ESP-JETA
ESP Journal of Engineering & Technology Advancements
ISSN: 2583-2646 / Volume 4 Issue 1 February 2024 / Page No: 70-74
Paper Id: JETA-V4I1P109 / Doi: 10.56472/25832646/JETA-V4I1P109

Original Article

Machine Learning in Power System

Gowshika[1], Rajasekar K[2]
[1,2]*Dept. of Electrical and Electronics Engineering, Grace College of Engineering, Thoothukudi, Tamilnadu, India*

Received Date: 30 December 2023 Revised Date: 30 January 2024 Accepted Date: 28 February 2024

Abstract: *Building a robust and effective grid is made possible by the rising use of renewable energy sources, the liberalization of the energy markets, and—above all—the integration of diverse monitoring, measuring, and communication infrastructures into contemporary power system networks. Energy stakeholders have prioritized the need for effective approaches for the faster identification and detection of these issues over the years. Power system studies are among the many applications where machine learning techniques have shown themselves to be useful in recent times. Artificial neural networks (ANNs), among other machine learning approaches, have been presented. These techniques have led to effective decision making and control actions in the safe and stable operations of the power system. This project offers a thorough analysis of the most recent research on machine learning approaches developed for power system security and stability, particularly in cyber-attack detection and dynamic security assessment studies, in light of this expanding trend. The goal is to draw attention to the approaches, successes, and—above all—the shortcomings in the datasets, test systems, and classifier(s) design used in the works under review.*

Keywords: *Machine Learning, Power System, Artificial Neural Network (ANN).*

I. INTRODUCTION

In order to integrate renewable energy and storage systems (RES), liberalize the market, and accommodate a multitude of measurement and communication technologies devices, to mention a few, power system operations have been continuously upgraded over the past few decades. Although the modernization has improved the distribution of cleaner, safer, and more dependable energy to customers, it also presents new risks to the stability and security of the network. The networks have become vulnerable to a number of threats due to the over-reliance of current power system applications, such as state estimation, Supervisory Control and Data Acquisition (SCADA) systems, and Phasor Measurement Units (PMUs), on open communication technologies like the internet. Because the country's power system is tightly linked to a variety of social, political, and economic activities, governments and utility stakeholders typically view the secure and stable operation of the power system as a crucial infrastructure. Adversaries can gain access to network nodes and change measures, including control commands. This can cause instability in the operation, lead to blackouts and financial losses, and in certain cases, jeopardize national security.

II. SYSTEM IMPLEMENTATION

A. Existing system

- The current system uses PMU data for detection and categorization using a machine learning-based approach.
- The current technique uses machine learning and wavelet analysis to identify and categorize the events.

Existing machine learning algorithms, such as SVM and DT, are utilized.

B. Proposed system

- This machine learning project's suggested scheme for the power system.
- This system makes use of methods and techniques for machine learning.
- The artificial neural network method used in this suggested system (ANN)

C. Artificial Neural Network (ANN)

- The Artificial Neural Network Tutorial covers both fundamental and sophisticated ANN principles. Our Artificial Neural Network course is designed for both novices and experts.
- "Artificial neural network" describes a branch of artificial intelligence that draws inspiration from biology and is based on brain models. Generally speaking, an artificial neural network is a computational network that is modeled after the biological neural networks that give the human brain its structure. Artificial neural networks feature neurons that are connected to one another at different layers of the network, just as neurons in a real brain. We refer to these neurons as nodes.
- This tutorial on artificial neural networks covers every facet of the technology. ANNs, adaptive resonance theory, Kohonen self-organizing maps, building blocks, unsupervised learning, genetic algorithms, etc. will all be covered in this tutorial.

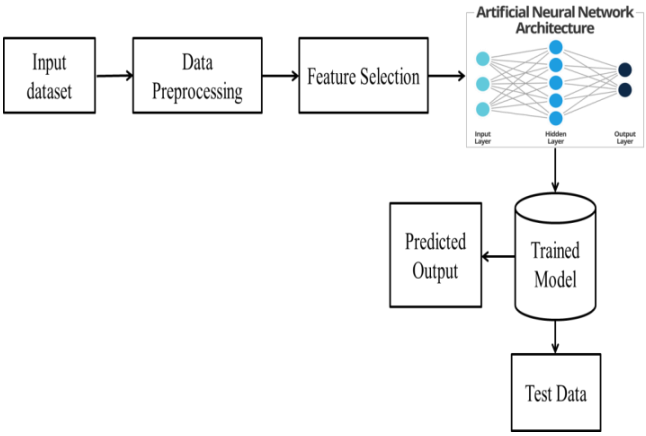

Figure 1: Artificial Neural Network (ANN)

a) What is Artificial Neural Network?

