International Journal of System Design and Computing (IJSDC)
Volume 02, Issue 02, July - December (2024)

RESEARCH ARTICLE

HYBRID NEURAL SYSTEM FOR CYBER-ATTACK DETECTION IN LARGE-SCALE SMART GRIDS

R.A. Mabel Rose [1, *] and V. Padmajothi [2]

[1] Department of Computer Science and Business Systems, Panimalar Engineering College, An Autonomous Institution, Affiliated to Anna University, Chennai, Bangalore Trank Road, India.

[2] Department of Electronics and Communication Engineering, SRM Institute of Science and Technology (SRMIST), Kattankulathur, Tamil Nadu 603203, India.

[*]*Corresponding e-mail: mabel.nidhu@gmail.com*

Abstract – The advancements in the distributed energy system and digital technology in the smart grid system increase efficiency, stability, and reliability. However, it increases the vulnerabilities in the grid network. The falsely injected data in the grid network leads to failures in energy production, and consumption. Hence, an Ant Lion-based Modular Neural network (ALbMNN) model was proposed to detect the normal and malicious data. The presented model integrates the ant lion fitness and MNN attribute to detect the falsely injected data in the grid system. The dataset was initialized and pre-processed using the divide-and-conquer principle of MNN. The optimal ant lion fitness solution helps in selecting features optimally from the dataset. Finally, the presented model was assessed with a large-scale smart grid dataset, and the results are estimated. Moreover, a comparative analysis was performed to verify the performance of the developed scheme. Based on performance and comparative analysis, the suggeated model performed better than other existing methods.

Keywords *– False Data Injection, Cyber-attack detection, Smart grids, Modular Neural Network, Ant Lion Optimization.*

1. INTRODUCTION

The power system consists of a grid of generators and sensors that permits two-way communication through the incorporation of Distributed Energy Resources [1]. This advanced power system has numerous advantages including increased energy reliability, efficiency, and network stability [2]. However, it increases the possibility of cyber-attack on the network due to a high number of associated network devices [3]. The cyber-attack in the smart grid leads to damage to components and causes false demand requests. The false demand request leads to increased energy production, and wastage [4]. In addition, it enables the power system to provide stable energy flow, and reliable performance [5]. Therefore, a continuous monitoring system must be designed to detect/ identify malicious events in the smart grid system [6]. Generally, in a large-scale smart grid system, individual sensors are the major target of security concessions [7]. To avoid false demand requests and cyber-attack in the grid system, advanced technology is developed. Initially, cryptography-based authentication techniques are developed to track and eliminate cyber-attacks [8]. But it does not apply to large-scale smart grids because of its high resource usage, and computational time [9]. The advanced malicious event detection approaches employ state estimation methodology to estimate cyber-attacks efficiently [10]. However, these techniques are mathematically expensive, and not scalable to large-scale grid networks. Moreover, the advancement in the grid network demands a real-time attack supervising system [11].

The conventional intrusion detection scheme cannot access the data from large-scale grid networks [12]. Exploring this huge collected data requires machine learning (ML) and deep learning (DL) methods to process the complex data structure for identifying the false demand request [13]. The cyber-attack detection mechanism identifies the malicious event by learning the complex data structure pattern through non-linear ML [14]. In recent times, studies based on ML-based cyber security are increasing day by day [15]. This scheme deploys a feature selection mechanism to test the dataset attributes. Different machine models like random forest algorithm, decision tree algorithm [16], gradient boost algorithm [17], etc., are applied to handle the complex data. This method maintains scalability and robustness of attack detection by processing high-dimensional data in this way [18].

However, the learning process requires high resource usage and increases the computational burden [19]. The performance comparison of ML and DL-based intrusion detection mechanism shows that the DL-based techniques reduce the computational burden and increases the accuracy in cyber-attack detection [20]. Thus, various DL algorithms like distributed data-driven intrusion detection schemes [21], real-time-based false data injection (FDI) attack detection [22], extremely randomized tree approach [23], deep

learning-based detection methods [24], etc., are developed to detect a malicious event in the smart grid system. However,

they face issues with implementation costs and data processing. Hence, an optimized DL-based cyber-attack detection approach was developed in this article.

The main contribution of the proposed research is described as follows,

- Smart grid datasets were collected from standard sites and imported into the system.
- Develop the optimized neural system (ALbMNN) to detect the falsely injected data.
- Initially, the dataset is pre-processed and then the features are selected to detect malicious events.
- The anti-Lion fitness solution in the proposed model effectively selects the features and increases the system's performance.
- Furthermore, the performance of the proposed model is determined and evaluated in terms of accuracy, true positive rate, and false positive rate.

The presented article is sequenced as follows, the works related to the cyber-detection in smart grid is described in 2nd section, the problems in the existing techniques are illustrated in 3rd section, the proposed model is explained with a flowchart and algorithm in 4th section, the results of the developed model is detailed in 5th section, and the conclusion of the article is mentioned in 6th section.

