Detecting Zero-Day Attacks Using Deep Learning with Pelican Optimization Algorithm in IIoT Environments

Khalid Ammar
Department of Electrical and Computer Engineering, College of Engineering and Information Technology, Ajman University, Ajman, UAE
k.ammar@ajman.ac.ae

Mohamad Khairi Ishak
Department of Electrical and Computer Engineering, College of Engineering and Information Technology, Ajman University, Ajman, UAE
m.ishak@ajman.ac.ae (corresponding author)

Received: 1 August 2025 | Revised: 1 September 2025, 17 September 2025, and 30 September 2025 | Accepted: 5 October 2025

 DOI: https://doi.org/10.48084/etasr.13778

ABSTRACT

5G arises as the base for the Industrial Internet of Things (IIoT); it enables the unified, low-latency hybrid of cloud computing and Artificial intelligence (AI), thus strengthening the complete industrial process within a structure of intelligent and smart IIoT environments. Simultaneously, the constantly evolving landscape of cybersecurity hazards in the Internet of Things (IoT) domain presents opportunities for enhanced safety complexities. Recognizing zero-day threats is a challenging task due to the indefinite nature of security exposures. This study proposes a new Metaheuristic Optimization Algorithm with Deep Learning Enabled Zero-Day Attack Detection (MHOA-DLZDAD) method for IIoT frameworks. The MHOA-DLZDAD method automates and effectively detects zero-day attacks. Initially, the MHOA-DLZDAD model undergoes min-max scalarization using data pre-processing to convert actual data into a suitable format. Moreover, the Elman Recurrent Neural Network (ERNN) method is utilized to detect zero-day attacks. Furthermore, the Pelican Optimization Algorithm (POA) method is employed for tuning the parameters. The experimental analysis of the MHOA-DLZDAD approach is conducted on a benchmark dataset, and the comparison study reveals a higher accuracy of 99.56% compared to other studies.

Keywords-pelican optimization algorithm; deep learning; zero-day attack; min-max scalar; industrial internet of things

I. INTRODUCTION

IoT is a fast-developing model in the computing field. The former has advanced in various technological areas, with hundreds of billions of devices from multiple systems, such as smart homes, smart grids, smart healthcare, and smart vehicles, connected to the internet [1]. However, this intersection has been followed by numerous cyberattacks on IoT methods because IoT combines the digital world with the physical world [2]. Intrusion Detection Systems (IDS) are among the most important methods used to address the growth in cyberattacks. These systems can identify zero-day cyberattacks. ML methods are widely used for building and designing robust IDS [3]. The latter rely on predefined signatures and patterns [4], which is one of their limitations. In addition, existing IDSs suffer from higher false positive rates, thereby restricting their performance and practical usage in real-world executions. Therefore, multiple zero-day attacks remain unnoticed, which increases their impact. The most popular IoT attacks are Denial of Service (DoS) and Distributed DoS (DDoS) [5]. These attacks can track susceptible IoT nodes and utilize them later to damage the remaining network, disrupt services, and cause data violations. Conventional ML-based techniques in detection attacks may perform relatively well in identifying data they were previously trained on [6]. However, these models face difficulty in distinguishing between data types that require further training. In contrast, Deep Learning (DL)-based methods are better suited to learn complex, non-linear patterns, enabling the improved detection of unfamiliar data [7]. Convolutional Neural Networks (CNNs) are a subset of DL, which can handle data as pixels and images. IDSs utilize the CNN method for the effective and initial recognition of the SDN method threats, encouraged by the effectiveness of CNN in resolving various complex classification problems. Furthermore, CNN presents the parameter sharing concept that substantially reduces the detection method of dimension

parameters [8]. However, CNN is still used to detect anomalies. The rapid development of IoT has transformed various sectors, connected billions of devices, and enhanced functionality across smart homes, healthcare, and transportation. However, this expansion has also led to an increase in cyber threats, necessitating the implementation of effective safety measures [9]. Conventional IDSs are effective at detecting known attacks but struggle with zero-day vulnerabilities, which are based on unseen threats. This highlights the need for adaptive ML-based approaches to ensure reliable security in increasingly complex and evolving IoT environments [10].

In [11], a Hybrid Meta-heuristic with DL-assisted Cyberattack Prevention (HMDL-CAP) technique was introduced. Other studies have used a deep learning approach, the Adaptive Swish-driven Deep Multi-Layer Perceptron (ASDMLP) method, in combination with the Probability-driven Fuzzy C-Means (PFCM) method. In [12], fusion optimization and DL-based IDS were proposed. After pre-processing, a DL-assisted Hybrid Neural Networks (DLHNN) classifier was utilized for classification. Authors in [13] presented an effective anomaly recognition method by utilizing an Improved Grey Wolf Optimizer (IGWO)-based LSTM methodology, with an AE for feature mitigation. The LSTM parameters were tuned employing IGWO models. Authors in [14] introduced a Billiard Optimization with a DL-based Anomaly Detection and Classification (BBODL-ADC) model. Also, the ERNN method was utilized to detect and classify anomalies. Furthermore, the BBO model was employed for tuning. Authors in [15] presented the ID with the heuristic-based DL method. Moreover, they employed the Cascaded Ensemble Learning (CEL) technique for recognizing the intrusions and an Improved Darts Game Optimizer (IDGO) model for fine-tuning.

