Design and Development of a Secured Model for Attack Detection in Smart Grid

[1]Otuniyi M. Otukelu, and [2]Ayobami T. Olusesi
[1]Department of Electrical/Electronics Engineering, Olabisi Onabanjo University, Ogun State, Nigeria
[2]Department of Computer Engineering, Olabisi Onabanjo University, Ogun State, Nigeria
otuniyimotukelu@yahoo.comolusesi.ayobami@oouagoiwoye.edu.ng

Received: 09-SEPT-2026; Reviewed: 25-SEPT-2026; Accepted: 30-SEPT-2026
https://dx.doi.org/10.46792/fuoyejet.v11i3.1657

ORIGINAL RESEARCH

Abstract—The Smart Grid (SG) is a state-of-the-art electrical power system that offers a clean, safe, dependable, robust, efficient, and sustainable electrical network by combining information and communication technologies (ICT), cyber-secure two-way communication, and computational intelligence. By facilitating real-time monitoring, automated control, efficient energy management, prompt problem diagnosis, and improved decision-making, this enhances the overall performance, dependability, and security of grid operations. Smart grid communication technologies offer numerous benefits, including lower operational costs, more customer control, and real-time energy usage monitoring. Despite all of the aforementioned advantages of smart grids, the integration of communication devices introduces significant security challenges, making effective attack detection one of the most critical and difficult issues in smart grid networks. Therefore, the aim of this study is to create a machine learning-driven attack detection model using Enhanced Ant Lion Optimization Algorithm (EALOA). In addition to offering a reliable classification within the smart grid network, the developed EALOA was intended to enhance the feature selection process by overcoming the drawbacks of the traditional Ant Lion Optimization (ALO) algorithm, specifically its slow convergence speed and decreased optimization efficiency when solving complex optimization problems. MATLAB was used to implement and assess the generated EALOA model. From the obtained result, EALOA achieved a better accuracy of 96.3% and precision of 95.6% at 300 iterations when compared with existing method. This indicate the effectiveness and better performance of EALOA in identifying and thwarting assaults in smart grid systems.

Keywords— Accuracy, EALOA, Smart Grid, Attack, Precision.

1 INTRODUCTION

The power grid technology is a network that is connected and sends the electric energy from production facilities to end users. The functioning of the power grid is a result of its components synchronously synchronized to achieve a balance between supply and demand. According to Maheshwari et al. (2023), the power grid is an important mechanism in promoting economic growth as well as the energy needs of the commercial, industrial and residential sectors. But the traditional systems rely on physical protection devices at various points in the power grid network to ensure the safety and reliability of the equipment. In addition to that, monthly meter readings are used to measure electricity use for billing purposes. This conventional approach is effective for many years but now faces challenges due to the increasing use of distributed energy resources (DERs), increased demand for electricity and the need for automation and real-time monitoring to improve grid resilience (Alsuwian et al., 2022).

Moreover, despite its importance in modern society, traditional electric power infrastructure is vulnerable to aging structures that are incapable of withstanding disruption and increasing complexity of operations. These flaws have hastened the development of the smart grid (SG), which integrates cutting-edge automation, communication, and information technologies to enhance the electric power system's intelligence, resilience, efficiency, and dependability. (Moretti et al. 2017). Integrated with the advanced monitoring and bi-directional communication systems, SG is more flexible, sustainable and ensures secure energy supply (Huseinovic et al., 2020). Intelligent sensors, smart meters, data concentrators, communication networks, and advanced data analytics platforms are just a few of the many interconnected technologies that have made SG a sophisticated system. These technologies have turned conventional power systems into intelligent electricity networks that can optimize the entire electricity supply chain while integrating cutting-edge control, communication, and information technologies.

Despite the resilience of SG networks, the intricate control and communication network of the smart grid is vulnerable to attacks (Alsuwian et al. 2022). Malicious entities may find the SG appealing because internet-based protocols are employed for surveillance and control (Gunduz & Das, 2020). One of the most important issues facing contemporary SG systems is protecting the SG from attack. As societies grow more reliant on digital technology for the production, transmission, distribution, and administration of power, safeguarding the electrical grid against cyber threats is crucial. This is especially crucial for SG, which have become an essential part of contemporary energy infrastructure because of their capacity to facilitate intelligent control, real-time monitoring, integration of renewable energy sources, and effective energy management. (Pourmirza and Srivastava, 2020).

The security issue in the SG has been addressed by a number of discoveries over the past decades. Asuhaimi et al. (2019) proposed integrating Heterogeneous Cellular Networks (HetNets) into SG NANs. The proposed framework includes a distributed intelligent channel access scheme and a power control mechanism to maximize energy efficiency while meeting communication delay constraints. Aladdin et al. (2020) created a Multi-Agent Reinforcement Learning for Smart Grids (MARLA-SG) to improve the effectiveness of demand response in Smart Grid (SG) settings. Barajas-Villarruel et al. (2022) proposed optimization models that make use of the energy hub idea. The authors suggested a dual-framework strategy: a mixed-integer linear programming (MILP) model. Using the current infrastructure, the suggested model significantly improved the energy aim by 30%, demonstrating its

Corresponding Author
Section B- ELECTRICAL/COMPUTER ENGINEERING & RELATED SCIENCES
Can be cited as:
Otukelu O. M., and Olusesi A. T., (2026). Design and Development of a Secured Model for Attack Detection in Smart Grid. FUOYE Journal of Engineering and Technology (FUOYE**JET**), **11(3), 1-3.** https://dx.doi.org/10.46792/fuoyejet.v11i3.1657

© 2026 The Author(s). Published by Faculty of Engineering, Federal University Oye-Ekiti.
This is an open access article under the CC BY NC license. (https://creativecommons.org/licenses/by-nc/4.0/)

feasibility for large-scale energy management.In order to increase the energy efficiency of smart houses, Alhasnawi et al. (2021) suggested an optimization model for Time-of-Use (ToU) scheduling in Residential Energy Management (REM) systems. The suggested methodology makes it easier to operate residential microgrids by figuring out how different household appliances and sensors prefer to consume energy.

