International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Artificial Intelligence Enabled Network Intrusion Detection Model (AI-NIDM) for Smart Grid Cyber-Physical Systems

P. Dhanasekaran[1], Sakthivel. V[2], N. Jayashri[3], M. S. Hemawathi[4], Vishnu Kumar Kaliappan[5]

Submitted: 14/07/2023 **Revised**: 07/09/2023 **Accepted**: 25/09/2023

Abstract: The increasing complexity and interconnectivity of Smart Grid Cyber-Physical Systems (SG-CPS) have raised significant concerns regarding the security and integrity of these systems. Network Intrusion Detection Model (NIDM) is an essential component of SG-CPS security infrastructure. However, the conventional rule-based and signature-based NIDM are becoming less effective in detecting advanced and sophisticated cyber-attacks. Artificial Intelligence (AI) technologies, named machine learning, deep learning, and neural networks, have shown great potential in enhancing the accuracy and efficiency of NIDM. This paper proposes an AI-Enabled Network Intrusion Detection Model (AI-NIDM) called GWA-ANN for SG-CPS, which integrates AI techniques with traditional NIDS for improved detection and response to cyber-attacks. The proposed system is evaluated on a public SG-CPS dataset, and the results establish that AI-NIDM can effectively detect and classify various types of cyber-attacks with high accuracy and low false-positive rates. The proposed AI-NIDM can significantly improve the security and resilience of SG-CPS against emerging cyber threats.

Keywords: *AI-Enabled Network Intrusion Detection Model, Smart Grid Cyber-Physical Systems, Artificial Intelligence, Cyber-attack detection, Cyber-attack response*

1. Introduction

Smart Grid Cyber-Physical Systems (CPS) is a type of advanced power grid that incorporates advanced communication, control, and monitoring technologies to improve the reliability, efficiency, and security of power systems. The Smart Grid CPS integrates power system operation with communication and information technologies, enabling a more robust, efficient, and sustainable grid [1]. A Smart Grid CPS uses smart devices and sensors to collect data and transfer it in real-time to control centers. The control centers can use this data to analyze the functioning of the grid and make decisions, such as rerouting power to avoid outages or altering power generation to meet fluctuating demand [2,3].

Cyber-Physical Systems for Smart Grids (SG-CPS) use analog and digital technology to track and manage the flow of electricity in a power grid which is represented in Figure 1. However, the SG-CPS's growing reliance on interconnected equipment and networks has also raised the danger of cyberattacks, which could have negative effects on the power grid's dependability and safety. Antivirus software and firewalls are examples of traditional security measures, but they are insufficient to identify and stop sophisticated cyberattacks. Consequently, more advanced intrusion detection techniques are required in order to recognize and respond to cyberattacks in real-time [4].

[1] *The Kavery Engineering College, Mechery, Salem-636453*
dhanawaves@gmail.com
[2]*School of Computer Science and Engineering, Vellore Institute of Technology, Chennai, Tamilnadu, India, 600127*
sakthivel.v@vit.ac.in
[3]*Faculty of Computer Applications, Dr. M.G.R Educational and Research Institute, Chennai.*
jayashrichandrasekar@yahoo.co.in
[4]*The Kavery Engineering College, Mechery, Salem-636453*
hemasomasundram@gmail.com
[5*]*Department of Computer Science and Engineering, KPR Institute of Engineering and Technology, Arasur, Coimbatore - 641047, Tamil Nadu, India*
vishnudms@gmail.com