Authors in [16] introduced a novel model for integrating DL-assisted and feature-based methodologies along with the African Vulture Optimization Algorithm (AVOA) technique to organize the FS. Authors in [17] incorporated a DQN model to improve mischievous traffic detection, while authors in [18] examined a DL-based IDS method, which is adapted to new threats through diverse stages. Authors in [19] presented a novel transferable IDS model that employs DL, incorporating effectual feature mapping, cascade models, and Transfer Learning (TL). The Cascade Feedforward Backpropagation Neural Networks (CFBPNN) model was used for detection and classification. Authors in [20] presented a DNN with a Federated Learning (FL) model. Authors in [21] proposed a Hybrid Multi-Stage IDS (HMS-IDS) technique, while authors in [22] presented the PIGNUS model, which utilizes an autoencoder for optimal FS and a CFBPNN technique. Authors in [23] developed a complex framework to model intricate zero-day attacks, and authors in [24] proposed an FL-based method. Authors in [25] explored how emerging technologies, such as 6G, IoE, AI, and WPA3, can collaborate to enhance security against known attack vectors and zero-day attacks. These studies encounter high computational overhead, weak generalization to ZDAs, and poor interpretability. Several lack effective FS, real-time scalability, or lightweight design for IIoT environments. The research gap lies in building an efficient, scalable, and explainable IDS that integrates optimized FS, robust DL, and XAI for handling dynamic, imbalanced data in distributed environments. The present study presents a new MHOA-DLZDAD method. The key contributions of the latter are:

- The utilization of min-max scaler in the comprehensive data pre-processing to normalize and transform the raw IIoT data into a suitable format. The former ensures consistent input ranges that improve model learning efficiency and stability, ultimately enhancing the accuracy and generalizability of the detection framework.
- The use of the ERNN technique to effectively detect intrinsic and emerging zero-day attacks in IIoT environments by utilizing its dynamic memory capabilities. This model also enabled accurate temporal pattern learning, precise recognition, and improved adaptability to real-time threat variations.
- The implementation of the POA to enhance the efficiency of the hyperparameter tuning, thereby improving the model's convergence speed, accuracy, and robustness. The approach also effectively balances exploration and exploitation, improving the overall detection performance in IIoT security contexts.
- A novel integration of ERNN with POA for detecting zero-day attacks in IIoT environments. This incorporation presents an adaptive architecture capable of capturing intrinsic temporal patterns. Unlike existing models, it ensures effective tuning for enhanced generalization. The novelty lies in jointly optimizing detection accuracy and computational efficiency, tailored for IIoT systems.

II. PROPOSED MODEL

This study proposes an MHOA-DLZDAD method for secure IIoT frameworks. The technique aims to automate and effectively identify zero-day attacks. The processes involved in the MHOA-DLZDAD approach comprise min-max scalar-based data pre-processing, ERNN-based detection and classification of a zero-day attack, and POA-based hyperparameter tuning, as demonstrated in Figure 1.

A. Data Pre-Processing

In this step, the MHOA-DLZDAD model was utilized to perform normalization using the min-max scalar technique. This model is chosen for its efficiency and simplicity in normalizing data in the interval of 0 and 1, which is significant for improving the convergence speed of neural networks such as ERNN. This method also preserves the original data distribution and is less sensitive to outliers when utilized with bounded activation functions. It is a data pre-processing model used in zero-day attack recognition for IIoT methods. By measuring feature values within an interval of 0 and 1, the min-max Scaler ensures that all input data are normalized, thereby improving the efficiency of ML methods. This normalization procedure aids in precisely classifying anomalies and perceiving probable zero-day attacks by certifying constant data ranges.

