IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 22 January 2023, accepted 14 February 2023, date of publication 22 February 2023, date of current version 27 February 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3247193

RESEARCH ARTICLE

Cyber Security in Power Systems Using Meta-Heuristic and Deep Learning Algorithms

SAYAWU YAKUBU DIABA, (Graduate Student Member, IEEE), MIADREZA SHAFIE-KHAH, (Senior Member, IEEE), AND MOHAMMED ELMUSRATI, (Senior Member, IEEE)
School of Technology and Innovations, University of Vaasa, 65200 Vaasa, Finland
Corresponding author: Sayawu Yakubu Diaba (sdiaba@uwasa.fi)

ABSTRACT Supervisory Control and Data Acquisition system linked to Intelligent Electronic Devices over a communication network keeps an eye on smart grids' performance and safety. The lack of algorithms protecting the power system communication protocols makes them vulnerable to cyberattacks, which can result in a hacker introducing false data into the operational network. This can result in delayed attack detection, which might harm the infrastructure, cause financial loss, or even result in fatalities. Similarly, attackers may be able to feed the system with fake information to hoax the operator and the algorithm into making bad decisions at crucial moments. This paper attempts to identify and classify such cyber-attacks by using numerous deep learning algorithms and optimizing the data features with a metaheuristic algorithm. We proposed a Restricted Boltzmann Machine-based nature-inspired artificial root foraging optimization algorithm. Using a publicly available dataset produced in Mississippi State University's Oak Ridge National Laboratory, simulations are run on the Jupiter Notebook. Traditional supervised machine learning algorithms like Artificial Neural Networks, Convolutional Neural Networks, and Support Vector Machines are measured with the proposed algorithm to demonstrate the effectiveness of the algorithms. Simulations show that the proposed algorithm produced superior results, with an accuracy of 97.8% for binary classification, 95.6% for three-class classification, and 94.3% for multi-class classification. Thereby outperforming its counterpart algorithms in terms of accuracy, precision, recall, and f1 score.

INDEX TERMS Artificial neural network, artificial root foraging, cyber security, deep learning, machine learning, metaheuristic algorithm, restricted Boltzmann machines, supervisory control and data acquisition, smart grid.

I. INTRODUCTION

The extraordinarily intricate architectural design of the electrical power systems must be handled cautiously and with the best control strategy feasible to ensure both the protection of human life and the system's safety [1]. The system becomes more complex as the control process must run more quickly [2]. Automated devices are introduced to modern power systems to make operating them easier. The number of pieces of protective equipment that are part of the system is directly impacted by operational demand and consumer count [3]. Recent years have seen the development of automated systems for connected power module protection, automation, and control [4]. Protective device performances have somewhat improved as a result of developments in algorithms and power systems architecture [5], [6].

However, the likelihood of security problems increases as the number of connections to the power system modules intensifies. Hence the quality of control is expected to be in the higher range for modern power systems. The contemporary power systems are implemented with various International Electrotechnical Commission (IEC) standards [7], [8] and are generally operated with six significant components, as depicted in Figure 1. Generators, transformers, and safety

The associate editor coordinating the review of this manuscript and approving it for publication was Christos Anagnostopoulos.

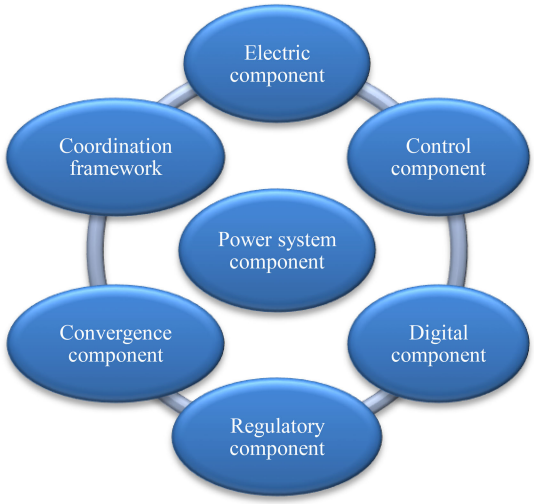

FIGURE 1. Component of the power system.

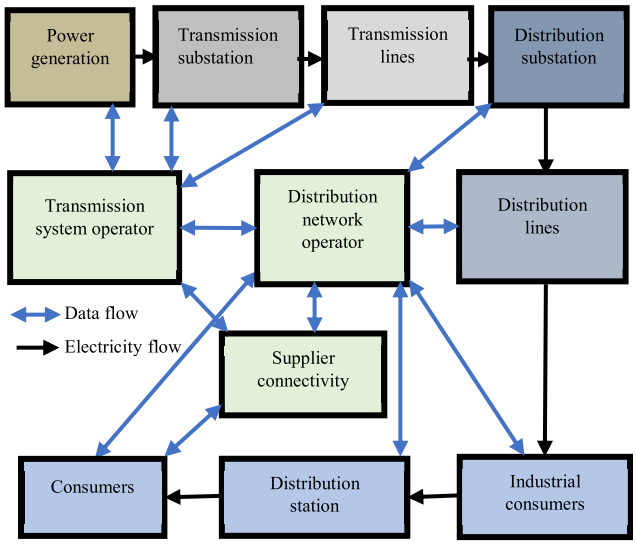

FIGURE 2. The architecture of a smart grid system.

equipment are all part of the power system's electrical components. These primary hardware ranges and ratings change depending on the loads connected to the network. The protection mechanisms built into the electrical system also differ depending on the linked equipment's location and nature [9]. The control components include the synchronization model and operational modules for transmitting the required signal to the digital modules used for the operation. The power system's information and communication devices, which transmit control signals between linked systems and components across wired or wireless networks, are represented by digital modules [10]. The convergence network regulates the power flow in the connected system by analyzing the load requirement and the power system state. The importance of the convergence networks increases when the power system is linked to Distributed Energy Resources (DERs) [11], [12]. The regulatory components ensure that the integration of power is constantly smooth and efficient.

In order to solve the problems with conventional digital components, which were designed to have certain limitations, smart grid power systems were developed. This is achieved by integrating distributed intelligence algorithms into the system. The distributed intelligence algorithms swiftly and efficiently support making decisions on the present digital components [13].

Smart grids, however, have more security concerns due to the distributed location of the control units. The architecture of the smart grid power systems includes the following four layers [14]. *Physical Layer:* It is identical to the layer found in every fundamental power system, which consists of a generation station, transmission lines, and a distribution unit. *Communication Layer:* The layer between the user and the service provider; this layer offers a network that allows for the discovery of the status of the power system's operation. *System Integration Layer:* This layer includes the computing and security infrastructure. It controls the data analytics process so that the control units can make several decisions. This is realized by importing a powerful algorithmic model. *Software Layer:* It enables the service provider to access the power consumption details from the user side. This layer provides information about the user and their nature to the system integration layer for future predictions.

Based on their general characteristics, the four kinds of cyber security problems for smart grid systems may be classified. They are issues with, *connectivity*, *trust*, *privacy*, and *software vulnerability* [15], [16].

Connectivity: Compared to other physical systems, the systems that make up the smart grid are more widely distributed. As a result, the smart grid power system's communication protocol necessitates constant operation and higher data transmission rates. The system transfers the data regularly; it poses numerous security concerns for the models. *Trust:* The smart grid systems are open to everyone. Some key equipment, specifically the Automated Meter Infrastructure (AMI) is situated in the user area. As a result, there is a greater chance that the system may be interfered with, and this risk is directly correlated with the user's level of trust, given that operational costs and other factors are involved. *Privacy:* The smart meters connected to the system contain the user's basic information, which is the most targeted device for intruders. *Software Vulnerabilities:* The smart grid systems are mostly monitored with Supervisory Control and Data Acquisition (SCADA) computer software. The SCADA system's modernization, standardization of communication protocols, and increasing interconnectivity have all contributed to a sharp rise in cyberattacks on the system over time, rendering it vulnerable to assault from anywhere around the globe [16]. Hence it is a must to protect the smart grids' SCADA systems from malicious cyber-attacks and malware disruption.

