Signal, Image and Video Processing
https://doi.org/10.1007/s11760-023-02813-7

ORIGINAL PAPER

Detection of cyber-attacks on smart grids using improved VGG19 deep neural network architecture and Aquila optimizer algorithm

Ahmed Abdulmunem Mhmood[1] · Özgür Ergül[1] · Javad Rahebi[2]

Received: 30 July 2023 / Revised: 1 September 2023 / Accepted: 25 September 2023

Abstract

This study introduces an innovative smart grid (SG) intrusion detection system, integrating Game Theory, swarm intelligence, and deep learning (DL) to protect against complex cyber-attacks. This method balances training samples by employing conditional DL using Game Theory and CGAN. The Aquila optimizer (AO) algorithm selects features, mapping them onto the dataset and converting them into RGB color images for training a VGG19 neural network. AO optimizes meta-parameters, enhancing VGG19 accuracy. Testing on the NSL-KDD dataset generates remarkable results: 99.82% accuracy, 99.69% sensitivity, and 99.76% precision in detecting attacks. Notably, the CGAN technique significantly improves performance over GAN. Importantly, this method surpasses various deep learning techniques such as VGG19, CNN-GRU, CNN-GRU-FL, LSTM, and CNN in accuracy. Addressing the critical need for robust SG intrusion detection, our work merges Game Theory, swarm intelligence, and deep learning, yielding superior security accuracy. The novelty of this study is implanted in the integrated approach, distinguishing it from previous research and contributing to effective protection against cyber threats in smart grids.

Keywords Cyber-attacks · Smart grid · Intrusion detection system · Deep learning · VGG19 architecture · Swarm intelligence

1 Introduction

The Internet of things (IoT) is an intelligent communication network that uses IoT networks and smart devices with various sensors to communicate with other network components. In this smart grid, data is created by sensors and sent to cloud layer services and servers through an intelligent communication network [1]. The Internet of things has a multi-layered architecture. The lowest level of the IoT is the perception layer, which has many smart devices. The higher layer is the network or fog layer, which performs some processing and sends pre-processed data to the highest layer. The highest layer is the cloud layer, which has different servers for storing information and providing intelligent cloud services [2]. The IoT is used in various applications, including transportation networks [3], agriculture [4], smart cities [5], and power grids [6].

A smart grid (SG) is one of the new application networks of the IoT. The SGs use information about the power grid to evolve and increase grid efficiency. The smart grid uses advanced sensors to improve energy systems' performance and reliability [7]. Power companies optimize electric power production, circulation, transmission, and control using smart grids' valuable information. A smart grid increases the abilities of engineers and technicians to analyze the electricity distribution networks and discover network faults faster. The smart grid makes more accurate predictions of electricity consumption in future. Using different energy production sources and combining them to increase productivity is one of the smart grid applications [8]. For an efficient power distribution system, controls of power generation resources are optimized through intelligent technologies. A smart grid intelligently integrates diverse technologies to improve power distribution systems' control and monitoring mechanisms [9]. Intelligent energy distribution networks

✉ Javad Rahebi
cevatrahebi@topkapi.edu.tr

Ahmed Abdulmunem Mhmood
ahmedabd.mahmood@gmail.com

Özgür Ergül
ergul@gazi.edu.tr

[1] Department of Electrical-Electronics Engineering, Faculty of Engineering, Gazi University, Ankara, Turkey

[2] Software Engineering Department, Istanbul Topkapi University, Istanbul, Turkey

Published online: 17 November 2023

develop in countries with scarce natural resources, such as oil, coal, or rare gases. Smart grids have different goals; the primary purpose of a smart grid is to integrate as many production facilities based on renewable energy sources [10]. According to studies, countries that want to advance must have a smart electricity system that can adequately, intelligently, and dynamically respond to infrastructure changes and consumer demand [11]. Smart grids guarantee energy security, economic growth, and environmental protection. Smart grids take into account technological advancements to boost dependability, availability, and efficiency, as well as to improve the global economy and protect the environment [12].

In smart grids, two-way data and power flows are based on modern communication and digital technologies. The purpose of the smart electricity network is to transform the traditional electricity network into a new and advanced network with the help of information and communication technology. It was impossible to transfer extensive data through traditional electricity networks because they used high-voltage transmission cables [13]. Different electrical components, such as transmission lines, transformers, substations, etc., are used in electricity distribution networks [14–16]. Traditional power distribution networks do not have large-scale energy storage facilities. Using renewable energy is one of the goals of smart grids. They connect electrical and digital data, unlike the traditional electricity transmission network. However, using digital technologies to send various data types in smart grids has increased data security challenges for power networks [17].

The infrastructure of smart grids depends on their communication systems, and any disruption in these systems can disrupt the entire smart grid function. The communication systems used in a smart grid are highly vulnerable to cyber-attacks. Cyber security in smart grids is a critical problem. It refers to data confidentiality, availability, and integrity in systems or smart devices connected to the Internet [18].

Cyber-attacks on the power system encompass diverse forms, including Malware, Denial-of-Service (DoS), Phishing, Man-in-the-Middle (MitM), and Physical attacks [19]. Power flow analysis and system configuration are crucial for detecting potential cyber-attacks on electric power systems [20]. The article emphasizes identifying vulnerable points in power systems against cyber-attacks and introduces static indicators for effective addressing. The proposed strategy involves integrating microgrids to enhance power system flexibility, decentralization, and counter targeted cyber-attacks, showcasing reduced outages and improved stability with distributed generators [21].

One of the motivations behind providing an intrusion detection system for smart grids is the increasing number of attacks on these networks. Studies show that cyber-attacks on smart grids have increased in recent years. Power interruptions and theft of subscribers' personal information are two effects of attacks on smart grids. In 2015, cyber-attacks on the power grids in Ukraine led to significant power disruptions that lasted for several hours. Estimates show that a cyber-attack on London's electricity network caused a loss of around 111 million pounds per day. The mentioned attacks negatively affected the lives of 1.5 million people [22]. With the digital development of smart grids, their level of vulnerability has increased, so it is necessary to provide intelligent approaches to deal with these attacks. The significant damage caused by attacks on the smart grids, widespread power outages, and disruptions in economic activities make these networks need smart intrusion detection systems.

An intrusion detection system (IDS) increases the security of smart grids against attacks. Although the provided intrusion detection systems effectively detect attacks on the smart grids, it is vital to provide more advanced approaches. Attacks on smart grids are evolving and improving, and for this reason, there is a need for hybrid methods based on artificial intelligence and group intelligence. Combining artificial intelligence and group intelligence in intrusion detection systems reduces their false alarm rate while detecting attacks. Deep learning processes, including long- and short-term memory (LSTM) [23], convolutional neural network (CNN) [24], and recurrent neural network (RNN) [25], are effective in detecting Smart grid attacks. However, their error rate can be significant. Swarm intelligence methods increase their accuracy in detecting attacks to reduce the error of deep learning methods [26]. This manuscript presents an intrusion detection system for smart grids by combining swarm intelligence and deep learning. The proposed penetration detection system aims to reduce attack detection errors and increase the security of smart grids. Reducing losses caused by attacks and timely detection of attacks are other goals of this research.

The research also presents a new and advanced approach to detecting attacks in the smart grid. First, the proposed method uses the deep learning method based on Game Theory to balance the dataset [27]. Balancing the dataset reduces the intrusion detection error. Intrusion detection datasets have many features, some of which are low values and cause the learning accuracy to decrease. A new Aquila optimizer (AO) algorithm-based method [28] has been presented that performs feature selection. Another innovation is converting selected features into RGB images for CNN neural network learning and VGG19 architecture. In the proposed method, the samples selected in the dataset are converted into color images and chosen as the input of VGG19. The role of CNN is to classify traffic into anomalous and normal categories. Another innovation is optimizing CNN parameters with the Aquila optimizer (AO) algorithm. The reasons behind using the Golden Eagle algorithm for feature selection and optimization of CNN parameters to reduce intrusion detection errors are as follows:

- The AO algorithm was presented in 2021 and has been used in advanced research.
- The AO algorithm includes exploitation and exploration searches.
- The AO algorithm is more accurate than some popular algorithms (genetic algorithms (GA) and particle swarm optimization (PSO)).
- The AO algorithm modeling is compelling and can search complex spaces.

The main contributions of the authors are summarized as follows:

- Balancing dataset samples with neighborhood information and deep learning based on Game Theory.
- Presenting a binary version of the Aquila optimizer (AO) algorithm for feature selection in attack detection.
- Coding the selected features of the dataset in the form of RBG color images for CNN training.
- Using the advanced VGG19 architecture in combination with the Aquila optimizer (AO) algorithm to detect attacks.
- Reducing the attack detection error in the VGG19 architecture by optimizing the neural network parameters with the Aquila optimizer (AO) algorithm.
- Applying the conditional version of GAN to balance the dataset.

This research paper has five sections. Section I introduces some key concepts. Section II explains the smart grids and their components and reviews related studies on network attacks and detection. Section III includes the proposed intrusion detection system to protect smart grids. Section IV presents the proposed approach to the implementation and analysis of experiments. Section V offers the conclusion and suggestions for future work.

