on the vehicles. Similarly, the gear and RPM spoofing attacks contain the messages related to the drive gear and RPM gauge, which affects the instrument panel.

FIGURE 5. ROC analysis for DoS attack.

VOLUME 9, 2021 156305
Moreover, the measures of precision, recall, MCC and F1 score are used to determine how the classifier could actually predict the accurate values during the attack detection process. The sensitivity is also termed as recall, and the other measures are calculated as follows (26)–(31), as shown at the bottom of the next page, where, TP indicates the True Positive, TN represents the True Negative, FP defines the False Positive, and FN represents the False Negative. Table 9 compares the accuracy, detection rate and f1-score of both existing and proposed intrusion detection approaches used in the SCADA security systems, which includes the existing techniques of decision tree, boosted decision, decision jungle, and risk assessment model. From the evaluation, it is observed that the RPCO-BCNN technique outperforms the other techniques by accurately detecting the intrusions from the given dataset based on the optimal number of feature selection and classification process. This shows the overall effectiveness of the proposed technique, when compared to the other existing techniques.

Moreover, the relevancy level of actual and predicted class labels can be estimated based on the classified outcomes, which ensures an improved performance of the proposed technique with reduced training level. From Table 10, it is evident that the RPCO-BCNN technique provides an increased sensitivity, specificity, precision, f1-score, kappa coefficient and MCC values, when compared to the DNN technique. Because, the clustering based optimization technique helps
TABLE 10. Comparative analysis between existing DNN and proposed RPCO-BCNN.

| Parameters      | DNN          | RPCO-BCNN   |
|-----------------|--------------|-------------|
| Sensitivity     | 0.998971     | 1           |
| Specificity     | 0.990566     | 0.997462    |
| Precision       | 0.980104     | 0.989922    |
| F1_Score        | 0.972632     | 0.999363    |
| MCC             | 0.986955     | 0.993405    |
| Kappa coefficient| 0.971        | 0.985       |

The classifier to accurately predict the attacks as normal or malicious.

Moreover, the overall effectiveness of the attack detection mechanism is highly dependent on the measure of accuracy. It is calculated based on the percentage of accurately detected flows with respect to the total number of predictions as shown in below:

\[
\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN} \quad (32)
\]

Fig 10 and 11 shows the accuracy value and AUC of existing DNN, binary classification, and proposed RPCO-BCNN techniques. This result indicated that the proposed technique provides an increased accuracy value, when compared to the other techniques by estimating the matching score based on the number of trained features.

Moreover, the error rate Fig 12 represents the error rate and FPR of existing DNN and proposed RPCO-BCNN techniques, which are calculated as follows:

\[
\text{FPR} = \frac{FP}{FP + TN} \quad (33)
\]
\[
\text{Error rate} = 1 - \text{Overall accuracy} \quad (34)
\]

In which, the increasing value of TPR ensures an improved accuracy, and the FPR is inversely proportional to TPR. The lowest FPR confirms the reduced error rate of classifier with misclassified results. Then, these results indicated that the proposed RPCO-BCNN outperforms the DNN technique with reduced error rate and FPR values.

D. DETECTION EFFICIENCY

The measure of detection rate is used to estimate the attack identification efficiency of the classification technique. In Fig 13 and Table 11, the detection efficiency of both existing [11] and proposed classification techniques are evaluated.
based on the different types of attacks. It includes Naïve Malicious Response Injection (NMRI), Complex Malicious Response Injection (CMRI), Malicious Parameter Command Injection (MPCI), Malicious State Common Injection (MSCI), Malicious Function Code Injection (MFCI), Denial of Service (DoS), and Reconnaissance (Reconn), which are the different types of attacks degrade the performance of SCADA systems. So, it must be detected based on the proper feature extraction and optimization models. Then, these results stated that the proposed RPCO-BCNN technique outperforms the other techniques with increased detection efficiency.

Table 12 and Fig 14 shows the kappa-coefficient of both existing and proposed classification techniques, which is one of the extensively used measure for testing the exactness of classifier and is estimated as follows:

\[
kappa \text{ coefficient} = \frac{P_o - P_e}{1 - P_e}
\]  

Based on this analysis, it is evident that the RPCO-BCNN technique outperforms the other techniques with increased kappa coefficient.

