Detection of Cyber Attacks on Smart Grids Using Improved VGG19 Deep Neural Network Architecture and Aquila Optimizer Algorithm

Ahmed Abdulmunem Mhmood
Gazi University
Özgür Ergül
Gazi University
Javad Rahebi (cevatrahebi@topkapi.edu.tr)
Istanbul Topkapi University

Research Article

Keywords: Cyber attacks, smart grid, intrusion detection system, Deep Learning, VGG19 architecture, Swarm Intelligence

Posted Date: August 7th, 2023

DOI: https://doi.org/10.21203/rs.3.rs-3217829/v1

Additional Declarations: No competing interests reported.

Version of Record: A version of this preprint was published at Signal, Image and Video Processing on November 17th, 2023. See the published version at https://doi.org/10.1007/s11760-023-02813-7.

Detection of Cyber Attacks on Smart Grids Using Improved VGG19 Deep Neural Network Architecture and Aquila Optimizer Algorithm

Ahmed Abdulmunem Mhmood[1], Özgür Ergül[2], Javad Rahebi[3]
[1,2]Electrical & Electronics Department, Gazi University, Ankara, Turkey
[3]Software Engineering Department, Istanbul Topkapi University, Istanbul, Turkey
awab12122019@gmail.com, ergul@gazi.edu.tr, cevatrahebi@topkapi.edu.tr

Abstract
Cyber attacks against Smart Grids (SG) have harmful effects. The first function of a defensive system is to provide an intelligent system to detect intrusions. The nature of attacks against smart grids is very complex, so the intrusion detection system must be able to detect complex attacks. Lack of balancing and optimization of deep learning methods are the main challenges for many intrusion detection systems. This research presents an intelligent intrusion detection system for a smart grid based on Game Theory, Swarm Intelligence, and Deep Learning (DL). First, the proposed method balances the training samples with a conditional DL technique based on Game Theory and CGAN. Secondly, the Aquila Optimizer (AO) algorithm selects features. The third step involves mapping the selected features on the dataset and coding reduced-dimension samples into RGB color images, which are used to train the VGG19 neural network. In the fourth step, the AO algorithm optimally adjusts meta-parameters to reduce the error of the VGG19 neural network. Tests performed on the NSL-KDD dataset show that the proposed method's accuracy, sensitivity, and precision in detecting attacks are 99.82%, 99.69%, and 99.76%, respectively. The CGAN method balances the dataset and increases the accuracy, sensitivity, and precision of the proposed method compared to the GAN method in detecting attacks on the smart grid. Experiments show that the proposed method more accurately detects attacks than deep learning methods such as VGG19, CNN-GRU, CNN-GRU-FL, LSTM, and CNN.

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 related to 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 discover faster. The smart grid makes more accurate predictions of electricity consumption in the 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 develop in countries with scarce natural resources, such as oil, coal, or rare gases. Smart grids have different goals; the primary goal 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 changes in infrastructure, especially changes in 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. Transferring extensive data through traditional electricity networks was impossible because they used high-voltage transmission cables [13]. Different electrical components, such as transmission lines, transformers, substations, etc., are used in electricity distribution networks. 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 [14].

The infrastructure of smart grids is dependent 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 [15].

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, cyberattacks 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 [16]. 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 makes 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 approaches 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) [18], Convolutional Neural Network (CNN) [17], and Recurrent Neural Network (RNN) [19], 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 [20]. 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 [21]. 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 [22] 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 data set are converted into color images and selected 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 search.
- 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 network 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 presents 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 Figure 1. In Singapore, consumers are allowed to make and use energy [23].

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 produces 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 addition 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 [23, 24].

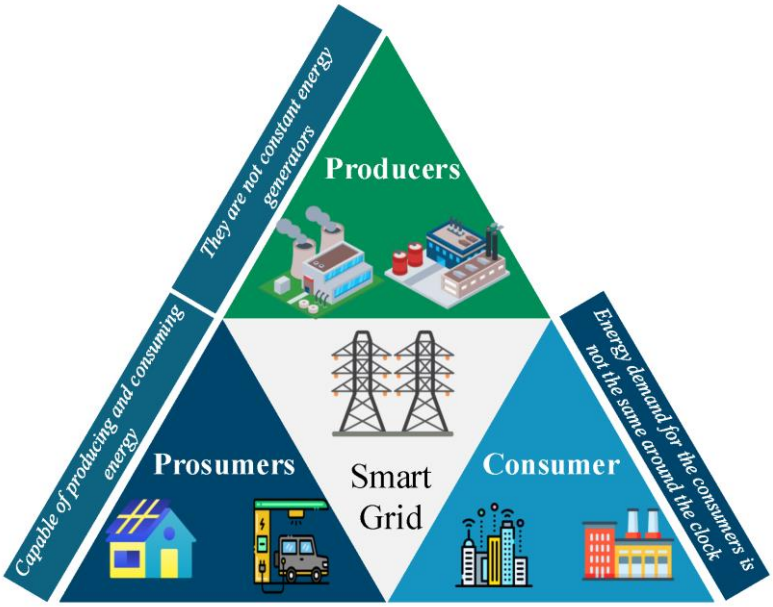

Figure 1: Smart grid beneficiaries [23]

Knowing the amount of energy consumed allows a producer to produce enough energy. Electrical equipment, smart meters, and sensors installed in consumer centers are used to acquire the data the producer needs [24]. Security issues and network intrusions are just 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, only analyze the data. Active attacks are more harmful than passive ones because they manipulate and alter the data [25]. According to a study [25], there are five primary objectives for cyber security in smart grids:

- User authentication and verification allow only authorized users to enter the system.
- User authorization allows 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.

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

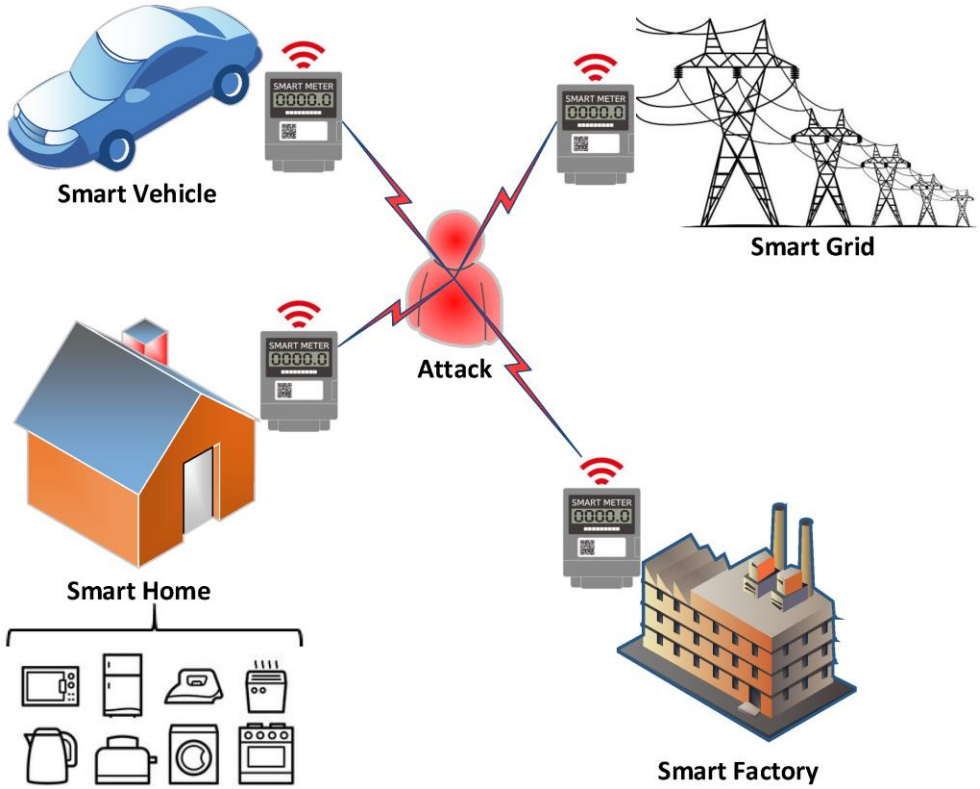

Figure 2: Attack on smart grid infrastructure [26]

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 230,000 persons, approximately. This cyberattack was the first successful one on a smart grid [25].