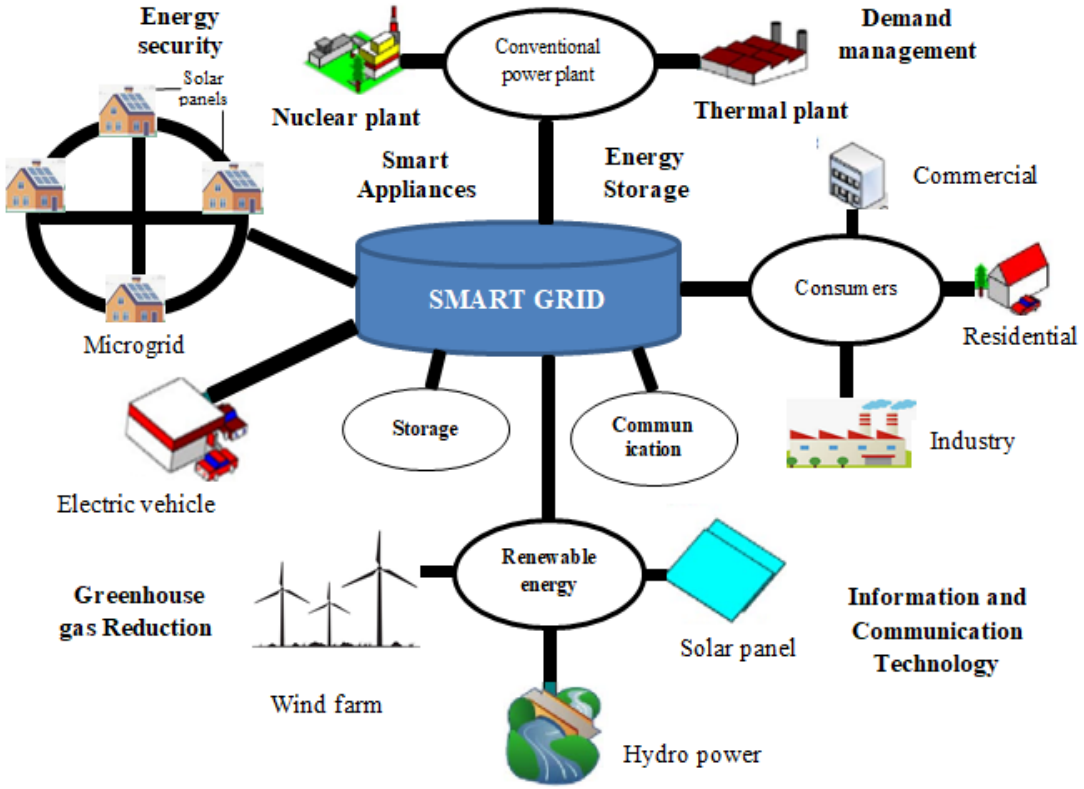

Fig 1. Smart Grid CPS

An intrusion detection system (IDS) is a security mechanism that observes over network or system activity for indications of hostile activity or policy breaches. It might be compared to a security guard who monitors your network or system looking for potential dangers and taking action when necessary. IDS functions by evaluating data from different sources, including network traffic, log files, and system events, to spot unusual behavior or trends that could point to an intrusion. IDS comes in two primary varieties: Network-based IDS (NIDS) This kind of IDS monitors network traffic in real-time and examines it to find suspicious activity. NIDS can identify a wide range of attacks, including port scanning, network probes, and malware. Host-based intrusion detection systems (HIDS): This sort of IDS is deployed on a specific host and monitors the host's actions. HIDS can detect assaults directed at a specific system or application, as well as insider threats. Signature-based and anomaly-based are the types of intrusion detection systems (IDS). Signature-based intrusion detection systems identify intrusion attempts by using pre-defined signatures or patterns of known assaults. Anomaly-based intrusion detection systems, on the other hand, use statistical analysis and machine learning techniques to detect anomalous behavior that deviates from the system's regular behavior [5].

AI has shown potential in terms of enhancing the accuracy and speed of intrusion detection in SG-CPS. AI-powered intrusion detection models can evaluate vast volumes of data in real-time, discover anomalies, and accurately classify attacks. Current AI-based intrusion detection methods, on the other hand, have disadvantages such as high false positives and false negatives, as well as limited scalability. As a result, an AI-based intrusion detection model that can overcome these constraints and provide effective security against cyber-attacks in SG-CPS is required. The goal of this research is to create an AI-based intrusion detection model capable of detecting and responding to cyber-attacks in SG-CPS while overcoming the limitations of existing intrusion detection approaches. This concept, known as the Artificial Intelligence Enabled Network Intrusion Detection concept (AI-NIDM), attempts to improve the security and dependability of SG-CPS while also ensuring that users continue to receive electricity.

2. Literature Review

[6] An Intrusion detection system (IDS) for Cognitive Cyber-Physical Systems (CPS) in the Industry 4.0 context that is AI enabled is proposed. The suggested system makes use of AI approaches to evaluate massive amounts of data in real-time, spot aberrant activity, and provide automatic reactions in order to get beyond the constraints of conventional IDS systems in the Industry 4.0 context. The suggested model performs data adaptation and data regulation as the first steps in the data pre-processing process. For the right feature selection, the “Improved Fish

Swarm Optimization-based Feature Selection (IFSO-FS)" method is used. The normal FSO algorithm's search procedure incorporates the Levy Flight (LF) idea to produce the IFSO approach, which does not have the local optima problem.

[7] Developed a method for the detection of False Data Injection (FDI) attacks in Smart Grid Cyber-Physical Systems (CPS). In order to improve the security and dependability of the Smart Grid CPS, the study looks into how FDI attacks can be identified in real time. To begin with, analytical system based on stochastic Petri net is created in order to assess and examine the system dependability of smart grid CPSs, especially with regard to topological attacks when system countermeasures are in place. The second is the proposal of a distributed host-based collective detection system to identify FmDI assaults in smart grid CPSs.

