Computers, Materials & Continua
DOI: 10.32604/cmc.2022.027483
Article

Tech Science Press

Hybrid Deep Learning Enabled Intrusion Detection in Clustered IIoT Environment

Radwa Marzouk[1], Fadwa Alrowais[2], Noha Negm[3], Mimouna Abdullah Alkhonaini[4], Manar Ahmed Hamza[5,*], Mohammed Rizwanullah[5], Ishfaq Yaseen[5] and Abdelwahed Motwakel[5]

[1]Department of Information Systems, College of Computer and Information Sciences, Princess Nourah Bint Abdulrahman University, Riyadh, 11671, Saudi Arabia
[2]Department of Computer Sciences, College of Computer and Information Sciences, Princess Nourah Bint Abdulrahman University, Riyadh, 11671, Saudi Arabia
[3]Department of Computer Science, College of Science & Art at Mahayil, King Khalid University, Abha, 62529, Saudi Arabia
[4]Department of Computer Science, College of Computer and Information Sciences, Prince Sultan University, Riyadh, 11586, Saudi Arabia
[5]Department of Computer and Self Development, Preparatory Year Deanship, Prince Sattam bin Abdulaziz University, AlKharj, Saudi Arabia
*Corresponding Author: Manar Ahmed Hamza. Email: ma.hamza@psau.edu.sa
Received: 18 January 2022; Accepted: 20 February 2022

Abstract: Industrial Internet of Things (IIoT) is an emerging field which connects digital equipment as well as services to physical systems. Intrusion detection systems (IDS) can be designed to protect the system from intrusions or attacks. In this view, this paper presents a novel hybrid deep learning with metaheuristics enabled intrusion detection (HDL-MEID) technique for clustered IIoT environments. The HDL-MEID model mainly intends to organize the IIoT devices into clusters and enabled secure communication. Primarily, the HDL-MEID technique designs a new chaotic mayfly optimization (CMFO) based clustering approach for the effective choice of the Cluster Heads (CH) and organize clusters. Moreover, equilibrium optimizer with hybrid convolutional neural network long short-term memory (HCNN-LSTM) based classification model is derived to identify the existence of the intrusions in the IIoT environment. Extensive experimental analysis is performed to highlight the enhanced outcomes of the HDL-MEID technique and the results were investigated under different aspects. The experimental results highlight the supremacy of the proposed HDL-MEID technique over recent state-of-the-art techniques.

Keywords: Industrial internet of things; security; intrusion detection; classification; deep learning

1 Introduction

The Industrial Internet of Things (IIoT) provides manufacturers in every industry with great connections that sequentially, generate intelligence and valuable information about the operation [1]. Through leveraging this intelligence, they are capable of manufacturing improvements and attaining significant efficiencies. The main objective of the IIoT is to exploit Internet of Things (IoT) technique in the industrial control system (ICS). ICS is an essential part of crucial infrastructure and has been employed for a longer period for supervising industrial processes and machines [2]. They implement real-time interacting and monitoring with the devices, realtime analysis, and collection of the information, in addition to sorting of each event that occurs in the industrial system [3]. Using IoT techniques in this system improves the network security and intelligence in the automation and optimization of industrial operations. But this extended network similarly opens up this recently interconnected device to substantial threat of cyber-attacks. Since industrial facility becomes closer integrated, attackers are getting increasingly complex, resultant in great vulnerability and bigger possibility of damaging cyber-attack [4]. Intrusion detection, the capacity to identify once attackers start searching devices, is the first critical stage to build a secured IIoT [5]. Intrusion Detection Solution (IDS) for IIoT must be personalized to the nature of the device [6]. Smaller devices with constrained resources want a personalized solution to the type of attack they are expected to encounter without over-whelming the computing resources and constrained memory of the devices. Fig. 1 shows the overview of clustered IIoT architecture.

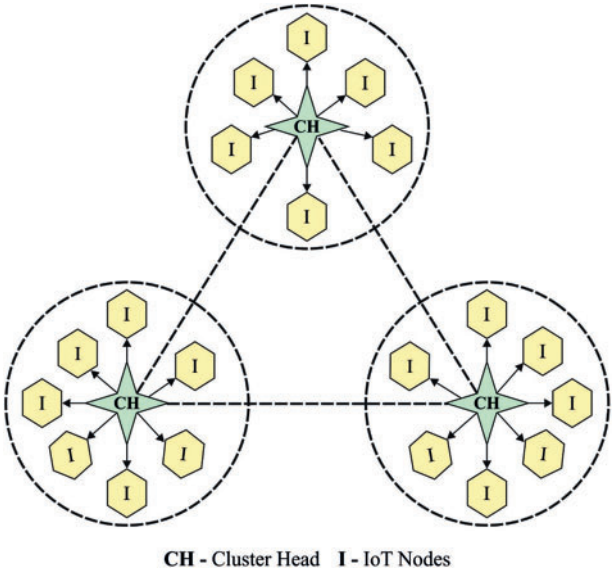

Figure 1: Clustered IoT environment

Simultaneously, the complexity of the IDS needs to scale up for supporting control and effective gateway systems [7]. Consequently, there is a need for building an adaptable architecture which could assist a wide-ranging device and simply personalized according to the requirements of the single network or device. In every case, the main step is to monitor for, quickly report, and detect anomaly traffics [8]. This needs incorporation with a security managing scheme in which IDS event is viewed and sent through an individual (or possibly an AI engine) to define whether the anomaly event indicates a cyberattack. On the IIoT, deep learning and machine learning approaches could improve

customer satisfaction, reliability, and production by merging technical innovation, sensor, program, and application [9,10].