2 Relevant works

Different energy sources provide electricity, including nuclear power plants, thermal power plants, hydroelectric power plants, gas power plants, solar cells, and wind turbines. Businesses, factories, and homes consume electricity and the energy produced in the power grid system. Figure 1 shows the elements involved in smart grids. An overview of the players in the smart grid environment is shown in Fig. 1. In Singapore, consumers are allowed to make and use energy [29].

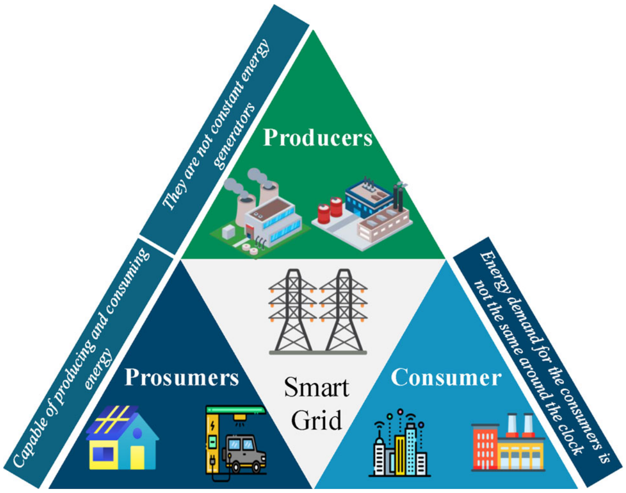
They are not constant energy generators
Producers
Capable of producing and consuming energy
Prosumers
Smart Grid
Consumer
Energy demand for the consumers is not the same around the clock

Fig. 1 Smart grid beneficiaries [29]

Producers can use solar panels and wind turbines to generate electrical energy, so in smart networks, energy flow between the grid and suppliers is two-way. In a smart grid, power is generated through both sources and consumers. The excess electrical energy produced through wind, thermal, and solar resources is injected into the main grid. The main advantage of smart grids is the exchange of data in this network in and to the power exchange. The data transmitted in smart grids can include the information and data of users and subscribers. Establishing a smart grid lets the producers know the actual energy needs of the consumers [29, 30].

Knowing the amount of energy consumed allows a generator to generate enough power. Electrical equipment, smart meters, and sensors installed in consumer centers are used to acquire the data the producer needs [30]. Security issues and network intrusions are two of the difficulties smart grids face. Besides, attackers may enter the network to attack the system. Attacks on the smart grids are classified into active and passive attacks. In passive attacks, no damage is done to network data. Attackers who use passive methods analyze the data. Active attacks are more harmful than passive ones because they manipulate and alter the data [31]. According to a study [31], there are five primary objectives for cybersecurity in smart grids:

- User authentication and verification allow only authorized users to enter the system.
- User authorization will enable users to access only authorized information.
- Confidentiality of access to information makes the attacker unable to manipulate user data.
- Data integrity.
- The availability of user data allows users to access their data and information at any time.

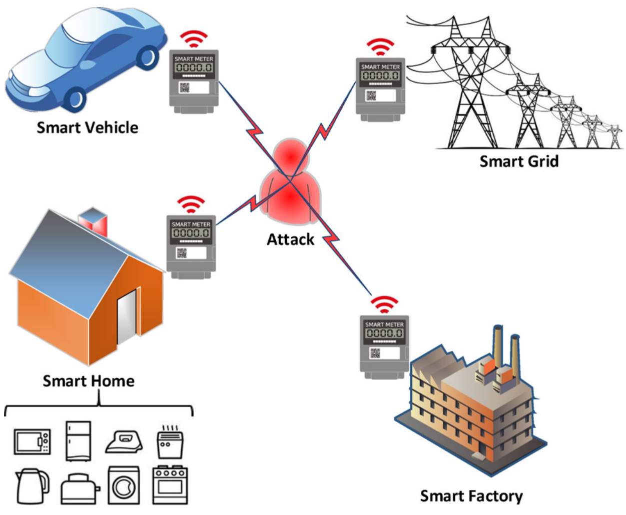

Fig. 2 Attack on smart grid infrastructure [32]

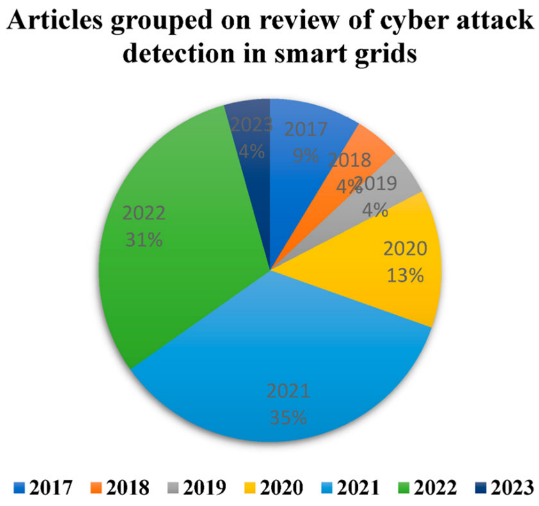

Fig. 3 Increasing number of smart grid cyber-security publications [36]

Figure 2 shows the cyber-attack on a smart grid. The hacker tries to attack smart meters and manipulate their data.

Cyber-attacks on smart grids have happened several times and caused widespread shutdowns or disruptions in the smart grids. For instance, successful assaults on the Ukrainian electrical infrastructure were launched in 2015 and 2016. Attackers gained access to the operator consoles of the distant distribution network during these incidents, causing extensive blackouts. The blackout affected approximately 230,000 persons. This cyber-attack was the first successful one on a smart grid [31].

Another example of an attack is the attack on Iran's nuclear facilities in 2010. In this attack, the Stuxnet caused many centrifuges to burn in Iran's Natanz uranium enrichment plant [33].

Another instance of an assault on the smart grid was the 2003 blackout in the USA and Canada. A high-voltage power line in Ohio struck some trees in 2003, resulting in a widespread loss of electricity. As a result of this disaster, estimated to have cost $6 billion and caused a total power loss for 50 million people over two days, at least 11 people died [34].

Another example is the 2011 blackout between Southern California and Arizona. The Arizona–Southern California blackout of September 8, 2011, disturbed the lives of 2.7 million people. On hot days, demand rises during peak hours, and as a result of this rise in demand, a high-pressure line fails because of a flaw that causes this issue [35].

Attacks on smart grids cause damage to the infrastructure, and for this reason, the number of cyber-security papers has increased in the last few years, as shown in Fig. 3.

An intrusion detection system is a valuable tool for identifying attacks on smart grids, which uses network traffic analysis to identify anomalies in traffic. Attacks on smart grids are detected utilizing blocklist approaches [37], heuristic techniques [38], and machine learning techniques [7]. Blocklist approaches have a database of network attack patterns, but they require a lot of memory and cannot detect zero-day attacks. The heuristic methods based on evidence and exploratory functions recognize the way of attacks. However, their error rate is significant. Deep learning and machine learning methods can detect zero-day attacks and are widely used in designing intrusion detection systems. This section reviews and analyzes relevant works on attack detection in smart grids.

Previous research presents a deep learning approach with a feature selection mechanism to detect cyber-intrusion in smart grids. The researchers proposed a Bayesian approach integrated with CNN in attack detection. In this research, convolutional neural network layers are used for feature selection. Their method implements real-time industrial control system datasets, and experiments showed that their approach, based on long short-term memory (LSTM) and recurrent neural networks (RNN), is entirely accurate in detecting attacks.

A research publication describes the detection of assaults on smart grids using a federated learning-based methodology. They frame the challenge of anomaly detection as one of the classifications. In order to distinguish between regular and aberrant traffic, this study employs several centralized machine learning and federated learning algorithms. To find anomalies in three datasets, they used logistic regression, 1D CNN binary classifier, neural network classifier, RNN classifier, LSTM binary classifier, GRU binary classifier, and autoencoder binary classifier. The evaluations showed that the 1D CNN method is more successful in detecting attacks than other methods.

In a research work, the detection of attacks using the adversarial generative network has been proposed. This research proposes the utilization of an XGBoost classifier alongside a conditional generative adversarial network for the purpose of attack detection. For stable model learning, WCGAN and gradient penalty are utilized. The GAN's function is to balance the dataset. Wasserstein has a lower loss rate for accurately generated data than other GAN techniques. Their methodology was tested using the UNSW-NB15, NSL-KDD, and BoT-IoT intrusion detection datasets. Evaluations revealed that their approach is more effective at identifying assaults than random forest (RF), decision tree (DT), and support vector machine (SVM) methods. Their method is more accurate than the DGM technique that uses GAN.

Another work presented a DDoS detection method using the SDNs' physical and cyber-systems. This method uses information entropy and unsupervised anomaly detection techniques to detect suspicious aspects and identify DDoS attacks. Their approach has a 99.13% average accuracy rate for identifying DDoS attacks. Their strategy lowers the false-positive rate by 35%–59% compared to other comparable efforts.

A research publication presented a blockchain platform to reduce attacks on smart grids. Their experiments show that even under high-impact attacks, their approach has a high ability to detect attacks.

In another work, a solution was found using an improved firefly algorithm and a convolutional neural network for identifying distributed denial-of-service attacks in an SDN-IoT environment. The firefly method is used in this study to enhance the ability of the convolutional neural network to recognize DDoS attacks. Tests revealed that their process of identifying attacks had a 98% accuracy rate.

