ISSN 1330-3651 (Print), ISSN 1848-6339 (Online)
https://doi.org/10.17559/TV-20250204002328
Original scientific paper

Chaos Mapping and Marine Predators Algorithm-Based Deep Learning Framework for Intrusion Detection in IIoT Networks

G. ANITHA*, Hariprasath MANOHARAN, Abirami MANOHARAN

Abstract: The Industrial Internet of Things (IIoT) extends IoT applications to industrial environments, driving significant enhancements in operational efficiency. However, this evolution brings heightened cybersecurity risks, posing challenges to the protection of IIoT systems. To address these issues, this study introduces a novel Chaos Mapping and Marine Predators Algorithm-based Deep Learning Intrusion Detection System (CMPADL-IDS). The proposed model employs a two-stage process: feature selection using Chaos Mapping and the Marine Predators Algorithm (CMPA) and anomaly detection using a Long Short-Term Memory Autoencoder (LSTM-AE). The CMPA effectively identifies optimal features by leveraging chaotic systems and MPA's intelligent optimization capabilities. For enhanced performance, Bayesian Optimization (BO) is employed to fine-tune LSTM-AE hyperparameters, optimizing detection accuracy and computational efficiency. The framework was tested on the ToN-IoT dataset and managed to reach an average accuracy of 98.40%, a precision of 80.30%, a recall of 77.80%, an F1-score of 78.62% and an AUC score of 88.80%. The evaluation proves that using the suggested feature selection and anomaly detection techniques improves IIoT network security more than existing methods.

Keywords: chaos mapping; industrial internet of things (IIoT); intrusion detection system (IDS); long short-term memory autoencoder (LSTM-AE); marine predators algorithm (MPA)

1 INTRODUCTION

IIoT has advanced fast and helped industrial systems by linking numerous devices, sensors and systems. In addition, using the internet more often has brought attention to many cybersecurity challenges. Because IIoT networks are big, active and consist of various elements, they are more vulnerable to cyber-attacks. These weaknesses can lead to serious disturbances in a company's work, significant financial losses or the destruction of important structures. IDS systems based on traditional approaches are not precise enough for IIoT because the environment changes rapidly and is very complicated. That is the reason why we need strong IDS models that detect complex threats without taking up too much of the system's resources [1-3]. This paper suggests using the CMPADL-IDS (Chaotic Mapping and Marine Predator Algorithm-based Deep Learning Intrusion Detection System) in IIoT applications. The CMPADL-IDS relies on chaotic mapping and the Marine Predator Algorithm (MPA) to pick the key features for intrusion detection, as shown in Fig. 1.

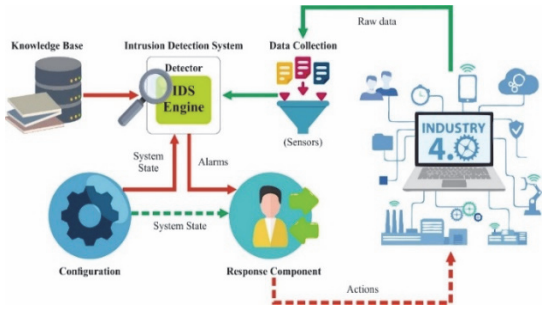

Figure 1 Structure of IDS in IIoT environment

Using this system, it becomes simpler to find issues and enhance the system's performance. An LSTM-AE model is used to study the features and look for unusual incidents in traffic by finding complicated patterns over time. Bayesian Optimization (BO) is applied to change the hyperparameters of the LSTM-AE model to make it work more efficiently [4-7]. The effectiveness of the system is verified by using the ToN-IoT dataset [21] which contains a lot of samples for both normal and attack-related traffic. The research results demonstrate that CMPADL-IDS is better than other IDS models in threat detection, accuracy, precision, recall and the resources it needs. By relying on advanced feature selection and deep learning in anomaly detection, CMPADL-IDS can protect IIoT networks from more dangerous cyber-attacks.

2 RELATED WORKS

Recently, people have become more worried about the safety of IIoT networks which has prompted more studies on how to create strong Intrusion Detection Systems (IDS). Various approaches such as ML, DL and combining them have been recommended to enhance the performance of IDS in IIoT networks [8].Many people are paying close attention to deep learning-based anomaly detection. There are many studies that recommend using stacked autoencoders (SAEs) to detect complex issues in IIoT data as soon as it is gathered. In fact, some authors have developed SAE-based models that efficiently identify advanced persistent threats (APTs) in industrial areas. They rely on stacked autoencoders to discover both challenging features and hidden patterns in IIoT data which makes it easier for them to detect attacks that other methods might miss [9].

