SSRG International Journal of Computer Science and Engineering
ISSN: 2348–8387 / https://doi.org/10.14445/23488387/IJCSE-V9I12P101

Volume 9 Issue 12, 1-6, May 2022
© 2022 Seventh Sense Research Group®

Original Article

Cyber Security in Wind Energy Generation Via Deep Learning

P. Rajadurai

Department of Computer Science, Tamilavel Umamaheswaranar Karanthai Arts College, State, Thanjavur, India.

Received: 01 November 2022 Revised: 01 December 2022 Accepted: 12 December 2022 Published: 30 December 2022

Abstract - *This paper introduces a novel cyberattack classification via a convolutional neural network. Initially, the data are gathered using wind turbine sensors. The designed infrastructure is used to keep an eye on the cyberattacks as they happen and to ensure the stability of CNC machines for efficient cutting processes that can assist in raising product quality. In order to detect the vibration conditions, for this reason, a force sensor has been installed in the milling CNC machine center. This paper proposes cyber security in wind energy via deep learning, an optimized algorithm that uses CNN to classify differences between CNC machines to maintain the CNC machine. Consequently, the proposed deep learning can properly classify four different types of attacks, namely combinatorial attacks, denial-of-service (DOS) attacks, phishing attacks, and zero-day attacks. Multiple schemes are shown to illustrate the reliability of the proposed system, namely one in which the scheme may instantly secure itself when the cyberattack triggers the backup broker to switch to the backup. Successful cyberattacks on wind farms can harm power systems in several ways, including the grid's stability, the operation of the energy market, and the stability of the wind farm system. Considering the cybersecurity of wind generators, the specific aspects of cyber-attack modeling, detection, and mitigation are the greatest priority. Ultimately, efforts must be made to create smart wind assets that are also cyber-resilient to keep uninterrupted operations. Sensitivity, accuracy, specificity, and recall are the parameters considered when evaluating the proposed model's effectiveness. The suggested technique exceeds RNN, ANN, and DNN in terms of global accuracy by 99.01%.*

Keywords - *Deep learning, Industry 4.0, Internet of Things, Smart machines, Milling process, Sensors, CNN.*

1. Introduction

Several rapid technical breakthroughs, such as Big Data analytics, AI, and the Internet of Things (IoT), drive the applications of Industry 4.0. The Internet of Things (IoT) and the technology that enables communication among them, with the internet, and within specific devices are formed by interconnected things. Artificial intelligence, or an artificial intelligence system, is able to perform tasks that a human being would normally perform because they require natural intelligence and judgment. Big data analytics, such as data analysis, diagnostic analytics, predictive analytics, and predictive analysis, can give a range of information when attached to the IoT. Data analysis provides detailed information about a linked device's actual performance. Those scientific discoveries are typically smart sensors, data analysis, and information assurance to accelerate the global manufacturing sector.

Producers can rapidly respond to marketplace demands by integrating the industrial IoT topology using machine learning, computer architecture, data analytics, and management. To provide safe and reliable computer numerical control (CNC) operations in practically all industries, decision-makers and industrial output planners are motivated to create new and effective techniques. Utilizing metal-cutting techniques to obtain precision parts and spreading knowledge about cyberattacks are two ways. In order to increase cutting productivity, the material depth of cut, feed, and spindle speed needs to be increased. The object will start humming at a performing process at a chattering frequency and then become excited on its own. Budak and Altintas identified this phenomenon. Chatter vibration must be recognized and regulated to ensure consistent cutting, boost productivity, and enhance product quality.

Historically, signal collecting, data gathering, extraction of features, feature selection, and classification has served as the components of machine learning-based noise detection. It is assumed that the repetitive and unnecessary features would be removed from the data set because they will degrade classification performance and elongate calculation times. Deep learning can address these issues by recognizing patterns and extracting relevant aspects immediately. An extreme method of machine learning called deep learning uses a computational model with different layers to extract the features from a vast amount of information.

