

Article

# A Proficient ZESO-DRKFC Model for Smart Grid SCADA Security

Osama Bassam J. Rabie <sup>1</sup>, Praveen Kumar Balachandran <sup>2,\*</sup>, Mohammed Khojah <sup>3</sup> and Shitharth Selvarajan <sup>4</sup>

<sup>1</sup> Department of Information Systems, Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah 21589, Saudi Arabia

<sup>2</sup> Department of Electrical and Electronics Engineering, Vardhaman College of Engineering, Hyderabad 501218, India

<sup>3</sup> Department of Management Information Systems, Faculty of Economics & Administration, King Abdulaziz University, Jeddah 21589, Saudi Arabia

<sup>4</sup> Department of Computer Science, Kebri Dehar University, Kebri Dehar P.O. Box 250, Ethiopia

\* Correspondence: praveenbala038@gmail.com

**Abstract:** Smart grids are complex cyber-physical systems that incorporate smart devices' communication capabilities into the grid to enable remote management and the control of power systems. However, this integration reveals numerous SCADA system flaws, which could compromise security goals and pose severe cyber threats to the smart grid. In conventional works, various attack detection methodologies are developed to strengthen the security of smart grid SCADA systems. However, they have several issues with complexity, slow training speed, time consumption, and inaccurate prediction outcomes. The purpose of this work is to develop a novel security framework for protecting smart grid SCADA systems against harmful network vulnerabilities or intrusions. Therefore, the proposed work is motivated to develop an intelligent meta-heuristic-based Artificial Intelligence (AI) mechanism for securing IoT-SCADA systems. The proposed framework includes the stages of dataset normalization, Zaire Ebola Search Optimization (ZESO), and Deep Random Kernel Forest Classification (DRKFC). First, the original benchmarking datasets are normalized based on content characterization and category transformation during preprocessing. After that, the ZESO algorithm is deployed to select the most relevant features for increasing the training speed and accuracy of attack detection. Moreover, the DRKFC technique accurately categorizes the normal and attacking data flows based on the optimized feature set. During the evaluation, the performance of the proposed ZESO-DRKFC method is validated and compared in terms of accuracy, detection rate, f1-score, and false acceptance rate. According to the results, it is observed that the ZESO-DRKFC mechanism outperforms other techniques with high accuracy (99%) by precisely spotting intrusions in the smart grid systems.

**Keywords:** smart grid; supervisory control and data acquisition (SCADA); internet of things (IoT); cyber-security; artificial intelligence; data normalization; Zaire Ebola search optimization (ZESO); deep random kernel forest classification (DRKFC)



**Citation:** Rabie, O.B.J.; Balachandran, P.K.; Khojah, M.; Selvarajan, S. A Proficient ZESO-DRKFC Model for Smart Grid SCADA Security.

*Electronics* **2022**, *11*, 4144. <https://doi.org/10.3390/electronics11244144>

Academic Editors: Taha Selim Ustun and Juan M. Corchado

Received: 7 November 2022

Accepted: 9 December 2022

Published: 12 December 2022

Corrected: 20 December 2023

**Publisher's Note:** MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



**Copyright:** © 2022 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

## 1. Introduction

Supervisory Control and Data Acquisition (SCADA) systems [1,2] play an essential role in smart grid systems. An Internet of Things (IoT) [3] has a wide range of uses, including in smart cities, businesses, and healthcare. An IoT uses cloud computing, which is one approach to meet the present needs of industrial systems. The integration of CPSs such as SCADA systems benefits the IoT and cloud combination [4]. The applications use the network to transport massive amounts of traffic to the end devices, because they work with both sensitive and non-sensitive data. Currently, most Intrusion Detection Systems (IDS) utilized in the SCADA power distribution networks are focused on the cyber sector while disregarding the process states in the physical field. Typically, assaults on protocol

traffic are identified, although it is challenging to locate some harmful network attacks [5,6]. Moreover, cyber-physical systems are frequently used to combine computations with physical processes so that the system may be successfully controlled. The system's performance depends on the proper control [7,8] of sensors and actuators. The system's performance is directly impacted by effective and secure communication between system components, making it of utmost importance. A severe problem in industrial control systems could result from defective device characteristics [9]. In addition, the sensing and data actuation of the system components are affected by significant security concerns [10,11]. Attacks on IT system networks result in congestion or data leakage, but attacks on ICS networks may damage the physical infrastructure and cause information leakage [12]. As a result, cyber-security is considered a crucial component of SCADA [13,14], frequently used in power distribution networks to protect the security of regulated processes. The most critical element of the smart grid, the SCADA system, is responsible for securing communication protocols, asset management, physical infrastructures, and controlled operations [15,16]. These cannot be protected in the same way as modern IT systems. Supporting software, comprising Human Machine Interface (HMI), Distributed Control Systems (DCS), Programmable Logical Controllers (PLC), Remote Terminal Units (RTU), network components, workstations, and processors, are some of the essential elements [11,17,18].

The use of IDS allows for the discovery of security threats and attacks in systems where detection is possible but prevention is not. However, attacks can be identified [19,20] without the need for manual intervention by properly training the detection systems.

### 1.1. Motivation

Due to the heterogeneous deployment of such systems, it is essential to detect intrusion using models based on machine learning algorithms [21,22]. Attack labels can be incredibly difficult, time-consuming, and occasionally even impossible to obtain [23–25]. The majority of unsupervised algorithms currently in use are unable to handle the intrinsic correlations and nonlinearity of multivariate time series, which make up a sizable portion of real-world data, including sensor data streams [6,26]. Figure 1 depicts the general architecture of smart grid SCADA systems. Cyber-physical systems are frequently utilized to combine calculations with physical processes so that the system may be successfully controlled. The system's performance depends on the sensors and actuators being properly controlled. The performance of the system is directly impacted by effective and secure communication between system components, making it of utmost importance.

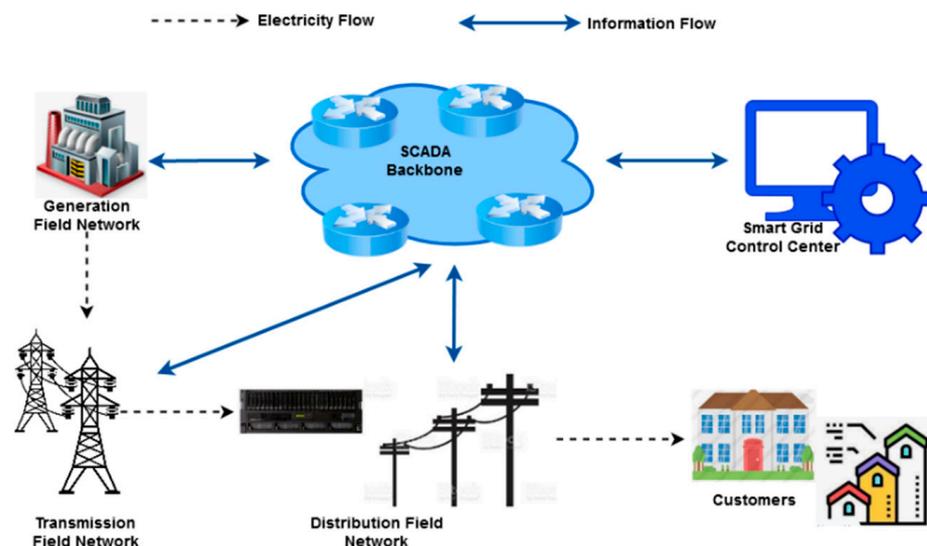


Figure 1. Smart grid SCADA network.

### 1.2. Problem Statement

In industrial control systems, malfunctioning device characteristics could result in a significant problem. The sensing and data actuation of the system components are affected by significant security concerns. Attacks on IT system networks result in congestion or data leakage, but attacks on ICS networks may inflict damage to the physical infrastructure in addition to data leakage. The SCADA smart grid systems [27,28] are protected by a variety of machine learning and deep learning-based technologies that have been developed in the past. However, they continue to have issues with overfitting, a confounding model, an ineffective attack detection rate, and a complex system architecture. As a result, the proposed effort encourages the creation of an innovative and clever security framework for SCADA smart grid systems. Also, cyber-security is regarded as a critical component of SCADA systems, which are frequently used in power distribution networks to ensure the security of regulated processes.

### 1.3. Objectives

The major research objectives of this paper are as follows:

- Data preprocessing is carried out to normalize the original SCADA benchmarking datasets, which includes the operations of content characterization, scalar calculation, and category transformation.
- An innovative Zaire Ebola Search Optimization (ZESO) method that offers the best option for producing the optimized feature set is used to extract the most pertinent features from the normalized dataset.
- A sophisticated Deep Random Kernel Forest Classification (DRKFC) mechanism is used to predict the normal and attack data flows from the SCADA dataset.
- Some of the well-known SCADA benchmarking datasets are used to evaluate the effectiveness and outcomes of the proposed ZESO-RKFC security framework.

### 1.4. Organization

The remaining sections of this article are divided into the following categories: The comprehensive literature assessment of the methods currently employed for protecting SCADA systems for the smart grid is provided in Section 2. In accordance with its operational strategy and security performance, it also examines the advantages and disadvantages of each work. The proposed ZESO-RKFC-based security framework is thoroughly explained in Section 3 along with its overall working methodology and architecture model. Using a wide range of performance metrics and datasets, Section 4 validates and evaluates the results of the suggested mechanism. The findings and future scope are presented in Section 5 to wrap up the entire research.

## 2. Literature Review

The comprehensive literature analysis for assessing various IDS frameworks [29,30] used to improve the security of smart grid networks is presented in this section. Additionally, it covers each model's benefits and drawbacks regarding how it functions and works.