Certain studies have also looked at applying improved autoencoder-based architectures for detecting intrusions in IIoT networks. Usually, these models use a mix of loss functions that enhance their ability to detect hidden anomalies and at the same time decrease the number of false alarms. As a result, IDS becomes more accurate and reliable because it does not often detect normal network traffic as malicious. According to the studies, autoencoder models are much better than traditional IDS methods at detecting low-frequency and unknown attacks [10].

Federated learning progress has also been considered for the purpose of intrusion detection in edge-enabled IoT networks. The authors suggest using a federated attention neural network (FANN) to deal with privacy and data

protection issues in distributed IoT systems. Since the processing is done on edge devices, federated learning saves on communication and still ensures accuracy in detection across many devices. This design boosts privacy and scalability and also makes it possible to train intrusion detection models using data that is not centralized [11-13].

One more technique is to use both deep learning and focal loss functions to enhance the detection of intrusions in IoT networks. If attack traffic is much less than benign traffic, focal loss helps to solve the issue of class imbalance. This approach helps the model spot even the most uncommon but significant security dangers [14-16].

Although there have been many improvements, it is still difficult to create efficient IDS for IIoT systems. In addition, most of the current methods are still very complex which makes them less suitable for real-time use in large-scale and resource-limited IIoT systems. Secondly, most models work well for known threats, but they tend to have difficulty detecting new or unknown attacks which are becoming a bigger issue as cybersecurity threats keep changing. Traditional IDS systems are not well-suited for IIoT networks because they do not handle the changing and different types of data on these networks [15-17].

Although deep learning IDS models have succeeded in detecting advanced and complicated attacks, the literature lacks lightweight models that can reach high accuracy without putting much strain on the system. It is also important for models to be able to spot known attacks and also detect new threats in IIoT settings. Another major issue is choosing the most important features for anomaly detection, since IIoT traffic is always changing and full of different data [18-20].

To address these gaps, there is a need for IDS models that integrate advanced feature selection techniques, such as chaotic mapping or optimization algorithms, along with deep learning methods that can efficiently detect both known and unknown attacks. Moreover, the integration of federated learning with anomaly detection models holds significant potential in addressing privacy and scalability concerns in IIoT networks. Research that combines these techniques could lead to more efficient and effective IDS models for IIoT environments, capable of operating in real-time while maintaining high accuracy and low computational cost.

3 PROPOSED WORK

The proposed solution framework given in Fig. 2 for IIoT networks is designed to ensure the system is robust, scalable, and able to efficiently handle high volumes of data while identifying a wide range of potential cyber threats. The framework is divided into the following key stages.

3.1 System Model

3.1.1 Feature Selection Using Chaotic Marine Predators Algorithm (CMPA)

At this stage, the system employs the Chaotic Marine Predators Algorithm (CMPA) to perform feature selection to minimize the data dimensionality. MPA copies the smart hunting behaviors of marine predators. MPA has powerful search and use capabilities, but it might sometimes get stuck early in the search. With Chaos Mapping, CMPA enjoys a wider range of initial conditions and disturbed iterations. By using chaotic dynamics, the algorithm helps the predator avoid getting stuck in the same local optimum and improves the stability of its feature selection. This process starts with the initialization of candidate solutions (features) within their feasible domains so as to ensure that the solution space is well searched. The addition of chaotic mapping improves the exploration and exploitation phase of the Marine Predators Algorithm (MPA).

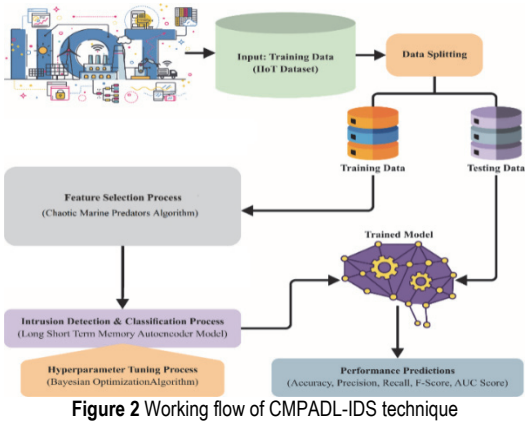

Figure 2 Working flow of CMPADL-IDS technique

Chaotic mapping in some way introduces controlled randomness into the algorithm, which helps to avoid the problem of the algorithm converging to suboptimal solutions too quickly and thus improves the selection of features. This fitness function in this stage is the trade-off between the error rate of classification and the number of selected features, by which the computational cost is reduced. A weighted parameter helps in assigning the priorities between the two important factors such as accuracy and computational purposes and correspondingly helps in finding the right features which is required to classify.