Given the view of all this, the recommended IoT topology with deep learning can offer a dependable probability of achieving, which improves industry 4.0 expenditures and economic outcomes. Our paper's contribution is as follows:

- The IoT platform can highlight the cyberattack mostly on the main dashboard owing to the newly introduced deep learning method.
- Tracking the CNC milling to assess the state of interruptions requires using a measurement system built on the IoT platform and CNN algorithms.
- The application of genetics can differentiate between unstable and stable cutting conditions to ensure efficient cutting processes.
- The developed scheme may evaluate the state of processing accurately because it is more precise than conventional machine-learning techniques. The proposed model may evaluate the machining state accurately since it is more precise than conventional machine-learning techniques.
- As a result, sensitivity, accuracy, specificity, and recall are the parameters taken into consideration when evaluating the effectiveness of the proposed model.

Following is a description of how this paper is organized, section 2 describes the literature review of previous research, Section 3 describes the in-depth evaluation of the proposed work, Section 4 describes the results, and Section 5 describes the conclusion.

2. Literature Survey

In 2020, Syeda Manjia Tahsien et al. proposed the structure of the IoT after a detailed analysis of the ML algorithmic study. They explored the significance of IoT security in light of several forms of potential threats. An in-depth assessment of current literature on IoT and its structure was also included in computer networks, as was a full examination of multiple security assaults, an attacking interface with impacts, various classes of ML-based algorithms, and ML-based cybersecurity.

In 2022, Mahmoud Elsisi et al. proposed that a new Internet of Things (IoT) design has indeed been integrated with deep learning for online power transformer state surveillance to safeguard from cyberattacks. The proposed IoT interface will enable highly secure monitoring of the transformer's state across the network connection and efficiently detect cyberattacks. Using the measured quantity of inert gases, a convolution neural network (1D-CNN) was utilized to analyze the defects of a power system and a cyberattack on the network connection.

In 2021, Elsisi. M et al. proposed an additional capacity built on deep learning that will be utilized to assess and track the output data from smart meters to determine whether it is accurate or not. Ineffective meters and manipulation are to blame for the bogus data. The manufacturing system's temperature, dryness, and noise signals have an impact on the meters' accuracy. Generally speaking, this technique improves modern IoT systems' dependability, raising industry 4.0 investment levels. Moreover, it can be used with various kinds of sensors.

In 2017, Feng. C et al. proposed an improved version of deep learning that allows an operator to carry out stealthy attacks with minimal to no prior experience with the target ICS, and we use two real-world ICS research studies to demonstrate well how our method performs for this purpose. This system attribute allows it to be autonomous of particular ICS types and thus applicable in various industrial scenarios. We suggest developing and implementing unique security mechanisms to protect against sneaky attacks generated by our approach.

In 2016, Wan. J et al. proposed a software-defined IoT to create a new idea for complex settings by enabling the network to be more resilient. Moreover, describe the data exchange between multiple devices, in addition to examining the IoT architecture, which comprises the physical layer, IWNs, industrial cloud, and smart connectors. In addition, a software-defined IoT architecture was assessed to distribute network capacity and accelerate information Network protocols are easily adapted to exchange processes. Implementation of Industry 4.0 will be accelerated through software-defined IoT

In 2021, Elsisi. M et al. proposed a modified neural network algorithm (MNNA) is suggested as an adaptive tuning technique for improving the performance of control systems. The modulation is produced via a variant of a polynomial. Two smart methods have been employed in the literature to assess the suggested algorithm: the genetic algorithm (GA) and the cuckoo search algorithm (CSA) with a PID controller. The proposed algorithm involves the better quality of the controller gain limits, agent count, and iteration count.

In 2021, Elsisi. M et al. proposed that the most efficient control method for nonlinear systems is a nonlinear MPC (NLMPC), which replaces the regular MPC. In particular, this work recommends using NLMPC to manage robotic manipulators. According to the neural network algorithm (NNA), this application is viable for adaptive smart technology. Comparative analysis is done between the proposed enhanced NNA (MNNA) and the PID control strategy based on genetic algorithms. With a mean absolute error of roughly 0.005, the output data show how the suggested method outperforms the competition and is more effective for monitoring both regular and odd pathways.

