BIG DATA MINING AND ANALYTICS
ISSN 2096-0654 08/15 pp399–418
DOI: 10.26599/BDMA.2023.9020022
Volume 7, Number 2, June 2024

An Intelligent Big Data Security Framework Based on AEFS-KENN Algorithms for the Detection of Cyber-Attacks from Smart Grid Systems

Sankaramoorthy Muthubalaji, Naresh Kumar Muniyaraj, Sarvade Pedda Venkata Subba Rao, Kavitha Thandapani, Pasupuleti Rama Mohan, Thangam Somasundaram, and Yousef Farhaoui*

Abstract: Big data has the ability to open up innovative and ground-breaking prospects for the electrical grid, which also supports to obtain a variety of technological, social, and financial benefits. There is an unprecedented amount of heterogeneous big data as a consequence of the growth of power grid technologies, along with data processing and advanced tools. The main obstacles in turning the heterogeneous large dataset into useful results are computational burden and information security. The original contribution of this paper is to develop a new big data framework for detecting various intrusions from the smart grid systems with the use of AI mechanisms. Here, an AdaBelief Exponential Feature Selection (AEFS) technique is used to efficiently handle the input huge datasets from the smart grid for boosting security. Then, a Kernel based Extreme Neural Network (KENN) technique is used to anticipate security vulnerabilities more effectively. The Polar Bear Optimization (PBO) algorithm is used to efficiently determine the parameters for the estimate of radial basis function. Moreover, several types of smart grid network datasets are employed during analysis in order to examine the outcomes and efficiency of the proposed AdaBelief Exponential Feature Selection- Kernel based Extreme Neural Network (AEFS-KENN) big data security framework. The results reveal that the accuracy of proposed AEFS-KENN is increased up to 99.5% with precision and AUC of 99% for all smart grid big datasets used in this study.

Key words: smart grid; big data analytics; Machine Learning (ML); AdaBelief Exponential Feature Selection (AEFS); Polar Bear Optimization (PBO); Kernel Extreme Neural Network (KENN)

- Sankaramoorthy Muthubalaji is with Department of Electrical and Electronics Engineering, CMR College of Engineering & Technology, Hyderabad 501401, India. E-mail: muthusa15@gmail.com.
- Naresh Kumar Muniyaraj is with Department of Electronics and Communication Engineering, Vardhaman College of Engineering Kacharam, Shamshabad 501218, India. E-mail: nareshece84@gmail.com.
- Sarvade Pedda Venkata Subba Rao is with Department of Electronics and Communication Engineering, Sreenidhi Institute of Science and Technology, Hyderabad 501301, India. E-mail: spvsubbarao@sreenidhi.edu.in.
- Kavitha Thandapani is with Department of Electronics and Communication Engineering, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Chennai 600062, India. E-mail: kavithaecephd@gmail.com.
- Pasupuleti Rama Mohan is with Department of Electrical and Electronics Engineering, Bharat Institute of Engineering and Technology, Hyderabad 501510, India. E-mail: rammohan.kadapa@gmail.com.
- Thangam Somasundaram is with Department of Computer Science and Engineering, Amrita School of Computing, Amrita Vishwa Vidhyapeetham, Bengaluru 560035, India. E-mail: s_thangam@blr.amrita.edu.
- Yousef Farhaoui is with T-IDMS, Department of Computer Science, Faculty of Sciences and Techniques, Moulay Ismail University, Errachidia 52000, Morocco. E-mail: y.farhaoui@fste.umi.ac.ma.

* To whom correspondence should be addressed.
Manuscript received: 2023-03-22; revised: 2023-07-20; accepted: 2023-08-06

1 Introduction

In the past few decades, the adoption of big data analytics in communication systems, transportation networks, healthcare, etc., has increased rapidly[1–5]. Moreover, the migration of power grid to smart grid is characterized by using big datasets with customized tools, controlling systems, and techniques. Also, it is widely believed that the application of big data to present and future smart grids would have immense potential. Recent years have seen significant advancements in the electrical power system[6]. Together with the transmission and distribution of power, there have been technological advancements in the power generation sector. The adoption of various demand management programs and strategies is another way that the new technology is anticipated to transform the end-user side[7, 8]. In addition to utility companies, end users and micro-grids also contribute to the generation of renewable energy sources, such as solar and wind sources. Moreover, the smart grids have been gradually replacing conventional power systems[9, 10]. To address the increasing demands and developing risks in the field of power systems, certain new and technologically advanced sensors called "smart grids" will eventually replace the conventional electric grids. These grids give real-time data to storage systems[11–14], which aids in the automatic detection of grid failures and allows for self-healing. The data given by the sensors are quite large and are generated at extremely brief periods of time. The heterogeneity is provided to smart grids by various forms of data that are generated by sensors.

The addition of numerous smart meters and other information extraction units is related to this shift. The cost-effective smart grid incorporates[15, 16] the behaviors and operations of all users, including generation units, customers, and power station. This integration process results in decreased power loss and high-quality power production, which keeps the power system affordable and sustainable. The system is additionally protected by security measures. Modern smart grids[17–19] today include new controls, communications, smart monitoring, and self-healing products, technologies, and services. These organizations offer a variety of advantages, including simple connection and operating efficiency for generators of all sizes and technology[20]. Customers here are aware of the information about the systems and play a crucial part in enhancing operation of the system. Also, it is possible to optimize the load demand, which can dramatically lessen environmental pollution throughout the entire electrical supply system. Since, the smart grid[21, 22] is a key infrastructure, any cyber or physical vulnerabilities might have significant consequences. Traditionally, the power system planners use vulnerability assessment techniques to provide protection from the effects of sudden disturbances caused by system faults. The majority of smart grid data consists of customer personal data, proprietary information, and economic transactions (see Fig. 1).

Hence, it is very essential to secure the smart grid datasets with ensured confidentiality, reliability, authentication, and secrecy. The big data framework is a model that is developed by integrating multiple machine learning methods[23–25]. The model is trained using the training portion of the dataset and validated against by the testing dataset. Intrusion Detection Systems (IDSs)[26–28] look for features that violate a system program's or a computer network's security agreement. IDS must consent to maintaining security precautions. Threats that result in defects in program design are found using the firewall for IDS. Moreover, the IDS[29, 30] makes it possible for forensic suspicion to recognize the program administrator's defenses against cyber threats. Systems for detecting intrusions into networks and systems are available. IDS tools are specifically designed to find system threats or network abuse, and notify the appropriate people when they are found. An IDS[6] examines all incoming and outgoing network traffic in order to look for any abnormal patterns that might point to a network or system attack by someone attempting to infiltrate a machine. The functionality of an IDS [31, 32] on a system or network is equivalent to that of a fixed intrusion alarm system.

For intelligent prediction and optimization of the many automated activities already present in the smart grids, the Machine Learning (ML)/Deep Learning (DL) is an appropriate computing tool highly used in recent times. In the conventional works, various big data analytics frameworks have been developed to increase the security of smart grid systems [32–34]. However, most of the approaches have difficulties in terms of computational burden in system design, ineffective predictions, and high time consumption. Therefore, the

Fig. 1 Sources big data used in smart grid systems.

proposed work motivates to develop a novel intelligent big data framework to secure smart grid systems, which has the following contributions:

- To effectively handle the input smart grid big datasets for enhancing security, an AdaBelief Exponential Feature Selection (AEFS) mechanism is implemented.
- To predict the security vulnerabilities with better performance efficacy, a Kernel based Extreme Neural Network (KENN) algorithm is deployed.
- To optimally compute the parameter for the estimation of radial basis function, the Polar Bear Optimization (PBO) algorithm is utilized.
- To analyze the results of the proposed AEFS-KENN based big data security framework, the different types of smart grid network datasets are used during analysis.

The remaining sections of this work are divided into the following categories: Section 2 presents the full literature assessment of several big analytics approaches utilized for smart grid security along with benefits and drawbacks. The work flow and algorithms are described along with a comprehensive explanation of the proposed AEFS-KENN technique in Section 3. Moreover, Section 4 uses several datasets to validate and evaluate the security performance results. In Section 5, the paper's conclusion and findings are presented, which has future scope.

2 Related Work

The cutting-edge big data analytical methods for the smart grid's sustainability are outlined in this review. In order to achieve sustainable goals, the first discussion is on socioeconomic, analytical, and ecological factors in relation to the smart grid and big data analytics. Moreover, the different types of data mining methodologies used for securing the smart grid systems are also investigated in this part.

Syed et al.[34] investigated a comprehensive survey on various technologies and methods used in the field of smart grid big data systems, they provided an outline of the phases of the big data process as well as the numerous big data analytics techniques that are available. Also, they talked about possible smart grid applications that could benefit from the unrealized potential of big data. Real-time and enormous quantities of information are generated by smart grids at an extremely rapid rate. For electricity grids, information must be extracted from smart grid data, which requires a thorough understanding of the data

inputs[35]. Consumption, transmission, storage, and generation data are the several types of data that can be found in smart grids. Typically, sensors, monitoring devices, electrical devices, analyzers, Supervisory Control And Data Acquisition (SCADA), etc., are used to collect these data[36]. The main scope of using big data analytics in smart grid systems is graphically depicted in Fig 2.

Cui et al.[35] intended to predict the false data attacks in smart grid systems by using ML techniques. The authors of this study gave a thorough overview of these advancements. A quick overview of the smart grid architecture and its information sources is given at the beginning of the study. Also, the types of false data attacks are discussed, followed by the data security standards. The most recent methods of ML-based detection are then condensed into three main detection instances: quasi losses, condition estimation, and predictive modeling. A significant threat is the misleading data assault. By manipulating sensor measurements in smart grid, it can attack all the levels of smart grid systems while getting around the conventional protections. The most common false data attack uses fraudulent packets to trick service providers, disrupt information flow, or deactivate edge devices to impair service between physical devices and networks. The attackers are motivated to undertake recurrent attacks in order to drain energy or physically harm the end devices. A replay assault, in contrast to false data attacks, keeps uploading the covert data into the end devices throughout the course of a specific time period. According to the study, it is identified that there are significant drawbacks to directly implementing current machine learning algorithms for electric data analytics in real smart grid applications. The fact that there are few public datasets and labelled samples makes it impossible to ensure the trained model's accuracy. Kumar et al.[36] implemented a new secured

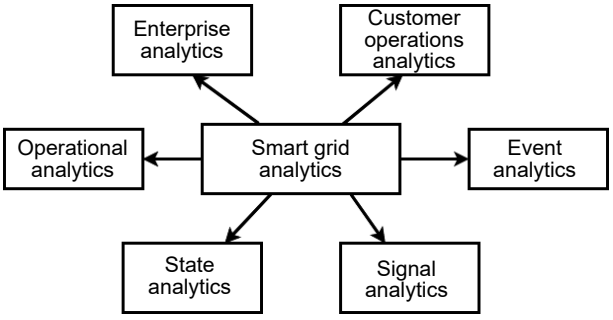

Fig. 2 Main scope of big data analytics in smart grid.

authentication protocol to assure security of smart grid systems. Here, an Elliptic Curve Cryptography (ECC) model has been used to preserve the demand response of smart grid systems. In this work, the different types of attacks that affect the smart grid networks have been discussed, which include man-in-the-middle attack, impersonation attack, replay attack, device attack, etc. Karimipour et al.[37] deployed an unsupervised classification mechanism to protect smart grid systems from cyberattacks. Here, the symbolic dynamic filtering mechanism is used to simplify the process of attack detection with low computational burden. Moreover, a model-free strategy is applied to both hierarchical and topological networks for various assault situations. Tarik and Farhaoui[38] presented a detailed study on various machine learning techniques for assuring security in wireless communication systems[39]. The concept of big data refers to a set of sophisticated hardware and development tools that gather enormous volumes of data, safely store it on a vast number of cloud servers, process it using intricate algorithms, and analyze data it in real-time.

