[1]Dr. Mrunal K. Pathak

[2]Arti Bang

[3]Dr. Ranjit M. Gawande

[4]Prof. Archana S. Banait

[5]Dr. G. B. Sambare

[6]Dr Ashfaq Amir Shaikh

Detecting Cyber-attacks in the Industrial Internet of Things using a Hybrid Deep Random Neural Network

Abstract: - Critical infrastructure now faces greater vulnerabilities and a higher risk of cyberattacks as a result of the (IIoT) quick expansion. The security and dependability of industrial systems must be ensured by identifying and thwarting these threats. In this paper, we use a hybrid approach of deep learning and RNN called hybrid deep random neural network (HDRNN) to offer a novel method of identifying cyber-attacks in the IIoT.The proposed HDRNN model combines the benefits of random neural networks with deep learning to improve the detection of IIoT cyberattacks. The deep learning component makes use of deep neural networks' capacity to extract intricate features from unstructured data, while the random neural network component offers robustness and adaptability to manage changing attack patterns.Realistic threats and benchmark datasets such as UNSW-NB15and DS2OS are used in experimental evaluations. High accuracy, precision, and recall rates are attained by the model, which successfully detects a variety of assaults including infiltration, data manipulation, and denial of service.The suggested HDRNN model offers a promising approach for improving the security of IIoT systems by precisely identifying cyber-attacks in real-time. The model's hybrid nature enables enhanced detection capabilities, adaptability to changing attack patterns, and a reduction in false positives, enabling efficient threat mitigation and protecting crucial infrastructure in the IIoT context.

Keywords: Deep Learning Network, Neural Network, Cyberattacks, Intrusion detection, Feature extraction, Industrial Internet of Things

I. INTRODUCTION

In recent time industrial IoT and security plays an important role in the 4.0 industry. This shift in the paradigm has resulted in changes to business conceptions, industrial processes, logistical services, and strategic plans aimed at boosting domestic industries [1]. The Internet of Things (IIoT) services are built on a foundation of Internet of Things (IoT) devices, intelligent communication protocols, and sophisticated security mechanisms [2]. These technologies provide a great deal of management flexibility for industrial operations when combined with the global Internet [3]. The quality of the industry, resource efficiency, and productivity are all increased. Due to the wide range of sensors, controllers, and actuators available today, businesses can gather and analyse large amounts of data to make informed business decisions. Additionally, IIoT makes it easier to detect errors and irregularities in intelligent industrial systems.The IIoT ecosystem provides a difficulty in terms of effectively using these

[1]Assistant Professor, Department of Information Technology, AISSMS Institute of Information Technology, Savitribai Phule Pune University, Pune, India, mrunal.pathak@aissmsioit.org.

[2]Department of Electronics and Telecommunication, Vishwakarma Institute of Information Technology, Pune, Maharashtra, India. Email: arti.bang@viit.ac.in

[3]Asst. Prof., Department of Computer Engineering, Matoshri College of Engineering & Research Centre Nashik, affiliated to Savitribai Phule Pune University., M.S. India, Email: ranjitgawande@gmail.com

[4]Department of Computer Engineering, MET's Institute of Engineering, Bhujbal Knowledge City, Nashik (SPPU), Maharashtra, India. Email: ar.ugale@gmail.com

[5]Pimpri Chinchwad College of Engineering, Pune, Maharashtra, India. Email: santosh.sambare@pccoepune.org

[6]PhD Computer Engineering, Assistant Professor Information Technology, M. H. Saboo Siddik College of Engineering, Mumbai, India. Email: ashfaq.shaikh@mjssce.ac.in

devices due to this resource limitation. Therefore, great thought must be given to maximising the use of the resources at hand in order to assure the best performance and lifetime of these gadgets.

The existence of edge devices has created a potential point of exploitation for third parties within the IIoT ecosystem. An IoT device's vulnerability could provide unauthorised access to important business plans, corporate data, and industrial records, as well as the communication of bogus data to cloud servers. Operational inefficiencies, financial losses, and reputational harm can all be brought on by such security breaches. Therefore, implementing effective cybersecurity measures in the IIoT is a key responsibility in modern industrial circumstances [5]. The classification of intrusion detectors is based on their signature or anomaly. In order to identify potential attacks, signature-based detection looks for specific patterns or signatures connected to well-known types of intrusions. These patternstypically drawn from a database of reported assaultsare used to track down and towards related attempts in real time. The effectiveness of systems for segue-based attack detection is questionable when it comes to new or previously unknown attack patterns.