SG abnormalities and assaults, can be successfully identified using data-driven methods like machine learning, deep learning, and artificial intelligence. Current research has increasingly concentrated on AI-driven detection techniques, especially those based on machine learning and edge intelligence (Sanjalawe et al. 2025). Wang et al. (2020a) developed a location model using deep learning. This was hybridized with CNN to filter poor data and also to capture the inaccurate power flow measurement. Zhao et al. (2017) proposed a model for a generic FDIA attack to determine the gap between obtained and predicted measures. Additionally, a detector is suggested to address key estimations and verify the limitations of the earlier detectors. An adaptive sliding mode controller was developed by Li et al. (2021) to identify dynamic load altering attacks. The designed controller can guaranty the dependable operations of the power system that is being assaulted. Additionally, the effect of many attacks is eliminated by estimating the upper bound of the attack signals. Nath et al. (2019) assert that they have created the fastest intrusion detection algorithm for FDIA detection. The technique is said to reduce the worst-case detection delay while detecting abrupt system modifications and FDIA attacks. Dou et al. (2020) introduce a hybrid FDIA detection mechanism to ensure the security of power system operations and control. The proposed mechanism combines machine learning and variational mode decomposition (VMD) technologies. To find and identify fake data, Hu et al. (2015) combined the weighted residual approach with equivalent measurement transformation. Yang et al. (2020) presented a learning machine approach to decrease the feature vectors redundancies. Jiang et al. (2017) present a power load forecasting model based on the paradigm of cyberphysical-social systems to account for social implications for load balancing. Li et al. (2021) presented an approach to solve the issue of delay in powers system using the approximation-based technique. Wu et al. (2020) investigate on the effects of FDIA in smart grids. Although it is only applicable to small topologies, a technique based on pattern extraction was proposed by Wang et al. (2020b) to reconstruct the entire attack path for all network attacks. Oozeer and Haykin (2019) developed a physical model to capture the cognitive dynamic system. However, the exact sensor affected by the attack could not be identified. Demir et al. (2018) employed a pseudo-state estimate technique to determine the DoS attack or clock accuracy. It provides dependable and useful outcomes and is based on a proof-of-concept prototype. Wang et al. (2017) presented a strategy to investigate the attackers and defenders interaction on how data can be protected in metering infrastructure. Risbud et al. (2020) aimed to prevent power grid spoofing attacks on the dynamic network model and the phasor measurement unit model.

Machine learning (ML), which enables computer systems to learn from historical data, identify hidden patterns, and make intelligent judgments or predictions without explicit programming, is one of the most important and rapidly expanding subfields in artificial intelligence (AI). Oluwole et al. (2026) presented a machine learning-based DDoS attack detection system to stop source-side attacks in VoIP networks. VoIP traffic was used as a classification problem, extracted SIP message features, and used slow droid to test actual attacks. In order to identify the distinctive features of both benign and malevolent system activities, machine learning models are trained on historical information. Nature-inspired machine learning methods are more effective than the conventional optimization strategy (Diaba et al., 2023). In engineering applications, optimization techniques are employed to determine the optimal solution. Because the algorithms are easy to develop and rely on relatively simple concepts, they do not require gradient information, which contributes to their wide variety of applications. Numerous problems in a variety of fields can be resolved using the nature inspired algorithms (Omar et al., 2022). Grasshopper optimization algorithm (GOA), sperm whale algorithm (SWA), dragon fly algorithm (DFA), particle swarm optimization (PSO), ant colony algorithm (ACO), ant lion optimization algorithm (ALOA), water strider algorithm (WSA), and bat algorithm (BA), from nature (Valdez et al, 2021).

Despite these developments, current approaches have not been able to strike a compromise between computing efficiency and detection sensitivity. Additionally, even while the literature now in publication covers a variety of SG security vectors, these methods frequently fail to address the growing sophistication of assaults and the intrinsic complexity of SG systems. A stronger attack detection system is needed to solve this. By creating a robust detection method that protects the SG from assault while improving overall system dependability and classification accuracy, this study fills this gap. Therefore, in order to detect and prevent smart grid against sophisticated attacks or vulnerabilities, this study developed a machine learning-driven approach model for attack detection in smart gird using the enhanced ant lion optimization algorithm (EALOA). The study created an improved method to boost the accuracy and precision of the ant lion optimization (ALO) algorithm, which struggles with slow convergence in challenging optimization situations (Tian et al. 2018). MATLAB was used to run the EALOA model. Accuracy and precision were employed as performance indicators to compare EALOA with previous research.

