IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received February 19, 2021, accepted April 5, 2021, date of publication April 8, 2021, date of current version April 16, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3071766

A Hybrid Deep Random Neural Network for Cyberattack Detection in the Industrial Internet of Things

ZIL E. HUMA[1], **SHAHID LATIF**[2], (Graduate Student Member, IEEE), **JAWAD AHMAD**[3], (Senior Member, IEEE), **ZEBA IDREES**[2], **ANAS IBRAR**[4], **ZHUO ZOU**[2], (Senior Member, IEEE), **FEHAID ALQAHTANI**[5], **AND FATMAH BAOTHMAN**[6]

[1]School of Electrical Engineering and Computer Science, National University of Science and Technology, Islamabad 44000, Pakistan
[2]State Key Laboratory of ASIC and System, School of Information Science and Engineering, Fudan University, Shanghai 200433, China
[3]School of Computing, Edinburgh Napier University, Edinburgh EH10 5DT, U.K.
[4]Department of Electrical Engineering, Wah Engineering College, University of Wah, Wah Cantt 47040, Pakistan
[5]Department of Computer Science, King Fahad Naval Academy, Saudi Arabia
[6]Faculty of Computing and Information Technology, King Abdul Aziz University, Jeddah 21431, Saudi Arabia

Corresponding author: Jawad Ahmad (J.Ahmad@napier.ac.uk)

ABSTRACT The Industrial Internet of Things (IIoT) refers to the use of traditional Internet of Things (IoT) concepts in industrial sectors and applications. IIoT has several applications in smart homes, smart cities, smart grids, connected cars, and supply chain management. However, these systems are being more frequently targeted by cybercriminals. Deep learning and big data analytics have great potential in designing and developing robust security mechanisms for IIoT networks. In this paper, a novel hybrid deep random neural network (HDRaNN) for cyberattack detection in the IIoT is presented. The HDRaNN combines a deep random neural network and a multilayer perceptron with dropout regularization. The proposed technique is evaluated using two IIoT security-related datasets: (i) DS2OS and (ii) UNSW-NB15. The performance of the proposed scheme is analyzed through a number of performance metrics such as accuracy, precision, recall, F1 score, log loss, Region of Convergence (ROC), and Area Under the Curve (AUC). The HDRaNN classified 16 different types of cyberattacks using with higher accuracy of 98% and 99% for DS2OS and UNSW-NB15, respectively. To measure the effectiveness of the proposed scheme, the performance metrics are also compared with several state-of-the-art attack detection algorithms. The findings of HDRaNN proved its superior performance over other DL-based schemes. The deployment perspective of the proposed work is also highlighted in this work.

INDEX TERMS Attack detection, cybersecurity, deep learning, Industrial Internet of Things, random neural network.

I. INTRODUCTION

The Industrial Internet of things (IIoT) brought a great revolution in the industrial sector [1]. The term IIoT can be closely related to the concept of Industry 4.0. This concept is rapidly introducing new trends in the development of business ideas, industrial processes, logistic services, and many other strategic initiatives to boost national industries. IIoT networks contain thousands of IoT devices, intelligent communication protocols, and advanced security mechanisms [2]. The integration of all these devices and technologies with the global internet provides great management flexibility in industrial operations [3]. It also enhances the quality and productivity of an industry with resource efficiency. Multiple industries including manufacturing, food processing, agriculture, and security surveillance have adopted IIoT in recent years. The diverse nature of sensors, controllers, and actuators enables modern industries for making intelligent business decisions

The associate editor coordinating the review of this manuscript and approving it for publication was Fatos Xhafa.

by collecting and analyzing a vast amount of data. It also spots the inefficiencies and detects anomalies in smart industrial environments. However, IoT enabled devices and sensors are considered as resource-constrained devices which have limited power, memory and communication resource. Therefore, edge devices including desktops, routers, laptops, small servers, smartphones, and hand-held devices are used as intermediaries between the cloud servers and sensors. These devices gather information from sensors and transmit it to the local servers after necessary preprocessing.

However, with the rapid increase in the number of IoT edge devices in the industry, several security and privacy problems have arisen that are a great challenge to the security and trustworthiness of the IIoT [4]. These edge devices can be a point of exploitation for intruders. A compromised IoT device can be a cause of transmitting false information to the cloud servers or lead to unauthorized access to valuable industrial documents, business plans, and corporate information. This may lead to operational inefficiencies, financial and reputational loss. Ensuring cybersecurity in the IIoT is one of the major challenges in modern industrial environments. It includes the protection of edge devices from malware, unauthorized access, and ensuring communication and physical privacy. The security, privacy, and trustworthiness of the IIoT can be improved by deploying advanced and robust security mechanisms. In the context of IoT/IIoT security, an intrusion detection system (IDS) is one of the widely adopted techniques. IDS is used to monitor networks for malicious activities or policy violations [5]. IDSs can be categorized into two types: signature-based and anomaly-based. Signature-based IDS detects possible attacks by looking for specific patterns [6]. Signature-based IDS can effectively detect known types of attacks, but it can detect new types of attacks. Anomaly-based IDS has a great capability to detect new and unknown attacks. This detection model uses machine/deep learning classifiers to detect new and diverse nature attacks [7]. In recent years, the use of deep learning (DL) schemes to design and develop cybersecurity solutions has received great attention from academia and industry. DL schemes have great potential to produce better results from the big data of industrial systems [8]. However, the design of robust and more effective attack detection schemes for the IIoT is still an open challenge.

A. MOTIVATION AND CONTRIBUTIONS

An IIoT network contains resource-constrained IoT devices that demand low cost, low power, and low storage cybersecurity solutions. Therefore, the main motivation of this research is to introduce a lightweight DL-based attack detection scheme that can classify several types of attacks in an IIoT network with great accuracy and a higher detection rate. The main contributions of this research are listed as follows.

- This paper assesses the potential of DL-based schemes for cybersecurity in IoT and IIoT networks.
- A novel deep learning-based scheme (HDRaNN) is proposed for cyberattack detection and classification in the IIoT.
- The proposed algorithm is evaluated by using the two latest IIoT security datasets, DS2OS and UNSW-NB15.
- Several performance metrics such as the accuracy, precision, recall, F1 score, log loss, and AUC-ROC are utilized to evaluate the performance of the proposed scheme.
- The results of the proposed HDRaNN are compared with several state-of-the-art attack detection algorithms.