Previous research presents a machine learning-based intrusion detection approach for identifying attacks on smart grids. Their proposed system detects attacks in real-time using Arduino, Zigbee, and Raspberry Pi voltage and current sensors. The mentioned research collected Zigbee data through XCTU and delivered it as input to machine learning algorithms. The evaluations showed that the Gaussian support vector machine is more accurate in detecting attacks than other algorithms.

In a research paper, an intrusion detection method is presented based on the SMOTE and the extremely randomized trees (ET) methods for smart grids' cyber-security. The proposed method uses a random tree classifier based on SMOTE for intrusion detection.

The suggested framework offers a multi-class classification of five types of network traffic, including regular, root-to-local, user-to-root, and denial-of-service attacks. The ET-SMOTE approach exhibits good accuracy in the NSL-KDD dataset, according to experiments.

In another work, the researchers presented an intrusion detection system for smart grids that uses five machine learning techniques. Tests showed that their intrusion detection system has an accuracy of 98.4%. The attack detection delay in their method is around 5 microseconds; the false-positive rate is 0.28%, and the false-negative rate is 1.32%.

A research work presents a hybrid decision tree-based solution for intrusion detection in smart grids. This approach combines three decision trees to find intrusions. Using the NSL-KDD dataset, experiments demonstrate that their strategy is more effective at identifying assaults than support vector machine, closest neighbor, and decision tree.

Another work presents an intrusion detection system for SDN-based smart grids that detects unusual traffic. In their method, local features are generalized by two-dimensional data using a CNN neural network. Two distinct datasets (UNSW_NB15 and KDDCup 99) are utilized to evaluate approach. According to experimental findings, they are more effective in detecting attacks than techniques like LSTM. Later, another work introduced an optimized feature selection method using the particle swarm optimization (PSO) algorithm to detect attacks. Their suggested strategy is implemented and examined using the benchmark datasets NSL-KDD and UNSW-NB15. They describe a deep learning-based anomaly detection algorithm that uses automatic encoders in each dataset. The results show that the F1 index in the NSL-KDD and UNSW-NB15 datasets is 92.09% and 92.90%, respectively.

A signature-based machine learning architecture for smart grid intrusion detection is presented in a study. This study integrates machine learning and signature-based techniques to detect attacks on smart energy grids. Their proposed system is highly capable of detecting intrusions on smart grid infrastructure.

In contrast to blocklisting and heuristic methods, machine learning and deep learning methods can detect zero-day attacks, as research on smart grids demonstrated. Signature-based intrusion detection systems offer higher detection rates, but adding rules and signatures to the list is time-consuming and requires a lot of memory. Machine learning-based intrusion detection systems can mitigate the drawbacks of signature-based systems but have high false-positive (FP) rates. Deep learning methods, such as CNN, have a higher level of learning than machine learning methods. Still, they have the following challenges to detect attacks accurately:

- CNN input should be in image format like RGB, but network traffic is not in the form of images.
- An imbalance in the dataset reduces the accuracy of CNN in detecting attacks.
- Failure to select the feature before learning by CNN increases the error and time of intrusion detection.

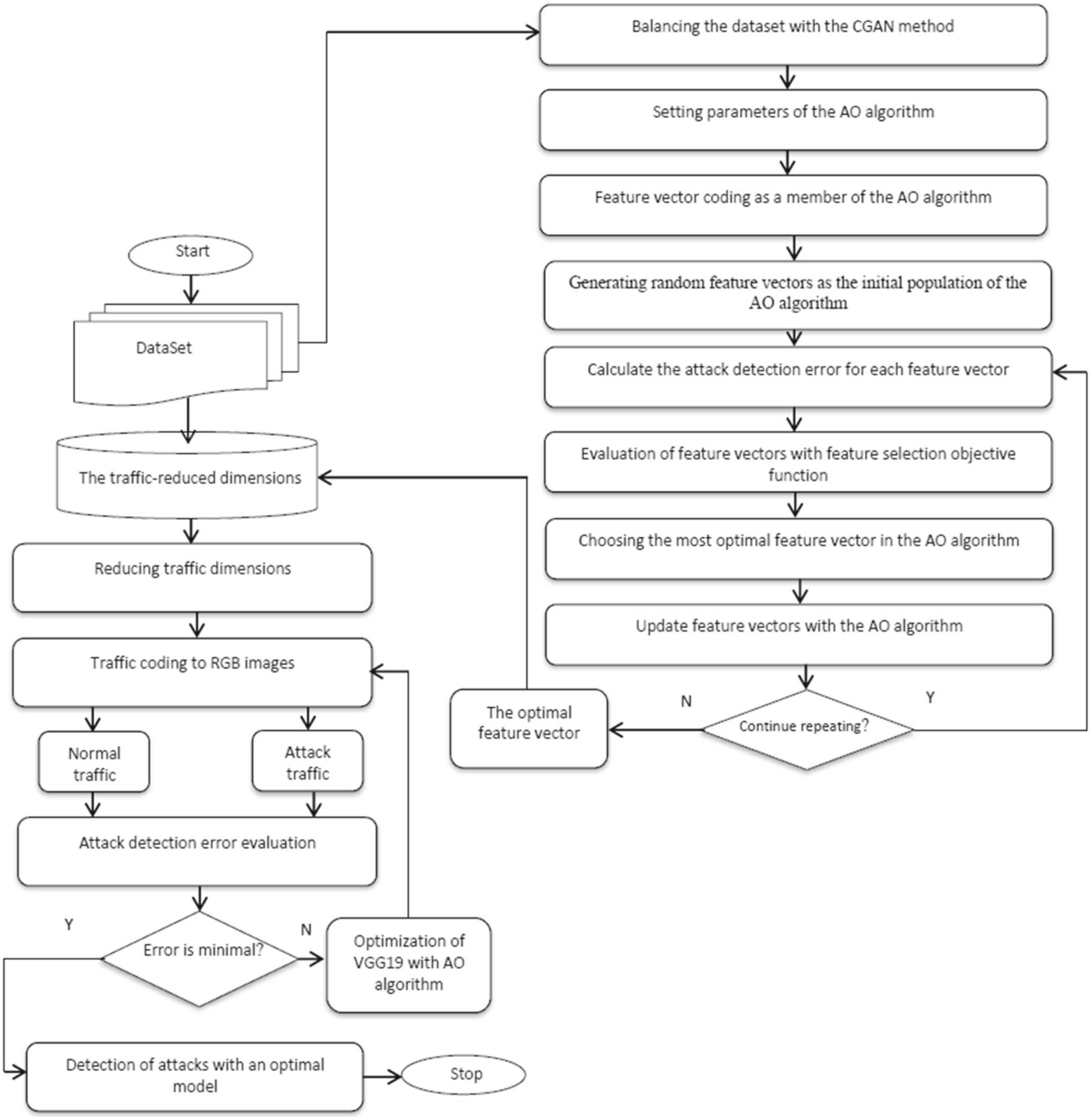
Start
DataSet
The traffic-reduced dimensions
Reducing traffic dimensions
Traffic coding to RGB images
Normal traffic
Attack traffic
Attack detection error evaluation
Y
Error is minimal?
N
Optimization of VGG19 with AO algorithm
Detection of attacks with an optimal model
Stop
Balancing the dataset with the CGAN method
Setting parameters of the AO algorithm
Feature vector coding as a member of the AO algorithm
Generating random feature vectors as the initial population of the AO algorithm
Calculate the attack detection error for each feature vector
Evaluation of feature vectors with feature selection objective function
Choosing the most optimal feature vector in the AO algorithm
Update feature vectors with the AO algorithm
N
Y
Continue repeating?
The optimal feature vector

Fig. 4 Framework of the proposed intrusion detection system or CAV

2.1 SCADA (Supervisory control and data acquisition)

SCADA systems generate comprehensive operational data concerning smart grid components. These data include power consumption, voltage, equipment status, and more. Integrating SCADA data into the feature selection step required identifying suitable features to increase the influence detection model's training. This integration helps to source SCADA information and enhances attack detection accuracy for smart grid SCADA components.

3 Methodology

The proposed method uses deep learning based on Game Theory and the VGG19 neural network to detect network attacks. It also involves swarm intelligence to improve performance and deep learning architecture. Figure 4 depicts the architecture of the proposed intrusion detection system, CGAN-AO-VGG19 (CAV), designed to detect smart grid attacks. The following stages comprise the proposed method to detect attacks on the smart grid:

- Balancing the dataset with CGAN.
- Feature selection with AO algorithm.

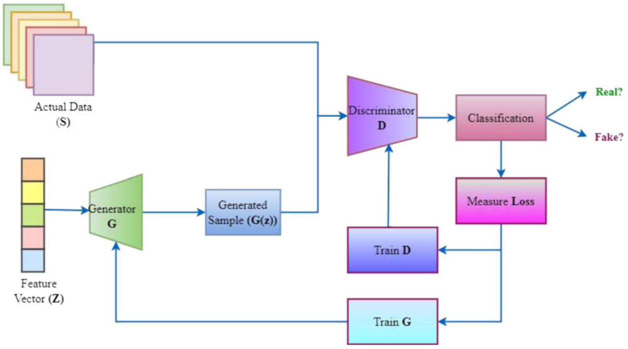

Fig. 5 Conditional performance of the GAN method in producing artificial and fake samples [27]

- Coding attack traffic and regular traffic in the form of RGB images.
- VGG19 neural network training with RGB images.
- Optimization of VGG19 neural network with AO algorithm.