The aforementioned issues prompted the following goals for this study, which are as follows:

1) To employ a nature-inspired artificial root foraging optimization algorithm with a Restricted Boltzmann

Machine (RBM), to provide an enhanced algorithm that reliably detects and classifies attack intrusions in the smart grids' SCADA systems.
2) Enhanced adaptability: Nature-inspired optimization algorithms are designed to be highly adaptable, and can be modified or fine-tuned to meet the specific needs of a particular application. By combining an RBM with a nature-inspired algorithm, we seek to create a system that is highly adaptable and able to learn and adapt to new threats as they arise.
3) Increased efficiency: Nature-inspired optimization algorithms are typically more efficient than traditional optimization methods, as they are able to explore a more extensive search space more quickly. By combining an RBM with a nature-inspired algorithm, we seek to propose an algorithm that is able to analyze large amounts of data more quickly and efficiently, allowing for faster and more effective threat detection.
4) Reduced reliance on labelled data: RBMs are capable of performing unsupervised learning, which means they can learn from data that is not labelled or categorized. By combining an RBM with a nature-inspired algorithm, it is possible to create a system that can learn from a larger and more diverse dataset, which may be particularly useful in cases where labelled data is scarce or difficult to obtain.
5) To demonstrate the performance of the proposed algorithm's efficiency to other existing algorithms in terms of accuracy, precision, recall, and f1 score.

Section I captures the introduction of the paper. Section II contains background information on related studies and theoretical frameworks from the literature. The proposed algorithm is covered in Section III, while the simulation results are described in Section IV. Section V serves as the paper's conclusion.

II. RELATED STUDIES

The smart grid protection strategy uses local measures or external devices to build a smart grid protection system that is both effective and efficient. However, one of the key issues is the ability to connect physical and digital components to suit the configuration of the system. Measurement of data source authentication system was developed to analyze the data flow of a power system by extracting the features through an ensemble empirical mode decomposition model with the Fast Fourier Transform (FFT) technique. The experiment was conducted with a back-propagation neural network for data classification. An accuracy of 80.9% is achieved, and comparatively, it is better than the traditional long short-term memory (LSTM) model's accuracy of 77.8% [17]. To train the neural network algorithms, a sizable dataset is required. The performance of a neural network algorithm's prediction process is influenced by the amount of training data present in the network. The authors of [18] generated a power system dataset based on IEC 61850 Generic Object-Oriented Substation Event (GOOSE) communication for developing a reliable cybersecurity system.

The components of the power system are divided into numerous categories to monitor the load demand in different areas. Due to environmental conditions, the associated field will see variations in demand in particular. The system is more vulnerable to cyber threats since the scattered devices are connected through different channels [19]. The testbed-based power system quality analysis is one of the familiar methods widely used for observing the response of the power system in different scenarios. The test bed generates different kinds of cyber security issues to analyze and formulate a defending algorithm. An OMNeT++-based simulation technique was structured [20] to analyze the nature of cyberattacks in a bidirectional communication network. The model was integrated with Power Systems Computer Aided Design (PSCAD) for the power simulation.

The physical power systems are open to dynamic data injection attacks. An example is the ease with which the energy consumption values on smart meters could be altered. So, an interval state estimation method was developed to analyze the possible variations in the readings with respect to time. A kernel quantile regression is also incorporated in the work to estimate the uncertainties in renewable and electric load forecasting applications [21]. The cyberattack on the Internet of Things (IoT)-based smart grids may affect the costly and important systems that are connected to the power system. The hospital equipment and electric train are some of the costlier and most needed systems that always depend upon the quality of the power supply. Therefore, a blockchain-based technique was equipped with Hilbert-Huang transform to estimate power quality through the data collected from voltage and current sensors. The experimental work founds satisfied with the performance of the proposed model on false data injection attacks [22].

The false data injection process can also be observed by estimating the phasor measurements of the connected loads. A two-layer defense system was developed [23] to observe the change in the values of the power system. The defense resources are optimized in the work with a zero-sum static game algorithm. It is demonstrated that the proposed two-layer model is useful for examining false data injection attacks. Providing cybersecurity to DER, such as photovoltaic systems (PV), is one of the challenging tasks in power systems. To accomplish this, the connected syste's active and reactive power is analyzed along with its permitted voltage level for transmission. The syste's network topology is used to observe the power changes on each terminal. The change in the difference in various estimations makes the work to predict the attack output on its class [24]. A decision-making algorithm was outlined to estimate the cyberattacks in multi-microgrid systems. A fuzzy static Bayesian game model was utilized in the work for predicting the optimal security strategy, and a hybrid approach based on a fuzzy algorithm was used to reach a consensus [25].

A cybersecurity risk management system was developed to predict attacks in cyber-physical systems. The work analyzes the criticality of the assets in cyberattacks and their effect on the output of the system. The attack scenario, control, and threats are considered in the work for estimations [26]. A stochastic coupling strategy was designed to estimate the cascading process in cyber-physical systems. This has been performed by keeping two asymmetric subnetworks for increasing the accuracy of random and frequent cyberattacks. The experimental projection indicates a reduced estimation time for frequent attacks over the random models [27]. A deep reinforcement learning technique was structured to provide cybersecurity protection on distributed power systems. The performance of the system was experimented on the IEEE 13-bus model and the simulation results are not found satisfactory under the greedy attack conditions [28].

When responding to hostile attacks on industrial control systems, machine learning techniques are particularly accustomed. The results of an experiment using the random forest and J48 algorithms to identify intrusions in control systems were found to be good in forecasting cyber-attack behaviors [29]. A dimensionality reduction and statistical hypothesis techniques were merged to ensure cybersecurity on smart grids. A concept drift methodology was utilized in the work to observe the differences between the physical grid change and data manipulation. Experimental work was performed in the work with and without concept drift and found satisfactory with the concept drift technique [30]. A physics-informed spline learning technique was developed to detect anomalies in power electronic circuits. The experiment was found satisfactory even when trained with minimal data [31].

The review of the literature looks at the various strategies developed to address security issues in power systems. The majority of the systems, however, were created to recognize the introduction of false data into power systems. This was accomplished by analyzing the system's typical behavior to anticipate the system's abnormal response when fictitious data was injected. Because their analysis is feature-based, deep learning and machine learning algorithms are quite good at making these kinds of predictions. In the part that follows, a feature optimization technique based on a meta-heuristics algorithm is used to assess the effectiveness of deep learning-based algorithms to observe security vulnerabilities in SCADA systems for smart grids.

III. METHODOLOGY

The overall artificial root foraging, RMB architecture, and our variation are all introduced in this section.

A. OVERVIEW OF THE SYSTEM

The proposed model utilizes a nature-inspired artificial root foraging method for optimizing the information collected through the power systems sensor and data transmitters. Voltage and power sensors are used to detect the anomaly of the power system; the abnormality of the power system is observed and forwarded to the base station through an IoT network. The receiving station tabulates the collected information and projects the outcome as a database. The dataset creation process makes the base station verify all the collected information and separates the readings that came up with errors and missing information. The dataset creation process can be limited with respect to time as it may provide the amount of data to be stored in the database. Figure 3 represents the workflow of the proposed model.

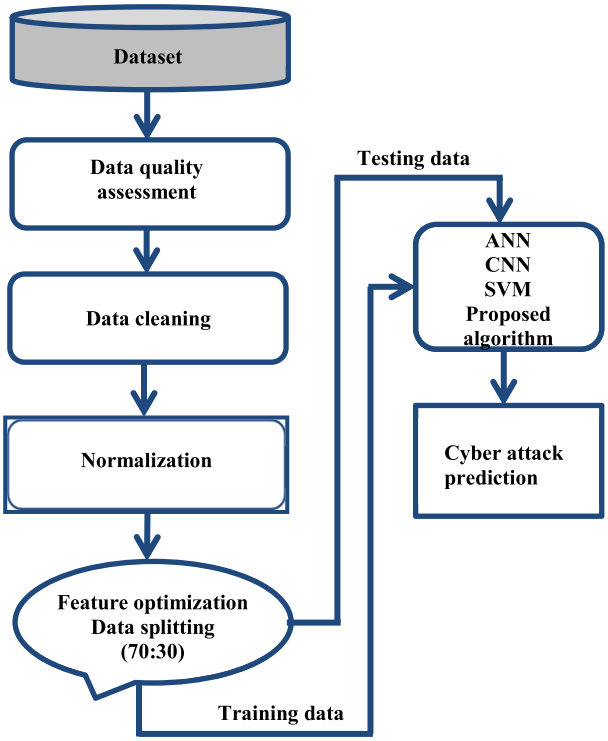

FIGURE 3. The workflow of the proposed model.

B. PREPROCESSING

Preprocessing is the fundamental technique for organizing the data gathered from the remote terminal unit (RTU) and other Intelligent Electronic Devices (IED) modules. In this step, the unstructured and unformatted data are organized to make the information reliable before it is used in the training process.