3. Proposed Methodology

This section proposes cybersecurity in wind energy via deep learning, an optimize algorithm for classifying differences between CNC machines based on CNNs. Consequently, the proposed deep learning can properly classify four different types of attacks, namely combinatorial attacks, denial-of-service (DOS) attacks, phishing attacks, and zero-day attacks.

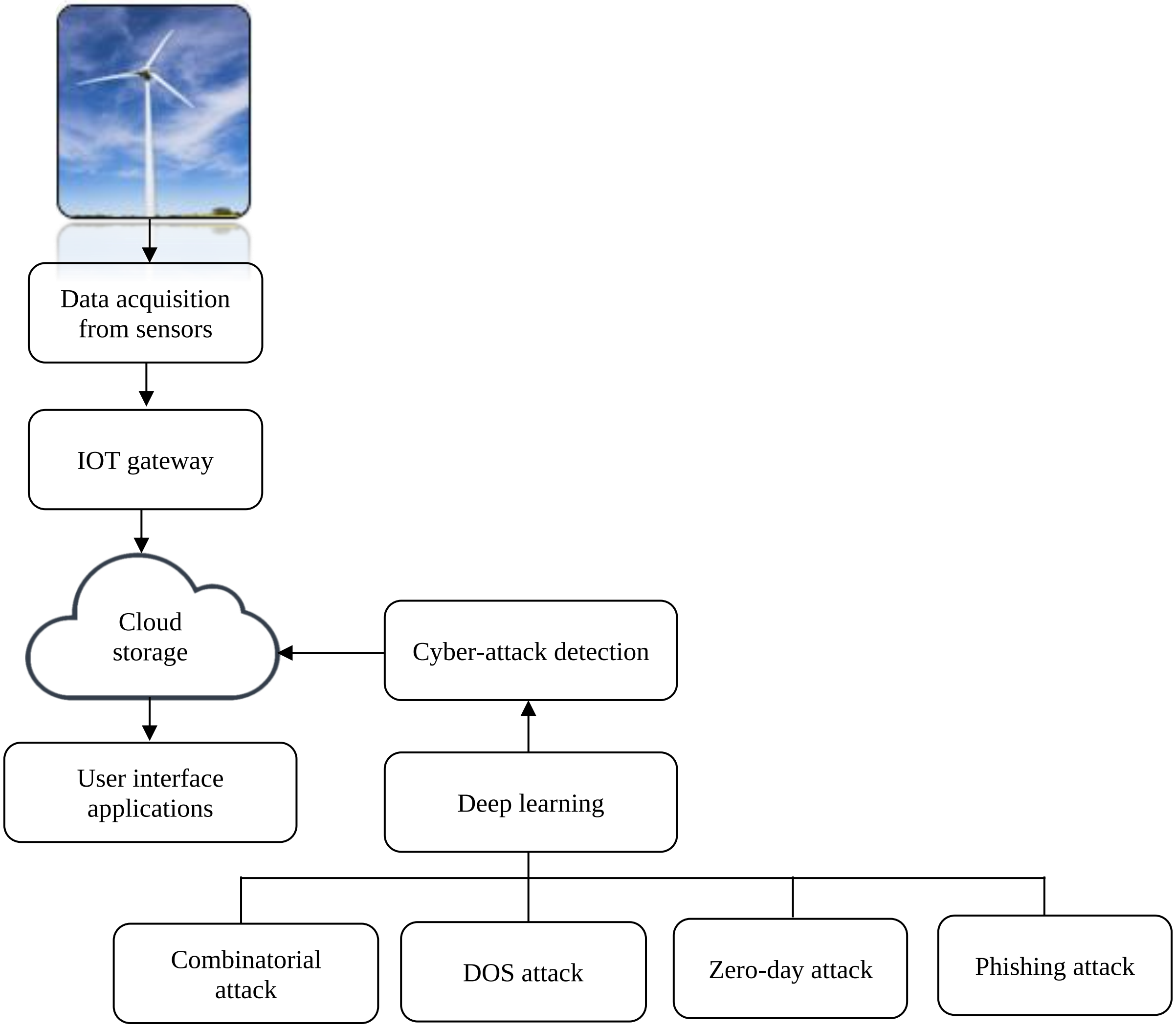

Fig. 1 Block diagram of the proposed methodology

3.1. Data Acquisition

An acquisition of data is the process of taking information from the outside world, digitizing it, and transferring it to a computer for presentation, processing, and storage. In this work, the data are gathered from six sensors; they are,