Alkadi et al. [11] presented a deep blockchain framework (DBF) to provide privacy-based and blockchain security-based distributed ID with smart contracts in IoT systems. The IDS is assessed by the datasets and can be utilized by a deep learning (DL) approach for handling consecutive network data. Vargas et al. [12] incorporate the preceding solution to generate an essential security method for IoT devices that will activate secured data transfer mechanism, enable the detection of threat, and it will be adopted to the computation capability of industrial IoT. The presented method accomplished a feasible method for containing and detecting intruders in an IoT. In [13], a security architecture helps comprehensive protection for the IIoT through blockchain (BC) and Coalition Formation concept has been introduced. In addition, we support a traditional DL-based classification method for effectively categorizing benign and malicious devices in IIoT. In the presented method, only connections could be determined whether the information of the linking is mined on the BC by the "sender" device.

Awotunde et al. [14] presented a DL-based IDS for IIoT using hybrid rule-based FS for training and verifying data taken from TCP/IP packets. The trained progression has been performed by a hybrid rule-based feature selection and DL method. The suggested method was tested by using two common network data sets. Li et al. [15] presented a DL method for IDS with a multiple convolutional neural network (CNN) fusion model. Based on the relationship, the feature data are separated into four parts, later the 1D feature data are transformed into a grayscale graph. By utilizing the data visualization model, CNN is presented into the ID problem and the best of the four outcomes arise. Latif et al. [16] introduced a deep random neural (DRaNN) based system for IDS in IIoT. The presented method is estimated through a novel generation IIoT security datasets UNSW-NB15. The experiment result proves that our presented model effectively categorized nine distinct kinds of attacks.

This paper presents a novel hybrid deep learning with metaheuristics enabled intrusion detection (HDL-MEID) technique for clustered IIoT environments. The HDL-MEID model designs a new chaotic mayfly optimization (CMFO) based clustering approach for the effective choice of the Cluster Heads (CH) and organizing clusters. Moreover, equilibrium optimizer with hybrid CNN long short-term memory (HCNN-LSTM) based classification model is derived to identify the existence of the intrusions in the IIoT environment. Extensive experimental analysis is performed to highlight the enhanced outcomes of the HDL-MEID technique and the results were investigated under different aspects.

2 The Proposed Model

This paper has presented a new HDL-MEID technique to organize the IIoT devices into clusters and allow secure communication with intrusion detection in clustered IIoT environments. Initially, the HDL-MEID technique designed an effective CMFO based clustering technique with HCNN-LSTM based intrusion detection. The proposed model utilizes IDS technology to enable secure communication and HCNN-LSTM model to identify the existence of intrusions in the IIoT environment.

2.1 Level I: CMFO Based Clustering Technique

Primarily, the CMFO algorithm is applied for the choice of CHs and organizing clusters. The MFO algorithm is based on the social behavior of the mayflies (MFs). Each candidate alters the trajectory based on the optimal position and optimal position to every MFs. The gathering of the male MMs (MMFs) reflected the understanding of every MMF in computing the position based on

the nearby positions [17]. Consider x_i^t as the present position of a candidate solution i at iteration t, the position can be modified through the inclusion of the velocity v_i^{t+1} as given below.

$$x_i^{t+1} = x_i^t + v_i^{t+1} \tag{1}$$

With $x_i^0 U\left(x_{min}, x_{max}\right)$.

With the consideration of the low velocity of the MMF population, the velocity is defined as follows.

$$v_{ij}^{t+1} = v_{ij}^t + a_1 e^{-\beta r_p^2}\left(pbest_{ij} - x_{ij}^t\right) + a_2 e^{-\beta r_g^2}\left(gbest_i - x_{ij}^t\right) \tag{2}$$

where v_{ij}^t implies the velocity of MF i, x_{ij}^t indicates the position of MF i, a_1 and a_2 are positive constants indicating attractiveness. $pbest_i$ indicates optimal position that a candidate solution i attained, and $pbest_{ij}$ at the following step $t+1$ can be determined using Eq. (3).

$$pbest_i = \{x_i^{t+1},\ if\ f\left(x_i^{t+1}\right) < f\left(pbest_i\right)\ same\ as\ before,\ otherwise \tag{3}$$

where $f : R^n \Rightarrow R$ indicates the minimization function, $gbest$ denotes the global optima attained iteration t. The coefficient restricted the population reflectiveness. r_p signifies the distance among x_i and $pbest_i$. In addition, r_g denotes the distance from x_i to $gbest$. r_p and r_g can be computed as follows.