In general, the data can be segregated into two categories: numerical data and categorical data. The binary format is used for categorical data, and whole numbers or fractions are used for numerical data. Information about the power system is gathered in numerical form for the proposed task.

The quality of the feature extraction mostly depends on the caliber of the data used in the operation. Therefore, the paper makes use of the data translation process, data cleaning process, and data quality assessment process. As previously shown, the data quality assessment sends the available data to the data cleaning process while moving the missing data to the trash. The data cleaning procedure enables the removal of duplicate data and requires the manual insertion of data when it is discovered to be abnormal or missing.

C. ARTIFICIAL ROOT FORAGING OPTIMIZATION

1) CLASSICAL PLANT ROOT GROWTH MODEL

The biological root growth optimization algorithm served as the basis for designing the artificial root foraging optimization algorithm. A biological plant's primary root advances toward the ground, while its lateral roots spread outward like a branch from the main root. Similarly, the lateral roots are also permitted to develop numerous lateral roots in diverse directions. While the primary roots are not permitted to do so, the lateral roots are permitted to form in all directions with varying degrees of movement. Hence, the artificial root foraging algorithm is also constructed using the conventional optimization model that is used to predict the growth of plant roots. Root growth is thought to be hindered by the nature of the soil, and the main root movement and lateral root movement are thought to be the best solutions. The change in direction and length adjustments are regarded as the fine-tuning parameters for the problems [32]. The following factors are considered for ideal plant growth, and the same has been followed in the artificial model.

Factor 1: The spatial structure of the roots is heavily influenced by the auxin concentration in the plants. It allows the root to be automatically structured by observing the problem.

Factor 2: A single root apex advances in the same direction and can generate children's root apices.

Factor 3: Auxin availability causes the root system to develop a variety of lateral roots and branches.

Factor 4: Hydrotropism allows the tip of the main root and lateral roots to move in their respective directions along the trajectory.

2) AUXIN REGULATION

The auxin concentration is the primary parameter for developing a new branch count and movement operations [33]. Therefore, the nutrition availability of the soil is formulated as follows.

$$f_x = \frac{fitness_x - f_{low}}{f_{high} - f_{low}} \tag{1}$$

Mathematically, the auxin concentration is written as

$$A_x = \frac{f_x}{\sum_{y=1}^{s} f_x} \tag{2}$$

where the function value is $finess_x$, f_x is the normalization value of the root fitness, f_{high} and f_{low} represent the current root population count and s is the population size.

3) STRATEGY ON MAIN ROOT GROWTH

The growing probability of the main root is free from the probability of branch and re-growing factor. The movement of the main root depends upon the best individual operation formulated from its current position [34]. It is mathematically represented as

$$I_x^t = I_x^{t-1} + l.\varepsilon.\left(I_{lbest} - I_x^{t-1}\right) \tag{3}$$

here, I_x^t implies a new location, I_x^{t-1} represents the location of root x. Learning inertia takes l, ε is the uniform random coefficient between 0 and 1 and I_{lbest} stands for the best individual from the present location.

4) BRANCHING OPERATOR

The branching operator develops a new individual based on the root apex estimations. It is predicted by estimating the available auxin concentration over the threshold value included in the branch [35]. The number of individuals generated from the branch is calculated as

$$\begin{cases} branch\ individuals\ \mathrm{w}_x & \text{if } A_x > threshold\ value \\ stop\ branching & otherwise \end{cases} \tag{4}$$

Therefore, the numbers of newly generated apices are estimated from the following equatio

$$W_x = \varepsilon.A_x(B_{\max} - B_{\min}) + B_{\min} \tag{5}$$

ε is the uniform random coefficient between 0 and 1, A_x is the auxin concentration level at the root. B_{max} and B_{min} represent the branching count. The location for developing a new branch root is predicted from the primary root through Gaussian distribution $N(I_x^t, \sigma^2)$. The standard deviation is written as

$$\sigma = \left(\frac{x_{\max} - x}{x_{\max}}\right)^2 \times \left(\sigma_{ini} - \sigma_{fin}\right) + \sigma_{fin} \tag{6}$$

where x_{max} is the maximum iteration, i is the current iteration index, σ_{ini} is the initial standard deviation, and σ_{fin} is the final standard deviation.

5) LATERAL OR BRANCH ROOT GROWTH

The lateral roots are allowed to conduct a random search on every feeding state [36], [37]. The length and growing degree of the lateral roots are changed between each other, and that can be mathematically projected as

$$I_x^t = I_x^{t-1} + \varepsilon\,(l_{\max} D_i * \phi) \tag{7}$$

$$\phi = \frac{\delta_i}{\sqrt{\delta_i^T \times \delta_i}} \tag{8}$$

where l_{max} stands for the maximum length of the lateral root, D_i is the dimension growth direction of the lateral root i, and ϕ stands for the growth angle formulated with a random vector δ_i.

6) DEAD ROOT GROWTH SHRINKABLE

The growing process might not be supported by the roots if they were unable to absorb nutrients. The auxin distribution evaluates the likelihood that the lateral roots will grow and, if they do not, they are removed from the main root.

D. RESTRICTED BOLTZMANN MACHINES

The RBM technique was primarily created for regression, feature learning, and dimensionality reduction applications. It is a subset of the family of energy-based models, where

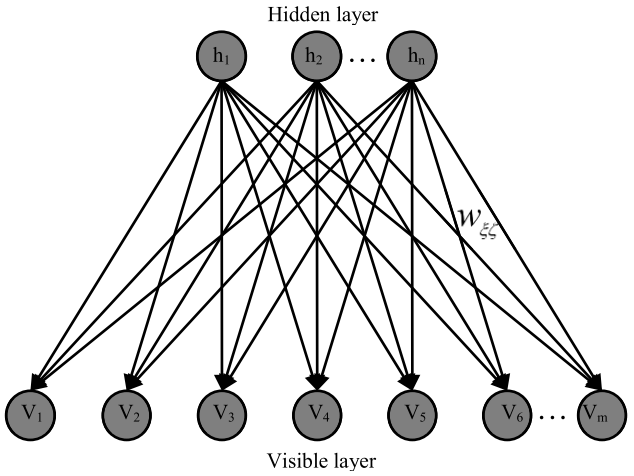

FIGURE 4. The architecture of the RBM.

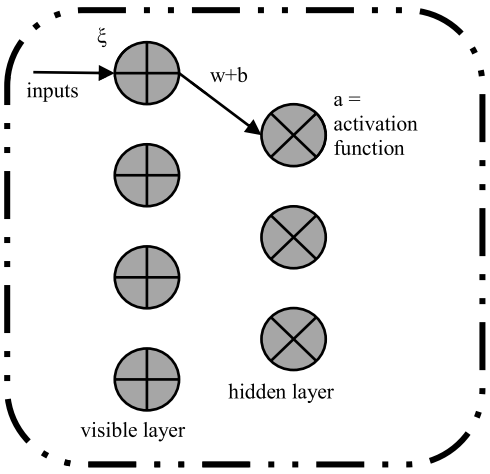

FIGURE 5. The input path of an RBM.

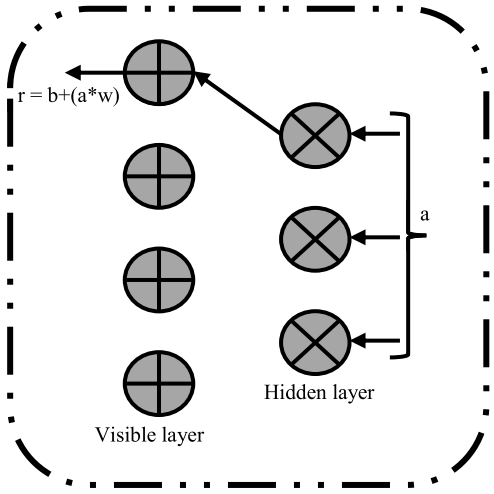

FIGURE 6. The reconstruction of RBM.

each configuration of the relevant variables corresponds to a training-relevant finite scalar energy value. The RBM algorithms are typically shallow and only use two levels of network connection [38]. As a result of their simplicity, RBMs are widely used in a variety of applications. The primary layer of the RBM is represented as the visible layer, and the second layer is mentioned as the hidden layer. The number of neural nodes included in the layer varies with respect to the count of inputs made to the approach and the interconnection between the nodes makes a neurological connection like a human brain. The RBM connections are very special, and there the intra-connections are restricted. The node analyzes the input received by the, computes it, and decides whether to permit it or not for neighbor node connection [39]. The bipartite interactional graph of the RBM is depicted in Figure 4.