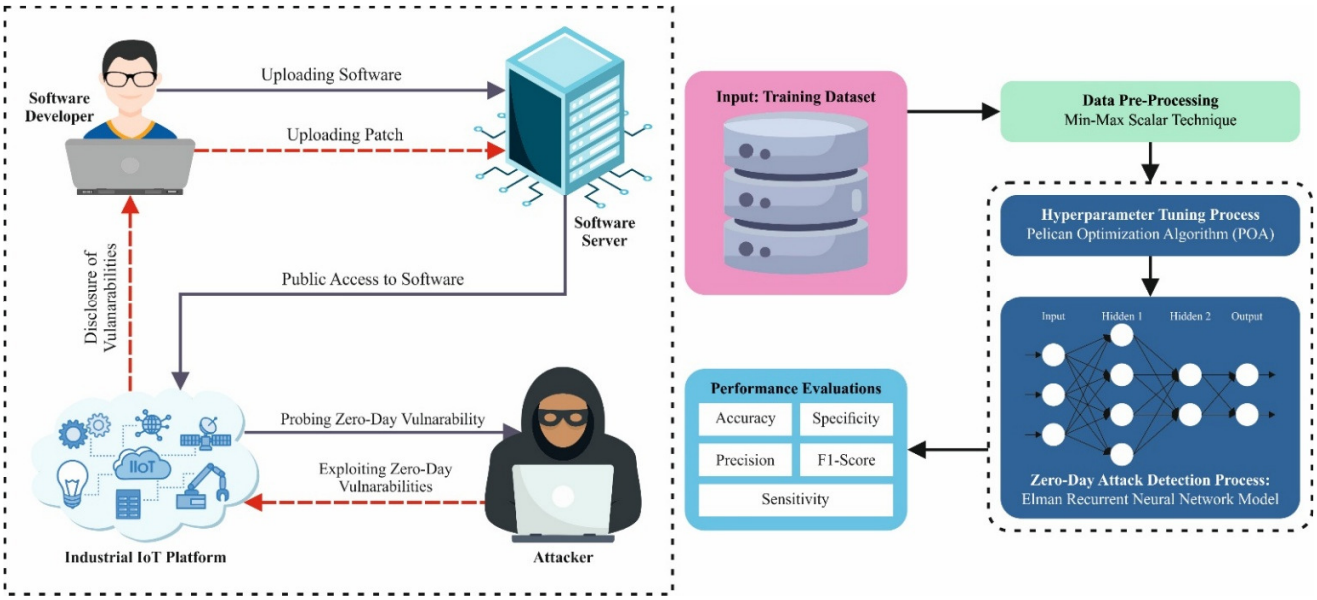


Fig. 1. Workflow of the MHOA-DLZDAD model.

B. ERNN-Based Detection and Classification

The MHOA-DLZDAD approach performs the detection and classification process using the ERNN model [26]. This model exhibits robust capability in modeling sequential and time-dependent data and also effectively detects growing network traffic patterns. Unlike conventional feedforward networks, ERNN maintains a form of memory through context units, allowing better handling of zero-day attacks. The feedback connections enhance the learning dynamics and facilitate improved performance compared to basic RNNs and other static models. The hyperparameters comprise a learning rate of 0.01, a single hidden layer with 50 neurons, and a batch size of 32. The training of the model was conducted over 100 epochs to ensure adequate learning while preventing overfitting. These settings strike a balance between computational efficiency and detection accuracy effectively. Figure 2 illustrates the ERNN model.

A Recurrent Neural Network (RNN) is a neural network with feedback loops that processes sequential data by joining new and prior outputs, allowing it to retain past data. A novel RNN variant replicates human memory using symmetric bidirectional links with equal weights, similar to Hopfield networks. The neurons, shown in (1), are in the non-linear step.

$$y = \sum_{i=1}^{d} w_i x_i + b \quad (1)$$

Neuron outputs are computed using activation functions, such as the sigmoid function, with a bias term b and fixed weights. The ERNN, inspired by feedforward networks, uses three interconnected layers. $(z, y, and\ z)$ with feedback from the hidden layer. During training, the backpropagation approach updates the network, and sigmoid functions help produce outputs between 0 and 1, as shown in:

$$y = \frac{1}{(1+e-sum)} \quad (2)$$

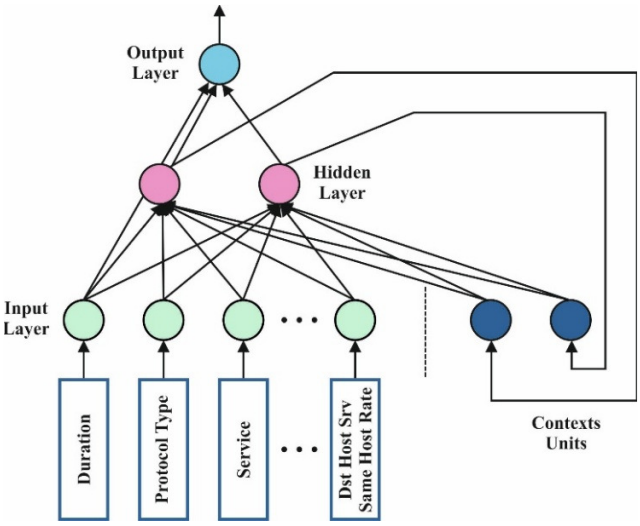


Fig. 2. Architecture of the ERNN technique.