[8] proposed the development and evaluation of an anomaly-based intrusion detection system (IDS) for security of Cyber-Physical Systems (CPS). The study aims to investigate how an IDS system can be designed to detect anomalous behavior in CPS and provide early warning of potential security threats. This paper aims to introduce a Machine Learning-based tool for detecting cyber-attacks in cyber-physical systems. By analyzing the values generated by Machine Learning, the paper evaluates the classification performance of three different models. The results of the analysis indicate that the model trained on the dataset can successfully distinguish between normal and anomalous behavior. To demonstrate the effectiveness of this approach, the tool is implemented in a water tank system to identify potential attacks and prevent hazardous situations, such as tank overflow. The results show promising outcomes, suggesting the tool can effectively enhance the security of cyber-physical systems.

False data injection attacks can destabilize interconnected systems and cause severe damage. To address this problem, **[9]** presented an adaptive robust state estimator that utilizes graphics-processing units. The estimator uses a nonlinear extended Kalman filter, long short-term memory, and a deep learning method, collectively known as LSTMKF. The estimator is integrated with an SDIoT controller to enable online parametric state estimation, with two levels of assessment for load management and secure communication. The suggested technique is deployed to a 6G and SDIoT-enabled smart grid and evaluated on IEEE 14, 30, and 118 bus systems. The outputs indicate that the LSTMKF method can be used to evaluate the state variables of the structure even during or after a cyberattack with high accuracy and decreased time complexity, beating existing ways.

[10] Presented different deep learning generation techniques and how well they performed at finding abnormalities in cyber-physical systems (CPSs). The performance is evaluated using the criteria of accuracy, precision, recall, and F1-value. [11] Developed an effective multi-level network detection approach to improve the understanding of network intrusions. The proposed approach involves identifying hidden patterns in network traffic data to accurately detect network abnormalities, developing a predictive model to determine the type of attacks with precision, and integrating a visual analytics tool to facilitate interactive visual analysis and provide transparent explanations for the detected intrusions. The proposed approach is expected to develop the intrusion detection accuracy by uniting the advantages of machine learning and visual analytics. The proposed predictive model has demonstrated a high level of accuracy in identifying the exact categories of network attacks. Based on the experimental results, the model achieved an accuracy rate of approximately 96%, which indicates its effectiveness in detecting and classifying network intrusions.

3. Proposed Network Intrusion Detection Model

The AI-NIDM proposed intrusion detection model is based on Gray Wolf Algorithm and Artificial Neural Network (GWA-ANN). The working process of the proposed model is represented in Figure 2 and explained further.

Dataset for training (CICIDS2017):

The intrusion detection system's input source is the CICIDS2017 dataset. It comprises tagged data, which entails that each data point is connected to the appropriate class (such as typical traffic or certain kinds of attacks). The intrusion detection model will be trained on this dataset, and it will also be evaluated.

Data for Training and Testing:

The input dataset is divided into two categories: data for training and data for testing. The intrusion detection model is trained using training data, and its performance is assessed using testing data. This difference makes it simpler to assess how well the model generalizes to new, untested data.