Khalid and Ameen [31] presented a comprehensive literature review to increase the security of IoT-SCADA networks. The original contribution of this work was to ensure the properties of integrity, availability, and confidentiality for protecting the SCADA networks against anomalous activities. Justinthas et al. [32] employed an Elephant Herding Optimization (EHO) integrated NK-RNN classification mechanism for improving the security of SCADA systems. In addition, a modified Elliptic Curve Cryptography (ECC) technique was used to prevent the network from attacks. Lu et al. [33] built a honey pot system for improving the security of SCADA against spoofed attacks. Huda et al. [34] employed an ensemble of deep belief networks for strengthening the security of SCADA-IoT systems. This paper purposes to incorporate two ensemble-based detection methodologies such as SVM and DBN for categorizing the normal and abnormal SCADA network traffic. Hossain et al. [35] developed a new consensus algorithm, named Proof of Random Count in Hashes (PoRCH),

for a blockchain-based SCADA system. The contribution of this work was to design a blockchain-enabled SCADA systems [36], where the blockchain technology has been used to improve the data acquisition process. Moreover, the block creation, verification, and addition processes were performed for data aggregation. Singh et al. [37] developed a two anomaly-based IDS for accurately spotting the stealthy cyber-attacks in the SCADA control system. The key contribution of this work was to highly mitigate the system disturbances by detecting the cyber-attacks within the acceptable time frame. Moreover, this framework includes the major operations of controller deployment, malicious script execution, altering attack generation, and false update transmission. Hasan et al. [38] deployed two distinct security mechanisms for protecting an inline security device in the SCADA systems. This paper mainly is motivated to maximize the link coverage, and minimize the path tolerance of the SCADA network by using a heuristic-based optimization mechanism. Here, the Quadratic Assignment Problem (QAP) was mainly considered to strengthen the security of SCADA systems with enhanced coverage. In addition, the centrality measurements were used to rank the nodes in the network, which helps to control vulnerability in the smart grid systems. For performance assessment, some of the common measures such as link coverage, redundancy, path tolerance, and frequency of occurrence were estimated. However, it requires the maximum amount of time to analyze the volume of traffic during attack detection, which was the key limitation of this work. Islam et al. [39] investigated the different types of vulnerabilities, threats, and countermeasures for improving the security of smart grid systems. Typically, the major components involved in the smart grid networks were generation units, transmission and distribution units, and the communication network. Moreover, this work [40] mainly concentrated on enhancing the physical layer security against different types of security attacks such as data fabrication, man in the middle, jamming, DoS, false data injection, spear phishing, and data compromise. In addition, it suggested suitable countermeasure methodologies to increase security, such as key generation mechanisms, spread spectrum mechanisms, resilience techniques, and machine learning-based approaches. The performance of this technique has been validated in terms of computational cost and communication overhead. Mir et al. [2] presented a detailed security assessment for analyzing the baseline requirements for SCADA systems. It includes the following key elements:

- Risk management;
- Malware protection;
- Vulnerability assessment;
- Security control;
- Cyber-risk analysis;
- Physical security.

Moreover, it suggested various controls used for fulfilling SCADA security requirements, such as single point of accountability, cyber security policy, security management, and information security. Abir et al. [41] highlighted some of the advanced technologies such as blockchain, machine learning, deep learning, and AI for securing the IoT-smart grid systems. This study comprises the communication, computation, sensor, cyber attack, SCADA, and blockchain technologies for ensuring the safety of IoT networks. Risco et al. [42] recommended a machine learning algorithm to maintain the stability and security of IoT-SCADA systems. The purpose of this work was to choose the most suitable algorithm for efficiently predicting the stability of grid systems. In paper [43], a detailed overview of an Intrusion Detection Prevention System (IDPS) is provided, which helps to ensure the security of smart grid systems. The purpose of this work was to investigate the different types of cyber-threats that affect the normal operations of the smart grid. Moreover, its object is to enable reliable and secured data transmission in the smart grid by using an IDPS framework. Martinelli et al. [26] utilized a supervised machine learning methodology for spotting intrusions in the smart grid—SCADA networks. This framework includes the modules of log under analysis, feature extraction, machine learning classification, and intrusion detection. However, this work failed to prove the efficacy and attack

detection competency of the suggested model. Singh et al. [44] developed a cyber-kill chain-based IDS framework for increasing the security of SCADA networks.

### *Research Gap*

In recent years, many hacks have increased the vulnerability of smart grid networks. These cyberattacks take many forms and aim to steal data, damage physical or digital infrastructure, or gain access to complex systems [45]. The detection of cyberattacks in smart-grid settings has been addressed using ML approaches; however, those studies should have considered cross-validation comparing algorithms with different parameter values. Furthermore, these ML algorithms cannot be used on various smart grids because they were often tested only on one smart-grid scenario. Typically, reducing the detection latency and increasing the robustness and consistency of the smart grid systems are highly crucial in smart grid systems. Hence, it is essential to implement a proper data management and security scheme for intrusion prevention and detection in smart grid systems. According to comprehensive examination, the traditional works are constrained by the significant issues listed below:

- High delay;
- Overfitting;
- Decreased detection accuracy;
- Ineffective handling of massive datasets;
- Complexity of computation.

This research presents a concatenated deep learning strategy to overcome these limitations. Furthermore, deep learning algorithms are more effective than machine learning approaches at handling high-dimensional data and producing good results. Thus, a straightforward and computationally effective AI-based security model is developed in the proposed work for smart grid systems. The objective is to protect private information and identify harmful activity in the network traffic of power systems.

### **3. Materials and Methods**

The proposed AI-based security paradigm for smart grid SCADA systems is completely described in this section. The purpose of this work is to develop a novel security framework for protecting smart grid SCADA systems against harmful network vulnerabilities or intrusions. The unique contribution of this research is the implementation of a straightforward and computationally effective AI mechanism based on meta-heuristic optimization for enhancing IoT-SCADA network security. This work employs sophisticated and intelligent strategies to accomplish this objective. This strategy employed a hybrid approach by leveraging the advantages of the consistent and predictable communication patterns that are used by in-ground devices in ICS. To scale and standardize the data, a limited number of preprocessing techniques are most often used. Then, a meta-heuristic optimization algorithm for dimensionality reduction was employed to improve the performance of anomaly detection. Here, the SCADA benchmarking datasets are obtained as the inputs for processing, which comprise some irrelevant fields and attributes. Hence, they are preprocessed at the beginning with the operations of content characterization, scalar model estimation, normalization, and categorical transformation. This kind of dataset normalization helps to increase the detection accuracy and efficiency of classification. Consequently, a Zaire Ebola Search Optimization (ZESO) algorithm is deployed to choose the relevant features from the normalized data. Specifically, this optimization technique is used to analyze the characteristics of attacks in the IoT-SCADA networks. Moreover, the Random Kernel Forest Classification (RKFC) algorithm is deployed to predict the label as normal or attack. In previous security frameworks, the authors have used various ML/DL techniques for detecting intrusions in the smart grid systems. However, the existing approaches face problems in terms of reduced performance rate, have slow processing, are expensive in computational cost, are more difficult to perform modifications on, and have poor detection performance. Thus, the computationally efficient ZESO-based RKFC mechanism is

implemented in this work. It effectively simplifies the process of intrusion prediction and classification by providing a suitable solution used to select the most relevant features for classifier training and testing. The key benefits of the proposed ZESO-RKFC-based security framework are as follows: increased convergence rate, reduced complexity, minimal time consumption, and high detection efficiency. The architectural model of the smart grid SCADA system with the cyber layer elements is shown in Figure 2. Then, the working model of the proposed ZESO-RKFC framework is depicted in Figure 3, which encompasses the following modules of operation:

- SCADA benchmark dataset obtainment;
- Normalization;
- ZESO-based feature selection;
- DRKFC-based attack prediction;
- Performance evaluation.