3.1 Dataset balancing with game theory

Balancing the dataset is one of the challenges for intrusion detection systems in smart grids. Machine learning and deep learning increase output error when the data is unbalanced.

If the training data has a balance in benign and malignant traffic, the learning error in intrusion detection is reduced. One of the methods to balance the dataset is using deep learning based on the GAN. The GAN is designed based on game theory and has two parts: generator and discriminator. The productive role produces artificial and fake samples, and the discriminating role is classifying the samples into real and fake categories. If the generator can deceive the discriminator, it wins. In this case, the discriminator is deceived and puts fake and artificial samples in the category of actual examples. A GAN deep learning network presented in a research work [27] is of a conditional type, an improved version of GAN. Figure 5 shows the structure of the dependent version of GAN.

Let G be the generator; the input set is $S = \{s1, s2, \ldots,$ sn$\}$. G uses z to generate artificial samples. The role of the discriminator or D is to classify samples into fake and actual classes. If a fake sample created by G is similar to normal samples, D puts them in the standard class. G attempts to deceive D and make artificial data so that D classifies it as real. The objective function for the GAN method is shown in Eq. (1) [27]

$$\min_{g}\max_{\mathfrak{D}} V(g, \mathfrak{D}) = \mathbb{E}_{s-p(s)}\left[\log \mathfrak{D}(s)\right] + \mathbb{E}_{z\sim p(z)}\left[\log\left(1-\mathfrak{D}(g(z))\right)\right] \tag{1}$$

Here, $p(s)$ is the dispersion of the actual data, $g(z)$ generates noise samples, and z is the random value for creating fake samples. In this equation, $D(s)$ is the probability of a sample placed in the class of real samples. In a study [27], a new objective function for GAN is presented, and it is a conditional version of GAN, and according to Eq. (2), it is presented as follows:

$$\min_{g}\max_{\mathfrak{D}} V(g, \mathfrak{D}) = \mathbb{E}_{s\sim p(s)}\left[\log \mathfrak{D}(s|x)\right] + \mathbb{E}_{z\sim p(z)}\left[\log\left(1-\mathfrak{D}(g(z|x))\right)\right] \tag{2}$$

In this equation, x shows the details associated with each class instance. The Lipschitz method and Wasserstein distance are used so that artificial and fake models are more similar to standard samples to optimize CGAN. If the loss rate reaches about 0.5 or less than this threshold, the objective function of CGAN is formulated like Eq. (3) [27]:

$$V(g, \mathfrak{D}) = \max_{\mathfrak{D}}\Big\{\mathbb{E}_{s\sim p(s)}[\mathfrak{D}(s|x)] - \mathbb{E}_{s\sim p(g)}[\mathfrak{D}(s|x)] - \varphi\mathbb{E}_{s\sim p(\omega)}[\|\nabla_s\mathfrak{D}(s|x)\| - 1]^2\Big\} \tag{3}$$

The CGAN method balances the network traffic to generate artificial samples in the proposed method. CGAN checks the samples in the minority class, and their number balances the dataset.

3.2 Feature selection with AO algorithm

Learning on a balanced dataset is critical in reducing network attack detection errors. Feature selection is another fundamental factor in reducing the detection error of network attacks by intrusion detection systems. The proposed intrusion detection system uses an AO algorithm to select features. The reasons behind using the AO algorithm in the proposed intrusion detection system are as follows:

- It was presented in 2021 and is an advanced meta-heuristic algorithm.
- It has a simultaneous search, exploration, and exploitation mechanism.
- It has robust modeling.
- It is more accurate than standard meta-heuristic algorithms such as PSO and GA.

Each feature vector is a member of the AO algorithm in the proposed method. A random population of feature vectors,

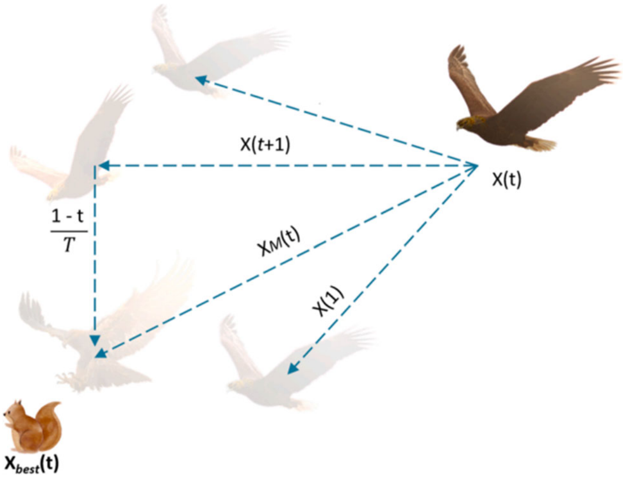

Fig. 6 Expanded exploration search [28]

according to Eq. (4), is created in the first step.

$$X = \begin{bmatrix} x_{1,1} & \cdots & x_{1,j} & x_{1,\text{ Dim - 1}} & x_{1,\text{ Dim}} \\ x_{2,1} & \cdots & x_{2,j} & \cdots & x_{2,\text{ Dim}} \\ \cdots & \cdots & x_{i,j} & \cdots & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ x_{N-1,1} & \cdots & x_{N-1,j} & \cdots & x_{N-1,\text{ Dim}} \\ x_{N,1} & \cdots & x_{N,j} & x_{N,\text{ Dim - 1}} & x_{N,Dim} \end{bmatrix} \quad (4)$$

In this equation, Dim is the number of dimensions of each feature vector and N is the number of feature vectors. Each row of Eq. (4) matrix is a feature vector with zero and one component. If a feature is selected, the component's value equals zero, and if it is not determined, its value is equal to one. Like the j's feature of the feature vector, the i's feature vector is displayed as X_{ij} . Equation 5 evaluates each feature vector.

$$F(X_i) = \mu_1 \times \frac{1}{n} E(X_i) + \mu_1 \times \frac{\|X_i\|}{41} \quad (5)$$

In Eq. (5), $\|X_i\|$ is the number of features selected by a feature vector X_i and $F(X_i)$ is the value of the objective function in feature selection. Any feature vector that minimizes the cost function is the optimal position in the AO algorithm. AO algorithm has two types: expanded exploration and narrowed exploration heuristic search.

Figures 6 and 7 show expanded exploration and narrowed exploration. The AO algorithm has two phases of exploitation or local search (developed exploitation with smooth descent), according to Fig. 8, and narrowed exploitation, according to Fig. 9.

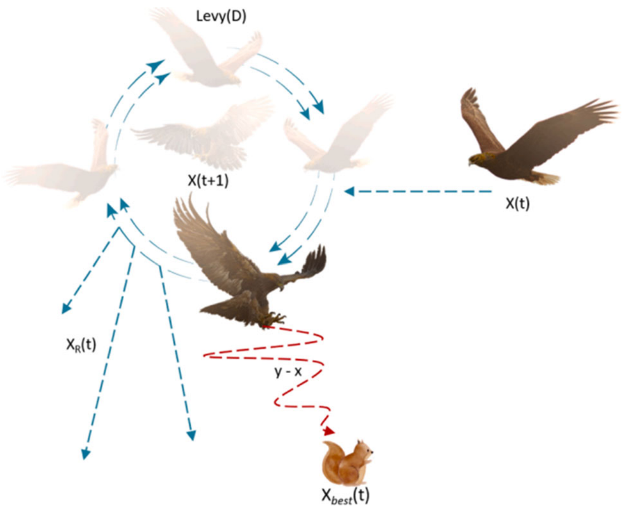

Fig. 7 Narrowed exploration search [28]

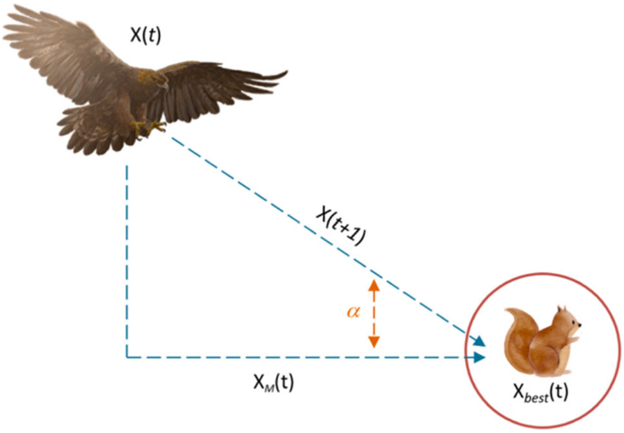

Fig. 8 Expanded exploitation search [28]