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 [27].

Another instance of an assault on the smart grid was the 2003 blackout in the United States 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 loss of energy for 50 million people over two days, at least 11 people died [28].

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 [29].

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 Figure 3.

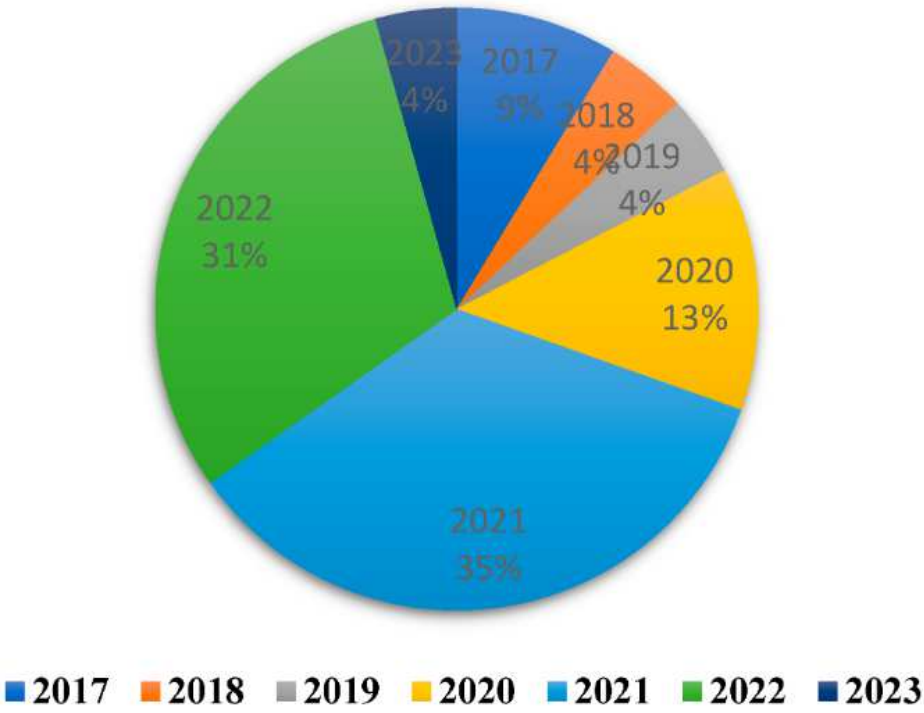

Figure 3: Increasing number of smart grid cyber security publications [30].

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 blacklist approaches [31], heuristic techniques [32], and machine learning techniques [33]. Blacklist 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 pattern 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 [34] 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 method, based on Long short-term memory (LSTM) and recurrent neural networks (RNN), is quite accurate in detecting attacks.

A research publication [35] 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 [36], the detection of attacks using the adversarial generative network has been proposed. In order to detect attacks, this study suggests using an XGBoost classifier and a conditional generative adversarial network. For stable model learning, WCGAN and gradient penalty are utilized. The GAN network'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 [37] presented a DDoS detection method using the SDN networks' physical and cyber systems. This method uses information entropy and unsupervised anomaly detection techniques to detect suspicious aspects and identify DDoS attacks. Their technique 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 [38] 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 [39], 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 method of identifying attacks had a 98% accuracy rate.

Previous research [40] 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 [41], 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 [42], 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 [43] 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 [44] 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 CNN neural network. In order to assess their approach, two datasets—UNSW_NB15 and KDDCup 99—are employed. According to experimental findings, they are more effective in detecting attacks than techniques like LSTM. Later, another work [45] introduced an optimized feature selection method using 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 [46]. 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. Table 1 summarizes the relevant works to detect attacks in the smart grids. This comparison states the method, advantages, disadvantages, and dataset used.

Table 1: Review of relevant works

Research	Method	Advantages	Disadvantages	Dataset
[34]	Bayesian approach integrated with CNN networks	More accuracy than RNN and LSTM	Low certainty Bayesian method	ICS
[35]	Federal learning	More accuracy than GRU, LSTM, and RNN	Unbalanced data set	KDD, NSL-KDD, and CIDDS
[36]	WCGAN	More accuracy than RF, DT, and SVM	No Dimension reduction	NSL-K, UNSW-NB15 and BoT-IoT
[37]	Cyber-physical system in SDN	Reduce the false positive rate in the range of 35% ~ 59%	Lack of intelligent feature selection	SDN traffic
[38]	Blockchain in smart grids	High confidentiality	Blockchain overhead	-
[39]	Enhanced Firefly Algorithm and CNN	Accuracy was almost 98%	No feature selection	SDN traffic
[40]	Machine learning using current and voltage sensors, Zigbee, Raspberry Pi, and Arduino,	Gaussian support vector machine is more accurate.	Lack of balancing and lack of feature selection	Zigbee traffic
[41]	SMOTE method and decision tree method	Detection of 5 types of attacks	Not reducing dimensions and selecting effective features	NSL-KDD
[42]	Five machine learning algorithms	Low latency and error	Not being able to detect all attacks	DER
[43]	Combination of three decision-trees	More accuracy than SVM, KNN, and DT	Not balancing the data set and not reducing traffic dimensions	NSL-KDD
[44]	CNN	More accurate than LSTM	Lack of CNN optimization	UNSW_NB15 and KDDCup 99
[45]	PSO algorithms and autoencoders	Appropriate accuracy	Lack of intelligent feature selection	NSL-KDD and UNSW-NB15
[46]	Machine learning and signature-based	Low false alarm rate	Memory waste and blacklist time overhead	The dataset includes MITM attacks.

In contrast to blacklisting 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 data set 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.

3. Methodology

The proposed method is based on deep learning based on Game Theory and 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
- Coding attack traffic and normal traffic in the form of RGB images
- VGG19 neural network training with RGB images
- Optimization of VGG19 neural network with AO algorithm