Table 13 and Fig 15 compares the conventional and proposed classification techniques based on the measures of accuracy, precision, recall, f-measure. Typically, it is defined that the detection performance and overall effectiveness of
any classification technique is highly depends on the measures of accuracy, precision, recall and f-measure. From the results, it is evident that the RPCO-BCNN technique offers an increased performance rate (around 99%), when compared to the other techniques. Because, the RPCO technique optimally selects the attributes based on the estimation of maximum likelihood and fitness function, which helps to improve the overall performance of the classification system.

Table 14 and 15 evaluates the False Acceptance Rate (FAR) and detection rate of both existing and propose RPCO-BCNN techniques for both CSE-CIC-IDS 2018 and Bot-IoT dataset respectively. The existing techniques considered for this evaluation are CNN, DNN, RNN, RF, NB, SVM and ANN, and the results stated that the proposed RPCO-BCNN provides the reduced FAR and increased detection ratio for both datasets. When compared to the other approaches, the proposed RPCO-BCNN technique provides an improved performance results.

E. COMPARATIVE ANALYSIS WITH OTHER CLASSIFICATION APPROACHES

Fig 16 and Table 16 compares the existing and proposed classification techniques based on the different measures of precision, recall, F1-score, error rate and FNR. Also, various classification techniques compared in this analysis are reduced inception-ResNet, LSTM (256 hidden units), ANN (2 hidden layers), Support Vector Machine (SVM), k-Nearest Neighbour (kNN) $k = 5$, Naïve Bayes (NB), and Decision Tree (DT). Based on these results, it is clear that the proposed RPCO-BCNN technique provides an increased precision, recall, F1-score and, reduced FNR and error rate, which
shows the overall efficacy of the proposed attack classification system. Table 17 evaluates the average classification accuracy of the existing [10] and proposed classification techniques with respect to the average and standard deviation measures. From the results, it is concluded that the RPCO-BCNN technique performs better than the other methods with increased training and testing values.

V. CONCLUSION

This paper proposed an advanced RPCO-BCNN mechanisms for accurately detecting and classifying the attacks in the SCADA systems. The main intention of this work is to provide an optimal solution for detecting the abnormal activities in the network architecture. Then, this objective is attained by applying the data clustering and feature selection models. Here, the MCC clustering technique is utilized to preprocess the input dataset by eliminating the noise contents and cluster the attribute labels. Then, the RPCO based feature selection mechanism is implemented to compute the best fitness function based on the weight value of each particle. Consequently, the BCNN technique is deployed to classify the predicted label as attack or non-attack based on the set of selected features. The main advantage of this work is, it selected the best suited features with reduced computational time. Also, the performance of this model is validated by using two different datasets such as ICS network traffic data, and real time vehicle dataset. The various evaluation metrics used in this analysis are sensitivity, specificity, accuracy, precision, f1-score, error rate, kappa-coefficient, and FPR. In addition to that, the obtained values of the proposed RPCO-BCNN is compared with some other conventional classification techniques. From the results, it is proved that the RPCO-BCNN technique outperforms the other technique with improved detection efficiency and overall performance. In future, this work can be extended by implementing a deep learning model for increasing the security of SCADA systems.

In future, this work has been extended by implementing a new prototype model for analyzing the different types of SCADA networking datasets. Also, an advanced risk assessment strategy can be employed for differentiating the different types of attacks by optimally tuning the parameters.

REFERENCES

[1] J. Suaboot, A. Fahad, Z. Tari, J. Grundy, A. N. Mahmood, A. Almalawi, A. Y. Zomaya, and K. Dirra, “A taxonomy of supervised learning for IDSs in SCADA environments,” ACM Comput. Surv., vol. 53, no. 2, pp. 1–37, Jul. 2020.

[2] A. A. Z. Khan and G. Serpen, “Intrusion detection and identification system design and performance evaluation for industrial SCADA networks,” 2020, arXiv:2012.09707.

[3] K. Chakraborti, “Intrusion detection of SCADA system using machine learning techniques: A study,” in IoT Security Paradigms and Applications. Boca Raton, FL, USA: CRC Press, 2020, pp. 135–164.

[4] A. Gumaei, M. M. Hassan, S. Huda, M. R. Hassan, D. Camacho, J. D. Ser, and G. Fortino, “A robust cyberattack detection approach using optimal features of SCADA power systems in smart grids,” Appl. Soft Comput., vol. 96, Nov. 2020, Art no. 106638.

[5] H. C. Altunay, Z. Albsyark, A. N. Ozalp, and M. Cakmak, “Analysis of anomaly detection approaches performed through deep learning methods in SCADA systems,” in Proc. 3rd Int. Congr. Hum.-Comput. Interact., Optim. Robotic Appl. (HORA), Jun. 2021, pp. 1–6.