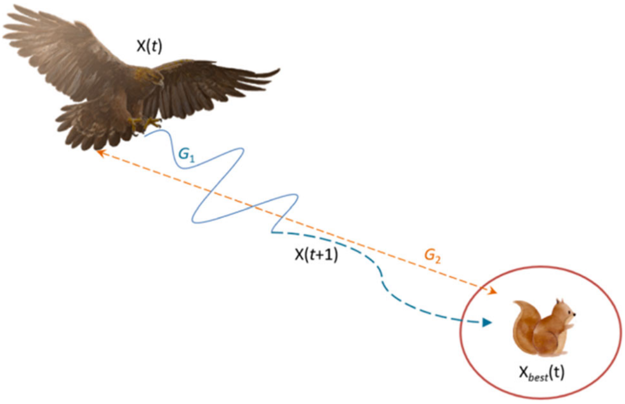

Fig. 9 Narrowed exploitation search [28]

Equation 6 uses the expanded exploratory search behavior of vertical peaking and falling in the AO algorithm.

$$X_i\,(t+1) = X_{\text{best}}\,(t) \times \left(1 - \frac{t}{T}\right) + (X_M\,(t) - X_{\text{best}}\,(t) * \text{ rand }) \tag{6}$$

In this equation, $X_{\text{best}}\,(t)$ is the bait position or the most optimal solution, t is the current iteration counter, and T is the maximum iteration of the algorithm. $X_i(t+1)$ is also the position of a solution in the new iteration, and $X_i(t)$ is the previous position of the solution. On the other hand, $X_M(t)$ is the average position of the solutions and it is calculated by applying Eq. (7).

$$X_M(t) = \frac{1}{N}\sum_{i=1}^{N} X_i(t),\ \forall j = 1, 2, \ldots, \text{Dim} \tag{7}$$

Equation (9) is used to perform narrowed exploration search behavior of the type of rotational and spiral dive toward the prey:

$$X_i(t+1) = X_{\text{best}}\,(t) \times \text{LF}(D) + X_R(t) + (y - x) \times \text{rand} \tag{8}$$

In this equation, $X_R(t)$ is a random position in the algorithm, D represents the dimensions of each problem solution, and LF is a random function like Eq. (9):

$$\text{LF}(D) = s \times \frac{u \times \sigma}{|v|^{\frac{1}{\beta}}} \tag{9}$$

In this equation, s and β are two parameters and numerical constants and parameters u and v are two random numbers between zero and one. Equation (10) is used to calculate σ:

$$\sigma = \frac{\Gamma(1+\beta) + \sin\left(\frac{\beta\pi}{2}\right)}{\Gamma\left(\frac{1+\beta}{2}\right) \times \beta \times 2^{\frac{\beta-1}{2}}} \tag{10}$$

In these equations, x and y are used for rotational movements and formulated as Eq. (11):

$$\begin{cases} x = r \times \sin(\theta) \\ y = r \times \cos(\theta) \\ r = r_3 + 0.00565 \times D \\ \theta = -\omega \times D1 + \frac{3\pi}{2} \end{cases} \tag{11}$$

In this equation, $r3$ is the number of search cycles (1 to 20), ω equals 0.005, and D consists of integers from 1 to dimension size (D). Equation (12) is used for direct movement of solution without spiral behavior or problem solutions toward prey:

$$X_i\,(t+1) = (X_{\text{best}}\,(t) - X_M\,(t)) \times \alpha - \text{rand} + ((\text{UB} - \text{LB}) \times \text{rand} + \text{LB}) \times \delta \tag{12}$$

In this equation, α and δ are two parameters of local search or productivity, and their number is between 0 and 0.1. Equation (13) is used for the behavior of movement toward the prey with a spiral movement mechanism.

$$X_i\,(t+1) = \text{QF} \times X_{\text{best}}\,(t) - (G_1 \times X_i\,(t) \times \text{rand}) - G_2 \times \text{Levy}\,(D) + \text{rand} \times G_1 \tag{13}$$

In this equation, QF represents a quality function used to balance search strategies, calculated using Eq. (14). G1 shows the different movements of the AO algorithm used to track the prey during the escape, using Eq. (15). $G2$ shows decreasing values from 2 to 0, representing the AO algorithm's flight slope to follow the prey during the escape, formulated by Eq. (16).

$$\text{QF}(t) = t^{\frac{2\times\text{rand}-1}{(1-T)^2}} \tag{14}$$

$$G_1 = 2 \times \text{rand} - 1 \tag{15}$$

$$G_2 = 2 \times \left(1 - \frac{t}{T}\right) \tag{16}$$

The most optimal solution is updated by executing the AO algorithm steps. The most optimal solution is sent to the output as the final solution. In the AO algorithm, if the repetition counter is less than $t \leq \frac{2T}{3}$, the search type is exploratory; otherwise, the search type will be descriptive.

3.3 Traffic classification with VGG19

CNN is a deep learning method for image processing and classification, and its input should be imaged. VGG19 uses the incoming traffic coding into the images for network traffic classification. The VGG19 approach provides higher accuracy, faster training speed, and fewer training samples per time than ResNet and GoogleNet methods. Suppose K features are selected from the dataset in the feature selection step. A K matrix is created if K examples of the attack class are isolated from the dataset. Each column of this matrix is a selected feature. If the values of the matrix K normalize in K examples are between 0 and 255, a gray image is created. In the proposed method, three matrices, K*K, are considered for three channels, R, G, and B, to create a color image of the dataset. The same is done for attack traffic and the regular traffic classes. Normal traffic samples are standard color images, and attack traffic samples are created as attack

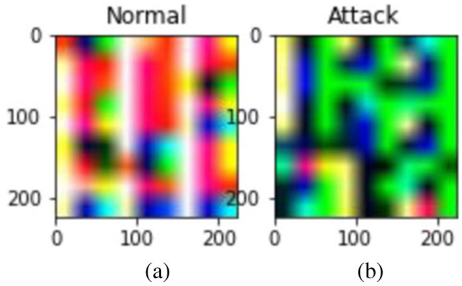

Fig. 10 **a** Traffic images, **b** attack images [39]

images. Attack images and normal images are used to train CNN. A CNN is trained by converting traffic samples into color images of attacks and normal traffic (Fig. 10).

In the proposed method, images of attacks and normal traffic are used as inputs to the VGG19 neural network in the CNN architecture. Figure 11 shows the architecture of VGG19 and classifies attack and normal images.

The input of the VGG19 neural network shows images of attack traffic and normal traffic, and the output of VGG19 architecture has two classes of images: attack type and normal.

3.4 The VGG19 optimization

The CNN and architectures like VGG19 have different meta-parameters. The precise adjustment of the learning parameters in the VGG19 neural network reduces classification errors. The number of epochs, frozen layers, early stop patience batch size, dropout ratio, and learning rate are the meta-parameters that effectively reduce CNN neural network classification errors. The proposed method uses the AO algorithm to optimize the CNN's hyperparameters. In this case, each member of the AO algorithm is a deep learning parameter, and the objective function shows the normal traffic classification error from the attack.

4 Experimental results

This section implements and evaluates the proposed intrusion detection system for detecting attacks on smart grids. Python, Keras, and Tensorflow libraries have been used for implementation. The population size of the AO algorithm is 15, and the maximum number of AO iterations is 50. The number of tests equals 25, and the training and test data sizes are considered 70% and 15%. 15% of samples are validation traffic. The value of α and δ in the AO algorithm is between [0, 0.1]. In this case, $r3$ in the AO algorithm is a value between 1 and 20, and D is an integer between 1 and dimension size (D). Moreover, ω is equivalent to 0.005, and u and v are two random numbers between 0 and 1 in the AO algorithm.

4.1 Dataset

The NSL-KDD dataset implements and evaluates the proposed intrusion detection system. The KDD-NSL dataset has 42 features, 41 of which are input features and 42 are output features. The NSL-KDD dataset has 23 types of traffic, 22 of which are attacks and just one is normal traffic. In the NSL-KDD dataset, the number of normal samples is more than the number of attack samples, the dataset is unbalanced, and the CGAN method is applied to balance the attack samples.

4.2 Evaluation metrics

Evaluation indicators such as precision, sensitivity, and precision to evaluate the proposed method are formulated according to Eqs. (17), (18), and (19).

$$\text{Accuracy} = \text{ACC} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{TN} + \text{FP} + \text{FN}} \tag{17}$$

$$\text{Sensitivity} = \text{Recall} = \text{DR} = \frac{\text{TP}}{\text{TP} + \text{FN}} \tag{18}$$

$$\text{Precision} = P = \frac{\text{TP}}{\text{TP} + \text{FP}} \tag{19}$$

4.3 Intrusion detection system (IDS)

Confusion matrices are crucial tools to evaluate the effectiveness of an intrusion detection system (IDS), revealing the alignment between predicted accuracy and actual outcomes. These matrices provide transparency and essential metrics such as accuracy, precision, recall, F1-score, and specificity. This deepens comprehension of system performance and strengthens its practical reliability.

TP, TN, FP, and FN parameters are defined as follows to calculate accuracy, sensitivity, and precision [40, 41]:

- True positive (TP): The traffic is attack type and classified in the attack class.
- False negative (FN): The traffic is attack-type but classified in the normal class.
- False positive (FP): The traffic is normal but classified in the attack class.
- True negative (TN): The traffic is normal and classified in the normal class.