2. RELATED WORKS

Following are some recent articles about cyber-attack detection in smart grid systems:

Jiayu Shi et al. [21] suggested a distributed data-driven intrusion detection scheme to identify the malicious event/FDI in the smart grids. Moreover, it helps in preventing the over-fitting issue which usually occurs in ML algorithms. Further, the developed model is simulated and verified with other conventional models. Although this model reduces the overfitting issue and estimates the malicious event precisely, it is highly expensive and requires more resources.

However, the FDI attack has become a serious threat to the state estimation approach Injecting malicious data into real-time data affects system performance. Thus, Debottam Mukherjee et al. [22] presented a real-time-based FDI attack detection model to ensure security in the grid system. The performance of this algorithm shows that it processes real-time data with minimum error. This provides highly accurate intrusion detection with less error using the error covariance matrix. However, the computational burden is high in this model.

However, the incorporation of digital communication techniques leads to vulnerabilities in the smart grid system. Hence, Seyed HosseinMajidi et al. [23] designed an approach to detect the FDI attack optimally. Further, the results obtained by this model are compared with traditional algorithms like support vector machine (SVM), Decision tree, random forest, k-nearest neighbor (KNN), etc., to verify the system performance. However, the system size and computational complexity are high in this model.

At the same time, the vulnerabilities are increasing because of the increased number of devices. Yucheng Ding et al. [24] reported a DL-based detection method to investigate information corruption. This conditional-based DL scheme analyzes and trains the huge input dataset to predict malicious events accurately. The developed scheme is validated using the IEEE standard test system. But the designed model reduces the reliability performance of the grid system.

The fully developed distributed and automated electricity grid system growths the possibility of cyber-attacks. The cyber-attacks increase the false demand request leading to the wastage of energy in smart grids. Moreover, the growth of cyber threats reduces grid reliability performances by injecting false data into it. Therefore, SudhakarSengan et al. [25] present the combination of true data integrity in the physical layers. This feedback-based network improves the FDI attack detection rate. Although the developed model earned 98.19% accuracy, the data processing consumes more time and size.

The data acquisition and supervisory control mechanism in the grid system enables the hacker to inject bas-data. This leads to huge energy and financial losses in the grid network. To overcome these cyber threats, Mario R. Camana Acosta et al. [26] suggested an effective intrusion detection model based on kernel and randomized tree principles. This technique reduces the component size, and system complexity. Additionally, for verification purposes, the outcomes are contrasted with the most advanced methods. However, it is not resistant to other types of attacks related to smart grids.

The power sector is rising as the major energy source across the world. The increasing energy demand and wide usage of network-connected devices pave the way for security threats. The security threats in the grid system cause corruption in power transmission, false demand requests, and energy wastage. To prevent these challenges, Yangyang Tian et al. [27] presented a hybrid model based on a different machine and DL schemes. This method uses a CNN and SVM techniques for classifying malicious attacks. This intrusion detection algorithm effectively reduces the over-fitting issue and identifies the damage in transmission and production lines in smart grids. The effectiveness of this model is validated with a comparative performance. However, the detection accuracy is low in this model.

ChunheSong et al. [28] suggested a feature selection-based DL model detect anomalous events. This combines the

attributes of LSTM and extreme gradient boosting topology to identify the dataset pattern. This model not only identifies the anomalous events but also prevents the false data injection attack by matching the dataset pattern. In addition, the detection accuracy of the developed model is estimated in two different ways. Hence, the system is more scalable and reliable. Moreover, Bayesian optimization is utilized to optimize the sensitive grid parameters. The integration of optimization reduces the effect of over-fitting and increases the system's efficiency. But this method does not apply to a large-scale smart grid system.

Ying Zhang et al. [29] suggested a auto-encoder-based intrusion detection scheme. In power systems, the FDI attack reduces the stability and scalability performance. This data-driven DL-based detection algorithm recognizes unobservable FDI attacks by identifying unconformity between abnormal and secure measurements. In addition, a GAN framework was deployed to capture the malicious data and neglect it. The efficiency of the developed scheme is determined by numerically simulating it in the unbalanced IEEE 123-bus and 13-bus systems. However, it does not identify the attacks other than FDI.

3. SYSTEM MODEL

The smart grid technology is electricity network which utilizes the advanced digital technologies to control and monitor the electricity transportation from all production sources to meet the energy demand. The false injected data reduces the grid performances like reliability, efficiency, and energy production. The present cyber-detection systems face challenges in detecting the all types of cyber-attacks accurately. Moreover, they require large resources to train and implement it. Developing easy and accurate cyber-attack detection mechanism is still a challenging factor in the smart grid system. Designing of cyber-attack detection model must incorporate an intelligent model with optimization technique to predict the falsely injected data effectively at cheap cost. Therefore, to overcome the challenges in the traditional system an optimized neural-based cyber-detection model was developed in this article.