The remainder of the article is organized as follows. Section 2 presents the overview of related DL-based attack detection schemes for IoT and IIoT networks and the limitations of existing research. Section 3 briefly describes materials and methods. Section 4 presents results and discussions and finally, section 5 concludes this research.

II. RELATED WORK

This section presents some of the latest state-of-the-art attack detection algorithms proposed by several researchers. These schemes are categorized based on the utilized DL algorithms, used datasets, and their performances. Li *et al.* [9] proposed a multi convolutional neural network fusion method for anomaly detection in the IoT. The NSL-KDD dataset is used to evaluate the proposed scheme. Their experimental results demonstrated that the proposed scheme successfully classified attacks with high accuracy and low complexity. Hassan *et al.* [10] introduced a hybrid deep learning model. They presented a convolutional neural network and weight dropped long short-term memory (WDLSTM) network. In the proposed technique, a CNN is used to extract the features from IDS big data and the WDLSTM is used for attack classification. The proposed approach proved its superior performance in comparison with state-of-the-art schemes. Zolanvari *et al.* [11] presented a machine learning-based scheme for the detection of vulnerabilities in an IIoT network. Researchers successfully classified backdoor, common injection, and structured query language injection attacks by using a real-world testbed. Li *et al.* [12] introduced a deep migration learning-based scheme for attack detection in IoT enabled smart cities. The authors analyzed the model's performance by using the KDD CUP 99 dataset. The experimental results proved the higher accuracy and short detection time. Self-adaptive attack detection schemes are very important to identifying new and diverse nature attacks. Zhang *et al.* [13] proposed a deep belief network (DBN) and an improved genetic algorithm (GA)-based hybrid scheme. The GA is used to select the optimal number of hidden layer neurons and the DBN classified the attacks with a higher accuracy and detection rate. Researchers utilized NSL-KDD dataset to evaluate the proposed scheme. In another latest work, Arshad *et al.* [14] presented an intrusion detection framework for energy-constrained IoT devices.

Researchers implemented their proposed scheme with Contiki operating system and done extensive experimentation to evaluate potential performance trade-offs. The obtained results proved the effectiveness of the proposed approach for intrusion detection in the IIoT system. Vasan *et al.* [15] developed a robust cross-architecture IoT malware threat hunting model. They efficiently optimized convolutional neural networks (CNN) and recurrent neural networks with higher accuracy on different IoT architectures. The proposed technique is evaluated by using a large IoT cross-architecture dataset.

Hassan *et al.* [16] proposed a novel cyberattack detection model for the SCADA system. Researchers combined random subspace learning with a random tree. The proposed scheme is evaluated over 15 datasets of the SCADA network. The experimental results proved the effectiveness of the scheme for the IIoT platform's security. Lee *et al.* [17] developed a lightweight machine learning-based attack detection model. In the proposed scheme, a support vector machine algorithm is deployed on IoT devices for feature extraction and attacks are classified by using a deep autoencoder. The proposed model is evaluated using the AWID dataset and achieved an accuracy of 98%. The detection of new cyberattacks is an open challenge for IIoT platforms. In this context, Saharkhizan *et al.* [18] proposed an advanced deep learning model for attack detection. Researchers integrated LSTM modules into an ensemble of detectors. They evaluated the effectiveness of the proposed scheme by using the Modbus network traffic dataset and obtained an accuracy of 99%. Souza *et al.* [19] proposed an attack detection scheme that operates in the fog computing layer of the IIoT network. They presented a hybrid binary classification method that contains a deep neural network (DNN) and the k-Nearest Neighbors (kNN). The researchers evaluated their model by using the CICIDS and NSL-KDD datasets. Huang *et al.* [20] proposed a novel fault detection scheme for the IIoT network. The authors introduced the Gaussian Bernoulli Restricted Boltzmann Machine (GBRBM)-based deep neural network (DNN). This scheme transformed fault detection into a classification problem. The authors also compared their model with state-of-the-art methods and the experimental results demonstrated the superior performance of the proposed model. In today's world, the huge amount of IIoT malware is one most serious security threats. Taheri *et al.* [21] presented a robust Featured Learning-based architecture for android malware detection in IIoT. Researchers evaluated their proposed scheme by conducting extensive experiments on three IoT datasets. The obtained results confirmed the higher attack detection accuracy of the proposed algorithm. In another research, Khoda *et al.* [22] proposed two novel techniques for the selection of adversarial samples to retrain a classifier. One technique is based on probability measures derived from kernel-based learning and the second is based on the distance from the malware cluster center. The experimental results indicate that proposed schemes improved the attack detection accuracy by 6%. The outcomes of this research can be very helpful for the designing of robust security systems for IIoT applications.

Several researchers have done great jobs by proposing efficient attack detection schemes for IoT and IIoT platforms. However, the existing studies have a few limitations. First, the majority of the researchers used the old generation NSL-KDD and KDD CUP 99 datasets, which have not been updated according to modern industrial requirements. Second, in recent studies, most of the researchers evaluated their schemes by defining a few performance matrices that don't provide in-depth analysis. Third, the feasibility of the proposed schemes for resource-constrained devices is not deeply considered. To address the aforementioned challenges, we propose a lightweight HDRaNN-based attack detection scheme for IIoT networks, which is an extension of our previous work [23]. We use two latest IIoT security-related datasets and define several performance parameters for the performance evaluation. Finally, we discuss the feasibility of the implementation of the proposed scheme on resource-constrained devices.

III. MATERIALS AND METHODS

In this section, we present the details about the IIoT security datasets, the mathematical background of the proposed neural network, and the implementation model.

A. INDUSTRIAL IoT DATASETS

We use two new generation IIoT security datasets, DS2OS and UNSW-NB15. The detailed descriptions of these datasets are given in the following.

1) DS2OS DATASET

Pahl and Aubet [24], [25] provided this open-source, new generation IIoT security dataset for study and research purposes. This dataset is very helpful for evaluating the effectiveness of ML/DL-based cybersecurity algorithms for smart cities, smart factories architectures, etc. The dataset contains a total of 357952 samples with 10017 anomalous and 347935 normal values. It contains 13 features and seven different types of attacks such as denial of service, malicious operation, malicious control, wrong setup, spying, scan, and data type probing attacks. All the classes of this dataset are shortly described in the following [23].