The confusion matrix formula is provided as follows [42–44]:

- Accuracy: $\frac{(\text{TP+TN})}{(\text{TP+TN+FP+FN})}$
- Precision: $\frac{(\text{TP})}{(\text{TP+FP})}$
- Recall (sensitivity or true-positive rate): $\frac{(\text{TP})}{(\text{TP+FP})}$

Fig. 11 VGG19 neural network architecture

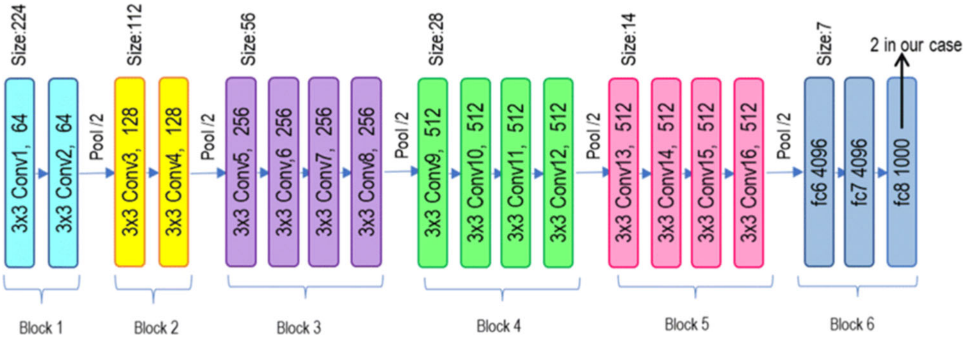

Table 1 Index of accuracy, sensitivity, and precision in four scenarios, balancing dataset by CGAN method

Scenarios	Accuracy	Sensitivity	Precision
*S*1	97.21	97.13	97.16
*S*2	98.82	98.25	98.64
*S*3	98.35	98.27	98.33
*S*4	99.82	99.69	99.76

- Specificity (true-negative rate): $\frac{(\mathrm{TN})}{(\mathrm{TN+FP})}$
- F1-score: $\frac{(2*(\mathrm{Precision}*\mathrm{Recall}))}{(\mathrm{Precision}+Recall)}$
- Parametric comparisons involve adjusting system parameters and evaluating metrics to find the optimal configuration that improves system performance for the detailed task.

4.4 Evaluation results

Several scenarios have been considered for evaluating the proposed method. The proposed intrusion detection system performs without VGG optimization in the first step. VGG is combined with the AO feature selection algorithm in the second scenario. In the third scenario, VGG is optimized with the AO optimization algorithm. In the fourth scenario, the AO algorithm selects features and optimizes VGG parameters. The experiment scenarios are shown with S1, S2, S3, and S4, respectively. Table 1 shows the proposed method's accuracy, sensitivity, and precision index in two VGG scenarios with and without the AO algorithm.

Figure 12 visually shows a bar chart's accuracy, sensitivity, and precision index. Experiments show that in the first scenario, if the AO optimization algorithm is not used to optimize and select the VGG19 feature, the intrusion detection system's accuracy, sensitivity, and precision are 97.21%, 97.13%, and 97.16%, respectively. In the second scenario, if the AO algorithm is used to optimize VGG19 for feature selection, the proposed method's accuracy, sensitivity, and precision are 98.82%, 98.25%, and 98.64%, respectively. In the third scenario, the AO algorithm is used to optimize the parameters of VGG19, and its accuracy, sensitivity, and precision are 98.35%, 98.27%, and 98.33%, respectively. In the fourth scenario, the proposed method's accuracy, sensitivity, and precision are 99.82%, 99.69%, and 99.76%, respectively. The evaluations show that the proposed IDS effectiveness maximizes if the AO algorithm uses feature selection and parameter optimization.

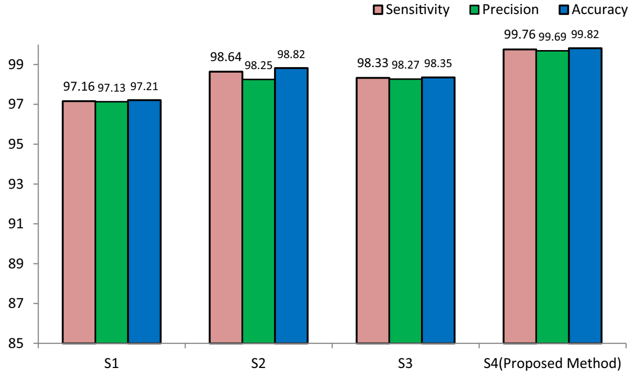

Fig. 12 Evaluation of the proposed intrusion detection system in four scenarios with CGAN

When the AO algorithm selects the features, the intrusion detection system's accuracy is more important than when utilized to optimize the AO parameters. In other words, using the AO algorithm in the feature selection phase has more considerable impact on improving the accuracy of attack detection than using the AO algorithm to optimize the VGG19 parameters.

If the GAN balancing method is used instead of CGAN in the experiments, the results of the scenarios will be according to Table 2. Figure 13 compares the accuracy, sensitivity, and precision index in four scenarios when balanced using the GAN method.

Experiments show that if GAN is used instead of CGAN in balancing the dataset, the proposed method's accuracy, sensitivity, and precision in detecting attacks will increase. If CGAN is used to balance the dataset in the proposed method, the accuracy, sensitivity, and precision are 99.82%, 99.69%, and 99.76%, respectively. If the GAN method balances the

Table 2 Index of accuracy, sensitivity, and precision in four scenarios when the dataset was balanced using the GAN method

Scenarios	Accuracy	Sensitivity	Precision
*S*1	97.09	96.92	96.98
*S*2	98.51	98.02	98.22
*S*3	98.14	97.82	97.94
*S*4	98.62	98.23	98.25

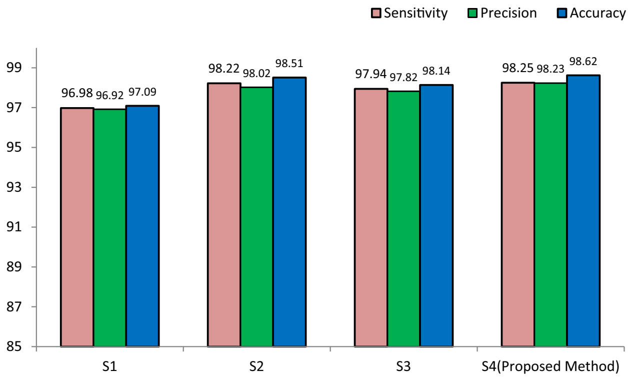

Fig. 13 Evaluation of the proposed intrusion detection system in four scenarios using GAN balancing

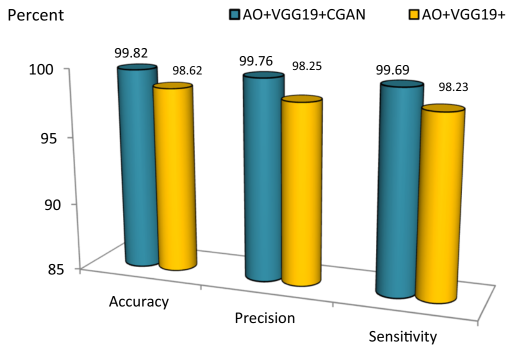

Fig. 14 Comparison of the proposed balancing intrusion detection system using GAN and CGAN

dataset, the proposed method has an accuracy, sensitivity, and precision of 99.62%, 99.23%, and 99.12%, respectively. Figure 14 compares the proposed method's accuracy, sensitivity, and precision with two GAN and CGAN methods.

When the CGAN method is used to balance the dataset, the accuracy, sensitivity, and precision improved by 1.2%, 1.51%, and 1.46%, respectively, compared to the GAN method, the proposed attack detection method was compared to previous research findings, which used machine learning methods, such as HDT, DT, KNN, and SVM, to detect attacks on smart grids. Figure 15 shows the proposed method's accuracy, sensitivity, and precision compared to machine learning methods.

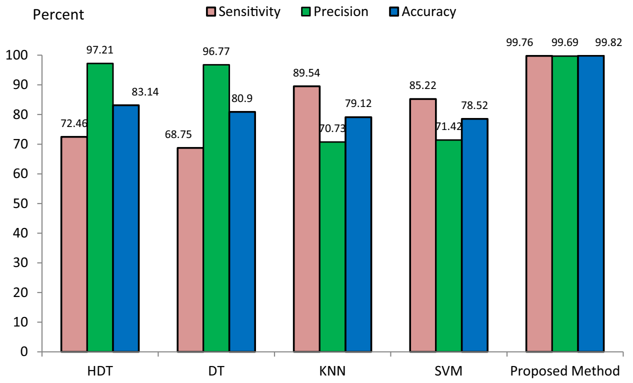

Fig. 15 Comparison of the proposed intrusion detection system and machine learning methods

Table 3 Comparison of accuracy, sensitivity, and precision index with deep and machine learning methods

Models	*P* (%)	DR (%)	ACC (%)
SVM	97.76	97.8	97.81
LR	97.94	97.95	97.95
KNN	98.76	98.79	98.79
MultinomialNB	91.09	88.65	88.65
DNN-3	98.48	98.49	98.5
GRU + MLP	97.98	98.04	98.05
DNN-16	98.86	98.91	98.92
Transformer-IDM	99.49	99.49	99.48
Proposed method	99.82	99.69	99.76

Comparisons show that the proposed method has more accuracy, sensitivity, and precision in detecting attacks than HDT, DT, KNN, and SVM methods. Among the machine learning methods (in terms of detecting network attacks), the support vector machine method has the worst performance in terms of accuracy index. The proposed method is compared with machine learning and deep learning findings of previous research [45]. Table 3 shows the comparison in terms of accuracy, sensitivity, and precision.