(a) Initialization of solution space

$$X_i^j = X_{\min}^j + r\left(X_{\max}^j - X_{\min}^j\right) \tag{1}$$

where, X_i^j - Initial position of the *i*-th solution of the *j*-th direction, $X_{\max}^j$ and $X_{\min}^j$ - Maximum and minimum boundaries of the *j*-th dimension and *r* - A random number in the range [0, 1].

(b) Chaotic Map Integration

$$x_{t+1} = \left(x_t + K\sin\left(2\pi x_t\right)\right)\bmod 1 \tag{2}$$

where, x_t - Current chaotic state and K - Control parameter of the chaotic map.

(c) Fitness Function

$$F = \alpha \cdot \text{Error}_{\text{classifier}} + \left(1-\alpha\right)\cdot\frac{|S|}{T} \tag{3}$$

For anomaly detection, the system uses LSTM-AE to work with sequential data, including network traffic. The

LSTM-AE performs the input data through the encoding and decoding of the input data. Its architecture utilizes LSTM cells which include the forget gate, input gate and the output gates. These gates enable the regulation of the flow of information, long term storage of dependencies and temporal capturing of information. In training, the LSTM-AE is trained to reconstruct normal data with minimal error as shown below. In the following section, the reconstruction loss is adopted as an anomaly metric, which is defined as the mean squared error between the input and the reconstructed data. High reconstruction errors suggest anomalies since the model fails to reconstruct data patterns it has not encountered. This approach makes the LSTM-AE essentially suitable for differentiating normal from the anomalous, feasible in the case of network traffic.

3.1.2 Anomaly detection using Long Short Term Memory Autoencoder (LSTM-AE)

(a) LSTM Cell Dynamics

$$f_t = \sigma\left(W_f x_t + U_f h_{t-1} + b_f\right) \tag{4}$$

$$i_t = \sigma\left(W_i x_i + U_i h_{t-1} + b_i\right) \tag{5}$$

$$\tilde{c}_t = \tanh\left(W_c x_t + U_c h_{t-1} + b_c\right) \tag{6}$$

$$c_t = f_t \odot c_{t-1} + i_t \odot \tilde{c}_t \tag{7}$$

$$o_t = \sigma\left(W_o x_t + U_o h_{t-1} + b_o\right) \tag{8}$$

$$h_t = o_t \odot \tanh\left(c_t\right) \tag{9}$$

where, f_t , i_t , o_t - Forget, input and output gates. $\tilde{c}_t$, c_t - Cell state and candidate cell state, h_t - Hidden state, W, U - Weight matrices, b - Bias terms and σ - Sigmoid activation function.

(b) Reconstruction Loss

$$L_{\text{reconstruction}} = \frac{1}{N}\sum_{i=1}^{N}\left(x_i - \hat{x}_i\right)^2 \tag{10}$$

where, x_i - Original input, $\hat{x}_i$ - Reconstructed input and N - Total number of samples.

Using Bayesian Optimization (BO), the hyperparameters of the LSTM-AE model such as the number of hidden units, learning rate and dropout rate, are tuned efficiently. The objective function is approximated in BO using Gaussian Processes (GPs) and new hyperparameter sets are chosen to maximize the expected improvement. With this approach, you do fewer expensive model evaluations and skip the need for exhaustive grid searches. BO allows the LSTM-AE to be configured well while keeping the computational cost low which is necessary for real-time IIoT applications.

3.1.3 Bayesian Optimization for Hyperparameter Tuning

(a) Surrogate Model for Objective Function

$$p\left(y|x\right) = \mathcal{N}\left(\mu\left(x\right), \sigma^2\left(x\right)\right) \tag{11}$$

where, $\mu(x)$ - Mean of the Gaussian process and $\sigma^2(x)$ - Variance of the Gaussian process.

(b) Acquisition Function (Expected Improvement)

$$EI\left(x\right) = \left(\mu\left(x\right) - y^* - \xi\right)\Phi\left(Z\right) + \sigma\left(x\right)\phi\left(Z\right) \tag{12}$$

3.2 Solution Framework

The CMPADL-IDS framework is created by applying a Chaotic Marine Predators Algorithm together with a Deep Learning-based Intrusion Detection System to secure IIoT networks. Because of the challenges of high costs and low accuracy, the CMPADL-IDS framework uses both selecting important features and classifying data. This method uses the Marine Predators Algorithm (MPA) and chaotic mapping which are inspired by nature, to improve the selection of features. The chaos theory in MPA helps the algorithm to search a wide area and prevents it from stopping at almost good results.