The feature that the visible layer node collects is denoted by the letter ξ and it is passed to the hidden layer by multiplying the weighted value w and adding the bias b [40]. The following expression can be used to describe the outcome of this operation as an activation function of the supplied input.

$$f((\xi \times w) + b) = a \tag{9}$$

where f represents the activation function, ξ is the input, and w stands for the weights. The bias is represented by b and a is for the activation function.

The hidden layer activations are considered as input in the reconstruction step, where the input is given to the hidden layer. Same as the input path, the reconstruction model also operates the input with the same multiplication factor. Hence the output gives a value to the original input. Figures 5 and 6 indicate the input path of an RBM and the reconstruction model of the RBM, respectively.

Generally, the values of the weights included are assumed randomly, and presumably, there will always be a huge deviation between the input and output of the RBM. So, the weights are modified continuously to reduce the error observations in estimating the reconstruction r value. The nodes are designed to take the low-level feature present in all the attributes available in the dataset. This paper considers that the RBM has a total of n visible neurons as $v = v_1, v_2, \ldots, v_n$ and total hidden neurons m has hidden neurons as $h = h_1, h_2, \ldots, h_m$. The model uses binary values since the study examines the binary problem (natural or attack) of the existence of anomalies. the random variable takes the values $(v, h) \in .\{0, 1\}^{m+n}$. Thus, the probability distribution according to [41] can be written as

$$P(v, h) = \frac{1}{z} e^{-E(v,h)} \tag{10}$$

Z is the partition function. An energy function E(v,h) of the model can be defined as [42] and [43]

$$E(v, h) = -\sum_{\xi=1}^{n}\sum_{\zeta=1}^{m} w_{\xi\zeta} h_m v_n - \sum_{\xi=1}^{n} g_n v_n - \sum_{\xi=1}^{m} q_m h_m \tag{11}$$

TABLE 1. Description of the employed dataset.

Data class	Data details	Event count out
Binary classification	Natural event	9
	Attack event	28
Three-Classification	No event	1
	Natural event	8
Multiclass classification	Attack event	28
	All class	37

Equation (11) can be re-written as

$$E(\mathbf{v}, \mathbf{h}) = \mathbf{g}^T \mathrm{v} - \mathrm{q}^T \mathbf{h} - \mathbf{v}^T \mathbf{W}\mathbf{h} \tag{12}$$

where the considered features for the training process of ξ is $\xi \in \{1, 2, \ldots, \mathrm{n}\}$ and $\zeta \in \{1, 2, \ldots, m\}$. The weight is denoted by $\mathrm{w}_{\xi\zeta}$, g_n is the n^{th} feature of the ξ^{th} input of the v^{th} visible neurons. Similarly, q_m is the m^{th} feature of the ζ^{th} input of the h^{th} hidden neuron. Due to the RBM's bipartite nature, there is no connection between a hidden neuron and a hidden neuron, just as there is no connection between a visible neuron and a visible neuron. The model for conditional independence is described as

$$p(\mathbf{v}, \mathbf{h}) = \Pi_{\zeta=1}^{m} p(v_\zeta | \mathbf{h}) \tag{13}$$

$$p(\mathbf{v}, \mathbf{h}) = \Pi_{\xi=1}^{n} p(\mathbf{v}_\xi | \mathbf{h}) \tag{14}$$

E. DATA DESCRIPTION

This paper utilizes the power system attack detection dataset developed by the Oak Ridge national laboratory of Mississippi State University [44]. The dataset is separated into three types, binary class, three class, and multi-class. It is created from a single dataset consisting of 15 sets of information from 37 types of power system events. Except for the multi-class dataset, the details are in CSV format. The content of the dataset is shown in Table 1.

Figure 7 shows a three-bus two-line transmission system modified from the IEEE four-bus three-generator system, it explores the architectural view of the test framework used for the analysis. Despite being a very modest system, it embodies the core of the broader power system and is simple enough to be understood in its entirety. The classifier suggested in this work would be used multiple times to monitor different parts of a power system. The framework merges two generator models consisting of four IEDs, specifically, relays (R_1 to R_4) for providing a switching operation to the circuit breakers (Bk_1 to Bk_4). Each circuit breaker is connected with a separate IED [44]. Therefore, it trips off the breaker unit when a real or fake fault is detected in the circuit. The IEDs are not equipped with any algorithm so far for analyzing the nature of the fault. Thus, this kind of model requires a manual operation to re-enable the circuit from its faulty condition. The major type of faults and attacks that can happen in a power system model is as follows [45].

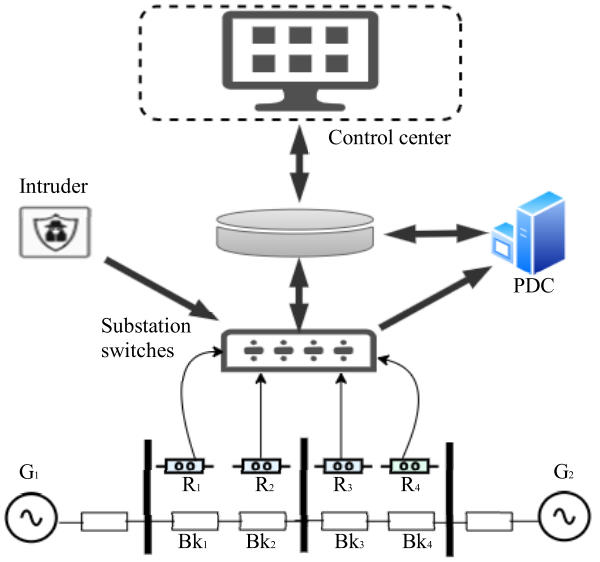

FIGURE 7. Overview of the power system framework.

1) FAULTS

a: SHORT CIRCUIT

These kinds of faults may happen in a power system owing to natural and manual errors at any location. The location of the fault can be identified by observing the current and voltage changes in the circuit. A short circuit fault in a power system occurs when there is an abnormal connection between two points in the electrical circuit that are not intended to be connected. This can cause a sudden and large increase in the flow of electrical current, which can damage or destroy electrical equipment and pose a risk of injury to personnel. Short circuit faults can be caused by a variety of factors, including damaged or faulty electrical components, loose connections, and the presence of foreign objects or debris in the electrical circuit. They can also be caused by natural disasters such as lightning strikes or earthquakes [46].

When a short circuit fault occurs, the electrical system is designed to automatically detect the fault and interrupt the flow of current to prevent damage to the equipment and protect personnel. This is typically done by using protective devices such as circuit breakers, fuses, and relays, which are designed to detect abnormal electrical conditions and interrupt the flow of current. It is important to promptly address short circuit faults in order to minimize the risk of damage to the electrical system and ensure the safe and reliable operation of the power system. This may involve identifying and repairing the root cause of the fault, as well as testing and inspecting the affected equipment to ensure it is safe to return to service [46].

b: LINE MAINTENANCE

For the duration of the maintenance period, the relay modules connected to the power system model are disconnected from the circuit. These kinds of errors are intentional and are

simple to fix. Line maintenance in power systems refers to the activities that are performed to ensure that transmission and distribution lines are operating safely and efficiently. These activities can include inspections, repairs, and upgrades of transmission and distribution lines, as well as the associated equipment such as transformers, switches, and other electrical components.

Line maintenance is an essential part of the overall operation and maintenance of a power system, as it helps to ensure the reliability and safety of the electrical grid. Line maintenance activities can be performed on both overhead and underground transmission and distribution lines, and may involve a range of tasks, such as: Inspecting and testing electrical equipment to identify any potential issues or problems. Replacing damaged or worn-out components. Upgrading equipment to improve performance or increase capacity. Cleaning and maintaining transmission and distribution lines to remove debris and vegetation that could cause problems. Performing preventive maintenance activities to prevent potential problems from occurring. Line maintenance is typically carried out by trained and certified professionals with the necessary knowledge and skills to work safely on high-voltage electrical equipment. In some cases, specialized equipment such as bucket trucks or aerial lifts may be used to access transmission and distribution lines for maintenance activities [46].

2) ATTACKS

a: DATA INJECTION ATTACK

A data injection attack in power systems, also known as a manipulation attack, is a type of cyber-attack that involves injecting false or malicious data into the control systems of a power grid. The goal of this type of attack is to disrupt the normal operation of the power grid and potentially cause damage to the system.