The focus of anomaly-based intrusion detection systems during a crisis is on identifying deviations from the system's expected behaviour. They establish a baseline of typical behaviour and provide alerts whenever the observed behaviour differs significantly from the average. The ability of anomaly-based infiltration systems to identify new or emerging threats without the need for pre-established signatures is one of their advantages. But since it's so hard to tell the difference between benign and malignant abnormalities, they can also result in more false positives.Because they are excellent at spotting novel and unidentified attacks, anomaly-based IDSs are useful in the context of IIoT security. To recognise and highlight various and original attack patterns, these detection algorithms make use of machine/deep learning classifiers [7]. Deep learning (DL) techniques' use in creating cybersecurity solutions has recently drawn a lot of attention from both academia and business. By skilfully analysing the vast amounts of data produced by industrial systems, DL methods have the ability to produce improved results [8].

Designing reliable and highly efficient attack detection techniques for the IIoT, notwithstanding the gains made, continues to be a difficult task. The development of comprehensive and adaptable IDS systems is significantly hampered by the specific features of the IIoT environment [10], such as the resource-constrained nature of edge devices, dynamic network topologies, and evolving attack vectors.Current research is focused on exploiting large-scale industrial data, optimising network designs, and refining model training methods to improve the capabilities of DL-based anomaly detection models. The accuracy and effectiveness of detection algorithms can also be increased by adding domain expertise, contextual data, and anomaly prioritisation techniques [11].

II. REVIEW OF LITERATURE

Comparing the proposed method to cutting-edge techniques, it demonstrated greater performance.These illustrations show the creative methods researchers are employing to create powerful attack detection systems utilising DL. Researchers use LSTM networks to improve their capacity for accurately classifying attacks and capturing temporal dependencies, while CNNs are used to extract pertinent information from IoT data[10].

Such improvements in attack detection algorithms for DL-based attacks are essential for enhancing the security of IIoT environments. These algorithms contribute to reducing risks, mitigating potential losses, and maintaining the ongoing operation of industrial systems by increasing the accuracy and efficiency of attack detection.In order to find vulnerabilities in IIoT networks, Zolanvari et al. [11] showed an approach using machine learning. Using a real-world testbed, the researchers successfully classified threats such as backdoor, common injection, and structured query language injection. They were able to identify and prevent some assault types thanks to their strategy. Li et al. [12] presented a deep migration learning-based approach for threat detection in IoT-enabled smart cities. To evaluate the effectiveness of their model, they used the KDD CUP 99 dataset. The experimental results demonstrated improved accuracy and quicker detection times as compared to other approaches. The proposed approach could effectively identify and respond to attacks in IoT-based smart city environments.

Self-adaptive attack detection algorithms must be created in order to effectively recognise new and different assault patterns. Zhang et al. [13] created a hybrid technique based on a DBN and an improved GA. Attack classification was handled by the DBN, and the GA was employed to determine the appropriate number of hidden layer neurons. The suggested plan demonstrated increased assault detection and classification rates. The researchers evaluated the performance using the NSL-KDD dataset. These papers present the state-of-the-art techniques that researchers are employing to enhance threat detection in IIoT environments. They want to create precise and effective detection systems that can adjust to new assault patterns by utilising machine learning and deep learning approaches. The performance and robustness of these systems are assessed using real-world testbed and a variety of datasets, making it possible to deploy them practically in IIoT networks [16].

It is significant to remember that these examples only scratch the surface of the research that is currently being done in the area, and new developments are always being made to create self-adaptive and intelligent attack detection algorithms that can successfully combat the changing threat landscape in IIoT systems [29].

Hassan et al.'s study [16] introduced a novel cyberattacks detection methodology that is designed especially for SCADA systems. The researchers merged a random tree technique with random subspace learning. The effectiveness of the suggested plan was assessed using 15 SCADA network datasets, proving its effectiveness in boosting the security of IIoT platforms.For IoT devices.

A straightforward machine learning-based assault detection model was produced by Lee et al. [17]. They employed a support vector machine approach to extract information from attacks and a deep auto encoder to classify attacks. The model was validated using the AWID dataset, and it demonstrated outstanding accuracy of 98%. Finding new and innovative cyberattacks in the context of IIoT systems is a challenging task. This was addressed in Saharkhizan et al.'s [18] suggestion of an improved deep learning model for attack detection. The system's accuracy, which the researchers verified using a dataset of Modbus network traffic, was 99%, made possible by the incorporation of LSTM modules into a group of detectors.