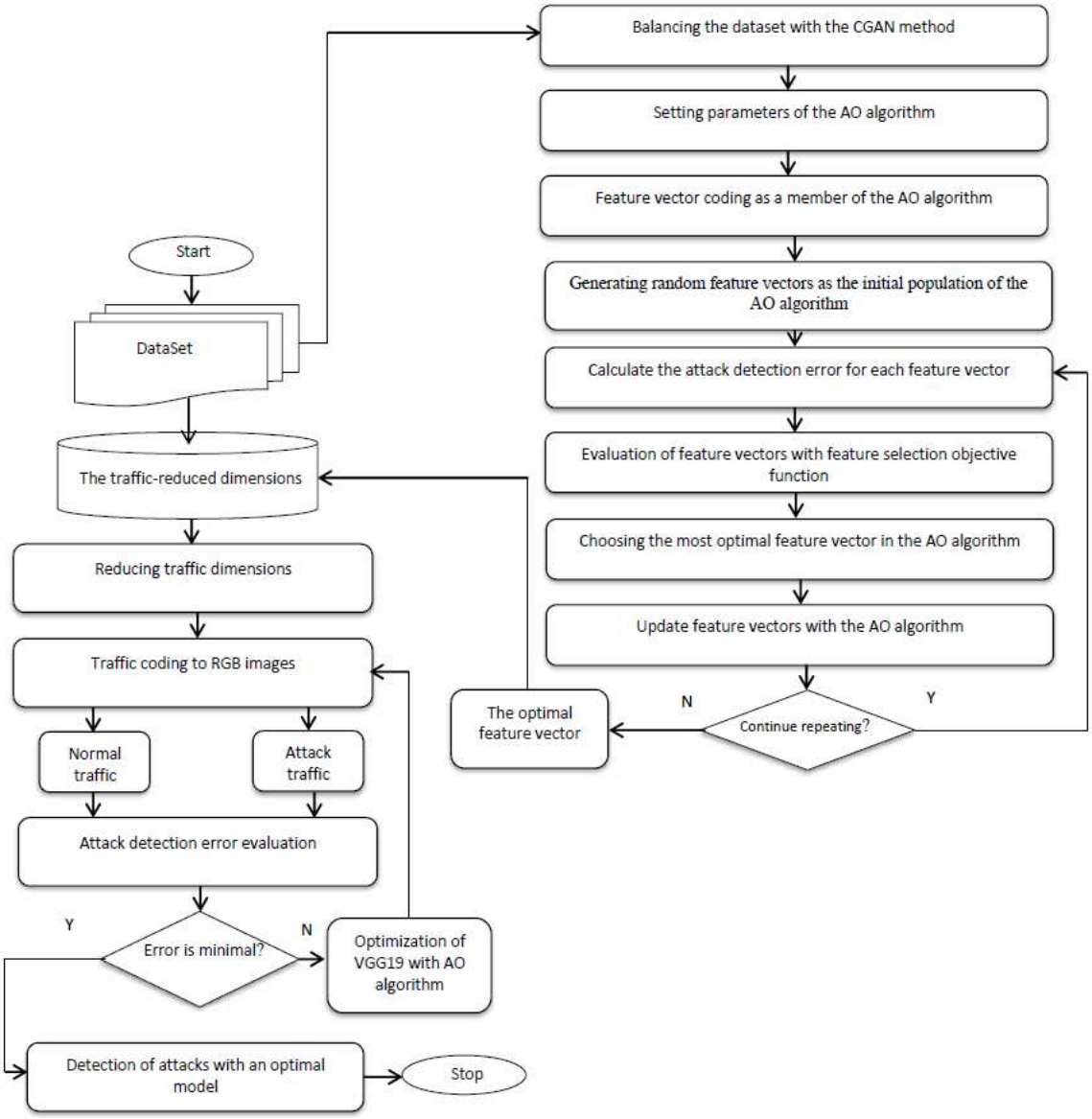

Figure 4: Framework of the proposed intrusion detection system or CAV

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 network. The GAN network is designed based on game theory and has two parts: generator and discriminator. The productive role is producing 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 samples. A GAN deep learning network presented in a research work [21] is of a conditional type, an improved version of GAN. Figure 5 shows the structure of the conditional version of GAN.

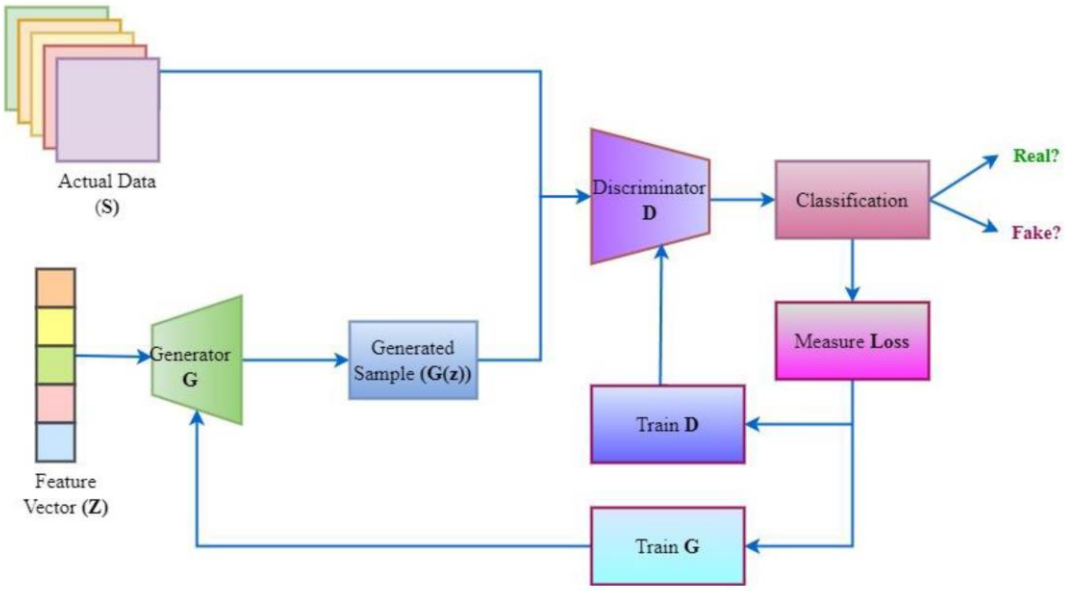

Figure 5: Conditional performance of the GAN method in producing artificial and fake samples [21]

Let G be the generator; the input set is S={s1, s2,…, sn}. G uses z to generate artificial samples. The role of the discriminator or D is to classify samples into fake and real classes. If a fake sample created by G is similar to normal samples, D puts them in the normal class. G attempts to deceive D and create artificial data so that D classifies it as real. The objective function for the GAN method is shown in Equation 1 [21]:

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

Here, p(s) is the dispersion of the real 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 [21], a new objective function for GAN is presented, and it is a conditional version of GAN, and according to Equation 2, it is presented as follows:

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

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 normal 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 Equation 3 [21]:

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

In the proposed method, the CGAN method balances the network traffic to generate artificial samples. 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, according to Equation 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 the Equation 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 selected, its value is equal to one. The j's feature of a feature vector, like 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 Equation 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 (expanded exploitation with smooth descent), according to Figure 8, and narrowed exploitation, according to Figure 9.

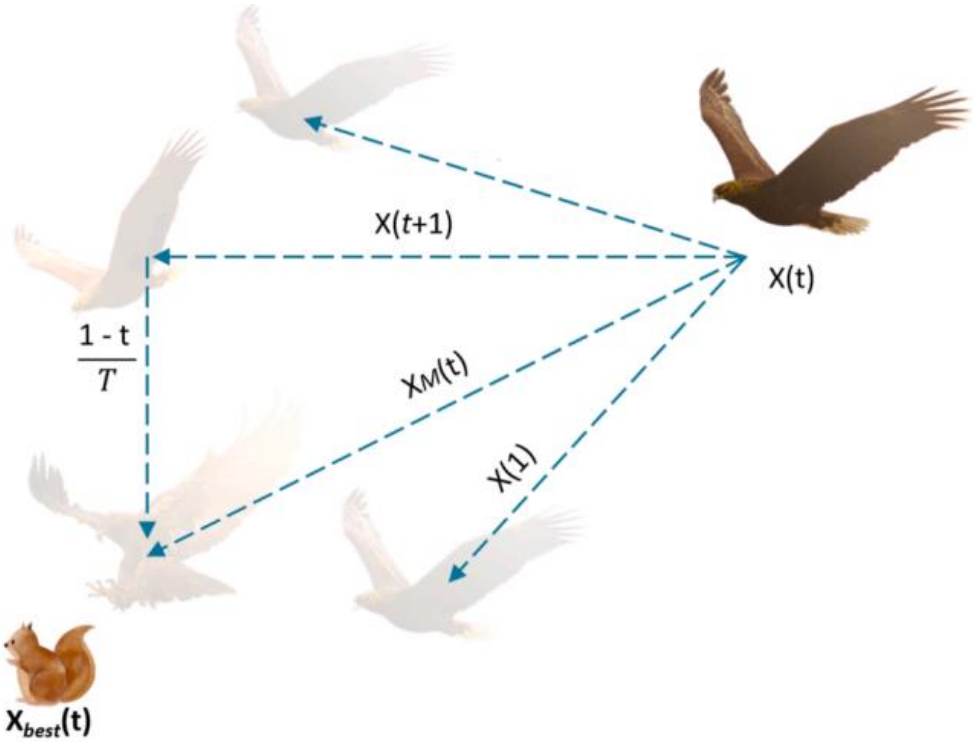

Figure 6: Expanded exploration search [22]