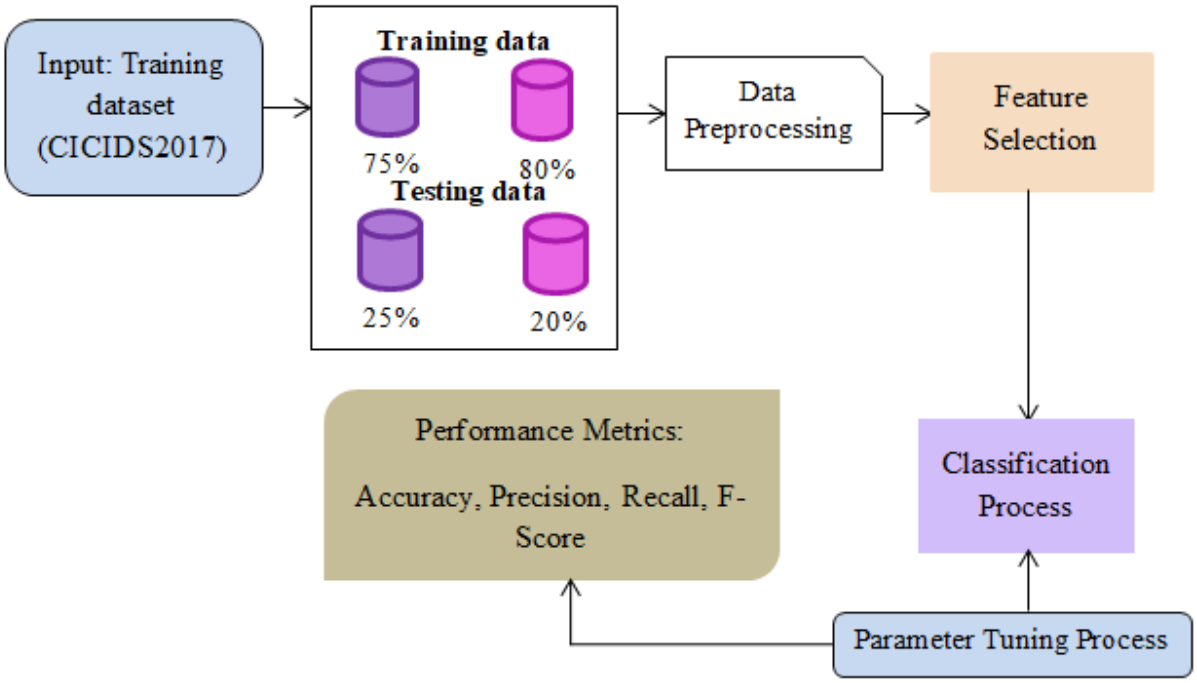

Fig 2. Proposed Model

Preprocessing of Data:

The system model's first phase is preprocessing of data. In order to get the raw data ready for further analysis, cleaning and preparation are needed. The handling of missing values, the elimination of noise, the normalization of data, and the resolution of any other data quality issues are typical preprocessing tasks.

$$min - max.Nor = \frac{d - d_{min}}{d_{max} - d_{min}} \qquad (1)$$

The objective is to equalize the sample into a normalized range between 0 and 1, as shown in equation (1).

Feature Selection:

The method of feature selection involves choosing pertinent features (characteristics) from the preprocessed data. According to the diagram, this stage comes after data preprocessing. In order to increase the efficiency and precision of the intrusion detection model, it is important to ease the dimensionality of the dataset and choose the best informative features [12].

Process of Classification:

The data that was chosen based on features is then put through the classification process. The basic function of an intrusion detection system is classification, which involves analyzing network traffic data and categorizing each data point into one of several classes, such as legitimate or malicious (anomalous) information.

Parameter Tuning Process:

AI models are frequently used in the classification process. To get optimal performance, several parameters of these models must be adjusted. Finding the ideal set of hyperparameters for the selected classification algorithm is the goal of the parameter tuning procedure.

Performance metrics:

The classification model is assessed using performance metrics after it has been trained and tweaked. The diagram includes the following popular performance indicators: Accuracy, Precision, Recall, F-Score.

3.1 Gray Wolf Algorithm

Since the exact optimal solution's position is unknown, the vector X_p is influenced by the three most promising solutions. The update equations for each individual agent (wolf) are as outlined below:

$$\vec{S_\alpha} = \left|\vec{C_1}.\vec{I_\alpha} - \vec{I}\right|, \vec{S_\beta} = \left|\vec{C_2}.\vec{I_\beta} - \vec{I}\right|, \vec{S_\delta} = \left|\vec{C_3}.\vec{I_\delta} - \vec{I}\right| \qquad (2)$$

$$\vec{I_1} = \vec{I_a} - \vec{A_1}. , \vec{I_2} = \vec{I_\beta} - \vec{A_2}. , \vec{I_3} = \vec{I_\delta} - \vec{A_3} \qquad (3)$$

$$\vec{I}(t+1) = \frac{\overrightarrow{I_1+I_2+I_3}}{3} \qquad (4)$$

In the given context, $\vec{I}$ represents the agent's current location, and $\vec{I}$ (t+1) indicates its revised position in the following iteration. According to the supplied equation, the agent's position will be modified based on the top three

performing agents from the previous iteration. It is crucial to note that the updated location will not be an exact average of these three top agents; rather, a tiny random displacement is introduced due to the influence of the vector $\vec{C}$.

Algorithm 1: Gray Wolf Optimization Algorithm

Begin by initializing a population of grey wolves represented by search agents, denoted as I_i where i ranges from 1 to n.

Set initial values for parameters a, A, and C.

Evaluate the fitness of each search agent based on their respective positions in the search space.

Identify the best, second-best, and third-best search agents as I_α, I_β, and I_δ respectively.

While t < max number of iteration do

For each search agent, perform the following steps:

Randomly generate values r1 and r2.

Utilize an equation (4) to update the position of the current search agent.

Update the values of parameters a, A, and C.

Calculate the fitness of all search agents based on their updated positions.

Update the best I_α, I_β and I_δ search agents.

Increment the iteration count by 1, setting T to t+1.

Continue looping until the maximum number of iterations is reached.

Conclude the process and return the position of the best search agent, I_α.