1) **Normal:** If data do not contain any anomalous values, then they are called normal data.
2) **Denial of Service:** In this attack, the attacker can suspend the machine and network resources for users. The attacker overloads the network by sending too much ambiguous traffic.
3) **Malicious Control:** This attack provides unauthorized access to system devices or networks. This attack is launched with the malicious intent to access valuable information.

4) **Malicious Operation:** In this attack system, the performance is badly affected by distracting the system from the original operation.
5) **Spying:** In spying, an attacker can get access to the secret information through a backdoor channel by exploiting the vulnerabilities of the system.
6) **Wrong Setup:** In this attack, an intruder can access the confidential and valuable information about customers or the industry by exploiting the wrong system setup.
7) **Scan:** The attacker scans the network devices and collects the information of the client's IP addresses and server port addresses.
8) **Data Type Probing:** In this attack, the attacker determines the weaknesses or vulnerabilities of a machine by scanning it.

2) UNSW-NB15 DATASET

The second dataset is the UNSWNB15 dataset. It is generated by the Cyber Range Lab of the Australian Centre for Cyber Security [26]. This is one of the new generation IIoT datasets that is extensively used for the efficiency evaluation of machine learning-based cybersecurity applications. This dataset consists of total 257673 samples in which 164673 are anomalous and 93000 are normal values. This dataset contains 49 features and 9 types of attacks. These attacks include fuzzer, backdoor, analysis, reconnaissance, exploit, generic, DoS, shellcode, and worm attacks. All the classes of this dataset are shortly described in the following.

1) **Fuzzers:** In this attack, the intruder attempts to crash a program, operating system, or network by inputting a massive amount of random data.
2) **Backdoor:** It is a type of malware in which cybercriminals can get unauthorized access to websites. Attackers spread the malware in the complete system by targeting unsecured entry points.
3) **Analysis:** This attack focuses on malware events and computer intrusions in which attackers get access to the system by using their technical capabilities.
4) **Reconnaissance:** The attacker collects the information about system vulnerabilities that can exploit the system control.
5) **Exploit:** This is a code that takes advantage of software vulnerabilities and security flaws. In this attack, an intruder can get unauthorized access.
6) **Generic:** This attack works against all the block ciphers without determining the structure of the block cipher.
7) **DoS:** In this attack, the attacker can suspend the machine and network resources for users. The attacker overloads the network by sending too much ambiguous traffic.
8) **Shellcode:** It is a set of instructions that execute commands in software to exploit a machine.
9) **Worm:** It contains malicious codes that attack the host computer and spread through the network. It can exploit the security vulnerabilities of different applications.

B. MATHEMATICS OF A RANDOM NEURAL NETWORK

E. Gelenbe introduced the random neural network (RaNN) in 1989 [27]. This model mimics the signal transmission process of the human brain. The RaNN is preferred due to better generalization capabilities. Moreover, RaNN is highly suitable for deployment on resource-constrained IoT devices or neuromorphic hardware because of lower computational requirements and highly distributed nature [28].

In an RaNN, the state of a neuron is represented by its potential. A neuron exchanges excitatory and inhibitory spikes probabilistically in RaNN layers. An inhibitory spike can only cancel the positive signal and it does not affect it if $v_x(t) = 0$. Neuron x will be in an ideal state when $v_x(t) = 0$. If $v_x(t) > 0$, then neuron x will be in an excited state. According to an exponential distribution, the firing rate $f(x)$ and the mean value of the time between signals $1/f(x)$ determine when the neurons transmit the signals. The signal transmitted to the next neuron y can be a positive excitatory or negative inhibitory signal with probabilities $p^+(y,x)$ or $p^-(y,x)$, respectively. The signal may also leave the network with probability $d(x)$.

$$\sum_{y=1}^{X}\left[p^+(y,x) + p^-(y,x)\right] + d(x) = 1, \quad \forall x \tag{1}$$

Here, X is the total number of neurons. According to the arrival rates of excitation $\varepsilon(x)$ and exhibition $\mu(x)$, the probability of neuron x firing can be described as [29]:

$$a_x = \frac{\mu^+(x)}{f(x) + \mu^-(x)} \tag{2}$$

Here,

$$\mu^+(x) = \sum_{y=1}^{X} a_y f(y)\, p^+(y,x) + \varepsilon(x) \tag{3}$$

$$\mu^-(x) = \sum_{y=1}^{X} a_y f(y)\, p^-(y,x) + \mu(x) \tag{4}$$

The output a_x is an activation function of excitatory inputs $\mu^+(x)$ divided by the sum of inhibitory inputs $\mu^-(x)$ and a firing rate$f(x)$.$w^+(x,y)$ and $w^+(x,y)$ are defined as follows.

$$w^+(x,y) = f(x)\, p^+(x,y) \geq 0 \tag{5}$$

$$w^-(x,y) = f(x)\, p^-(x,y) \geq 0 \tag{6}$$

By using Equations 1, 5, and 6, the firing rate's expression $f(x)$ can be derived as:

$$f(x) = (1 - d(x))^{-1} \sum_{y=1}^{X} \left[w^+(x,y) + w^-(x,y)\right] \tag{7}$$

$$\mu^+(x) < \left[f(x) + \mu^-(x)\right] \tag{8}$$

Here, Eq. 8 is a necessary condition for the existence of a unique solution in an RaNN. The values $w^+(x,y)$ and $w^-(x,y)$ are equivalent to weights of the neural network and can be trained with traditional learning algorithms such as gradient descent.

1) GRADIENT DESCENT ALGORITHM

In this section, the standard gradient descent (GD) for the training of the RaNN is described. Let the training set (A, B) contain K input-output pairs. Here, $A = \{a, \ldots, a_K\}$ are inputs and $B = \{b_1, \ldots, b_K\}$ are output vectors.

$$\left\{ \begin{array}{l} \varepsilon_l(x) > 0, \ \mu_l(x) = 0 \quad if\ a_{xk} > 0 \\ \varepsilon_l(x) > 0, \ \mu_l(x) > 0 \quad if\ a_{xk} \leq 0 \end{array} \right\} \tag{9}$$

The error cost function E_k of k^{th} input-output pair for the GD is:

$$E_k = \frac{1}{2} \sum_{x=1}^{X} \alpha_x (q_x - b_{xk})^2, \quad \alpha_x \geq 0 \tag{10}$$

