*Section: Research Paper*

# Cognitive Computing on Cyber Attacks in Smart Grid System for Minimizing Energy Loss

**M. Mythreyee [1]*, Nalini, A[2]**

[1]Research Scholar, [2]Professor, Department of Electrical and Electronics Engineering, Dr. M.G.R. Educational and Research Institute, Maduravoyal, Chennai-600 095, Tamilnadu, India.

Corresponding Author: M. Mythreyee. Email: mythreyee.researchineee@gmail.com

**Abstract**

The use of Smart Grid (SG) technologies has modernized and improved the current electrical infrastructure. Modern computer, control, and advanced networking technologies form the backbone for SGs. The Information and communication technologies (ICTs) have been incorporated into the SG, which utilizes the conventional electrical power system. By empowering both the suppliers and users of electrical utilities, whereas an integration enhances the effectiveness and the power system availability as well as continuously monitors, governs, and manages client needs. Cyber-physical SG systems need to be secure from evolving security risks and intrusions. In SGs, flooding attacks and Distributed Denial-of-Service (DDoS) attack have received the greatest attention. These hacks have the potential to compromise SGs' efficient operation and cause significant financial losses, damage to equipment, and malicious regulation. Several researchers have reveal that Machine Learning (ML) techniques outperform traditional attack detection algorithms in detecting attacks. The ML approaches were used to examine malicious activity and intrusion detection challenges at the network layer of SG communication system. This paper focuses on ML algorithm that have been utilized for classifying the measurements as either being attacked (Unstable) or secured (Stable) and it can be obtained through bat sequence algorithm. The dataset used in this research is Electrical Grid Stability Simulated Dataset has been used to classify the stability assess in SGs and try to minimize the power loss by avoiding the unstable (attacked) distribution. The accuracy of proposed bat sequence algorithm using Artificial Neural Network (ANN) is 99.43% which is higher while compared to other classification method.

## 1. Introduction

Grid operators have encountered recent issues as a result of the change in paradigm occurring in the energy sector as a result of the increase in usage of Distributed Energy Resources (DERs), specifically at the grid level distribution [1]. To address these issues, the distribution of grid operators will need to take on greater responsibility through the development of sensors and actuators that enable telecontrol hyperlinks in the resources namely controllable DERs using ICTs. The SG has been developed by integrating contemporary technologies with conventional

electrical infrastructure. There are numerous approaches for controlling operations and power in the SG. A production meter, renewable energy generators, smart inverters, resources deployed at the grid's position for smart meters as well as energy efficiency and appliances provided at the client's site are the certain instance in operational and energy measures [2]. The generation of renewable energy has minimized energy costs due to its easy availability in producing energy from renewable resources. Nevertheless, it's not available always but based on variables such as humidity, location, temperature, humidity, direction and speed of the wind. Solar energy has influenced by the sun's temperature, brightness and cloud cover. The energy consumed from the wind dependency is essential to its speed and direction. By efficient renewable energy as well as potential dependably due to certain methodology suitable in forecasting solar, battery charge state and wind. The data of SG can be communicated into and fro data through sensors due to its capability of data reception and transmission [3]. The communication system which links to the electricity system has become crucial to the SGs functioning of an entire infrastructure. A cyber-system depends on the data flow whereas a power system completely relies on the flow of electricity. The communication channel makes use of a variety of tools and technology. Cyberattacks on communication systems have become very likely in accessing physical systems as well as altering or preventing data flow in which the attackers plan to assault the communication channels [4].

Figure 1 provides an overview of the SG system that outlines its various elements [5]. The SG system is primarily composed of power plants, transmission and distribution networks, ICT, distributed generation, prosumers, and energy storage. Hydroelectric facilities, diesel power plants, microturbines, nuclear power plants, wind turbines, and solar plants are all potential sources of power for large-scale generation [6].

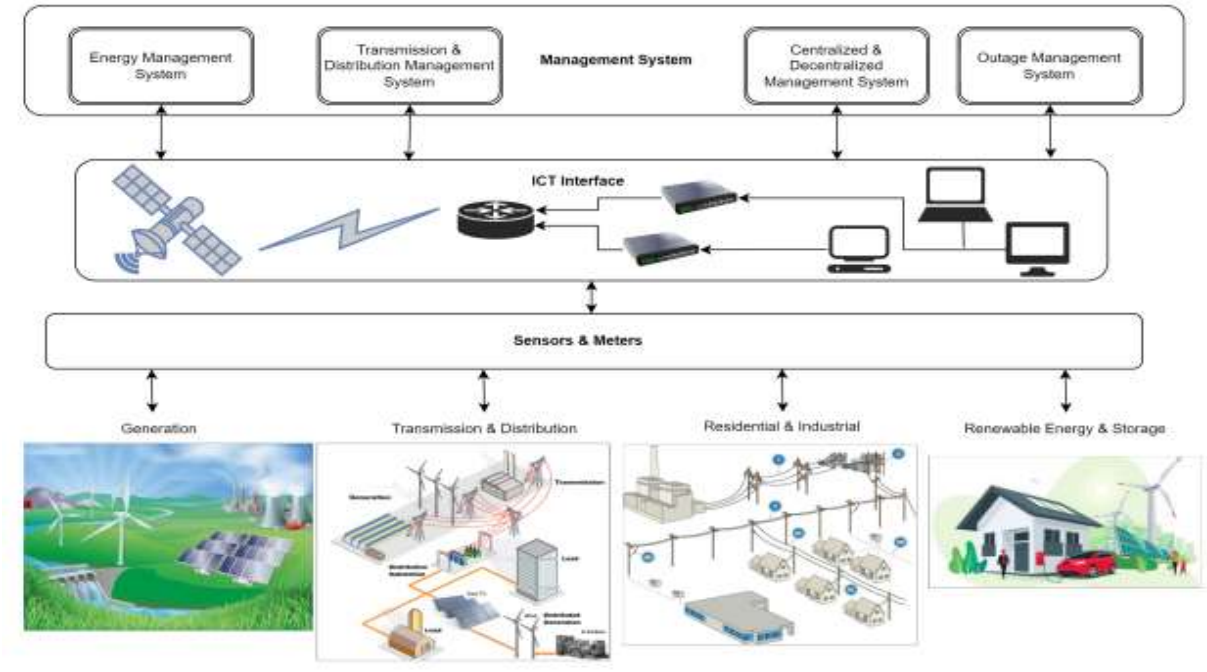


Figure 1 Standard Smart Grid infrastructure

Power is produced for transferring it in home and industrial applications usage by three major sources. Interconnected lines in a transmission network make it easier to transmit power to the distribution end. Transmission lines are used to transfer high voltage AC current, whilst the regional transmission of electrical power uses lower voltage. Bulk electrical power is stimulated from the production plant to the distribution substation during the primary stage. Electricity is transmitted from distribution substations to various cities as well as rural areas during the secondary stage. However, the energy storage from Grid is utilized in storing energy on a big scale for storage of additional electricity. Hence, the sensors as well as Intelligent Electronic Devices (IEDs) in a SG system may be recorded, controlled, and maintained [7]. The level of transmission and distribution involves intelligent substations, power lines as well as monitoring and controlling automation systems whereas the transformers have been equipped with sensors. Moreover, all the components and devices have been maintained by four major management systems namely

1. Outage
2. Centralized and decentralized
3. Transmission and distribution
4. Energy

The management system and legislative have been interfaced with the power network using ICT layer. Cyberattacks on SG security involve perceptive customer data breaches through adversaries, malfunctions propagation over cyber system as well as vulnerabilities over devices of distributed controls [8]. Due to the rising penetration of ICTs, secure and reliable grid operations progressively rely on functional communication technologies and procedures which renders it more susceptible to malfunctions and cyberattacks [9].