3.3 Dimensionality Reduction

The CMPADL-IDS framework includes feature extraction as an important feature to choose the most useful features from many available and to improve the accuracy of classification. A new method for choosing features is used which involves the Marine Predators Algorithm (MPA) and chaotic mapping. Because marine animals are known to be predatory, the MPA relies on these strategies to find the best solutions.

It begins when the search space is filled with possible solutions. Chaotic mapping leads to patterns that are easy to predict, but they greatly increase the number of initial solutions. The MPA operates in three stages: exploration, transition, and exploitation. In the global exploration phase, predators with high velocity search the environment using the Brownian motion in order to provide a coverage of the entire space. When the algorithm changes, it uses both Brownian and Lévy motions to achieve a global and local search. In the exploitation stage, predators use Lévy migration to concentrate on the local neighborhood of promising solutions. Also, a chaos-based randomization step is used to avoid getting stuck in local optima and to search the solution space more effectively.

To evaluate potential solutions, a fitness function is employed, balancing two key objectives: The goals are to accomplish the highest accuracy of the classification and to determine the minimum number of features to be chosen. The fitness function has also a model to use weighting so that the selected features are very much important to the classifier.

3.4 DL Model Selection

To accomplish intrusion detection and classification, the CMPADL-IDS framework integrates a novel deep learning model called LSTM-AE. The LSTM-AE is particularly suitable for time series data, which is common in IIoT networks due to traffic and sensor data temporal

characteristics. The LSTM architecture, a variant of recurrent neural networks (RNNs), includes specialized gates for controlling information flow: It consists of input, forget and output gates. These gates allow the LSTM to have a long short-term memory and hence be able to figure out the patterns and anomalies in big IIoT data.

The LSTM-AE operates in three stages: including: embedding, encoding and decoding. The map learning phase comprises of encoding the input data into a lower-dimensional density space that describes its important aspects. In the encoding stage, LSTM is applied to the sequences in order to deal with the sequential characteristics of the data; in the decoding stage the original data representation is reconstructed from the encoded one. The error of reconstruction is used as a measure of anomaly detection and is defined as the difference between the input and the output. A high reconstruction error means that there is an anomaly because the model cannot reconstruct data it has not been trained on.

The LSTM-AE model is trained with normal and anomalous samples dataset. During the training process, the model is trained to minimize the error that is committed while reconstructing normal data. In case of receiving anomalous data, the reconstruction error rises, which allows to identify possible intrusions. This learning approach does not require labeled data, which makes it very flexible in terms of intrusion scenarios. To enhance the robustness and scalability of the LSTM-AE, its architecture is designed to deal with big data nature and complexity of the IIoT networks.

3.5 Fine-Tuning the DL Model

The CMPADL-IDS uses Bayesian Optimization (BO) to adjust the hyperparameters of the LSTM-AE model. The number of LSTM layers, the size of the hidden units, the learning rate and the dropout rate are now important in deciding how well the model can learn and detect anomalies. Hyperparameter tuning takes up a significant part of the BO approach, as a probabilistic model of the objective function is created to find the optimal hyperparameter values.

Optimization in fact starts with defining a range of values that can be searched over with respect to each hyperparameter. BO is then called with a starting set of samples and then proceeds to value the objective function at these points. These evaluations provide the basis to build a surrogate model, which is commonly a GP, that will mimic the objective function. The acquisition function that considers both exploration and exploitation define which set of hyperparameters should be used next. This process is carried out iteratively until some convergence factors are met or when the specified computational cycle is used up.

The second BO framework to be discussed as part of this work is the one where the objective function for BO is defined in order to minimize the validation error of the LSTM-AE model. In this way, BO is able to identify hyperparameter combinations for achieving the best fit of the surrogate model for a specific level of model complexity and corresponding detection accuracy. Besides improving the LSTM-AE, this procedure also helps its ability to generalize over unseen data and also minimizes overfitting of the model. BO in the existing CMPADL- IDS is an appropriate example of the application of machine learning and optimization techniques for solving complex problems in IIoT security. Through adjusting the LSTM-AE structured framework, precision significantly boosts up to the detection of intrusions, where using this framework is beneficial to secure IIoT settings.

4 RESULTS AND DISCUSSION

The performance of the proposed CMPADL-IDS framework is evaluated using ToN-IoT dataset [21], which is a comprehensive dataset for intrusion detection in IoT context. The dataset has a total of 119957 samples and is divided into nine classes where each class is a type of network behavior or attack. The classes include normal activity and eight types of malicious activities: Malware attacks based on man-in-the-middle attacks, denial-of-service attacks, distributed denial-of-service attacks as well as traditional attacks based on passwords and injections, Cross-Site Scripting (CSS) attacks, ransom attacks, and backdoor attacks.