In the IIoT network's fog computing layer, Souza et al. [19] suggested an attack detection method. They used a hybrid DNN and kNN technique for binary classification. The CICIDS datasets were used to assess the model's efficacy. For the IIoT network, Huang et al. [20] presented a unique failure detection technique. To put their idea into practise, they developed a deep neural network (DNN) based on the GBRBM. Modern techniques were outpaced by their model, which turned fault detection into a classification issue

III. DATASET AVAILABILITY

1.Dataset 1:

A total of 357,952 samples make up the dataset, of which 10,017 samples are considered abnormal and 347,935 samples are considered normal. It includes seven different sorts of attacks [2],An open-source dataset created by Pahl and Aubet [2, 3] has been made available for the purpose of exploring and studying security in the second-generation Industrial Internet of Things (IIoT). This dataset is essential for assessing the efficacy of deep learning (DL) and machine learning (ML) algorithms in the context of smart city and smart factory architectures for cybersecurity.

2. Dataset 2:

In the field of cybersecurity, the UNSW-NB15 dataset is frequently used for creating and evaluating machine learning models, network security methods, and intrusion detection systems (IDS). It now serves as a benchmark dataset for assessing the effectiveness of various security measures.It is frequently used to assess how well machine learning-based cybersecurity systems work.There are 257,673 samples altogether in this dataset, 164,673 of which have been classified as anomalous, and 93,000 of which have been classified as normal [24].

Table 1: Description of Dataset

Dataset	No of Records	Attributes	No of Attacks	Classes	Normal	Anomaly
DS2OS	357,952	13	4	2	347,935	10,017
UNSE-NB15	257,673	49	9	2	93,000	164,673

IV. METHODOLOGY

1. Convolution Neural Networks (CNN):

The classification of Big Data is a common challenge for CNNs. They are made up of pooling layers for dimensionality reduction and convolutional layers that automatically identify pertinent characteristics from input photos. CNNs are frequently employed in computer vision problems because they are good at capturing spatial dependencies [19].

- Layer of Input: A collection of photographs are input as a matrix of pixel values.
- Convolutional Layer: To extract local characteristics from the input image, convolutional filters (also known as kernels) are employed. A definition of the convolution operation is:

$$S(i, j) = (I * K)(i, j)$$

Where, If I is the input picture, K is the convolutional filter, and S(i, j) is the value at position (i, j) in the feature map.

- Activation Function: To introduce non-linearity, an activation function, such as ReLU, is applied element-by-element:

$$A(x) = Max(0, x)$$

- Pooling Layer: Max or average pooling is used to reduce the spatial dimensions of the feature maps while keeping the most important features.

2. Random Neural Network (RaNN):

The RaNN (Random Neural Network) model is intended to mimic how the human brain transmits signals. Because of its higher generalisation skills, it is favoured. RaNN's lower processing requirements and highly distributed architecture thus make it proper for arrangement on IoT devices with limited resources [5].A neuron's potential in RaNN serves as a proxy for its condition. RaNN layers of neurons probabilistically exchange excitatory and inhibitory pulses. Only a positive signal can be cancelled by an inhibitory spike; otherwise, it has no impact (potential vtxt(t) = 0). Neuron Xt is at its optimum state when Vtxt(t) = 0. In contrast, neuron xt is in an excited state if vtxt(t) > 0.

$$\sum_{y=1}^{X} Q + (yt, xt) + Q - (yt, xt) + D(xt) = 1, \forall x \qquad (1)$$

There exist probability Q(yt, xt) and Q-(yt, xt) for positive excitatory or negative inhibitory signals, respectively, when delivering signals to the following neuron yt. The signal leaving the network has a probability of d(xt) as well.

$$Hx = \frac{\mu^{+}(xt)}{f\,(xt) + \mu{-}(xt)} \qquad (2)$$

Where,

$$\mu^{+}(xt) = \sum_{v=1}^{u} ayf\,(yt)\,Q^{+}\,(yt, xt) + \varepsilon\,(xt) \qquad (3)$$

$$\mu^{-}(xt) = \sum_{v=1}^{u} ayf\,(yt)\,Q^{-}\,(yt, xt) + \varepsilon\,(xt) \qquad (4)$$

In the RaNN model, an activation function that considers the excitatory inputs $\mu^{+}(xt)$, the inhibitory inputs $\mu^{-}(xt)$, and the firing rate f(xt) determines the output axe of a neuron x. The excitatory and inhibitory inputs from neuron yt to neuron xt are denoted by the weights wt+(xt, yt) and wt-(xt, yt), respectively.