2 MATERIALS AND METHOD

This study proposes an AI-based solution for the data-driven security component of the smart grid system using machine learning and the optimal features subset. To accomplish this, it is essential to use the right feature selection. The enhanced ant lion optimization algorithm (EALOA) method was applied to select the best features from a given set of attributes while CIC-IDS-2017 databases serve as the study's data sets. Reading and going through each of the CIC-IDS-2017 datasets one at a time is the first step. Data preparation, the second step, entails scaling the data by performing data normalization after removing any outliers and substituting the mean for missing values. The enhanced ALOA (EALOA) technique is used in the third phase, optimal feature

© 2026 The Author(s). Published by Faculty of Engineering, Federal University Oye-Ekiti.
This is an open access article under the CC BY NC license. (https://creativecommons.org/licenses/by-nc/4.0/)

http://.doi.org/10.46792/fuoyejet.v11i3.1657 engineering.fuoye.edu.ng/journal

selection, which is the last stage of data preparation. Feeding machine learning-selected models with relevant features from EALOA is the fourth stage. The created model was used to label, train, and test the data in the fifth stage.

2.1 Data Set

An enhanced version of the KDDCUP99 dataset is called CIC-IDS-2017. The most recent threats and features are included in this state-of-the-art dataset, which satisfies all criteria for real-world attacks, including the most recent network attacks, to evaluate the effectiveness of an attack detection system. The dataset has been utilized for a variety of research analyzes and the creation of new models and algorithms, highlighting threats that the earlier databases did not address. It also evaluates the effectiveness of a set of network traffic data using machine learning methods to determine the best feature set for detecting an attack.

2.2 Data Preprocessing

After the datasets were chosen, they underwent data cleaning techniques to remove noise and normalize the features. Although a number of normalization techniques are explored, min-max normalization is used in this study because it scales well and solves the issues with z-score normalization brought on by outliers.

2.3 Feature Selection

Not only is feature optimization a precision improvement process, it also improves detection rate and efficiency of the system. The goal of feature optimization is to identify which features are most informative and can be easily used by different classifiers to achieve better results. The feature selection is based on the classification of the best classifier and the most informative set of features from the traffic data in the network and will improve the accuracy of classification and reduce the size of the dataset. To achieve this goal, metaheuristic optimization techniques are often used to explore the feature space for the best classifier and feature set. In this context, the enhanced ant lion optimization (EALOA), a nature-inspired metaheuristic, was used for feature selection and dimensionality reduction on the network traffic dataset.

2.4 Ant Lion Optimization

The Ant Lion Optimization Algorithm (ALOA) is a metaheuristic optimization technique that draws inspiration from nature. ALOA is based on the ant lion predator mechanism. The two primary phases of an ant lion's life cycle are larvae and adults. A natural lifespan of three years is achievable, and it primarily occurs in larvae (3 to 5 weeks for adults). Ants go through a metamorphosis in a cocoon to become adults (Guo et al., 2020). As larvae, they hunt, and as adults, they procreate. The ant lion's hunting behavior is seen in Figure 1. It has demonstrated excellent optimization abilities in a range of difficult applications, drawing inspiration from the natural hunting strategy of antlion larvae and as well surpasses a number of well-known optimization techniques, such as the Genetic Algorithm (GA) and Particle Swarm Optimization (PSO), in tackling a variety of engineering optimization problems, according to comparative studies. The mathematical model of the ALOA is based on the interaction between the antlion and the ants. The matrix shown in Equation (1) records the ant positions. The ant is evaluated using a fitness

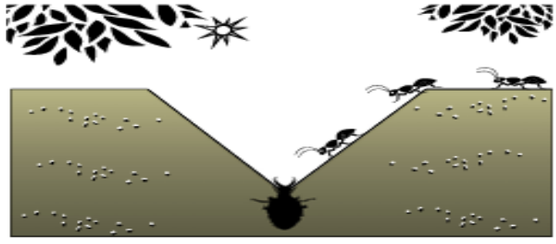

Fig. 1. Hunting Behavior of Ant Lion

(objective) function throughout optimization, and the fitness value of the outcomes is preserved using the following matrix.

$$M_{ant} = \begin{bmatrix} A_{1,1} & A_{1,2} & A_{1,d} \\ A_{2,1} & A_{2,2} & A_{1,d} \\ A_{n,1} & A_{n,2} & A_{n,d} \end{bmatrix} \quad (1)$$

The matrix in Equation (2) is used to store the fitness value that is determined throughout the optimization process so that each ant can be evaluated more effectively.

$$M_{OA} = \begin{bmatrix} f([AL_{1,1} & AL_{1,2} & AL_{1,d}]) \\ f([AL_{2,1} & AL_{2,2} & AL_{1,d}]) \\ f([AL_{n,1} & AL_{n,2} & AL_{n,d}]) \end{bmatrix} \quad (2)$$

M_{ant} is used to store the position of each ant

M_{OA} is the matric fitness value of each ant

n is the number of ant

d is the dimension of the variable

$AL_{i,j}$ is the value of the j_{th} dimension of the i_{th} ant lion

The ants move randomly around the antlion while searching for food within the search space, whereas the antlions construct traps to capture them. In the Ant Lion Optimizer (ALO), the ants' movement is modeled using a random walk, which simulates their stochastic exploration of the search space. This random walk is mathematically represented as shown in Equation (3)

$$X_{(t)} = [0;\ cumsum(2r(t_1)) - 1, \ldots\ldots, cumsum(2r(t_n)) - 1 \quad (3)$$

$$r = \begin{cases} 1 & if\ rand > 0.5 \\ 1 & if\ rand \leq 0.5 \end{cases} \quad (4)$$

$rand$ is uniformly distributed random number generated within the range of [0,1].