$$\|x_i - X_i\| = \sqrt{\sum_{j=1}^{n}\left(x_{ij} - X_{ij}\right)^2} \tag{4}$$

where x_{ij} is the j^{th} component of the i^{th} candidate. X_i is linked pbest. The optimal fitting candidate sustains by carrying out the upward and downward movement via adjusting the velocity, which can be computed using Eq. (5):

$$v_{ij}^{t+1} = v_{ij}^t + d * r \tag{5}$$

where d denotes a coefficient linked to upward and downward movement; and r is an arbitrary value. The female MFs (FMFs) do not gather however it moves in the direction of MMFs. Consider y_i^t as the present position of FMF i at iteration t. The variation in position can be defined as follows.

$$y_i^{t+1} = y_i^t + v_i^{t+1} \tag{6}$$

with $y_i^0 U\left(x_{min}, x_{max}\right)$.

The FMFs' velocity can be computed using Eq. (7).

$$v_{ij}^{t+1} = \{v_{ij}^t + a_2 e^{-\beta r_{mf}^2}\left(x_{ij}^t - y_{ij}^t\right),\ iff\ \left(y_i\right) > f\left(x_i\right)\ \ v_{ij}^t + fl * r,\ if\ f\left(y_i\right) \le f\left(x_i\right) \tag{7}$$

where v_{ij}^t implies the velocity of the i^{th} female at iteration t.

Crossover operation is employed as the mutation function. A set of male as well as female parents is selected and produces offspring as given below.

$$offspringl = L * male + (1 - L) * female$$

$$offspring2 = L * female + (1 - L) * male \tag{8}$$

where L is an arbitrary number.

The chaotic order is generated using the logistic map [18], as given below.

$$x_{i+1} = ux_i\,(1 - x_i) \tag{9}$$

u denotes control parameter and implies a chaotic state. The primary MF population undergoes mapping in a chaotic way. The CMFO algorithm derives a fitness function with four parameters namely $f1, f2, f3$, and $f4$. The objective function to elect CHs is given as follows.

$$F = Maximize\ Fitness = \alpha * f_1 + \beta * f_2 + \gamma * \frac{1}{f_3} + \delta * \frac{1}{f_4} \tag{10}$$

where α, β, γ, & δ indicates weight coefficients of f_1, f_2, f_3, & f_4 FF variables lie in the range of [0, 1]. Here, f_1, f_2, f_3, & f_4 indicates energy efficiency, node density, average intra-cluster distance, and inter-cluster distance.

2.2 Level II: HCNN-LSTM Based Intrusion Detection Approach

At this stage, the HCNN-LSTM based intrusion detection technique is applied for determining the existence of intrusions in the network. The standard CNN infrastructure basically has convolution, pooling, and fully connected (FC) layers [19]. The LSTM network is a class of recurrent neural networks (RNN) which utilizes memory block which supports running effectively and learning faster than typical RNN. The LSTM network defines practical solutions to vanish and explode gradient problems of RNNs. Besides the RNN, a cell state was utilized from the LSTM network for saving long-term conditions containing input, forget, and output gates. Therefore, the network is remember preceding data and attaches it with present ones. In addition, it resolves difficult tasks complex for determining a solution by preceding RNNs. A CNN-LSTM method is a group of CNN layers which remove the feature in input data and LSTM layer for providing sequence forecast, as shown in Fig. 2. It can be considered that infrastructure of our method with 9 layers: input layer, 4 CNN layers wrapped by time-distributed layer, LSTM layer, dense layer, dropout layer, and output layer correspondingly. If every data is padding and vectorizing, the network developed is arranged to the feature extracting method.

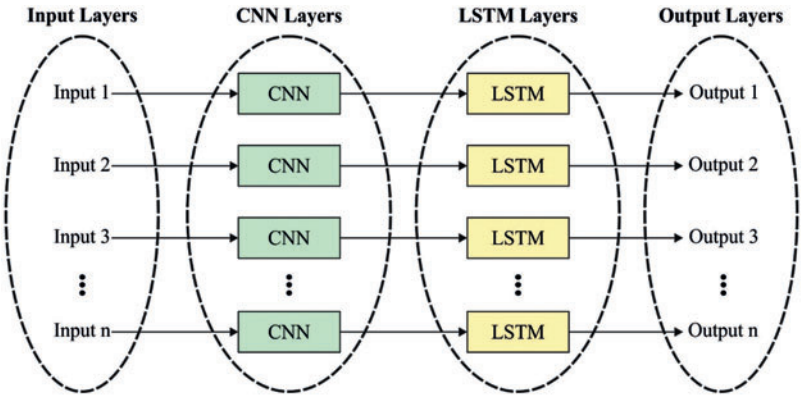

Figure 2: Structure of CNN-LSTM model

During this phase, 3 convolution layers are utilized for automatically extracting features in input orders utilizing the rectified linear unit (ReLU) activation function. During these convolution layers, 128 filters are utilized. The kernel height is chosen as 6 and kernel width is chosen 4 to convolutional function. This kernel size provides maximum efficiency. During these convolution steps. It can be

wrapped the convolutional layers from time-distributed wrapper for reshaping input data by more dimensional finally. In order to concatenation of every extracting feature, it can be utilized a fatten layer to pass the LSTM layer.