Here, $\alpha_x \in [0, 1]$ decides whether neuron x is an output neuron, where q_x is a differentiable function and b_{xk} is the desired value. The GD minimizes the error cost function. Suppose two random neurons u and v are connected. Then, $w^+(u, v)$ and $w^-(u, v)$ can be updated according to the expressions

$$w_t^+(u,v) = w_{t-1}^+(u,v) - \delta \sum_{x=1}^{X} \alpha_x (d_x - b_{xk}) \left[\frac{\partial d_x}{\partial w^+(u,v)} \right]_{t-1} \tag{11}$$

$$w_t^-(u,v) = w_{t-1}^-(u,v) - \delta \sum_{n=1}^{N} \alpha_x (d_x - b_{xk}) \left[\frac{\partial d_x}{\partial w^-(u,v)} \right]_{t-1} \tag{12}$$

Here, δ is the learning rate and $\partial d_x / \partial w^+(u, v)$ and $\partial d_x / \partial w^-(u, v)$ are the derivatives of the activation functions with respect to the weights. The partial derivative of Eq. 11 and Eq. 12 can be calculated by defining a vector $j = (j_1, \ldots . j_X)$ and a matrix W of size $X \ \times X$.

Here W is

$$W = \frac{\left[w^+(x,y) - w^-(x,y) j_y \right]}{\left[f(y) + \mu^-(y) \right]}, \quad x, y = 1, \ldots . X. \tag{13}$$

The defining vectors are $\gamma^+(u, v)$ and $\gamma^-(u, v)$ with X entries, where each entry x is defined as:

$$\gamma_x^+(u,v) = \begin{cases} \dfrac{-1}{f(x) + \mu^-(x)} & if\ u = x, \ v \neq x \\ \dfrac{1}{f(x) + \mu^-(x)} & if\ u \neq x, v = x \\ 0 & otherwise \end{cases} \tag{14}$$

$$\gamma_x^-(u,v) = \begin{cases} \dfrac{-1 + j_x}{f(x) + \mu^-(x)} & if\ u = x, \ v = x \\ \dfrac{-1}{f(x) + \mu^-(x)} & if\ u = x, \ v \neq x \\ \dfrac{-j_x}{f(x) + \mu^-(x)} & if\ u \neq x, v = x \\ 0 & otherwise \end{cases} \tag{15}$$

The above notation can be used to derive the vector equation from Eq. 2.

$$\frac{\partial j}{\partial w^+(u,v)} = \frac{\partial j}{\partial w^+(u,v)} W + \gamma^+(u,v) j_u \tag{16}$$

$$\frac{\partial j}{\partial w^-(u,v)} = \frac{\partial j}{\partial w^-(u,v)} W + \gamma^-(u,v) j_u \tag{17}$$

The training algorithm stops its execution when the desired criteria is achieved or the program reaches its maximum number of iterations.

C. PROPOSED HYBRID DEEP RANDOM NEURAL NETWORK

The architecture of the proposed cyberattack detection is presented in Figure 1. The HDRaNN consists of a deep random neural network (DRaNN) and a multilayer perceptron (MLP). This model contains one input layer, three RNN layers, three MLP layers, and one output layer. The proposed architecture is implemented with dropout regularization to avoid overfitting the model. This architecture gave us the best optimum results through hit and trial method. Since we used two different datasets, DS2OS and UNSW-NB15, that have different features, we adjust the model according to the requirements of each dataset. The implementation of the HDRaNN for both datasets is described in the following.

1) IMPLEMENTATION WITH DS2OS DATASET

The DS2OS dataset contains 13 features and 8 classes. Preprocessing is an essential requirement to make the data the most compatible with a neural network. This dataset consists of some missing data in two feature columns. The "Access Node Type" consists of 148 "NaN" values that are replaced by some malicious values in preprocessing. In the "Value" column, some data are unassigned. "Twenty", "nan", "True" and "False" are replaced with 20.0, 0.0, 1.0, and 0.0, respectively. The features of the dataset contain numerical and categorical values. Label encoding is used to convert the categorical values into nominal values. For DS2OS, 11 features are used as input. Therefore, all the parameters of the neural network are adjusted according to input requirements for optimum processing.

2) IMPLEMENTATION WITH UNSW-NB15 DATASET

The UNSW-NB15 dataset contains a total of 49 features and 10 classes. Two techniques, data conversion and data normalization, are used for the preprocessing of this dataset. All the nominal data are converted into numerical data using data conversion. This process assures the complete processing of numerical data. Data normalization is used reduce the large variance of features. All the null values of the dataset are removed during normalization. Min-max scaling is used to normalize the large values to a range from zero to one. Feature selection is performed by using an Association Rule Mining (ARM). ARM is a data mining technique that estimate the correlation of two or more than two features in a dataset. We selected forty-one most prominent features of the dataset based on confidence score. Therefore, all the parameters of the neural network are adjusted according to the input requirements for optimum processing.

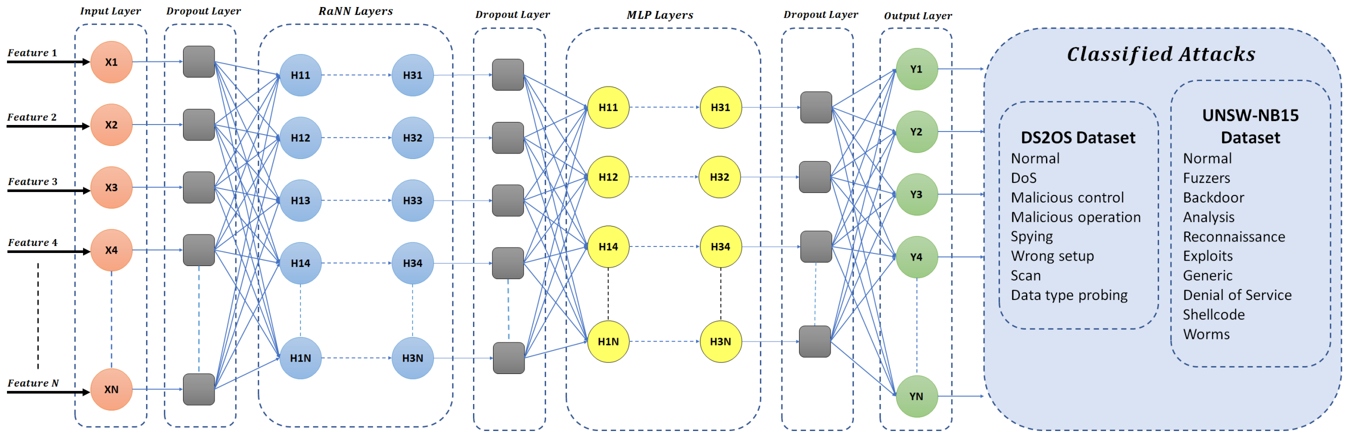


FIGURE 1. Proposed HDRaNN attack detection model.