Data injection attacks can take many different forms, but they generally involve the attacker injecting false or malicious data into the control systems of the power grid to mislead the operators or cause the system to malfunction. For example, an attacker might inject false data into the control systems of a power grid to indicate that there is a fault in the system, when in fact there is not. This could lead to the operators taking inappropriate or unnecessary actions to respond to the false fault, which could potentially cause damage to the power grid.

Data injection attacks can be difficult to detect, as they often involve the injection of small amounts of false data into the control systems of the power grid. They can also be difficult to prevent, as they require a high level of access to the control systems of the power grid. Power grid operators need to implement robust cybersecurity measures to protect against these types of attacks [45].

b: RELAY SETTINGS CHANGE ATTACK

A relay settings change attack in power systems is a type of cyber-attack that involves altering the settings of protective relays in the power grid. Protective relays are electrical devices that are used to automatically detect and respond to abnormal conditions in the power grid, such as short circuits or over currents. They are an essential component of the power grid's protection system, as they help to ensure the stability and reliability of the grid [45].

In a relay settings change attack, an attacker may attempt to manipulate the settings of protective relays to disrupt the regular operation of the power grid. For example, the attacker may change the settings of the relays so that they do not respond to certain types of fault conditions, or so that they respond in a way that is not appropriate for the specific fault condition. This can lead to widespread power outages and other disruptions in the power grid [45].

Relay settings change attacks can be challenging to detect, as they often involve subtle changes to the settings of the protective relays. They can also be difficult to prevent, as they require a high level of access to the power grid's control systems. Power grid operators need to implement robust cybersecurity measures to protect against these types of attacks [45].

c: TRIPPING COMMAND INJECTION ATTACK

It is a command kind of attack that makes the relay open the circuit with a command received from a remote location. A tripping command injection attack in power systems is a type of cyber-attack that involves injecting false or malicious commands into the control systems of a power grid in order to disrupt the normal operation of the system. The goal of this type of attack is to cause equipment to trip or shut down, potentially leading to widespread power outages and other disruptions in the power grid [45].

In a tripping command injection attack, an attacker may inject false or malicious commands into the control systems of the power grid in an effort to cause equipment to trip or shut down. For example, the attacker might inject a command to trip a circuit breaker or shut down a generator. This could lead to widespread power outages and other disruptions in the power grid. Tripping command injection attacks can be challenging to detect, as they often involve the injection of small amounts of false or malicious data into the control systems of the power grid. They can also be difficult to prevent, as they require a high level of access to the control systems of the power grid. To defend against these kinds of attacks, power grid operators must install strong cybersecurity safeguards [45].

F. DEEP LEARNING PERFORMANCE EVALUATION METRICS

Deep learning is a type of machine learning that uses deep neural networks to learn and make predictions or decisions. The performance metrics used to evaluate the effectiveness of a deep learning model are similar to those used for other types of machine learning models. Because of the task under study and the kind of model being employed, we concentrate only on the four threshold parameters that the classification problem's performance metric is defined by

TABLE 2. Confusion matrix for a binary classifier.

	Actual true	Actual false
Predicted true	True positive	False positive
Predicted false	False positive	True Negative

Accuracy: This is a common metric for classification tasks, and it is defined as the number of correct predictions made by the model divided by the total number of predictions. Mathematically represented as [56]

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \tag{15}$$

Precision: This metric is used to measure the precision of a classifier, and it is defined as the number of true positive predictions made by the model divided by the total number of positive predictions [56].

$$Precision = \frac{TP}{TP + FP} \tag{16}$$

Recall: This metric is used to measure the recall of a classifier, and it is defined as the number of true positive predictions made by the model divided by the number of positive cases in the dataset [56].

$$Recall = \frac{TP}{TP + FN} \tag{17}$$

F1 score: This is a metric that combines precision and recall, and it is defined as the harmonic mean of precision and recall [56].

$$F1score = \frac{2\,(Presicion \times Recall)}{Presicion + Recall} \tag{18}$$

Equations (15), (16), (17), and (18) are derived using the confusion matrix. The confusion matrix is a table that is used to evaluate the performance of a classifier, and it is often used in conjunction with various performance metrics to provide a more complete picture of the classifier's effectiveness.

IV. EXPERIMENTAL ANALYSIS

The experiment was performed in a Jupyter notebook on a 16GB RAM Intel 7 processor system. The proposed RF-RBM technique was tested against conventional CNN, ANN, and SVM algorithms because those were found to be successful models in several intrusion detection studies [37], [49]. In this, the SVM is a machine learning-based technique, whereas CNN and ANN are deep learning-based techniques. We utilize the hyperparameters given in Table 3 for the simulations, and we classify the network intrusion through different algorithms.

One of the most used neural network algorithms, CNN, can provide a higher accuracy rate when the training data samples are plentiful. However, because CNN learns characteristics from a large dataset, preprocessing of the training data is minimal. Three layers make up a conventional CNN: a convolution layer, a pooling layer, and a fully connected layer. The convolution layer is set up to separate the kernel's learnable parameters from the input data. The kernel clarifies to the layer the kind of information that is available [47] and [49]. Data is forwarded by the kernel to different neurons in the pooling layer, which lowers the spatial complexity of the retrieved information in the convolution layer. All of the CNN's neurons are interconnected in the fully connected layer with their biases toward comprehending the data that has been gathered [50].

TABLE 3. Hyperparameter settings.

Model parameter	Total
Visible node	128
Hidden neurons for CNN, ANN	2
Batch size	128
Epoch	1000
Activation functions	ReLU, Sigmoid
Learning rate	0.1

The ANN is one of the successful models that can mimic the nature of the human brain. All neurons are interconnected between them as different layers, just like in a human brain. The input, output, and hidden layers are the principal layers of an ANN, and the number of hidden layers can be increased depending on the demands of a situation. The hidden layer is used to extract different features and patterns from the input data, while the input layer is used to provide diverse information to the neural network design. Additionally, the hidden layer applies a bias value to the gathered characteristics to do an efficient calculation [48], [51].

The SVM is a supervised machine learning technique that handles the classification problem by drawing the best distinction between the various classes. The optimal boundary line can be determined by locating an extreme vector point in the available dimension space. SVMs are frequently used for binary classification and can be applied to multiple classifications by generating a non-linear function that generates new variables as the kernel [49], [52].

In machine learning, feature selection is a crucial operation [53]. We opted for our algorithm because the meta-heuristic nature-inspired algorithm can provide a strong foundation for identifying patterns and anomalies in the data, by using the input and output without needing gradient information [54]. The RBM can be used to learn and recognize more complex features that may be indicative of an intrusion. Together, these two approaches can provide a powerful tool for detecting and responding to threats in smart grid systems.

A. RESULTS

The 15 sets of information from 37 types of power system events were combined into a single dataset. For the experiments in this paper, 70% of the data is used for training, and 30% is used for testing. Using the hyperparameter settings in Table 3, the three distinct experiments are conducted.

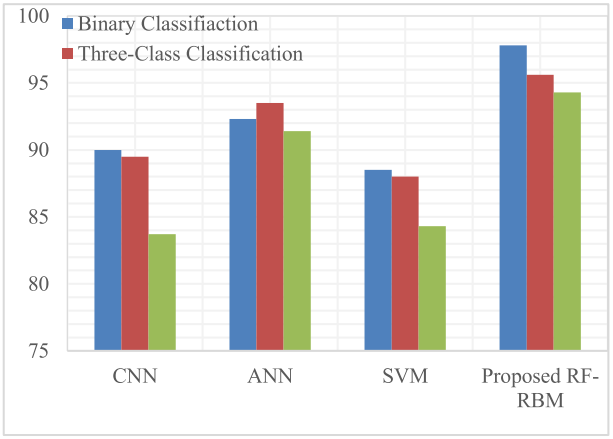

FIGURE 8. The accuracy of the conducted experiments.

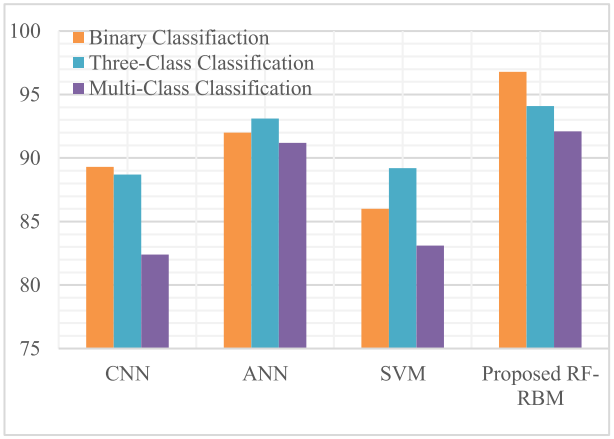

FIGURE 10. The recall score of the conducted experiments.