Afterward, 1 LSTM layer has been structured with 100 units subsequent to a dropout layer (0.5) on FC layer. Lastly, to binary classification, the softmax activation function is utilized to specify output. This technique is optimization for 30 epochs, 6 for batch size, and 0.1 for validation split with trained. The validation data set monitor the convergence from the trained procedure thus the trained technique is canceled early based on the modification under this convergence. In addition, Adam optimizing with 0,001 rates of learning to optimized and categorical cross entropy (CE) to loss function is chosen under the optimized procedure. Adam is most gradient descent technique which computes adaptive learning rate to all momentums as parameter and categorical CE is most loss function chosen if there are more than two one hot encoding label classes. It optimizes multi-class classifier techniques with softmax activation functions.

2.3 Level III: Hyperparameter Tuning

For optimally tuning the hyperparameters of the HCNN-LSTM model, the EO algorithm can be utilized. The EO algorithm is stimulated by the law of physics, which can be used to solve the optimization problem [20]. The EO algorithm can be mathematically formulated as follows. At the time of initialization, the EO algorithm utilizes a collection of particles, where every individual one indicates a concentration vector comprising solution. The primary concentration vector is arbitrarily produced in the search space by the use of Eq. (11):

$$\vec{v} = c_{min} + (c_{max} - c_{min}) * ri = 0, 1, 2, \ldots, n \tag{11}$$

where $\vec{v}_i$ indicates the concentration vector, c_{min}, c_{max} are minimum and maximum limits for all dimensions. r a is an arbitrary number of n indicates the particle count in the set. Then, the candidate solutions are saved in a vector, named as equilibrium pool, as given below.

$$\vec{p}_{eq,pool} = \left[\vec{p}_{eq(1)}, \vec{p}_{eq(2)}, \vec{p}_{eq(3)}, \vec{p}_{eq(4)}, \vec{p}_{eq(5)}\right] \tag{12}$$

For concentration updates, the EO algorithm holds a reasonable tradeoff among intensification as well as diversification. As turnover rate varied over time in a real control volume, $\vec{\lambda}$ can be represented as an arbitrary vector in the range of 0 to 1.

$$\vec{F} = e^{-\vec{\lambda}(t-t_0)} \tag{13}$$

where t gets reduced with a rise in iteration (it) by the use of Eq. (14):

$$t = (1 - \frac{it}{t_{max}})^{(a2*(\frac{it}{t\,max}))} \tag{14}$$

where it and t_{max} denotes the present and higher iteration. Also, $a2$ is a constant value employed for controlling the exploitation abilities.

$$\vec{t}_0 = \frac{1}{\vec{\lambda}} ln\left(-a_1 sign\left(\vec{r} - 0.5\right)\left[1 - e^{-\vec{\lambda}t}\right)\right) + t \tag{15}$$

The generation rate (R) can be utilized for improving the intensification operator as given below:

$$\overrightarrow{R} = \overrightarrow{R}_0 * e^{-\vec{\lambda}*(t-t_0)} \tag{16}$$

where $\vec{\lambda}$ denotes an arbitrary vector and $\overrightarrow{R}_0$ indicates initial value as given below:

$$\overrightarrow{R}_0 = \overrightarrow{RCP} * \left(\overrightarrow{c_{eq}} - \vec{\lambda} * \overrightarrow{C}\right) \tag{17}$$

$$\overrightarrow{RCP} = \{0.5r_1\ r_2 > RP\ 0\ otherwise' \tag{18}$$

where r_1 and r_2 denotes arbitrary numbers in the range of [0, 1]. Here, $\overrightarrow{RCP}$ vector denotes the generation rate control variable. Lastly, the EO algorithm can update using Eq. (19):

$$\overrightarrow{C} = \overrightarrow{c_{eq}} + \left(\tilde{C} - \overrightarrow{c_{eq}}\right) * F \rightharpoonup + \frac{\vec{R}}{\vec{\lambda} * V} * \left(1 - \vec{F}\right) \tag{19}$$

where V is equivalent to 1.

3 Results and Discussion

The performance validation of the HEL-MEID technique takes place under several aspects. Fig. 3 inspects the packet delivery ratio (PDR) analysis of the HEL-MEID technique is compared with other techniques [21,22] under distinct sensor nodes (SNs).