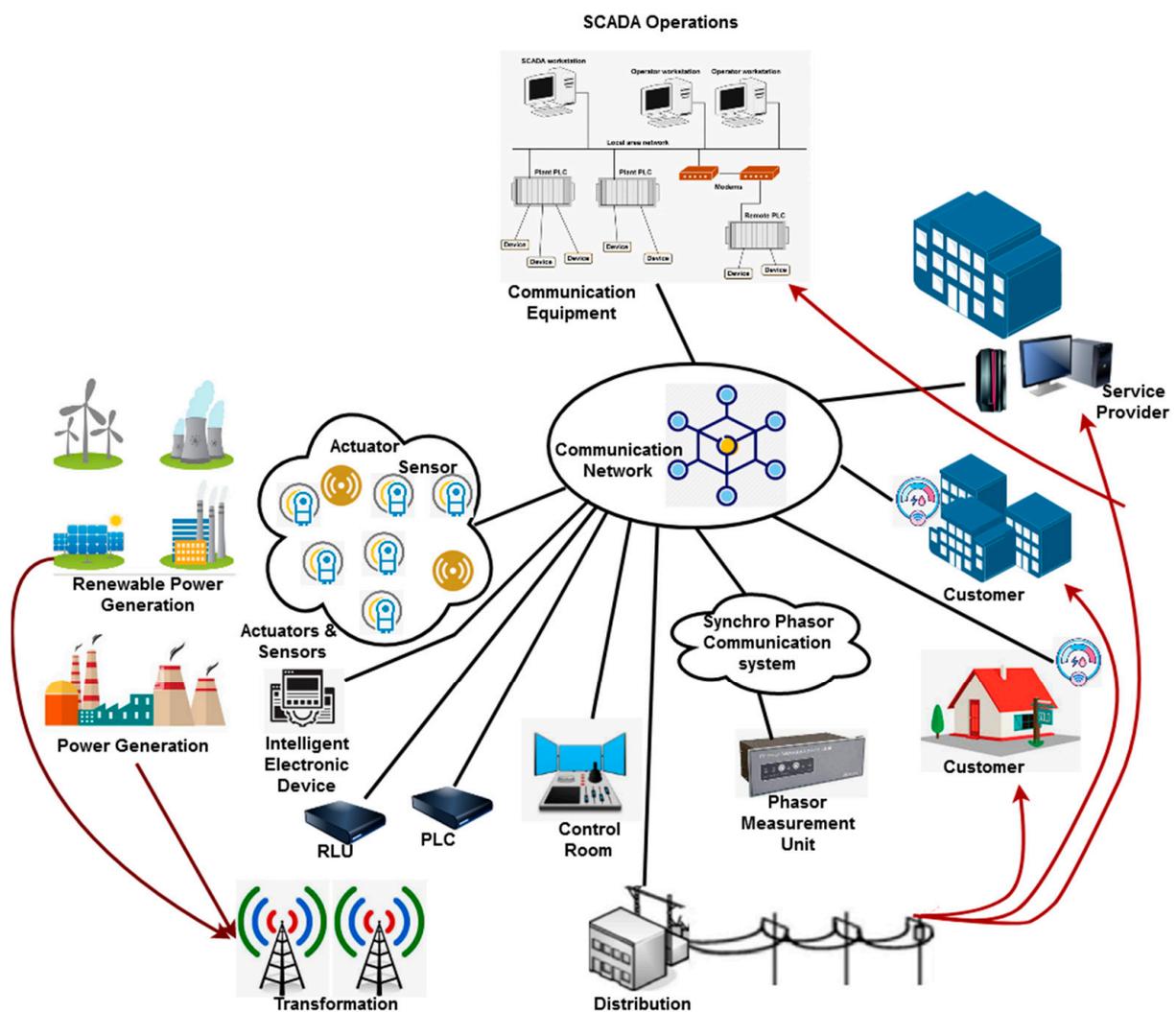


Figure 2. Architecture model of the smart grid network with cyber layer elements.

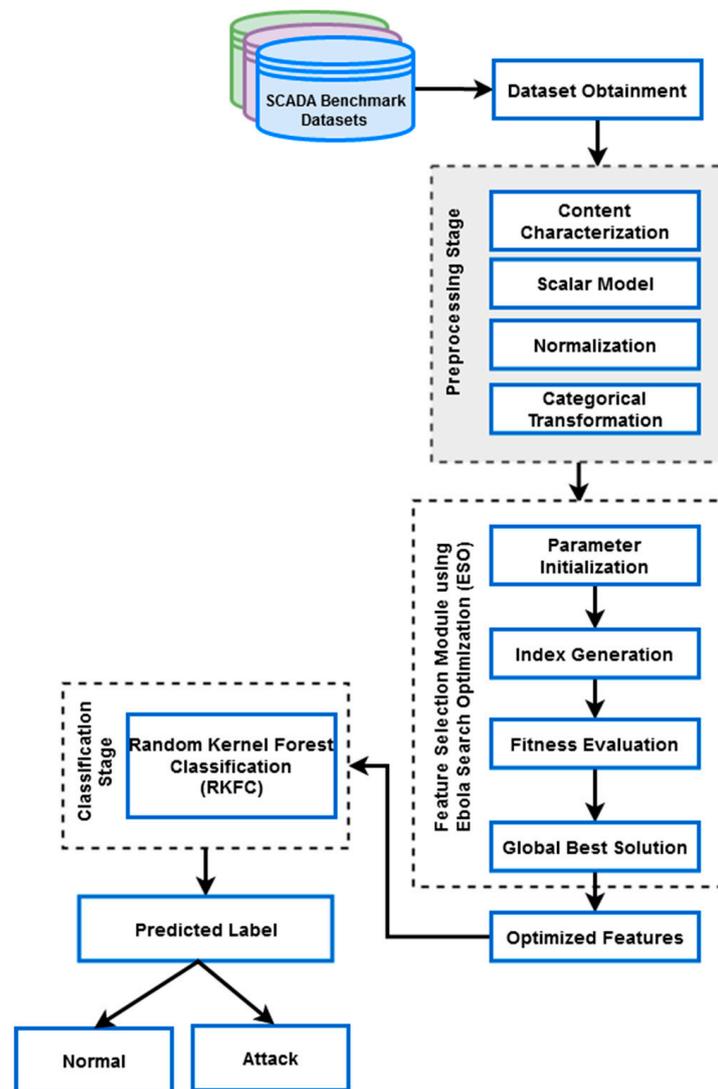


Figure 3. Working flow of the ZESO-RKFC-based security framework.

The list of symbols and their descriptions are presented in Table 1.

Table 1. Symbols and their descriptions.

Parameters	Descriptions
$N_F$	Transformed input parameter
$mn, mx$	Specified range of input variables
$d_{mx}$ & $d_{mn}$	Initial range of input parameters (minimum and maximum values of the dataset)
$\alpha_c$	Infected individual
$e_c$	Exposed individual
$\rho_s$	Susceptible
$\beta_c$	Recovered
$\gamma_c$	Dead
$\vartheta_c$	Vaccinated
$\mathcal{H}_c$	Hospitalized
$\mathcal{Q}_c$	Quarantined
$AI$	Agents can infect people
$\varepsilon_1$	Contact rate of infection
$\varepsilon_2$	Contact rate of pathogen

Table 1. Cont.

Parameters	Descriptions
$\varepsilon_3$	Contact rate of deceased
$\varepsilon_4$	Contact rate of recovered
$\sigma$	Natural death rate
$\varphi$	Disease-induced death rate
$\pi$	Recruitment rate
$\eta$	Rate response to vaccination
Z	Recovery rate
S	Rate of burial of deceased individual
V	Rate of vaccination of individual
$\tau$	Rate of quarantine
K	Number of trees
$\delta$	Number of leaves
M	Matrix
P	Regularization parameter
$g(c_i, \hat{c}_i)$	Loss function

### 3.1. Preprocessing

Here, the data preprocessing is mainly performed to transform the data values from the original datasets for optimizing the attributes. At first, the content characterization is performed to analyze the characteristics of the dataset, since it helps to represent the protocol connections that are similar to the characteristics of the dataset. Then, the flow and content characteristics are also used to analyze the attributes and http connections. Moreover, the attributes correlated to the time are estimated based on the time characteristics. Typically, normalizing the data reduces the complexity of the algorithm for processing them because there is a large contrast between the dataset's maximum and minimum values. Moreover, the data normalization is used to boost the accuracy and efficiency of classification, and also it speeds up the training process for minimizing time consumption. Thus, the data normalization is performed in this work, where normalization-based data scaling is performed by using the min-max algorithm. It converts the data within the interval ranges of  $-1$  to  $1$  and  $0$  to  $1$ , and the function is estimated as shown below:

$$N_F = \frac{((d - d_{mn})(mx - mn))}{(d_{mx} - d_{mn}) + min} \quad (1)$$

where  $N_F$  is the transformed input parameter,  $mn, mx$  are the specified range of input variables,  $d_{mx}$  and  $d_{mn}$  are the initial range of input parameters (minimum and maximum values of the dataset). Consequently, the standardization or z-score computation is performed to properly normalize the attributes of the given SCADA benchmark datasets. This function is mainly used to normalize the standard distribution based on the attributed values of the dataset. The function is represented as follows:

$$d^{(j)} = \frac{d^{(j)} - Mean^{(j)}}{SD^{(j)}} \quad (2)$$

Based on this operation, the normalized dataset is generated from the preprocessing stage, which can be used for further processing.

### 3.2. Zaire Ebola Search Optimization (ZESO)

After preprocessing the dataset, an advanced optimization algorithm, called ZESO, is utilized to choose the optimal features from the normalized SCADA datasets. In the existing work, various meta-heuristic algorithms are developed for feature optimization and attribute selection. For instance, Firefly (FF), Whale Optimization (WO), Artificial Jelly Fish (AJF), Spider Monkey (SM), and Greedy Search (GS) are the recently developed optimization algorithms, which are widely applied in many application domains for

solving complex problems. However, these methods suffer with the problems of reduced convergence rate, local optimum, time consumption, and difficulty in understanding. Therefore, the proposed work is motivated to deploy a computationally effective ZESO algorithm for feature selection.

In this technique, all vectors and scalar quantities are initialized at first, which includes susceptible ( $\rho_s$ ), infected ( $\alpha_c$ ), recovered ( $\beta_c$ ), dead ( $\gamma_c$ ), vaccinated ( $\vartheta_c$ ), hospitalized ( $\mathcal{H}_c$ ), and quarantined ( $\mathbb{Q}_c$ ). After that, the index case ( $\rho$ ) is randomly generated according to the susceptible individuals. Here, the index case ( $\delta$ ) is set as the global best, and its fitness value is estimated. There is at least one infected person and the number of iterations has not reached its limit; the following conditions are executed: Based on the displacement, each susceptible person creates and updates their position. Let us consider that the number of infections increases with distance; hence, a short displacement reflects exploitation, whereas a long displacement describes exploration:

- The newly infected persons ( $nP$ ) are generated based on the set (s);
- Then, the generated persons are added in  $\alpha_c$ ;
- According to the size of  $\alpha_c$ , the number of individuals is estimated and added to  $\mathcal{H}_c$ ,  $\mathbb{Q}_c$ ,  $\beta_c$ ,  $\gamma_c$ , and  $\vartheta_c$ .
- Consequently, update ( $\rho_s, \alpha_c$ ) based on  $nP$ ;
- Choose the current best value from  $\alpha_c$ , and compare it with the global best;
- Finally, return the global best solution with the optimal solution;