Latif et al.[40] designed a light weight dense random neural network methodology to detect cyber-attacks in the smart grid systems. The key benefits of using this approach are easy to understand, better generalization capability, and simplified computations. The variables known as hyper parameters govern the network structure and regulate the learning process. The authors conducted a comprehensive test to identify the ideal hyper parameters to guarantee the performance of suggested deep learning algorithm. Here, the learning rate, speed, number of iterations, and time duration are some of the important hyper parameters considered in this work. Alkahtani and Aldhyani[41] deployed three different deep learning mechanisms such as, Convolutional Neural Network (CNN), Long Short Term Memory (LSTM), and hybrid convolutional network for protecting smart grid networks from cyber-attacks. Moreover, the swarm intelligence based optimization algorithm is deployed for estimating the subset of features. However, the time taken for training and testing is very high, which degrades the security performance of the suggested framework. Vijayanand et al.[42] introduced a hierarchical deep learning based attack detection system for guaranteeing the cyber security of smart meter communication network. The purpose of this paper is to spot intrusions in the smart

grid systems with better prediction accuracy. Here, the stochastic gradient algorithm is used to tune the hyper parameters of the deep learning model.

Zhang et al.[43] and Mouatasim and Farhaoui[44] utilized a Genetic Algorithm (GA) based extreme learning machine for identifying intrusions in the smart grid systems. Power distribution networks and communication networks make up the two components of the smart grid. A variety of gadgets communicate with one another over the communication network. The fact that the communication network is frequently linked to a machine creates a number of new security concerns. Grammatikis et al.[45] designed a multi-variate intrusion detection framework for protecting smart grid networks with high level of security. Here, the GAN model is also utilized to minimize the error functions with better efficiency. This framework includes the major modules of data collection phase, analysis engine module, and response phase. In which, the network traffic dataset is taken as the input for processing and analysis, where the network flow statistics are extracted for improving the performance of detection. Li et al.[46] deployed a federated deep learning methodology based cyber physical systems for protecting heterogeneous industrial networks against intrusions. The authors created a federated learning system that enables various industrial cyber physical systems to jointly create an extensive intrusion detection model while maintaining privacy. In addition, a secure communication protocol based on the Paillier public-key cryptosystem was designed for the federated learning framework, which can effectively maintain the confidentiality and security of model parameters during training. However, the suggested framework has the limitations of increased computational burden, difficult to deploy, and slow processing. Mahdavisharif et al.[47] utilized a big data aware framework for developing an intrusion detection framework with the use of LSTM. Due to the increased speed of processing, and reduced system complexity, the big data analytics methodology is implemented in this work. Table 1 compares the previous methodologies used for securing smart grid systems, where the different types of parameters and datasets used in the conventional works are also investigated.

The reviews [48–51] show that most big data analytics-based security frameworks might utilize AI (i.e., both ML and DL) methods to protect smart grid networks. Nevertheless, the main issues with the present works are their inability to handle huge datasets, slow processing speeds, low attack detection rates, and complex system designs. Thus, the proposed work motivates to develop a novel and unique security framework based on big data analytics for protecting smart grid systems.

3 Proposed Methodology

The detailed explanation of the proposed Rapid AEFS-KENN based big data security framework for smart grid systems is presented in this section. The original contribution of this paper is to design a unique and reliable attack detection framework based on Artificial Intelligence (AI) for increasing the security level of smart grid systems. Presently, several cyber-physical systems are developed in the baseline works for improving the security of smart grid networks. Due to their increased computational burden and system complexity, the proposed work motivates to develop a

Table 1 Comparative study on previous works.

Reference	Method	Dataset used	Finding
[36]	LSTM-auto encoder based robust security model	Gas Pipeline and UNSW-NB 15	accuracy = 97.95%
[37]	Cyber SCADA security model using ML approaches	ORNL Electric test bed	AUC = 99%
[38]	Adversarial machine learning model	Authentic power system dataset	time = 25.21s, precision = 94%, recall = 94%, and accuracy = 94%
[39]	Three tiered intrusion detection system	Industrial gas pipeline dataset	F-measure = 87.4%, precision = 87.9%, and recall = 88.4%
[40]	Deep multi-modal cyber security mechanism	ICS dataset	precision = 99%, recall = 98%, and F-measure = 98%
[41]	Honey badger world optimization based deep learning algorithm	ICS dataset	accuracy = 99%
[42]	CNN-GRU based security model	WUSTL-IIoT 2018 and WUSTL-IIoT-20 121 dataset	accuracy = 99%

simple and novel security model. Typically, understanding the data is the initial stage in an information-driven methodology like AI. Several forms of data, such as host actions and network connection, can describe the behavior of particular attack. The network traffic is a representation of network behavior, while server logs provide host behaviors. There are various attack types, and each has a unique pattern. To detect different attacks in accordance with the characteristics of the threat, it is crucial to choose appropriate data sources. AI is a key component of cybersecurity, and numerous studies have suggested the development of network security solutions based on AI. The workflow model of the proposed system is depicted in Fig. 3, which includes the following key stages:

- Smart grid big dataset obtainment;
- Preprocessing & normalization;
- AEFS;
- KENN;
- PBO.

In the proposed security framework, a combination on intelligence algorithms, including AEFS, KENN, and PBO, are used for feature selection, classification, and optimal parameter computation. Moreover, the overall proposed work is named as rapid AEFS-KENN based big data security framework for spotting cyber-attacks from smart grid systems. Preprocessing involves the conversion of categorical features with nominal values into numerical values to make sure the data are compatible with the neural network's input. In this work, label encoding is used to transform categorical information into numerical values. These columns are removed during preprocessing since the data, time, and time stamp attributes have no bearing on it or contribution to the result prediction. Several features in the dataset have bigger values than others due to the model's bias towards large values, which may lower the accuracy of the results. Data are mapped between 0 and 1 during data normalization to maintain the consistency of the data's behavior. After that, the AEFS mechanism is used to select the best optimal

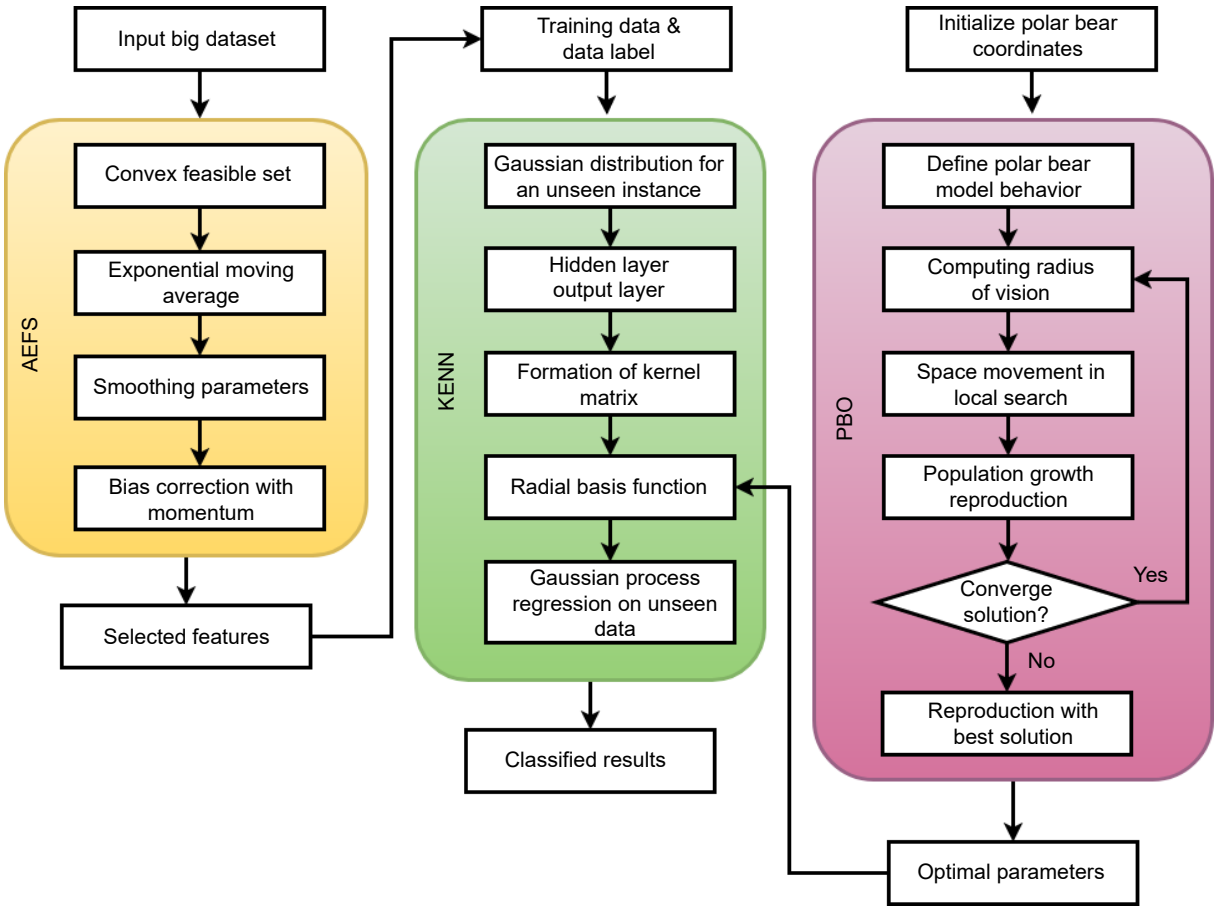

Fig. 3 Work flow of the proposed model.

features from the smart grid big dataset based on the Exponential Moving Average (EMA) function. Consequently, the training data are modeled with the selected feature set for attack prediction and categorization. During this process, the Gaussian distribution function estimation, kernel matrix formation, computation of radial basis function, and regression process have been performed to improve the accuracy of attack detection. In order to optimally compute the radial basis function, the PBO algorithm is used in this work. The primary advantages of using the proposed security model are increased attack rate, lower computational complexity, and effective performance outcomes. Yet, the amount of time required for training and testing big datasets need to be reduced, which could be the major limitation of this study.

3.1 AEFS

In this work, the AEFS algorithm is used to optimally identify the set of features for classifier training. Conventionally, several optimization techniques are implemented in the existing works for feature selection. Among other techniques, the proposed AEFS provides enormous benefits to the security system. Moreover, the proposed AdaBelief is easily customizable from Adam without additional parameters. The three major characteristics of AdaBelief include:

- Quick convergence, similar to adaptive gradient algorithms;
- Excellent generalization capability;
- Training resilience.