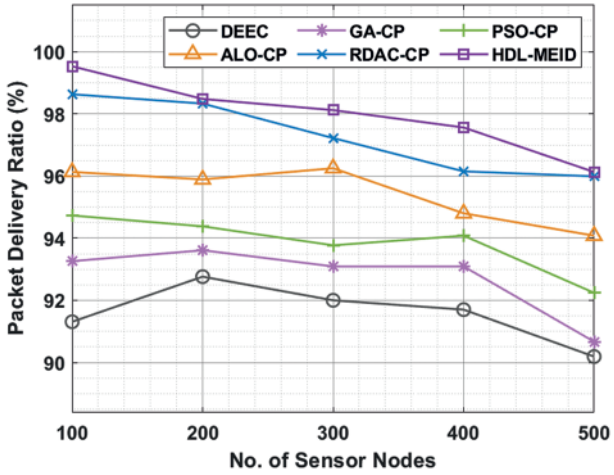

Figure 3: Comparative PDR analysis of HDL-MEID with recent models

The results demonstrate that the HEL-MEID technique has attained higher PDR under all SNs. For instance, with 100 SNs, the HEL-MEID technique has offered higher PDR of 99.53% whereas the DEEC, GA-CP, PSO-CP, ALO-CP, and RDAC-CP techniques have obtained lower PDR of 91.31%, 93.26%, 94.73%, 96.13%, and 98.63% respectively. Along with that, with 500 SNs, the HEL-MEID technique has resulted in maximum PDR of 96.13% whereas the DEEC, GA-CP, PSO-CP, ALO-CP, and RDAC-CP techniques have reached minimal PDR of 90.19%, 90.67%, 92.24%, 94.08%, and 95.99% respectively.

Fig. 4 illustrates throughput (THRP) analysis of the HEL-MEID technique with recent models under varying SNs. The results indicated the betterment of the HEL-MEID technique with increased THRP under every SN. For instance, with 100 SNs, the HEL-MEID technique has provided improved THRP of 97.84% whereas the DEEC, GA-CP, PSO-CP, ALO-CP, and RDAC-CP techniques have reached lower THRP of 67.17%, 73.31%, 80.34%, 88.82%, and 96.54% respectively. In line with, with 500 SNs, the HEL-MEID technique has depicted increased THRP of 96.13% whereas the DEEC,

GA-CP, PSO-CP, ALO-CP, and RDAC-CP techniques have exhibited decreased THRP of 54.18%, 62.41%, 70.53%, 77.81%, and 85.49% respectively.

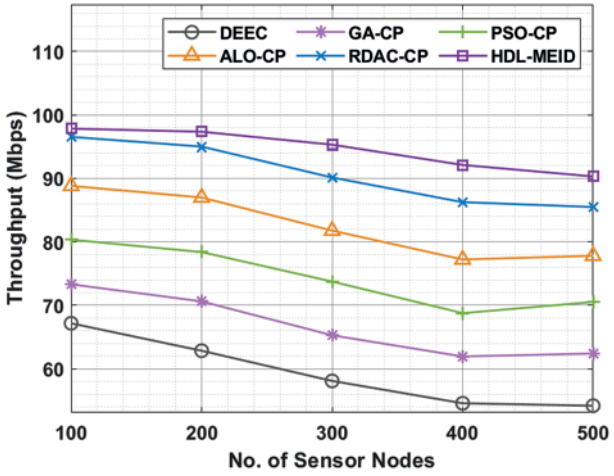

Figure 4: Comparative THRP analysis of HDL-MEID with recent models

An energy consumption (ECM) analysis of the HDL-MEID technique with compared methods is offered in Fig. 5. The figure portrayed the enhanced outcomes of the HEL-MEID technique with minimal ECM under every round. For instance, with 100 SNs, the HEL-MEID technique has reached to least ECM of 0.00654 mJ whereas the DEEC, GA-CP, PSO-CP, ALO-CP, and RDAC-CP techniques have resulted in increased ECM of 0.2615, 0.2056, 0.1757, 0.1326, and 0.0974 mJ respectively. In addition, with 500 SNs, the HEL-MEID technique has displayed lower ECM of 0.3546 MJ whereas the DEEC, GA-CP, PSO-CP, ALO-CP, and RDAC-CP techniques have revealed increased ECM of 0.8158, 0.7755, 0.6326, 0.5778, and 0.4440 respectively.

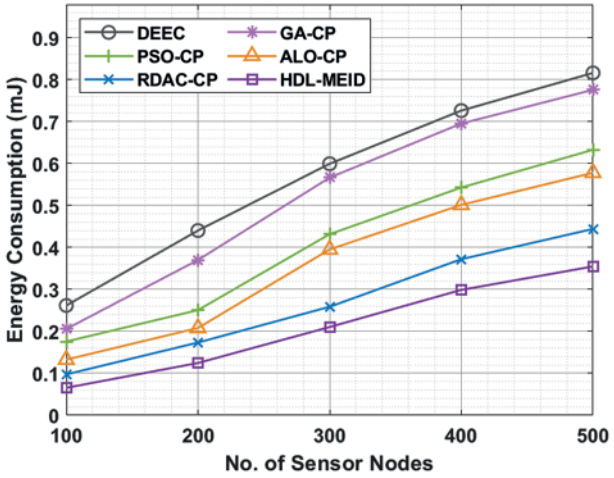

Figure 5: Comparative ECM analysis of HDL-MEID with recent models

Fig. 6 exemplifies network lifetime (NLFT) analysis of the HEL-MEID technique with latest models under varying SNs. The results designated the improvement of the HEL-MEID technique with amplified NLFT under every SN. For instance, with 100 SNs, the HEL-MEID technique has extended