In [45], federated hierarchical learning is used to detect attacks on smart grids. Table 2 compares the proposed method with SVM, LR, KNN, multinomialNB, and deep learning methods, such as GRU + MLP, DNN-3, Transformer-IDM, and DNN-16. According to the comparisons, the proposed method is more accurate than the federal learning method in detecting attacks on smart grids. In Fig. 16, the proposed method in attack detection is compared with federal deep learning methods such as Fed-GRU + MLP, Fed-DNN-3, Fed-Transformer-IDM, and Fed-DNN-16 on the accuracy index.

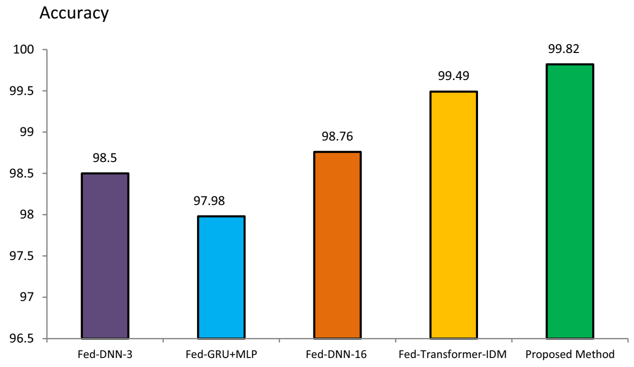

Fig. 16 Comparison of the proposed intrusion detection system with federated learning methods

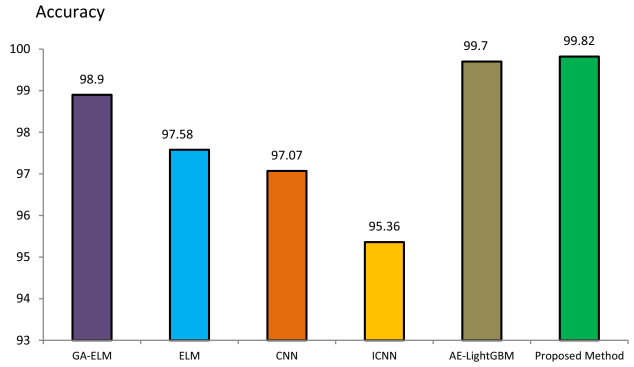

Fig. 17 Comparison of the proposed method with extreme learning methods

According to tests and comparisons, the accuracy of detecting attacks by federated deep learning, such as Fed-GRU + MLP, Fed-DNN-16, Fed-Transformer-IDM, and Fed-DNN-3, is 97.98%, 98.76%, 99.49%, and 98.5%. The accuracy of the proposed method in detecting attacks is 99.82%, so it is more accurate than deep learning methods in detecting intrusion into the smart grids. In a study [46], deep learning methods are used to detect attacks on the smart grids, and the results of the proposed method are compared to the results of this study (Fig. 17).

Figure 17 presents the proposed method on the accuracy index with GA-ELM, ELM, CNN, ICNN, and AE-LightGBM methods in detecting attacks on the smart grid. Comparisons show that the accuracy of GA-ELM, ELM, CNN, ICNN, and AE-LightGBM methods in detecting attacks is 98.9%, 97.58%, 97.07%, 95.36%, and 99.70%, respectively. The results of the comparisons showed that the accuracy of these methods is lower than the proposed method in detecting attacks. The analysis of the detection time of the proposed method with different methods is shown in Fig. 18. For comparison, the results obtained in the research [47] are used, and the detection time of penetration is considered in seconds.

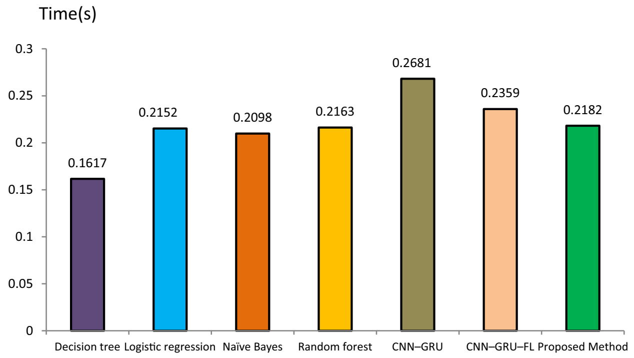

Fig. 18 Comparison of attack detection time in seconds

The analysis of attack detection time shows that the decision tree method has the lowest attack detection time among the compared methods. Its accuracy is much lower than the proposed method. The proposed method only has more detection time than the decision tree method and the Bayesian network. The proposed method has less time in intrusion detection than methods like logistic regression, random forest, CNN-GRU, and CNN-GRU-FL.

5 Limitations and future work

It would be beneficial to offer readers a comprehensive understanding of potential limitations and areas for further increase in your research. The current work focuses on the crucial need for an efficient intrusion detection system for smart grids (SGs) due to their vulnerability to various intrusions and attacks. Despite the success of the proposed method in detecting attacks, one notable disadvantage during the training phase is time limitations. Furthermore, while swarm smart and deep learning are significant strengths, the suggest model may require adaptation for various attacks and networks, like 5G. In future efforts, exploring the combination of CNN and LSTM architectures and expanding the intrusion detection system's utilization to 5G networks could prove valuable for advancing this field.

6 Conclusion

Smart grids (SGs) are essential in data and energy transmission today. However, this network is susceptible to all kinds of intrusions and attacks. Attacks on the SG network are very harmful and can cause disaster, so it is necessary to provide an efficient intrusion detection system to deal with them. A significant challenge in delivering an intrusion detection system for the SG network is that traffic imbalance reduces the ability to detect attacks with deep learning methods. An efficient method for pattern recognition is CNN. It is used for image processing and analysis, but the network traffic does not have an image-type nature. This manuscript uses the network traffic balance by a deep learning method based on conditional Game Theory called CGAN. In the second step, a binary version of the AO algorithm is presented to select the main features of the dataset. The training samples are converted to RGB color image format in the third step and coded to train the VGG19 architecture, a CNN. The last step was VGG19 neural network training with RGB images and its hyperparameters optimization with the AO algorithm.

Experiments and evaluations showed that if the AO algorithm is used in the feature selection phase and optimization of VGG19 parameters, the proposed method's accuracy, sensitivity, and precision are 99.82%, 99.69%, and 99.76%, respectively. The evaluations showed that the proposed method is more accurate in detecting attacks than similar architectures such as LSTM and CNN. Experiments show that using the CGAN method in balancing the dataset compared to the GAN method improves the accuracy, sensitivity, and precision of the proposed method by 1.2%, 1.51%, and 1.46%, respectively. The proposed method has less time to detect attacks than random forest, CNN-GRU, and LSTM. The main advantage of the proposed method is the more optimal balancing of the dataset than the GAN method and more accuracy than the CNN architecture in detecting attacks. Another advantage of the proposed method is combining swarm intelligence with deep learning to detect nested and zero-day attacks. The challenge of deep learning methods and the proposed method for detecting attacks is the considerable time in the training phase. Combining CNN and LSTM architectures in attack detection and providing an intrusion detection system for 5G networks is a recommendation for future work.

Author contribution AAM wrote the main manuscript text and ÖE advised the paper and JR analysed the results and programming.

Funding The authors received no financial support for the research, authorship, and/or publication of this article.

Data availability Datasets used in the research are publicly available for download.

Declarations

Conflict of interest The authors have no relevant financial or non-financial interests to disclose.

Ethical approval This research does not require ethics approval.

Consent to participate This research uses public available anonymous data.

Consent to publish This research does not contain any individual person's data.