$X_{(t)}$ is the random walk step sequence, t is the indicates the current step of the random walk, and *r(t)* is a stochastic function defined by a uniformly distributed random variable rand within the interval [0, 1]. Every time the optimization procedure is repeated, each ant's position is updated. Equation (5) illustrates the normalization procedure used to guaranty that the random walks stay inside the search space's bounds (Tian, et al., 2018).

$$X_i^t = \frac{(x_i^t - a_i)(d_i^t - c_i^t)}{(b_i - a_i)} + c_i^t \quad (5)$$

a_i is the minimum value of the random walk of the ith variable

b_i is the minimum value of the random walk of the ith variable

c_i^t is the minimum value of the ith variable

d_i^t is the minimum value of the ith variable

At each iteration, every ant randomly selects an antlion to guide its movement. The selected antlion acts as a trap that influences the ant's random walk, thereby directing the search toward promising regions of the solution space. This interaction mimics the hunting behavior of antlions in nature, where ants wander randomly within the influence of an antlion's pit. The mathematical representation of this process is given as shown in Equations (6) and (7)

$$c_i^t = Antlion_j^t + c^t \quad (6)$$

© 2026 The Author(s). Published by Faculty of Engineering, Federal University Oye-Ekiti.
This is an open access article under the CC BY NC license. (https://creativecommons.org/licenses/by-nc/4.0/)

http://.doi.org/10.46792/fuoyejet.v11i3.1657 engineering.fuoye.edu.ng/journal

$$d_i^t = Antlion_j^t + d^t \quad (7)$$

$Antlion_j^t$ is the position of the selected j-th antlion at t-th iteration. c^t and d^t indicate the minimum and maximum values of all variables for the i-th ant at the t-th iteration.

The ALOA employs a roulette wheel selection mechanism to choose antlions according to their fitness values. Antlions with higher fitness have a greater probability of being selected, enabling better candidate solutions to exert more influence on the search process. As the optimization proceeds, the search region continues to shrink with each iteration, causing the ants to move increasingly closer to the selected antlions. This adaptive reduction in the search space enhances local exploitation, allowing the algorithm to refine candidate solutions and improve convergence toward the global optimum. The mathematical formulation describing the adaptive reduction of the trap radius (search boundary) with increasing iterations is presented in Equations (8) and (9).

$$c^t = c^t / I \quad (8)$$

$$d^t = d^t / I \quad (9)$$

After an ant is successfully trapped, the antlion updates its position to that of the captured ant if the ant represents a better solution. This strategy allows the antlion to improve its fitness and increases its likelihood of attracting and capturing other ants in subsequent iterations. By continuously replacing inferior antlion positions with better ant positions, the algorithm preserves high-quality solutions and accelerates convergence toward the global optimum. The mathematical expression for this position update is shown in Equation (10).

$$Antlion_j^t = Ant_i^t \; if \; f(Ant_i^t) > f(Antlion_j^t) \quad (10)$$

$Antlion_j^t$ is the position of the j-th antlion selected at the t-th iteration, Ant_i^t is the position of the i-th ant at the t-th iteration and f is the objective function. In each iteration, the antlion with the best fitness is retained as the elite antlion. This elite solution is preserved throughout the optimization process and guides the movements of all ants, preventing the algorithm from losing the best solution found so far. The mathematical expression for the position of the i-th ant at the t-th iteration is shown in Equation (11)

$$Ant_i^t = \frac{R_A^t + R_E^t}{2} \quad (11)$$

R_A^t and R_E^t are the random walk around elite at the t-th iteration. Consequently, every ant performs a random walk influenced by two antlions simultaneously: the antlion selected through the roulette wheel mechanism and the elite antlion. ALOA demonstrates its superiority by proving its ability to solve a wide range of applications, such as feature selection, networking, economic power dispatch planning, optimal reactive dispatch problem, proportional integral derivative controller, economic load dispatch problem, quadratic assignment problem among others.

2.5 Enhanced Ant Lion Optimization Algorithm (EALOA)

Because ALO effectively balances exploration and exploitation, it surpasses a number of well-known optimization techniques, in tackling a variety of engineering optimization problems, according to comparative studies. But the Ant Lion Optimizer (ALO) has several drawbacks, just like a lot of other sophisticated optimization techniques. These include a propensity to get stuck in local optima and a comparatively slow rate of convergence, especially when tackling challenging, high-dimensional optimization problems. As a result, its optimization performance can still be improved to increase resilience, convergence speed, and solution correctness (Tian et al., 2018). This study developed an Enhanced Ant Lion Optimization Algorithm (EALOA) that combines the advantages of Cuckoo Search (CS). Cauchy mutation in CS enables ALOA to overcome the shortcomings of the traditional ALOA. Cauchy Mutation which is one of the properties of CS was employed to enhance ant population variability, expand the search space, quicken the rate of convergence, and improve the search ability. This helped to improve the ALOA exploration and exploitation capabilities, convergence is accelerated, solution accuracy is increased, and the chance of premature convergence to local optima is decreased. The following is the definition of the origin-centered 1D Cauchy density function as shown in Equation (12).

$$f(x) = \frac{1}{\pi}\left(\frac{t}{x^2 + t^2}\right) \quad (12)$$

The ants spend more time looking for the global optima and less time searching the nearby intervals following Cauchy mutation. Consequently, Cauchy mutation helps to boost population variety and improved the EALOA capacity for global searches. The Cauchy mutation that an ant undergoes in this work was computed as shown in Equation (13).

$$Ant_i^{t+1} = Ant_i^t + \oplus \; Cauchy\,(0,1) \quad (13)$$

$Cauchy\,(0,1)$ is the random number produced by the Cauchy distribution at t = 1.