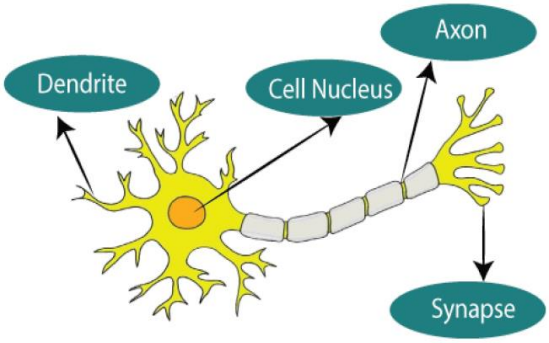

Figure 2: Typical Diagram of Biological Neural Network

The biological neural networks that give rise to the human brain's structure are the source of the phrase "Artificial Neural Network". Artificial neural networks also feature neurons that are connected to one another in different layers of the networks, just like neurons do in the human brain. We refer to these neurons as nodes.

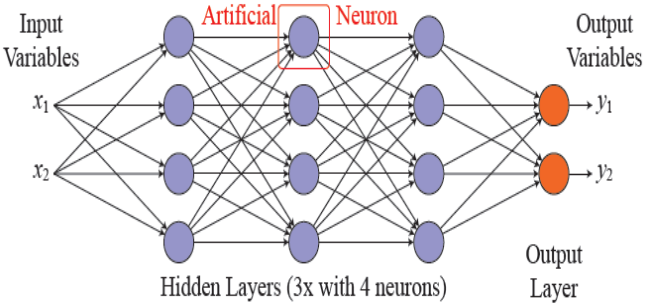

Figure 3: Artificial Neural Network

Artificial neural networks' inputs are represented by dendrites from biological neural networks, nodes by cell nuclei, weights by synapses, and outputs by axons. In the science of artificial intelligence, an artificial neural network aims to replicate the neuronal network that makes up a human brain so that computers can comprehend information and make judgments that resemble those of humans. In order to create an artificial neural network, computers are programmed to act like linked brain cells. The human brain has roughly a billion billion neurons. An connection point is present in every neuron, and they range from 1,000 to 100,000. Data is distributedly stored in the human brain, and humans are able to retrieve many pieces of this data from memory concurrently when needed. We can state that the human brain is composed of extraordinarily powerful parallel processing units.

An example of a digital logic gate that accepts an input and outputs an output can help us comprehend artificial neural networks. The "OR" gate accepts two inputs. An output of "On" results when any or both of the inputs are "On." We obtain a "Off" output if both inputs are "Off." In this case, input determines output. The functions of our brain differ from one another. Because our brain's neurons are "learning," the relationship between the inputs and outputs is always shifting."

b) The architecture of an Artificial Neural Network:

We must comprehend what makes up a neural network before we can comprehend the idea of an artificial neural network's architecture. To describe a neural network made up of many artificial neurons, also known as units grouped in a layer-by-layer fashion. Let's examine the many kinds of layers that artificial neural networks can have.

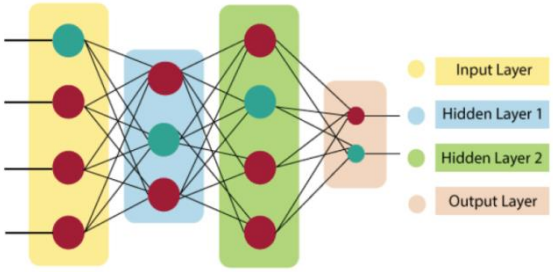

Figure 4: Architecture of an Artificial Neural Network

Artificial Neural Network primarily consists of three layers:

i) Input Layer:

As the name suggests, it accepts inputs in several different formats provided by the programmer.

ii) Hidden Layer:

The hidden layer presents in-between input and output layers. It performs all the calculations to find hidden features and patterns.

iii) Output Layer:

The input goes through a series of transformations using the hidden layer, which finally results in output that is conveyed using this layer. The artificial neural network takes input and computes the weighted sum of the inputs and includes a bias. This computation is represented in the form of a transfer function.

$$\sum_{i=1}^{n} W_i * X_i + b$$

In order to generate the output, it ascertains that the weighted total is supplied as an input to an activation function. A node's activation function determines whether or not it should fire. The output layer is only accessible to individuals who are fired. There exist unique activation functions that can be utilized for the type of task we are carrying out.

c) How do Artificial Neural Networks Work?