$$wt^{+}(xt, yt) = f\,(x)\,Q^{+}\,(xt, yt) \geq 0 \qquad (5)$$

$$wt^{-}(xt, yt) = f\,(x)\,Q^{-}\,(xt, yt) \geq 0 \qquad (6)$$

Rate expression written as:

$$f\,(xt) = \left(1 - d\,(xt)\right)^{-1} \sum_{u=1}^{t} [W^{+}(xt, yt) + Wt^{-}(xt, yt)] \qquad (7)$$

3. Gradient Descent Algorithm:

The GDM is a typical method of enhancing ML real-life examples. It is a way to predicting minimize the error of instances by adjusting the weights and biases of the system. The algorithm works by calculating the gradient of the error function with respect to the weights and biases and then adjusting the values of the weights and biases in the direction of the negative gradient. This process repeats until the error is minimized to a satisfactory degree. The learning library has ways to make gradient descent work better by using different methods.

- Initialize the parameters: Begin by assigning random or predetermined values to the model's parameters, commonly denoted as.
- Define the cost function: Describe the cost function, also known as the loss function J(), which calculates the difference between the model's predicted and actual values. The effectiveness of the model is quantified by this function.
- Calculate the gradient: Determine the cost function's gradient with respect to the parameters. The gradient gives the surface of the function's steepest ascent's direction and amplitude.

The error cost function calculated as:

$$E_k = \frac{1}{2}\sum_{x=1}^{x} \mathrm{\alpha x}\,(\mathrm{qx} - \mathrm{bxk}\,)^2 \;, \mathrm{\alpha x} \geq 0$$

The weights v+(x, y) and v-(x, y) can be changed throughout the optimisation process if two randomly linked neurons u and v are connected. These weights are updated using the gradient descent technique in an effort to reduce the error cost function.

The weight update expressions for v+(x, y) and v-(x, y) are as follows:

$$\mathrm{v} + (\mathrm{x,y}) := \mathrm{v} + (\mathrm{x,y}) - \alpha * \frac{\partial \mathrm{J}}{\partial \mathrm{w}} + (x, \mathrm{y})$$

$$\mathrm{v} - (\mathrm{x,y}) := \mathrm{v} - (\mathrm{x,y}) - \alpha * \frac{\partial \mathrm{J}}{\partial \mathrm{w}} - (\mathrm{x,y})$$

In the context of the gradient descent algorithm and the given equations, the partial derivatives of Equations can be calculated using vector and matrix notation if is the learning rate and dx/w+(u, v) and dx/w-(u, v) represent the derivatives of the activation functions with respect to the weights.The HDRaNN proposed architecture for cyberattack detection is included in the proposed technique displayed in Figure 1. The two main components of the HDRaNN model are the multilayer perceptron (MLP) and the deep random neural network (DRaNN). Three MLP layers, three recurrent neural network (RNN) layers, three output layers, and an input layer make up the design.

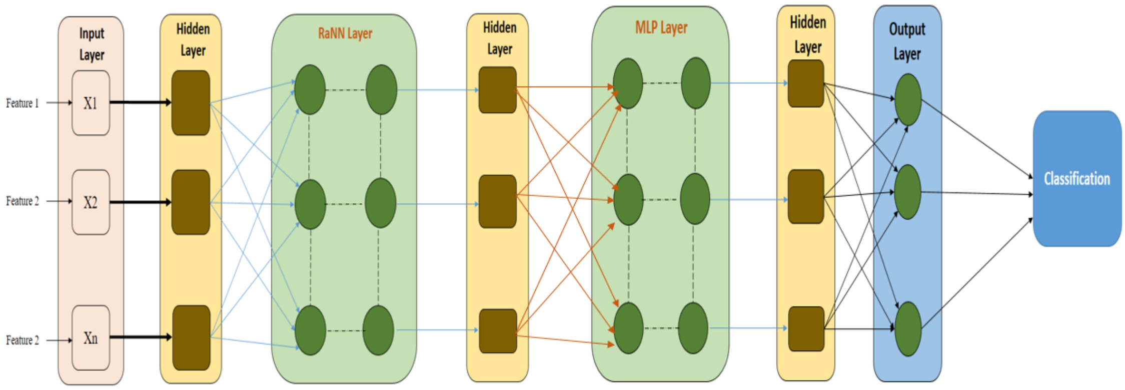

Figure 1: Proposed Method for network attack detection

The model includes dropout regularisation to guarantee robustness and avoid overfitting. With less dependency on specific neurons and improved generalisation skills, this method randomly removes some units during training.To get the best results, the HDRaNN architecture was refined through a process of trial and error. The model was modified to suit the needs of each dataset because two distinct datasets, DS2OS and UNSW-NB15, were employed.