In addition, the proposed work intends to obtain an increased attack detection accuracy and efficiency with the use of AEFS. The term "AdaBelief" describes the process of modifying the training strides in accordance with one's belief of the gradient direction. In the conceptual framework, the optimizer will adapt this adjustment to take the curvature of the loss function into account rather than performing a huge (low) step where the gradient is big (small). In other words, this strategy takes into account both the consistency of the gradient direction through time and the modulus size of the historical gradient of parameters. Moreover, it updates the stochastic gradient descent function based on the curvature information, where the parameters such as learning rate and step size have been used. In this algorithm, the parameters such as real number, Exponential Moving Average (EMA), step parameter, time stamp, and feature data are taken as the inputs for dataset optimization. Then, the selected subset of features is produced as the output. At first, the loss function is minimized with respect to the dimension of real numbers as represented in below:

$$f(\varphi) = \mathbf{R},\ \varphi \in \mathbf{R}^d \tag{1}$$

where d indicates the dimension of real numbers. Until reaching the maximum number of iterations, the gradient of convex feasible set is computed by using the following model:

$$\beta_t \leftarrow \nabla_\varphi f_t(\varphi_t - 1) \tag{2}$$

Consequently, the EMA is updated, and its step parameter is computed based on the following equations:

$$\bar{\varrho}_t \leftarrow \tau_1 \bar{\varrho}_{t-1} + (1-\tau_1)\beta_t \tag{3}$$

$$s_p^t = \tau_2 s_p^{t-1} + (1-\tau_2)(\beta_t - \bar{\varrho}_t)^2 + \varepsilon \tag{4}$$

Then, the bias correction is performed with the EMA of gradient and step, as shown in below:

$$\widehat{\bar{\varrho}_t} \leftarrow \frac{\bar{\varrho}_t}{1-\tau_1^t} \tag{5}$$

$$\widehat{s_p^t} \leftarrow \frac{s_p^t}{1-\tau_2^t} \tag{6}$$

Moreover, the estimated parameters are updated with the bias corrected values based on the following equation:

$$\varphi_t \leftarrow \prod_{\sqrt{s_p^t}} \left(\varphi_{t-1} - \frac{\vartheta \widehat{\bar{\varrho}_t}}{\sqrt{s_p^t} + \varepsilon} \right) \tag{7}$$

Based on this process, the optimal set of features f_s are obtained as the output of this algorithm, which is in the following form:

$$f_s \leftarrow f_d[i,:],\ \forall\ \text{mean}(f_d[i,:]) > \varphi_t \tag{8}$$

The obtained features can be further used by the classifier for proper training and testing operations in order to detect attacks in the smart grid systems. The list of symbols used in this algorithm with its corresponding descriptions are given in Table 2. Algorithm 1 explains the feature selection procedure of AEFS mechanism.

Table 2 List of symbols and its descriptions.

Symbol	Description
$\bar{\varrho}$	EMA
$\mathbf{R}$	Real number
φ	Temporary parameter
s_p	Step parameter
t	Time stamp
f_d	Feature data
$f(\cdot)$	Loss function
d	Dimension
$\max_{\text{iter}}$	Maximum number of iterations
β_t	Gradient of convex set
τ_1 and τ_2	Smoothing parameters
ε	Constant
φ	Parameter in $\mathbf{R}$
ϑ	Learning rate
f_s	Selected features

3.2 KENN

In this stage, the proposed KENN classifier can use the optimal set of features for identifying intrusions from the smart grid big dataset based on training and testing modules. Most of the existing security frameworks used in the smart grid systems are mainly using the machine learning based classification algorithms for intrusion detection. When compared to the deep learning models, the machine learning techniques are simpler to implement with less computational burden. However, the conventional machine learning approaches have the major difficulties of high time for training features, overfitting, increased false positives, and low detection rate. Therefore, the proposed big data analytics framework intends to use the novel KENN algorithm for detecting attacks from the smart grid systems. It is a kind of non-iterative learning algorithm that trains the single hidden-layer feed-forward neural networks for an accurate prediction of results. Moreover, it analytically calculates the weights for the output layer while selecting the input layer, weights, and hidden layer biases at random. Specifically, it eliminates the overfitting issue with improved kernel efficiency. In this technique, the

Algorithm 1 AEFS

Input: Parameter φ, EMA $\bar{\varrho}$, step parameter s_p, time stamp t, feature data f_d

Output: Selected features f_s

Procedure:

- Loss function is minimized, $f(\varphi) = \mathbf{R}$, where $\varphi \in \mathbf{R}^d$;
- **while** $t < \max_{\text{iter}}$ and φ_t not converged
  - Gradient of convex feasible set β_t is computed using Formula (2);
  - Then, EMA $\bar{\varrho}_t$ of β_t is computed by Formula (3);
  - Step parameter s_p^t from EMA is estimated based on Eq. (4);
  - Perform bias correction $\widehat{\bar{\varrho}_t}$ and $\widehat{s_p^t}$ using Formulas (5) and (6);
  - Update parameter φ_t with bias corrected values as represented in Formula (7);
- **end while**
- Selected features f_s;
- Form of obtained output is shown in Formula (8).

training data Tr^{d}, unseen data $\text{T}_{\text{u}}^{\text{d}}$, and label data La^{d} are taken as the inputs for processing, and the output data $\text{cl}_{\text{o}}^{\text{d}}$ is produced as the final result of classification. At first, the output class of unseen data is predicted based on the joint Gaussian distribution model as represented in the following:

$$\begin{bmatrix} \text{cl}_{\text{o}}^{\text{d}} \\ \widehat{\text{cl}_{\text{o}}^{\text{d}}} \end{bmatrix} \sim \left[0, \begin{bmatrix} K(E, E) & k^{\text{T}}\left(e\left(\widehat{\text{cl}_{\text{o}}^{\text{d}}}\right), E\right) \\ k\left(e\left(\widehat{\text{cl}_{\text{o}}^{\text{d}}}\right), E\right) & k\left(e\left(\widehat{\text{cl}_{\text{o}}^{\text{d}}}\right), e\left(\widehat{\text{cl}_{\text{o}}^{\text{d}}}\right)\right) \end{bmatrix} \right] \tag{9}$$

Here, the vector value of the j-th hidden layer is estimated with the training instance as shown in below:

$$e\left(\text{cl}_{\text{o}}^{\text{d}}\right) = \left[a\left(w_1 \text{Tr}^{\text{d}}(1) + b_1\right), a\left(w_1 \text{Tr}^{\text{d}}(2) + b_2\right), \ldots, a\left(w_n \text{Tr}^{\text{d}}(j) + b_n\right)\right] \tag{10}$$

where $e\left(\widehat{\text{cl}_{\text{o}}^{\text{d}}}\right)$ is the vector value of output data, $b_1, b_2, \ldots, b_n$ is the bias value, $w_1, w_2, \ldots, w_n$ is the weight value, and k is the kernel vector. Moreover, the kernel matrix $K(E,E)$ with set of rows E and columns E is formulated with the use of kernel vector by using the following model:

$$K(E, E) = \begin{bmatrix} k\left(e\left(\widehat{\text{cl}_{\text{o}}^{\text{d}}}(1)\right), e\left(\widehat{\text{cl}_{\text{o}}^{\text{d}}}(1)\right)\right) \ldots k\left(e\left(\widehat{\text{cl}_{\text{o}}^{\text{d}}}(1)\right), e\left(\widehat{\text{cl}_{\text{o}}^{\text{d}}}(M)\right)\right) \\ \vdots \\ k\left(e\left(\widehat{\text{cl}_{\text{o}}^{\text{d}}}(M)\right), e\left(\widehat{\text{cl}_{\text{o}}^{\text{d}}}(1)\right)\right) \ldots k\left(e\left(\widehat{\text{cl}_{\text{o}}^{\text{d}}}(M)\right), e\left(\widehat{\text{cl}_{\text{o}}^{\text{d}}}(M)\right)\right) \end{bmatrix} \tag{11}$$

Here, the kernel vector is expressed in the following form:

$$k\left(e\left(\widehat{\mathrm{cl}_{\mathrm{o}}^{\mathrm{d}}}\right), E\right) = \left[k\left(e\left(\widehat{\mathrm{cl}_{\mathrm{o}}^{\mathrm{d}}}\right), e\left(\widehat{\mathrm{cl}_{\mathrm{o}}^{\mathrm{d}}}(1)\right)\right), \ldots, k\left(e\left(\widehat{\mathrm{cl}_{\mathrm{o}}^{\mathrm{d}}}\right), e\left(\widehat{\mathrm{cl}_{\mathrm{o}}^{\mathrm{d}}(M)}\right)\right)\right] \quad (12)$$

Moreover, the Radial Basis Function (RBF) of the kernel vector is computed based on the optimal parameter generated by using the PBO algorithm. The RBF is in the following form:

$$k(g, h) = \exp\left(-\frac{\|g-h\|^2}{2\delta^2}\right) \quad (13)$$

where δ is the optimal parameter generated using PBO algorithm. Consequently, the posterior distribution of the predicted output is computed with the mean and variance as represented in the following models:

$$\mathrm{pr}\left[e\left(\widehat{\mathrm{cl}_{\mathrm{o}}^{\mathrm{d}}}(M)\right), \mathrm{La}^{\mathrm{d}}, \mathrm{cl}_{\mathrm{o}}^{\mathrm{d}}\right] = N\left(\mu, \sigma^2\right) \quad (14)$$

$$\mu = k\left(e\left(\widehat{\mathrm{cl}_{\mathrm{o}}^{\mathrm{d}}}\right), E\right)\left[K(E, E) + \sigma_M^2 I_m\right]^{-1}\mathrm{cl}_{\mathrm{o}}^{\mathrm{d}} \quad (15)$$

$$\sigma^2 = k\left(e\left(\widehat{\mathrm{cl}_{\mathrm{o}}^{\mathrm{d}}}\right), e\left(\widehat{\mathrm{cl}_{\mathrm{o}}^{\mathrm{d}}}\right)\right) - k\left(e\left(\widehat{\mathrm{cl}_{\mathrm{o}}^{\mathrm{d}}}\right), E\right)\left[K(E, E) + \sigma_M^2 I_m\right]^{-1} \times k\left(e\left(\widehat{\mathrm{cl}_{\mathrm{o}}^{\mathrm{d}}}\right), E\right) \quad (16)$$

where μ and σ^2 are the mean and variance of the Gaussian distribution, respectively, I_m is an $M \times M$ identity matrix, and μ is used as the predictive output of the unseen data. At last, the final output data are obtained, representing the predicted result as shown below:

$$\widehat{\mathrm{cl}_{\mathrm{o}}^{\mathrm{d}}} = k\left(e\left(\widehat{\mathrm{cl}_{\mathrm{o}}^{\mathrm{d}}}\right), E\right)\left[K(E, E) + \sigma_M^2 I_m\right]^{-1} \times \mathrm{cl}_{\mathrm{o}}^{\mathrm{d}} \quad (17)$$

$$e\left(\widehat{\mathrm{cl}_{\mathrm{o}}^{\mathrm{d}}}\right) = \left[a\left(\mathrm{w}_1 \mathrm{T}_{\mathrm{u}}^{\mathrm{d}}(1) + \mathrm{b}_1\right), \ldots, a\left(\mathrm{w}_n \mathrm{T}_{\mathrm{u}}^{\mathrm{d}}(j) + \mathrm{b}_n\right)\right], \quad \forall j = 1, 2, \ldots, M \quad (18)$$

Based on this classification operation, the intrusions or cyber-attacks in the smart grid systems are accurately detected with low system complexity and time consumption. Algorithm 2 illustrates the steps involved in the KENN classification model, which provides the overview of attack detection operation.

Algorithm 2 KENN

Input: Training data Tr^{d}, unseen data $\mathrm{T}_{\mathrm{u}}^{\mathrm{d}}$, label data La^{d}

Output: Output data $\mathrm{cl}_{\mathrm{o}}^{\mathrm{d}}$

Procedure:

Step 1: For an unseen data $\mathrm{T}_{\mathrm{u}}^{\mathrm{d}}$, the output class $\mathrm{cl}_{\mathrm{o}}^{\mathrm{d}}$ is predicted according to the joint Gaussian distribution as represented in Formula (9).