3.1.1. Speed Sensor

Wheel speed sensors (WSS) or vehicle speed sensors seem to be a unique type of sensor (VSS). It is a sender unit used to determine a vehicle's wheel rotation speed. Generally, it comprises a pickup and a toothed ring. Devices' internal spinning speeds are observed through speed sensors. Many vehicles, such as automobiles, airplanes, construction and off vehicles, trains, and military vehicles, use speed sensors.

3.1.2. Vibration Sensor

A vibration sensor, usually referred to as a vibration detector, is used to filter and analyze the vibration levels of machines. Machine vibration levels are filtered and analyzed using a vibration sensor, also known as a vibration detector. Also, it determines that vibrations in a device, system, or machine are measured in terms of their amount and frequency. An asset's metrics can detect instabilities or other issues, and predict impending disasters, based on these factors.

3.1.3. Temperature Sensor

The measurement of temperature in solids, liquids, or gases is done with the use of temperature sensors. They have many more commercial uses outside of just being employed in industry sectors. The majority of the temperature sensors we offer to detect the temperature by tracking variations in electrical current resistance.

3.1.4. Level Sensor

In a liquid level sensor, liquid (possibly solid) levels can be preserved, detected, and maintained. Once the fluid level has been detected, the sensor converts observational data into an electric signal.

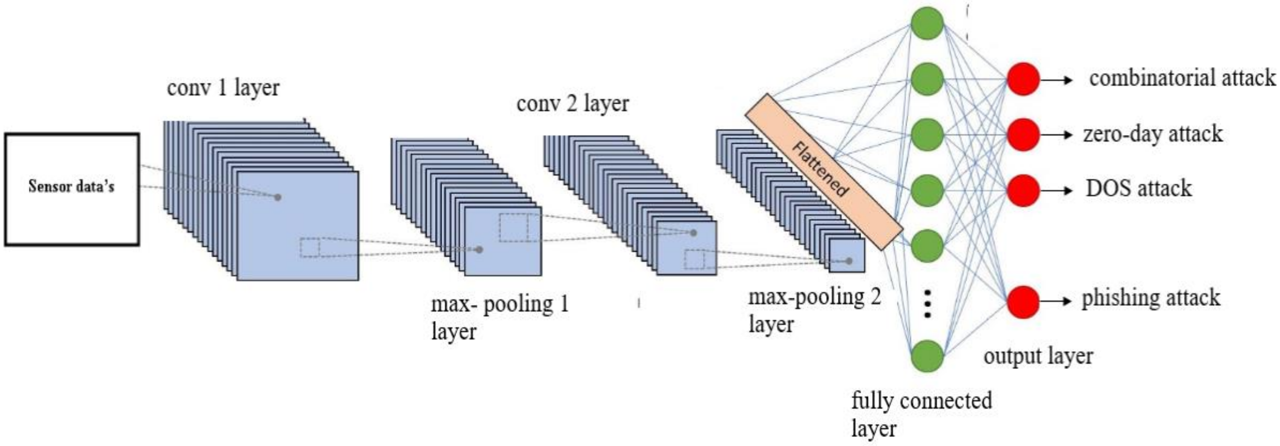

Fig. 2 Structure of CNN

3.1.5. Pressure Sensor

Sensors that measure pressure gauge gases or liquids. In order to refer to the force required to stop fluid from spreading, pressure is frequently expressed in terms of force per unit area. Pressure sensors are transducers because they provide a signal in response to applied pressure. The purpose of a pressure sensor is to observe, change, or maintain pressure and transform physical data into an electronic signal.