NLFT of 1860 rounds whereas the DEEC, GA-CP, PSO-CP, ALO-CP, and RDAC-CP techniques have offered reduced NLFT of 1214, 1260, 1337, 1473, and 1556 rounds respectively. Furthermore, with 500 SNs, the HEL-MEID technique has depicted increased NLFT of 3794 rounds whereas the DEEC, GA-CP, PSO-CP, ALO-CP, and RDAC-CP techniques have exhibited decreased NLFT of 2912, 3035, 3107, 3245, and 3325 rounds respectively.

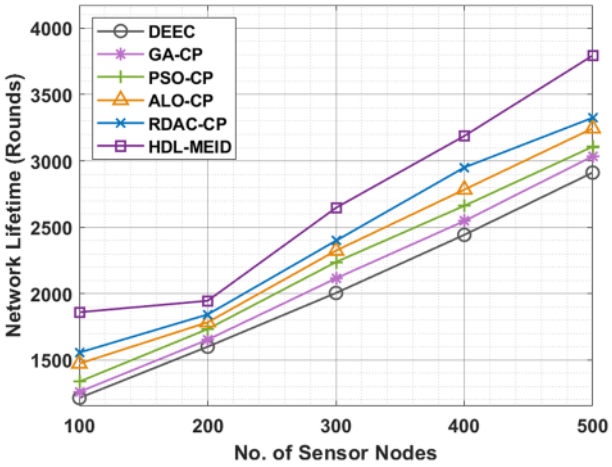

Figure 6: Comparative NLFT analysis of HDL-MEID with recent models

Fig. 7 performs a comparative number of alive SNs (NASN) analysis of the HEL-MEID technique with existing techniques under distinct rounds. The experimental results reported the better outcomes of the HEL-MEID technique with increased NASN under every round. For instance, with 400 rounds, the HEL-MEID technique has attained higher NASN of 500 whereas the DEEC, GA-CP, PSO-CP, ALO-CP, and RDAC-CP techniques have achieved decreased NASN of 354, 362, 386, 417, and 498 respectively. Moreover, with 500 SNs, the HEL-MEID technique has exhibited maximum NASN of 168 whereas the DEEC, GA-CP, PSO-CP, ALO-CP, and RDAC-CP techniques have shown reduced NASN of 2, 3, 4, 2, and 131 respectively.

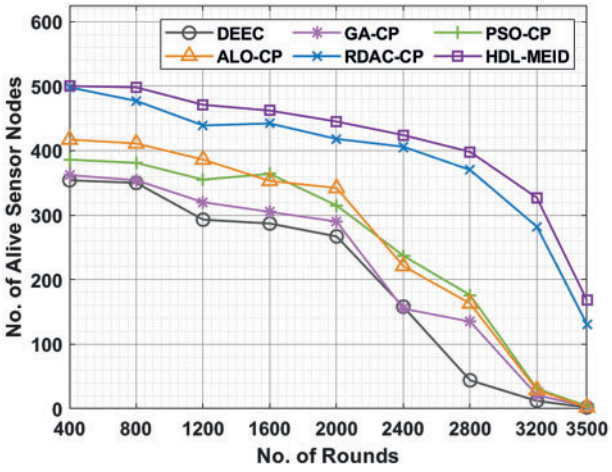

Figure 7: Comparative NASN analysis of HDL-MEID with recent models

Fig. 8 offers a comparative number of dead SN (NDSN) analyses of the HEL-MEID technique with existing techniques under distinct rounds. The figure implied that the HEL-MEID technique has resulted in effectual outcome with least NDSN under every round. For instance, with 400 rounds, the HEL-MEID technique has attained lower NDSN of 0 whereas the DEEC, GA-CP, PSO-CP, ALO-CP, and RDAC-CP techniques have resulted in raised NDSN of 146, 138, 114, 83, and 2 respectively.