Here, the hidden-layer output vector of the j-th (j = 1, 2, …, M) training instance is estimated by Eq. (10).

Step 2: Construct the kernel matrix $K(E, E)$ with the use of predicted class data as represented in Eq. (11).

Here, the kernel vector $k\left(e\left(\widehat{\mathrm{cl}_{\mathrm{o}}^{\mathrm{d}}}\right), E\right)$ used to form the kernel matrix is estimated by Eq. (12).

Step 3: Compute the kernel of RBF $k(g, h)$ as defined in Eq. (13).

Here, δ parameter is obtained by using the PBO algorithm.

Step 4: Estimate the posterior distribution of the predicted output $\widehat{\mathrm{cl}_{\mathrm{o}}^{\mathrm{d}}}$ as shown in Eq. (14).

Here, the mean μ and variance σ^2 of this Gaussian distribution are estimated by Eqs. (15) and (16).

Step 5: Finally, the output data $\widehat{\mathrm{cl}_{\mathrm{o}}^{\mathrm{d}}}$ for the predicted result is computed by Eqs. (17) and (18).

3.3 PBO

In the proposed security framework, the PBO algorithm is mainly used to compute the parameter in order to estimate the value of RBF required for the classification. In the literature works, several optimization algorithms are used to optimize the features of classification. Here, the PBO algorithm is used to compute the optimal parameter for accurate classification. The conventional meta-heuristics based optimization techniques have the major difficulties in terms of reduced efficiency, more iterations to find the optimal solution, and low convergence. Therefore, the proposed work intends to use the PBO algorithm for a proper optimization. PBO is a meta-heuristic method that draws inspiration from how polar bears hunt in the hostile arctic environments by using only their vision. In the wild, polar bears pursue their prey using both their excellent senses of scent and sight. Thus, a unique improved PBO variation that improves its functionality by giving it tracking capabilities using polar bears' sense of smell has been utilized in this work. In the search space, the PBO algorithm has three unique phases of search: local search by encircling and trapping prey, exploitation of the search space by floating ice oats, and variable population. Each of these phases highlights a key element of the polar bear's arctic hunting strategy. The PBO algorithm starts its search by arbitrarily altering each polar bear's n coordinates, and then uses global and local search tactics to propel itself towards the best possible solution in the search space. The bears encircle their prey while hunting locally and use their teeth to attack it. In this model, the Trifolium equations are effectively

used to model the performance. Moreover, two parameters known as distance of vision and angle of tumbling are randomly selected to represent the behavior of polar bears. In this model, the polar population p_n is obtained as the input for optimization, and the optimal parameters δ is produced as the output. At first, the set of populations of polar bears are initialized as represented in below:

$$\bar{p} = (p_0, p_1, \ldots, p_{z-1}) \tag{19}$$

where p_{z-1} is the number of polar bears.

The population's behavior of gliding on polar icebergs in search of food is represented by the following equation:

$$\left(\bar{p}_j^t\right)^k = \left(\bar{p}_j^{t-1}\right)^k + \text{sign}(\theta)\beta + \gamma \tag{20}$$

where $\left(\bar{p}_j^t\right)^k$ is the movement of k-th polar bear having k coordinates in t-th iteration towards the optimum, β denotes the random number within the range of [0 to 1], θ represents the distance between the present and optimum bear and, γ represents the random number in the range $(0, \omega)$, where ω is the weight value. Then, the distance is computed based on the Euclidean metrics as shown in below:

$$\text{dist}\left(\left(\bar{p}_j^t\right)^k, \left(\bar{p}_j^t\right)^j\right) = \sqrt{\sum_{s=0}^{g-1}\left[(\bar{p}_s^t)^k, (\bar{p}_s^t)^j\right]^2} \tag{21}$$

Moreover, the behavior of polar bears is transmuted by selecting the parameters of distance of vision ∂ in the range of (0, 0.3), and angle of tumbling Ψ_0 at random in the range of $(0, \pi/2)$. Based on these limits, the radius of vision is estimated according to the following equation:

$$\check{r} = 4h \times \cos(\Psi_0) \times \sin(\Psi_0) \tag{22}$$

where h is a random value.

By using this radius, each spatial coordinate's movement in the local search space is calculated as follows:

$$\begin{cases} p_0^{\text{new}} = p_0^{\text{actual}} \pm \check{r} \times \cos(\Psi_1), \\ p_1^{\text{new}} = p_1^{\text{actual}} \pm [\check{r} \times \sin(\Psi_1) + \check{r} \times \cos(\Psi_2)], \\ p_2^{\text{new}} = p_2^{\text{actual}} \pm [\check{r} \times \sin(\Psi_1) + \check{r} \times \sin(\Psi_2) + \check{r} \times \cos(\Psi_3)], \\ \qquad \cdots \\ p_{g-2}^{\text{new}} = p_{g-2}^{\text{actual}} \pm \sum_{w=1}^{g-2}\left[\check{r} \times \sin(\Psi_w) + \check{r} \times \cos\left(\Psi_{g-1}\right)\right], \\ p_{g-1}^{\text{new}} = \text{p}_{\text{g}-1}^{\text{actual}} \pm \sum_{\text{w}=1}^{\text{g}-2}\left[\check{r} \times \sin(\Psi_{\text{w}}) + \check{r} \times \cos\left(\Psi_{\text{g}-1}\right)\right] \end{cases} \tag{23}$$

where Ψ_1, Ψ_2, and Ψ_3 are chosen randomly in the range of $(0, \pi)$. Depending on the value of k, the individuals are eliminated whenever the population reaches greater than 50%, whereas the reproduced individual is represented in the following form:

$$\delta = \frac{\left(\bar{p}_j^t\right)^{\text{best}} - \left(\bar{p}_j^t\right)^k}{2} \tag{24}$$

where $\left(\bar{p}_j^t\right)^{\text{best}}$ is the best optimal solution is up to current iteration and $\left(\bar{p}_j^t\right)^k$ is arbitrarily selected. Based on this optimization algorithm, the parameter used to compute the RBF of classification is obtained, which helps to improve the overall prediction attack prediction accuracy. Algorithm 3 represents the steps involved in the PBO based optimal parameter computation.

4 Result and Discussion

To evaluate the performance of the proposed AEFS-KENN model with the benchmark schemes, simulations are carried out in this subsection. Online network-based datasets are widely available for the research community to train and test their methods for

Algorithm 3 PBO

Input: Polar population p_n

Output: Optimal paramaters δ

Procedure:

- Initialize polar bears nature population, $\bar{p} = (p_0, p_1, \ldots, p_{g-1})$.
- Then, the population to grid behavior $\left(\bar{p}_j^t\right)^k$ is modeled by using Eq. (20).
- Distance among the polar bears $\text{dist}\left(\left(\bar{p}_j^t\right)^k, \left(\bar{p}_j^t\right)^j\right)$ is estimated according to the Euclidian metrics as given in Eq. (21).
- Parameters such as the parameters of distance of vision ∂ in the range of (0, 0.3) and angle of tumbling Ψ_0 at random in the range of $(0, \pi/2)$ are selected.
- Based on these limits, radius of vision $\check{r}$ is computed as shown in Eq. (22).
- The obtained radius value is utilized to calculate movement in local search space for each spatial coordinate as illustrated in Eq. (23).
- Depending on the value of k, the individuals are eliminated, whereas the reproduced individual is represented as shown in Eq. (24).

the detection of abnormal network behaviors on various platforms. Moreover, obtaining the suitable dataset with the correct data properties in terms of usability format and labelling results is not an easy operation. It should contain current attack scenarios, such as botnet, brute force, DoS, etc. In this study, the proposed AEFS-KENN security model is validated and tested by using smart grid big datasets such as power system dataset[52–54], State Grid Corporation of China (SGCC) dataset, CICIDS 2017, Industrial Control System (ICS), and UNSW-NB 15[55–58]. Here, several machine learning algorithms in the current research works have been used for comparison with the above mentioned datasets. This is due to the fact that these datasets include a variety of recent attack instances that satisfy the real-world requirements, and also they are open to the public. The ICS cyber-attack dataset for power systems is also utilized because it represents the different types of assaults on platforms used in power systems. The percentage of attack occurrences is greater than that of occurrences of normal behavior, in contrast to the preceding datasets.

Furthermore, the test error, accuracy, false positive rate, detection rate, loss, f1-score and precision are the different indicators that are primarily used to evaluate the smart grid intrusion detection algorithm. The term True Positive (TP) indicates the quantity of normal sorts that accurately recognized themselves as normal types and triggered smart grid attack detection. Then, False positive (FP) is a term used to describe the number of false alarms that are wrongly identified as the right kind of alarm and the provoked smart grid attack detection. The number of abnormal alerts that triggered the smart grid attack detection and were accurately classified as abnormal alarms is known as true negative (TN). Moreover, the False negative (FN) refers to the proper kind of numbers that triggered the smart grid attack detection but were incorrectly recognized as an abnormal notification. The evaluation parameters are computed by using the following equations:

$$\mathrm{ACC} = \frac{\mathrm{TP} + \mathrm{TN}}{\mathrm{TP} + \mathrm{TN} + \mathrm{FP} + \mathrm{FN}} \tag{25}$$

$$\mathrm{PRE} = \frac{\mathrm{TP}}{\mathrm{TP} + \mathrm{FP}} \tag{26}$$

$$\mathrm{REC} = \frac{\mathrm{TP}}{\mathrm{TP} + \mathrm{FN}} \tag{27}$$

$$\mathrm{DR} = \frac{\mathrm{TP}}{\mathrm{TP} + \mathrm{FN}} \tag{28}$$

$$\text{F1-score} = \frac{2 \times \mathrm{TP}}{2 \times \mathrm{TP} + \mathrm{FP} + \mathrm{FN}} \tag{29}$$

$$\mathrm{FPR} = \frac{\mathrm{FP}}{\mathrm{TN} + \mathrm{FP}} \tag{30}$$

where TP – true positives, TN – true negatives, FP – false positives, FN – false negatives, ACC – accuracy, PRE – precision, REC – recall, DR – detection rate, and FPR – false positive rate.

Typically, the precision relates to how well the measurements agree with one another, whereas accuracy refers to the proportion of all correctly classified items. Recall quantifies the proportion of true positives that are labelled as assaults. FPR calculates the proportion of regular traffic that is marked as an attack on regular network data. The test accuracy is gauged by the F1-score. The TPR and FPR trade-off employing a different probability threshold is summarized by the Area Under the ROC Curve (AUC), which measures the size of the area under the Receiver Operating Characteristics (ROC) curve.

The confusion matrix and evaluation indices of the proposed AEFS-KENN method for both CICIDS and UNSW-NB 15 datasets are shown in Figs. 4 and 5, respectively. Accurate detection performance is influenced by the amount of labelled data used in the training process. By using the confusion matrix, performance is assessed based on the ability to classify network data into the appropriate attack patterns. The similarity between the true label and the predicted label can be represented based on a confusion matrix. Based on the predicted classes, it is stated that the proposed AEFS-KENN model performs better with reduced false positives.