4. PROPOSED ALBMNN FRAMEWORK FOR ANOMALY DETECTION

A novel hybrid Ant-Lion-based Modular Neural Network (MNN) was proposed in the particle to identify the malicious events in the large-scale smart grid. First, a sizable dataset on smart grids was collected from the standard website (Kaggle) and added to the system. Then the hybrid cyber-attack detection model was developed with the attributes of the ant-lion optimization (ALO) algorithm, and the MNN. Further, the initialized dataset is trained and pre-processed to eliminate the errors data or null values using the MNN features.

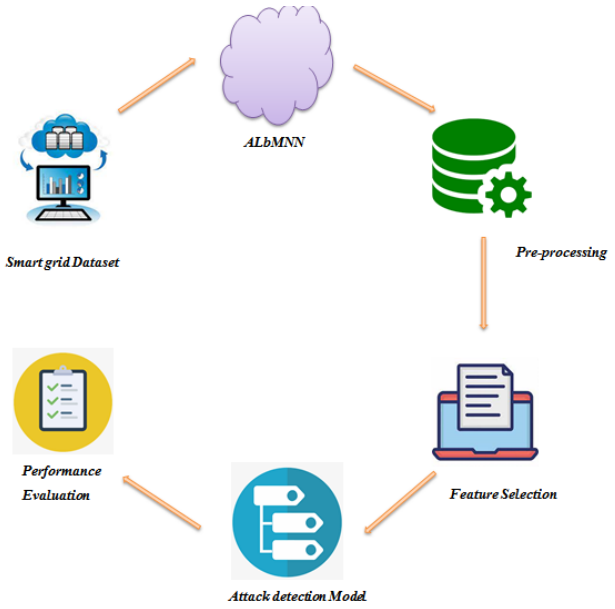

Figure 1. ALbMNN Framework

The ant-lion fitness function is used in the classification layer to choose features from the dataset. The features of the extracted data are then classified as either benign or harmful. For validation reasons, the performance of the model that is being given is also estimated and contrasted with a few conventional approaches. Fig. 1 shows the proposed methodology.

4.1. ALbMNN Layers

The input layer, hidden layer and output layer are the three layers that make up the developed ALbMNN model. The input dataset is set up and trained in the system in the input layer. Hidden Layer 1, hidden layer 2, and hidden layer 3 are the three partitions of the hidden layer. To remove incorrect data and null values, the input dataset is pre-processed and filtered in hidden layer 1.

In hidden layer 2, the dataset features are extracted using the MNN features and in hidden layer 3, the extracted features are classified as benign or malicious. The results of the model are calculated and contrasted with traditional schemes in the last layer. The layers of the suggested model are illustrated in Fig 2.

4.1.1. Data Pre-processing

The dataset contains the attributes like energy production rate, reaction time, grid stability factor, energy consumption rate, etc. To start the prediction process, the collected dataset was trained and initialized in the system. The initialization function is represented in Eqn. (1).

$$f_{in}(S_{GD}) = \{Dt_1, Dt_2, Dt_3, Dt_4, \ldots . Dt_k\} \quad (1)$$

Here, f_{in} refers to the dataset initialization function, S_{GD} denotes the large-scale smart grid dataset, f_{in} defines the data present in the dataset, and $k$indicates the total number of data

present in the dataset. pre-processing not only removes the errors but also makes the attack-detection process easy.