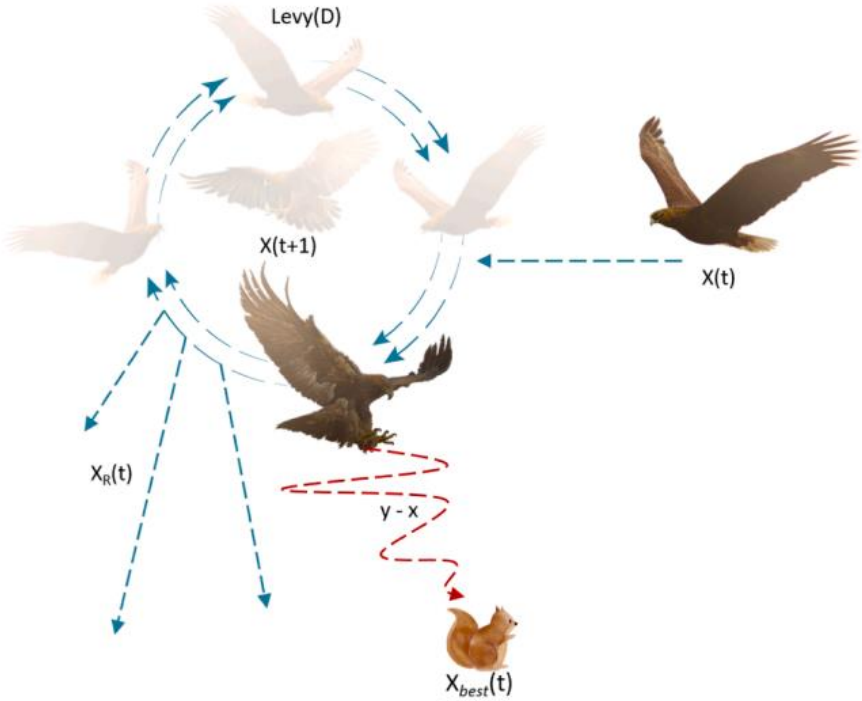

Figure 7: Narrowed exploration search [22]

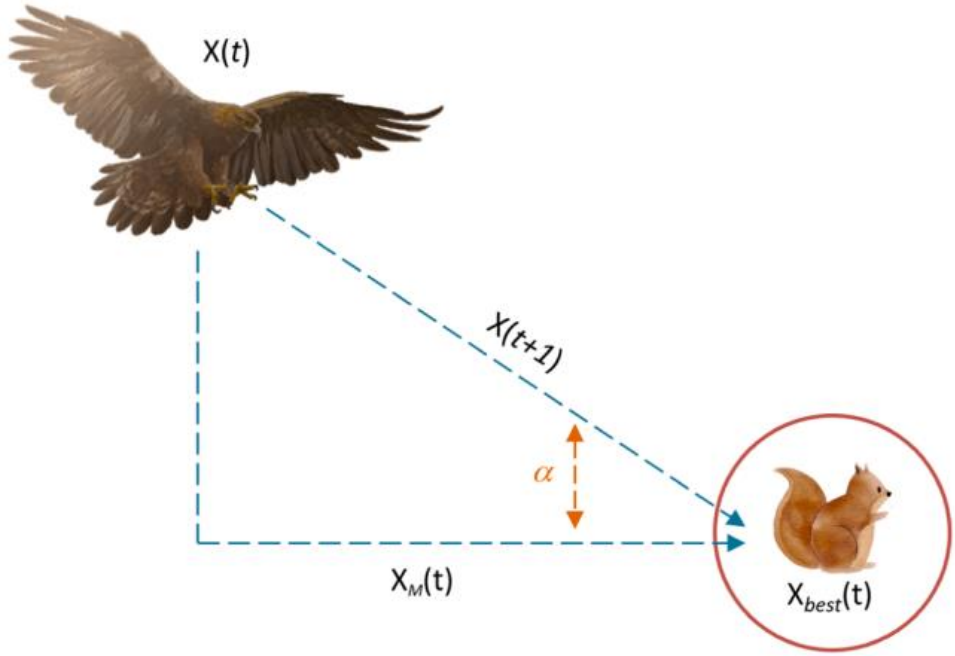

Figure 8: Expanded exploitation search [22]

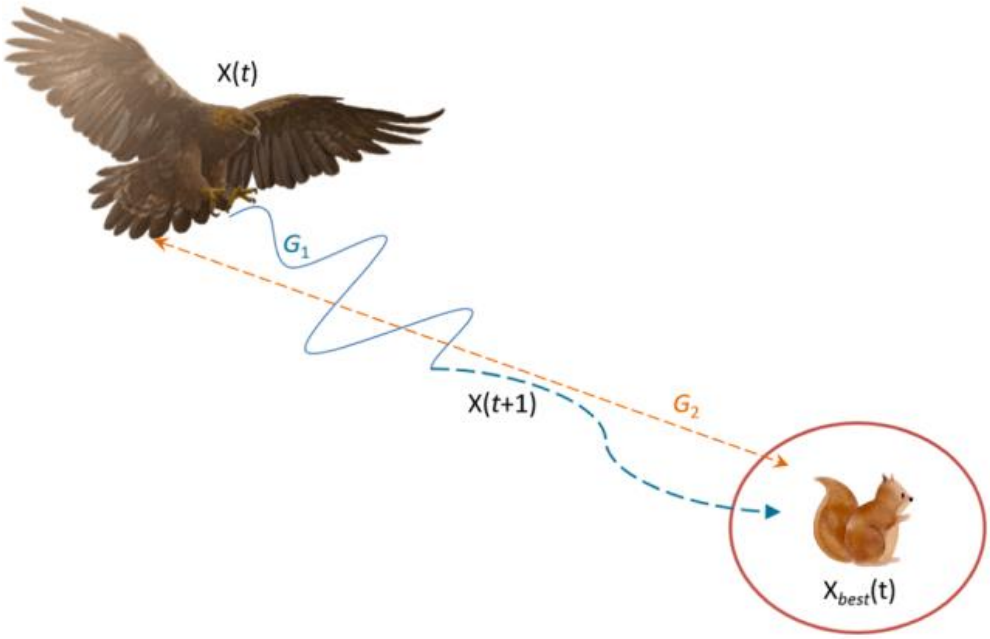

Figure 9: Narrowed exploitation search [22]

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

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

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 Equation 7.

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

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

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

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 Equation 9:

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

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:

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

In these equations, x and y are used for rotational movements and formulated as Equation 11:

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

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 towards prey:

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

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.

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

In this equation, QF represents a quality function used to balance search strategies, calculated using Equation 14. G1 shows the different movements of the AO algorithm used to track the prey during the escape, using Equation 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 Equation 16.

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

$$G_1 = 2 \times rand - 1 \quad (15)$$

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

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 network is a deep learning method for image processing and classification, and its input should be in the form of images. VGG19 uses the incoming traffic coding into the images for network traffic classification. Suppose that K features select from the dataset in the feature selection step. A K matrix is created if K examples of the attack class are isolated from the data set. Each column of this matrix is a selected feature. If the values of the matrix K normalize in K examples are between 0-255, 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 normal traffic classes. A set of normal traffic samples are created as standard color images, and attack traffic samples are created as attack images. Attack images and normal images are used to train CNN. A CNN neural network is trained by converting traffic samples into color images of attacks and normal traffic (Figure 10).

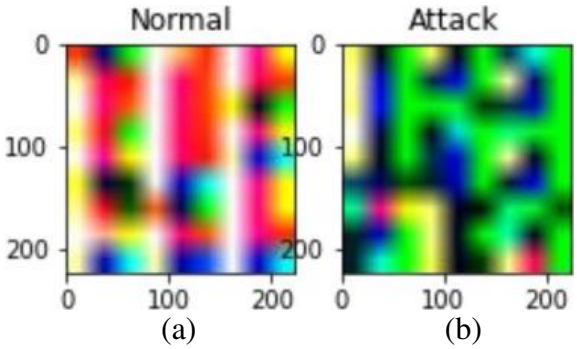

Figure 10: a) Traffic images, b) Attack images [47]

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.

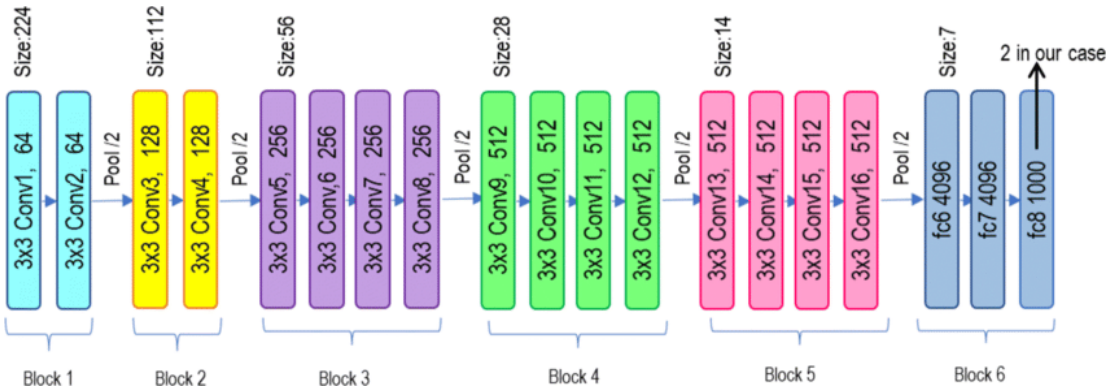

Figure 11: VGG19 neural network architecture

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 network and architectures like VGG19 have different meta-parameters. The precise adjustment of the learning parameters in the VGG19 neural network really 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 network'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 and 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 with 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 [48]. 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 equations 17, 18, and 19.

$$Accuracy = ACC = \frac{TP+TN}{TP+TN+FP+FN} \quad (17)$$

$$Sensitivity = Recall = DR = \frac{TP}{TP+FN} \quad (18)$$

$$Precision = P = \frac{TP}{TP+FP} \quad (19)$$

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

- 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.