V. RESULT AND DISCUSSION

The model HDRaNN was used with the data from DS2OS and UNSW-NB15, and numerous experiments were run to gauge its effectiveness. The learning rate plays a significant role in the speed at which the algorithm learns in the model's deep learning component.To maximise the model's productivity during a specific training time, the appropriate training pace is essential. Although it may result in better learning, a very low learning rate might also cause learning to take longer. The model could, however, quickly converge to a solution that is suboptimal or even reach a local optimum if the learning rate is set too high.

Table 2: Attack distribution of Dataset 1

Class	**Count**	**Train**	**Test**
Normal	348076	260950	87126
DoS	5780	4340	1440
Malicious-Control	890	670	220
Malicious-Operation	804	600	204
Scan	530	400	130
Spying	124	90	34
Wrong Setup	1547	1150	397
Probing	342	250	92

Table 3: Attack distribution of Dataset 2

Class	**Total**	**Training**	**Testing**
Normal	93000	69457	23543
Fuzzer	2330	1956	374
Backdoor	24245	16872	7373
Analysis	2680	1978	702
Exploit	13879	9870	4009
Generic	44550	32879	11671
DoS	58871	46871	12000

ShellCode	16355	11232	5123
Worms	1512	953	559
Other	175	92	83

With a total of 348,076 samples, the "Normal" class has the most samples overall, of which 260,950 are used for training and 87,126 are set aside for testing. The remaining classes have smaller sample numbers and represent different styles of attacks.The distribution shown here, which shows the number of examples available for each class and the division between training and testing subsets, is crucial to note because it depicts the distribution of classes in the dataset.

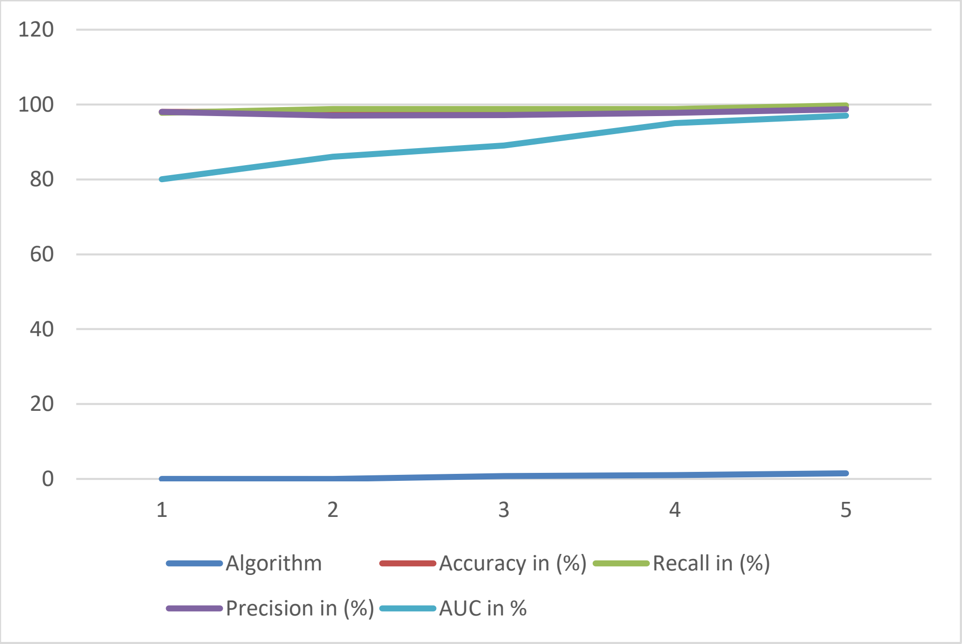

Figure 2: Comparison of performance metrics of proposed method for Dataset 1

The dataset consists of 93,000 samples in total, which are divided into various groups for training and testing. The majority of the samples belong to the "Normal" class, with 69,457 cases designated for training and 23,543 instances for testing. This class indicates instances of typical network behaviour or non-attacks.Different kinds of cyberattacks are represented by a number of other classes. There are 374 testing samples and 1,956 training samples for the "Fuzzer" class. 16,872 training instances and 7,373 testing instances make up the "Backdoor" class. Likewise, there are 1,978 training samples and 702 test samples in the "Analysis" class as discussed in table 3.