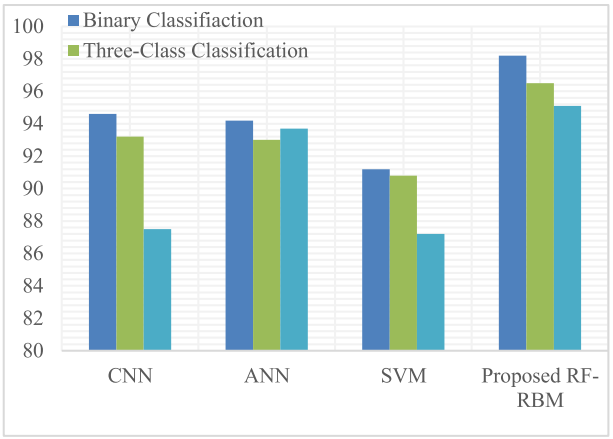

FIGURE 9. The precision of the conducted experiments.

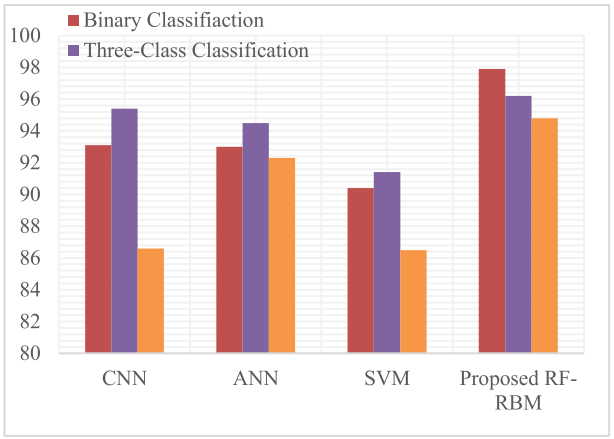

FIGURE 11. The f1 score of the conducted experiments.

Figures 8, 9, 10, and 11 show the experiment's findings, demonstrating the accuracy, precision, recall, and f1 score of the verified algorithms in more detail. Figure 8 depicts the performance of the verified algorithms measured in terms of accuracy across all three experiments. The results show that the accuracy of the algorithms in the binary classification experiment consistently outperformed the other two experiments, with the exception of the ANN algorithm in the three-class classification experiment. In this case, the ANN algorithm performed slightly better in the three-class classification experiment compared to the binary classification experiment and the multi-class classification.

According to the results depicted in Figure 9, the precision of the multi-class classification experiment improved considering the three-class classification experiment, but this improvement was only observed for the ANN algorithm. These results suggest that the ANN algorithm may be more effective at achieving higher precision in multi-class classification tasks. However, the performance of the multi-class classification experiment was subpar when utilizing the CNN and SVM algorithms.

As illustrated in Figure 10, the recall of the experiment revealed an improvement in the three-class classification for both the ANN and SVM algorithms compared to the other two experiments. The performance of the binary classification experiment is higher for the proposed RF-RBM because the sample counts on either one class in the binary classification are very large. However, the irregular distribution of the three-class classification experiment is a result of the significant drop in data for the no-event class, leading to a decrease in performance.

The results of the f1 score estimations shown in Figure 11 indicate that the outcomes of the three-class classification are better in all the experiments, except for the proposed RF-RBM. The proposed algorithm outperforms the other three algorithms in three-class classification and multi-class classification, but it extremely outperforms them in binary classification.

Furthermore, we compare the results of this paper to the result of comparable papers that employed the same dataset. The comparison using the binary classification dataset is shown in Table 4, and the three-class classification dataset is shown in Table 5.

TABLE 4. Comparison of models results with binary classification dataset.

Model	Accuracy	Precision	Recall	F1-score	Ref
SVM-AC	84.4	86	84.9	-	[52]
Linear SVM	76.2	76.2	75.4	73.3	[57]
GA-Linear SVM	87.0	85.2	86.6	80.1	[57]
RBF SVM	81	80.1	82.5	76	[57]
GA-RBF SVM	91.9	93.7	95	87	[57]
MLPNN	78.8	78.5	80.2	75.3	[57]
GA-MLPNN	86.4	87.2	85.7	84.9	[57]
RF	81.9	82.6	83.9	77.9	[57]
GA-RF	88.2	87.4	89.1	86.1	[57]
JRipper	-	85.0	70.0	-	[47]
PSO SVM	89.5	90.2	80.7	-	[51]
AdaBoost + JRipper	-	94	89	-	[47]
Proposed RF-RBM	**97.8**	**98.2**	**96.8**	**97.9**	

TABLE 5. Comparison of models results with three-class classification dataset.

Model	Accuracy	Precision	Recall	F1 score	Ref
SVM-ACO	78	80.5	77.4	NA	[56]
GA-RBF SVM	90.9	89.9	91.3	85.8	[57]
PSO-SVM	85.7	86.5	83.1	NA	[58]
AdaBoost + JRipper	99	95	**100**	NA	[47]
Proposed RF - RBM	**94.3**	**95.1**	92.1	**90.3**	

V. CONCLUSION

In this study, we present a nature-inspired restricted Boltzmann machine algorithm to detect and classify the types of attacks in the smart grids' SCADA systems. The fundamental notion is that the artificial root foraging optimization method is designed on the biological root growth optimization algorithm. To demonstrate the optimization capability, the dataset features were fine-tuned using the artificial root foraging algorithm before the neural network algorithm. The proposed RF-RBM algorithm is compared to three cutting-edge neural network algorithms in the experimental study, which was conducted in three categories: binary classification, three-class classification, and multi-class classification. The outcomes of the experiments demonstrate that the proposed algorithm RF-RBM is best suited for cyberattack detection and classification in SCADA systems for smart grids. This is shown by the excellent accuracy, sufficient precision, respectable recall, and a high f1 score demonstrated by the proposed algorithm.

REFERENCES

[1] A. N. Milioudis, G. T. Andreou, and D. P. Labridis, "Enhanced protection scheme for smart grids using power line communications techniques—Part I: Detection of high impedance fault occurrence," *IEEE Trans. Smart Grid*, vol. 3, no. 4, pp. 1621–1630, Dec. 2012, doi: 10.1109/TSG.2012.2208987.

[2] C. P. Vineetha and C. A. Babu, "Smart grid challenges, issues and solutions," in *Proc. Int. Conf. Intell. Green Building Smart Grid (IGBSG)*, Apr. 2014, pp. 1–4, doi: 10.1109/IGBSG.2014.6835208.

[3] M. Zhengyou, "Study on the application of advanced power electronics in smart grid," in *Proc. 6th Int. Conf. Future Gener. Commun. Technol. (FGCT)*, Aug. 2017, pp. 1–4, doi: 10.1109/FGCT.2017.8103739.

[4] M. Cao, K. Cao, B. Wu, and M. Tan, "Intelligent condition monitoring and management for power transmission and distribution equipments in Yunnan power grid," in *Proc. Int. Conf. High Voltage Eng. Appl.*, Sep. 2012, pp. 8–11, doi: 10.1109/ICHVE.2012.6357153.

[5] J. Shair, H. Li, J. Hu, and X. Xie, "Power system stability issues, classifications and research prospects in the context of high-penetration of renewables and power electronics," *Renew. Sustain. Energy Rev.*, vol. 145, Jul. 2021, Art. no. 111111.

[6] K. Ullah, A. Basit, Z. Ullah, S. Aslam, and H. Herodotou, "Automatic generation control strategies in conventional and modern power systems: A comprehensive overview," *Energies*, vol. 14, no. 9, p. 2376, Apr. 2021.

[7] Y. Himri, S. M. Muyeen, F. H. Malik, S. Himri, K. A. bin Ahmad, N. K. Merzouk, and M. Merzouk, "A review on applications of the standard series IEC 61850 in smart grid applications," in *Cyberphysical Smart Cities Infrastructures: Optimal Operation and Intelligent Decision Making*. 2022, pp. 197–253.