The enduring performance and resource limitations of legacy devices need preventative measures with a substantial performance overhead, which are expensive to install through upgrades or other alternatives [10]. Network based Intrusion Detection System (IDS), that continuously monitor traffic of the communication and execute detection of attacks in the process network at specified places [11], are more proactive than reactive security measures. The two main categories of IDS are blacklisting, which compares observed data to established attack signatures, as well as whitelisting, which compares observed data to known knowledge of the system's properties during normal circumstances [12]. The support vector machines (SVM) and anomaly detection technique is used to investigate various ML-based techniques in finding FDI attacks that may be supervised and unsupervised. Based on statistical discrepancies in data, it has been established that both ML techniques are effective at identifying FDI attacks [13]. For the purpose of detecting FDI attacks, various ML algorithms have been tested and compared. This research involves linear and Gaussian SVM, K-Nearest Neighbor (KNN), and a Single-Layer Perceptron (SLP) are utilized as supervised learning techniques. According to the study's findings, KNN is highly sensible in system size as well as might function more effectively in smaller systems. Additionally, it was found that SVM, particularly when combined with a

Gaussian kernel, perform better on large scale systems. The SLP is found with less system size sensitive but less precise than SVM. Due to its added complexities, a multi-layered perceptron, referred to as an ANN is thought to be more precise [14].

## 2. Literature Review

A lot of research work and studies have looked into whether they are appropriate of Cyber-Physical System (CPS)-based detection mechanisms in SGs as IDS using ML technique. This research discusses the FDI attack detection with in the SGs system using ML methods.

The FDIA has been involved and its physical and financial effects on SGs are examined along with possible detection methods [15]. The effects of cyber-attacks on SGs are examined in the following piece, which also discusses future research advancements in China. The researchers evaluated the integrity and Denial-of-Service (DoS) security concerns in the SGs system [16]. For just FDIA in SG systems, only ML-based detection approaches are explored [17]. The researcher has addressed the effects of cyber-attacks on the SG system management and stability [18]. However, these review has not investigate other attacks like DDoS as well as GPS spoofing assaults alongside with DoS and FDIA which cause all the layer to be vulnerable. Hence, injection attacks have been occur whenever an attacker attempts to delete, modify, or introduce novel information to a network. This could disrupt the SGs operation and cause a blackout. Additionally, this cyber-attack affects data, jeopardizes data security, and infiltrates the network with malicious nodes. Injection attacks differ from previous assaults in that they may focus on the transport layer as well as the data-link layer or network layer [19]. A different technique that might be utilized on SG networks is a flooding attack. At the networking or application layer, this kind of assault may restrict system access [20]. Processing the bogus messages that are delivered to the target can use up all of its available assets. Individual nodes are unable to connect to the network as a result of this attack. Another sort of cyber-attack on the SG is man-in-the-middle attacks. These assaults purpose is to compromise the session and network layers [21].

Based on numerous perspectives, the researchers have assessed IDS in the cyber-physical of the SG. Li et al., have recommended a variety of monitoring techniques for tracking unusual load deviations and suspect branch flow fluctuations. False data injection (FDI) assaults are recommended to be recognized using two-stage techniques. This study investigate how FDI assaults affect system reliability by introducing the FDI cyber-attack [22]. The basis for proposed FDI detection method is an alert system with defined distinctive metrics. To overcome the shortcomings of the conventional firewall system in safeguarding the SCADA networks, the SCADAWall has customized firewall model [23]. The existing SCADA systems functioned in accordance with deep packet inspection, which was created in investigating the communication's message components. The SCADAWall was enhanced with the addition of a custom industrial protocols extensions algorithm as well as an out-of-sequence detection technique to better detection of abnormal modifications to industrial activities. By ensuring the SCADA system's latency characteristics, the experimental study shows that the frame work of SCADAWall has performs well at detection process [23]. Singh, Ebrahem and Govindarasu have discussed test

bed model for SCADA systems in validating the proposed algorithm efficiency in a current time setting. The computer simulation has an energy management system that is controlled by a SCADA system. A variety of real-world scenarios, including attack creation and defense methods, are provided by the test bed. In order to track malicious packet movement in the SCADA network, an anomaly-based approach was developed. The study conducted shows a superior rate of detection as well as latency [24].

Feedforward Neural Networks (FNN) using back-propagation training technique have been especially utilized in this research. The evaluation results using real data showed that NN-based IDS produces favorable results. Peng, Li, and Wang have used deep learning-based techniques in network IDS whereas Deep NN is used in the model for extracting characteristics from network monitoring data, as well as back propagation NN is used to classify intrusion patterns at the top level [25]. This results have determined that the suggested approach significantly outperforms the precision of traditional ML techniques. Hai-He has developed an IDS based on an enhanced NN, with feature extraction done through the adaptive weighted influence method. The back propagation NN has been used for classifying as well as detecting the model with high accuracy [26]. The researcher has illustrated a software counter in each mobile user, either inside their mobile devices or in signaling systems, as a storm detection and mitigation strategy [27]. According to a review of various current proposed systems, it is essential for addressing the limitations contained in the current models for the purpose of enhancing the effectiveness of the countermeasures for DDoS attacks. This is especially HTTP flood attacks as well as specifically most of them are primarily discussion-based.

## 3. Research Methodology

The proposed method for SGs assessed with the similarities in HTTP transactions due to ICT with normal (Stable) and flood data (Unstable) have been selected in training. The ANN sequential model has extract the features from requested stream that experiential at an absolute reacting time instead of user sessions as well as packet patterns. There are certain unique feature sets are considered to be robust and scaled mutative search technique named Bat sequence algorithm. It is utilized in performing search in assessing the rapport at test phase. However, the cosine metric has utilized in identifying the signatures of available transactions that assigned during training phase. Hence, the equivalent of cosine assist in identifying the attribute set which inflicts a prominence relation. The arrival rate with respect to the users have involved for a proxy server serves to establish the cases of non-pattern. Thus it became a challenge for it constraint and can manuscript created a novel metric sets that have derived from an absolute reaction time instead of the packet delivery patterns. The advantage in using bat algorithm is to determine the bats behavior with echo based location in resolving both single objective as well as multi-objective optimization issues shown in figure 2. The proposed bat sequence with ANN algorithm is utilized in classification to detect the attack traffic as unstable and normal traffic as stable.