3.2 Artificial Neural Network

The ANN classification approach includes training and testing steps. The following is how the input weight summation was determined:

$$S_l = \sum_{i=1}^{n} I_i \partial_{il} + \rho_l \qquad (5)$$

I_i- Input variable

l- latent node

i - Input node

∂_{il}- the linkage weight

ρ_l- latent node bias

4. Results Analysis

In order to distinguish between routine occurrences and significant events in energy systems, the GWA-ANN approach requires training an Artificial Neural Network (ANN). The GWA (Grey Wolf Algorithm) is employed in this technique to optimize the neural network. Each search agent is initially optimized to improve a candidate neural network that consists of weight and bias vectors. In a Multi-Layer Perceptron (MLP) network, these vectors indicate the connections between the input and hidden layers as well as between the hidden and output layers [13].

Equation 6 reveals the bias and weight parameters in Multi-Layer Perceptron (MLP) networks that will be tuned using the GWA (Grey Wolf Algorithm). 'm' stands for the total number of input nodes, while 'n' stands for the total number of neurons in the hidden layer.

$$V = mn + 2m + 1 \qquad (6)$$

The GWA-ANN method has an advantage over local optimum avoidance. This approach makes it simpler to find the best MLP's bias and weight values, improving the suggested model's accuracy and overall performance. The below performance measures are used in this research to evaluate the proposed model performance result.

Accuracy: Evaluate the model's predictions' overall accuracy.

$$Accuracy\ (\%) = \frac{TP + TN}{TP + FP + TN + FN} \qquad (7)$$

Precision: Calculates the percentage of accurate positive predictions among all positive forecasts.

$$Precision\ (P) = \frac{TP}{TP + FP} \qquad (8)$$

Recall: calculates the percentage of accurate forecasts among all instances of actual success.

$$Recall = \frac{TP}{TP + FN} \qquad (9)$$

F-Score: represents the harmonic mean of recall and precision and offers a balanced evaluation of the performance of the model.

$$F - Score = \frac{2\ (Precision\ X\ Recall)}{(Precision + Recall)} \qquad (10)$$

Where, TP represent True Positive, TN represent True Negative, FP is False Positive and FN is False Negative.

The overall performance comparison of the proposed artificial intelligence based algorithm with the existing intrusion detection framework is denoted in Table 1. The highest accuracy, precision, recall and F-score rate among the five datasets is tabulated below.

Table 1. Overall Performance Comparison

Methods	Accuracy	Precision	Recall	F-Score
SVM	97.24	96.96	96.81	97.65
KNN	96.64	96.58	97.39	98.11
Proposed GWA-ANN	98.96	98.50	98.47	98.91

Several common metrics, such as F score, recall, precision, and accuracy, are used to evaluate the effectiveness of the suggested GWA-ANN technique. The outcomes of the experiments show how effective the approach is in spotting crucial events in electrical systems. The robust ability of the GWA-ANN to seek and avoid local optima beats that of other classification techniques like SVM and KNN.

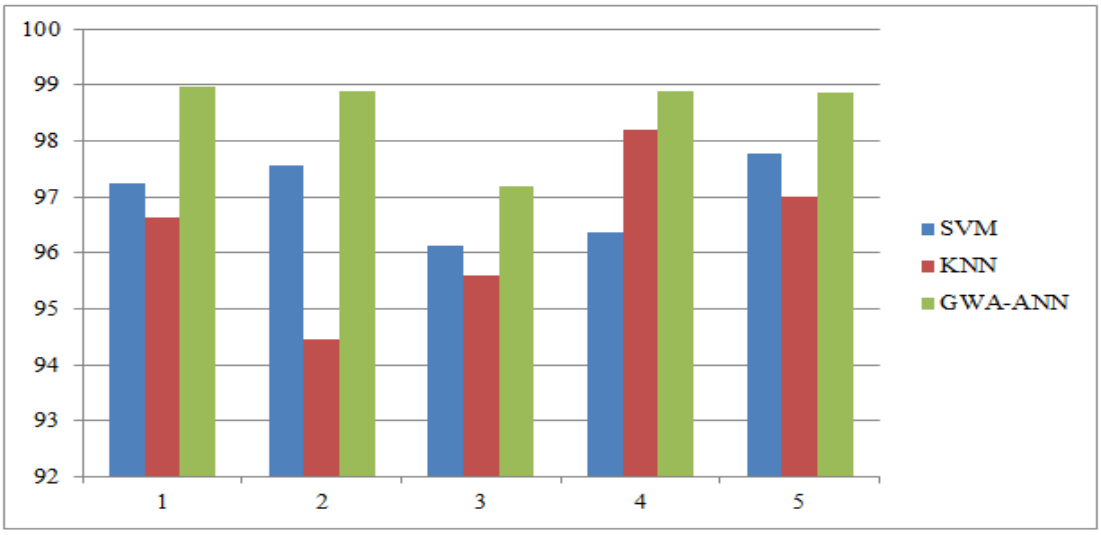

Fig 3. Accuracy Comparison

Figure 3 depicts a detailed overview of accuracy comparisons using the first five datasets. The results clearly demonstrate the proposed GWA-ANN artificial intelligence-based network intrusion detection system's superior performance. The GWA-ANN system outperforms the "Support Vector Machine (SVM)" and "K-Nearest Neighbor (KNN)" algorithms in terms of accuracy [14]. This demonstrates the innovative system's efficacy and potential for improving network security through efficient and precise intrusion detection.