3.1.6. Position Sensor

A sensor that evaluates an object in the image is called a position sensor. A position sensor might show the object's exact location. A range of sensing technologies can be utilized with position sensors to determine either linear or circular positions. Position sensors are utilized in a broad range of applications; anything involving motion observation will do so.

3.2. Cyberattack Detection

Deep learning Convolutional Neural Network (CNN) is used to recognize cyberattacks. In contrast to existing knowledge of deep neural network approaches, Deep learning can provide higher-level traits and abstract concepts that reveal complicated and intricate relationships. A much greater number of progressively connected neuronal layers characterize deep learning. Higher levels of complexity also typically demand more data for training and computational loads due to more adjustments. The primary strength of the architecture for deep learning, the capacity for end-to-end learning, is made possible by these advancements, which provide the capability to efficiently calculate repeated nonlinear adjustments of the vital input data.

Both biases and weights connect the neurons at different levels. The initial level is referred to as the input layer, and the final level serves as the output layer, for example, in the hypothetical classification of plants into species. Hidden layers work together to alter the feature space of the input so that it resembles the output. CNNs employ at least one convolutional layer as a hidden layer to take advantage of patterns. Other non-convolutional levels may also contain convolutional layers. The network can therefore analyze and combine incredibly small visual elements, exposing new information by integrating several consecutive convolutional layers and their various filters. By combining numerous progressive fully connected layers and their various filters, the network may learn and accumulate micro-visual input and determine whether a given class is present in a given image.

The hyper-parameters, which include the number and features of hidden layers, pooling strategies, normalization schemes, and cost functions, further affect a CNN structure's complexity and overall performance. Remote sensing data and additional reference annotations—also known as labels or targets—were needed to train a CNN model for visualizing a landscape. Machine learning techniques like support vector networks and random forests make use of relatively straightforward array-type data structures. However, CNN-based training enables the use of more powerful data structures called convolution layers.

The architecture and properties of CNNs can be applied in various ways, opening up a wide range of opportunities for using vegetative remotely sensed data. The different positions of CNNs into 1D-, 2D-, and 3D-CNNs are based on kernel dimensions. Since 1D-CNNs do not directly take spatial context into account, they are utilized less frequently than 8% of the reviewed research and are mostly used to analyze optical spectrum or multi-temporal- satellite data.

The pooling operation will fall entirely down the insight along the spatial representation to decrease the number of elements in that stimulation. Using additional-level methods in between the sequence of several convolutional layers, the feature maps are frequently dynamically down-sampled. Max-pooling is the most used pooling operation. Massive activations (instead of, say, average pooling) are the idea behind max-pooling. The term "CNN architecture," which refers to how the neural or pooling layers of a CNN could be connected, can refer to a variety of distinct structures. As a result, CNNs can have a wide variety of ideas primarily controlled by the objective.

The strength of the input volume-connected area and the weight of the neurons whose output is connected to specific input volume regions will be estimated as a scalar product by the convolutional layer. By adding a "definite data" kernel function, such as a logarithmic, the rectified unit, often known as ReLu, aims to stimulate the output from the activation of the previous layers.

Then, the fully-connected layers will accomplish things similar to those in conventional ANNs in an attempt to obtain output values from the kernel function that can ultimately be used for classifications. ReLu may also be utilized between these layers in order to improve performance.

Multiple programming frameworks can be used for CNNs. PyTorch and TensorFlow are the two most popular deep learning platforms right now. Numerous DL architectures, including old and new, can be utilized manually and with the system. Both open-source enable the ability through documentation, several tutorials, and Java-based notebooks for a simple start. As a way, trained and realized models can be moved to a suitable framework.

To integrate the content and establish broad trends, a number of criteria, including primary CNN architecture, the spatial data platform, the sensor, the spatial resolution of the remote sensing techniques, and the method of comparison data collecting, were specified.