C. POA-Based Tuning

In this step, the parameter fine-tuning of the MHOA-DLZDAD technique is performed by using the POA model, a unique approach inspired by nature [27]. This model shows excellence in balancing exploration and exploitation, presenting faster convergence and improved global search capability. The pelican's natural hunting strategy inspires this model. Also, it aids in tuning the model parameters, thereby enhancing accuracy while avoiding local optima, making it suitable for intrinsic hyperparameter optimization tasks. The POA method is based on population; pelicans are included in these populations. In this population-based method, every component denotes a potential solution. Initially, the population elements were randomly distributed according to (3), controlled by the problem's lower and upper limits:

$$X_{i,j} = l_j + rand.\left(u_j - l_j\right), i = 1,2,\ldots,N, j = 1,2,\ldots,m \quad (3)$$

where the j^{th} variable values are decided by determining the i^{th} possible solution, represented as $X_{i,j}$. The population is denoted by N, and there are m problem variables. $rand$ represents an arbitrarily produced value in [0, 1]. The lower and upper bounds of the j^{th} variable are denoted by $l_j$and u_j., respectively.

$$X = \begin{bmatrix} X_1 \\ \vdots \\ X_i \\ \vdots \\ X_N \end{bmatrix}_{N\times m} = \begin{bmatrix} x_{1,1} & \cdots & x_{1,j} & \cdots & x_{1,m} \\ \vdots & \ddots & \vdots & \iddots & \vdots \\ x_{i,1} & \cdots & x_{i,j} & \cdots & x_{i,m} \\ \vdots & \iddots & \vdots & \ddots & \vdots \\ x_{N,1} & \cdots & x_{N,j} & \cdots & x_{N,m} \end{bmatrix}_{N\times m} \quad (4)$$

where X represents the matrix that characterizes the population of pelicans, and X_i denotes the i^{th} individual pelican. As each pelican is distinct from the population of POA, it may represent a solution. Therefore, the objective function is estimated by examining each potential resolution.

$$F = \begin{bmatrix} F_1 \\ \vdots \\ F_i \\ \vdots \\ F_N \end{bmatrix}_{N\times 1} = \begin{bmatrix} F(X_1) \\ \vdots \\ F(X_i) \\ \vdots \\ F(X_N) \end{bmatrix}_{N\times 1} \quad (5)$$

The POA simulates hunting with two phases: exploration, where pelicans randomly move toward prey to enhance search diversity, and exploitation, where they fly near the water surface to refine their position and capture prey.

$$x_{i,j}^{P_1} = \begin{cases} x_{i,j} + rand.\left(p_j - l.x_{i,j}\right), & F_p^1 < F_j, \\ x_{i,j} + rand.\left(x_{i,j} - p_j\right), & else, \end{cases} \quad (6)$$

where F_p and $x_{i,j}^{P_1}$ denote the objective function value of the prey, randomly formed values l equivalent to one or more, and the i^{th} pelican's novel position during the j^{th} dimension, depending on the primary level. A novel location of a pelican has become allowable inside the POA limits when the value of the objective function improves at that specific position. Using these methods, recognized as "effective updating", this technique prevents its development over a region of suboptimal conditions.

$$X_i = \begin{cases} X_i^{P_1}, & F_i^{P_1} < F_i; \\ X_i, & else, \end{cases} \quad (7)$$

where $X_i^{P_1}$ denotes the updated i^{th} pelican status, while $F_i^{P_1}$ signifies the pelican's objective function value measured in the first level; in the next level, pelicans use the surface of the water to create increasing propulsion for the fish by lengthening their wings. The exploitation possibility of POA is improved at this level, as the algorithmic techniques provide more optimal solutions in the hunting area.

$$x_{i,j}^{P_2} = x_{i,j} + R.\left(1 - \frac{t}{T}\right).(2.rand - 1).x_{i,j} \quad (8)$$

where $x_{i,j}^{P_2}$ represents the i^{th} pelican's updated position in the j^{th} size during the next level. The constant R is 0.2. The neighbouring radius of $x_{i,j}$ is established using the number of iterations t and the highest iteration number T. At this stage, the rejection or approval of the latest pelican location is determined through efficient updating.

$$X_i = \begin{cases} X_i^{P_2}, & F_i^{P_2} < F_i; \\ X_i, & else, \end{cases} \quad (9)$$

where $X_i^{P_2}$ represents the updated position of the i^{th} pelican, which is the pelican's objective function value. The following iterations begin when all population members have been upgraded. An operation sequence directed by (6-9) is repeated until the operation is completed. To achieve an enhanced classifier performance, the POA develops a fitness function. It designates a positive number to represent the improved performance of the candidate solution. Additionally, decreasing the classifier error rate is selected as the fitness function in:

$$fitness(x_i) = ClassifierErrorRate(x_i) = \frac{No.of\ misclassified\ samples}{Overall\ samples} \times 100 \quad (10)$$