The most effective way to visualize an artificial neural network is as a weighted directed graph, with the artificial neurons acting as the nodes. One way to conceptualize the relationship between neuron inputs and outputs is as directed edges with weights. The input signal for the artificial neural network is sent in the form of a vector picture and pattern from an external source. The notations x(n) are then used to mathematically allocate these inputs for each n numbers of inputs.

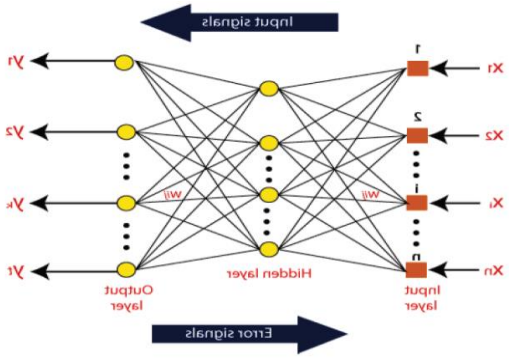

Figure 5: Work Flow for ANN

Subsequently, every input is multiplied by its respective weights, which are the unique details that the artificial neural networks use to solve a given problem. Generally speaking, these weights typically indicate how strongly the neurons inside the artificial neural network are connected to one another. Within the computing unit, a summary of each weighted input is provided.