4.3. 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 2 shows the proposed method's accuracy, sensitivity, and precision index in two VGG scenarios with and without the AO algorithm.

Table 2: Index of accuracy, sensitivity, and precision in four scenarios, balancing dataset by CGAN method

Scenarios	Accuracy	Sensitivity	Precision
S1	97.21	97.13	97.16
S2	98.82	98.25	98.64
S3	98.35	98.27	98.33
S4	99.82	99.69	99.76

Figure 12 visually shows the accuracy, sensitivity, and precision index in a bar chart. 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.

When the AO algorithm is used to select the features, the intrusion detection system's accuracy is greater than when it is utilized to optimize the AO parameters. In other words, using the AO algorithm in the feature selection phase has a greater impact on improving the accuracy of attack detection than using the AO algorithm to optimize the VGG19 parameters. In Table 2, regularization is applied using the CGAN method.

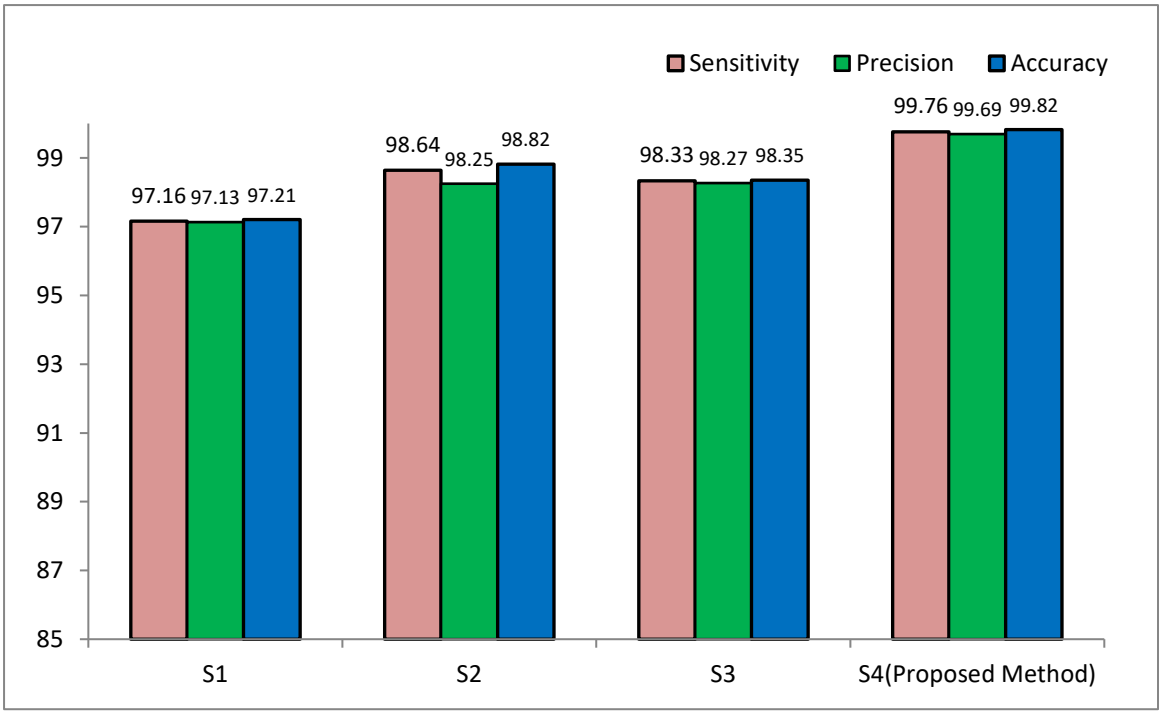

Figure 12: Evaluation of the proposed intrusion detection system in four scenarios with CGAN

If the GAN balancing method is used instead of CGAN in the experiments, the results of the scenarios will be according to Table 3. Figure 13 compares the accuracy, sensitivity, and precision index in four scenarios when balanced using the GAN method.

Table 3: Index of accuracy, sensitivity, and precision in four scenarios when the dataset was balanced using the GAN method

Scenarios	Accuracy	Sensitivity	Precision
S1	97.09	96.92	96.98
S2	98.51	98.02	98.22
S3	98.14	97.82	97.94
S4	98.62	98.23	98.25

Experiments show that if GAN is used instead of CGAN in balancing the data set, the proposed method's accuracy, sensitivity, and precision in detecting attacks will increase. If CGAN is used to balance the data set in the proposed method, the accuracy, sensitivity, and precision are 99.82%, 99.69%, and 99.76%, respectively. If the GAN method balances the data set, 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 data set, 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 [48], which used machine learning methods, such as HDT, DT, KNN, and SVM, to detect attacks on smart grids. Figure 15 diagram compares the accuracy, sensitivity, and precision of the proposed method in comparison with machine learning methods.

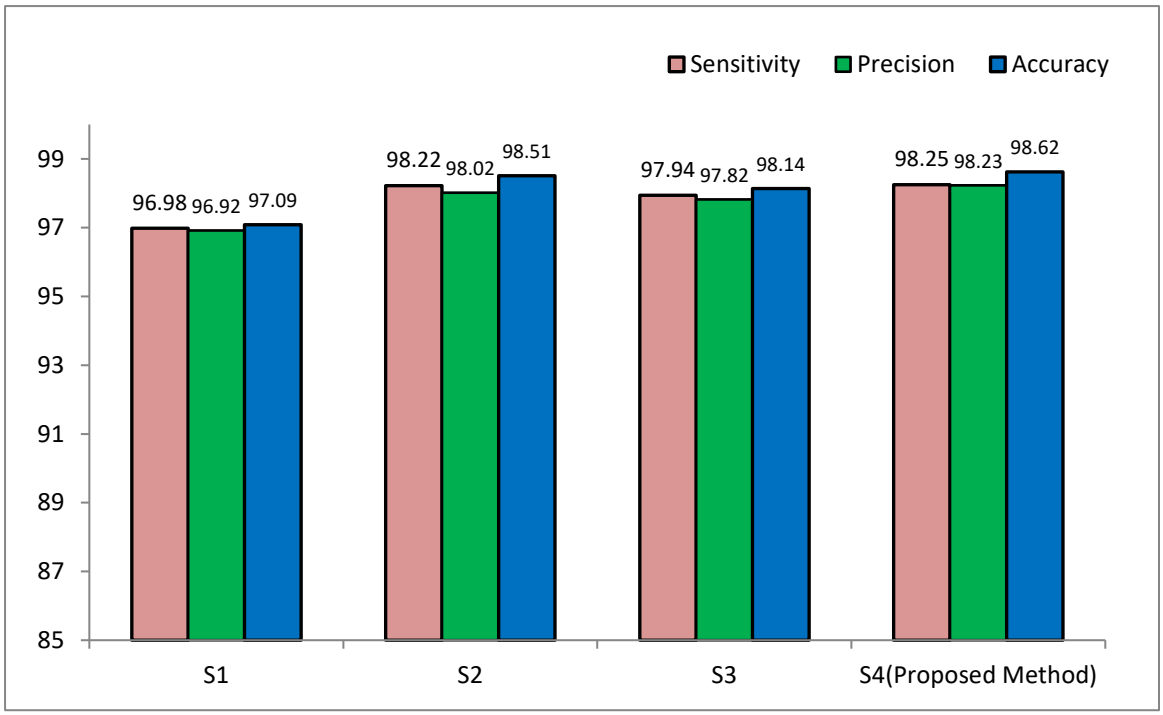

Figure 13: Evaluation of the proposed intrusion detection system in four scenarios using GAN balancing