References

1. Ghiasi, M., Niknam, T., Wang, Z., Mehrandezh, M., Dehghani, M., Ghadimi, N.: 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. **215**, 108975 (2023)
2. Rath, C.K., Mandal, A.K., Sarkar, A.: Microservice based scalable IoT architecture for device interoperability. Comput. Stand. Interfaces **84**, 103697 (2023)
3. Padmanaban, S., Samavat, T., Nasab M.A., Nasab, M.A., Zand, M. Nikokar, F.: Electric vehicles and IoT in smart cities. Artif. Intell. Smart Power Syst. 273–290, (2023)
4. Zhao, Y., Li, Q., Yi, W., Xiong, H.: Agricultural IoT data storage optimization and information security method based on blockchain. Agriculture **13**(2), 274 (2023)
5. Siddiqui, S., Hameed, S., Shah, S.A., Khan, A.K., Aneiba, A.: Smart contract-based security architecture for collaborative services in municipal smart cities. J. Syst. Archit. **135**, 102802 (2023)
6. Gandhi, I., Ravi, L., Vijayakumar, V., Subramaniyaswamy, V.: Improving security for wind energy systems in smart grid applications using digital protection technique. Sustain. Cities Soc. **60**, 102265 (2020)
7. Nafees, M.N., Saxena, N., Cardenas, A., Grijalva, S., Burnap, P.: Smart grid cyber-physical situational awareness of complex operational technology attacks: a review. ACM Comput. Surv. **55**(10), 1–36 (2023)
8. Gan, J., Zeng, L., Liu, Q., Liu, X.: A survey of intelligent load monitoring in IoT-enabled distributed smart grids. Int. J. Ad Hoc Ubiquitous Comput. **42**(1), 12–29 (2023)
9. Ravinder, M., Kulkarni, V.: A review on cyber security and anomaly detection perspectives of smart grid. In 2023 5th international conference on smart systems and inventive technology (ICSSIT), pp. 692–697. (2023)
10. Mirzaee, P.H., Shojafar, M., Cruickshank, H., Tafazolli, R.: Smart grid security and privacy: from conventional to machine learning issues (threats and countermeasures). IEEE access **10**, 52922–52954 (2022)
11. Minh, Q.N., Nguyen, V.-H., Quy, V.K., Ngoc, L.A., Chehri, A., Jeon, G.: Edge computing for IoT-enabled smart grid: the future of energy. Energies **15**(17), 6140 (2022)
12. Bhattarai, T.N., Ghimire, S., Mainali, B., Gorjian, S., Treichel, H., Paudel, S.R.: Applications of smart grid technology in Nepal: status, challenges, and opportunities. Environ. Sci. Pollut. Res. **30**(10), 25452–25476 (2023)
13. Ghiasi, M., Wang, Z., Mehrandezh, M., Jalilian, S., Ghadimi, N.: Evolution of smart grids towards the Internet of energy: concept and essential components for deep decarbonisation. IET Smart Grid **6**(1), 86–102 (2023)
14. Abed, A.H., Rahebi, J., Sajir, H., Farzamnia, A.: Protection of sensitive loads from voltages fluctuations in Iraqi grids by DVR. In 2017 IEEE 2nd international conference on automatic control and intelligent systems (I2CACIS), pp. 144–149. (2017)
15. Sajir, H., Rahebi, J., Abed, A., Farzamnia, A.: Reduce power losses and improve voltage level by using distributed generation in radial distributed grid. In 2017 IEEE 2nd international conference on automatic control and intelligent systems (I2CACIS), pp. 128–133. (2017)
16. Al-jumaili, M., Rahebi, J., Akbas, A., Farzamnia, A.: Economic dispatch optimization for thermal power plants in Iraq. In 2017 IEEE 2nd international conference on automatic control and intelligent systems (I2CACIS), pp. 140–143. (2017)
17. Jaiswal, D.M., Thakre, M.P.: Modeling & designing of smart energy meter for smart grid applications. Glob. Trans. Proc. **3**(1), 311–316 (2022)

18. Acarali, D., Rao, K.R., Rajarajan, M., Chema, D., Ginzburg, M.: Modelling smart grid IT-OT dependencies for DDoS impact propagation. Comput. Secur. **112**, 102528 (2022)
19. Ocaka, A., Briain, D.Ó., Davy, S., Barrett, K.: Cybersecurity threats, vulnerabilities, mitigation measures in industrial control and automation systems: a technical review. In 2022 Cyber research conference-Ireland (Cyber-RCI), pp. 1–8. (2022)
20. Davis, K.R., Morrow, K.L., Bobba, R., Heine, E.: Power flow cyber attacks and perturbation-based defense. In 2012 IEEE third international conference on smart grid communications (SmartGridComm), pp. 342–347. (2012)
21. Yusupov, Z., Yaghoubi, E., Soyibjonov, V.: Reducing the vulnerability in microgrid power systems. Sci. Innov. **2**(A5), 166–175 (2023)
22. Merlino, J.C., Asiri, M., Saxena, N.: Ddos cyber-incident detection in smart grids. Sustainability **14**(5), 2730 (2022)
23. Albaseer, A., Abdallah, M.: Fine-tuned LSTM-based model for efficient honeypot-based network intrusion detection system in smart grid networks. In 2022 5th international conference on communications, signal processing, and their applications (ICCSPA), pp. 1–6. (2022)
24. Haq, E.U., Pei, C., Zhang, R., Jianjun, H., Ahmad, F.: Electricity-theft detection for smart grid security using smart meter data: a deep-CNN based approach. Energy Rep. **9**, 634–643 (2023)
25. Eddin, M.E., et al.: Fine-tuned rnn-based detector for electricity theft attacks in smart grid generation domain. IEEE Open J. Ind. Electron. Soc. **3**, 733–750 (2022)
26. Sarwar, A., Alnajim, A.M., Marwat, S.N.K., Ahmed, S., Alyahya, S., Khan, W.U.: Enhanced anomaly detection system for iot based on improved dynamic SBPSO. Sensors **22**(13), 4926 (2022)
27. Babu, K.S., Rao, Y.N.: MCGAN: modified conditional generative adversarial network (MCGAN) for class imbalance problems in network intrusion detection system. Appl. Sci. **13**(4), 2576 (2023)
28. Abualigah, L., Yousri, D., Abd Elaziz, M., Ewees, A.A., Al-Qaness, M.A.A., Gandomi, A.H.: Aquila optimizer: a novel meta-heuristic optimization algorithm. Comput. Ind. Eng. **157**, 107250 (2021)
29. Bhattacharya, S., et al.: Incentive mechanisms for smart grid: state of the art, challenges, open issues, future directions. Big Data Cogn. Comput. **6**(2), 47 (2022)
30. Muqeet, H.A., Liaqat, R., Jamil, M., Khan, A.A.: A state-of-the-art review of smart energy systems and their management in a smart grid environment. Energies **16**(1), 472 (2023)
31. Tufail, S., Parvez, I., Batool, S., Sarwat, A.: A survey on cybersecurity challenges, detection, and mitigation techniques for the smart grid. Energies **14**(18), 5894 (2021)
32. Abdalzaher, M.S., Fouda, M.M., Ibrahem, M.I.: Data privacy preservation and security in smart metering systems. Energies **15**(19), 7419 (2022)
33. Kamiński, M.A.: Operation 'Olympic Games'. Cyber-sabotage as a tool of American intelligence aimed at counteracting the development of Iran's nuclear programme. Secur. Def. Q. **29**(2), 63–71 (2020)
34. Haes Alhelou, H., Hamedani-Golshan, M.E., Njenda, T.C., Siano, P.: A survey on power system blackout and cascading events: research motivations and challenges. Energies **12**(4), 682 (2019)
35. Khazeiynasab, S.R., Qi, J.: Resilience analysis and cascading failure modeling of power systems under extreme temperatures. J. Mod. Power Syst. Clean Energy **9**(6), 1446–1457 (2021)
36. Pinto, S.J., Siano, P., Parente, M.: Review of cybersecurity analysis in smart distribution systems and future directions for using unsupervised learning methods for cyber detection. Energies **16**(4), 1651 (2023)
37. Liu, Q., Hagenmeyer, V., Keller, H.B.: A review of rule learning based intrusion detection systems and their prospects in smart grids. IEEE Access **9**, 57542–57564 (2021)
38. Sakhnini, J., Karimipour, H., Dehghantanha, A.: Smart grid cyber attacks detection using supervised learning and heuristic feature selection. In 2019 IEEE 7th international conference on smart energy grid engineering (SEGE), pp. 108–112. (2019)
39. El-Ghamry, A., Darwish, A., Hassanien, A.E.: An optimized CNN-based intrusion detection system for reducing risks in smart farming. Internet Things **22**, 100709 (2023)
40. Al Shalchi, N.F.A., Rahebi, J.: Human retinal optic disc detection with grasshopper optimization algorithm. Multimed. Tools Appl. **81**, 1–19 (2022)
41. Al-Safi, H., Munilla, J., Rahebi, J.: Patient privacy in smart cities by blockchain technology and feature selection with harris hawks optimization (HHO) algorithm and machine learning. Multimed. Tools Appl. **81**, 1–25 (2022)
42. Mohamed, A.A.A., Hançerlioğullari, A., Rahebi, J., Ray, M.K., Roy, S.: Colon disease diagnosis with convolutional neural network and grasshopper optimization algorithm. Diagnostics **13**(10), 1728 (2023)
43. Rahebi, J.: Fishier mantis optimiser: a swarm intelligence algorithm for clustering images of COVID-19 pandemic. Int. J. Nanotechnol. **20**(1–4), 25–49 (2023)
44. Alsafi, H., Munilla, J., Rahebi, J.: An approach for cardiac coronary detection of heart signal based on harris hawks optimization and multichannel deep convolutional learning. Comput. Intell. Neurosci. **2022**, (2022)
45. Sun, X., et al.: A hierarchical federated learning-based intrusion detection system for 5g smart grids. Electronics **11**(16), 2627 (2022)
46. Yao, R., Wang, N., Liu, Z., Chen, P., Ma, D., Sheng, X.: intrusion detection system in the smart distribution network: a feature engineering based AE-LightGBM approach. Energy Rep. **7**, 353–361 (2021)
47. Zhai, F., Yang, T., Chen, H., He, B., Li, S.: Intrusion detection method based on CNN–GRU–FL in a smart grid environment. Electronics **12**(5), 1164 (2023)

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.