Here, the location of each person who is exposed is updated by using the following equation:

$$k\alpha_{ci}^{t+1} = k\alpha_{ci}^t + SK(\alpha_c) \tag{3}$$

where  $S$  indicates the displacement scale factor of the individual,  $k\alpha_{ci}^{t+1}$ ,  $k\alpha_{ci}^t$  represents the updated and original positions,  $t$  is the time.  $K(\alpha_c)$  represents the movement rate estimated by the individuals and is estimated by using the following equations:

$$K(\alpha_c) = sD \times rand(0,1) + K(I_B) \tag{4}$$

$$K(\rho_s) = lD \times rand(0,1) + K(I_B) \tag{5}$$

where  $sD$  indicates the short distance movement, and  $lD$  represents the average neighborhood range. These parameters are regulated based on the neighborhood parameter range  $\geq 0.5$ . In this optimization, the initial population is generated based on the random number distribution, and positions are initially updated as 0. Then, the upper and lower bounds are estimated for the individual  $i = 1, 2, 3 \dots N$  in the population size.

$$ind_i = lb_i + rand(0, 1) \times (up_i + lb_i) \tag{6}$$

Consequently, the current best is selected according to the set of infected individuals at time  $t$  as shown below:

$$BS = \begin{cases} GB, & fitness(CB) < fitness(GB) \\ CB, & fitness(CB) \geq fitness(GB) \end{cases} \tag{7}$$

where  $BS$  indicates the best solution, and  $GB$  and  $LB$  are the global best and current best solution, respectively. Moreover, the parameters  $GB$  and  $LB$  are treated as the super spreader and spreader of the Ebola. Moreover, the differential calculus is applied to attain the rate of quantities such as  $\rho_s$ ,  $\alpha_c$ ,  $\beta_c$ ,  $\gamma_c$ ,  $\vartheta_c$ ,  $\mathcal{H}_c$ , and  $\mathbb{Q}_c$ . Then, the scalar functions are computed as follows:

$$\frac{\partial \rho_s(t)}{\partial t} = \pi - (\varepsilon_1 \alpha_c + \varepsilon_3 \gamma_c + \varepsilon_4 \beta_c + \varepsilon_2(AI))\rho_s - (\sigma \rho_s + \varphi \alpha_c) \tag{8}$$

$$\frac{\partial \alpha_c(t)}{\partial t} = (\varepsilon_1 \alpha_c + \varepsilon_3 \gamma_c + \varepsilon_4 \beta_c + \varepsilon_2(AI)\lambda)\rho_s - (\varphi + Z)\alpha_c - (\sigma)\rho_s \tag{9}$$

$$\frac{\partial \mathcal{H}_c(t)}{\partial t} = R\alpha_c - (Z + \omega)\mathcal{H}_c \tag{10}$$

$$\frac{\partial \beta_c(t)}{\partial t} = Z\alpha_c - \varphi\beta_c \tag{11}$$

$$\frac{\partial \vartheta_c(t)}{\partial t} = Z\alpha_c - (\eta + V)\vartheta_c \tag{12}$$

$$\frac{\partial \gamma_c(t)}{\partial t} = (\sigma\rho_s + \varphi\alpha_c) - S\gamma_c \tag{13}$$

$$\frac{\partial Q_c(t)}{\partial t} = (\pi\alpha_c - (Z\beta_c + \varphi\gamma_c)) - \tau Q_c \tag{14}$$

To calculate the population of susceptible individuals at time t, the rate of change of the susceptible population is calculated and applied to the size of the susceptible vector as it is at the moment. The flow of the proposed ZESO algorithm is depicted in Figure 4.

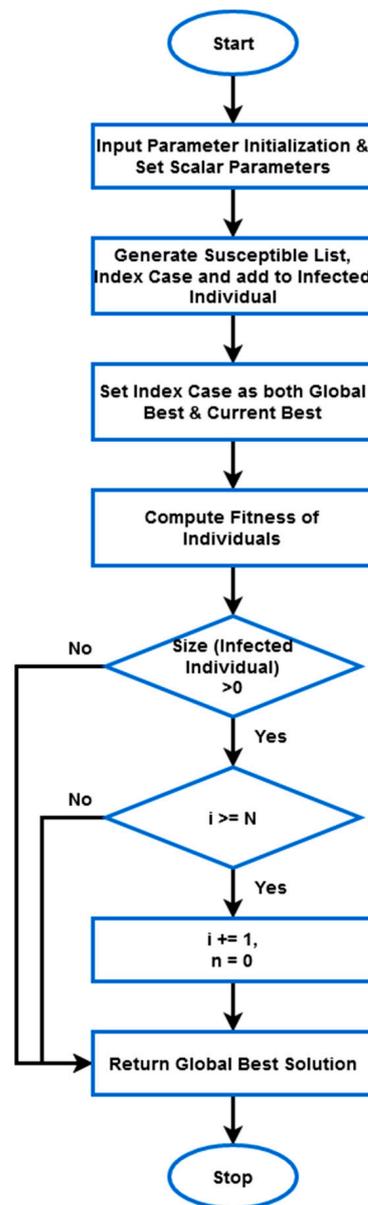


Figure 4. Flow of ZESO algorithm.

Based on the obtained solution, the optimal number of features is selected from the normalized SCADA dataset, which can be used for training the sample of classifier. The primary benefits of using this algorithm are as follows: simple to implement, increased convergence rate, reaches best optimal solution with minimal number of iterations, and computational efficacy.

### 3.3. Deep Random Kernel Forest Classification (DRKFC)

After feature selection, an intelligent DRKFC model is deployed to categorize the normal and attacking data flows according to the set of extracted features. Conventionally, various machine learning and deep learning techniques are implemented for security applications. But it degrades with key problems of complex mathematical modulations, high false positives, overlapping results, and incapability to handle huge dimensional datasets. Therefore, this paper motivates to implement a new and smart DRKFC model for securing the smart grid SCADA systems. A random forest constructed from trees with kernel decision splitters is called a Kernel Forest. A general top-down induction process is followed in the top-level training of such trees. The traditional random forest algorithm greedily locates a quasi-optimal distribution of classes to sub-trees at each stump and trains this stump as a binary classifier. In this approach, the data is processed progressively through a number of layers, which is a variant of the deep forest. Each sample from the training set is used to build a set of objects in that layer, and each object is labeled with the class of the original sample. The layered architecture model of the proposed DRKFC is shown in Figure 5. The fundamental idea behind that strengthening procedure is to swap out the initial class empirical likelihoods previously stored in each tree leaf of a pre-trained forest with new ones produced by explicitly reducing a global loss function in accordance with the random forest’s averaging rule. Let consider, the forest has  $K$  number of trees and  $\delta$  number of leaves, which is in the form of  $\Psi : \mathbb{N}^f \rightarrow \{0, 1\}^{K\delta}$ . This is the function for any sample  $t$  that returns the binary vector and its elements are 1, if  $t$  goes to the corresponding decision tree; otherwise, it is set as 0 [46].

$$\Psi(t) = (\varphi_1(t), \varphi_2(t) \dots \varphi_{K\delta}(t)) \tag{15}$$

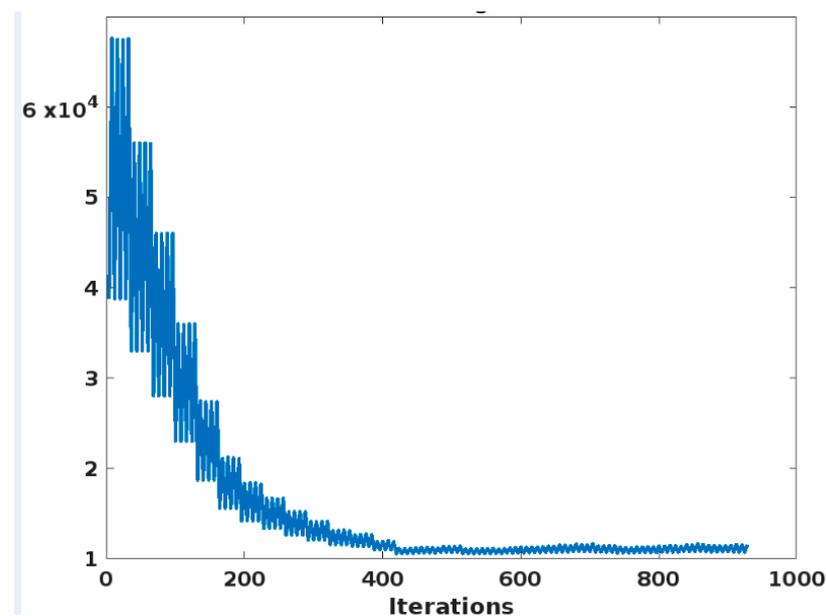


Figure 5. Fitness plot of ZESO.

For all decision trees, the matrix  $M$  having the corresponding class weight is shown below:

$$M = (\alpha_1, \alpha_2, \dots \alpha_{K\delta}) \tag{16}$$

Consequently, the linear function is estimated by using the following model:

$$b = M^* \Psi(t) \quad (17)$$

$$M^* = \underset{M}{\operatorname{argmin}} \frac{1}{2} \|M\|_X^2 + \frac{P}{w} \sum_{i=1}^w g(c_i, \hat{c}_i) \quad (18)$$

$$c_i = M\Psi(t), \forall i \in [1, w] \quad (19)$$

where  $P$  indicates the regularization parameter;  $g(c_i, \hat{c}_i)$  denotes the loss function. After pruning, the random kernel forest is used to process the sample-extracted features. The produced synthetic class probabilities obtained from the kernel forest's trees are represented by these embedding. The original features and the empirical probability vectors that the improved forest trees have returned are included in the hidden states. Moreover, the global refinement procedure of DRKFC is significantly more useful for performing the embedding operations. Based on this operation, the normal and attacking data flows are accurately predicted from the SCADA benchmarking datasets using the optimized features.