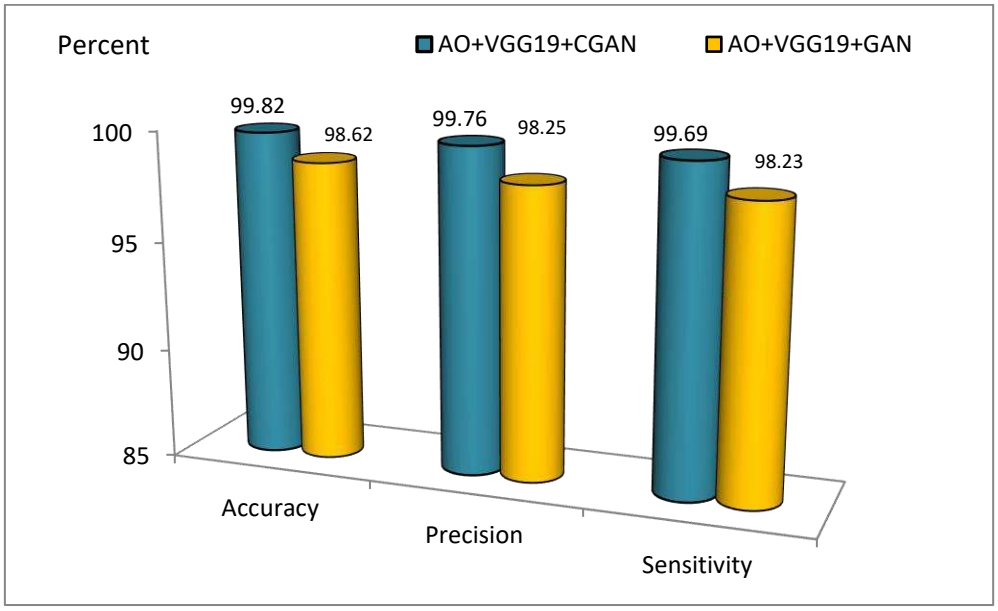

Figure 14: Comparison of the proposed balancing intrusion detection system using GAN and CGAN

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 [49]. Table 4 shows the comparison in terms of accuracy, sensitivity, and precision.

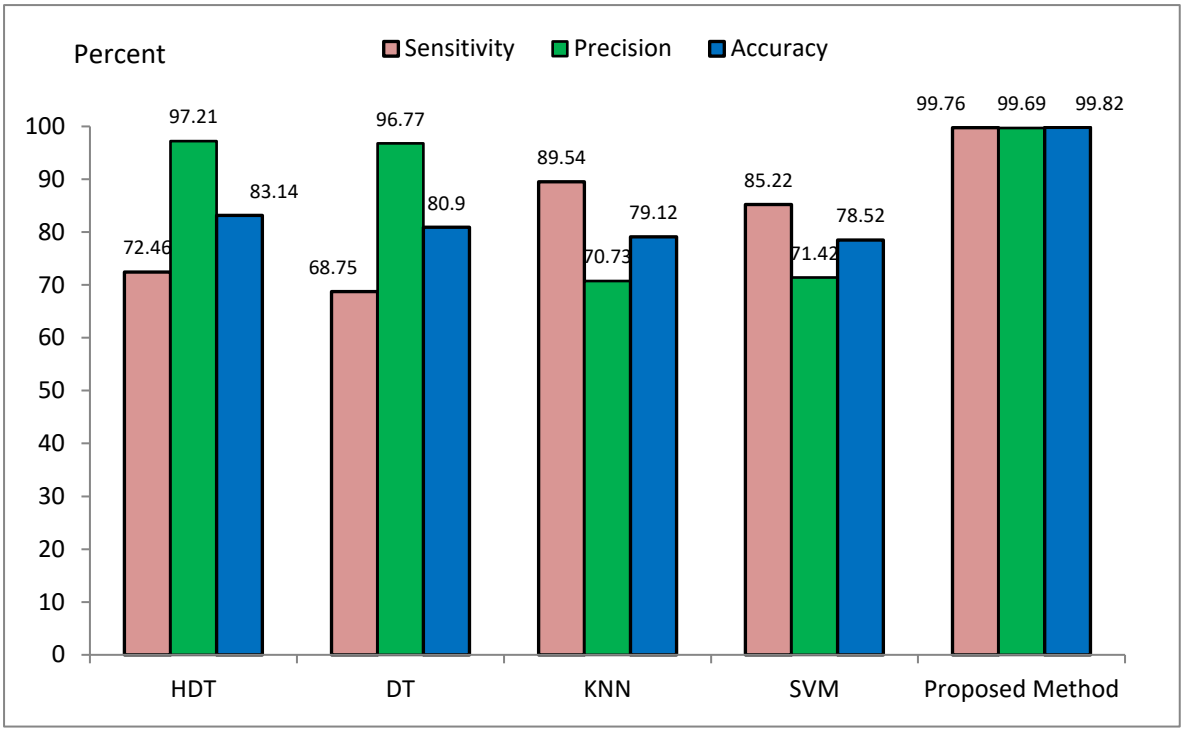

Figure 15: Comparison of the proposed intrusion detection system and machine learning methods

Table 4: 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

In [49], federated hierarchical learning is used to detect attacks on smart grids. Table 4 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 Figure 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.

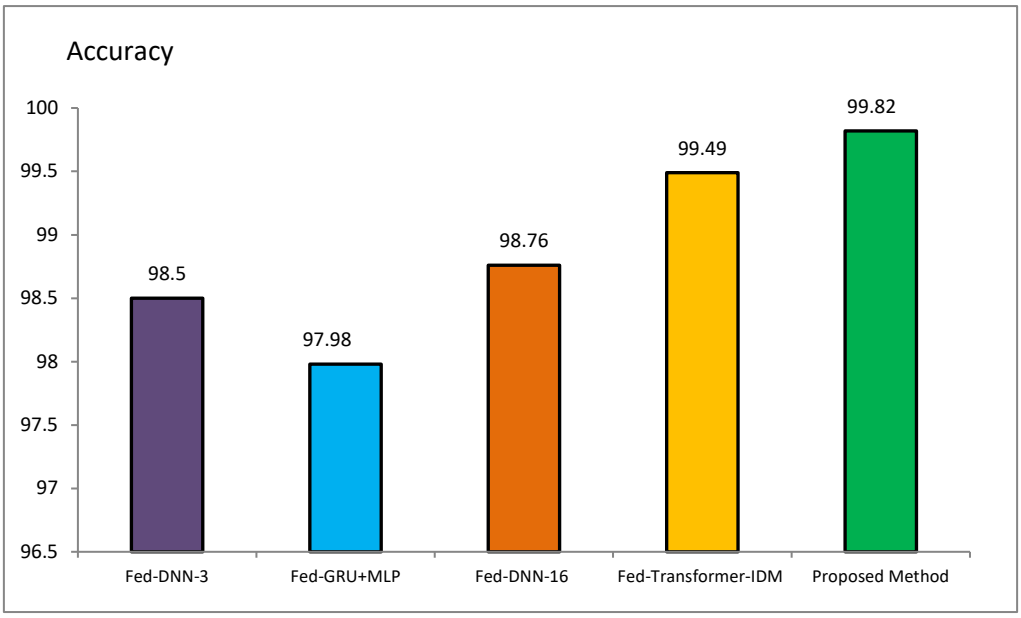

Figure 16: Comparison of the proposed intrusion detection system with federated learning methods

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 [50], 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 (Figure 17).