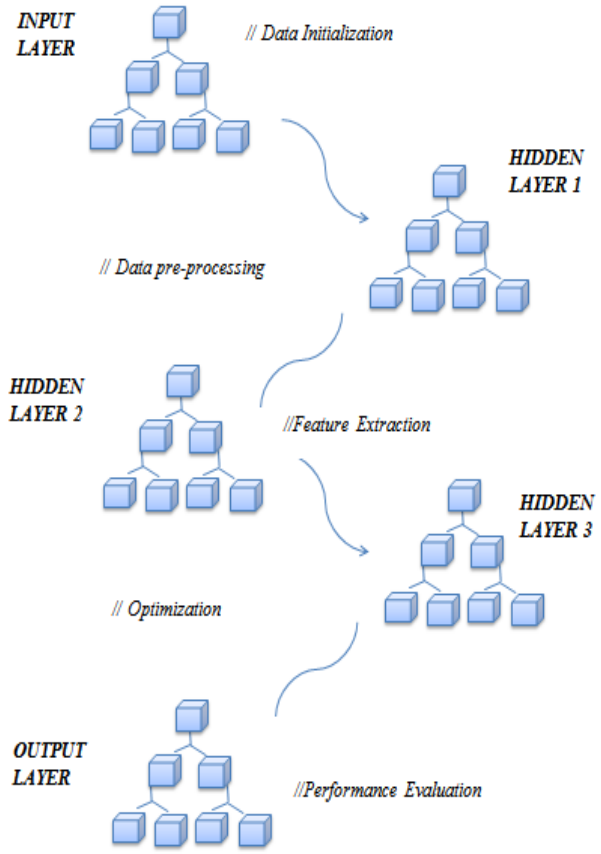

Figure 2. ALbMNN Layers

In the proposed model, the dataset was filtered using the attributes of the MNN algorithm. The key feature of the MNN algorithm is that it can process a huge dataset with less complexity. The data pre-processing function is expressed in Eqn. (2).

$$P_r^*(S_{GD}) = \sigma \sum_{i=1}^{k} (Dt_i - \delta Dt_i) \quad (2)$$

Where P_r^*represents the pre-processing function, σ indicates the pre-processing variable, andδDt_i denotes the error or null values.

4.1.2. Feature Extraction

Feature extraction is the process of selecting the important features from the pre-processed image. Both significant and insignificant structures can be found in the pre-processed dataset. But for attack detection, only meaningful features are considered. Therefore, in this stage, the pre-processed dataset's important features are retrieved, and its nonsensical features are eliminated. To extract the features, an ant-lion fitness solution is applied in the proposed model. An ALO is an algorithm based on the hunting nature of the ant lions. It involves five hunting steps namely: agent's random walk, entrapments of ants in traps, building traps, rebuilding traps, and catching prey. The ant lion fitness function is expressed in Eqn. (3).

$$F_{er}^{'}(S_{GD}) = Al_f + \frac{S_{GD} \times (Dt)}{\nu(nDt, mDt)} = ef \quad (3)$$

Where, $F_{er}^{'}$indicates the feature extraction function, Al_frepresents the ant lion fitness, nDtrefers to the normal data, mDtdenotes the malicious data, efspecifies the extracted features, and νdefines the feature tracking variable. The extracted features are further compared with the trained normal features for classification purposes.

4.1.3. Cyber-attack detection

After feature extraction, the next step is false data classification. The extracted features contain both malicious and normal data. The classification is carried out to categorize the normal and malicious data separately. The attack classification is represented in Eqn. (4).

$$A_{cl} = \begin{cases} if\left(ef = T_{nf}\right); Normal \\ if\left(ef \neq T_{nf}\right); FalseData \end{cases} \quad (4)$$

Here, A_{cl}refers to the attack classification function, and T_{nf}indicates the trained normal features. If the extracted features match with the trained normal features, it is classified as “Normal Data”. If the extracted feature does not match the trained features, it is classified as "Malicious data". Thus, the presented model detects and classifies the data as normal or malicious. Algorithm 1 provides an example of how the presented model operates.

Algorithm 1: ***Cyber-attack detection model***

Step 1: *Initialize the input smart grid dataset* S_{GD}

Step 2: *Develop the proposed model with the AOA and MNN features*

Step 3: *Pre-process the dataset to eliminate the errors*

$$P_r^* \Rightarrow \sigma(Dt_i - \delta Dt_i)$$

Step 4: *Extract the features from the dataset for classification*

$$F_{er}^{'} = Al_f + \nu(nDt, mDt) = ef$$

Step 5: *Classification of data as “Injected” or Normal*

Step 6: *Evaluate the system performance*

Step 7: *Terminate the process*

The flowchart of the developed model is displayed in Fig 3. Initially, the dataset was filtered and pre-processed to eliminate errors. Then the optimal features are extracted using the ant lion fitness function. Then the extracted data are classified as normal or malicious data by matching it with the trained normal features.

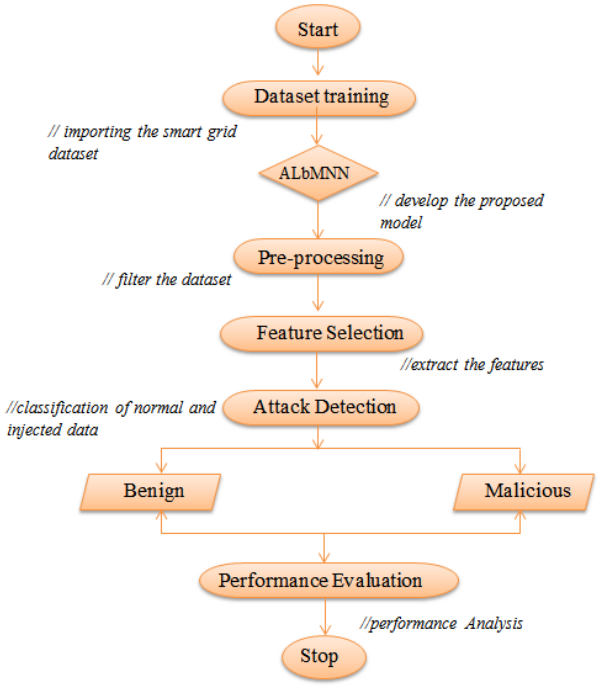

Figure 3. Flowchart of the suggested model

5. RESULTS AND DISCUSSION

A hybrid cyber-attack detection model was developed in this article to detect and classify normal and malicious data. The presented model was executed in the MATLAB software version R2020a running in windows 10. Initially, the dataset was initialized and filtered to eliminate unwanted features. Further, the features are extracted and classified as normal or false data.