#### 4. Results

This section validates the performance and results of the proposed ZESO-DRKFC model by using various evaluation measures. For this evaluation, the different types of SCADA benchmarking datasets are used to analyze the security of the proposed framework. Character-based features cannot be processed by deep learning models; hence, preprocessing operations such as normalization and feature screening must be carried out on the input data before they are fed into the deep learning model in order to simplify and process them. Following preprocessing, the features are converted to numerical features, which are then integrated with the dataset's already-existing numerical features. Additionally, the labels in the dataset have been numerically processed so that normal behavior is denoted by the number "0," whereas abnormal behavior is denoted by the number "1". The dataset is normalized and uniformly mapped to reduce feature differences. Uniform mapping has an interval range of (0, 1). The performance parameters used in this study are computed by using the following equations:

$$Accuracy = \frac{TrP + TrN}{TrP + TrN + FaP + FaN} \times 100\% \quad (20)$$

$$Precision = \frac{TrP}{TrP + FaP} \times 100\% \quad (21)$$

$$F1 - score = \frac{2 \times Pre \times Sen}{Pre + Sen} \times 100\% \quad (22)$$

$$Recall = \frac{TrP}{TrP + FaN} \times 100\% \quad (23)$$

$$Sensitivity = \frac{TrP}{TrP + FaN} \times 100\% \quad (24)$$

$$Specificity = \frac{TrN}{TrN + FaP} \times 100\% \quad (25)$$

where  $TrP$ —true positive,  $TrN$ —true negative,  $FaP$ —false positive, and  $FaN$ —false negative. For assessing the performance of the ZESO technique, the parameters such as fitness plot and convergence curve are validated as shown in Figures 5 and 6, respectively. Here, the reason for estimating these parameters is to analyze the efficacy and competency of the proposed optimization mechanism. Typically, the convergence rate is one of the most essential parameters used to assess the performance of the optimization mechanism. According to the analysis, it is analyzed that the proposed ZESO provides effective optimization results with an increased convergence rate.

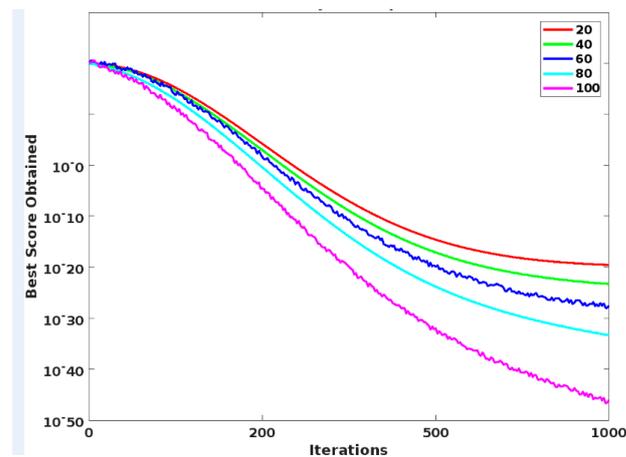


Figure 6. Convergence analysis of ZESO.

In this study, the most popular benchmarking datasets used for analysis are represented in Table 2. The description of dataset 1 is provided in Figure 7, which includes the attacking classes of normal, DoS, Probe, R2L, and U2R. Consequently, the description of dataset 2 is provided in Figure 8, which includes the attacking classes of DoS, fuzzy, RPM spoofing, and gear spoofing.

Table 2. Datasets used for analysis.

Datasets	Name
Dataset 1	NSL-KDD
Dataset 2	CAN intrusion
Dataset 3	CIC-IDS 2017
Dataset 4	BoT-IoT
Dataset 5	DS2OS
Dataset 6	UNSW-NB 15
Dataset 7	CIRA-CIC-DoHBrw-2020

Attack Type	Total Number of	Training	Testing
Normal	67,343	53,874	13,469
DoS	45,927	36,742	9185
Probe	11,656	9325	2331
R2L	995	796	199
U2R	52	42	10

Figure 7. NSL-KDD dataset description.

Attack Type	Total number of samples	Training Samples	Testing Samples
Normal	14,037,293	9,826,105	4,211,188
DoS	587,521	411,265	176,256
Fuzzy	491,847	344,293	147,554
RPM Spoofing	654,897	458,428	196,469
Gear Spoofing	597,252	418,076	179,176

Figure 8. CAN-intrusion dataset description.

Figure 9 validates the training loss characteristics of the proposed ZESO-DRKFC technique with respect to the varying number of epochs. Based on the results, it is analyzed that the training loss is gradually reduced after reaching the ninth epoch. Due to the optimal selection of attributes, the training loss of the proposed model is efficiently reduced in this model. Figures 10 and 11 depict the ROC characteristics for dataset 1 and dataset 2, respectively. According to the analysis, it is observed that the proposed ZESO-DRKFC provides an improved true positive rate with reduced false positives. Overall, the ROC of the suggested methodology is greatly enhanced as a result of the appropriate feature selection. The confusion matrix of several datasets produced using the suggested ZESO-DRKFC methodology is shown in Figures 12–16. Usually, the confusion matrix is used to gauge the effectiveness and outcomes of the assault detection methods. The results show that the proposed technique offers better outcomes since the parameters were properly chosen and categorized.

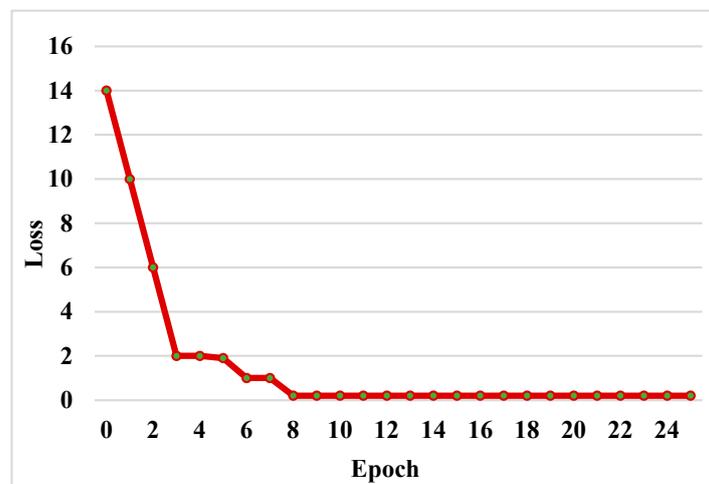


Figure 9. Training loss analysis.

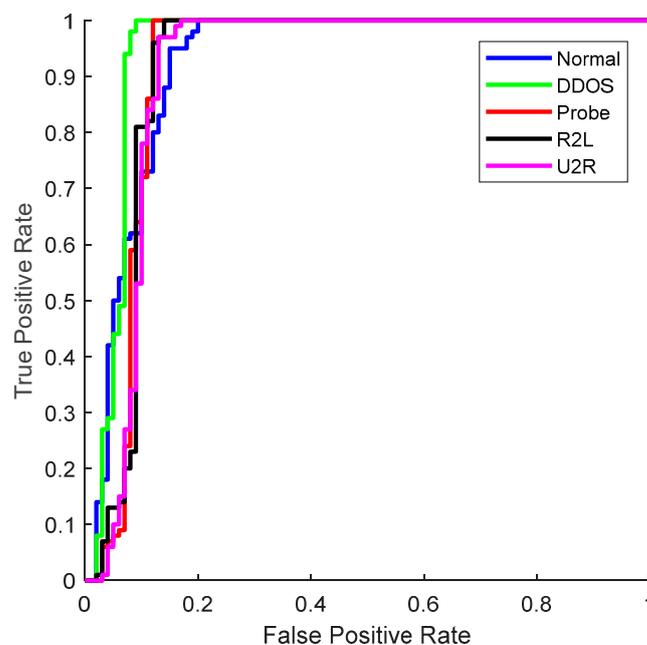


Figure 10. ROC for dataset 1.

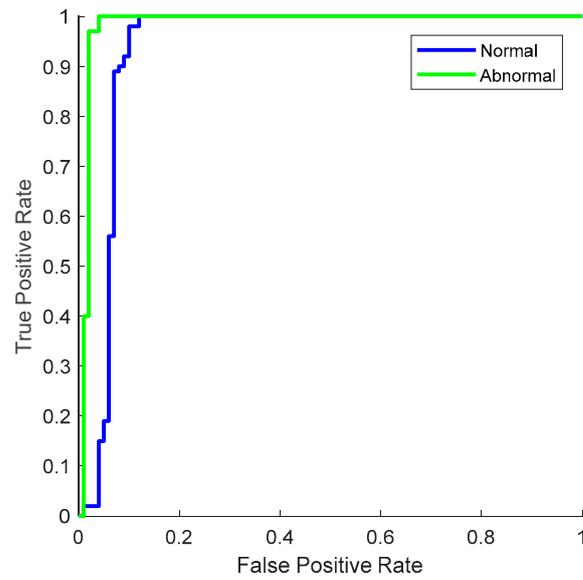


Figure 11. ROC for dataset 3.

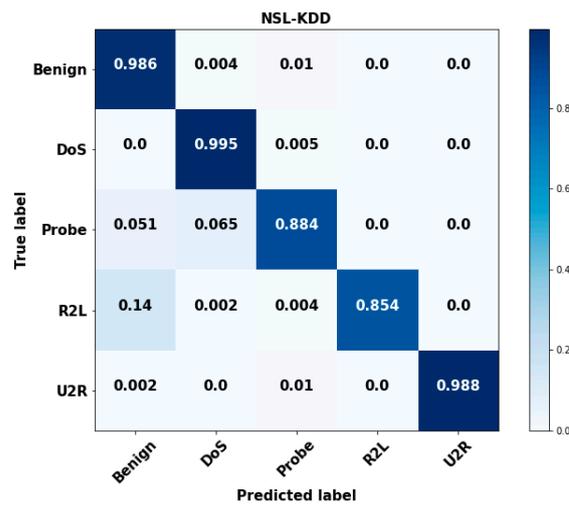


Figure 12. Confusion matrix for dataset 1.