Figure 6 depicts the convergence analysis of the proposed PBO technique used in the security framework. Based on the improved convergence rate, the performance and optimization efficiency of the algorithm have been determined. Similarly, the ROC of the proposed AEFS-KENN model with and without optimization process is assessed with respect to varying TPR and FPR as shown in Fig. 7. Overall, the observed results denote that the proposed framework provides an accurate prediction outcomes with the inclusion feature selection and RBF computation operations. Figure 8 shows the training and testing accuracy of the proposed AEFS-KENN model with respect to varying number of

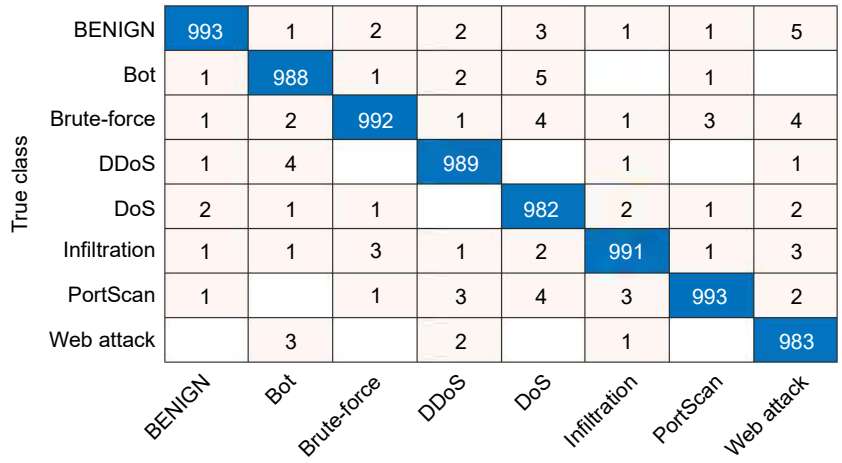

Fig. 4 Confusion matrix for CICIDS 2017 dataset.

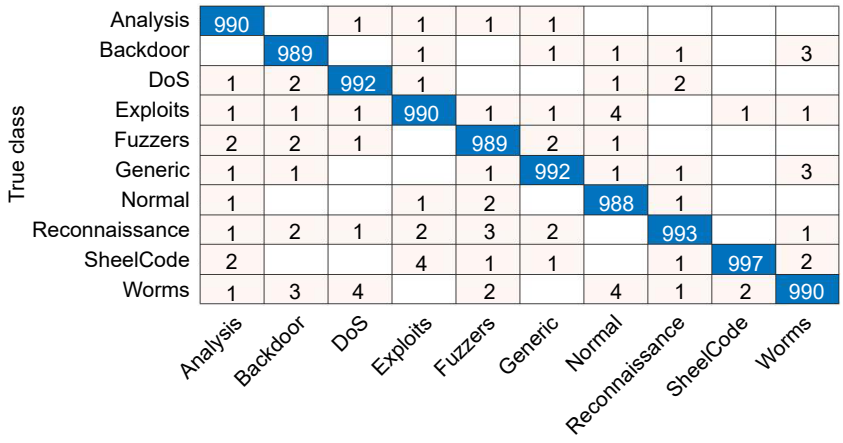

Fig. 5 Confusion matrix for UNSW-NB 15 dataset.

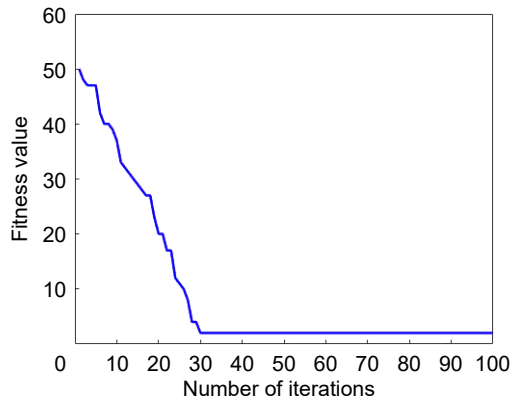

Fig. 6 Convergence analysis.

epochs. Similarly, the training and testing loss are also validated according to the number of epochs as shown in Fig. 9. The observed results indicate that the combination of proposed AEFS-KENN provides the better accuracy with low loss by accurately identifying the type of intrusions.

As shown in Fig. 7, the ROC of proposed security model is greatly maximized to 0.995 with optimization technique. Consequently, the training accuracy of the proposed technique is 0.999 and testing accuracy is 0.997, since the KENN technique could effectively predicts the normal and intrusion data with high training and testing accuracy by using the AEFS based feature selection methodology. Similarly, the training and testing loss factors of the AEFS-KENN is reduced up to 0.2% and 0% by properly detecting attacks from the given data, respectively.

Figure 10 compares the FPR and precision of the proposed AEFS-KENN technique with respect to training and testing models. The TP rate and FP rate are illustrated graphically by the ROC curve. It is employed to assess a classifier's effectiveness. The distribution of the deceptive class is distinguished from the fair class using the area under the ROC curve, or AUC. Based on the obtained results, it is stated that the

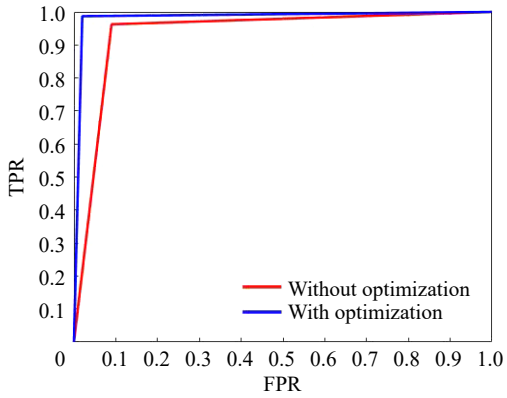

Fig. 7 ROC analysis.

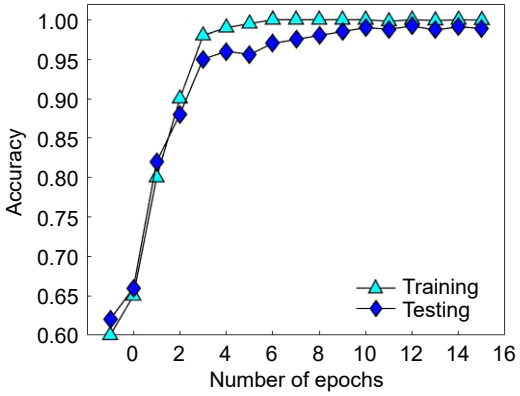

Fig. 8 Training and testing accuracy.

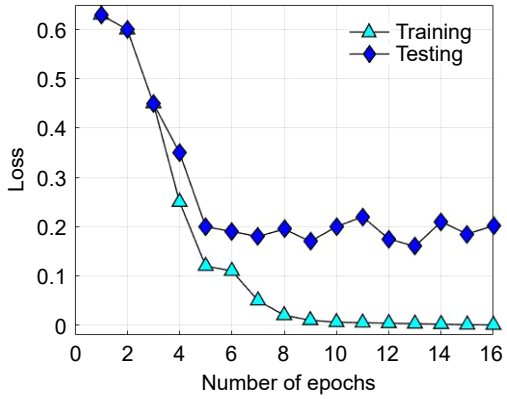

Fig. 9 Training and testing loss.

proposed KENN classifier provides an improved AUC and precision up to 0.99 with the inclusion of AEFS based feature selection model.

Figure 11 shows the precision, recall, and accuracy values of the proposed security model with respect to varying number of labeled data. Moreover, the overall comparative analysis among the traditional and proposed classification approaches are validated and contrasted by using the power system dataset as shown in Fig. 12. When compared to benchmark methods, the

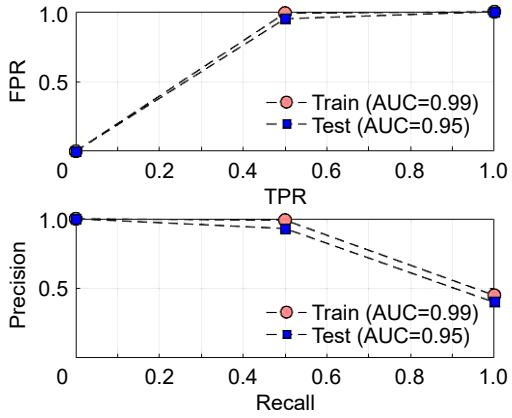

Fig. 10 Precision and FPR analysis.

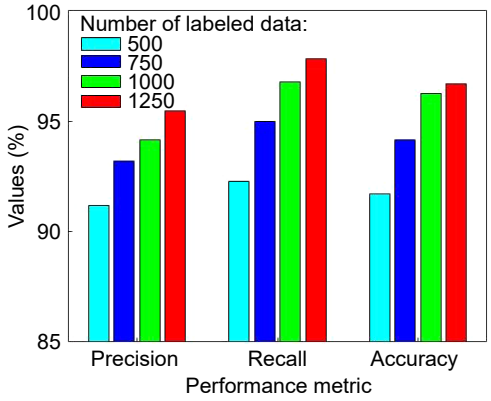

Fig. 11 Performance analysis with respect to number of labeled data.

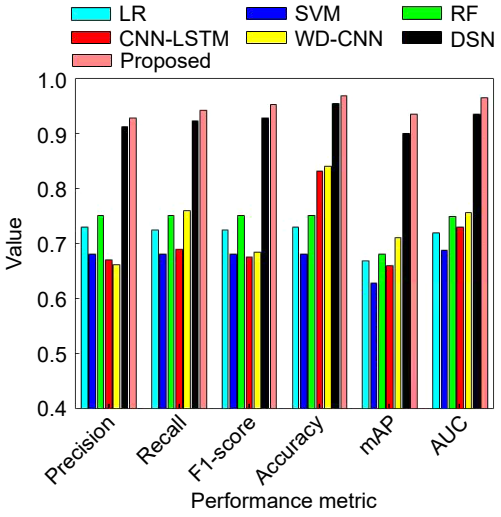

Fig. 12 Comparative analysis using power system dataset.

AEFS-KENN achieves the greatest values across the range for all performance parameters. Then, the detection accuracy of the standard and proposed classification models for the power system dataset is validated and compared as shown in Fig 13. Similarly,

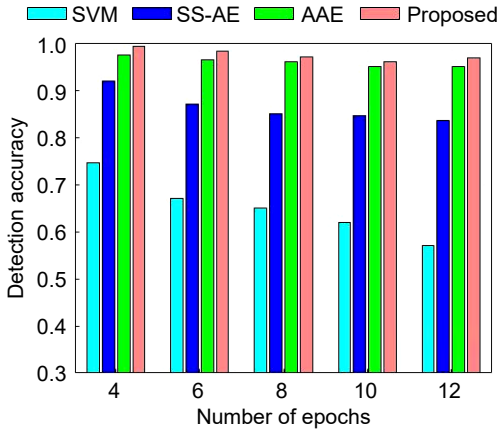

Fig. 13 Detection accuracy.

each performance statistic is detailed in order to better understand of its significance. All of the findings produced using the proposed classifier demonstrate an upward trend. The analysis of the results reveals that an increase in training instances improves the performance of classifiers.