Table 1. Parameters and specifications

Implementation Tools	
Parameters	**Specification**
Platform	MATLAB
Version	R2020a
OS	Windows 10
Datasets	Large-scale smart grid dataset
Application	Smart Grid

The integration of ant lion fitness in the hidden layer of the MNN offers better accuracy in detecting false data or attacks. Table 1 lists the implementation parameters and its specification.

5.1. Performance Analysis

In order to validate the suggested model, its performance is calculated and contrasted with a few traditional attack detection algorithms in this section. Performance parameters including accuracy, false positive rate and true positive rate are determined in this instance utilizing MATLAB software. Comparative analysis is conducted using the standard cyber-attack detection algorithms, such as Unsupervised ML Systems for Cyber-Attack Detection (UMLS_CD) [31], Extremely Randomized Trees-Based Schemes for Cyber-Attack Detection (ERTbS_CD) [32], Whale Optimization Algorithm-based Artificial Neural Network (WOA_ANN) [33], and Wavelet Convolutional Neural Network for Cyber Attack Detection (WCNN_CAD) [34].

5.1.1. Accuracy

The system accuracy defines the cyber-attack detection/ identification rate, i.e.) how precisely the system identifies the injected data in the smart grid. The accuracy of the presented model is formulated in Eqn. (5).

$$S_{AR} = \frac{\lambda^{+}+\lambda^{-}}{\lambda^{+}+\lambda^{-}+\alpha^{+}+\alpha^{-}} \quad (5)$$

Where, S_{AR} indicates the system accuracyλ^{+}, λ^{-} α^{+} and α^{-}denotes the true-positive, true-negative, false-positive, and false-negative, respectively.

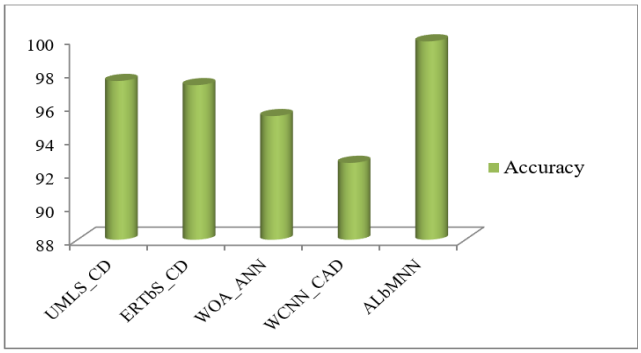

Figure 4. Comparison of Accuracy

Here, the accuracy in the existing models is calculated by executing it in the same platform for the same grid dataset. The accuracy that the existing approaches like UMLS_CD, ERTbS_CD, WOA_ANN, and WCNN_CAD attained accuracy of 97.5%, 97.25%, 95.4%, and 92.6%, respectively. Similarly, the accuracy earned by the developed model for detecting cyber-attack in large-scale datasets is 99.87%. The accuracy validation is illustrated in Fig 4.

5.1.2. True Positive Rate (TPR)

The entire positive prediction of the positive class divided by the correct prediction of malicious traits is known as the TPR. Another name for it is sensitivity. The true-positive value is divided by the true-positive and false-negative values to find it. The TPR of the system is formulated in Eqn. (6).

$$T_{PR} = \frac{\lambda^{+}}{\lambda^{+}+\alpha^{-}} \quad (6)$$

Here, T_{PR}indicates the system TPR.

The TPR percentage must be high for an effective intrusion detection mechanism. Hence, to manifest that the presented cyber-attack detection model attained higher TPR

it is compared with some existing algorithms. Here, the existing techniques like UMLS_CD, ERTbS_CD, WOA_ANN, and WCNN_CAD are implemented in the same execution platform for detecting false data injection in large-scale smart grid datasets. Following implementation, the aforementioned algorithm is used to determine the TPR from the confusion matrix.