[6] M. Al-Asiri and E.-S.-M. El-Alfy, “On using physical based intrusion detection in SCADA systems,” Proc. Comput. Sci., vol. 170, pp. 34–42, Jan. 2020.

[7] G. Yadav and K. Paul, “Architecture and security of SCADA systems: A review,” Int. J. Crit. Infrastruct. Protection, vol. 34, Sep. 2021, Art no. 100433.

[8] F. Zhang, J. Coble, and J. Hines, “Data-driven model application for attack detection of SCADA system,” in Proc. 11th Nucl. Plant Instrum., Control Hum.-Mach. Interface Technol. (NPIC&HMIT), Orlando, FL, USA, Feb. 2019, pp. 1370–1379.

[9] D. Platios, P. Sarigiannidis, T. Lagkas, and A. G. Sarigiannidis, “A survey on SCADA systems: Secure protocols, incidents, threats and tactics,” IEEE Commun. Surveys Tuts., vol. 22, no. 3, pp. 1942–1976, 3rd Quart., 2020.

[10] J. Qian, X. Du, B. Chen, B. Qu, K. Zeng, and J. Liu, “Cyber-physical integrated intrusion detection scheme in SCADA system of process manufacturing industry,” IEEE Access, vol. 8, pp. 147471–147481, 2020.

[11] I. A. Khan, D. P., Z. U. Khan, Y. Hussain, and A. Nawaz, “HML-IDS: A hybrid-multilevel anomaly prediction approach for intrusion detection in SCADA systems,” IEEE Access, vol. 7, pp. 89507–89521, 2019.

[12] V. A. Kamaev, A. G. Finogeve, A. A. Finogeve, and D. S. Parygin, “Attacks and intrusion detection in wireless sensor networks of industrial SCADA systems,” J. Phys., Conf. Ser., vol. 803, Jun. 2017, Art no. 012063.

[13] A. Almalawi, A. Fahad, Z. Tari, A. Alamri, R. Aighamdi, and A. Y. Zomaya, “An efficient data-driven clustering technique to detect attacks in SCADA systems,” IEEE Trans. Inf. Forensics Security, vol. 11, no. 5, pp. 893–906, May 2016.

[14] P. Zeng and P. Zhou, “Intrusion detection in SCADA system: A survey,” in Intelligent Computing and Internet of Things. Singapore: Springer, 2018, pp. 342–351.

[15] A. F. S. Prisco and M. J. Freddy Duitama, “Intrusion detection system for SCADA platforms through machine learning algorithms,” in Proc. IEEE Colombian Conf. Comput. Commun. (COLCOM), Aug. 2017, pp. 1–6.

[16] R. B. Benisha and S. R. Rata, “Design of intrusion detection and prevention in SCADA system for the detection of bias injection attacks,” Secur. Commun. Netw., vol. 2019, pp. 1–12, Nov. 2019.

[17] R. L. Perez, F. Adamsky, R. Soua, and T. Engel, “Forget the myth of the air gap: Machine learning for reliable intrusion clustering in SCADA systems,” ICST Trans. Secur. Syst., vol. 6, no. 19, Jan. 2019, Art no. 159348.

[18] Y. Lai, J. Zhang, and Z. Liu, “Industrial anomaly detection and attack classification method based on convolutional neural network,” Secur. Commun. Netw., vol. 2019, pp. 1–11, Sep. 2019.

[19] M. Keshk, N. Moustafa, E. Sitnikova, and G. Creech, “Privacy preservation intrusion detection technique for SCADA systems,” in Proc. Mil. Commun. Int. Symp. Conf. (MILCOM), Nov. 2017, pp. 1–6.

[20] S. Huda, J. Yearwood, M. M. Hassan, and A. Almogren, “Securing the operations in SCADA-IoT platform based industrial control system using ensemble of deep belief networks,” Appl. Soft Comput., vol. 71, pp. 66–77, Oct. 2018.