The Cauchy mutation and cuckoo search were used alternately as shown in Equation (14).

$$\begin{cases} Ant_i^* = Ant_i^t + \beta_0(Ant_i^t - elite) \oplus Levy(\delta), & p < 0.5 \\ Ant_i^* = Ant_i^t + \oplus \; Cauchy\,(0,1), & p \geq 0.5 \end{cases} \quad (14)$$

where p is a random number in [0,1]

After the mutation operation, a greedy criterion is employed as shown in Equation (15) to compare the fitness of the mutated ant with that of its original position. If the mutated position yields a better fitness value, the ant's position is updated to the new solution; otherwise, the original position is retained. This strategy ensures that only improvements are accepted, thereby enhancing the quality of the population while preventing deterioration in solution performance.

$$\begin{cases} Ant_i^{t+1} = Ant_i^* & f(Ant_i^*) > f(Ant_i^t) \\ Ant_i^{t+1} = Ant_i^* & f(Ant_i^*) \leq f(Ant_i^t) \end{cases} \quad (15)$$

Algorithm 1: Enhanced Ant Lion Optimization Algorithm (EALOA)

Set the parameters:

The population size N, the dimension d, maximum iteration number T

Initialize ant and antlions randomly

Calculate the antlions fitness and the best antlion as elite

While $(t < T)$

  For $i = 1$ *to* N

    Select an antlion using the roulette wheel

Update the boundary of a random walk using Equations (8) and (9)

Create a random walk and normalize it using Equation (3),(4) and (5)

Update ants positions using Equations (11) ,(13) and (14)

End For

© 2026 The Author(s). Published by Faculty of Engineering, Federal University Oye-Ekiti.

This is an open access article under the CC BY NC license. (https://creativecommons.org/licenses/by-nc/4.0/)
http://.doi.org/10.46792/fuoyejet.v11i3.1657 engineering.fuoye.edu.ng/journal

Replace an antlion with its corresponding ant using Equation (10).

For $i = 1$ *to* N

Update ants positions using Equations (8),(9) and (10)

Update the elite of antlion ants' positions

$t = t + 1$

End While

2.6 Evaluation Metrics

Accuracy, and precision are the performance indicators utilized to assess the developed model in this study. The performance indicators mentioned above are based on True Positive (TP), False Negative (FN), True Negative (TN), and False Positive (FP).

Accuracy: The number of instances that are accurately categorized as normal and attack classes is known as accuracy. By dividing the entire number of cases represented in Equation (16) by the sum of correctly classified instances, accuracy is attained.

$$\text{Accuracy} = \frac{TP+TN}{TP+FP+FN+TN} \quad (16)$$

Precision: Assessing the true positive (TP) entities in connection to false positive (FP) entities is the precision goal. The approach for precision is shown in Equation (17)

$$\text{Precision} = \frac{TP}{TP+FP} \quad (17)$$

3 RESULT AND DISCUSSION

The results of the enhanced ant lion optimization algorithm (EALOA) model for attack detection were presented. The feature selection of the data set is crucial throughout the data preprocessing phase. Finding feature subsets that can collaborate with various classifiers to achieve improved outcomes is the primary goal of feature optimization. Therefore, in this study, the enhanced ant lion optimization (EALOA) algorithm approach was used for feature selection. The study's experiment and simulation were carried out using an Intel Core i7 CPU, 8GB of RAM, a 500GB SSD, the MATLAB programming environment, and Windows 10. The CIC-IDS-2017 dataset was used to evaluate this developed model. In order to verify the effectiveness of (EALOA), the model's performance was assessed by contrasting it with the current Genetic Algorithm (GA), Particle Swarm Optimization (PSO), Improved Gravitational Search Algorithm (IGSA), and Ant Lion Optimization Algorithm (ALOA). Tables 1, 2, and Figure 2, 3 present a performance comparison between EALOA and the current feature selection methods (GA, PSO, GSA and ALOA) on the CIC-IDS-2017 dataset. The two parameters that served as the foundation for the assessment were accuracy and precision.

3.1 Accuracy

As shown in Table 1 and Figure 2, the developed Enhanced Ant Lion Optimization Algorithm (EALOA) outperformed the benchmark optimization algorithms Genetic Algorithm (GA), Particle Swarm Optimization (PSO), Improved Gravitational Search Algorithm (IGSA) and Ant Lion Optimization Algorithm (ALOA) in terms of classification accuracy on the CIC-IDS-2017 dataset.