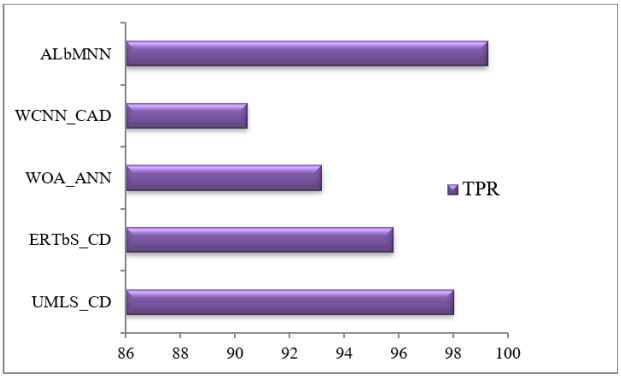

Figure 5. TPR validation

The TPR obtained by the existing algorithms is 98%, 95.8%, 93.18%, and 90.45%, respectively. However, from the comparative analysis, it is observed that the TPR achieved by the developed model is high i.e. 99.25%. The TPR comparison is shown in Fig 5.

5.1.3. False Positive Rate (FPR)

In FPR, the number of negative events is classified as a positive event. A false-positive value is definite as the ratio of false-positives to true-negatives. It is expressed in Eqn. (7).

$$F_{PR} = \frac{\alpha^{+}}{\lambda^{-}+\alpha^{+}} \tag{7}$$

WhereF_{PR} indicates the false-positive rate.

The comparison of FPR is displayed in Fig 6. FPR is one of the important parameters which determine the efficiency of the detection model.

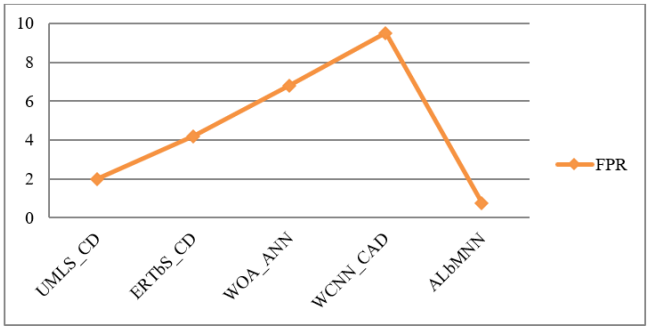

Figure 6. Comparison of FPR

The lower FPR represents the detection model correctly classifies the malicious and benign data in the dataset. Hence, the FPR of the intrusion detection model must be low. The proposed model's FPR is verified by contrasting it with the existing algorithms like UMLS_CD, ERTbS_CD, WOA_ANN, and WCNN_CAD. It is noticed that the existing techniques earned FPR of 2%, 4.2%, 6.8%, and 9.5%, respectively, whereas the proposed technique earned very FPR of 0.75%.

5.2. Discussion

An optimized neural-based intrusion detection model was presented in this paper to detect a malicious event in the smart grid system. The presented model was implemented and verified with a large-scale smart grid dataset.

Table 2. Comparative Assessment

Techniques	Accuracy (%)	TPR (%)	FPR (%)
UMLS_CD	97.5	98	2
ERTbS_CD	97.25	95.8	4.2
WOA_ANN	95.4	93.18	6.8
WCNN_CAD	92.6	90.45	9.5
ALbMNN	99.87	99.25	0.75

Finally, the outcomes of the established model were estimated and compared with different traditional schemes for validation purposes. Furthermore, the performance improvement score was determined from the comparative analysis. The overall comparative analysis was tabulated in Table 2.

6. CONCLUSION

The growth of intelligent technologies in the power grid system increases the possibility of vulnerabilities. Thus, detecting false data in smart grid systems requires an effective detection scheme. The presented detection model integrates the key features of ALO and MNN. The presented model performances are validated with a large-scale smart grid dataset. In the initial phase, the dataset was imported and trained into the system. Further, the dataset was pre-processed and the effective features are extracted to classify the normal and false data. Additionally, the parameter enhancement score was calculated by comparing the created scheme's results with those of existing methodologies. From the comparative performance of different techniques, it is observed that in the suggested model the accuracy was enhanced by 2.37%, the FPR is minimized by 1.25%, and TPR is increased by 1.25%. Thus, the developed detection scheme effectively detects and classifies the malicious data in the grid system.

CONFLICTS OF INTEREST

Not applicable.

FUNDING STATEMENT

Not applicable.

ACKNOWLEDGEMENTS

The supervisor's advice and continuous support during this research have been greatly appreciated by the author.