With varying quantities of training and testing samples, the classes "Exploit," "Generic," "DoS," "ShellCode," and "Worms" reflect numerous forms of attacks. With 92 training samples and 83 testing samples, the "Other" class has fewer instances.In the subject of cybersecurity, this dataset is crucial for developing and testing machine learning algorithms. Researchers and practitioners can evaluate the effectiveness of their models for identifying and categorising various cyberattacks by distributing samples across classes. The models may be trained and evaluated successfully since distinct training and testing sets are available.

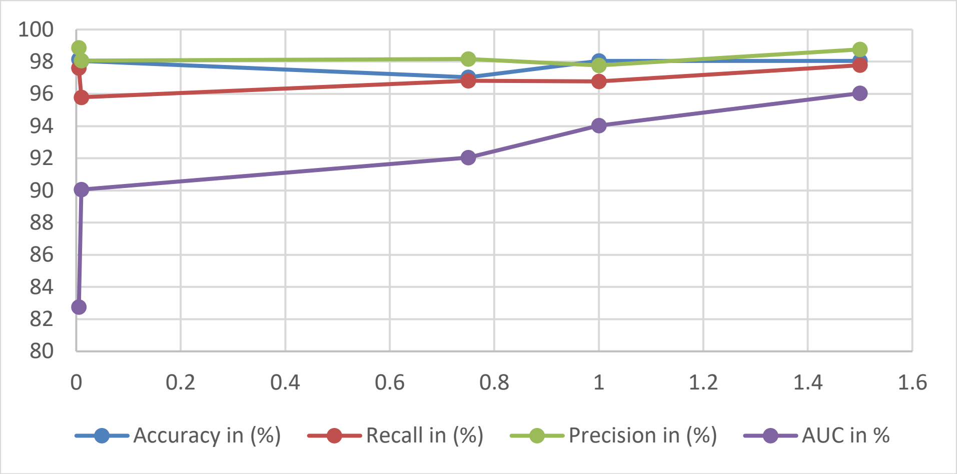

Figure 3: Comparison of performance metrics of Proposed method for Dataset 2

The performance metrics of various algorithms for detecting cyberattacks are summarised in the table 4.The RNN model obtains a 0.64 accuracy, 0.78 precision, 0.93 recall, 0.8 specificity, 0.69 F1 score, and 0.78 AUC.With accuracy of 0.81, precision of 0.96, recall of 0.85, specificity of 0.85, F1 score of 0.95, and AUC of 0.94, the GD (Gradient Descent) model performs better.With an accuracy of 0.86, precision of 0.89, recall of 0.74, specificity of 0.76, F1 score of 0.87, and AUC of 0.78, the CNN (Convolutional Neural Network) model continues to advance.

Table 4: Proposed method Accuracy comparison

Model	Model Accuracy	Model Precision	Model Recall	Model Specificity	Model F1 Score	Model AUC
RNN	0.64	0.78	0.93	0.8	0.69	0.78
GD	0.81	0.96	0.85	0.85	0.95	0.94
CNN	0.86	0.89	0.74	0.76	0.87	0.78
HDRaNN (Proposed Method)	0.98	0.97	0.94	0.96	0.97	0.98

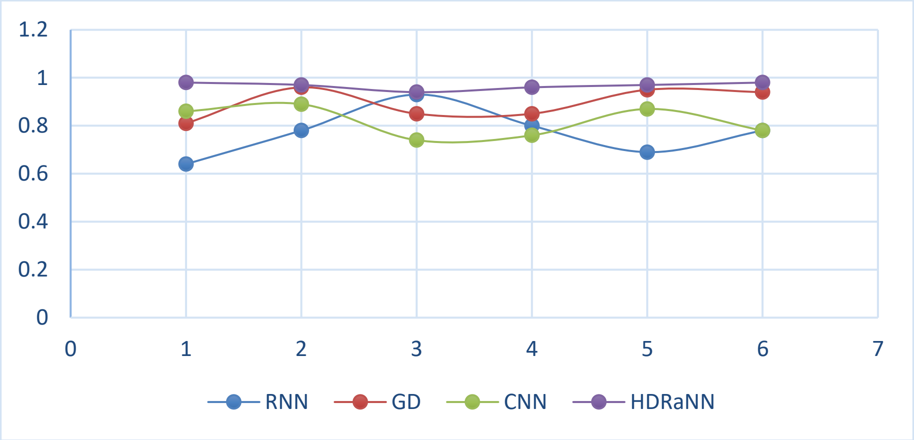

Figure 4: Accuracy comparison for proposed method with other ML method

The proposed HDRaNN (Hybrid Deep Random Neural Network) approach, however, performs better than the other models. The HDRaNN model outperforms all other metrics tested, demonstrating its potency in identifying cyberattacks. In comparison to the previous models, it greatly increases accuracy, precision, recall, and F1 score. The model's great ability to distinguish between attack and non-attack occurrences is indicated by the high AUC.These results show that the proposed HDRaNN technique outperforms the other tested models in terms of accuracy and overall performance, making it a potential strategy for cyberattack detection.