D. PERFORMANCE EVALUATION METRICS

Several performance parameters are considered for the performance evaluation of the proposed technique.

1) ACCURACY

The accuracy describes the percentage of correct predictions.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \tag{18}$$

2) PRECISION

The precision describes the ratio of correctly predicted positive outcomes with the total number of positive predictions.

$$Precision = \frac{TP}{TP + FP} \tag{19}$$

3) RECALL

The recall is the ratio between the correctly predicted positive outcomes and the total outcomes in a given class.

$$Recall = \frac{TP}{TP + FN} \tag{20}$$

4) F1 SCORE

The F1 score is described as a weighted average of the precision and recall, and it produces a result that ranges from 0 to 1.

$$F1\ Score = \frac{2\ \times (recall\ \ \times precision)}{recall + precision} \tag{21}$$

5) LOG LOSS

The log loss measures the performance of the model by using the probability of expected outcomes. If the actual class probability is high, then the log loss will be high. A lower score indicates a better performing model.

$$-\sum_{c=1}^{M} y_{o,c} \log(p_{o,c}) \tag{22}$$

6) ROC AUC

The ROC is a graph that is plotted by the model at various thresholds. This graph uses the true positive rate (TPR) and false positive rate (FPR).

$$TPR = \frac{TP}{TP + FN} \tag{23}$$

$$FPR = \frac{FP}{FP + TN} \tag{24}$$

IV. EXPERIMENTS AND RESULTS

In this section, we describe the implementation of the proposed scheme and evaluate the potential of the HDRaNN using the preprocessed datasets. The comparative analysis of the HDRaNN with other state-of-the-art DL schemes is also presented.

A. IMPLEMENTATION PLATFORM

The implementation and results analysis of the proposed algorithm is performed on a Dell Alienware Aurora R11 desktop computer. The system is equipped with a 10th Gen Intel Core i7-10700KF processor and 16GB of Dual Channel HyperX^{TM} FURY DDR4 XMP RAM^{TM}. An NVIDIA GeForce RTX^{TM} 2070 Super 8GB GDDR6 graphics card ensures the smooth execution of the deep learning algorithm. The software of the proposed algorithm is written and executed in "Anaconda Navigator" with "Keras" and "TensorFlow".

B. SIMULATIONS AND RESULTS DISCUSSION

The proposed HDRaNN is implemented using the DS2OS and UNSW-NB15 datasets. Several performance metrics were calculated for the performance evaluation. In the deep learning model, the learning rate regulates the learning speed of the DL algorithm. The model achieves its best performance for a specific number of epochs with the optimum learning rate. At a very low learning rate, the model will be learning better, but the training time will be high and the model can fall into the local optimum. Conversely, a high

TABLE 1. Attacks distribution in the DS2OS dataset.

Class Name	Total	Training	Testing
Normal	347935	260951	86984
Denial of service	5780	4335	1445
Malicious control	889	667	222
Malicious operation	805	604	201
Spying	532	399	133
Wrong setup	122	92	31
Scan	1547	1160	387
Data type probing	342	257	86

TABLE 2. Performance evaluation of the proposed algorithm with the DS2OS dataset.

Performance	Learning Rates				
Parameters	0.005	0.01	0.75	1.00	1.50
Accuracy	0.9789	0.9856	0.9812	0.9634	0.9610
Precision	0.9773	0.9825	0.9808	0.9222	0.9598
Recall	0.9745	0.9836	0.9797	0.9733	0.9602
F1 Score	0.9759	0.9830	0.9802	0.9471	0.9600
Log Loss	0.4523	0.3624	0.4102	0.5682	0.7125
AUC-ROC	0.8025	0.9128	0.8834	0.7422	0.6653

learning rate allows for fast learning but it can also the cause a high output error. Therefore, the optimum performance of the model can be ensured with the selection of an accurate learning rate. The number of neurons in the hidden layers is the second factor can also affect the performance of the model. There is no typical rule for the exact determination of the number of neurons in the hidden layer; therefore, we can determine it according to the number of input features. Ten-fold cross-validation was performed on the both dataset for detailed analysis. All the results are generated and analyzed by simulating the HDRaNN model for 150 epochs.

1) PERFORMANCE ANALYSIS WITH THE DS2OS DATASET

The DS2OS dataset is split into training and testing sets at rates of 75% and 25%, respectively. The distribution of the attacks is presented in Table 1. 11 features of the dataset are selected as the input. We selected the number of neurons in the RaNN layers and MLP layers as 11. The simulation is executed on the five learning rates of 0.005, 0.01, 0.75, 1.00 and 1.50. A detailed performance comparison is presented in Table 2. Figure 2 presents the accuracy comparison with different learning rates after ten-fold cross-validation for DS2OS dataset. According to the results, the overall performance for the learning rates of 0.005, 1.00, and 1.50 is less than 98%. The model performed better with learning rates of 0.001 and 0.75. The best performance is achieved at 0.01, as shown in the accuracy comparison graph in Figure 3. According to the results, the best training and testing accuracies are achieved as 98.75% and 98.56% respectively. The other performance scores of the precision, recall, and F1 score are 98.25%, 98.36%, and 98.30%, respectively. The log loss score is low as 0.3624, which indicates the optimum performance. The overall AUC-ROC is higher than 0.9128, which represents that the model

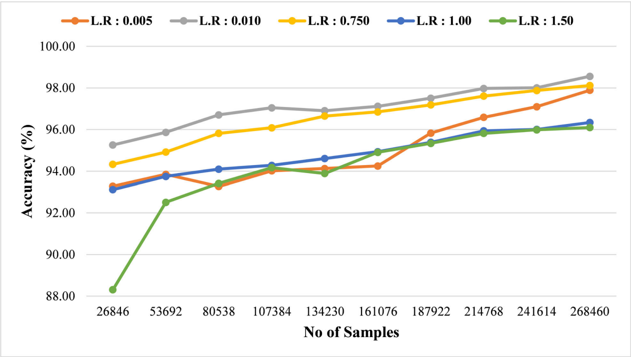


FIGURE 2. Comparitive analysis of accuracy with different learning rates for 10-fold cross validation using DS2OS dataset.