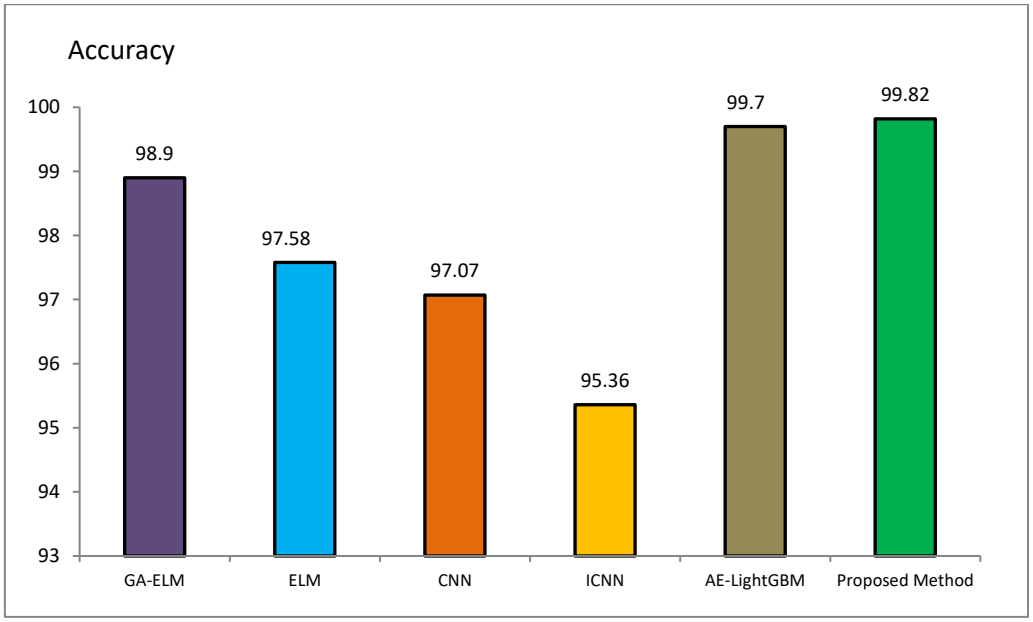

Figure 17: Comparison of the proposed method with extreme learning methods

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 Figure 18. For comparison, the results obtained in the research [51] are used, and the detection time of penetration is considered in seconds.

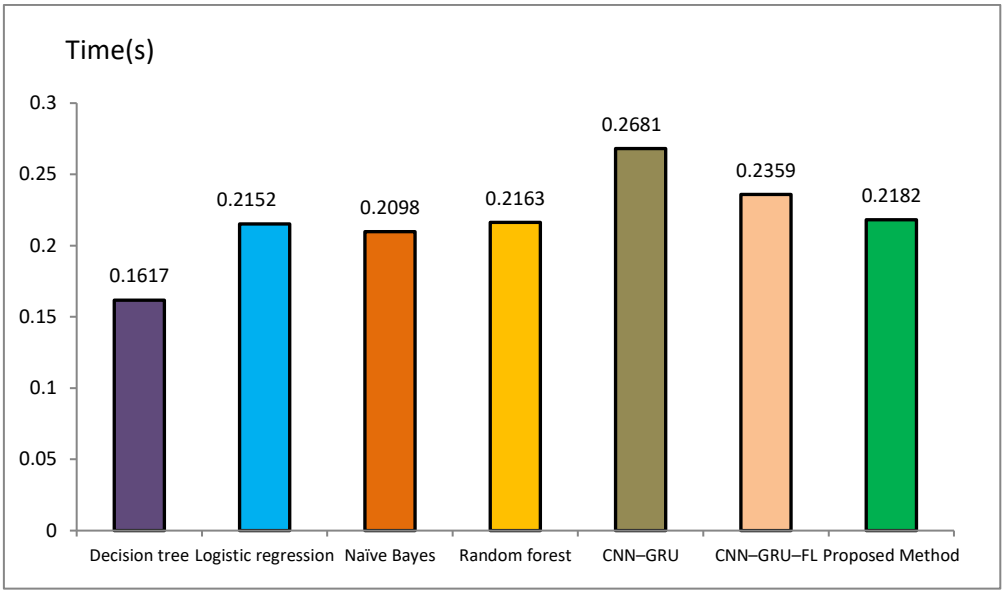

Figure 18: Comparison of attack detection time in seconds

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. Conclusion

Smart grids (SG) 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 providing 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 data set. In the third step, the training samples are converted to RGB color image format and coded to train the VGG19 architecture, a CNN neural network. The last step was VGG19 neural network training with RGB images and its hyper-parameters 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%. 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 generation networks is a recommendation for future work.

Declarations

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.

Competing Interests. The authors have no relevant financial or non-financial interests to disclose.

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

Authors' Contributions. Authors have contributed equally in the paper.

Availability of data and materials. Datasets used in the research are publicly available for download.

References

1. Ghiasi, M., Niknam, T., Wang, Z., Mehrandezh, M., Dehghani, M., & Ghadimi, N. (2023). A comprehensive review of cyber-attacks and defense mechanisms for improving security in smart grid energy systems: Past, present and future. *Electric Power Systems Research*, *215*, 108975.
2. Rath, C. K., Mandal, A. K., & Sarkar, A. (2023). Microservice based scalable IoT architecture for device interoperability. *Computer Standards & Interfaces*, *84*, 103697.
3. Padmanaban, S., Samavat, T., Nasab, M. A., Nasab, M. A., Zand, M., & Nikokar, F. (2023). Electric Vehicles and IoT in Smart Cities. *Artificial Intelligence-based Smart Power Systems*, 273-290.
4. Zhao, Y., Li, Q., Yi, W., & Xiong, H. (2023). Agricultural IoT Data Storage Optimization and Information Security Method Based on Blockchain. *Agriculture*, *13*(2), 274.
5. Siddiqui, S., Hameed, S., Shah, S. A., Khan, A. K., & Aneiba, A. (2023). Smart contract-based security architecture for collaborative services in municipal smart cities. *Journal of Systems Architecture*, *135*, 102802.
6. Ghiasi, M., Niknam, T., Wang, Z., Mehrandezh, M., Dehghani, M., & Ghadimi, N. (2023). A comprehensive review of cyber-attacks and defense mechanisms for improving security in smart grid energy systems: Past, present and future. *Electric Power Systems Research*, *215*, 108975.

7. Nafees, M. N., Saxena, N., Cardenas, A., Grijalva, S., & Burnap, P. (2023). Smart grid cyber-physical situational awareness of complex operational technology attacks: A review. *ACM Computing Surveys*, *55*(10), 1-36.
8. Gan, J., Zeng, L., Liu, Q., & Liu, X. (2023). A survey of intelligent load monitoring in IoT-enabled distributed smart grids. *International Journal of Ad Hoc and Ubiquitous Computing*, *42*(1), 12-29.
9. Ravinder, M., & Kulkarni, V. (2023, January). 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). IEEE.
10. Mirzaee, P. H., Shojafar, M., Cruickshank, H., & Tafazolli, R. (2022). Smart Grid Security and Privacy: From Conventional to Machine Learning Issues (Threats and Countermeasures). *IEEE Access*, *10*, 52922-52954.
11. Minh, Q. N., Nguyen, V. H., Quy, V. K., Ngoc, L. A., Chehri, A., & Jeon, G. (2022). Edge Computing for IoT-Enabled Smart Grid: The Future of Energy. *Energies*, *15*(17), 6140.
12. Bhattarai, T. N., Ghimire, S., Mainali, B., Gorjian, S., Treichel, H., & Paudel, S. R. (2022). Applications of smart grid technology in Nepal: status, challenges, and opportunities. *Environmental Science and Pollution Research*, 1-25.
13. Ghiasi, M., Wang, Z., Mehrandezh, M., Jalilian, S., & Ghadimi, N. (2023). Evolution of smart grids towards the Internet of energy: Concept and essential components for deep decarbonisation. *IET Smart Grid*, *6*(1), 86-102.
14. Jaiswal, D. M., & Thakre, M. P. (2022). Modeling & designing of smart energy meter for smart grid applications. *Global Transitions Proceedings*, *3*(1), 311-316.
15. Acarali, D., Rao, K. R., Rajarajan, M., Chema, D., & Ginzburg, M. (2022). Modelling smart grid IT-OT dependencies for DDoS impact propagation. *Computers & Security*, *112*, 102528.
16. Merlino, J. C., Asiri, M., & Saxena, N. (2022). Ddos cyber-incident detection in smart grids. *Sustainability*, *14*(5), 2730.
17. Haq, E. U., Pei, C., Zhang, R., Jianjun, H., & Ahmad, F. (2023). Electricity-theft detection for smart grid security using smart meter data: A deep-CNN based approach. *Energy Reports*, *9*, 634-643.
18. Albaseer, A., & Abdallah, M. (2022, December). 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). IEEE.
19. Eddin, M. E., Albaseer, A., Abdallah, M., Bayhan, S., Qaraqe, M. K., Al-Kuwari, S., & Abu-Rub, H. (2022). Fine-Tuned RNN-Based Detector for Electricity Theft Attacks in Smart Grid Generation Domain. *IEEE Open Journal of the Industrial Electronics Society*, *3*, 733-750.
20. Sarwar, A., Alnajim, A. M., Marwat, S. N. K., Ahmed, S., Alyahya, S., & Khan, W. U. (2022). Enhanced anomaly detection system for IoT based on improved dynamic SBPSO. *Sensors*, *22*(13), 4926.
21. Babu, K. S., & Rao, Y. N. (2023). MCGAN: Modified Conditional Generative Adversarial Network (MCGAN) for Class Imbalance Problems in Network Intrusion Detection System. *Applied Sciences*, *13*(4), 2576.
22. Abualigah, L., Yousri, D., Abd Elaziz, M., Ewees, A. A., Al-Qaness, M. A., & Gandomi, A. H. (2021). Aquila optimizer: a novel meta-heuristic optimization algorithm. *Computers & Industrial Engineering*, *157*, 107250.