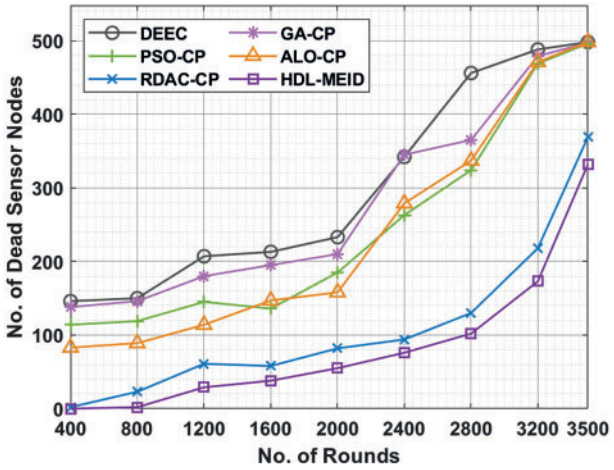

Figure 8: Comparative NDSN analysis of HDL-MEID with recent models

The intrusion detection results of the HDL-MEID technique are validated using the NSL-KDD 2015 dataset. Tab. 1 and Fig. 9 provide the classification result analysis of the HDL-MEID technique with existing techniques [23]. The results indicated that the KNN, SVM, and LR techniques have reached lower intrusion detection outcomes. At the same time, the RF and DNN models have attained considerably improved intrusion classification performance. Followed by, the DT model has resulted in near optimal intrusion detection results with the precision of 0.9218, recall of 0.6402, accuracy of 0.7881, and F1-score of 0.7556. However, the HDL-MEID technique has resulted in maximum intrusion detection performance with the precision of 0.9856, recall of 0.9424, accuracy of 0.9532, and F1-score of 0.9264.

Table 1: Intrusion detection results of HDL-MEID with other techniques

Methods	Precision	Recall	Accuracy	F1-score
KNN algorithm	0.9218	0.6402	0.7881	0.7556
DT algorithm	0.9737	0.7801	0.8956	0.8662
RF algorithm	0.9722	0.6289	0.8029	0.7637
SVM algorithm	0.9226	0.5676	0.7638	0.7028
DNN algorithm	0.9149	0.7801	0.8533	0.8421
LR algorithm	0.8923	0.6122	0.7634	0.7262
HDL-MEID	0.9856	0.9424	0.9532	0.9264

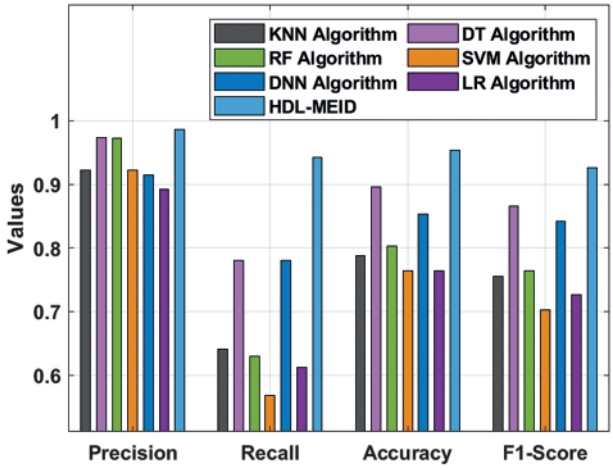

Figure 9: Comparative intrusion detection results of HDL-MEID with other techniques

Finally, a computation time (CT) analysis of the HDL-MEID with recent models is made in Tab. 2. The results demonstrated that the SVM model has accomplished least performance with the CT of 28.7 min whereas the KNN and DNN methods have obtained slightly reduced CT of 4.717 and 3.950 min respectively. At the same time, the DT and RF techniques have resulted in moderately closer CT of 0.028 and 0.040 min respectively. But the HDL-MEID technique has accomplished superior results with the least CT of 0.018 min. From the detailed result analysis, it is ensured that the HDL-MEID technique has outperformed the existing methods in the IIoT environment.

Table 2: Computation time (CT) results of HDL-MEID with other techniques

Methods	Time (min)
KNN algorithm	4.717
DT algorithm	0.028
RF algorithm	0.040
SVM algorithm	28.700
DNN algorithm	3.950
LR algorithm	1.050
HDL-MEID	0.018

4 Conclusion

This paper has presented a new HDL-MEID technique to organize the IIoT devices into clusters and allow enabled secure communication with intrusion detection in clustered IIoT environments. Initially, the HDL-MEID technique designed an effective CMFO based clustering technique with HCNN-LSTM based intrusion detection. The proposed model utilizes IDS technology to enable secure communication and HCNN-LSTM model to identify the existence of intrusions in the IIoT environment. Extensive experimental analysis is performed to highlight the enhanced outcomes of the HDL-MEID technique and the results were investigated under different aspects. The experimental results highlight the supremacy of the proposed HDL-MEID technique over recent state-of-the-art

techniques. As a part of future scope, lightweight cryptographic solutions can be derived to boost security in the IIoT environment.

Acknowledgement: The authors would like to acknowledge the support of Prince Sultan University for paying the Article Processing Charges (APC) of this publication.

Funding Statement: The authors extend their appreciation to the Deanship of Scientific Research at King Khalid University for funding this work under Grant Number (RGP 2/42/43). Princess Nourah bint Abdulrahman University Researchers Supporting Project Number (PNURSP2022R77), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] Q. Wang, X. Zhu, Y. Ni, L. Gu and H. Zhu, "Blockchain for the IoT and industrial IoT: A review," *Internet of Things*, vol. 10, pp. 100081, 2020.

[2] T. Alladi, V. Chamola, R. M. Parizi and K. R. Choo, "Blockchain applications for industry 4.0 and industrial iot: A review," *IEEE Access*, vol. 7, pp. 176935–176951, 2019.