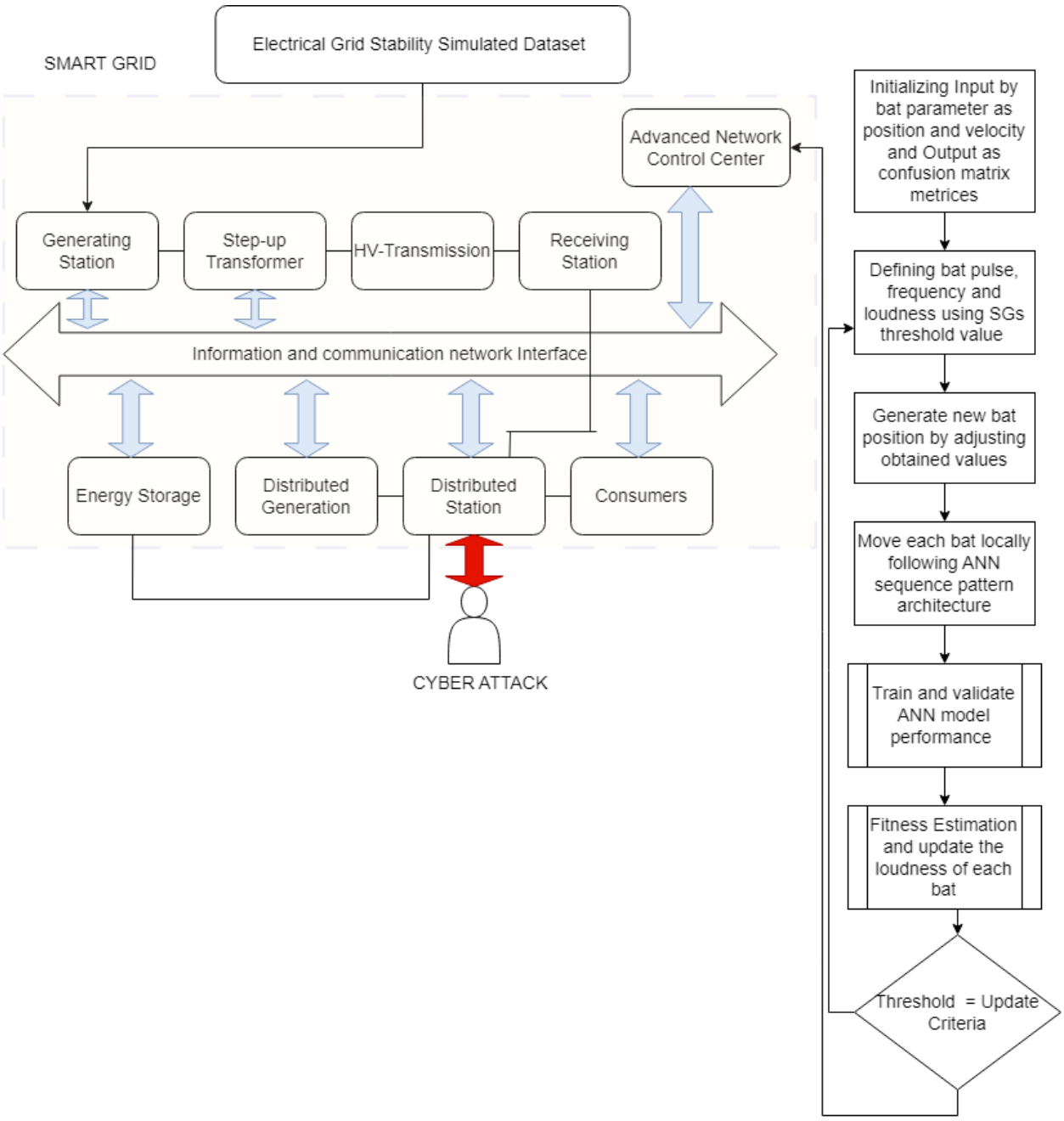


Figure 2 Cyber-Security of Smart Grid using Bat sequence with ANN technique

**Dataset collection**

The development of renewable energy sources offers the world's population a much-needed substitute for conventional, exhaustible, and environment-unfriendly fossil fuels. In a SG, collected data from the consumer demand is made to centralized demand. The supply analysis are performed, and the resultant proposed price data has forwarded to customers which may assist in deciding the usage limits. This dynamic calculation on the stability of grid establishes both trouble as well as crucial requirement because the entire process is depend on time. Grid

stability has been observed using the DSGC differential equation-based computational framework for an analogous architecture of a 4-node star that has one power source named centralized generation node that distributes energy to other three consumer nodes. However, the original dataset consists of 10,000 observations and the permutation of three customers have been occupied by three consuming nodes illustrates that dataset is increases with 6 times because of symmetric reference grid. Hence, there are 60,000 records in the upgraded edition which has two variables that are dependent and 12 significant predictive features. Thus, the dataset consist of 14 attributes and 60000 records of reaction time and total power balance with its energy price elasticity as a major attribute shown in figure 3.

| | tau1 | tau2 | tau3 | tau4 | p1 | p2 | p3 | p4 | g1 | g2 | g3 | g4 | stab | stabf |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 2.959060 | 3.079885 | 8.381025 | 9.780754 | 3.763085 | -0.782604 | -1.257395 | -1.723086 | 0.650456 | 0.859578 | 0.887445 | 0.958034 | 0.055347 | unstable |
| 1 | 9.304097 | 4.902524 | 3.047541 | 1.369357 | 5.067812 | -1.940058 | -1.872742 | -1.255012 | 0.413441 | 0.862414 | 0.562139 | 0.781760 | -0.005957 | stable |
| 2 | 8.971707 | 8.848428 | 3.046479 | 1.214518 | 3.405158 | -1.207456 | -1.277210 | -0.920492 | 0.163041 | 0.766689 | 0.839444 | 0.109853 | 0.003471 | unstable |
| 3 | 0.716415 | 7.669600 | 4.486641 | 2.340563 | 3.963791 | -1.027473 | -1.938944 | -0.997374 | 0.446209 | 0.976744 | 0.929381 | 0.362718 | 0.028871 | unstable |
| 4 | 3.134112 | 7.608772 | 4.943759 | 9.857573 | 3.525811 | -1.125531 | -1.845975 | -0.554305 | 0.797110 | 0.455450 | 0.656947 | 0.820923 | 0.049860 | unstable |
| ... | ... | ... | ... | ... | ... | ... | ... | ... | ... | ... | ... | ... | ... | ... |
| 59995 | 2.930406 | 2.376523 | 9.487627 | 6.187797 | 3.343416 | -1.449106 | -0.658054 | -1.236256 | 0.601709 | 0.813512 | 0.779642 | 0.608385 | 0.023892 | unstable |
| 59996 | 3.392299 | 2.954947 | 1.274827 | 6.894759 | 4.349512 | -0.952437 | -1.663661 | -1.733414 | 0.502079 | 0.285880 | 0.567242 | 0.366120 | -0.025803 | stable |
| 59997 | 2.364034 | 8.776391 | 2.842030 | 1.008906 | 4.299976 | -0.943884 | -1.380719 | -1.975373 | 0.487838 | 0.149286 | 0.986505 | 0.145984 | -0.031810 | stable |
| 59998 | 9.631511 | 2.757071 | 3.994398 | 7.821347 | 2.514755 | -0.649915 | -0.966330 | -0.898510 | 0.365246 | 0.889118 | 0.587558 | 0.818391 | 0.037789 | unstable |
| 59999 | 6.530527 | 4.349695 | 6.781790 | 8.673138 | 3.492807 | -1.532193 | -1.390285 | -0.570329 | 0.073056 | 0.378761 | 0.505441 | 0.942631 | 0.045263 | unstable |

60000 rows × 14 columns

Figure 3 Dataset for Electrical Grid Stability Simulated

Bat has the capability to locate their prey even in total darkness and also able to distinguish what kind of prey it is. However, the principle of bat algorithm is an evolutionary with population based algorithm in which each bat has represented with a solution. Hence, it can be designed based on the virtual bat ecological behavior which assist in detecting the prey position. Thus, the modulated frequency signal s have been utilized for echolocation. Mostly, the bat admitted with pulse emitted sound produced from them while it rebounds from the surrounding objects or prey. As a result, the bat reaches closer to prey, the echo loudness has been reduced as well as increases the sound pulse rate.