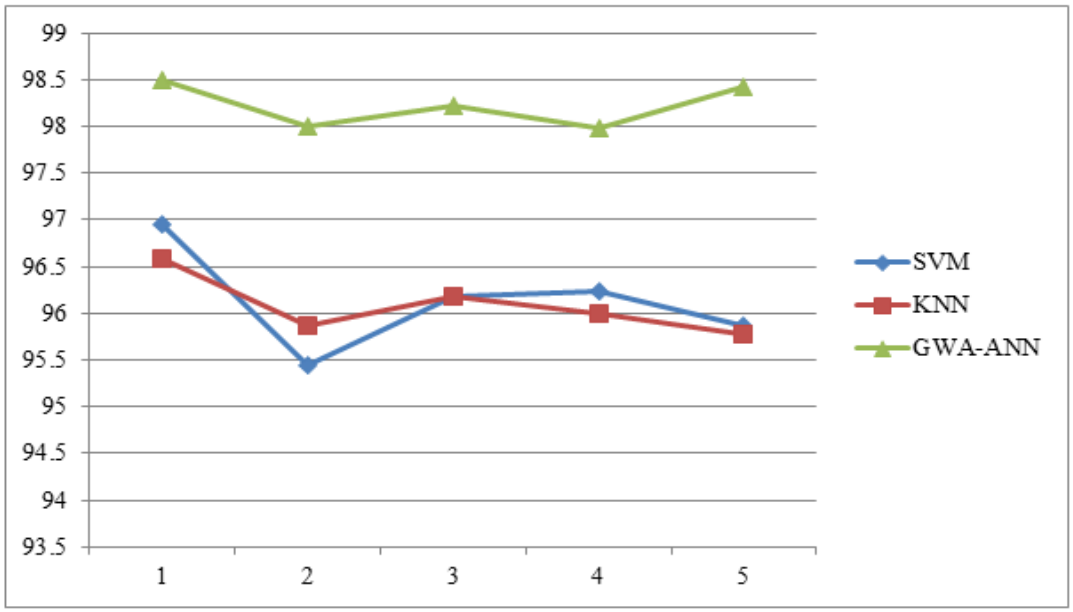

Fig 4. Precision Comparison

Figure 4 depicts a comprehensive comparison of precision rates utilizing the first five data points. The data clearly highlight the GWA-ANN artificial intelligence-driven network intrusion detection system's remarkable

capabilities. Notably, GWA-ANN outperforms the SVM and KNN algorithms in terms of precision rate. This enhances the system's ability to precisely detect and categorize unwanted intrusions, highlighting its potential for bolstering cybersecurity safeguards.