The Tab. 1 and Fig. 3 shows the detection outcomes CMPADL-IDS Algorithm with 80% TRAS: 20% TESS.

Table 1 Detection Outcomes of CMPADL-IDS Algorithm (80% TRAS: 20% TESS)

Class	Acc / %	Pre / %	Recall / %	F-Score / %	AUC Score / %
Normal	97.50	95.70	98.95	97.31	94.87
MiTM	99.85	100.00	98.91	99.45	98.80
DoS	98.40	72.50	73.40	72.95	87.50
DDoS	98.10	79.60	76.90	78.21	89.30
Password	97.80	77.30	72.80	74.97	86.10
Injection	98.00	81.50	74.60	77.95	87.30
XSS	98.20	75.10	78.90	77.96	88.40
Ransomware	98.60	80.10	74.90	77.35	88.10
Backdoor	98.40	76.80	72.80	74.75	89.20
Average	98.10	80.60	76.25	77.89	87.45

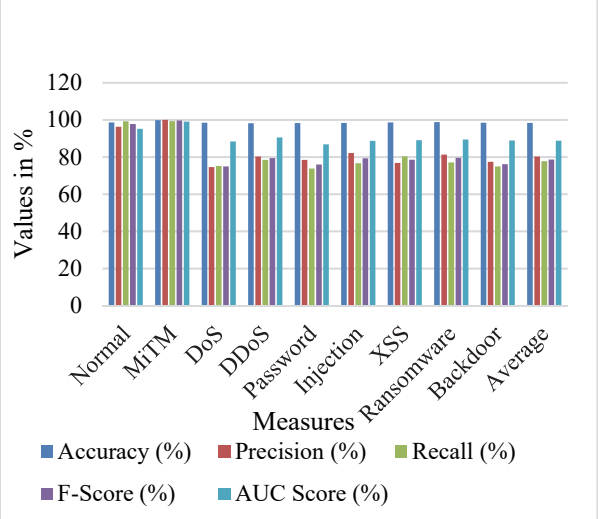

Figure 3 Detection outcomes of CMPADL-IDS Algorithm (80% TRAS: 20% TESS)

As for the CMPADL-IDS algorithm, the results are impressive; the accuracy was 98.10% on average. The system also obtains the highest accuracy in the "MiTM" class (99.85%), which shows good classification for this type of intrusion. The accuracy of "Normal" and "DDoS"

is high enough, which means that the model can recognize the benign data and some kind of attacks. But the precision for some of the attack types such as "DoS" and "Backdoor" is slightly low meaning that there could be some of the alarms that are false. The F-Score of 77.89 percent and the AUC Score of 87.45 percent reveal that the model's precision and recall does not significantly differ.

The Tab. 2 and Fig. 4 shows the detection outcomes CMPADL-IDS Algorithm with 70% TRAS: 30% TESS.

Table 2 Detection outcomes of CMPADL-IDS Algorithm (70% TRAS: 30% TESS)

Class	Acc / %	Pre / %	Recall / %	F-Score / %	AUC Score / %
Normal	98.60	96.30	99.20	97.73	95.20
MiTM	99.80	100.00	99.30	99.65	99.10
DoS	98.50	74.60	75.20	74.90	88.40
DDoS	98.20	80.30	78.50	79.40	90.50
Password	98.30	78.50	73.80	75.95	86.80
Injection	98.40	82.20	76.70	79.35	88.70
XSS	98.60	76.80	80.40	78.55	89.10
Ransomware	98.80	81.30	77.10	79.60	89.40
Backdoor	98.50	77.40	74.90	76.12	88.90
Average	98.40	80.30	77.80	78.62	88.80

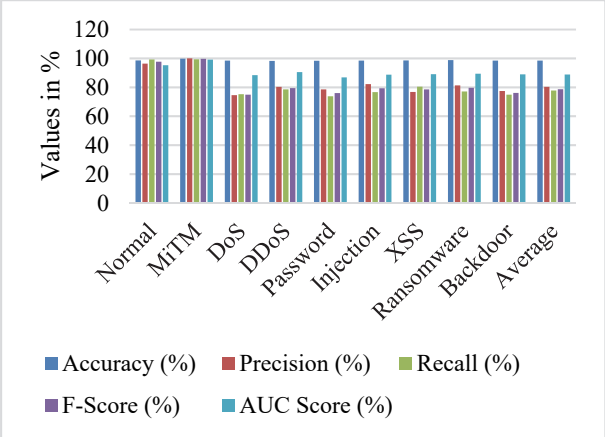

Figure 5 Detection outcomes of CMPADL-IDS Algorithm (70% TRAS: 30% TESS)