The three major rules considered in bat algorithm are

1) All bats utilize echolocation to determine distance, and in a strange manner, bats are able to identify the difference among prey as well as background obstructions.

2) To identify the prey, bats glide randomly with velocity ($V_i$) at a location of ($P_i$) with a continuous frequency ($f_{min}$), using regulating wavelength, and a loudness ($A_0$). Based on their target closeness, it might habitually change the pulse frequency which it releases as well as the rate at which they generate it.

3) The loudness is presumed to range from a big (positive) $A_0$ to a minimum constant value $A_{min}$, despite the fact that it can change in a wide variety of manner.

A bat population is created initially and once the startup has alter the fitness-related parameters, and then each bat in the population is assessed for fitness.

**Working of ANN model building**

The ANN model has acquire from sequence data patterns and tried to accomplish as probable as an accurate prediction. Assume, the set of X data pairs containing the variables and the results, $(m^1, t^1)$, $(m^2, t^2)$, ….$(m^X, t^X)$ in which the $m^i$ is the input value and $t^i$ is the target value for i= 1, 2, 3, …, X. We would like to build a neural net F so that ideally as

$$F(m^i) = t^i \quad (3.1)$$

Moreover, it allow for error $\in^i$ typically. Let n denotes the output of ANN is expressed in equation 3.2 and 3.3.

$$n^i = F(m^i) \quad (3.2)$$

And

$$t^i = n^i + \in^i \quad (3.3)$$

However, the $n^i$ is based on the parameter with respect to weight and bias which turn as an optimizer issue. In this, setting the ANN in F that minimize the error function represent in equation 3.4.

$$E = \frac{1}{N}\sum_{i=1}^{X}\left\|t^i - n^i\right\|^2 \quad (3.4)$$

Where,

N = Number of training patterns.

When the ANN has become a two-way classification then N = 2. Based on the equation, E is a parameter function of F, and required in determining the weight values that minimize the error through differentiating E.

When the research is focused on one term of the sum and it is expressed in equation 3.5.

$$\|t - n\|^2 = (t_1 - n_1)^2 + (t_2 - n_2)^2 + \cdots + (t_x - n_x)^2 \quad (3.5)$$

Thus, the values of input and output have been fixed, and only the parameter is consider to be calculated through weight and it can differentiate from both sides is expressed in equation 3.6.

$$\frac{\partial}{\partial W_{ij}}(\|t - n\|^2) = -2(t - n).\frac{\partial n}{\partial W} \quad (3.6)$$

There are highly specific and also verify the fits over the context of neural net. From a neural net, the output is defined as $n^i = W_{ij}m^i + b$.

Hence, the output is rely on weight and while differentiating both sides in accordance with $W_{ij}$ by chain rule as per equation 3.7

$$\frac{\partial}{\partial \mathrm{W_{ij}}}(\|\mathrm{t} - \mathrm{n}\|^2) = -2(\mathrm{t_i} - \mathrm{n_i})\mathrm{m_i} \quad (3.7)$$

Where,

$m_j$is the $i^{th}$ coordinate position. The derivative has provided direction to the maximum for accomplishing the minimum point, and subsequently in opposite direction of this gradient. In addition, this derivative as close to 0 as possible for obtaining the minimum of error.

Relu is a function and major benefit of Relu activation function and doesn't activate all neuron simultaneously in which a neuron with negative value have converted into zero or it gets deactivated. Networks become sparse as well as computationally effective as a result. The gradient value of the graphs at the negative side is zero. It suggests that neurons terminate are never stimulated during back propagation. The sigmoid function is utilized to maintain issues with multi-class which maps the value of output from 0 to 1. It works best when utilised in the classifier's output layer. There isn't a guideline that may be used to select the activation function. The characteristics of the issue might assist in choosing a quicker converging network. Certain characteristics are based on the research as the Relu and sigmoid for activation functions.

A procedure called optimization aims to decrease network error. This is essential for increasing the model's accuracy. The optimizer has three different iterations: Adam, SGD, and RMSProp. SGD is iterative gradient descent technique that uses iteration to search for an optimal error. These models produce predictions in every iteration that follows and predicted results are compared to the predictions. Error is defined as the difference between the projected value and the actual result. The internal parameters of the model as well as the weights of the network are updated using this error. The back propagation algorithm follows this updating process. SGD also finds it challenging to get away from the saddle points. The most popular choices for handling saddle points are AdaGrad, RMSprop, ADAM, and AdaDelta. To modify the gradient with the slop and quicken the SGD, Nesterov accelerating gradient is utilized. Due to its ability to execute more updates for infrequently parameters as well as fewer changes for frequent parameters, AdaGrad outperforms Nesterov accelerated gradient. As a result, SGD becomes faster, more scalable, and more resilient. In order to train ANN, it is utilized and the fundamental disadvantage in AdaGrad optimizer has minimized the model's ability for training through the sequential pattern better. Two optimizers like RMSProp as well as AdaDelta, have been created individually to address the problem with AdaGrad. Moreover, the optimizer like AdaDelta and RMSProp are identical whereas the main difference is AdaDelta which is not fixed as an early learning rate with constant. Adam is an optimizer which incorporate the beneficial features of RMSprop as well as Adadelta. Adam is deemed a good choice since it get improves RMSProp as well as Adadelta. As a result, the optimizers used in this experiment is Adam.

The sequential pattern ANN has effectively extract the multifaceted characteristics between the applicable variables of classifying the intruder in the AODV routing. The selection of optimizer is significant for improving the optimum selection of route path in AODV of the MANET. This can be determined through better prediction with model accuracy. Thus, the model efficiency improved by optimizing the best obtained sequence in increasing the predicting IDS accuracy by enhancing the ANN model accuracy.

**Bat sequence with ANN algorithm**

Step 1: Let i = 1, 2, …, X and j = 1, 2, …, m in which i represent iteration amount based on weight wt, distance iteration using j.

Step 2: Read and calculate every bat frequency using Pulse Rate Controller (PRC) and distance as

$f_j = PRC_1 * Average(D_j)$

Step 3: Calculating object distance from bat as $O_j = f_j * D_j * wt$ and each object class can be expressed as $C_j = O_j - 1$ and update wt = wt-2*μ*$C_j$

Step 4: Calculating the new location as $L_j$ and modify PRC of bat if $E_j < E_j - 1$ , then compute $L_j = L_j + E_j$ and $PRC_1 = f_j + PRC_2 * L_j * E_j$

Step 5: Neural network (F) sequence is build based on target value as bat iteration for training model.

Step 6: If threshold = update wt criteria, calculate wt = wt - delwt and error ($Err_i$) = Mean (Err) else go to spet 3 and repeat the process.