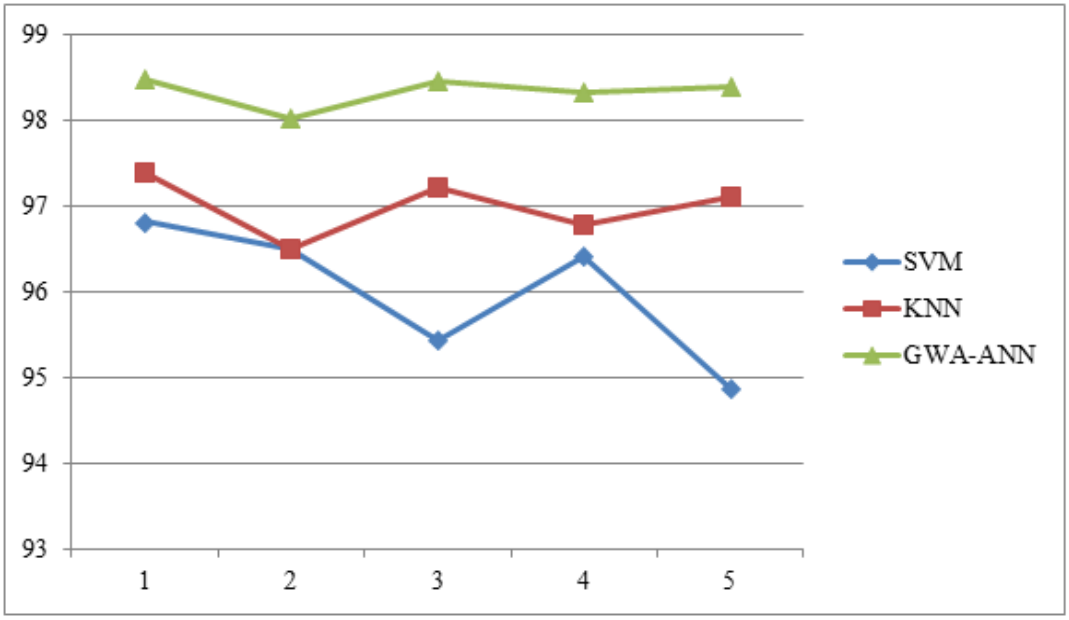

Fig 5. Recall Comparison

Figure 5 compares the GWA-ANN artificial intelligence-based network intrusion detection system to classical SVM and KNN algorithms in terms of recall rate. Notably, GWA-ANN has the highest recall rate, indicating its greater capacity to detect network intrusions. A critical parameter is recall, which assesses the system's accuracy in detecting genuine positives. The significant recall gap highlights GWA-ANN's superiority to SVM and KNN in reducing false negatives and improving overall system reliability. This finding demonstrates GWA-ANN's ability to dramatically increase network security measures, proving its worth as an innovative AI-driven intrusion detection solution.

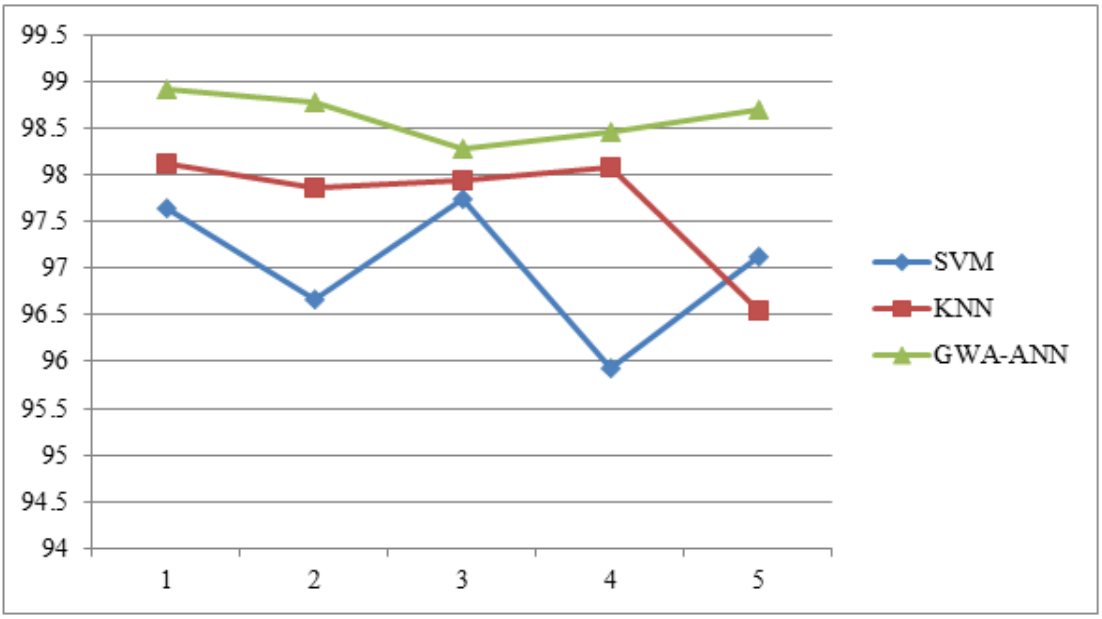

Fig 6. F-Score Comparison

Figure 6 depicts a complete F-Score comparison comparing the performance of the advanced artificial intelligence-driven network intrusion detection system, GWA-ANN, to the existing SVM and KNN algorithms. The findings highlight GWA-ANN's superiority in detecting and characterizing network intrusions.

The F-Score, a critical indicator that balances precision and recall, provides a comprehensive assessment of a system's capacity to reliably identify positive situations while avoiding false positives. The graph clearly shows that GWA-ANN outperforms SVM and KNN in terms of F-Score, demonstrating its ability to achieve a balanced trade-off between precision and recall.

5. Conclusion

In conclusion, the Artificial Intelligence Enabled Network Intrusion Detection Model (AI-NIDM) called GWA-ANN is an effective solution to enhance the security and resilience of Smart Grid Cyber-Physical Systems (CPS). Smart grids are complex systems that integrate advanced communication and control technologies, making them vulnerable to cyber-attacks that can cause significant economic loss and pose a threat to public safety. AI-NIDM utilizes advanced machine learning algorithms and techniques to analyze network traffic patterns and identify potential anomalies and cyber-attacks in real time. By doing so, it can detect and respond to various types of cyber-attacks, malware, and intrusion attempts. Moreover, AI-NIDM has the potential to improve the overall performance of Smart Grid CPS by reducing false positives and improving detection accuracy. As Smart Grid CPS continues to grow in complexity and scale, the implementation of AI-NIDM will become increasingly important for ensuring the security and resilience of these critical infrastructure systems.