III. RESULTS

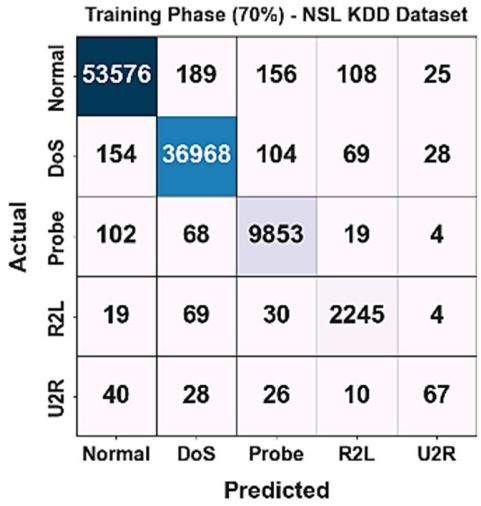
The MHOA-DLZDAD approach is verified using the NSL-KDD dataset [28]. It contains 148,517 instances across five classes: Normal (77,054), DoS (53,385), Probe (14,410), R2L (3,416), and U2R (252). These categories comprise benign and other attack types, making the dataset appropriate for training and evaluating detection models. The simulation was conducted using Python 3.6.5 with an i5-8600k CPU, 4GB GPU, 16GB RAM, 250GB SSD, and 1TB HDD, with a 0.01 learning rate, ReLU, 50 epochs, 0.5 dropout, and batch size 5. Figures 3(a) and 3(b) display the confusion matrices of the MHOA-DLZDAD method using a 70:30 split for the Training Phase (TRPH) and Testing Phase (TSPH) on the NSL-KDD dataset. Furthermore, Figures 4(a) and 4(b) depict the PR and ROC analysis of the MHOA-DLZDAD model, highlighting robust performance with optimal ROC across various classes.

Table I portrays the attack recognition outcomes of the MHOA-DLZDAD technique on the NSL-KDD dataset. On 70% TRAPH, the MHOA-DLZDAD model achieved an average $accu_y$ of 99.52%, $prec_n$ of 87.86%, $sens_y$ of 86.05%, $spec_y$ of 99.65%, and F1-score of 86.76%; with reaming 30% TESPH, the proposed method achieved an average $accu_y$ of 99.56%, $prec_n$ of 90.03%, $sens_y$ of 88.56%, $spec_y$ of 99.68%, and F1-score of 89.17%.

TABLE I. ATTACK DETECTION ON NSL-KDD DATASET

CLass	$Accu_y$	$Prec_n$	$Sens_y$	$Spec_y$	F-1 Score
TRAPH (70%)					
Normal	99.24	99.42	99.12	99.37	99.27
DoS	99.32	99.05	99.05	99.47	99.05
Probe	99.51	96.89	98.08	99.66	97.48
R2L	99.68	91.60	94.85	99.80	93.19
U2R	99.84	52.34	39.18	99.94	44.82
Average	99.52	87.86	86.05	99.65	86.76
TESPH (30%)					
Normal	99.31	99.45	99.21	99.42	99.33
DoS	99.42	99.17	99.23	99.53	99.20
Probe	99.52	97.37	97.73	99.71	97.55
R2L	99.71	92.05	96.00	99.80	93.98
U2R	99.85	62.12	50.62	99.94	55.78
Average	99.56	90.03	88.56	99.68	89.17

(a)



(b)

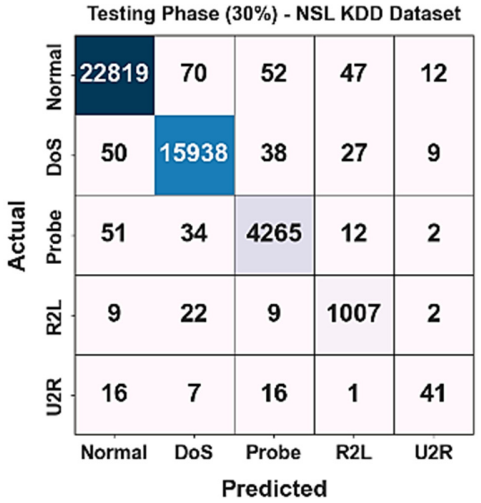
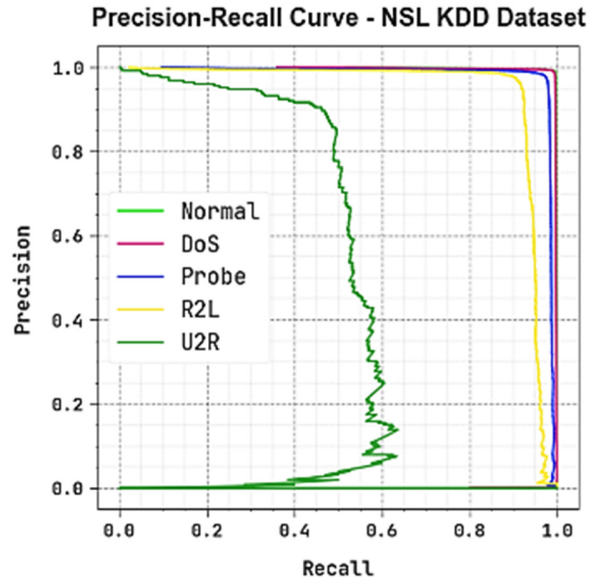


Fig. 3. NSL-KDD dataset confusion matrices of the MHOA-DLZDAD method under: (a) 70% of the TRPH dataset, (b) 30% of the TSPH dataset.