VI. CONCLUSION

This article addresses the important cybersecurity issues that the IIoT sector raises in light of the increasing number of IoT devices that operate on insecure networks and generate substantial data. We offer HDRaNN , a novel technique for cyberattack detection in IIoT networks that combines the advantages of a deep-random neural network (DRNN) and a multilayer perceptron. We conducted experiments utilising the DS2OS and UNSW-NB15 IIoT security-related datasets to assess the efficacy of our suggested strategy. To evaluate the superiority of our strategy, a number of performance indicators were computed. The results demonstrate the exceptional performance of the recommended HDRaNN approach. For the DS2-OS and UNSWNB-15 datasets, respectively, its accuracy in classifying 16 various assault types was over 98% and 99%. When tested, our suggested method outperformed existing deep learning-based approaches in each performance indicator. The outcomes show how effective and trustworthy the HDRaNN technique is at spotting cyberattacks in IIoT networks.It demonstrates the capability of deep learning-based solutions to handle security concerns in the IIoT space, enhancing overall industrial cybersecurity.

REFERENCES

[1] S. Latif, Z. Zou, Z. Idrees, and J. Ahmad, ‘‘A novel attack detection scheme for the industrial Internet of Things using a lightweight random neural network,’’ IEEE Access, vol. 8, pp. 89337–89350, 2020.

[2] M.-O. Pahl and F.-X. Aubet. (2018). Ds2os Traffic Traces IoT Traffic Traces Gathered in a the Ds2Os IoT Environment. [Online]. Available: https://www.kaggle.com/francoisxa/ds2ostraffictraces

[3] M.-O. Pahl and F.-X. Aubet, ‘‘All eyes on you: Distributed multidimensional iotmicroservice anomaly detection,’’ in Proc. 14th Int. Conf. Netw. Service Manage. (CNSM), Nov. 2018, pp. 72–80

[4] N. Moustafa and J. Slay, ‘‘The evaluation of network anomaly detection systems: Statistical analysis of the UNSW-NB15 data set and the comparison with the KDD99 data set,’’ Inf. Secur. J., Global Perspective, vol. 25, nos. 1–3, pp. 18–31, Apr. 2016.

[5] A. Tahir, J. Ahmad, G. Morison, H. Larijani, R. M. Gibson, andD. A. Skelton, ‘‘HRNN4F: Hybrid deep random neural network for multichannel fall activity detection,’’ Probab. Eng. Informational Sci., vol. 35,pp. 1–14, Aug. 2019

[6] E. Sisinni, A. Saifullah, S. Han, U. Jennehag, and M. Gidlund, ‘‘Industrial Internet of Things: Challenges, opportunities, and directions,’’ IEEE Trans. Ind. Informat., vol. 14, no. 11, pp. 4724–4734, Nov. 2018.

[7] Y. Luo, Y. Duan, W. Li, P. Pace, and G. Fortino, ‘‘A novel mobile and hierarchical data transmission architecture for smart factories,’’ IEEE Trans. Ind. Informat., vol. 14, no. 8, pp. 3534–3546, Apr. 2018.

[8] S. Huda, J. Yearwood, M. M. Hassan, and A. Almogren, ‘‘Securing the operations in SCADA-IoT platform based industrial control system using ensemble of deep belief networks,’’ Appl. Soft Comput., vol. 71, pp. 66–77, Oct. 2018.

[9] K. A. P. da Costa, J. P. Papa, C. O. Lisboa, R. Munoz, and V. H. C. de Albuquerque, ‘‘Internet of Things: A survey on machine learning-based intrusion detection approaches,’’ Comput. Netw., vol. 151, pp. 147–157, Mar. 2019.

[10] N. Moustafa, B. Turnbull, and K.-K.-R. Choo, ‘‘An ensemble intrusion detection technique based on proposed statistical flow features for protecting network traffic of Internet of Things,’’ IEEE Internet Things J., vol. 6, no. 3, pp. 4815–4830, Jun. 2019.

[11] S. Aljawarneh, M. Aldwairi, and M. B. Yassein, ‘‘Anomaly-based intrusion detection system through feature selection analysis and building hybrid efficient model,’’ J. Comput. Sci., vol. 25, pp. 152–160, Mar. 2018.