Even with a slightly lower number of training data, the CMPADL-IDS method shows good detection rates with an average accuracy of 98.40%. Once more, the "MiTM" class yields the highest precision, which is 100%, thus providing for precise identification of this kind of attacks that are rather infrequent. The training and testing phases for the attacks "DoS" and "Backdoor" classification are presented, and as can be observed, their precision and report values remain quite low, which means that there is a need to optimize the model to better identify these type of attacks. However, the average F-score of 78.62% and AUC Score of 88.80% indicate that the system has a reasonably good performance in a relatively more difficult testing scenario.

The ROC curves are depicted in the Fig. 7b and Fig. 7d which plot the true positive rate (sensitivity) against the false positive rate. A curve that is closer to the upper left corner of the graph is an indication of good discriminatory ability of a model. In both cases of dataset division, the ROC curves of the CMPADL-IDS framework have a very high performance with high AUC values in all classes. This result actually proves that the proposed model can accurately differentiate normal and malicious behaviors irrespective of the environment. The PR and ROC curves of the CMPADL-IDS framework for the two datasets split also endorse the flexibility and robustness of the model. Both curves depict the performance of the model as constant and of high quality in different scenarios, which makes it accurate. Thus, we can state that the preservation of high values of precision, recall, and AUC confirms the efficiency of the proposed framework for its application in real-life IIoT conditions, where the problem of intrusion detection is critical.

Tab. 3 and Fig. 6, shows the comparison of the proposed CMPADL-IDS framework with other intrusion detection models such as LSTM, GRU, RF, and the EBWO-HDLID model. The comparison is based on key performance metrics: We used accuracy, precision, recall, F-score, and AUC score for the evaluation of the models.

Table 3 Performance comparison of CMPADL-IDS with

Method	Acc / %	Pre / %	Recall / %	F-Score / %	AUC Score / %
CMPADL-IDS	98.10	80.60	76.25	77.89	87.45
LSTM	96.50	76.20	72.30	74.50	85.20
GRU	96.80	77.00	73.60	75.50	85.90
RF	97.50	85.10	78.40	80.75	86.10
EBWO-HDLID	97.90	88.10	79.80	81.80	87.90

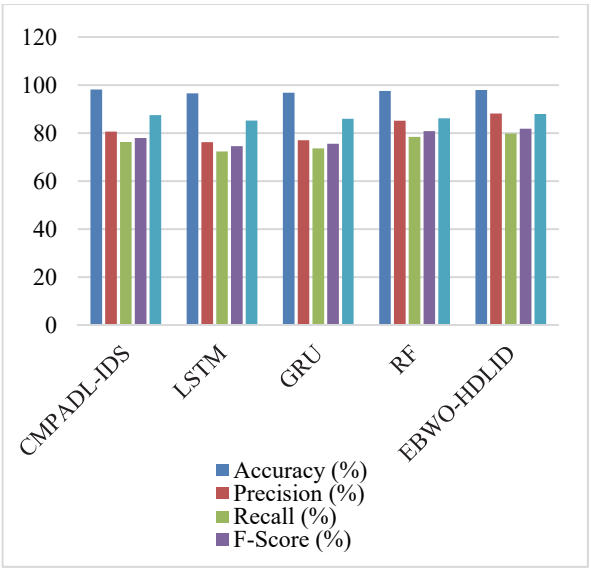

Figure 6 Performance Comparison of CMPADL-IDS with Existing Algorithms

The proposed CMPADL-IDS framework attains the highest accuracy of 98.10 % and outperforms all the other models [22]. This superior performance points to its efficiency in correctly classifying both normal and anomalous traffic in the IIoT networks. The EBWO-HDLID model is very close to the proposed model with an accuracy of 97.90%, RF is at 97.50%, LSTM is at 96.50% and GRU is at 96.80%. The findings further substantiate that the proposed hybrid feature selection and integration of deep learning in CMPADL-IDS improves the detection accuracy. As for the accuracy, CMPADL-IDS has an impressive result of 80.60% which shows that the IDS is capable of reducing false alarm while at the same time has high true alarm detection rate. Although the EBWO-HDLID model achieves 1% more than CMPADL-IDS with a precision of 88.10%, the

compromise between precision and other measures such as recall and F-score in CMPADL-IDS yields better general performance. RF also shows better accuracy compared to competitors at 85.10%, while LSTM and GRU are behind at 76.20% and 77.00% correspondingly. The recall of CMPADL-IDS is 76.25% while that of EBWO-HDLID is 79.80%. Recall means the ability of the system to correctly identify malicious activities, including the less frequent attacks. Despite the fact that CMPADL-IDS has a slightly lower recall than EBWO-HDLID it has a much higher accuracy than LSTM (72.30%) and GRU (73.60%). This is an indication that the proposed CMPA feature selection and LSTM-AE are efficient in identifying multiple intrusion types without overlooking important anomalies.