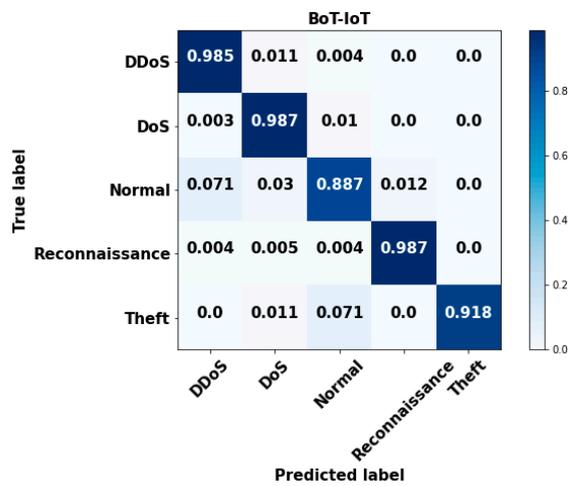


Figure 13. Confusion matrix for dataset 4.

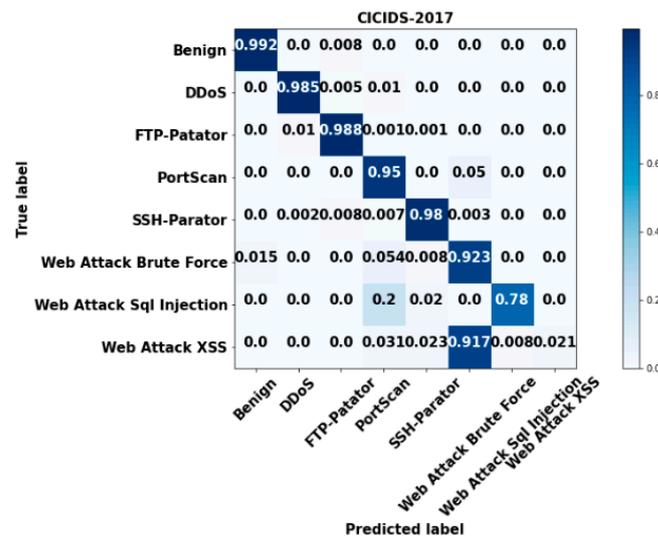


Figure 14. Confusion matrix for dataset 3.

Normal	22465	412	3	2	0	259	1	107	1	0
Fuzzers	159	5849	0	1	19	15	5	4	8	1
Backdoor	4	1	561	0	6	1	0	9	0	0
Analysis	8	1	3	650	1	0	1	3	0	2
Reconnaissance	16	7	0	1	3449	0	2	12	0	1
Exploits	12	793	1	0	8	9845	1	472	0	0
Generic	6	17	0	0	0	20	14676	1	0	0
DoS	220	63	4	2	0	77	0	3721	0	1
Shell Code	4	11	0	2	0	5	0	1	357	0
Worms	3	0	0	0	0	0	0	0	0	41

Figure 15. Confusion matrix for dataset 6.

Normal	86328	588	0	2	4	2	60	0
DoS	299	1124	3	3	0	1	15	0
Malicious Control	2	0	219	1	0	0	2	0
Malicious Operation	4	3	0	188	0	2	4	0
Spying	2	0	0	1	128	0	1	3
Wrong Setup	1	2	1	0	0	26	0	2
Scan	66	31	0	0	0	0	289	1
Datatype Probing	2	0	0	0	0	0	0	84

Figure 16. Confusion matrix for dataset 5.

Figure 17 validates the false detection rate of the conventional and proposed attack detection methodologies using dataset 1. The false detection rate is mainly estimated for how exactly the classifier forecasts the normal and attacking data flows according to the optimized set of features. Moreover, the false prediction rate is minimized to ensure better system performance. Figure 18 shows the precision, detection rate, f1-score and FPR of the proposed methodology concerning different types of attacks in dataset 1. These parameters are mainly used to determine the classifier’s overall performance, and the perfect attack detection methodology should improve the values of these parameters. Moreover, Table 3 and Figure 19 present the comparative analysis of the existing and proposed security methodologies using dataset 3. The overall performance of the proposed ZESO-DRKFC beats those of cutting-edge methods. As a result, it is usually appropriate to quantify measures such as testing and training time succinctly. Although the proposed model performed better than the baseline models, it is still not determined if the proposed technique completely surpassed the alternatives. Nevertheless, it is indicated that the suggested solution enables outstanding network protection and the quick detection of dangerous attacks.

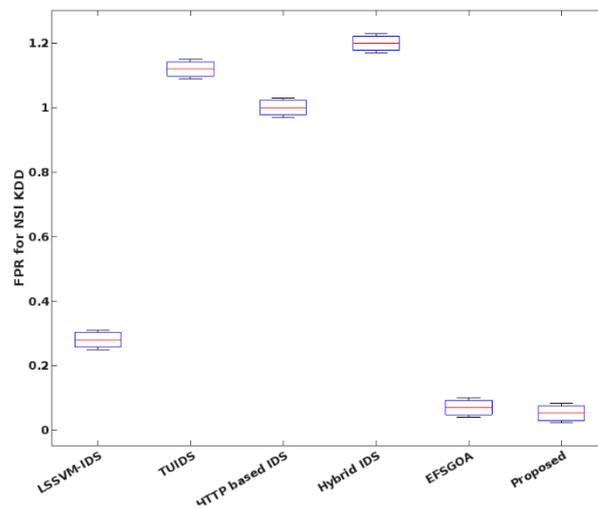


Figure 17. False detection rate.

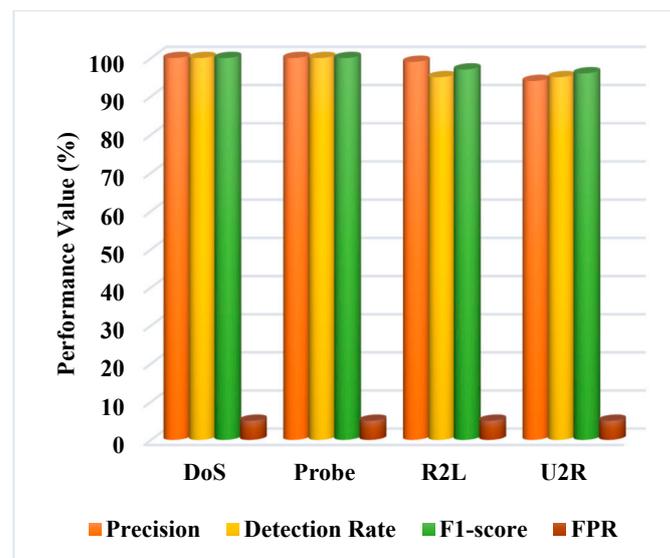
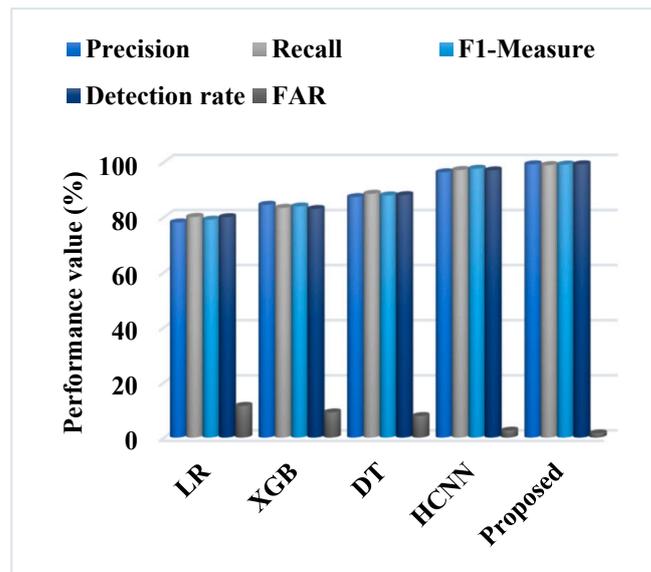


Figure 18. Overall performance analysis using dataset 1.

**Table 3.** Comparative analysis using dataset 3.

Methods	Precision	Recall	F1-Measure	Detection rate	FAR
LR	78.1	80.1	79.1	80	11.50
XGB	84.5	83.4	83.9	83	9.13
DT	87.3	88.5	87.9	88	7.8
HCNN	96.3	97.12	97.6	97	2.5
Proposed	99.2	98.9	99.1	99.2	1.5



**Figure 19.** Performance analysis using dataset 3.

Table 4 compares the classification accuracy of conventional and proposed security mechanisms by using dataset 3. Zaire Ebola Search Optimization could optimize the features of SCADA benchmarking datasets based on the global best solution, which helps to speed up the training process with increased detection results. The suggested technique provides maximum accuracy when compared to other models because of effective feature selection and a concatenated procedure. Moreover, the results show that the proposed model effectively identifies network assaults and offers a higher detection rate and accuracy. Also, it is adequate for an industrial system intrusion detection model to effectively detect the attacks.

**Table 4.** Accuracy analysis using dataset 3.

Methods	Accuracy
DBN	95
DNN	90.25
DL	95
LSTM	96.2
IDS-DL	96
CNN IDS	96
HCRNN	97.75
Proposed	99.3

Figure 20 presents the overall comparative analysis of the existing [47] and proposed security mechanisms based on the parameters of accuracy, detection rate, FAR, and f1-score. From the findings, it is apparent that the proposed model performs better than alternative models. The proposed model’s maximum precision and detection rate show that all normal and aberrant network activity is efficiently detected. The results show that the

ZESO-DRKFC methodology is superior to alternative methods with better values for these parameters. Consequently, Figure 21 presents the overall performance analysis of the existing and proposed methods by using dataset 3. This analysis also indicates that the proposed model provides an improved result over the other techniques, due to the proper normalization and optimization operations.