[8] H. F. Habib, N. Fawzy, and S. Brahma, "Performance testing and assessment of protection scheme using real-time hardware-in-the-loop and IEC 61850 standard," *IEEE Trans. Ind. Appl.*, vol. 57, no. 5, pp. 4569–4578, Sep. 2021.

[9] A. Draz, M. M. Elkholy, and A. A. El-Fergany, "Soft computing methods for attaining the protective device coordination including renewable energies: Review and prospective," *Arch. Comput. Methods Eng.*, vol. 28, no. 7, pp. 4383–4404, Dec. 2021.

[10] Y.-F. Li and C. Jia, "An overview of the reliability metrics for power grids and telecommunication networks," *Frontiers Eng. Manage.*, vol. 8, no. 4, pp. 531–544, Dec. 2021.

[11] Y. Shi, Y. Li, Y. Zhou, R. Xu, D. Feng, Z. Yan, and C. Fang, "Optimal scheduling for power system peak load regulation considering short-time startup and shutdown operations of thermal power unit," *Int. J. Elect. Power Energy Syst.*, vol. 131, Oct. 2021, p. 107012.

[12] A. Oshnoei, M. Kheradmandi, S. M. Muyeen, and N. D. Hatziargyriou, "Disturbance observer and tube-based model predictive controlled electric vehicles for frequency regulation of an isolated power grid," *IEEE Trans. Smart Grid*, vol. 12, no. 5, pp. 4351–4362, Sep. 2021.

[13] D. K. Panda and S. Das, "Smart grid architecture model for control, optimization and data analytics of future power networks with more renewable energy," *J. Cleaner Prod.*, vol. 301, Jun. 2021, Art. no. 126877.

[14] A. Ghasempour, "Internet of Things in smart grid: Architecture, applications, services, key technologies, and challenges," *Inventions*, vol. 4, no. 1, p. 22, Mar. 2019.

[15] M. Z. Gunduz and R. Das, "Cyber-security on smart grid: Threats and potential solutions," *Comput. Netw.*, vol. 169, Mar. 2020, Art. no. 107094.

[16] M. Srivastava, "An overview of cyber-security issues in smart grid," in *Computer Networks, Big Data and IoT* (Lecture Notes on Data Engineering and Communications Technologies), vol. 66, A. Pandian, X. Fernando, and S. M. S. Islam, Eds. Singapore: Springer, 2021, pp. 643–650, doi: 10.1007/978-981-16-0965-7_49.

[17] S. Liu, S. You, H. Yin, Z. Lin, Y. Liu, W. Yao, and L. Sundaresh, "Model-free data authentication for cyber security in power systems," *IEEE Trans. Smart Grid*, vol. 11, no. 5, pp. 4565–4568, Sep. 2020.

[18] P. P. Biswas, H. C. Tan, Q. Zhu, Y. Li, D. Mashima, and B. Chen, "A synthesized dataset for cybersecurity study of IEC 61850 based substation," in *Proc. IEEE Int. Conf. Commun., Control, Comput. Technol. Smart Grids (SmartGridComm)*, Oct. 2019, pp. 1–7.

[19] C. Mu, T. Ding, M. Qu, Q. Zhou, F. Li, and M. Shahidehpour, "Decentralized optimization operation for the multiple integrated energy systems with energy cascade utilization," *Appl. Energy*, vol. 280, Dec. 2020, Art. no. 115989.

[20] E. Hammad, M. Ezeme, and A. Farraj, "Implementation and development of an offline co-simulation testbed for studies of power systems cyber security and control verification," *Int. J. Electr. Power Energy Syst.*, vol. 104, pp. 817–826, Jan. 2019.

[21] H. Wang, J. Ruan, B. Zhou, C. Li, Q. Wu, M. Q. Raza, and G.-Z. Cao, "Dynamic data injection attack detection of cyber physical power systems with uncertainties," *IEEE Trans. Ind. Informat.*, vol. 15, no. 10, pp. 5505–5518, Oct. 2019.

[22] M. Ghiasi, M. Dehghani, T. Niknam, A. Kavousi-Fard, P. Siano, and H. H. Alhelou, "Cyber-attack detection and cyber-security enhancement in smart DC-microgrid based on blockchain technology and Hilbert Huang transform," *IEEE Access*, vol. 9, pp. 29429–29440, 2021.

[23] Q. Wang, W. Tai, Y. Tang, M. Ni, and S. You, "A two-layer game theoretical attack-defense model for a false data injection attack against power systems," *Int. J. Electr. Power Energy Syst.*, vol. 104, pp. 169–177, Jan. 2019.

[24] A. Khan, M. Hosseinzadehtaher, M. B. Shadmand, D. Saleem, and H. Abu-Rub, "Intrusion detection for cybersecurity of power electronics dominated grids: Inverters PQ set-points manipulation," in *Proc. IEEE CyberPELS (CyberPELS)*, Oct. 2020, pp. 1–8.

[25] B. Hu, C. Zhou, Y.-C. Tian, X. Hu, and X. Junping, "Decentralized consensus decision-making for cybersecurity protection in multimicrogrid systems," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 51, no. 4, pp. 2187–2198, Apr. 2021.

[26] H. Kure, S. Islam, and M. Razzaque, "An integrated cyber security risk management approach for a cyber-physical system," *Appl. Sci.*, vol. 8, no. 6, p. 898, May 2018.

[27] R. Lai, X. Qiu, and J. Wu, "Robustness of asymmetric cyber-physical power systems against cyber attacks," *IEEE Access*, vol. 7, pp. 61342–61352, 2019.

[28] T. Bailey, J. Johnson, and D. Levin, "Deep reinforcement learning for online distribution power system cybersecurity protection," in *Proc. IEEE Int. Conf. Commun., Control, Comput. Technol. Smart Grids (SmartGridComm)*, Oct. 2021, pp. 227–232.

[29] E. Anthi, L. Williams, M. Rhode, P. Burnap, and A. Wedgbury, "Adversarial attacks on machine learning cybersecurity defences in industrial control systems," *J. Inf. Secur. Appl.*, vol. 58, May 2021, Art. no. 102717.

[30] M. Mohammadpourfard, Y. Weng, M. Pechenizkiy, M. Tajdinian, and B. Mohammadi-Ivatloo, "Ensuring cybersecurity of smart grid against data integrity attacks under concept drift," *Int. J. Electr. Power Energy Syst.*, vol. 119, Jul. 2020, Art. no. 105947.

[31] V. S. B. Kurukuru, M. A. Khan, and S. Sahoo, "Cybersecurity in power electronics using minimal data—A physics-informed spline learning approach," *IEEE Trans. Power Electron.*, vol. 37, no. 11, pp. 12938–12943, Nov. 2022.

[32] Y. Liu, J. Liu, L. Ma, and L. Tian, "Artificial root foraging optimizer algorithm with hybrid strategies," *Saudi J. Biol. Sci.*, vol. 24, no. 2, pp. 268–275, Feb. 2017.

[33] Y. Liu, J. Liu, L. Tian, and L. Ma, "Hybrid artificial root foraging optimizer based multilevel threshold for image segmentation," *Comput. Intell. Neurosci.*, vol. 2016, pp. 1–16, 2016.

[34] X. He, H. Chen, B. Niu, and J. Wang, "Root growth optimizer with self-similar propagation," *Math. Problems Eng.*, vol. 2015, pp. 1–12, 2015.

[35] Z. Wang, M. V. Kleunen, H. J. During, and M. J. A. Werger, "Root foraging increases performance of the clonal plant potentilla reptans in heterogeneous nutrient environments," *PLoS ONE*, vol. 8, no. 3, 2013, Art. no. e58602.

[36] L. Ma, K. Hu, Y. Zhu, and H. Chen, "A hybrid artificial bee colony optimizer by combining with life-cycle, Powell's search and crossover," *Appl. Math. Comput.*, vol. 252, pp. 133–154, Feb. 2015.

[37] L. Ma, Y. Zhu, Y. Liu, L. Tian, and H. Chen, "A novel bionic algorithm inspired by plant root foraging behaviors," *Appl. Soft Comput.*, vol. 37, pp. 95–113, Dec. 2015.

[38] M. Kuchhold, M. Simon, and T. Sikora, "Restricted Boltzmann machine image compression," in *Proc. Picture Coding Symp. (PCS)*, Jun. 2018, pp. 243–247, doi: 10.1109/PCS.2018.8456279.