F-measure is another broader measure that is a harmonic mean of the two, the precision and the recall. Thus, the proposed CMPADL-IDS obtains an F-score of 77.89%, which is quite comparable to EBWO-HDLID (81.80%) and higher than RF (80.75%), LSTM (74.50%), and GRU (75.50%). Due to the balance of both precision and recall, CMPADL-IDS can be depended on for real world applications where both metrics are important. The AUC score of CMPADL-IDS is 87.45%, which shows a good performance of the proposed CMPADL-IDS to distinguish between normal and malicious activities at different thresholds. The score of EBWO-HDLID is 87.90% which is slightly higher than this score, but RF has a score of 86.10%, LSTM has 85.20% and GRU has 85.90%. The strong AUC score of CMPADL-IDS suggests that it performs well in different situations.

5 CONCLUSION

The framework shows superior results when it comes to protecting IIoT networks from many types of cyber threats. To keep the computation low, it makes use of CMPA for selecting important features and LSTM-AE for detecting anomalies, leading to high accuracy. Bayesian Optimization (BO) helps to adjust parameters which makes the system more stable in unstable IIoT settings. When applied to the ToN-IoT dataset, the framework outperforms usual intrusion detection methods in terms of precision, recall and F-score for multiple attack types. In the future, we plan to use adaptive learning in real time to address new threats and use federated learning so training can be done securely and in a decentralized way across various IIoT nodes. With lightweight deep learning architectures, edge devices can use machine learning too. Also, using blockchain can help ensure that data used in industry is more reliable. Using the CMPADL-IDS framework, researchers and engineers can work on more advanced intrusion detection in IIoT networks and develop useful tools for industrial security.

6 REFERENCES

[1] Dina, A. S., Siddique, A. B., & Manivannan, D. (2023). A deep learning approach for intrusion detection in the Internet of Things using focal loss function. *Internet of Things*, *22*, 100699. https://doi.org/10.1016/j.iot.2023.100699

[2] Ismail, S., Dawoud, D. W., & Reza, H. (2023). Securing wireless sensor networks using machine learning and blockchain: A review. *Future Internet*, *15*(6). https://doi.org/10.3390/fi15060200

[3] He, K., Kim, D. D., & Asghar, M. R. (2023). Adversarial machine learning for network intrusion detection systems: A comprehensive survey. *IEEE Communications Surveys & Tutorials*, *25*(1), 538-566. https://doi.org/10.1109/COMST.2022.3233793

[4] Kerdjidj, O., Himeur, Y., Sohail, S. S., Amira, A., Fadli, F., Atalla, S., Mansoor, W., Copiaco, A., Gawanmeh, A., Miniaoui, S., & Dawoud, D. W. (2024). Uncovering the potential of indoor localization: Role of deep and transfer learning. *IEEE Access*, *12*(73). https://doi.org/10.1109/ACCESS.2024.3402997

[5] Rejeb, A., Rejeb, K., Appolloni, A., Jagtap, S., Iranmanesh, M., Alghamdi, S., Alhasawi, Y., & Kayikci, Y. (2024). Unleashing the power of the Internet of Things and blockchain: A comprehensive analysis and future directions. *Internet of Things and Cyber-Physical Systems*, *4*. https://doi.org/10.1016/j.iotcps.2023.06.003

[6] Elappila, M. & Chinara, S. (2024). Implementation of survivability aware protocols in WSN for IoT applications using Contiki-OS and hardware testbed evaluation. *Microprocessors and Microsystems*, *104*, 104988. https://doi.org/10.1016/j.micpro.2023.104988

[7] Yazdinejad, A., Kazemi, M., Parizi, R. M., Dehghantanha, A., & Karimipour, H. (2023). An ensemble deep learning model for cyber threat hunting in the industrial internet of things. *Digital Communications and Networks*, *9*(1), 101-110. https://doi.org/10.1016/j.dcan.2023.01.004

[8] Pampapathi, B. M., Guptha, N., & Hema, M. S. (2022). Towards an effective deep learning-based intrusion detection system in the Internet of Things. *Telematics and Informatics Reports*, *7*, 100009. https://doi.org/10.1016/j.teler.2022.100009