(a)



(b)

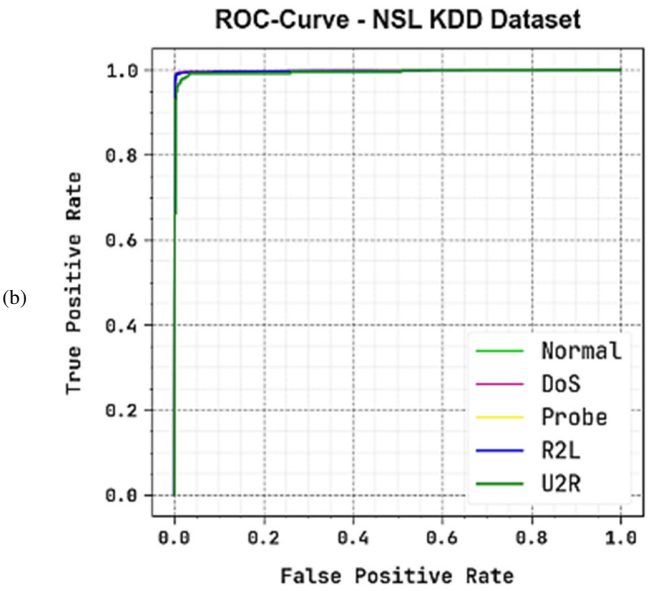


Fig. 4. NSL-KDD dataset (a-b) PR and ROC curve of the MHOA-DLZDAD method under: (a) 70% of the TRPH dataset, (b) 30% of the TSPH dataset.

TABLE II. COMPARATIVE STUDY OF MHOA-DLZDAD MODEL ON NSL-KDD DATASET [28]

NSL-KDD Dataset				
Models	$Accu_y$	$Prec_n$	$Reca_l$	**F1-score**
NB [29]	50.14	56.87	49.46	50.42
LR Model [29]	68.97	75.07	62.76	67.86
ANN Algorithm [29]	86.54	89.89	80.77	87.66
RNN [30]	76.10	88.00	60.50	71.70
KNN [31]	88.80	86.90	86.24	84.66
Decision Tree [31]	74.31	74.35	74.34	74.32
XGBoost [32]	86.70	81.30	84.00	69.80
MHOA-DLZDAD (Proposed method)	99.56	90.03	88.56	89.17

Table II presents the comparison output of the MHOA-DLZDAD technique with existing models [30-33]. The MHOA-DLZDAD model demonstrated an excellent performance with an $accu_y$ of 99.56%, $prec_n$ of 90.03%, $reca_l$ of 88.56%, and F1-score of 89.17%, while recent models, such as Naïve Bayes (NB), Logistic Regression (LR), Artificial Neural Networks (ANN), RNN, k-Nearest Neighbour (kNN), Decision Tree (DT), and XGBoost, showed lower performance.

IV. CONCLUSION

This study proposes a Metaheuristic Optimization Algorithm with Deep Learning Enabled Zero-Day Attack Detection (MHOA-DLZDAD) method for secure Industrial Internet of Things (IIoT) frameworks. The study automates and effectively identifies zero-day attacks. The proposed method includes the use of min-max scalar pre-processing, with the Elman Recurrent Neural Network (ERNN) model to detect and classify zero-day threats. Moreover, the Pelican Optimisation Algorithm (POA) is implemented to tune the ERNN model parameters. The MHOA-DLZDAD model was evaluated on a benchmark dataset, achieving a superior accuracy of 99.56%

compared to existing methods across various metrics. Future work should focus on developing more flexible models that dynamically adapt to emerging threats and integrate multiple data sources to enhance detection accuracy. Moreover, exploring advanced privacy-preserving models with Federated Learning (FL) could improve user security while maintaining high performance in anomaly detection.

DATA AVAILABILITY STATEMENT

The NSL-KDD dataset used in this study is publicly available on Kaggle at: https://www.kaggle.com/datasets/hassan06/NSL-KDD.

REFERENCES

[1] T. M. Booij, I. Chiscop, E. Meeuwissen, N. Moustafa, and F. T. H. D. Hartog, "ToN_IoT: The Role of Heterogeneity and the Need for Standardization of Features and Attack Types in IoT Network Intrusion Data Sets," *IEEE Internet of Things Journal*, vol. 9, no. 1, pp. 485–496, Jan. 2022, https://doi.org/10.1109/JIOT.2021.3085194.

[2] A. Alsaedi, N. Moustafa, Z. Tari, A. Mahmood, and A. Anwar, "TON_IoT Telemetry Dataset: A New Generation Dataset of IoT and IIoT for Data-Driven Intrusion Detection Systems," *IEEE Access*, vol. 8, pp. 165130–165150, 2020, https://doi.org/10.1109/ACCESS.2020.3022862.