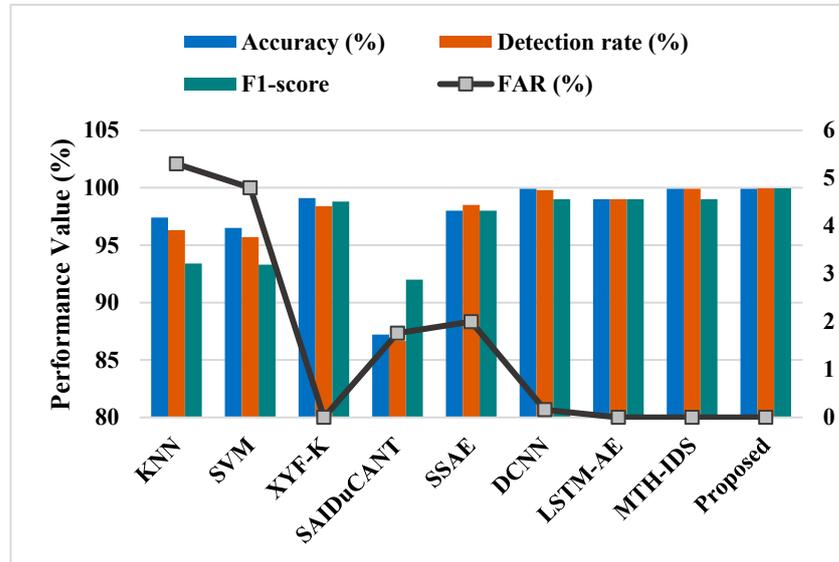


Figure 20. Overall performance analysis using dataset 2.

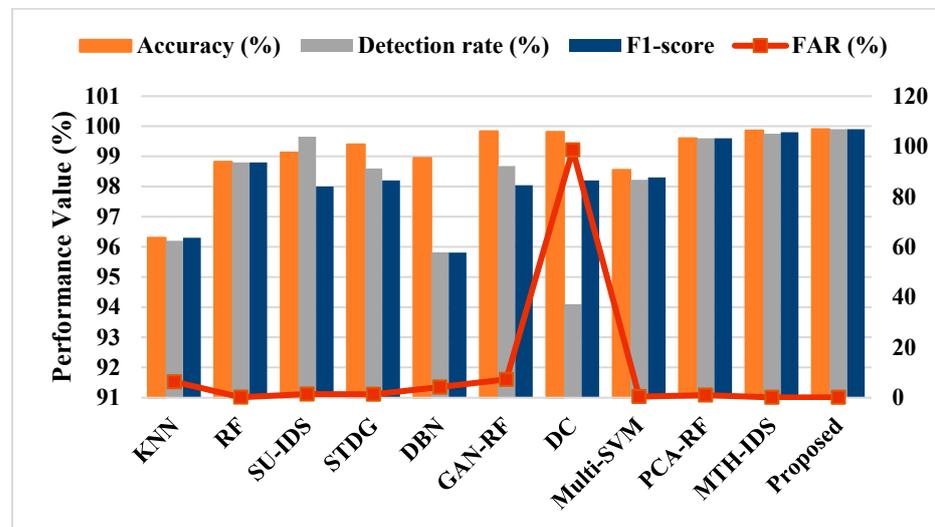


Figure 21. Performance comparative analysis using dataset 3.

### 5. Discussion

Deep learning models cannot process character-based features; thus, before feeding the input into the model, preprocessing operations such as normalization and feature screening are carried out to simplify and process the input data. As a result, the computational complexity of the suggested model is slightly higher than that of the existing methodologies. However, the proposed model is adequate for an industrial intrusion detection model to identify attacks effectively. This paper’s minor limitation is that the detection performance may somewhat alter due to environmental and system changes. Additionally, this paper could be strengthened by concentrating on the additional grid environment factors.

## 6. Conclusions

Smart grid CPSs, a crucial component of the infrastructure of every nation, have recently become the targets of more cyberattacks of various kinds. Examples of CPS security difficulties include the theft of private information, the insertion of fake data, and the destruction of assets and data in a smart grid via hacked physical devices deployed in a physical environment and managed by SCADA systems. The early identification of these intrusions is therefore necessary to protect the data and equipment of the smart grid. The work already undertaken on intrusion detection techniques for smart grids is insufficient. For the purpose of detecting cyberattacks on a smart grid, a number of machine learning (ML) techniques have been deployed in recent years that employ supervised or unsupervised methodologies. These techniques classify cyberattacks using a number of smart grid network parameters.

This paper presents a new security framework for protecting the IoT-SCADA systems by using computationally efficient and intelligent techniques. The main contribution of this work is to accurately detect cyber-attacks from the SCADA benchmarking datasets by using a novel meta-heuristic-based AI mechanism. Here, the operations of categorical transformation, scalar modeling, and normalization are used to perform dataset preprocessing in order to first normalize the dataset before classification. The ZESO technique offers the best optimal solution to choose the pertinent qualities for improving the speed of classifier training and testing. It also helps to improve the detection accuracy and efficiency of the classifier. The categorized label is then predicted to determine whether the data flow is normal or attacking using the DRKFC technique. Reduced overfitting, higher convergence rates, quick training, and simplicity are the main advantages of this approach. During experimental analysis, the performance of the proposed mechanism is validated and tested by using various parameters. Also, system implementation and performance assessment are carried out by using the standard and popular benchmarking datasets. The overall results reveal that the suggested technique produces better outcomes for all datasets, demonstrating the effectiveness and enhanced functionality of the proposed methodology. The novel ZESO-DRKFC outperforms the other strategies due to effective parameter optimization and training procedures.

In future, this work could be extended by implementing a deep learning methodology for increasing the security smart grid networks.

**Author Contributions:** Data curation: O.B.J.R. and M.K.; Writing original draft: S.S. and P.K.B.; Supervision: S.S. and P.K.B.; Project administration: S.S. and P.K.B. Conceptualization: S.S. and P.K.B.; Methodology: S.S. and P.K.B.; Validation: O.B.J.R. and M.K.; Visualization O.B.J.R. and M.K.; Resources: O.B.J.R. and M.K.; Review and Editing: O.B.J.R. and M.K.; Funding acquisition: O.B.J.R. and M.K. All authors have read and agreed to the published version of the manuscript.

**Funding:** This project was funded by the Deanship of Scientific Research (DSR) at King Abdulaziz University (KAU), Jeddah, Saudi Arabia, funded under grant no. (RG-9-611-43). Therefore, the authors acknowledge DSR's technical and financial support with thanks.

**Conflicts of Interest:** The authors declare no conflict of interest.

## References

1. Jakaria, A.; Rahman, M.A.; Gokhale, A. Resiliency-aware deployment of SDN in smart grid SCADA: A formal synthesis model. *IEEE Trans. Netw. Serv. Manag.* **2021**, *18*, 1430–1444. [[CrossRef](#)]
2. Khadidos, A.O.; Khadidos, A.O.; Manoharan, H.; Alyoubi, K.H.; Alshareef, A.M.; Selvarajan, S. Integrating Industrial Appliances for Security Enhancement in Data Point Using SCADA Networks with Learning Algorithm. *Int. Trans. Electr. Energy Syst.* **2022**, *17*, 5235. [[CrossRef](#)]
3. Baker, T.; Asim, M.; MacDermott, Á.; Iqbal, F.; Kamoun, F.; Shah, B. A secure fog-based platform for SCADA-based IoT critical infrastructure. *Softw. Pract. Exp.* **2020**, *50*, 503–518. [[CrossRef](#)]
4. Sajid, A.; Abbas, H.; Saleem, K. Cloud-assisted IoT-based SCADA systems security: A review of the state of the art and future challenges. *IEEE Access* **2016**, *4*, 1375–1384. [[CrossRef](#)]
5. Katyara, S.; Shah, M.A.; Chowdhary, B.S.; Akhtar, F.; Lashari, G.A. Monitoring, control and energy management of smart grid system via WSN technology through SCADA applications. *Wirel. Pers. Commun.* **2019**, *106*, 1951–1968. [[CrossRef](#)]