[3] S. Dwivedi, P. Roy, C. Karda, S. Agrawal and R. Amin, "Blockchain-based internet of things and industrial iot: A comprehensive survey," *Security and Communication Networks*, vol. 2021, pp. 1–21, 2021.

[4] S. Tang, L. Chen, K. H. Xia, L. Fan and A. Nallanathan, "Computational intelligence and deep learning for next-generation edge-enabled industrial IoT," arXiv preprint arXiv:2110.14937, 2021.

[5] J. Huang, L. Kong, G. Chen, M. Y. Wu, X. Liu *et al.,* "Towards secure industrial iot: Blockchain system with credit-based consensus mechanism," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 6, pp. 3680–3689, 2019.

[6] E. S. Lohan, M. Koivisto, O. Galinina, S. Andreev, A. Tolli *et al.,* "Benefits of positioning-aided communication technology in high-frequency industrial IoT," *IEEE Communications Magazine*, vol. 56, no. 12, pp. 142–148, 2018.

[7] D. Mazzei, G. Baldi, G. Fantoni, G. Montelisciani, A. Pitasi *et al.,* "A blockchain tokenizer for industrial IOT trustless applications," *Future Generation Computer Systems*, vol. 105, pp. 432–445, 2020.

[8] Z. Lv, Y. Han, A. K. Singh, G. Manogaran and H. Lv, "Trustworthiness in industrial IoT systems based on artificial intelligence," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 2, pp. 1496–1504, 2021.

[9] E. Aydogan, S. Yilmaz, S. Sen, I. Butun, S. Forsstrom *et al.,* "A central intrusion detection system for rpl-based industrial internet of things," in *2019 15th IEEE Int. Workshop on Factory Communication Systems (WFCS)*, Sundsvall, Sweden, pp. 1–5, 2019.

[10] 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 of Things Journal*, vol. 6, no. 4, pp. 6822–6834, 2019.

[11] O. Alkadi, N. Moustafa, B. Turnbull and K. -K. R. Choo, "A deep blockchain framework-enabled collaborative intrusion detection for protecting iot and cloud networks," *IEEE Internet Things Journal*, vol. 8, no. 12, pp. 9463–9472, 2021.

[12] H. Vargas, C. L. Garzon, G. A. Montoya and Y. Donoso, "Detection of security attacks in industrial iot networks: A blockchain and machine learning approach," *Electronics*, vol. 10, no. 21, pp. 2662, 2021.

[13] M. Sharma, S. Pant, D. K. Sharma, K. D. Gupta, V. Vashishth *et al.,* "Enabling security for the industrial internet of things using deep learning, blockchain, and coalitions," *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 7, 2021.

[14] J. B. Awotunde, C. Chakraborty and A. E. Adeniyi, "Intrusion detection in industrial internet of things network-based on deep learning model with rule-based feature selection," *Wireless Communications and Mobile Computing*, vol. 2021, pp. 1–17, 2021.
[15] Y. Li, Y. Xu, Z. Liu, H. Hou, Y. Zheng *et al.,* "Robust detection for network intrusion of industrial IoT based on multi-CNN fusion," *Measurement*, vol. 154, pp. 107450, 2020.
[16] S. Latif, Z. Idrees, Z. Zou and J. Ahmad, "DRaNN: A deep random neural network model for intrusion detection in industrial IoT," in *2020 Int. Conf. on UK-China Emerging Technologies (UCET)*, Glasgow, United Kingdom, pp. 1–4, 2020.
[17] K. Zervoudakis and S. Tsafarakis, "A mayfly optimization algorithm," *Computers & Industrial Engineering*, vol. 145, pp. 106559, 2020.
[18] J. Gupta, P. Nijhawan and S. Ganguli, "Parameter estimation of fuel cell using chaotic mayflies optimization algorithm," *Advanced Theory and Simulations*, vol. 4, no. 12, pp. 2100183, 2021.
[19] T. Y. Kim and S. -B. Cho, "Predicting residential energy consumption using CNN-LSTM neural networks," *Energy*, vol. 182, pp. 72–81, 2019.
[20] A. Faramarzi, M. Heidarinejad, B. Stephens and S. Mirjalili, "Equilibrium optimizer: A novel optimization algorithm," *Knowledge-Based Systems*, vol. 191, pp. 105190, 2020.
[21] G. N. Nguyen, N. H. Le Viet, A. F. S. Devaraj, R. Gobi and K. Shankar, "Blockchain enabled energy efficient red deer algorithm based clustering protocol for pervasive wireless sensor networks," *Sustainable Computing: Informatics and Systems*, vol. 28, pp. 100464, 2020.
[22] C. Han, Q. Lin, J. Guo, L. Sun and Z. Tao, "A clustering algorithm for heterogeneous wireless sensor networks based on solar energy supply," *Electronics*, vol. 7, no. 7, pp. 103, 2018.
[23] Y. Tang, L. Gu and L. Wang, "Deep stacking network for intrusion detection," *Sensors*, vol. 22, no. 1, pp. 25, 2021.