Table 1. Accuracy for CIC-IDS-2017 data set

Iteration	GA	PSO	IGSA	ALOA	**EALOA**
50	0.532	0.591	0.733	0.832	**0.881**
100	0.583	0.602	0.764	0.845	**0.883**
150	0.623	0.642	0.792	0.861	**0.905**
200	0.684	0.721	0.816	0.884	**0.924**
250	0.742	0.748	0.832	0.905	**0.952**
300	0.755	0.79	0.885	0.916	**0.963**

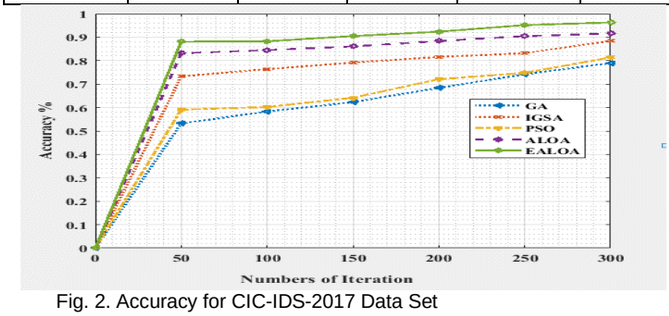

Fig. 2. Accuracy for CIC-IDS-2017 Data Set

Table 1 and Figure 2 demonstrate that the EALOA outperforms the current Genetic Algorithm (GA), Particle Swarm Optimization (PSO), and Improved Gravitational Search Algorithm (IGSA) in terms of classification accuracy on the CIC-IDS2017 dataset. The EALOA model outperformed GA (58.3%), PSO (60.2%), IGSA (76.4%) and ALOA (84.5%) with an accuracy of 88.3% after 100 iterations. The generated model attained an accuracy of 96.3% when the number of iterations was extended to 250, while the corresponding results for GA, PSO, IGSA and ALOA were 74.2, 74.8, 83.2 and 90.5%.

3.2 Precision

The Enhanced Ant Lion Optimization Algorithm (EALOA) outperformed the benchmark optimization algorithms, namely the Genetic Algorithm (GA), Particle Swarm Optimization (PSO), Artificial Bee Colony (ABC), Improved Gravitational Search Algorithm (IGSA), on the CIC-IDS-2017 dataset, as shown in Table 2 and Figure 3.

Table 1. Precision for CIC-IDS-2017 data set

Iteration	GA	PSO	IGSA	ALOA	**EALOA**
50	0.622	0.664	0.722	0.751	**0.852**
100	0.643	0.672	0.787	0.825	**0.891**
150	0.657	0.691	0.818	0.844	**0.903**
200	0.713	0.735	0.829	0.861	**0.927**
250	0.708	0.746	0.841	0.911	**0.944**
300	0.724	0.752	0.868	0.937	**0.956**

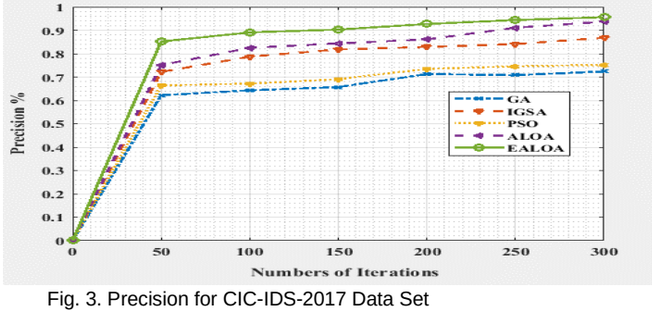

Fig. 3. Precision for CIC-IDS-2017 Data Set

The EALOA model outperformed GA (64.3%), PSO (67.2%), IGSA (78.7%), and ALOA (82.5%) with a precision of 89.1% after 100 iterations. EALOA attained a precision of 94.4% when the number of iterations was raised to 250, while GA, PSO, IGSA, and ALOA achieved 70.8%, 74.6%, 84.1%, and 91.1%, respectively. The

© 2026 The Author(s). Published by Faculty of Engineering, Federal University Oye-Ekiti.
This is an open access article under the CC BY NC license. (https://creativecommons.org/licenses/by-nc/4.0/)

http://.doi.org/10.46792/fuoyejet.v11i3.1657 engineering.fuoye.edu.ng/journal

simulated results shows that as the number of iterations increases, the EALOA model's precision steadily increases. EALOA fared better than the current optimization methods in every experimental situation, demonstrating its greater capacity to precisely detect attack cases. This increased precision attests to the established optimization algorithm's efficacy in enhancing SG's robustness, performance, and dependability.

4 CONCLUSION

The growing need for efficiency, sustainability, dependability, and security is causing the global energy scene to rapidly change. Conventional power grids, which were initially intended for one-way power flow and centralized electricity generation, are starting to fall short of the demands of contemporary energy systems. Grid operations are becoming much more complex due to the increasing integration of distributed energy resources, renewable energy technologies, bidirectional power flows, and dynamic load changes. Power generation, transmission, substations, distribution, and consumption are all integrated into a secure, dependable, robust, effective, and sustainable system by the smart grid (SG), an enhanced electrical network. It makes use of computational intelligence, cyber-secure two-way communication, and information and communication technologies (ICT) to provide real-time power system monitoring, control, and optimization. Despite these benefits, smart grid systems' extensive reliance on interconnected communication networks which are susceptible to a variety of cyberattacks makes guaranteeing their security a major concern. This study developed an Enhanced Ant Lion Optimization Algorithm (EALOA) model for optimal feature selection in order to improve the accuracy and precision of attack detection in smart grid networks. The model enhances the traditional Ant Lion Optimization (ALO) algorithm's global search capabilities, convergence speed, and ability to avoid local optima by incorporating Cuckoo Search (CS). By choosing the most pertinent features from attack detection datasets, this hybrid optimization method increases the effectiveness of the attack detection procedure. The EALOA works better than current attack detection methods, according to MATLAB simulation trials utilizing the CIC-IDS-2017 datasets. However, despite these encouraging outcomes of this study, it is open to the following future work. Firstly, generalizability may be limited because our evaluation is based on public datasets rather than real-time smart-grid traffic. Secondly, the scope of the evaluation metrics was limited to accuracy and precision. Further studies can be done to determine computational time, F1-score and recall of the system. Lastly, research into how IoT sensors offer a thorough perspective on cyber-physical activities can as well be seen as one of the future paths for smart grids.