6. Altaha, M.; Hong, S. Anomaly Detection for SCADA System Security Based on Unsupervised Learning and Function Codes Analysis in the DNP3 Protocol. *Electronics* **2022**, *11*, 2184. [[CrossRef](#)]
7. Ivanković, I.; Peharda, D.; Novosel, D.; Žubrinić-Kostović, K.; Kekelj, A. Smart grid substation equipment maintenance management functionality based on control center SCADA data. *J. Energy: Energ.* **2018**, *67*, 30–35. [[CrossRef](#)]
8. Shitharth, S.; Prasad, K.M.; Sangeetha, K.; Kshirsagar, P.R.; Babu, T.S.; Alhelou, H.H. An Enriched RPCO-BCNN Mechanisms for Attack Detection and Classification in SCADA Systems. *IEEE Access* **2021**, *9*, 156297–156312. [[CrossRef](#)]
9. Ramesh, A.; Satvik, D.; Nagasundari, S.; Honnavalli, P.B. Simulation of SCADA System for Advanced Metering Infrastructure in Smart Grid. In Proceedings of the International Conference on Smart Electronics and Communication (ICOSEC), Trichy, India, 10–12 September 2020; pp. 1071–1077.
10. Tsitaitse, T.J.; Cai, Y.; Ditta, A. Secure self-healing group key distribution scheme with constant storage for SCADA systems in smart grid. *Wirel. Pers. Commun.* **2018**, *101*, 1749–1763. [[CrossRef](#)]
11. Chan, A.C.-F.; Zhou, J. Toward Safe Integration of Legacy SCADA Systems in the Smart Grid. In Proceedings of the International Conference on Applied Cryptography and Network Security, Kyoto, Japan, 19–22 June 2022; pp. 338–357.
12. Gozuoglu, A.; Ozgonenel, O. Training Set Design for Smart Grids and Scada Co-Simulations. In Proceedings of the 7th International Istanbul Smart Grids and Cities Congress and Fair (ICSG), Istanbul, Turkiye, 25–26 April 2019; pp. 124–128.
13. Kermani, M.; Adelmanesh, B.; Shirdare, E.; Sima, C.A.; Carni, D.L.; Martirano, L. Intelligent energy management based on SCADA system in a real Microgrid for smart building applications. *Renew. Energy* **2021**, *171*, 1115–1127. [[CrossRef](#)]
14. Wertani, H.; Salem, J.B.; Lakhua, M. Analysis and supervision of a smart grid system with a systemic tool. *Electr. J.* **2020**, *33*, 106784. [[CrossRef](#)]
15. Gusrialdi, A.; Qu, Z. Smart grid security: Attacks and defenses. In *Smart Grid Control*; Springer: Berlin/Heidelberg, Germany, 2019; pp. 199–223.
16. Kim, Y.; Hakak, S.; Ghorbani, A. Smart grid security: Attacks and defence techniques. *IET Smart Grid* **2022**, 1–21. [[CrossRef](#)]
17. Sangeetha, K.; Shitharth, S.; Mohammed, G.B. Enhanced SCADA IDS Security by Using MSOM Hybrid Unsupervised Algorithm. *Int. J. Web Based Learn. Teach. Technol.* **2022**, *17*, 1–9. [[CrossRef](#)]
18. Kao, C.-Y.; Chueh, H.-E. A Vendor-Managed Inventory Mechanism Based on SCADA of Internet of Things Framework. *Electronics* **2022**, *11*, 881. [[CrossRef](#)]
19. Ghosh, U.; Chatterjee, P.; Shetty, S. Securing SDN-enabled smart power grids: SDN-enabled smart grid security. In *Research Anthology on Smart Grid and Microgrid Development*; IGI Global: Hershey, PA, USA, 2022; pp. 1028–1046.
20. Shitharth, S.; Satheesh, N.; Kumar, B.P.; Sangeetha, K. IDS Detection Based on Optimization Based on WI-CS and GNN Algorithm in SCADA Network. In *Architectural Wireless Networks Solutions and Security Issues, Lecture Notes in Network and Systems*; Springer: Singapore, 2021; Volume 196, pp. 247–266. [[CrossRef](#)]
21. Nafees, M.N.; Saxena, N.; Cardenas, A.; Grijalva, S.; Burnap, P. Smart Grid Cyber-Physical Situational Awareness of Complex Operational Technology Attacks: A Review. *ACM Comput. Surv.* **2022**, *74*, 5570. [[CrossRef](#)]
22. Reda, H.T.; Anwar, A.; Mahmood, A. Comprehensive survey and taxonomies of false data injection attacks in smart grids: Attack models, targets, and impacts. *Renew. Sustain. Energy Rev.* **2022**, *163*, 112423. [[CrossRef](#)]
23. Ding, J.; Qammar, A.; Zhang, Z.; Karim, A.; Ning, H. Cyber Threats to Smart Grids: Review, Taxonomy, Potential Solutions, and Future Directions. *Energies* **2022**, *15*, 6799. [[CrossRef](#)]
24. Khoei, T.T.; Slimane, H.O.; Kaabouch, N. A Comprehensive Survey on the Cyber-Security of Smart Grids: Cyber-Attacks, Detection, Countermeasure Techniques, and Future Directions. *arXiv* **2022**, arXiv:2207.07738.
25. Mahi-Al-rashid, A.; Hossain, F.; Anwar, A.; Azam, S. False Data Injection Attack Detection in Smart Grid Using Energy Consumption Forecasting. *Energies* **2022**, *15*, 4877. [[CrossRef](#)]
26. Martinelli, F.; Mercaldo, F.; Santone, A. A Method for Intrusion Detection in Smart Grid. *Procedia Comput. Sci.* **2022**, *207*, 327–334. [[CrossRef](#)]
27. Khadidos, A.O.; Manoharan, H.; Selvarajan, S.; Khadidos, A.O.; Alyoubi, K.H.; Yafoz, A. A Classy Multifacet Clustering and Fused Optimization Based Classification Methodologies for SCADA Security. *Energies* **2022**, *15*, 3624. [[CrossRef](#)]
28. Rajawat, A.S.; Rawat, R.; Barhanpurkar, K. Security Improvement Technique for Distributed Control System (DCS) and Supervisory Control-Data Acquisition (SCADA) Using Blockchain at Dark Web Platform. *Cyber Secur. Digit. Forensics* **2022**, *56*, 317–333.
29. Minh, Q.N.; Nguyen, V.-H.; Quy, V.K.; Ngoc, L.A.; Chehri, A.; Jeon, G. Edge Computing for IoT-Enabled Smart Grid: The Future of Energy. *Energies* **2022**, *15*, 6140. [[CrossRef](#)]
30. Hussain, S.Z.R.; Osman, A.; Moin, M.A.; Memon, J.A. IoT Enabled Real-time Energy Monitoring and Control System. In Proceedings of the 9th International Conference on Smart Grid (icSmartGrid), Setubal, Portugal, 29 June–1 July 2021; pp. 97–102.
31. Khalid, L.F.; Ameen, S.Y. Secure Iot integration in daily lives: A review. *J. Inf. Technol. Inform.* **2021**, *1*, 6–12.
32. Justindhas, Y.; Jeyanthi, P. Attack detection and prevention in IoT-SCADA networks using NK-classifier. *Soft Comput.* **2022**, *26*, 6811–6823. [[CrossRef](#)]
33. Lu, K.-C.; Liu, I.-H.; Liao, J.-W.; Wu, S.-C.; Liu, Z.-C.; Li, J.-S. Evaluation and Build to honeypot System about SCADA Security for Large-Scale IoT Devices. *J. Robot. Netw. Artif. Life* **2019**, *6*, 157–161. [[CrossRef](#)]
34. Huda, S.; Yearwood, J.; Hassan, M.M.; Almogren, A. Securing the operations in SCADA-IoT platform based industrial control system using ensemble of deep belief networks. *Appl. Soft Comput.* **2018**, *71*, 66–77. [[CrossRef](#)]

35. Hossain, M.T.; Badsha, S.; Shen, H. Porch: A novel consensus mechanism for blockchain-enabled future scada systems in smart grids and industry 4.0. In Proceedings of the 2020 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS), Vancouver, Canada, 9–12 September 2020; pp. 145–477.
36. Rivera, A.O.G.; Tosh, D.K.; Ghosh, U. Resilient sensor authentication in SCADA by integrating physical unclonable function and blockchain. *Clust. Comput.* **2022**, *25*, 1869–1883. [[CrossRef](#)]
37. Singh, V.K.; Ebrahim, H.; Govindarasu, M. Security evaluation of two intrusion detection systems in smart grid scada environment. In Proceedings of the 2018 North American Power Symposium (NAPS), Fargo, ND, USA, 9–11 September 2018; pp. 1–6.
38. Hasan, M.M.; Mouftah, H.T. Optimization of trust node assignment for securing routes in smart grid SCADA networks. *IEEE Syst. J.* **2018**, *13*, 1505–1513. [[CrossRef](#)]
39. Islam, S.N.; Baig, Z.; Zeadally, S. Physical layer security for the smart grid: Vulnerabilities, threats, and countermeasures. *IEEE Trans. Ind. Inform.* **2019**, *15*, 6522–6530. [[CrossRef](#)]
40. Masri, A.; Al-Jabi, M. Toward fault tolerant modelling for SCADA based electricity distribution networks, machine learning approach. *PeerJ Comput. Sci.* **2021**, *7*, e554. [[CrossRef](#)] [[PubMed](#)]
41. Abir, S.A.A.; Anwar, A.; Choi, J.; Kayes, A. Iot-enabled smart energy grid: Applications and challenges. *IEEE Access* **2021**, *9*, 50961–50981. [[CrossRef](#)]
42. Risco, A.B.; Salinas, R.I.G.; Guerrero, A.O.; Esparta, D.L.B. IoT-based SCADA System for Smart Grid Stability Monitoring using Machine Learning Algorithms. In Proceedings of the IEEE XXVIII International Conference on Electronics, Electrical Engineering and Computing (INTERCON), Online, 5–7 August 2021; pp. 1–4.
43. Radoglou-Grammatikis, P.I.; Sarigiannidis, P.G. Securing the smart grid: A comprehensive compilation of intrusion detection and prevention systems. *IEEE Access* **2019**, *7*, 46595–46620. [[CrossRef](#)]
44. Singh, V.K.; Govindarasu, M. Cyber Kill Chain-Based Hybrid Intrusion Detection System for Smart Grid. In *Wide Area Power Systems Stability, Protection, and Security*; Springer: Berlin/Heidelberg, Germany, 2021; pp. 571–599.
45. Holik, F.; Flå, L.H.; Jaatun, M.G.; Yayilgan, S.Y.; Foros, J. Threat modeling of a smart grid secondary substation. *Electronics* **2022**, *11*, 850. [[CrossRef](#)]
46. Devyatkin, D.A. Estimation of Vegetation Indices With Random Kernel Forests. *IEEE Access* **2023**, *11*, 29500–29509. [[CrossRef](#)]
47. Yang, L.; Moubayed, A.; Shami, A. MTH-IDS: A multitiered hybrid intrusion detection system for Internet of vehicles. *IEEE Internet Things J.* **2021**, *9*, 616–632. [[CrossRef](#)]