[9] Qathrady, M. A., Ullah, S., Alshehri, M. S., Ahmad, J., Almakdi, S., Alqhtani, S. M., Khan, M. A., & Ghaleb, B. (2024). SACNN-IDS: A self-attention convolutional neural network for intrusion detection in the industrial Internet of Things. *CAAI Transactions on Intelligence Technology*, *9*(6), 1398-1411. https://doi.org/10.1049/cit2.12352

[10] Gopi, R., Sheeba, R., Anguraj, K., Chelladurai, T., Alshahrani, H. M., Nemri, N., & Lamoudan, T. (2023). Intelligent intrusion detection system for industrial Internet of Things environment. *Computer Systems Science & Engineering*, *44*(2). https://doi.org/10.32604/csse.2023.025216

[11] Ahmad, J., Shah, S. A., Latif, S., Ahmed, F., Zou, Z., & Pitropakis, N. (2022). DRaNN_PSO: A deep random neural network with particle swarm optimization for intrusion detection in the industrial Internet of Things. *Journal of King Saud University-Computer and Information Sciences*, *34*(10), 8112-8121. https://doi.org/10.1016/j.jksuci.2022.01.008

[12] Alalayah, K. M., Alrayes, F. S., Alzahrani, J. S., Alaidarous, K. M., Alwayle, I. M., Mohsen, H., Ahmed, I. A., & Al Duhayyim, M. (2023). Optimal deep learning-based intruder identification in industrial Internet of Things environment. *Computer Systems Science & Engineering*, *46*(3), 3121-3139. https://doi.org/10.32604/csse.2023.036352

[13] Zhang, Y., Yang, L., Xu, Y., & Qiu, M. (2022). Real-time intrusion detection using hybrid ensemble learning in industrial Internet of Things. *International Journal of Industrial Ergonomics*, *94*, 102702.

[14] Abdu, A., Hossain, M. S., Al-Raweshidy, H., & Lee, M. H. (2023). Smart intrusion detection system for industrial Internet of Things with feature fusion and attention mechanisms. *Sensors*, *23*(6), 1519.

[15] Rashid, T., Sardar, S., & Awais, M. (2024). Intrusion detection system for industrial Internet of Things based on long short-term memory (LSTM) neural networks. *Future Generation Computer Systems*, *125*, 21-34. https://doi.org/10.1016/j.future.2024.02.001

[16] Khan, W., Ahmed, M., Siddiqi, S., & Ibrahim, M. (2023). Blockchain-based intrusion detection system for industrial

IoT: A survey and future directions. *Future Internet*, *15*(10), 350.
[17] Thiruppathi, M. & Vinoth Kumar, K. (2023). Seagull optimization-based feature selection with optimal extreme learning machine for intrusion detection in fog-assisted WSN. *Technical Gazette*, *30*(5), 1547-1553. https://doi.org/10.17559/TV-20230130000295
[18] Rehman, E., Haseeb-ud-Din, M., Malik, A. J., Khan, T. K., Abbasi, A. A., Kadry, S., Khan, M. A. & Rho, S., (2022). Intrusion detection based on machine learning in the internet of things, attacks and countermeasures. *The Journal of Supercomputing*, *78*(1), 1-35. https://doi.org/10.1109/LSP.2020.3006417
[19] Kumar, V., Das, A. K. & Sinha, D. (2021). UIDS: A unified intrusion detection system for IoT environments. *Evolutionary Intelligence*, *14*(1), 47-59. https://doi.org/10.1109/LSP.2020.3006417
[20] Rajakani, V. & Kumar, K. V., (2023). Barnacles Mating Optimizer with Hopfield Neural Network-Based Intrusion Detection in Internet of Things Environment. *Tehnicki vjesnik - Technical Gazette*, *30*(6). https://doi.org/10.17559/TV-20230414000533
[21] See https://research.unsw.edu.au/projects/toniot-datasets
[22] Veeramakali, T., Siva, R., Sivakumar, B. et al. (2021). An intelligent internet of things-based secure healthcare framework using blockchain technology with an optimal deep learning model. *The Journal of Supercomputing*, *77*, 9576-9596. https://doi.org/10.1007/s11227-021-03637-3

Contact information:

G. ANITHA
(Corresponding author)
Department of Electronics and Communication Engineering, RMD, Engineering College, Chennai, Tamil Nadu, India
E-mail: anitha.ece@hotmail.com

Hariprasath MANOHARAN
Department of Electronics and Communication Engineering, Panimalar Engineering College, Poonamallee, Tamil Nadu, India

Abirami MANOHARAN
Department of Electrical and Electronics Engineering, Government College of Engineering, Srirangam, Trichy, Tamil Nadu, India