[21] H. Yang, L. Cheng, and M. C. Chuaah, “Deep-learning-based network intrusion detection for SCADA systems,” in Proc. IEEE Conf. Comput. Commun. ISC. Security (CNS), Jun. 2019, pp. 1–7.

| TABLE 17. Training and testing accuracy of existing and proposed classification techniques. |
|---|---|---|
| Methods | Training (AVG % ± STD) | Testing (AVG % ± STD) |
| RPCO-BCNN | 98.2 ± 0.53 | 97.8 ± 0.65 |
| NHFC | 97.9 ± 0.52 | 97.2 ± 0.64 |
| SVM | 87.4 ± 0.46 | 85.3 ± 0.49 |
| OCSCVM | 90.3 ± 0.51 | 87.6 ± 0.58 |
| FCMSVM | 91.1 ± 0.47 | 88.7 ± 0.53 |
| GENFLS | 81.3 ± 0.59 | 78.2 ± 0.64 |
S. SHITHARTH (Member, IEEE) received the B.Tech. degree in information technology from the KGIStL Institute of Technology, Coimbatore, India, in affiliation with Anna University, Chennai, India, in 2012; the M.E. degree in computer science and engineering from the Thigagarajar College of Engineering, Madurai, India, in affiliation with Anna University, in 2014; and the Ph.D. degree from the Department of Computer Science and Engineering, Anna University. He is currently working as an Associate Professor with the Department of Computer Science and Engineering, Kebri Dehar University, Somali, Ethiopia. Previously, he was associated with the Vardhaman College of Engineering, Hyderabad. He has published more than ten international journals along with 12 international and national conferences. He has even published three patents in IPR. His current research interests include cyber security, critical infrastructure systems, and network security and ethical hacking. He is also an Active Member of the IEEE Computer Society and in five more professional bodies. He is an active researcher, a reviewer, and an editor for many international journals.

KANTIPUDI MV PRASAD (Senior Member, IEEE) received the B.Tech. degree in electronics and communications and the M.Tech. degree in digital electronics and communication systems from Jawaharlal Nehru Technological University, Kakinada, in 2009 and 2011, respectively, and the Ph.D. degree in signal processing specialization from BITS, VTU, Belgaum, in 2018. He is currently working as an Associate Professor with the Department of Electronics and Telecommunication, Symbiosis Institute of Technology, Pune. Previously, he worked as the Director of advancements for the Sreyas Institute of Engineering & Technology, Hyderabad, and an Associate Professor with RK University, Rajkot, having teaching experience around 10.8 years. He has authored and coauthored many papers in international journals, national conferences, and national conferences, and published five Indian patents. His current research interests include signal processing with machine learning, education, and research. He is recognized as a Technical Resource Person for Telangana state by IIT Bombay Spoken Tutorial Team and he conducted Key Training Workshops on Open-Source Tools for Education, Signal Processing, and Machine Learning focused topics, and Educational Technology.
THANIKANTI SUDHAKAR BABU (Senior Member, IEEE) received the B.Tech. degree from Jawaharlal Nehru Technological University, Anantapur, India, in 2009, the M.Tech. degree in power electronics and industrial drives from Anna University, Chennai, India, in 2011, and the Ph.D. degree from VIT University, Vellore, India, in 2017. He is currently working as an Associate Professor with the Department of Electrical Engineering, Chaitanya Bharathi Institute of Technology (CBIT), Hyderabad, India. He had completed his Postdoctoral Researcher Fellowship from the Institute of Power Engineering, Universiti Tenaga Nasional (UNITEN), Malaysia. Before that, he was worked as an Assistant Professor at the School of Electrical Engineering, VIT University. He has published more than 80 research articles in various renowned international journals. His research interests include the design and implementation of solar PV systems, renewable energy resources, power management for hybrid energy systems, storage systems, fuel cell technologies, electric vehicles, and smart grids. He has been acting as an Associate Editor of IET RPG, IEEE ACCESS, ITEES (Wiley), Frontiers in Energy Research, a Section Editor of Energies and Sustainability (MDPI Publications), and a reviewer for various reputed journals.

HASSAN HAES ALHELOU (Senior Member, IEEE) was with the School of Electrical and Electronic Engineering, University College Dublin, Ireland. He is currently with Tishreen University, Syria. He has participated in more than 15 industrial projects. He has published more than 160 research articles in high-quality peer-reviewed journals and international conferences. He is included in the 2018 Publons list of the top 1% best reviewer and researchers in the field of engineering in the world. His research interests include power system operation, power system dynamics and control, smart grids, microgrids, demand response, and load shedding. He was a recipient of the Outstanding Reviewer Award from many journals, such as Energy Conversion and Management (ECM), ISA Transactions, and Applied Energy. He was also a recipient of the Best Young Researcher in the Arab Student Forum Creative among 61 researchers from 16 countries at Alexandria University, Egypt, in 2011. He has performed more than 800 reviews for high prestigious journals, including IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, IEEE TRANSACTIONS ON POWER SYSTEMS, and International Journal of Electrical Power and Energy Systems.