REFERENCES

[1] S. Ali, and Y. Li, "Learning multilevel auto-encoders for DDoS attack detection in smart grid network," *IEEE Access*, vol. 7, pp. 108647-108659, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[2] A. Sultana, A. Bardalai, and K. K. Sarma, "Salp swarm-artificial neural network based cyber-attack detection in smart grid," *Neural Processing Letters*, vol. 54, no. 4, pp. 2861-2883, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[3] S. Y. Diaba, M. Shafie-khah, and M. Elmusrati, "On the performance metrics for cyber-physical attack detection in smart grid," *Soft Computing*, vol. 26, no. 23, pp. 13109-13118, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[4] Ö. Sen, D. van der Velde, K. A. Wehrmeister, I. Hacker, M. Henze, and M. Andres, "On using contextual correlation to detect multi-stage cyber attacks in smart grids," *Sustainable Energy, Grids and Networks*, vol. 32, pp. 100821, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[5] T. Berghout, M. Benbouzid, and S. M. Muyeen, "Machine learning for cybersecurity in smart grids: A comprehensive review-based study on methods, solutions, and prospects," *International Journal of Critical Infrastructure Protection*, vol. 38, pp. 100547, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[6] J. Chen, A. J. Gallo, S. Yan, T. Parisini, and S. Y. R. Hui, "Cyber-attack detection and countermeasure for distributed electric springs for smart grid applications," *IEEE Access*, vol. 10, pp. 13182-13192, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[7] J. J. Yan, G. H. Yang, and Y. Wang, "Dynamic reduced-order observer-based detection of false data injection attacks with application to smart grid systems," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 10, pp. 6712-6722, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[8] Y. Li, X. Wei, Y. Li, Z. Dong, and M. Shahidehpour, "Detection of false data injection attacks in smart grid: A secure federated deep learning approach," *IEEE Transactions on Smart Grid*, vol. 13, no. 6, pp. 4862-4872, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[9] M. Abdel-Basset, N. Moustafa, and H. Hawash, "Privacy-preserved generative network for trustworthy anomaly detection in smart grids: A federated semisupervised approach," *IEEE transactions on industrial informatics*, vol. 19, no. 1, pp. 995-1005, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[10] R. Sharma, A. M. Joshi, C. Sahu, G. Sharma, K. T. Akindeji, and S. Sharma, "Semi supervised cyber attack detection system for smart grid," In *2022 30th Southern African Universities Power Engineering Conference (SAUPEC)*, pp. 1-5, 2022. IEEE. [CrossRef] [Google Scholar] [Publisher Link]

[11] P. K. Jena, S. Ghosh, and E. Koley, "Identification of strategic sensor locations for intrusion detection and classification in smart grid networks," *International Journal of Electrical Power & Energy Systems*, vol. 139, pp. 107970, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[12] A. N. Alkuwari, S. Al-Kuwari, and M. Qaraqe, "Anomaly detection in smart grids: a survey from cybersecurity perspective," In *2022 3rd International Conference on Smart Grid and Renewable Energy (SGRE)*, pp. 1-7, 2022. IEEE. [CrossRef] [Google Scholar] [Publisher Link]

[13] Y. Li, and J. Yan, "Cybersecurity of smart inverters in the smart grid: A survey," *IEEE Transactions on Power Electronics*, vol. 38, no. 2, pp. 2364-2383, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[14] O. Boyaci, M. R. Narimani, K. Davis, and E. Serpedin, "Cyberattack detection in large-scale smart grids using chebyshev graph convolutional networks," In *2022 9th International Conference on Electrical and Electronics Engineering (ICEEE)*, pp. 217-221, 2022. IEEE. [CrossRef] [Google Scholar] [Publisher Link]

[15] D. An, F. Zhang, Q. Yang, and C. Zhang, "Data integrity attack in dynamic state estimation of smart grid: Attack model and countermeasures," *IEEE Transactions on Automation Science and Engineering*, vol. 19, no. 3, pp. 1631-1644, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[16] S. Sharda, K. Sharma, and M. Singh, "False Data Injection and Detection in Smart Grid Cyber-Physical Systems by Iterative Load Flow Analysis," In *Advances in Information Communication Technology and Computing: Proceedings of AICTC 2021*, pp. 245-257, 2022, Singapore: Springer Nature Singapore. [CrossRef] [Google Scholar] [Publisher Link]

[17] Q. Li, J. Zhang, J. Zhao, J. Ye, W. Song, and F. Li, "Adaptive hierarchical cyber attack detection and localization in active distribution systems," *IEEE transactions on smart grid*, vol. 13, no. 3, pp. 2369-2380 2022. [CrossRef] [Google Scholar] [Publisher Link]