ACKNOWLEDGMENT

The content of this study is entirely the authors responsibility. The authors disclosed no conflicts of interest.

REFERENCES

Aladdin, S, El-Tantawy, S. Fouda, M.M. & Tag Eldien, A.S. (2020). MARLA-SG: Multi-Agent Reinforcement Learning Algorithm for Efficient Demand Response in Smart Grid. IEEE Access, 8, 210626–210639. https:// doi.org/10.1109/ACCESS.2020.3038863

Alhasnawi, B.N., Jasim, B.H., Rahman, Z.A., & Siano, P. A. (2021). Novel Robust Smart Energy Management and Demand Reduction for Smart Homes Based on Internet of Energy. Sensors 21, pp. 4756. https://doi.org/10.3390/s21144756

Alsuwian, T., Shahid Butt, A., & Ahmed Amin, A. (2022). Smart Grid Cyber Security Enhancements: Challenges and Solutions. A Review. Sustainability, 14, 1 – 21. https://doi.org/10.3390/su142114226

Asuhaimi, F.A., Bu, S., Klaine, P.V., & Imran, M.A. (2019). Channel Access and Power Control for Energy-Efficient Delay-Aware Heterogeneous Cellular Networks for Smart Grid Communications Using Deep Reinforcement Learning. IEEE Access, 7, 133474 – 133484. https://doi.org/10.1109/ACCESS.2019.2939827

Barajas-Villarruel, L.R., Rico-Ramirez, V., & Castrejón-González, E.O. (2022). Optimization models for the generation, distribution and transmission of electricity in a macroscopic system: Representation of operational regions as energy hubs. Chemical Engineering Research and Design. 187, 645–661. https:// doi.org/10.1016/j.cherd.2022.08.026

Demir, K., Ismail, H., Vateva-Gurova, T., & Suri, N. (2018). Securing the cloud-assisted smart grid. International Journal of Critical Infrastructure Protection, 23, 100–111. https:// doi.org/10.1016/j.ijcip.2018.08.004

Diaba, S.Y., Shafie-Khah, M., & Elmusrati, M. (2023). Cyber Security in Power Systems Using Meta-Heuristic and Deep Learning Algorithms. IEEE Access, 11, 18660 – 18672. https://doi.org/ 10.1109/ACCESS.2023.3247193

Dou,C., Wu,D., Yue, D., Jin, B., & Xu, S. (2020). A hybrid method for false data injection attack detection in smart grid based on variational mode decomposition and OS-ELM. CSEE Journal of Power And Energy Systems. 8 (6), 1 – 10. https:// doi.org/ 10.17775/CSEEJPES.2019.00670

Gunduz, M. Z., & R. Das, (2020). Internet of things (iot) Evolution, components and applications fields. Pamukkale University Journal of Engineering Sciences. 24 (2), 327 – 335. https:// doi.org/ 10.5505/pajes.2017.89106

Guo, M.W., Wang, J.S., Zhu, L.F., Guo, S.S.. & Xie, W. (2020). Improved Ant Lion Optimizer Based on Spiral Complex Path Searching Patterns, IEEE Access, 8, 22095 – 22126. https:// doi.org/ 10.1109/ACCESS.2020.2968943

Hu,Z., Wang, Y., Tian, X., Yang, X., Meng, D., & Fan, R. (2015). False data injection attacks identification for smart grids. In Proceedings of the 2015 Third International Conference on Technological Advances in Electrical, Electronics and Computer Engineering (TAEECE), Beirut, Lebanon, 139–143.https:// doi.org/ 10.1109/TAEECE.2015.7113615

Huseinovic, A., Mrdovic, S., Bicakci, K. & Uludag, S. (2020). A Survey of Denial-of-Service Attacks and Solutions in the Smart Grid. IEEE Access, 8, 177447–177470. https:// doi.org/ 10.1109/ACCESS.2020.3026923

Jiang, Q., Chen, H., Xie, L., & Wang, K. (2017). Real-time detection of false data injection attack using residual prewhitening in smart grid network. In Proceedings of the 2017 IEEE International Conference on Smart Grid Communications (SmartGridComm), Dresden, 83–88. https://doi.org/ 10.1109/SmartGridComm.2017.8340659

Li, J., Yang, D.F., Gao, Y.C., & Huang, X. (2021). An adaptive sliding-mode resilient control strategy in smart grid under mixed attacks. IET Control Theory and Application. 15, 1971–1986.