[39] Z. Liu, R. Wang, N. Japkowicz, D. Tang, W. Zhang, and J. Zhao, "Research on unsupervised feature learning for Android malware detection based on restricted Boltzmann machines," *Future Gener. Comput. Syst.*, vol. 120, pp. 91–108, Jul. 2021.

[40] R. W. R. de Souza, D. S. Silva, L. A. Passos, M. Roder, M. C. Santana, P. R. Pinheiro, and V. H. C. de Albuquerque, "Computer-assisted Parkinson's disease diagnosis using fuzzy optimum-path forest and restricted Boltzmann machines," *Comput. Biol. Med.*, vol. 131, Apr. 2021, Art. no. 104260.

[41] L. Xing, K. Demertzis, and J. Yang, "Identifying data streams anomalies by evolving spiking restricted Boltzmann machines," *Neural Comput. Appl.*, vol. 32, pp. 6699–6713, Jun. 2020.

[42] X. Lü, L. Meng, C. Chen, and P. Wang, "Fuzzy removing redundancy restricted Boltzmann machine: Improving learning speed and classification accuracy," *IEEE Trans. Fuzzy Syst.*, vol. 28, no. 10, pp. 2495–2509, Oct. 2020.

[43] K. Demertzis, L. Iliadis, E. Pimenidis, and P. Kikiras, "Variational restricted Boltzmann machines to automated anomaly detection," *Neural Comput. Appl.*, vol. 1, pp. 15207–15220, Mar. 2022.

[44] Mississippi State University Critical Infrastructure Protection Center. (Apr. 2014). *Industrial Control System Cyber Attack Data Set*. [Online]. Available: http://www.ece.msstate.edu/wiki/index.php/ICS_Attack_Dataset

[45] S. Pan, T. Morris, and U. Adhikari, "Developing a hybrid intrusion detection system using data mining for power systems," *IEEE Trans. Smart Grid*, vol. 6, no. 6, pp. 3104–3113, Nov. 2015, doi: 10.1109/TSG.2015.2409775.

[46] S. Pan, T. Morris, and U. Adhikari, "Classification of disturbances and cyber-attacks in power systems using heterogeneous time-synchronized data," *IEEE Trans. Ind. Informat.*, vol. 11, no. 3, pp. 650–662, Jun. 2015, doi: 10.1109/TII.2015.2420951.

[47] R. C. Borges Hink, J. M. Beaver, M. A. Buckner, T. Morris, U. Adhikari, and S. Pan, "Machine learning for power system disturbance and cyber-attack discrimination," in *Proc. 7th Int. Symp. Resilient Control Syst. (ISRCS)*, Aug. 2014, pp. 1–8, doi: 10.1109/ISRCS.2014.6900095.

[48] B. Riyaz and S. Ganapathy, "A deep learning approach for effective intrusion detection in wireless networks using CNN," *Soft Comput.*, vol. 24, no. 22, pp. 17265–17278, Nov. 2020.

[49] L. Haghnegahdar and Y. Wang, "A whale optimization algorithm-trained artificial neural network for smart grid cyber intrusion detection," *Neural Comput. Appl.*, vol. 32, no. 13, pp. 9427–9441, Jul. 2020.

[50] 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.

[51] J. Kim, J. Kim, H. Kim, M. Shim, and E. Choi, "CNN-based network intrusion detection against denial-of-service attacks," *Electronics*, vol. 9, no. 6, p. 916, Jun. 2020.

[52] M. Choraś and M. Pawlicki, "Intrusion detection approach based on optimised artificial neural network," *Neurocomputing*, vol. 452, pp. 705–715, Sep. 2021.

[53] G. O. Young, "Synthetic structure of industrial plastics," in *Plastics*, vol. 3, J. Peters, Ed., 2nd ed. New York, NY, USA: McGraw-Hill, 1964, pp. 15–64.

[54] P. Agrawal, H. F. Abutarboush, T. Ganesh, and A. W. Mohamed, "Metaheuristic algorithms on feature selection: A survey of one decade of research (2009–2019)," *IEEE Access*, vol. 9, pp. 26766–26791, 2021, doi: 10.1109/ACCESS.2021.3056407.

[55] L. Wang, Q. Cao, Z. Zhang, S. Mirjalili, and W. Zhao, "Artificial rabbits optimization: A new bio-inspired meta-heuristic algorithm for solving engineering optimization problems," *Eng. Appl. Artif. Intell.*, vol. 114, Sep. 2022, Art. no. 105082, doi: 10.1016/j.engappai.2022.105082.

[56] X. Li, A. Zheng, X. Zhang, C. Li, and L. Zhang, "Rolling element bearing fault detection using support vector machine with improved ant colony optimization," *Measurement*, vol. 46, no. 8, pp. 2726–2734, Oct. 2013.

[57] O. A. Alimi, K. Ouahada, A. M. Abu-Mahfouz, and S. Rimer, "Power system events classification using genetic algorithm based feature weighting technique for support vector machine," *Heliyon*, vol. 7, no. 1, Jan. 2021, Art. no. e05936, doi: 10.1016/j.heliyon.2021.e05936.

[58] C. L. Huang and J. F. Dun, "A distributed PSO–SVM hybrid system with feature selection and parameter optimization," *Appl. Soft Comput.*, vol. 8, pp. 1381–1391, Sep. 2008.

SAYAWU YAKUBU DIABA (Graduate Student Member, IEEE) was born in Suhum, Ghana. He received the B.Eng. and M.Sc. degrees in telecommunications engineering from the Kwame Nkrumah University of Science and Technology. He is currently pursuing the D.Sc. (Tech.) degree in telecommunication engineering with the University of Vaasa, Finland. He was formerly employed with Electricity Company of Ghana, where he worked as a Power Distribution Specialist for 13 years. His research interests include the use of machine learning in smart grids, developing cyber security algorithms for smart grids SCADA networks, and performance analysis of smart grids. He is also interested in wireless communication and automation.

MIADREZA SHAFIE-KHAH (Senior Member, IEEE) received the first Ph.D. degree in electrical engineering from Tarbiat Modares University, Tehran, Iran, the second Ph.D. degree in electromechanical engineering from the University of Beira Interior (UBI), Covilha, Portugal. He held postdoctoral positions at UBI and the University of Salerno, Salerno, Italy. Currently, he is a Professor (tenure-track) with the University of Vaasa, Vaasa, Finland. He has coauthored more than 500 papers that received more than 12000 citations with an H-index of 62. His research interests include electricity markets, power system optimization, demand response, electric vehicles, price and renewable forecasting, and smart grids. He has won five best paper awards at IEEE conferences. He was considered one of the Outstanding Reviewers of the IEEE TRANSACTIONS ON SUSTAINABLE ENERGY, in 2014 and 2017, the IEEE TRANSACTIONS ON POWER SYSTEMS, in 2017 and 2018, and the IEEE OPEN ACCESS JOURNAL OF POWER AND ENERGY, in 2020 and 2021; and one of the Best Reviewers of the IEEE TRANSACTIONS ON SMART GRID, in 2016 and 2017. He is a Top Scientist in the Research.com ranking in engineering and technology. He is an Editor of the IEEE TRANSACTIONS ON SUSTAINABLE ENERGY and the IEEE OPEN ACCESS JOURNAL OF POWER AND ENERGY; an Associate Editor of the IEEE SYSTEMS JOURNAL, IEEE ACCESS, and *IET-RPG*; the Guest Editor-in-Chief of the IEEE OPEN ACCESS JOURNAL OF POWER AND ENERGY; and the Guest Editor of the IEEE TRANSACTIONS ON CLOUD COMPUTING and more than 14 special issues. He is also the Volume Editor of the book titled *Blockchain-Based Smart Grids* (Elsevier, 2020).

MOHAMMED ELMUSRATI (Senior Member, IEEE) received the B.Sc. and M.Sc. degrees (Hons.) in electrical and electronic engineering from the University of Benghazi, Libya, in 1991 and 1995, respectively, and the Licentiate of Science degree (Hons.) in technology and the D.Sc. degree in technology, automation and control engineering from Aalto University, Finland, in 2002 and 2004, respectively. He is a Full Professor of communication, automation, and digitalization with the School of Technology and Innovations, University of Vaasa, Finland. He has developed several international programs, such as the Communication and Systems Engineering Program and the Industrial Digitalization Program. Now, he is the Head of the International Program of Sustainable and Autonomous Systems (SAS). He has published about 160 papers, books, and book chapters. His research interests include wireless communications, artificial intelligence, machine learning, biotechnology, data analysis, stochastic systems, and game theory.