23. Bhattacharya, S., Chengoden, R., Srivastava, G., Alazab, M., Javed, A. R., Victor, N.,... & Gadekallu, T. R. (2022). Incentive mechanisms for smart grid: state of the art, challenges, open issues, future directions. *Big Data and Cognitive Computing*, *6*(2), 47.
24. Muqeet, H. A., Liaqat, R., Jamil, M., & Khan, A. A. (2023). A State-of-the-Art Review of Smart Energy Systems and Their Management in a Smart Grid Environment. *Energies*, *16*(1), 472.
25. Tufail, S., Parvez, I., Batool, S., & Sarwat, A. (2021). A survey on cybersecurity challenges, detection, and mitigation techniques for the smart grid. *Energies*, *14*(18), 5894.
26. Abdalzaher, M. S., Fouda, M. M., & Ibrahem, M. I. (2022). Data privacy preservation and security in smart metering systems. *Energies*, *15*(19), 7419.
27. Kamiński, M. A. (2020). Operation "Olympic Games." Cyber-sabotage as a tool of American intelligence aimed at counteracting the development of Iran's nuclear programme. *Security and Defence Quarterly*, *29*(2), 63-71.
28. Haes Alhelou, H., Hamedani-Golshan, M. E., Njenda, T. C., & Siano, P. (2019). A survey on power system blackout and cascading events: Research motivations and challenges. *Energies*, *12*(4), 682.
29. Khazeiynasab, S. R., & Qi, J. (2021). Resilience analysis and cascading failure modeling of power systems under extreme temperatures. *Journal of Modern Power Systems and Clean Energy*, *9*(6), 1446-1457.
30. Pinto, S. J., Siano, P., & Parente, M. (2023). Review of Cybersecurity Analysis in Smart Distribution Systems and Future Directions for Using Unsupervised Learning Methods for Cyber Detection. *Energies*, *16*(4), 1651.
31. Liu, Q., Hagenmeyer, V., & Keller, H. B. (2021). A review of rule learning-based intrusion detection systems and their prospects in smart grids. *IEEE Access*, *9*, 57542-57564.
32. Sakhnini, J., Karimipour, H., & Dehghantanha, A. (2019, August). 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). IEEE.
33. Nafees, M. N., Saxena, N., Cardenas, A., Grijalva, S., & Burnap, P. (2023). Smart grid cyber-physical situational awareness of complex operational technology attacks: A review. *ACM Computing Surveys*, *55*(10), 1-36.
34. Kaur, D., Anwar, A., Kamwa, I., Islam, S., Muyeen, S. M., & Hosseinzadeh, N. (2023). A Bayesian Deep Learning Approach With Convolutional Feature Engineering to Discriminate Cyber-Physical Intrusions in Smart Grid Systems. *IEEE Access*, *11*, 18910-18920.
35. Jithish, J., Alangot, B., Mahalingam, N., & Yeo, K. S. (2023). Distributed Anomaly Detection in Smart Grids: A Federated Learning-Based Approach. *IEEE Access*.
36. Kumar, V., & Sinha, D. (2023). Synthetic attack data generation model applying generative adversarial network for intrusion detection. *Computers & Security*, *125*, 103054.
37. Cai, T., Jia, T., Adepu, S., Li, Y., & Yang, Z. (2023). ADAM: an adaptive DDoS attack mitigation scheme in software-defined cyber-physical system. *IEEE Transactions on Industrial Informatics*.
38. Neupane, R. L., Bhandari, P., Calyam, P., & Mitra, R. (2023, February). SGChain: Blockchain Platform for Availability Attack Mitigation in Smart Grid Environments. In *2023 International Conference on Computing, Networking and Communications (ICNC)* (pp. 324-330). IEEE.

39. Sivanesan, N., & Archana, K. S. (2023). Detecting distributed denial of service (DDoS) in SD-IoT environment with enhanced firefly algorithm and convolution neural network. *Optical and Quantum Electronics*, *55*(5), 393.
40. Sriranjani, R., Saleem, M. D., Hemavathi, N., & Parvathy, A. (2023, February). Machine Learning Based Intrusion Detection Scheme to Detect Replay Attacks in Smart Grid. In *2023 IEEE International Students' Conference on Electrical, Electronics and Computer Science (SCEECS)* (pp. 1-5). IEEE.
41. Massaoudi, M., Refaat, S. S., & Abu-Rub, H. (2022, March). Intrusion Detection Method Based on SMOTE Transformation for Smart Grid Cybersecurity. In *2022 3rd International Conference on Smart Grid and Renewable Energy (SGRE)* (pp. 1-6). IEEE.
42. Abdelkhalek, M., Ravikumar, G., & Govindarasu, M. (2022, April). Ml-based anomaly detection system for der communication in smart grid. In *2022 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)* (pp. 1-5). IEEE.
43. Taghavinejad, S. M., Taghavinejad, M., Shahmiri, L., Zavvar, M., & Zavvar, M. H. (2020, April). Intrusion detection in IoT-based smart grid using hybrid decision tree. In *2020 6th International Conference on Web Research (ICWR)* (pp. 152-156). IEEE.
44. Ding, P., Li, J., Wang, L., Wen, M., & Guan, Y. (2020). HYBRID-CNN: An efficient scheme for abnormal flow detection in the SDN-Based Smart Grid. *Security and communication networks*, *2020*, 1-20.
45. Chohra, A., Shirani, P., Karbab, E. B., & Debbabi, M. (2022). Chameleon: Optimized feature selection using particle swarm optimization and ensemble methods for network anomaly detection. *Computers & Security*, *117*, 102684.
46. Yadav, N., Truong, L., Troja, E., & Aliasgari, M. (2022, June). Machine Learning Architecture for Signature-based IoT Intrusion Detection in Smart Energy Grids. In *2022 IEEE 21st Mediterranean Electrotechnical Conference (MELECON)* (pp. 671-676). IEEE.
47. El-Ghamry, A., Darwish, A., & Hassanien, A. E. (2023). An optimized CNN-based intrusion detection system for reducing risks in smart farming. *Internet of Things*, *22*, 100709.
48. Taghavinejad, S. M., Taghavinejad, M., Shahmiri, L., Zavvar, M., & Zavvar, M. H. (2020, April). Intrusion detection in IoT-based smart grid using hybrid decision tree. In *2020 6th International Conference on Web Research (ICWR)* (pp. 152-156). IEEE.
49. Sun, X., Tang, Z., Du, M., Deng, C., Lin, W., Chen, J.,... & Zheng, H. (2022). A Hierarchical Federated Learning-Based Intrusion Detection System for 5G Smart Grids. *Electronics*, *11*(16), 2627.
50. Yao, R., Wang, N., Liu, Z., Chen, P., Ma, D., & Sheng, X. (2021). Intrusion detection system in the Smart Distribution Network: A feature engineering based AE-LightGBM approach. *Energy Reports*, *7*, 353-361.
51. Zhai, F., Yang, T., Chen, H., He, B., & Li, S. (2023). Intrusion Detection Method Based on CNN–GRU–FL in a Smart Grid Environment. *Electronics*, *12*(5), 1164.