III. RESULT

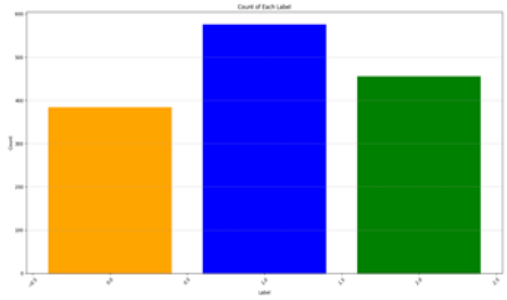

Figure 6: Count Label

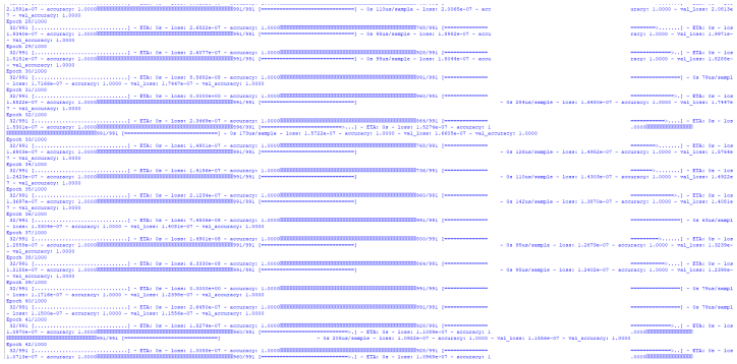

Figure 7: Training Epochs

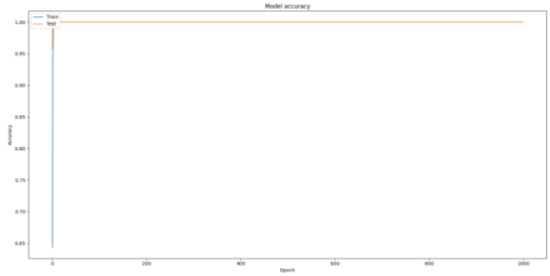

Figure 8: Model Accuracy

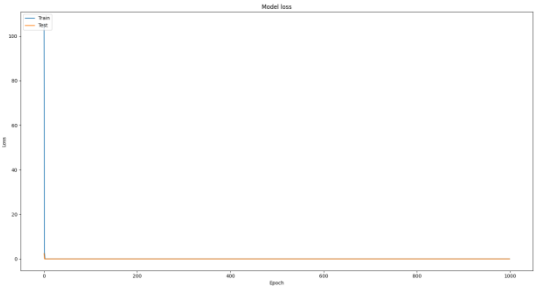

Figure 9: Model Loss

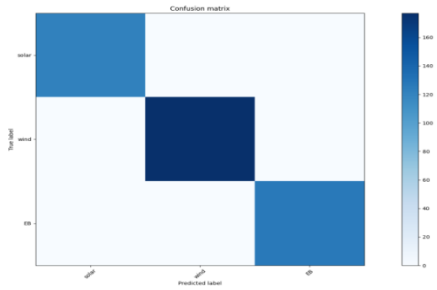

Figure 10: Confusion Matrix

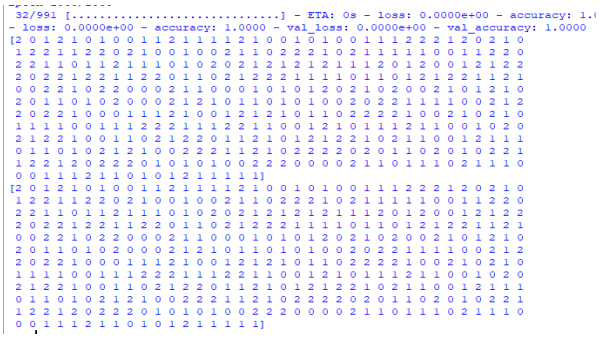

Figure 11: Accuracy

IV. CONCLUSION

Security and stability of the power system have been top priorities for all parties involved in the energy industry, particularly operators, in the recent past. Operators need to be very skilled at quickly identifying possible intrusions, attacks, disruptions, and situational awareness. The implementation of traditional techniques has revealed shortcomings, particularly with regard to resilience and adaptability to the current and future power system trends. In order to tackle these issues, the following study provides an extensive analysis of the latest MLT-based strategies for countering the threats to the dominating power system: voltage stability evaluation, transient stability assessment, SCADA network vulnerability and threats, and power quality disturbance. In contrast to numerous other previously published efforts, this study discusses the limits and the approaches used. definitions for each acronym that is used throughout the project. Current trends in MLT applications and how they can be used to power stability and security measures for systems.

V. REFERENCES

[1] Shouxiang Wang, Haiwen Chen “A novel deep learning method for the classification of power quality disturbances using deep convolutional neural network”2019.

[2] Oludamilare Bode Adewuyi, Ryuto Shigenobu, Kazuki Ooya, Tomonobu Senjyu, Abdul Motin Howlader “Static voltage stability improvement with battery energy storage considering optimal control of active and reactive power injection”2019.

[3] Jun Gao,Luyun Gan,Fabiola Buschendorf “Omni SCADA Intrusion Detection Using Deep Learning Algorithms”,2019.

[4] Xinyu Wang, Xiaoyuan Luo, Mingyue Zhang “Distributed detection and isolation of false data injection attacks in smart grids via nonlinear unknown input observers”2019.

[5] Tatiana Chakravorti a, N.R. Nayak a, Ranjeeta Bisoi “A new robust kernel ridge regression classifier for islanding and power quality disturbances in a multi distributed generation based microgrid”2019.

[6] Oyeniyi Akeem Alimi,Khmaies Ouahada “Real Time Security Assessment of the Power System Using a Hybrid Support Vector Machine and Multilayer Perceptron Neural Network Algorithms”2019.

[7] "DIFFERENTIAL PRIVACY TECHNIQUES IN MACHINE LEARNING FOR ENHANCED PRIVACY PRESERVATION", International Journal of Emerging Technologies and Innovative Research (www.jetir.org), ISSN:2349-5162, Vol.11, Issue 2, page no.b148-b153, February-2024, Available: http://www.jetir.org/papers/JETIR2402116.pdf

[8] Meir Kalech “Cyber-attack detection in SCADA systems using temporal pattern recognition techniques”2019.

[9] Fayyaz Jandan,Syed Abid Ali Shaha “Recognition and Classification of Power Quality Disturbances by DWT-MRA and SVM Classifier”2019.

[10] U.Singh,S.N.Singh“A new optimal feature selection scheme for classification of power quality disturbances based on ant colony framework” 2020

[11] 10.Lu Zhou, Chunhua Su, Zhen Li, Zhe Liu, Gerhard. Hancke “Automatic fine-grained access control in SCADA by machine learning”2019.