Step 7: Print Confusion matrix and compute security classification model accuracy as Return

Each instance from Bat algorithm is considered as an instance get prepared as dataset that includes both normal as well as attack data. Moreover, each record is treated as one bat in a typical dataset, and its distance from the other bats is calculated by comparing it to them. All of the surviving bats must be treated in this manner. Records that have been updated are handed over to the following generation. The most iterations possible must be run in order to acquire accurate classification. The normal classifier is retrieved and designated as a normal signature after all iterations have been accomplished. For obtaining the attack signature, the same procedure is used in attack training records.

## 4. Result and discussion

The stability of the grid can be predicted through mathematical model but this experiment has initiated a tool in predicting the grid stability that meet the binary classification namely stable for normal records and unstable for attack based records. However, the stability of the SG with proposed bat sequence ANN model relies on IDS from cyber-attacks that can be significantly simplified by bat sequence algorithm with adam optimizer using python tool library like sklearn, tensor flow and pandas. Hence, the goal of this research is to minimize the energy transmission and avoid unwanted energy to consumers which are stored in the energy storage. Thus, it can be executed by avoiding intruders who can alter the distribution and consumption of power which get received from main station. This can assist in avoiding fluctuation of energy consumption and fluctuation by system participants in a dynamic manner. The participant respond in altering the associated economic power balance along with better reaction time of each network that get participated. The attribute 'tau1' to 'tau4' represent the reaction time of each participant of network and its real value in the range of 0.5 to 10. The general produced power through attack (Unstable) distributed lines as positive value whereas the negative value represent the normal (Stable) distributed line.

There are no missing values because the dataset's content was obtained using simulated operations. Additionally, since all features are initially numeric, feature coding is not necessary. Without the requirement for feature engineering or data preparation, these dataset qualities enable a direct transition to ML modeling. Figure 4 illustrates the power distributed station status for distributing the power with stable (Normal) distribution or power with unstable (Attack) distribution.

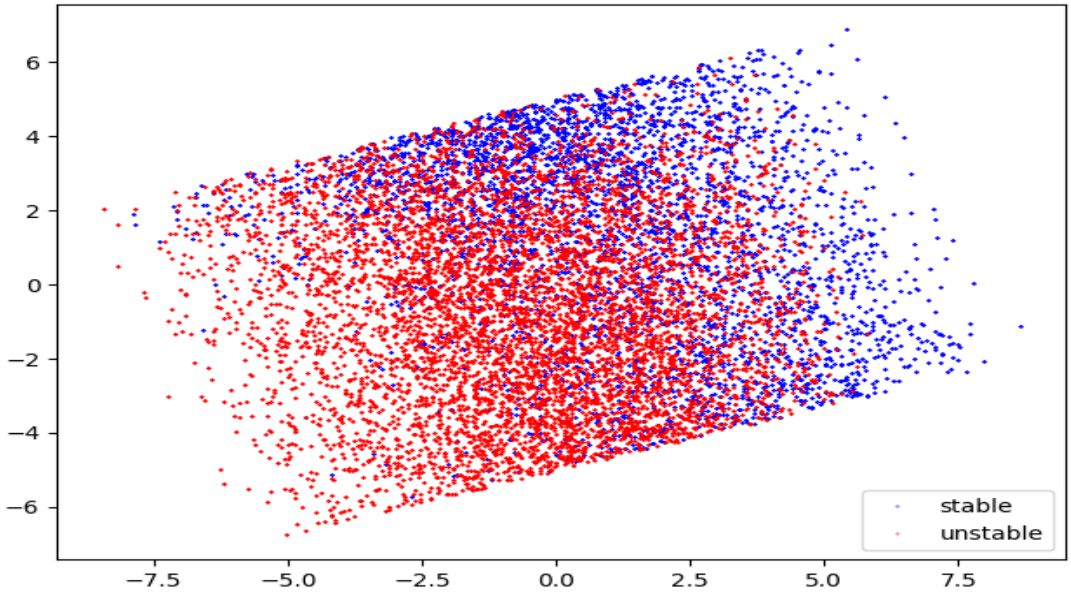


Figure 4 Stability status of SG from distributed station

```
Model: "nn_clf"
_________________________________________________________________
Layer (type)                 Output Shape              Param #
=================================================================
batch_normalization (BatchNo (None, 13)                52
_________________________________________________________________
dense (Dense)                (None, 64)                896
_________________________________________________________________
dense_1 (Dense)              (None, 256)               16640
_________________________________________________________________
dense_2 (Dense)              (None, 1)                 257
=================================================================
Total params: 17,845
Trainable params: 17,819
Non-trainable params: 26
_________________________________________________________________
```

Figure 5 Bat sequence ANN model dense layer

```
Epoch 1/40
1500/1500 [==============================] - 3s 2ms/step - loss: 0.1205 - accuracy: 0.9489 - val_loss: 0.0537 - val_accuracy:
0.9812
Epoch 2/40
1500/1500 [==============================] - 2s 2ms/step - loss: 0.0939 - accuracy: 0.9589 - val_loss: 0.0458 - val_accuracy:
0.9837
Epoch 3/40
1500/1500 [==============================] - 2s 2ms/step - loss: 0.0931 - accuracy: 0.9599 - val_loss: 0.0458 - val_accuracy:
0.9922
Epoch 4/40
1500/1500 [==============================] - 2s 2ms/step - loss: 0.0922 - accuracy: 0.9604 - val_loss: 0.0405 - val_accuracy:
0.9927
Epoch 5/40
1500/1500 [==============================] - 2s 1ms/step - loss: 0.0919 - accuracy: 0.9613 - val_loss: 0.0358 - val_accuracy:
0.9943
Epoch 6/40
1500/1500 [==============================] - 2s 1ms/step - loss: 0.0919 - accuracy: 0.9605 - val_loss: 0.0375 - val_accuracy:
0.9927
Epoch 7/40
1500/1500 [==============================] - 2s 1ms/step - loss: 0.0910 - accuracy: 0.9609 - val_loss: 0.0431 - val_accuracy:
0.9935
Epoch 8/40
1500/1500 [==============================] - 2s 2ms/step - loss: 0.0876 - accuracy: 0.9632 - val_loss: 0.0380 - val_accuracy:
0.9925
Epoch 9/40
1500/1500 [==============================] - 2s 1ms/step - loss: 0.0921 - accuracy: 0.9600 - val_loss: 0.0419 - val_accuracy:
0.9945
Epoch 10/40
1500/1500 [==============================] - 2s 1ms/step - loss: 0.0846 - accuracy: 0.9632 - val_loss: 0.0384 - val_accuracy:
0.9955
Epoch 11/40
1500/1500 [==============================] - 2s 1ms/step - loss: 0.0880 - accuracy: 0.9630 - val_loss: 0.0361 - val_accuracy:
0.9940
Epoch 12/40
1500/1500 [==============================] - 2s 1ms/step - loss: 0.0899 - accuracy: 0.9627 - val_loss: 0.0362 - val_accuracy:
0.9938
Epoch 13/40
1500/1500 [==============================] - 2s 1ms/step - loss: 0.0886 - accuracy: 0.9628 - val_loss: 0.0423 - val_accuracy:
0.9918
Epoch 14/40
1500/1500 [==============================] - 2s 1ms/step - loss: 0.0883 - accuracy: 0.9613 - val_loss: 0.0406 - val_accuracy:
0.9943
Epoch 15/40
1500/1500 [==============================] - 2s 2ms/step - loss: 0.0916 - accuracy: 0.9611 - val_loss: 0.0422 - val_accuracy:
0.9925
```

Figure 6 Epochs for Bat sequence ANN model for accuracy and validation accuracy

Figure 5 illustrates the sequence associated with bat in ANN model and the bat new location will varies based on the sequence in ANN model and setting the dense layer with respect to increase the accuracy of the model. Figure 6 illustrates the number of epochs for training the bat sequence with ANN model. This assist in analyzing the accuracy and validation accuracy of the bat sequence ANN model. The epochs have been executed till 15 passes in which the training dataset takes around an algorithm for producing the high accuracy of model as 96.11% and in validation accuracy is 99.25%.