In order to demonstrate the intrusion detection efficacy of the proposed AEFS-KENN model, the accuracy of several classifiers are validated and compared as shown in Figs. 14–16. Based on the improved level of accuracy, the overall performance of the security methodology has been determined. The AEFS-KENN method achieves accuracy for the CICIDS-2017 dataset of 0.999, while the other algorithms range from 0.560 to 0.900. The AEFS-KENN, on the other hand, produces the greatest results when using the ICS cyber-attack datasets, with an accuracy of 0.999, compared to other algorithms that

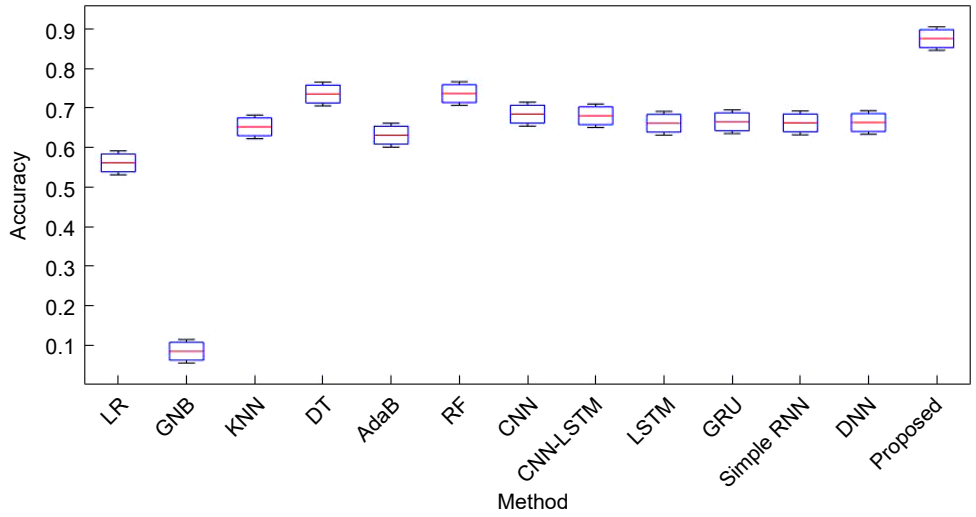

Fig. 14 Accuracy analysis using UNSW-NB 15 dataset.

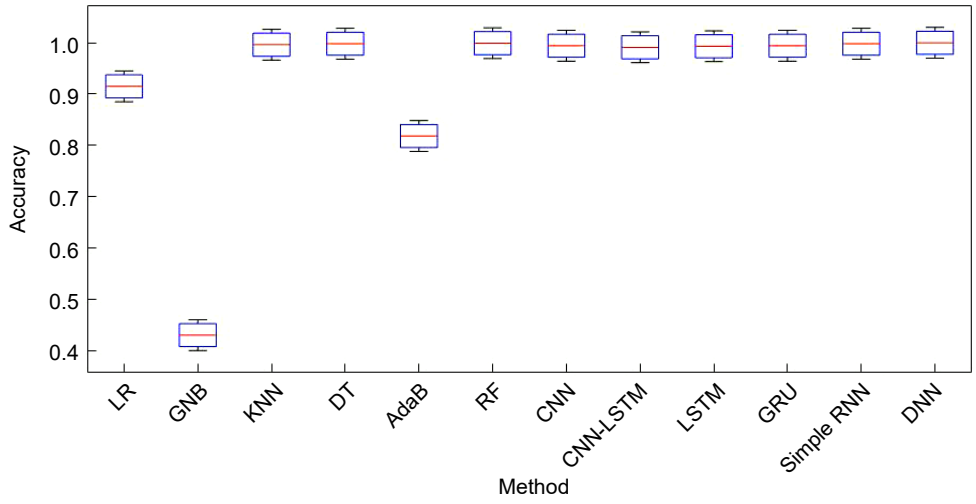

Fig. 15 Accuracy analysis using CICIDS-2017 dataset.

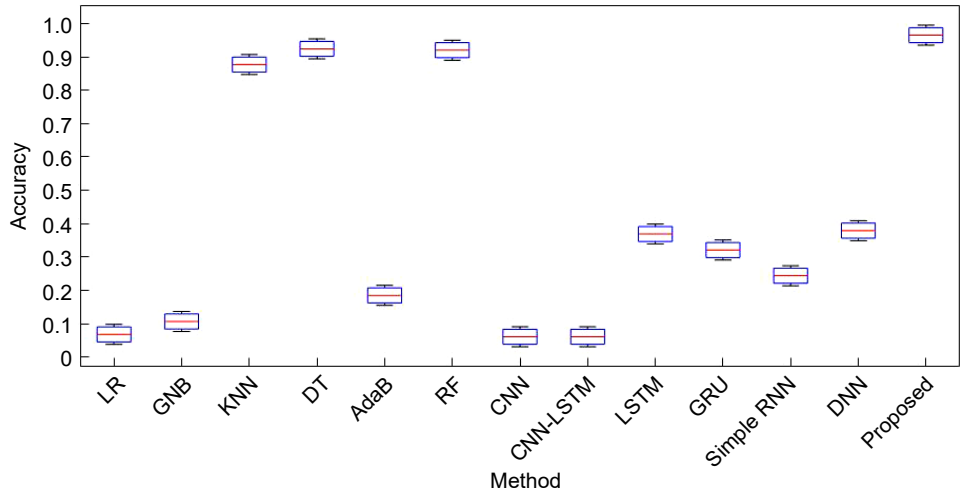

Fig. 16 Accuracy analysis using ICS dataset.

vary from 0.700 to 0.990.

Figure 17 validates the precision, recall and F1-score of several machine learning, deep learning and proposed classification models used for the intrusion detection. Similarly, Figs. 18–20 presents the overall comparative analysis of the existing and proposed models by using UNSW, CICIDS, and ICS dataset, respectively. The findings indicate that among other approaches utilized in this paper, the AEFS-KENN classification offers the best accuracy, precision, and recall. This might be because existing approaches are not more capable to handle the enormous amounts of data with better accuracy. But, the proposed AEFS-KENN utilizes an improved optimization integrated classification model for intrusion detection, which supports to obtain the better outcomes.

Overall, the obtained results state that the proposed AEFS-KENN technique provides an improved attack detection performance outcomes for all the big datasets used in this study. Here, the AEFS based feature selection and PBO based optimal parameter tuning are the major reasons for gaining improved performance outcomes, since it supports the classifier to make an accurate decision at the time of intrusion identification and class categorization.

5 Conclusion

In this paper, the new big data framework is created to detect intrusions in the smart grid systems with the use of AEFS-KENN techniques. The primary contribution of this research is the development of an original and trustworthy threat detection framework based on AI for enhancing smart grid system security. Here, the categorical data conversion is performed at first for converting numerical values based on label encoding. Since, the data, time, and time stamp attributes have no

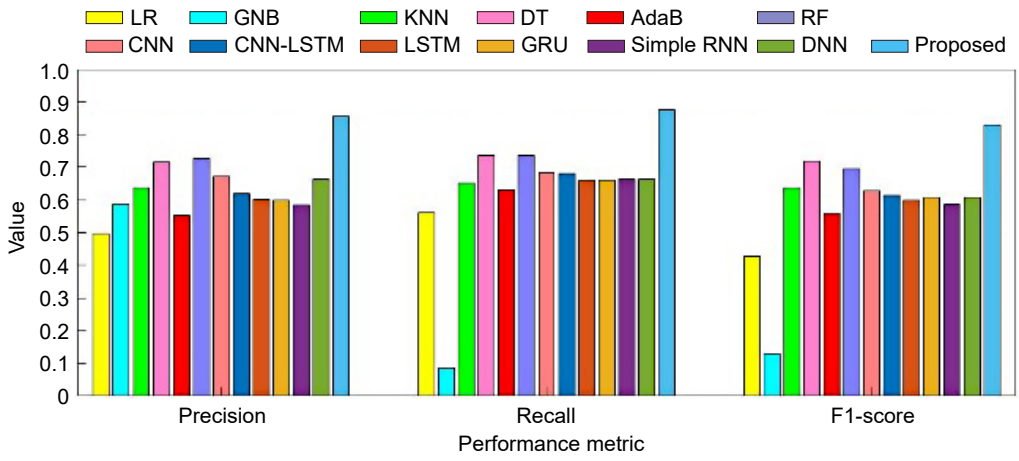

Fig. 17 Comparative analysis with other recent state of the art approaches.

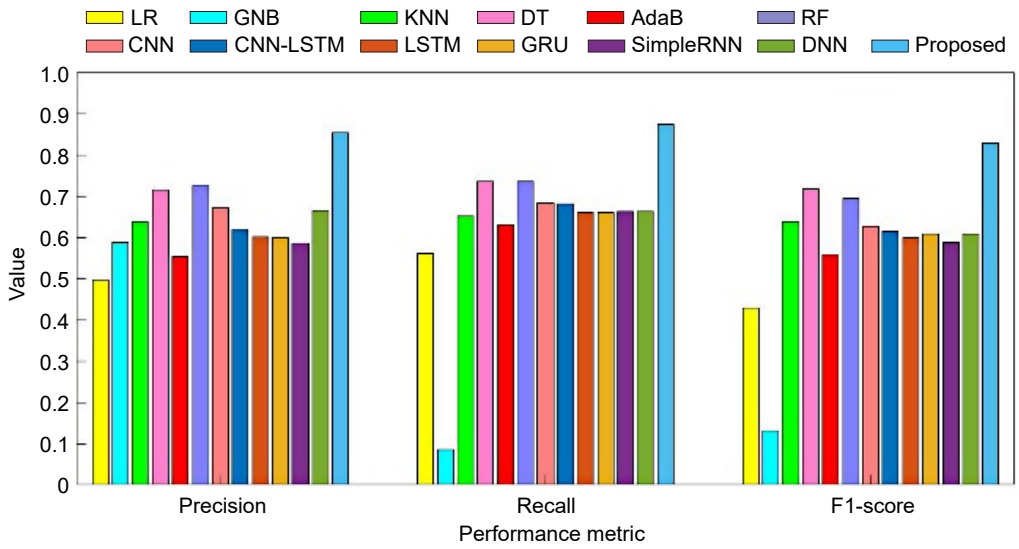

Fig. 18 Comparative analysis using UNSW-NB 15.

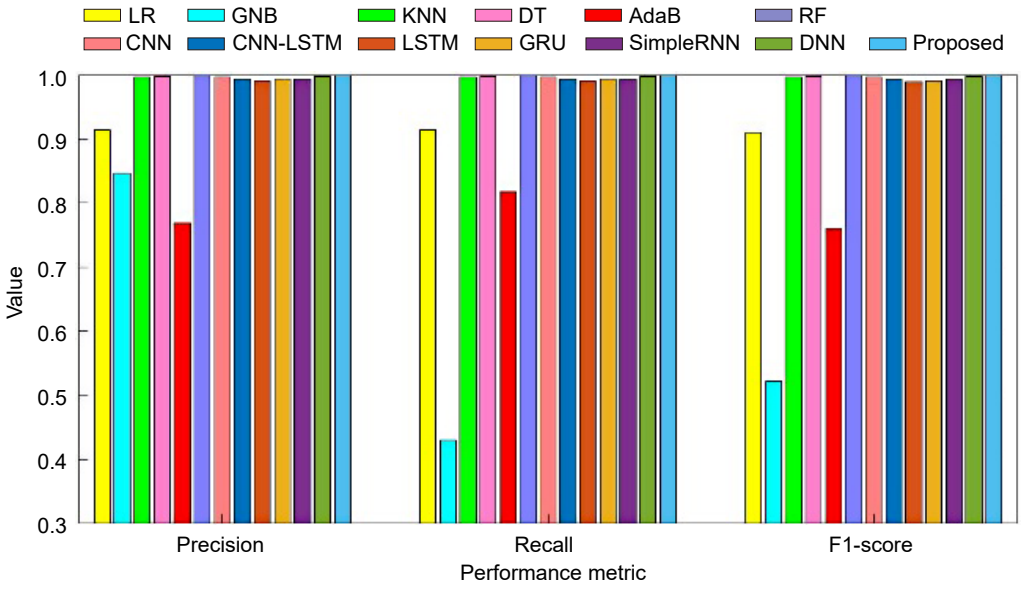

Fig. 19 Comparative analysis using CICIDS 2017.