[3] M. S. Elsayed, N. A. Le-Khac, S. Dev, and A. D. Jurcut, "DDoSNet: A Deep-Learning Model for Detecting Network Attacks," in *2020 IEEE 21st International Symposium on "A World of Wireless, Mobile and Multimedia Networks"*, Cork, Ireland, Aug. 2020, pp. 391–396, https://doi.org/10.1109/WoWMoM49955.2020.00072.

[4] M. A. Ahmed and S. Alnatheer, "Intrusion Detection in a Digital Twin-Enabled Secure Industrial Internet of Things Environment for Industrial Sustainability," *Engineering, Technology & Applied Science Research*, vol. 15, no. 2, pp. 21263–21269, Apr. 2025, https://doi.org/10.48084/etasr.10128.

[5] M. S. Elsayed, N.A. Le-Khac, M. A. Azer, and A. D. Jurcut, "A Flow-Based Anomaly Detection Approach With Feature Selection Method Against DDoS Attacks in SDNs," *IEEE Transactions on Cognitive Communications and Networking*, vol. 8, no. 4, pp. 1862–1880, Dec. 2022, https://doi.org/10.1109/TCCN.2022.3186331.

[6] M. I. H. Okfie and S. Mishra, "Anomaly Detection in IIoT Transactions using Machine Learning: A Lightweight Blockchain-based Approach," *Engineering, Technology & Applied Science Research*, vol. 14, no. 3, pp. 14645–14653, June 2024, https://doi.org/10.48084/etasr.7384.

[7] Y. Li *et al.*, "A Survey on Dropout Methods and Experimental Verification in Recommendation," *IEEE Transactions on Knowledge and Data Engineering*, pp. 6595–6615, 2022, https://doi.org/10.1109/TKDE.2022.3187013.

[8] C. Atheeq, R. Sultana, S. A. Sabahath, and M. A. K. Mohammed, "Advancing IoT Cybersecurity: Adaptive Threat Identification with Deep Learning in Cyber-Physical Systems," *Engineering, Technology & Applied Science Research*, vol. 14, no. 2, pp. 13559–13566, Apr. 2024, https://doi.org/10.48084/etasr.6969.

[9] R. H. Hwang, M. C. Peng, C. W. Huang, P.-C. Lin, and V.-L. Nguyen, "An Unsupervised Deep Learning Model for Early Network Traffic Anomaly Detection," *IEEE Access*, vol. 8, pp. 30387–30399, 2020, https://doi.org/10.1109/ACCESS.2020.2973023.

[10] Y. Xiao, C. Xing, T. Zhang, and Z. Zhao, "An Intrusion Detection Model Based on Feature Reduction and Convolutional Neural Networks," *IEEE Access*, vol. 7, pp. 42210–42219, 2019, https://doi.org/10.1109/ACCESS.2019.2904620.

[11] P. B. Arun, V. Mohan and K. V. Kumar, "Hybrid Metaheuristics with Deep Learning Enabled Cyberattack Prevention in Software Defined Networks," *Tehnicki vjesnik - Technical Gazette*, vol. 31, no. 1, Feb. 2024, https://doi.org/10.17559/TV-20230621000752.

[12] S. K. Gupta, M. Tripathi, and J. Grover, "Hybrid Optimization and Deep Learning Based Intrusion Detection System," *Computers and Electrical Engineering*, vol. 100, May 2022, Art. no. 107876, https://doi.org/10.1016/j.compeleceng.2022.107876.

[13] J. Manokaran and G. Vairavel, "DL-ADS: Improved Grey Wolf Optimization Enabled AE-LSTM Technique for Efficient Network Anomaly Detection in Internet of Thing Edge Computing," *IEEE Access*, vol. 12, pp. 75983–76002, 2024, https://doi.org/10.1109/ACCESS.2024.3405628.

[14] P. Manickam *et al.*, "Billiard Based Optimization With Deep Learning Driven Anomaly Detection in Internet of Things Assisted Sustainable Smart Cities," *Alexandria Engineering Journal*, vol. 83, pp. 102–112, Nov. 2023, https://doi.org/10.1016/j.aej.2023.10.039.

[15] A. Shali, A. Chinnasamy, and P. Selvakumari, "Development of Novel Intrusion Detection in Internet of Things Using Improved Dart Game Optimizer-derived Optimal Cascaded Ensemble Learning," *Transactions on Emerging Telecommunications Technologies*, vol. 35, no. 7, July 2024, Art. no. e5018, https://doi.org/10.1002/ett.5018.

[16] A. Alsirhani, M. Mujib Alshahrani, A. M. Hassan, A. I. Taloba, R. M. Abd El-Aziz, and A. H. Samak, "Implementation of African vulture optimization algorithm based on deep learning for cybersecurity intrusion detection," *Alexandria Engineering Journal*, vol. 79, pp. 105–115, Sept. 2023, https://doi.org/10.1016/j.aej.2023.07.077.