References

[1] Jha, A. V., Appasani, B., Ghazali, A. N., Pattanayak, P., Gurjar, D. S., Kabalci, E., & Mohanta, D. K. (2021). Smart grid cyber-physical systems: communication technologies, standards and challenges. *Wireless Networks*, *27*, 2595-2613.

[2] Liu, Y., Yang, X., Wen, W., & Xia, M. (2021). Smarter grid in the 5G Era: a framework integrating power internet of things with a cyber-physical system. *Frontiers in Communications and Networks*, *2*, 689590.

[3] Vijayanand, R., Devaraj, D., & Kannapiran, B. (2019, April). A novel deep learning based intrusion detection system for smart meter communication network. In *2019 IEEE International Conference on Intelligent Techniques in Control, Optimization and Signal Processing (INCOS)* (pp. 1-3). IEEE.

[4] Reza, S. S., Mahbub, T. N., Islam, M. M., Arifeen, M. M., Remu, S. R. H., & Hossain, D. A. (2019, November). Assuring Cyber Security in Smart Grid Networks by Fuzzy-logic based Trust Management Model. In *2019 IEEE International Conference on Robotics, Automation, Artificial-intelligence and Internet-of-Things (RAAICON)* (pp. 1-4). IEEE.

[5] Sahani, N., Zhu, R., Cho, J. H., & Liu, C. C. (2023). Machine Learning-based Intrusion Detection for Smart Grid Computing: A Survey. *ACM Transactions on Cyber-Physical Systems*.

[6] Alohali, M. A., Al-Wesabi, F. N., Hilal, A. M., Goel, S., Gupta, D., & Khanna, A. (2022). Artificial intelligence enabled intrusion detection systems for cognitive cyber-physical systems in industry 4.0 environment. *Cognitive Neurodynamics*, *16*(5), 1045-1057.

[7] Li, B., Lu, R., & Xiao, G. (2020). *Detection of False Data Injection Attacks in Smart Grid Cyber-Physical Systems*. Springer Nature.

[8] Colelli, R., Magri, F., Panzieri, S., & Pascucci, F. (2021, June). Anomaly-based intrusion detection system for cyber-physical system security. In *2021 29th Mediterranean Conference on Control and Automation (MED)* (pp. 428-434). IEEE.

[9] Tariq, M., Ali, M., Naeem, F., & Poor, H. V. (2020). Vulnerability assessment of 6G-enabled smart grid cyber–physical systems. *IEEE internet of things journal*, *8*(7), 5468-5475.

[10] Yadav, S., & Kalpana, R. (2021). A Survey on Network Intrusion Detection Using Deep Generative Networks for Cyber-Physical Systems. *Artificial Intelligence Paradigms for Smart Cyber-Physical Systems*, 137-159.

[11] Ji, S. Y., Jeong, B. K., Choi, S., & Jeong, D. H. (2016). A multi-level intrusion detection method for abnormal network behaviors. *Journal of Network and Computer Applications*, *62*, 9-17.

[12] Manikanthan, S.V., Padmapriya, T., Hussain, A., Thamizharasi, E., Artificial Intelligence Techniques for Enhancing Smartphone Application Development on Mobile Computing, 2020, 14(17), pp. 4-19.

[13] Kasongo, S. M., & Sun, Y. (2020). Performance analysis of intrusion detection systems using a feature selection method on the UNSW-NB15 dataset. *Journal of Big Data*, *7*, 1-20.

[14] Qiao, W., Khishe, M., & Ravakhah, S. (2021). Underwater targets classification using local wavelet acoustic pattern and Multi-Layer Perceptron neural network optimized by modified Whale Optimization Algorithm. *Ocean Engineering*, *219*, 108415.

[15] Jackson, B., Lewis, M., Herrera, J., Fernández, M., & González, A. Machine Learning Applications for Performance Evaluation in Engineering Management. Kuwait Journal of Machine Learning, 1(2). Retrieved from http://kuwaitjournals.com/index.php/kjml/article/view/126

[16] Kumar M, G. ., & Goswami, A. D. . (2023). Deep Convolutional Neural Network Classifier for Effective Knee Osteoarthritis Classification . International Journal on Recent and Innovation Trends in Computing and Communication, 11(3), 242–249. https://doi.org/10.17762/ijritcc.v11i3.6343

[17] Sharma, R., & Dhabliya, D. (2019). A review of automatic irrigation system through IoT. International Journal of Control and Automation, 12(6 Special Issue), 24-29. Retrieved from www.scopus.com