4. Result & Discussion

Data sensors are developed in CNN architecture to classify combinatorial attacks, zero-day attacks, and phishing attacks as part of the overall results. The efficiency of DOS attacks is also assessed, and their effectiveness is evaluated and compared with other methodologies. Its comparative study confirms the performance effectiveness of the proposed method.

4.1. Evaluation Metrics

The proposed model has been evaluated using the conventional numerical parameters listed below. Accuracy, recall, specificity, and sensitivity were each determined using Equations (1), (2), (3), and (4), respectively. The accuracy was determined using equation (1):

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \tag{1}$$

$$Sensitivity = \frac{TP}{TP+FP} \tag{2}$$

$$Recall = \frac{TP}{TP+FN} \tag{3}$$

$$specificity = \frac{TP}{TP+FN} \tag{4}$$

Four alternative results for the given data exist False Negative (FN), True Negative (TN), False Positive (FP), and True Positive (TP). False Negative data is labeled positively, whereas genuine positive data is labeled positively and categorized as such. False positive data is referred to as positive, while TN data is labeled negative and labeled as negative.

Figure 3 illustrates a graphical overview of proposed and existing methods with various parameters, including recall, accuracy, specificity, and precision rate. The output of the graphs makes it clearly visible that the proposed methodology is superior to all currently used techniques and suitable for detecting attacks. The proposed methods' specificity and sensitivity are 98.07% and 98.02%, respectively. Compared to previous models, the suggested framework was more sensitive and specific than the existing RNN, ANN, and DNN models

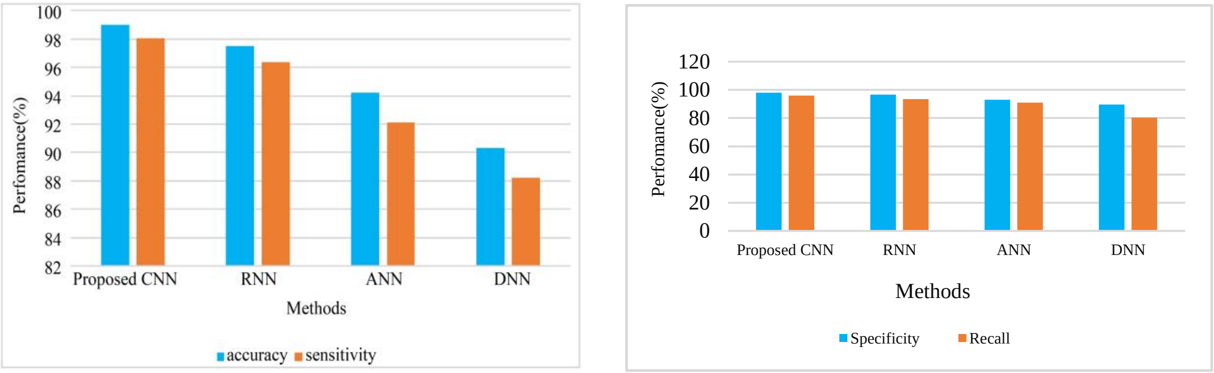

Fig. 3 Comparitive analysis of the proposed method

5. Conclusion

In this paper, cyber security in wind energy via deep learning, an optimized CNN model is proposed to maintain the CNC machine to classify the differences. A deep learning algorithm has been implemented in a more modern IoT architecture recently rebuilt for vibration control and monitoring in order to maintain the goal of maintaining the stability of CNC machines. Various mailing states, such as stable cutting, unstable cutting, and false cutting, can be identified by updating the deep-learning neural network model. This assessment has been developed with the concept of a cyber-physical system in the Industry 4.0 era, where deep learning and IoT play important roles. Benefits show that the proposed method may reduce vibration more effectively than other conventional machine-learning techniques. This leads to the definition of the four sorts of attacks: combinatorial assault, denial-of-service attack (DOS), phishing attack, and zero-day attack. The metrics taken into account for evaluating the suggested model's efficacy are sensitivity, accuracy, specificity, and recalls. The proposed methodology effectively improves accuracy by about 99.01% when compared to RNN, ANN, and DNN.