https://doi.org/10.1007/s12555-021-0916-0Maheshwari, M.K., Gupta, AK., Pathak, H.K., Khan4, H., & Maurya, A.K. (2023). Cyber Security in Power System: Challenges and Opportunities. Advancement and Research in Instrumentation Engineering, 6 (2), 1 – 18. https://doi.org/10.5281/zenodo.8112668

Moretti, Djomo, S. N., Azadi, H., May, K., De Vos,K., Van Passel, S., & Witters, N. (2017). A systematic review of environmental and economic impacts of smart grids, Renewable and Sustainable Energy Reviews 68, 888–898.https://doi.org/10.1016/j.rser.2016.03.039

Nath, S., Akingeneye, I., Wu, J., & Han, Z. (2019). Quickest detection of false data injection attacks in smart grid with dynamic models. IEEE Journal of Emerging and Selected Topics in Power Electronics , 10 (2), 1292–1302. https:// doi.org/ 10.1109/JESTPE.2019.2936587

Omar, M.B., Bingi, K., Prusty, B., & Ibrahim, R. (2022). Recent Advances and Applications of Spiral Dynamics Optimization Algorithm: A Review. Fractal and Fractional, 6, (27), 1 – 31. https://doi.org/10.3390/fractalfract6010027

Oluwole, A.S., Akhionbare, H.E., & Akinsanmi, O. (2026). Detection of Distributed Denial of Service Attacks in a VOIP Network using Machine

© 2026 The Author(s). Published by Faculty of Engineering, Federal University Oye-Ekiti.
This is an open access article under the CC BY NC license. (https://creativecommons.org/licenses/by-nc/4.0/)

Learning Technology and OPNET Modeler. FUOYE Journal of Engineering and Technology, 11 (2), https://dx.doi.org/10.46792/fuoyejet.v11i1.1602

Oozeer, M.I., & Haykin, S. (2019). Cognitive risk control for mitigating cyber-attack in smart grid. IEEE Access, 7, 125806–125826.https://doi.org/10.1109/ACCESS.2019.2939089

Pourmirza, Z & Srivastava, A. (2020). Cybersecurity Analysis for the Communication Protocol in Smart Grids. 2020 the 8th International Conference on Smart Energy Grid Engineering, 58 – 63. https://doi.org/10.1109/SEGE49949.2020.9182015

Risbud, P., Gatsis, N., & Taha, A. (2020). Multi-period power system state estimation with PMUs under GPS spoofing attacks. Journal of Modern Power Systems and Clean Energy 8, 597–606.https://doi.org/10.35833/MPCE.2020.000125

Sanjalawe, Y., Al-Emari, S., Fraihat, S., Makhadmeh, S.N., & Alzubi, E. (2025). AI-Powered Smart Grids in the 6G Era: A Comprehensive Survey on Security and Intelligent Energy Systems. IEEE Open Journal of the Communications Society, 7677 – 7719.https://doi.org/10.1109/OJCOMS.2025.3609144

Tian, T., Liu, C., Guo, Q., Yuan, Y., Li, W., & Yan, Q (2018) An improved ant lion optimization algorithm and its application in hydraulic turbine governing system parameter identification. Energies 2018, 11, 95. https://doi.org/10.3390/en11010095

Valdez, F., Castillo, O., & Melin, P. (2021). Bio-Inspired Algorithms and Its Applications for Optimization in Fuzzy Clustering. MDPI Journal of Algorithm, 14, 1 – 21. https://doi.org/10.3390/a14040122

Wang, S., Bi, S., & Zhang, Y.J. (2020a). Locational Detection of the False Data Injection Attack in a Smart Grid: A Multilabel Classification Approach. IEEE Internet Things, 7, 8218–8227.https://doi.org/10.1109/JIOT.2020.2983911

Wang, L., Qu, Z., Li, Y., Hu, K., Sun, J., Xue, K., & Cui, M. (2020b). Method for extracting patterns of coordinated network attacks on electric power CPS based on temporal–topological correlation. IEEE Access 2020, 8, 57260–57272. https://doi.org/10.1109/ACCESS.2020.2982057

Wang, K., Du, M., Maharjan, S., & Sun, Y. (2017). Strategic honeypot game model for distributed denial of service attacks in the smart grid. IEEE Transactions on Smart Grid , 8, 2474–2482. https://doi.org/10.1109/TSG.2017.2670144

Wu, G., Wang, G., Sun, J., & Chen, J. (2020). Optimal partial feedback attacks in cyber-physical power systems. IEEE Transactions on Automatic Control, 65 (9), 3919–3926.https://doi.org/10.1109/TAC.2020.2981915

Yang, L., Zhang, X., Li, Z., Li, Z., & He, Y. (2020). Detecting bi-level false data injection attack based on time series analysis method in smart grid. Computers & Security, 96, 101899. https://doi.org/10.1016/j.cose.2020.101899

Zhao, J., Zhang, G., La Scala, M., Dong, Z.Y., Chen, C., & Wang, J. (2017). Short-Term State Forecasting-Aided Method for Detection of Smart Grid General False Data Injection Attacks. IEEE Transactions on Smart Grid , 8, 1580–1590.https://doi.org/10.1109/TSG.2015.2492827

© 2026 The Author(s). Published by Faculty of Engineering, Federal University Oye-Ekiti.
This is an open access article under the CC BY NC license. (https://creativecommons.org/licenses/by-nc/4.0/)