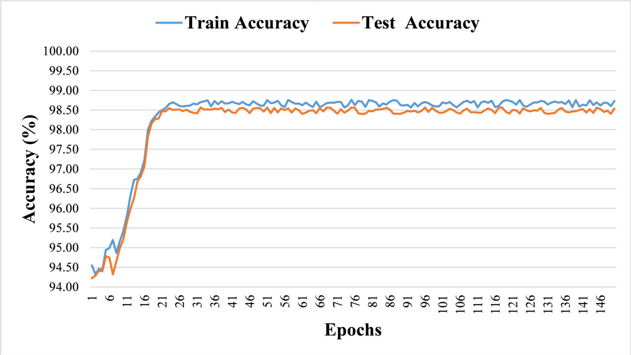


FIGURE 3. Best Performance of the HDRaNN with the DS2OS dataset.

achieved high detection results. This dataset contains 7 types of attacks. The attack classification is represented by the confusion matrix, as shown in Table 5. According to the confusion matrix, the proposed HDRaNN model more accurately classified "Malicious Control", "Data Type Probing", "Spying", and "Malicious Operation". In the "Normal" class, 657 samples are misclassified as anomalous data. In the "DoS", "Scan" and "Wrong Setup", 320, 98, and 5 samples are misclassified, respectively. The overall performance of the HDRaNN for DS2OS is very good and satisfactory.

2) PERFORMANCE ANALYSIS WITH THE UNSW-NB15 DATASET

UNSW-NB15 dataset is also split into training and testing set at rate of 75% and 25%, respectively. The attacks distribution is presented in Table 3. The 41 most significant features are used as the input. We selected 41 neurons for the RaNN layers and 30 for the MLP layers. The simulation is executed for the same five learning rates that we used in the previous experiment. A detailed performance comparison is presented in Table 4. The accuracy comparison with different learning rates after ten-fold cross-validation for UNSW-NB15 dataset is presented in Figure 4. According to the results, the overall performance on the learning rates of 0.005, 1.00, and 1.50 is less than 98%. The best performance is achieved at a learning

TABLE 3. Distribution of attacks in the UNSW-NB15 dataset.

Class Name	Total	Training	Testing
Normal	93000	69750	23250
Fuzzers	24246	18185	6062
Backdoor	2329	1747	582
Analysis	2677	2008	669
Reconnaissance	13987	10490	3497
Exploits	44525	33394	11131
Generic	58871	44153	14718
Denial of Service	16353	12265	4088
Shellcode	1511	1133	378
Worms	174	131	44

TABLE 4. Performance evaluation of the proposed algorithm with the UNSW-NB15 dataset.

Performance	Learning Rates				
Parameters	0.005	0.01	0.75	1.00	1.50
Accuracy	0.9721	0.9793	0.9919	0.9523	0.9487
Precision	0.9718	0.9790	0.9907	0.9485	0.9463
Recall	0.9690	0.9772	0.9898	0.9498	0.9472
F1 Score	0.9704	0.9781	0.9902	0.9491	0.9467
Log Loss	0.4625	0.4235	0.1223	0.7223	1.0522
AUC-ROC	0.8054	0.8684	0.9882	0.7153	0.6220

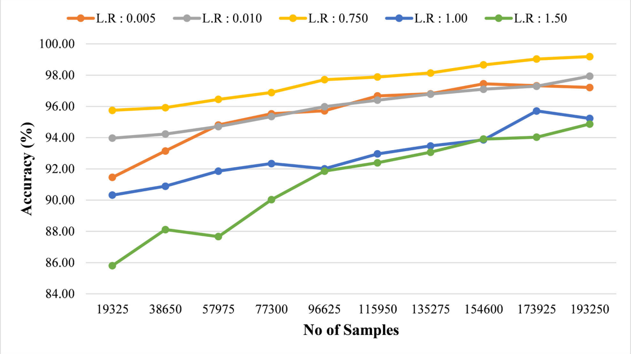


FIGURE 4. Comparitive analysis of accuracy with different learning rates for 10-fold cross validation using UNSW-NB15 dataset.

rate of 0.75. as shown in the accuracy comparison graph in Figure 5. According to the results, the best training and testing accuracies are achieved as 99.43% and 99.19% respectively. The other performance scores of the precision, recall, and F1 score that are achieved are 99.07%, 98.98%, and 99.10%, respectively. The log loss score is very low at 0.122, which indicates the best performance. The overall AUC-ROC is higher at 0.98, which represents that model achieved the best detection results. This dataset contains 9 different types of attacks. The attack classification is represented by the confusion matrix, as shown in Table 6. According to the confusion matrix, the proposed HDRaNN model classified "Generic", "Reconnaissance", "Analysis", "Worms" and "Backdoor" attacks with higher detection rates. In "Fuzzer", "Exploits", "Shellcode" and "DoS", 213, 1287, 22, and 368 samples are misclassified. In "Normal", 785 samples are misclassified as anomalous data. The overall performance of HDRaNN for UNSW-NB15 is excellent and better than that for DS2OS.

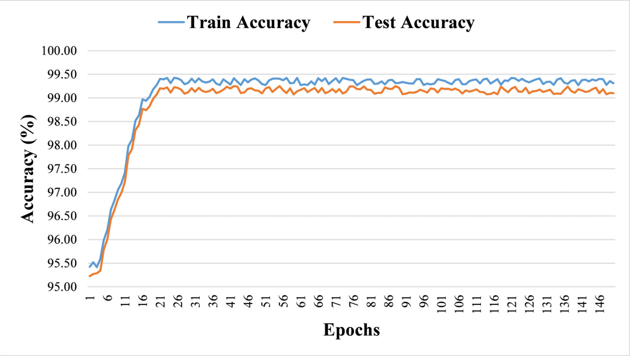


FIGURE 5. Best performance of the HDRaNN with the UNSW-NB15 dataset.