[18] T. Teng, and L. Ma, "Deep learning-based risk management of financial market in smart grid," *Computers and Electrical Engineering*, vol. 99, pp. 107844, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[19] Y. Liu, and L. Cheng, "Relentless false data injection attacks against Kalman-filter-based detection in smart grid," *IEEE Transactions on Control of Network Systems*, vol. 9, no. 3, pp.1238-1250, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[20] H. T. Reda, A. Anwar, A. Mahmood, and N. Chilamkurti, "Data-driven approach for state prediction and detection of false data injection attacks in smart grid," *Journal of Modern Power Systems and Clean Energy*, vol. 11, no. 2, pp. 455-467, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[21] J. Shi, S. Liu, B. Chen, and L. Yu, "Distributed data-driven intrusion detection for sparse stealthy FDI attacks in smart grids," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 68, no. 3, pp. 993-997, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[22] D. Mukherjee, S. Chakraborty, A. Y. Abdelaziz, and A. El-Shahat, "Deep learning-based identification of false data injection attacks on modern smart grids," *Energy Reports*, vol. 8, pp. 919-930, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[23] S. H. Majidi, S. Hadayeghparast, and H. Karimipour, "FDI attack detection using extra trees algorithm and deep learning algorithm-autoencoder in smart grid," *International Journal of Critical Infrastructure Protection*, vol. 37, pp. 100508, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[24] S. H. Majidi, S. Hadayeghparast, and H. Karimipour, "FDI attack detection using extra trees algorithm and deep learning algorithm-autoencoder in smart grid," *International Journal of Critical Infrastructure Protection*, vol. 37, pp. 100508, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[25] S. Sengan, V. Subramaniyaswamy, V. Indragandhi, P. Velayutham, and L. Ravi, "Detection of false data cyber-attacks for the assessment of security in smart grid using deep learning," *Computers & Electrical Engineering*, vol. 93, pp.107211, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[26] M. R. C. Acosta, S. Ahmed, C. E. Garcia, and I. Koo, "Extremely randomized trees-based scheme for stealthy cyber-attack detection in smart grid networks," *IEEE access*, vol. 8, pp.19921-19933, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[27] Y. Tian, Q. Wang, Z. Guo, H. Zhao, S. Khan, W. Mao, and J. Zhao, "A hybrid deep learning and ensemble learning mechanism for damaged power line detection in smart grids," *Soft Computing*, vol. 26, no. 20, pp.10553-10561, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[28] C. Song, Y. Sun, G. Han, and J. J. Rodrigues, "Intrusion detection based on hybrid classifiers for smart grid," *Computers & Electrical Engineering*, vol. 93, pp. 107212, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[29] Y. Zhang, J. Wang, and B. Chen, "Detecting false data injection attacks in smart grids: A semi-supervised deep learning approach," *IEEE Transactions on Smart Grid*, vol. 12, no. 1, pp. 623-634, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[30] L. Abualigah, and A. Diabat, "A novel hybrid antlion optimization algorithm for multi-objective task scheduling problems in cloud computing environments," *Cluster Computing*, vol. 24, no. 1, pp. 205-223, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[31] S. Varela-Santos, and P. Melin, "A new modular neural network approach with fuzzy response integration for lung disease classification based on multiple objective feature optimization in chest X-ray images," *Expert Systems with Applications*, vol. 168, pp. 114361, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[32] H. Karimipour, A. Dehghantanha, R. M. Parizi, K. K. R. Choo, and H. Leung, "A deep and scalable unsupervised machine learning system for cyber-attack detection in large-scale smart grids," *Ieee Access*, vol. 7, pp. 80778-80788, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[33] L. Haghnegahdar, and Y. Wang, "A whale optimization algorithm-trained artificial neural network for smart grid cyber intrusion detection," *Neural computing and applications*, vol. 32, no. 13, pp. 9427-9441, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[34] J. P. Li, G. U. Nneji, A. Z. Yutra, B. D. Lemessa, S. Nahar, E. C. James, and A. U. Haq, "The Capability of Wavelet Convolutional Neural Network for Detecting Cyber Attack of Distributed Denial of Service in Smart Grid," In *2021 18th International Computer Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP)*, pp. 413-418, 2021. IEEE. [CrossRef] [Google Scholar] [Publisher Link]

AUTHORS

R.A. Mabel Rose received her B.E. degree and M.E. degree in Computer Science and Engineering from Anna University, Chennai, India. She started her career as Lecturer and has 13 years of experience. Currently she is working as Assistant Professor in Panimalar Engineering College, Chennai. Her research interests include Cyber Security and Cloud Computing. She is a lifetime member of ISTE.

V. Padmajothi Obtained Ph.D. at Veltech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology in the year 2023, M.E. (Applied Electronics) in Arulmigu Meenakshi Ammal College of Engineering (ANNA University) in the year 2005, Obtained B.E. (EEE) in Adhiparasakthi College of Engineering (Madras University). Currently working as Assistant professor in SRM Institute of Science and Technology, Kattankulathur, Chennai from the year 2005. Having 19 years of teaching experience and teaching various courses such as Embedded Linux, Hardware Interfacing and Networking, Embedded C, Embedded System Design using Raspberry Pi, Embedded System Design using Arduino, Real Time Systems, Control Systems to B.Tech students. Areas of interest Embedded Control Systems, Cyber Physical Systems, Deep Learning, Machine Learning.

Arrived: 27.09.2024
Accepted: 11.10.2024