References

[1] Syeda Manjia Tahsien, Hadis Karimipour, and Petros Spachos, “Machine Learning Based Solutions for Security of Internet of Things (IoT): A Survey,” *Journal of Network and Computer Applications*, vol. 161, p. 102630, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[2] Mahmoud Elsisi et al., “Effective IoT-Based Deep Learning Platform for Online Fault Diagnosis of Power Transformers Against Cyber Attacks and Data Uncertainties,” *Measurement*, vol. 190, p. 110686, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[3] S.Veerapandi, R.Surendiran, and K.Alagarsamy, "Enhanced Fault Tolerant Cloud Architecture to Cloud based Computing using Both Proactive and Reactive Mechanisms," *DS Journal of Digital Science and Technology*, vol. 1, no. 1, pp. 32-40, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[4] Mahmoud Elsisi et al., “Reliable Industry 4.0 Based on Machine Learning and IoT for Analyzing, Monitoring, and Securing Smart Meters,” *Sensors*, vol. 21, no. 2, p. 487, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[5] Diptiban Ghillani, “Deep Learning and Artificial Intelligence Framework to Improve the Cyber Security,” *Authorea Preprints*, 2022. [Google Scholar] [Publisher Link]

[6] Peravali Kavya, "An Efficient Machine Learning based Algorithm for Preventing Phishing Websites," *SSRG International Journal of Computer Science and Engineering*, vol. 5, no. 12, pp. 10-13, 2018. [CrossRef] [Publisher Link]

[7] Cheng Feng et al., “A Deep Learning-Based Framework for Conducting Stealthy Attacks in Industrial Control Systems,” *arXiv preprint arXiv:1709.06397*, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[8] B Sunaina Sharma, "Enlargement of an Intellectual and Energy Proficient Spindle System," *SSRG International Journal of Mechanical Engineering*, vol. 3, no. 12, pp. 5-9, 2016. [CrossRef] [Publisher Link]

[9] Jiafu Wan et al., “Software-Defined Industrial Internet of Things in the Context of Industry 4.0,” *IEEE Sensors Journal*, vol. 16, no. 20, pp. 7373-7380, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[10] Mahmoud Elsisi et al., “An Improved Neural Network Algorithm to Efficiently Track Various Trajectories of Robot Manipulator Arms,” *IEEE Access*, vol. 9, pp. 11911-11920, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[11] Ganiyu Adedayo Ajenikoko et al., "Development of a Technique for Identification of Critical Locations for Maintaining Voltage Stability with Penetration of Wind Generation in Power Systems," *SSRG International Journal of Electrical and Electronics Engineering*, vol. 7, no. 5, pp. 9-20, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[12] Mahmoud Elsisi et al., “Effective Nonlinear Model Predictive Control Scheme Tuned by Improved NN for Robotic Manipulators,” *IEEE Access*, vol. 9, pp. 64278-64290, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[13] Zewen Li et al., “A Survey of Convolutional Neural Networks: Analysis, Applications, and Prospects,” *IEEE Transactions on Neural Networks and Learning Systems*, vol. 33, no. 12, pp. 6999-7019, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[14] Mulumudi Rajesh, and A. Lakshmi Devi, "Wind, PV Solar, Hydro and Hybrid Energy Storage System-Based Intelligent Adaptive Control for Standalone Distributed Generation System," *SSRG International Journal of Electrical and Electronics Engineering*, vol. 9, no. 11, pp. 67-94, 2022. [CrossRef] [Publisher Link]

[15] Jiuxiang Gu et al., “Recent Advances in Convolutional Neural Networks,” *Pattern Recognition*, vol. 77, pp. 354-377, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[16] S. Priyanka et al., "IoT Based Hybrid Artificial Tree for Solar/Wind Power Generation with Pollution Control and Monitoring," *SSRG International Journal of Computer Science and Engineering*, vol. 8, no. 4, pp. 1-3, 2021. [CrossRef] [Publisher Link]