[12] 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.

[13] Y. Li, Y. Xu, Z. Liu, H. Hou, Y. Zheng, Y. Xin, Y. Zhao, and L. Cui, ‘‘Robust detection for network intrusion of industrial IoT based on multiCNN fusion,’’ Measurement, vol. 154, Mar. 2020, Art. no. 107450.

[14] M. M. Hassan, A. Gumaei, A. Alsanad, M. Alrubaian, and G. Fortino, ‘‘A hybrid deep learning model for efficient intrusion detection in big data environment,’’ Inf. Sci., vol. 513, pp. 386–396, Mar. 2020.

[15] M. Zolanvari, M. A. Teixeira, L. Gupta, K. M. Khan, and R. Jain, ‘‘Machine learning-based network vulnerability analysis of industrial Internet of Things,’’ IEEE Internet Things J., vol. 6, no. 4, pp. 6822–6834, Aug. 2019

[16] D. Li, L. Deng, M. Lee, and H. Wang, ‘‘IoT data feature extraction and intrusion detection system for smart cities based on deep migration learning,’’ Int. J. Inf. Manage., vol. 49, pp. 533–545, Dec. 2019.

[17] Y. Zhang, P. Li, and X. Wang, ''Intrusion detection for IoT based on improved genetic algorithm and deep belief network,'' IEEE Access, vol. 7, pp. 31711–31722, 2019.

[18] J. Arshad, M. A. Azad, M. M. Abdeltaif, and K. Salah, ''An intrusion detection framework for energy constrained IoT devices,'' Mech. Syst. Signal Process., vol. 136, Feb. 2020, Art. no. 106436.

[19] D. Vasan, M. Alazab, S. Venkatraman, J. Akram, and Z. Qin, ''MTHAEL: Cross-architecture IoT malware detection based on neural network advanced ensemble learning,'' IEEE Trans. Comput., vol. 69, no. 11, pp. 1654–1667, Nov. 2020.

[20] M. M. Hassan, A. Gumaei, S. Huda, and A. Almogren, ''Increasing the trustworthiness in the industrial IoT networks through a reliable cyberattack detection model,'' IEEE Trans. Ind. Informat., vol. 16, no. 9, pp. 6154–6162, Sep. 2020.

[21] S. J. Lee, P. D. Yoo, A. T. Asyhari, Y. Jhi, L. Chermak, C. Y. Yeun, and K. Taha, ''IMPACT: Impersonation attack detection via edge computing using deep autoencoder and feature abstraction,'' IEEE Access, vol. 8, pp. 65520–65529, 2020.

[22] M. Saharkhizan, A. Azmoodeh, A. Dehghantanha, K.-K.-R. Choo, and R. M. Parizi, ''An ensemble of deep recurrent neural networks for detecting IoT cyber attacks using network traffic,'' IEEE Internet Things J., vol. 7, no. 9, pp. 8852–8859, Sep. 2020.

[23] C. A. de Souza, C. B. Westphall, R. B. Machado, J. B. M. Sobral, and G. D. S. Vieira, ''Hybrid approach to intrusion detection in fog-based IoT environments,'' Comput. Netw., vol. 180, Oct. 2020, Art. no. 10741

[24] Z. Zhang, Q. Liu, S. Qiu, S. Zhou and C. Zhang, "Unknown Attack Detection Based on Zero-Shot Learning", IEEE Access, vol. 8, pp. 193981-193991, 2020.

[25] L. N. Tidjon, M. Frappier and A. Mammar, "Intrusion Detection Systems: A Cross-Domain Overview", IEEE Communications Surveys & Tutorials, vol. 21, no. 4, pp. 3639-3681, 2019.

[26] A. S. Alzahrani, R. A. Shah, Y. Qian and M. Ali, "A novel method for feature learning and network intrusion classification", Alexandria Engineering Journal, vol. 59, no. 3, pp. 1159-1169, 2020.

[27] H. Liu and B. Lang, "Machine learning and deep learning methods for intrusion detection systems: A survey", Applied Sciences (Switzerland), vol. 9, no. 20, 2019.

[28] M. Hasan, M. M. Islam, M. I. I. Zarif and M. M. A. Hashem, "Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches", Internet of Things (Netherlands), vol. 7, pp. 100059, 2019.

[29] N. Chouhan, A. Khan, H. Ur and R. Khan, "Network anomaly detection using channel boosted and residual learning based deep convolutional neural network", Applied Soft Computing Journal, vol. 83, pp. 105612, 2019.