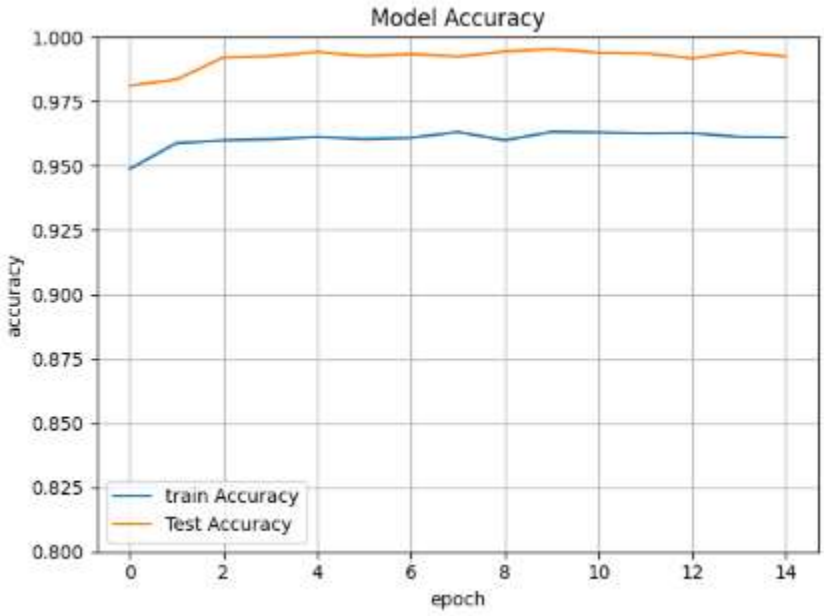


Figure 7 comparison of accuracy for train and validation of Bat sequence ANN model

The proposed bat sequence with ANN model has shown better accuracy with 95% in train model as the epoch's iteration increases the train model accuracy increases up to 96.11% is shown in figure 7. Similarly, the test model accuracy with initial epoch as 98% which get increase based on trained model weights and bias. The test model accuracy increases as the epochs of proposed model increases up to 99.25%. This proposed model need to be validated for better prediction in classifying the SG architecture power distribution stability by detecting the cyber-attacks and which can be compared with actual label count. The evaluation can be carried through confusion matrix class values namely True Positive (TP), False Positive (FP), True Negative (TN) and False Negative (FN).

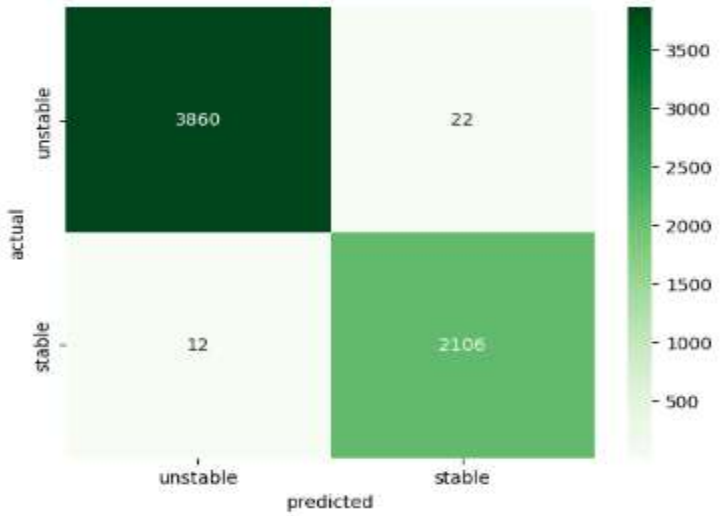


Figure 8 Confusion matrix of Bat sequence ANN model

The predicted SG power stability status with proposed model has been evaluated through confusion matrix metrics like accuracy, precision, recall and F1-score. According to the security model Detection Rate (DR) is said to be precision metric score and False Alarm Rate (FAR) is defined through recall metric score. The evaluated metric of proposed bat sequence with ANN model is compared with existing ML model shown in Table 1.

Table 1 Confusion matrix class value for various classification ML method

| **Classification ML method** | **Confusion Matrix Values** | | | |
|---|---|---|---|---|
| | **TP** | **TN** | **FP** | **FN** |
| Proposed Bat sequence ANN | 3860 | 2106 | 22 | 12 |
| Nearest centroid | 2665 | 1626 | 1136 | 573 |
| k-Neighbor Classifier (KNC) | 3350 | 1585 | 451 | 614 |
| Logistic Regression | 3692 | 2073 | 109 | 126 |

ACC is said to be distribution of overall stability of SG has correctly classified in term of TP and TN to the overall SG stability sample size test dataset and the formulae is in equation 4.1.

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

(4.1)

DR defines the exact stable in sample data classification is known as precision. The ratio of TP to all the stability of SG sample is provided as an intrusion and the formulae is in equation 4.2.

$$DR = \frac{TP}{TP+FP}$$

(4.2)

True Positive Rate (TPR) defines the exact stable in sample data classification (TP) by total instances that involves TP and FN of class named as recall and the formulae is in equation 4.3.

$$TPR = \frac{TP}{TP+FN}$$

(4.3)

FAR is defined as the total instance of an attack data measured as FP to the total attack dataset instances which is sensitivity and is expressed in equation 4.4.

$$FPR = \frac{FP}{TN+FP}$$

(4.4)

F1-Score illustrates the DR and TPR has been comprised in detecting the evaluation measure. The F1-Score values are expressed in equation 4.5.

$$F1 - Score = 2 * \frac{DR*TPR}{DR+TPR}$$

(4.5)

Table 2 Confusion matrix metrics for various model

| ML Model Name | Accuracy (%) | Detection Rate (%) | False Alarm Rate (%) | True Positive Rate score | F1-Score |
|---|---|---|---|---|---|
| Bat sequence ANN | 99.43 | 99.43 | 99.69 | 0.9969 | 99.56 |
| Nearest centroid | 71.52 | 70.11 | 82.3 | 0.8230 | 75.72 |
| k-Neighbor classifier | 82.25 | 88.13 | 84.51 | 0.8451 | 86.28 |
| Logistic Regression | 96.08 | 97.13 | 96.7 | 0.9670 | 96.92 |

Table 2 illustrate the evaluation metrics of security based parameter associated with confusion matrix class value. The metrics considered are accuracy, DR, FAR, TPR and F1-Score in which it get compared proposed bat sequence ANN method with existing nearest centroid, LR and KNC.