3) PERFORMANCE COMPARISON WITH STATE-OF-THE-ART ATTACK DETECTION ALGORITHMS

We tested four state-of-the-art deep learning algorithms, including the recurrent neural network (RNN), deep belief network (DBN), deep autoencoder (DAE), and restricted Boltzmann machine (RBM), on our preprocessed datasets using open source Python codes. For a better comparison with the HDRaNN, we maintained the test and training data split rates for both datasets and selected a moderate learning rate. A detailed performance comparison is presented in Table 7. For the DS2OS dataset, the DBN and DAE performed well, and the attack detection accuracies achieved were 97.89% and 98.13%, respectively. The attack detection accuracy and other performance scores of the RNN and RMB are less than 97% for the DS2OS dataset. The DAE achieved good performance for the UNSW-NB15 dataset with an attack detection accuracy of 98.75% and its other scores were also greater than 98%. The RNN, DBN, and RNN achieved overall scores ranging from 95% to 97%. To summarize this comparison, the performance of the proposed HDRaNN is superior for both datasets compared to the performances of other deep learning classifiers.

C. DEPLOYMENT PERSPECTIVE IN AN IIoT NETWORK

Different IoT applications such as smart factories, smart cities, and smart transportation etc. communicate with the network layer using different communication technologies. The network layer facilitates users' requests and provides internet services to individuals and industrial applications. The proposed attack detection approach can be deployed in the network layer to secure incoming and outgoing traffic. Our model is flexible and does not require any specific topology for its implementation. It can be integrated with an IIoT network according to the user's requirement. Since the proposed scheme consists of a lightweight deep learning algorithm, it can be easily implemented on a single board computer such as Raspberry Pi with a Neural Computing Stick (NCS) or low power ARM Cortex M4 processor-based development board. However, the HDRaNN cannot be directly trained on low-performance devices. Therefore, we train the model by using a high-power computing device

TABLE 5. Confusion matrix of the attack classification of the DS2OS dataset.

Classes	Normal	DoS	Malicious Control	Malicious Operation	Spying	Wrong Setup	Scan	Data Type Probing
Normal	86327	589	0	2	4	1	61	0
DoS	300	1125	2	2	0	1	15	0
Malicious Control	2	0	218	0	0	0	2	0
Malicious Operation	3	4	0	188	0	3	3	0
Spying	2	0	0	1	127	0	0	3
Wrong Setup	1	2	1	0	0	26	0	2
Scan	65	32	0	0	0	0	289	1
Data Type Probing	2	0	0	0	0	0	0	84

TABLE 6. Confusion matrix of the attack classification with the UNSW-NB15 dataset.

Classes	Normal	Fuzzers	Backdoor	Analysis	Reconnaissance	Exploits	Generic	DoS	Shellcode	Worms
Normal	22465	412	3	2	0	259	1	106	2	0
Fuzzers	160	5849	0	1	19	15	5	4	8	1
Backdoor	4	2	560	0	6	1	0	9	0	0
Analysis	8	0	3	652	0	0	1	3	0	2
Reconnaissance	16	7	0	0	3459	0	2	12	0	1
Exploits	12	793	1	0	8	9844	1	472	0	0
Generic	6	17	0	0	0	22	14673	0	0	0
DoS	220	63	4	2	0	78	0	3720	0	1
Shellcode	4	11	0	2	0	5	0	0	356	0
Worms	3	0	0	0	0	0	0	0	0	41

TABLE 7. Performance comparison with the state-of-the-art schemes.

DL Classifier	DS2OS					UNSW-NB15				
	Accuracy	Precision	Recall	F1 Score	Log Loss	Accuracy	Precision	Recall	F1 Score	Log Loss
RNN	0.9593	0.9562	0.9544	0.9553	0.8512	0.9535	0.9548	0.9545	0.9546	0.9876
DBN	0.9789	0.9792	0.9774	0.9783	0.7221	0.9710	0.9699	0.9701	0.9700	0.5827
DAE	0.9813	0.9826	0.9818	0.9822	0.4226	0.9875	0.9881	0.9869	0.9875	0.4322
RBM	0.9661	0.9643	0.9657	0.9650	0.5779	0.9725	0.9782	0.9755	0.9768	0.5674
HDRaNN	0.9856	0.9825	0.9836	0.9830	0.3624	0.9919	0.9907	0.9898	0.9902	0.1223

such as the Dell Alienware desktop computer used here. Then, the trained model is converted in a deployable graph file using some suitable software application. Finally, this graph file can be implemented in a Raspberry Pi or ARM Cortex M4 process using Python script.

V. CONCLUSION

IIoT cybersecurity is critical due to increasing number of IoT devices that generate a huge amount of data on insecure networks. DL-based schemes have great potential to address the security problems in IoT networks. In this paper, we presented a novel HDRaNN-based approach for cyberattack detection in IIoT. The proposed HDRaNN expolit the applications of a deep random neural network and multilayer perceptron. The proposed scheme is evaluated using IIOT security-related datasets i.e., DS2OS and UNSW-NB15. Several performance metrics such as the accuracy, recall, precision, F1 score, and log loss prove the superiority of the proposed scheme. The proposed HDRaNN classified 16 different types of attacks with an accuracy of more than 98% and 99% for DS2OS and UNSW-NB15 datasets, respectively. When compared with other DL-based scheme, all performance metrics were favour of the proposed scheme.

REFERENCES

[1] H. Boyes, B. Hallaq, J. Cunningham, and T. Watson, "The industrial Internet of Things (IIoT): An analysis framework," *Comput. Ind.*, vol. 101, pp. 1–12, Oct. 2018.

[2] 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.

[3] 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.

[4] 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.

[5] 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.

[6] 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.

[7] 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.

[8] 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.

[9] 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 multi-CNN fusion," *Measurement*, vol. 154, Mar. 2020, Art. no. 107450.

[10] 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.

[11] 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.

[12] 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.

[13] 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.

[14] 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.

[15] 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.

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

[17] 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.

[18] 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.

[19] 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. 107417.

[20] H. Huang, S. Ding, L. Zhao, H. Huang, L. Chen, H. Gao, and S. H. Ahmed, "Real-time fault detection for IIoT facilities using GBRBM-based DNN," *IEEE Internet Things J.*, vol. 7, no. 7, pp. 5713–5722, Jul. 2020.

[21] R. Taheri, M. Shojafar, M. Alazab, and R. Tafazolli, "FED-IIoT: A robust federated malware detection architecture in industrial IoT," *IEEE Trans. Ind. Informat.*, early access, Dec. 9, 2020, doi: 10.1109/TII.2020.3043458.