influence on it, hence these information are eliminated during the preprocessing operation. After that, the best ideal features are selected from the large smart grid dataset with the use of AEFS mechanism incorporated with EMA function. Consequently, the obtained training data is modelled with the selected feature set, which is used for attack prediction and classification. To increase the precision of attack detection, this procedure included the estimation of the Gaussian distribution function, kernel matrix construction, computation of the radial basis function, and regression process. The PBO technique is applied in this study to compute the radial basis function as efficiently as possible. In this study, the proposed AEFS-KENN security model is validated and tested by using smart grid big datasets such as power system dataset, SGCC dataset, CICIDS 2017, ICS, and UNSW-NB 15. The current research efforts have used a number of machine learning techniques for comparison with the aforementioned datasets. This is owing to the fact that these datasets are public and contain a wide range of recent attack instances that meet the real-world requirements. To assess the performance outcomes, the proposed AEFS-KENN is validated and compared using a variety of parameters such as accuracy, precision, recall, f1-score, and loss values. The findings

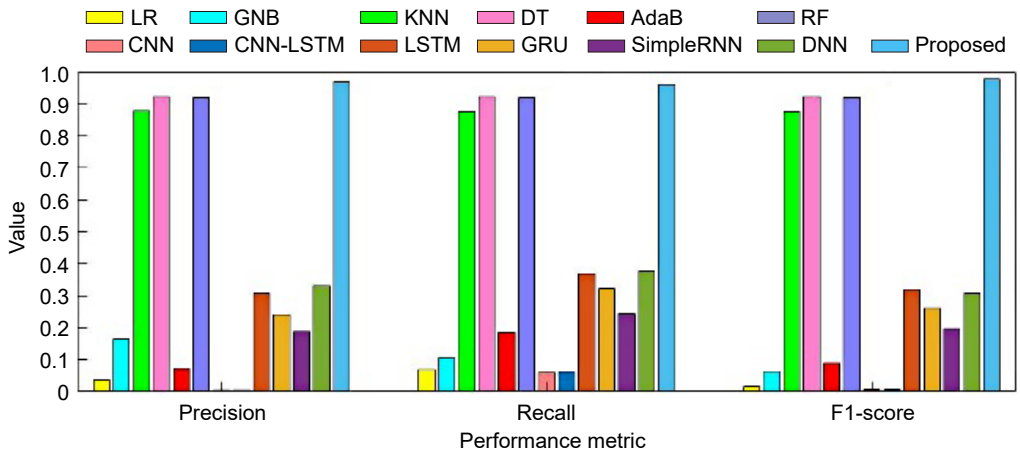

Fig. 20 Comparative analysis using ICS dataset.

indicate that the proposed AEFS-KENN technique outperforms other approaches with the average accuracy of 0.995, precision and recall of 0.990, low loss value of 0.002, and F1-score of 0.992. With the inclusion of AEFS technique, the proposed KENN classifier could accurately detect the disease with overall 0.990 of efficiency. In future, the current work can be extended by implementing a new cryptographic based framework for smart grid security.

References

[1] P. Ganesan and S. A. E. Xavier, An intelligent intrusion detection system in smart grid using PRNN classifier, *Intell. Autom. Soft Comput.*, vol. 35, no. 3, pp. 2979–2996, 2023.

[2] Y. Farhaoui, Design and implementation of an intrusion prevention system, *Int. J. Netw. Secur.*, vol. 19, no. 5, pp. 675–683, 2017.

[3] N. Sahani, R. Zhu, J. H. Cho, and C. C. Liu, Machine learning-based intrusion detection for smart grid computing: A survey, *ACM Trans. Cyber-Phys. Syst.*, vol. 7, no. 2, p. 11, 2023.

[4] P. Liao, J. Yan, J. M. Sellier, and Y. Zhang, Divergence-based transferability analysis for self-adaptive smart grid intrusion detection with transfer learning, *IEEE Access*, vol. 10, pp. 68807–68818, 2022.

[5] Y. Farhaoui, Intrusion prevention system inspired immune systems, *Indones. J. Electr. Eng. Comput. Sci.*, vol. 2, no. 1, pp. 168–179, 2016.

[6] S. Y. Diaba and M. Elmusrati, Proposed algorithm for smart grid DDoS detection based on deep learning, *Neural Netw.*, vol. 159, pp. 175–184, 2023.

[7] T. T. Khoei and N. Kaabouch, A comparative analysis of supervised and unsupervised models for detecting attacks on the intrusion detection systems, *Information*, vol. 14, no. 2, p. 103, 2023.

[8] M. N. Nafees, N. Saxena, A. Cardenas, S. Grijalva, and P. Burnap, Smart grid cyber-physical situational awareness of complex operational technology attacks: A review, *ACM Comput. Surv.*, vol. 55, no. 10, p. 215, 2023.

[9] Y. Farhaoui, Editorial, *Big Data Mining and Analytics*, vol. 6, no. 3, pp. 1–2, 2023.

[10] I. Ortega-Fernandez and F. Liberati, A review of denial of service attack and mitigation in the smart grid using reinforcement learning, *Energies*, vol. 16, no. 2, p. 635, 2023.

[11] M. Skoumperdis, N. Vakakis, M. Diamantaki, C. R. Medentzidis, D. Karanassos, D. Ioannidis, and D. Tzovaras, A novel self-learning cybersecurity system for smart grids, in *Power Systems Cybersecurity*: *Methods, Concepts, and Best Practices*, H. H. Alhelou, N. Hatziargyriou, and Z. Y. Dong, eds. Switzerland: Springer, 2023, pp. 337–362.

[12] Y. Farhaoui, Big data analytics applied for control systems, in *Proc. Int. Conf. Advanced Information Technology, Services and Systems*, Tangier, Morocco, 2018, pp. 408–415.

[13] Y. Farhaoui, Editorial, *Big Data Mining and Analytics*, vol. 5, no. 4, pp. 1–2, 2022.

[14] M. Ghiasi, T. Niknam, Z. Wang, M. Mehrandezh, M. Dehghani, and N. Ghadimi, A comprehensive review of cyber-attacks and defense mechanisms for improving security in smart grid energy systems: Past, present and future, *Electr. Power Syst. Res.*, vol. 215, p. 108975, 2023.

[15] L. Z. Velimirović, A. Janjić, and J. D. Velimirović, Machine learning applications in smart grid, in *Multi-criteria Decision Making for Smart Grid Design and Operation*: *A Society 5.0 Perspective*, L. Z. Velimirović, A. Janjić, and J. D. Velimirović, eds. Singapore: Springer, 2023, pp. 207–220.

[16] S. R. Devi, P. S. L. Kalyampudi, and N. S. Charitha, Cyber attacks, security data detection, and critical loads in the power systems, in *Smart Energy and Electric Power Systems*: *Current Trends and New Intelligent Perspectives*, S. Padmanaban, J. B. Holm-Nielsen, K. Padmanandam, R. K. Dhanaraj, and B. Balusamy, eds. Elsevier, 2023, pp.

169–184.

[17] S. S. Alaoui, Y. Farhaoui, and B. Aksasse, Hate speech detection using text mining and machine learning, *Int. J. Decis. Support Syst. Technol*., vol. 14, no. 1, p. 80, 2022.

[18] S. S. Alaoui, Y. Farhaoui, and B. Aksasse, Data openness for efficient e-governance in the age of big data, *Int. J. Cloud Comput.*, vol. 10, nos. 5&6, pp. 522–532, 2021.

[19] P. Liao, J. Yan, J. M. Sellier, and Y. Zhang, TADA: A transferable domain-adversarial training for smart grid intrusion detection based on ensemble divergence metrics and spatiotemporal features, *Energies*, vol. 15, no. 23, p. 8778, 2022.

[20] S. Mishra, Blockchain-based security in smart grid network, *Int. J. Commun. Netw. Distrib. Syst.*, vol. 28, no. 4, pp. 365–388, 2022.

[21] T. Kisielewicz, S. Stanek, and M. Zytniewski, A multi-agent adaptive architecture for smart-grid-intrusion detection and prevention, *Energies*, vol. 15, no. 13, p. 4726, 2022.

[22] C. Hu, J. Yan, and X. Liu, Reinforcement learning-based adaptive feature boosting for smart grid intrusion detection, *IEEE Trans. Smart Grid*, no. 14, pp. 3150–3163, 2023.

[23] Y. Farhaoui, Securing a local area network by IDPS open source, *Procedia Comput. Sci.*, vol. 110, pp. 416–421, 2017.

[24] A. Dehlaghi-Ghadim, M. H. Moghadam, A. Balador, and H. Hansson, Anomaly detection dataset for industrial control systems, arXiv preprint arXiv: 2305.09678, 2023.

[25] B. Kim, M. A. Alawami, E. Kim, S. Oh, J. Park, and H. Kim, A comparative study of time series anomaly detection models for industrial control systems, *Sensors*, vol. 23, no. 3, p. 1310, 2023.

[26] I. Ortega-Fernandez, M. Sestelo, J. C. Burguillo, and C. Piñón-Blanco, Network intrusion detection system for DDoS attacks in ICS using deep autoencoders, *Wirel. Netw*., doi: 10.1007/s11276-022-03214-3.

[27] E. Vincent, M. Korki, M. Seyedmahmoudian, A. Stojcevski, and S. Mekhilef, Detection of false data injection attacks in cyber–physical systems using graph convolutional network, *Electr. Power Syst. Res.*, vol. 217, p. 109118, 2023.

[28] Y. Farhaoui, Teaching computer sciences in morocco: An overview, *IT Prof.*, vol. 19, no. 4, pp. 12–15, 2017.

[29] D. Kaur, A. Anwar, I. Kamwa, S. Islam, S. M. Muyeen, and N. Hosseinzadeh, A Bayesian deep learning approach with convolutional feature engineering to discriminate cyber-physical intrusions in smart grid systems, *IEEE Access*, vol. 11, pp. 18910–18920, 2023.

[30] A. Abid, F. Jemili, and O. Korbaa, Real-time data fusion for intrusion detection in industrial control systems based on cloud computing and big data techniques, *Cluster Comput*., doi: 10.1007/s10586-023-04087-7.

[31] R. Chaganti, W. Suliman, V. Ravi, and A. Dua, Deep learning approach for SDN-enabled intrusion detection system in IoT networks, *Information*, vol. 14, no. 1, p. 41, 2023.

[32] C. I. Nwakanma, L. A. C. Ahakonye, J. N. Njoku, J. C. Odirichukwu, S. A. Okolie, C. Uzondu, C. C. Ndubuisi Nweke, and D. S. Kim, Explainable artificial intelligence (XAI) for intrusion detection and mitigation in intelligent connected vehicles: A review, *Appl. Sci.*, vol. 13, no. 3, p. 1252, 2023.

[33] S. Sossi Alaoui, Y. Farhaoui, and B. Aksasse, A comparative study of the four well-known classification algorithms in data mining, in *Proc. Int. Conf. Advanced Information Technology, Services and Systems*, Tangier, Morocco, 2018, pp. 362–373.

[34] D. Syed, A. Zainab, A. Ghrayeb, S. S. Refaat, H. Abu-Rub, and O. Bouhali, Smart grid big data analytics: Survey of technologies, techniques, and applications, *IEEE Access*, vol. 9, pp. 59564–59585, 2020.