Figure 9 illustrates the accuracy performance of various ML model in which the proposed bat sequence with ANN model has produce better secured SG stability model and through its accomplish result as 99.43% while comparing to other model like nearest centroid classifier, KNC, and LR model.

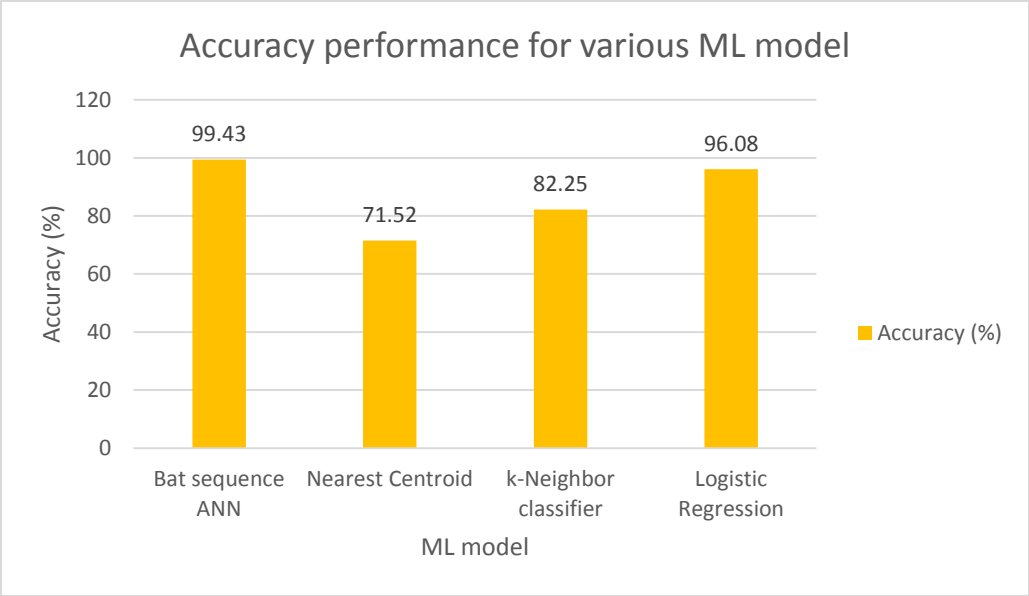


Figure 6 Accuracy for various ML model

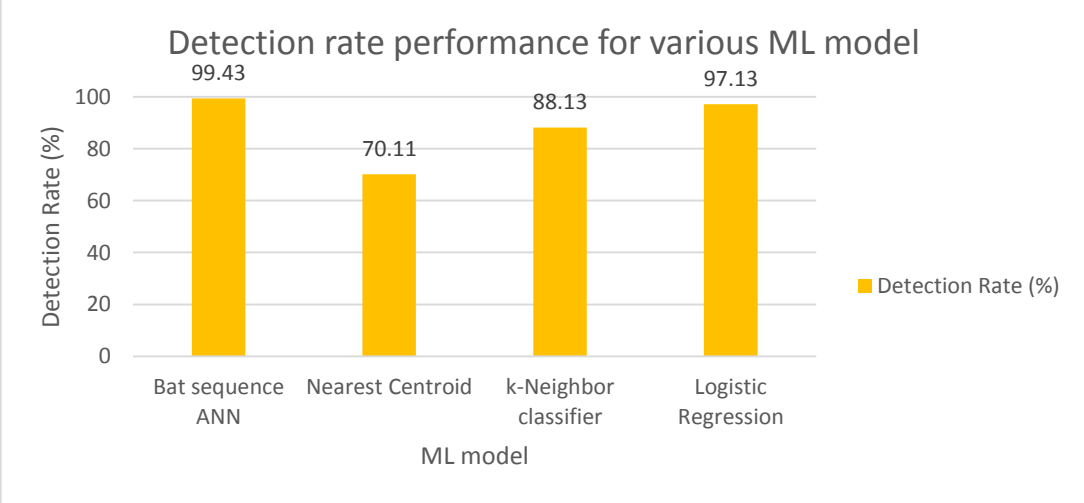


Figure 7 DR for various ML model

Figure 10 illustrates the performance of DR for various ML model in which the proposed bat sequence with ANN model has produce high detection of intruder get accomplished through its obtained result as 99.43% while comparing to other model such as nearest centroid classifier, KNC, and LR model.

Figure 11 illustrates the performance of FAR performance for various ML model in which the proposed bat sequence with ANN model has better false alarm with 99.69% which shows that bat sequence produce excellent alarm of cyber-attack. As a default, the good false alarm is 96% whereas the proposed bat sequence with ANN model has excellence than LR which comes under good flase alarm. The other two existing ML model is below the goof false alarm rate is KNC and nearest centroid classifier as 84.51% and 82.3% correspondingly.

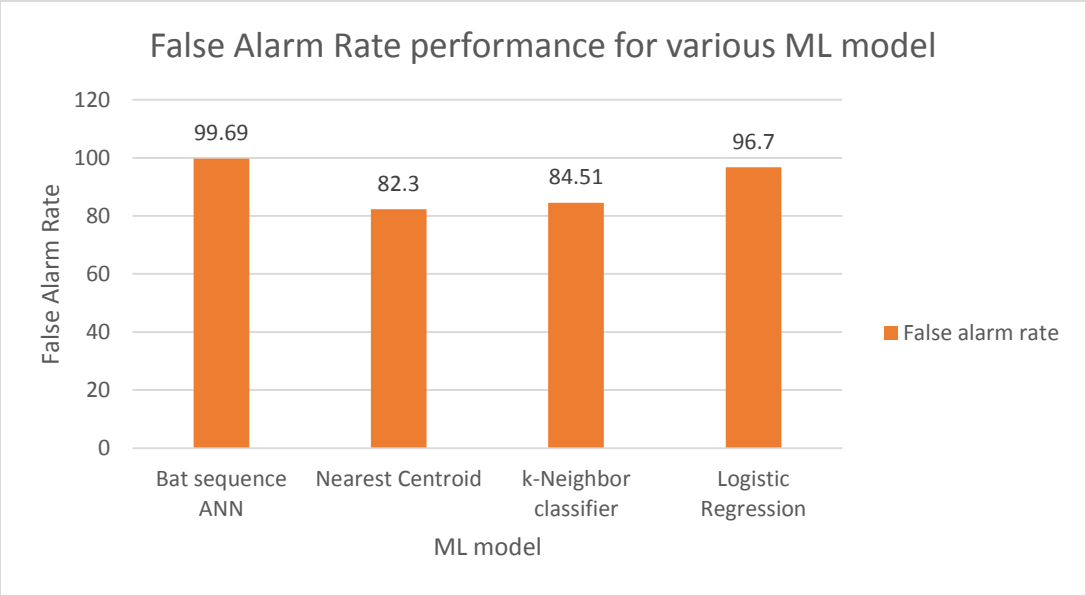


Figure 8 FAR for various ML model

Therefore, the cybersecurity of SG architecture with bat sequenced ANN model has improved in IDS against cyber-attack which assist in waste distribution of power through consumer and distributed generator that get stored in the energy storage. Hence, the received station power has distributed with exact consumer as well as distribution generator. Thus, the proposed SG architecture with ML model has minimize the power distribution by avoiding the unstable termination lines.