[22] M. Khoda, T. Imam, J. Kamruzzaman, I. Gondal, and A. Rahman, "Robust malware defense in industrial IoT applications using machine learning with selective adversarial samples," *IEEE Trans. Ind. Appl.*, vol. 56, no. 4, pp. 4415–4424, Aug. 2020.

[23] 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.

[24] 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

[25] M.-O. Pahl and F.-X. Aubet, "All eyes on you: Distributed multi-dimensional iot microservice anomaly detection," in *Proc. 14th Int. Conf. Netw. Service Manage. (CNSM)*, Nov. 2018, pp. 72–80.

[26] 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.

[27] E. Gelenbe, "Random neural networks with negative and positive signals and product form solution," *Neural Comput.*, vol. 1, no. 4, pp. 502–510, Dec. 1989.

[28] Y. Yin, "Deep learning with the random neural network and its applications," 2018, *arXiv:1810.08653*. [Online]. Available: http://arxiv.org/abs/1810.08653

[29] A. Tahir, J. Ahmad, G. Morison, H. Larijani, R. M. Gibson, and D. A. Skelton, "HRNN4F: Hybrid deep random neural network for multi-channel fall activity detection," *Probab. Eng. Informational Sci.*, vol. 35, pp. 1–14, Aug. 2019.

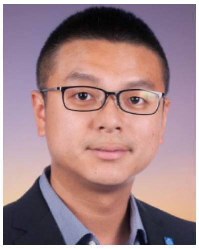
ZIL E. HUMA received the bachelor's degree in electrical engineering from HITEC University, Taxila, Pakistan, in 2017, and the master's degree in electrical engineering from the National University of Sciences and Technology (NUST), Islamabad, Pakistan, in 2020. During her master's studies, she worked on the design and development of non-linear energy management techniques for hybrid electric vehicles. Her major research interests include robotics, control, the Internet of Things, and electric vehicles.

SHAHID LATIF (Graduate Student Member, IEEE) received the B.Sc. and M.Sc. degrees in electrical engineering from HITEC University Taxila, Pakistan, in 2013 and 2018, respectively. He is currently pursuing the Ph.D. degree with the School of Information Science and Engineering, Fudan University, Shanghai, China. From 2015 to 2019, he served as a Lecturer with the Department of Electrical Engineering, HITEC University Taxila. During his Teaching Carrier, he has supervised several projects in the field of electronics, embedded systems, control systems, and the Internet of Things. He is currently working in the research area of cybersecurity of the Industrial Internet of Things (IIoT).

JAWAD AHMAD (Senior Member, IEEE) is currently an Experienced Researcher with more than ten years of cutting-edge research and teaching experience in prestigious institutes, including Edinburgh Napier University, U.K.; Glasgow Caledonian University, U.K.; Hongik University, South Korea; and HITEC University Taxila, Pakistan. During his career, he taught various courses both at undergraduate (UG) and postgraduate (PG) levels. He has coauthored more than 70 research papers, in international journals and peer-reviewed international conference proceedings. He regularly organizes timely special sessions and workshops for several flagship IEEE conferences. He is also an invited reviewer for numerous world-leading high-impact journals (reviewed more than 50 journal articles to date). His research interests include cybersecurity, multimedia encryption, machine learning, and application of chaos theory in cybersecurity.

ZEBA IDREES received the bachelor's degree in telecommunication engineering from Government College University Faisalabad, Pakistan, in 2012, and the master's degree in electrical engineering from the National University of Sciences and Technology (NUST), Islamabad, Pakistan, in 2014. She is currently pursuing the Ph.D. degree with the School of Information Science and Engineering, Fudan University, China. She possesses professional and research experience of more than five years in academia as well as industry. She was with FAST National University, as a Lecturer for one year and the Electrical Engineering Department, UET Lahore at Faisalabad, since 2015. Her current research interests include electronic circuits, wireless sensors networks and systems for ambient intelligence, cognitive radio networks, and the Internet of Things.

ANAS IBRAR received the B.Sc. degree in electrical engineering from HITEC University, Taxila, Pakistan, in 2013 and the M.Sc. degree in electrical engineering from Air University, Islamabad, Pakistan, in 2017. She is currently pursuing the Ph.D. degree with Wah Engineering College, University of Wah, Pakistan. Since 2017, she has been serving as a Lecturer with the Department of Electrical Engineering, Wah Engineering College, University of Wah. During her Teaching Carrier, she has supervised projects in the field of power electronics, control systems and the Internet of things (IoT). She is also working in the research area of observer based non-linear control and the Internet of Things.



ZHUO ZOU (Senior Member, IEEE) received the Ph.D. degree in electronic and computer systems from KTH Royal Institute of Technology, Sweden, in 2012. He has been an Adjunct Professor and a Docent with the University of Turku, Finland. He is currently with Fudan University, Shanghai, as a Professor, where he is conducting research on integrated circuits and systems for the IoT and ubiquitous intelligence. Prior to joining Fudan, he was the Assistant Director and a Project Leader with the VINN iPack Excellence Center, KTH, Sweden, where he coordinated the research project on ultra-low-power embedded electronics for wireless sensing. He is the Vice Chairman of IFIP WG-8.12.

FEHAID ALQAHTANI received the B.Sc. degree in computer science from King Khalid University, Saudi Arabia, in 2008, the M.Sc. degree in IT project management from Teesside University, U.K., in 2014, and the Ph.D. degree in computer science from the University of the West of Scotland, U.K., in 2020. He is currently an Assistant Professor with the Department of Computer Science, King Fahad Naval Academy, Ministry of Defense, Saudi Arabia. He has authored or coauthored several research papers, including leading international journals and peer-reviewed international conference proceedings. His research interests include affective computing and machine learning. He is also a Leading Team Member with the AI Society research committee, Saudi Arabia.

FATMAH BAOTHMAN received the Ph.D. degree in modern artificial intelligence (AI) from the School of Computing and Engineering, University of Huddersfield, in 2003. She is currently a Faculty Member with King Abdul Aziz University, Saudi Arabia. She is the first Saudi to join the Artificial Intelligence Global Educational Theater, and she led the project successfully in two academic institutes. She also participated in the 20th AI lab anniversary and the 50th AI anniversary among AI global scientists. She is a Member of G20-Taskforce4. She is also the Founder and the Board President of the AI Society, Saudi Arabia. She received the First Woman Internationally Awarded AI prize from the USA and U.K., and gained several trophies from different ministries and governmental bodies for her input on various occasions and programs.