[35] L. Cui, Y. Qu, L. Gao, G. Xie, and S. Yu, Detecting false data attacks using machine learning techniques in smart grid: A survey, *J. Netw. Comput. Appl.*, vol. 170, p. 102808, 2020.

[36] N. Kumar, G. S. Aujla, A. K. Das, and M. Conti, ECCAuth: A secure authentication protocol for demand response management in a smart grid system, *IEEE Trans. Ind. Inform*., vol. 15, no. 12, pp. 6572–6582, 2019.

[37] H. Karimipour, A. Dehghantanha, R. M. Parizi, K. K. R. Choo, and H. Leung, A deep and scalable unsupervised machine learning system for cyber-attack detection in large-scale smart grids, *IEEE Access*, vol. 7, pp. 80778–80788, 2019.

[38] A. Tarik and Y. Farhaoui, Recommender system for orientation student, in *Big Data and Networks Technologies*, Y. Farhaoui, ed. Switzerland: Springer, 2020, pp. 367–370.

[39] P. Rohini, S. Tripathi, C. M. Preeti, A. Renuka, J. L. A. Gonzales, and D. Gangodkar, A study on the adoption of wireless communication in big data analytics using neural networks and deep learning, in *Proc. 2nd Int. Conf. Advance Computing and Innovative Technologies in Engineering* (*ICACITE*), Greater Noida, India, 2022, pp. 1071–1076.

[40] S. Latif, Z. e Huma, S. S. Jamal, F. Ahmed, J. Ahmad, A. Zahid, K. Dashtipour, M. U. Aftab, M. Ahmad, and Q. H. Abbasi, Intrusion detection framework for the internet of things using a dense random neural network, *IEEE Trans. Ind. Inform.*, vol. 18, no. 9, pp. 6435–6444, 2022.

[41] H. Alkahtani and T. H. H. Aldhyani, Intrusion detection system to advance internet of things infrastructure-based deep learning algorithms, *Complexity*, vol. 2021, p. 5579851, 2021.

[42] R. Vijayanand, D. Devaraj, and B. Kannapiran, A novel deep learning based intrusion detection system for smart meter communication network, in *Proc. IEEE Int. Conf. Intelligent Techniques in Control, Optimization and Signal Processing* (*INCOS*), Tamilnadu, India, 2019, pp. 1–3.

[43] K. Zhang, Z. Hu, Y. Zhan, X. Wang, and K. Guo, A smart

grid AMI intrusion detection strategy based on extreme learning machine, *Energies*, vol. 13, no. 18, p. 4907, 2020.
[44] A. El Mouatasim and Y. Farhaoui, Nesterov step reduced gradient algorithm for convex programming problems, in *Big Data and Networks Technologies*, Y. Farhaoui, ed. Switzerland: Springer, 2020, pp. 140–148.
[45] P. R. Grammatikis, P. Sarigiannidis, G. Efstathopoulos, and E. Panaousis, ARIES: A novel multivariate intrusion detection system for smart grid, *Sensors*, vol. 20, no. 18, p. 5305, 2020.
[46] B. Li, Y. Wu, J. Song, R. Lu, T. Li, and L. Zhao, DeepFed: Federated deep learning for intrusion detection in industrial cyber–physical systems, *IEEE Trans. Ind. Inform.*, vol. 17, no. 8, pp. 5615–5624, 2021.
[47] M. Mahdavisharif, S. Jamali, and R. Fotohi, Big data-aware intrusion detection system in communication networks: A deep learning approach, *J. Grid Comput.*, vol. 19, no. 4, p. 46, 2021.
[48] I. A. Khan, M. Keshk, D. Pi, N. Khan, Y. Hussain, and H. Soliman, Enhancing IIoT networks protection: A robust security model for attack detection in Internet industrial control systems, *Ad Hoc Netw.*, vol. 134, p. 102930, 2022.
[49] J. E. Efiong, B. O. Akinyemi, E. A. Olajubu, G. A. Aderounmu, and J. Degila, CyberSCADA network security analysis model for intrusion detection systems in the smart grid, in *Advances in Intelligent Systems, Computer Science and Digital Economics IV*, Z. Hu, Y. Wang, and M. He, eds. Switzerland: Springer, 2022, pp. 481–499.
[50] E. Anthi, L. Williams, M. Rhode, P. Burnap, and A. Wedgbury, Adversarial attacks on machine learning cybersecurity defences in industrial control systems, *J. Inform. Secur. Appl.*, vol. 58, p. 102717, 2021.
[51] E. Anthi, L. Williams, P. Burnap, and K. Jones, A three-tiered intrusion detection system for industrial control systems, *Journal of Cybersecurity*, vol. 7, no. 1, p. tyab006, 2021.
[52] S. Bahadoripour, E. MacDonald, and H. Karimipour, A deep multi-modal cyber-attack detection in industrial control systems, in *Proc. IEEE Int. Conf. Industrial Technology* (*ICIT*), Orlando, FL, USA, 2023, pp. 1–6.
[53] S. Nagarajan, S. Kayalvizhi, R. Subhashini, and V. Anitha, Hybrid honey badger-world cup algorithm-based deep learning for malicious intrusion detection in industrial control systems, *Comput. Ind. Eng.*, vol. 180, p. 109166, 2023.
[54] A. Alzahrani and T. H. H. Aldhyani, Design of efficient based artificial intelligence approaches for sustainable of cyber security in smart industrial control system, *Sustainability*, vol. 15, no. 10, p. 8076, 2023.
[55] M. Panthi and T. K. Das, Intelligent intrusion detection scheme for smart power-grid using optimized ensemble learning on selected features, *Int. J. Crit. Infrastruct. Prot.*, vol. 39, p. 100567, 2022.
[56] Y. Zhang, J. Wang, and B. Chen, Detecting false data injection attacks in smart grids: A semi-supervised deep learning approach, *IEEE Trans. Smart Grid*, vol. 12, pp. 623–634, 2021.
[57] N. Javaid, N. Jan, and M. U. Javed, An adaptive synthesis to handle imbalanced big data with deep siamese network for electricity theft detection in smart grids, *J. Parallel Distrib. Comput.*, vol. 153, pp. 44–52, 2021.
[58] N. Elmrabit, F. Zhou, F. Li, and H. Zhou, Evaluation of machine learning algorithms for anomaly detection, in *Proc. Int. Conf. Cyber Security and Protection of Digital Services* (*Cyber Security*), Dublin, Ireland, 2020, pp. 1–8.

Sankaramoorthy Muthubalaji received the BEng degree in electrical & electronics engineering from University of Madras, India, the MEng degree in power electronics & drives from Anna University Chennai, India, and the PhD degree in power system engineering from Anna University Chennai, India. He is working as professor in CMR College of Engineering & Technology, India. His other research areas of interests are power electronics, intelligent techniques, power quality, smart grid, solar PV systems, distributed generation. He is a member of the Institution of Engineers (India). He received RULA Award 2018 for innovative researcher in power systems and the Institute of Scholar Research Excellence Award 2019. He is an editorial and review board member of many Scopus and SCI international journals.

Kavitha Thandapani currently works as a professor at Department of Electronics and Communication Engineering (ECE), Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Chennai, Tamilnadu, India. She received the BEng degree from Madurai Kamaraj University, India in 1999, the MEng degree in applied electronics from Anna University, India in 2004, and the PhD degree in information technology from Anna University, India in 2014. Her research interests are optical networking, wirelecommunication, antennas, and VLSI. She has published more than 50 research papers in referred international journals. She has published 45 papers in international and national conferences, and published 56 books and book chapters.

Naresh Kumar Muniyaraj received the BEng degree in electronics and communication engineering from Anna University, Chennai, India in 2005, the MEng degree in the specialization of communication systems from Anna University of Technology Coimbatore (university campus), India in 2010, and the PhD degree from Anna University, Chennai, India in 2017. He has started his career as lecturer in 2005, and now he is having around 17+ years of teaching and learning experience in the field of engineering education. Currently he is working as an associate professor at Department of Electronics and Communication Engineering, Vardhaman College of Engineering, Shamshabad, India. His three innovation international patents and one inventive (utility) Indian patent are granted, he has published 14 inventive patents, and two design patents are accepted in chosen fields. He received many awards for his excellent contribution on research and teaching, like Dr. Sarvepalli Radhakrishnan Best Teacher & Researcher Award 2022, Global Faculty Award, International Achievers Award and Gold Medal, Bharat Excellence Award and Gold Medal, Leading Educationist of India Award for Educational Excellence, Best Indian Golden Personalities Award in the Field of Education, Young Faculty in Engineering, Distinguished Scientist Award, Research Excellence Award, Honorable Jury Mention Certificate, Teaching Awards in Engineering by Staffordshire University, UK & Education Matters, etc. He has published around 40 national and international research articles. He has given around 20 technical, scientific, and motivational talks to young minds. His research area includes biomedical devices, wireless communication, satellite communication, IoT, and he is very much interest in design of inventive & innovative products.

Yousef Farhaoui is a professor at Faculty of sciences and Techniques, Moulay Ismail University, Morocco. He is the chair of IDMS Team and director of STI Laboratory, local publishing and research coordinator, Cambridge International Academics in UK. He received the PhD degree in computer security from Ibn Zohr University of Science, Morocco. His research interests include learning, e-learning, computer security, big data analytics, and business intelligence. He has three books in computer science. He is a coordinator and member of the organizing committee, a member of the scientific committee of several international congresses, and a member of various international associations. He has authored 7 books and many book chapters with reputed publishers, such as Springer and IGI. He is a reviewer for IEEE, IET, Springer, Inderscience, and Elsevier journals. He is also a guest editor of many journals with Wiley, Springer, Inderscience, etc. He has been the general chair, session chair, and panelist in several conferences. He is a senior member of IEEE, IET, ACM, and EAI Research Group.

Pasupuleti Rama Mohan currently works as an assistant professor at Department of Electrical and Electronics Engineering, Bharat Institute of Engineering and Technology, Hyderabad, Telangana, India. He received the BEng degree in electrical and electronics engineering from Sir MVIT College, Bangalore, Karnataka, India in 1999, the MEng degree in power electronics from BMS College of Engineering, Bangalore, Karnataka, India in 2002, and the PhD degree from JNTU, Anantapur, Andhra Pradesh, India in 2017. He has published around 30 research papers in various international and national journals and conferences. His research interests are power electronics, eectrical drives, and PWM techniques.

Sarvade Pedda Venkata Subba Rao currently works as a professor, he is the head Department of Electronics and Communication Engineering, Sreenidhi Institute of Science and Technology, Hyderabad, India. He received the PhD degree from Jawaharlal Nehru Technological University, Hyderabad, India in the area of wireless communications in 2014, the MEng degree in signal processing and communications from S. K University, India, and the BEng degree in electronics and communication engineering from JNTU Hyderabad, India. His research areas include data communications and networking, ad-hoc wireless networks, signal processing, 5G wireless networks, Internet of things, and development of micro satellite. He is editorial board member of *International Journal of Distributed and Parallel Systems* (*IJDPS*), *International Journal of Wireless and Mobile Networking* (*IJWAMN*), *Journal of Advanced Electronics*, and *Signal Processing & Communication* (*JAESPC*). He is a reviewer of *IEEE Sensor Letters*.

Thangam Somasundaram currently serves as an assistant professor at School of Computing, Amrita Vishwa Vidyapeetham, Bengaluru, India. She received the PhD degree in computer science and engineering from Anna University, Chennai. India. She has 22 years of teaching experience. She has presented number of papers in conferences and journals. Her areas of interest are system software, IoT, artificial intelligence, machine learning, service oriented architecture, and computer architecture.