## 5. CONCLUSION

Based on the increase in usage of internet, there are several cyber-attacks have been identified in the user applications. The security performance of an ICT are considerably afflicted by these cyber-attacks. However, there are various IDS have been employed in preventing these cyber-attacks in which bat sequence pattern get introduced in ANN model which assist in modifying the layer of hidden to produce better accuracy through understanding the features weight and bias. Hence, bat sequence ANN model can successfully guarantee data security in SG architecture which received the power from station and distribution station has distributed the power with secured and stable distribution generators as well as consumers. The proposed model is evaluated through model accuracy, DR and FAR which is 99.43%. 99.43% and 99.69% respectively. This is comparatively higher than other existing ML model. Thus, the secured stability model can generate adequate power and distribute exact power which is required for consumer and distributed generator which cause in minimizing power usage from this SG architecture. This proposed bat sequenced ANN model minimize the power loss by avoiding unstable terminal lines. In future work, the power loss can be measured through sensor and monitored in the building management system of the SG management system.

**Reference**

1. Ourahou M, Ayrir W, Hassouni BE, Haddi A (2020) Review on smart grid control and reliability in presence of renewable energies: challenges and prospects. Math Comput Simul 167:19–31.
2. Ding, J.; Qammar, A.; Zhang, Z.; Karim, A.; Ning, H. Cyber Threats to Smart Grids: Review, Taxonomy, Potential Solutions, and Future Directions. Energies 2022, 15, 6799.
3. Mololoth, V.K.; Saguna, S.; Åhlund, C. Blockchain and Machine Learning for Future Smart Grids: A Review. Energies 2023, 16, 528.
4. Inayat, U.; Zia, M.F.; Mahmood, S.; Khalid, H.M.; Benbouzid, M. Learning-based methods for cyber attacks detection in IoT systems: A survey on methods, analysis, and future prospects. Electronics 2022, 11, 1502.
5. Moreno Escobar, J.J.; Morales Matamoros, O.; Tejeida Padilla, R.; Lina Reyes, I.; Quintana Espinosa, H. A comprehensive review on smart grids: Challenges and opportunities. Sensors 2021, 21, 6978.
6. Salkuti, S.R. Emerging and Advanced Green Energy Technologies for Sustainable and Resilient Future Grid. Energies 2022, 15, 6667.
7. Elbouchikhi, E.; Zia, M.F.; Benbouzid, M.; El Hani, S. Overview of signal processing and machine learning for smart grid condition monitoring. Electronics 2021, 10, 2725.
8. Otuoze, A.O.; Mustafa, M.W.; Larik, R.M. Smart grids security challenges: Classification by sources of threats. J. Electr. Syst. Inf. Technol. 2018, 5, 468–483.
9. Klaer B, Sen Ö, van der Velde D, Hacker I, Andres M, Henze M (2020) Graph-based model of smart grid architectures. in Proceedings of the 3rd International Conference on Smart Energy Systems and Technologies (SEST), 1-6. DOI:10.48550/arXiv.2009.00273
10. Tanveer A, Sinha R, Kuo MM (2020) Secure links: secure-by-design communications in IEC 61499 industrial control applications. IEEE Trans Ind Inform 17(6):3992–4002.
11. Konrad Wolsing, Eric Wagner, Antoine Saillard, and Martin Henze. 2022. IPAL: Breaking up Silos of Protocol-dependent and Domain-specific Industrial Intrusion Detection Systems. In 25th International Symposium on Research in Attacks, Intrusions and Defenses (RAID 2022), October 26–28, 2022, Limassol, Cyprus. ACM, New York, NY, USA, 16 pages. https://doi.org/10. 1145/3545948.3545968.
12. Krause T, Ernst R, Klaer B, Hacker I, Henze M (2021) Cybersecurity in power grids: challenges and opportunities. Sensors 21(18):6225.
13. S. Mohammadi, V. Desai, and H. Karimipour, "Multivariate mutual information-based feature selection for cyber intrusion detection," 10 2018, pp. 1–6.
14. M. Ozay, I. Esnaola, F. T. Yarman Vural, S. R. Kulkarni, and H. V. Poor, "Machine learning methods for attack detection in the smart grid," IEEE Transactions on Neural Networks and Learning Systems, vol. 27, no. 8, pp. 1773–1786, Aug 2016.
15. Liang, G.; Zhao, J.; Luo, F.; Weller, S.R.; Dong, Z.Y. A review of false data injection attacks against modern power systems. IEEE Trans. Smart Grid 2016, 8, 1630–1638.

16. Shi, L.; Dai, Q.; Ni, Y. Cyber–physical interactions in power systems: A review of models, methods, and applications. Electr. Power Syst. Res. 2018, 163, 396–412.
17. Cui, L.; Qu, Y.; Gao, L.; Xie, G.; Yu, S. Detecting false data attacks using machine learning techniques in smart grid: A survey. J. Netw. Comput. Appl. 2020, 170, 102808.
18. Yohanandhan, R.V.; Elavarasan, R.M.; Manoharan, P.; Mihet-Popa, L. Cyber-Physical Power System (CPPS): A Review on Modeling, Simulation, and Analysis With Cyber Security Applications. IEEE Access 2020, 8, 151019–151064.
19. Rouzbahani, H.M.; Karimipour, H.; Lei, L. Multi-layer defense algorithm against deep reinforcement learning-based intruders in smart grids. Int. J. Electr. Power Energy Syst. 2023, 146, 108798. [CrossRef]
20. Khoei, T.T.; Kaabouch, N. Densely Connected Neural Networks for Detecting Denial of Service Attacks on Smart Grid Network. In Proceedings of the 2022 IEEE 13th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), New York, NY, USA, 26–29 October 2022; pp. 0207–0211.
21. Chahal, A.; Gulia, P.; Gill, N.S.; Chatterjee, J.M. Performance Analysis of an Optimized ANN Model to Predict the Stability of Smart Grid. Complexity 2022, 2022, 7319010. [CrossRef]
22. Li, X., & Hedman, K. W. (2020). Enhancing power system cyber-security with systematic two-stage detection strategy. IEEE Transactions on Power Systems, 35(2), 1549–1561.
23. Li, D., Guo, H., Zhou, J., Zhou, L., & Wong, J. W. (2019). SCADAWall: A CPI-enabled firewall model for SCADA security. Computers & Security, [ISSN: 0167-4048] 80, 134–154.
24. Singh, V. K., Ebrahem, H., & Govindarasu, M. (2018). Security evaluation of two intrusion detection systems in smart grid SCADA environment. In 2018 north American power symposium (pp. 1–6).
25. Peng, W., Kong, X., Peng, G., Li, X., & Wang, Z. (2019). Network intrusion detection based on deep learning. In 2019 international conference on communications, information system and computer engineering (pp. 431–435).
26. Hai-He, T. (2018). Intrusion detection method based on improved neural network. In 2018 international conference on smart grid and electrical automation (pp. 151–154).
27. Erol Gelenbe, Omer H. Abdelrahman and Gokce Gorbil, "Detection and mitigation of signaling storms in mobile networks," IEEE ICNC 2016: 1-5.