[17] S. Shen, C. Cai, Z. Li, Y. Shen, G. Wu, and S. Yu, "Deep Q-Network-Based Heuristic Intrusion Detection Against Edge-Based SIoT Zero-Day Attacks," *Applied Soft Computing*, vol. 150, Jan. 2024, Art. no. 111080, https://doi.org/10.1016/j.asoc.2023.111080.

[18] M. Soltani, B. Ousat, M. Jafari Siavoshani, and A. H. Jahangir, "An Adaptable Deep Learning-based Intrusion Detection System to Zero-day Attacks," *Journal of Information Security and Applications*, vol. 76, Aug. 2023, Art. no. 103516, https://doi.org/10.1016/j.jisa.2023.103516.

[19] H. Cui, T. Xue, Y. Liu, and B. Liu, "Transferable Intrusion Detection Model for Industrial Internet Based on Deep Learning: IIDS Model Combining Hybrid Deep Learning Model and Transfer Learning," in *Proceedings of the 2024 3rd International Conference on Cryptography, Network Security and Communication Technology*, Harbin, China, Jan. 2024, pp. 107–113, https://doi.org/10.1145/3673277.3673296.

[20] X. Wang, Y. Wang, Z. Javaheri, L. Almutairi, N. Moghadamnejad, and O. S. Younes, "Federated Deep Learning for Anomaly Detection in the Internet of Things," *Computers and Electrical Engineering*, vol. 108, May 2023, Art. no. 108651, https://doi.org/10.1016/j.compeleceng.2023.108651.

[21] K. Saurabh, V. Sharma, U. Singh, R. Khondoker, R. Vyas, and O. P. Vyas, "HMS-IDS: Threat Intelligence Integration for Zero-Day Exploits and Advanced Persistent Threats in IIoT," *Arabian Journal for Science and Engineering*, vol. 50, no. 2, pp. 1307–1327, Jan. 2025, https://doi.org/10.1007/s13369-024-08935-5.

[22] P. L. S. Jayalaxmi, R. Saha, G. Kumar, M. Alazab, M. Conti, and X. Cheng, "PIGNUS: A Deep Learning Model for IDS in Industrial Internet-of-Things," *Computers and Security*, vol. 132, Sept. 2023, Art. no. 103315, https://doi.org/10.1016/j.cose.2023.103315.

[23] A. Arun, A. S. Nair, and A. G. Sreedevi, "Zero Day Attack Detection and Simulation through Deep Learning Techniques," in *14th International Conference on Cloud Computing, Data Science and Engineering (Confluence)*, Noida, India, Jan. 2024, pp. 852–857, https://doi.org/10.1109/Confluence60223.2024.10463429.

[24] J. Zhang, S. Liang, F. Ye, R. Q. Hu, and Y. Qian, "Towards Detection of Zero-Day Botnet Attack in IoT Networks Using Federated Learning," in *ICC 2023 - IEEE International Conference on Communications*, Rome, Italy, May 2023, pp. 7–12, https://doi.org/10.1109/ICC45041.2023.10279423.

[25] M. Sayduzzaman, A. Rahman, J. T. Tamanna, D. Kundu, and T. Rahman, "Interoperability and Explicable AI-based Zero-Day Attacks Detection Process in Smart Community." arXiv, Oct. 11, 2025, https://doi.org/10.48550/arXiv.2408.02921.

[26] G. Parimala and R. Kayalvizhi, "Improved Elman Deep Learning Model for Intrusion Detection System in Internet of Things," *Journal of Internet Services and Information Security*, vol. 14, no. 1, pp. 121–137, Mar. 2024, https://doi.org/10.58346/JISIS.2024.I1.008.

[27] A. R. Sagor *et al.*, "Pelican Optimization Algorithm-Based Proportional–Integral–Derivative Controller for Superior Frequency Regulation in

Interconnected Multi-Area Power Generating System," *Energies*, vol. 17, no. 13, July 2024, Art. no. 3308, https://doi.org/10.3390/en17133308.

[28] Z. Hasan, "NSL-KDD Dataset." Kaggle, 2018, [Online]. Available: https://www.kaggle.com/datasets/hassan06/NSL-KDD.

[29] I. Priyadarshini, "Anomaly Detection of IoT Cyberattacks in Smart Cities Using Federated Learning and Split Learning," *Big Data and Cognitive Computing*, vol. 8, no. 3, Feb. 2024, Art. no. 21, https://doi.org/10.3390/bdcc8030021.

[30] A. Meliboev, J. Alikhanov, and W. Kim, "Performance Evaluation of Deep Learning Based Network Intrusion Detection System across Multiple Balanced and Imbalanced Datasets," *Electronics*, vol. 11, no. 4, Feb. 2022, Art. no. 515, https://doi.org/10.3390/electronics11040515.

[31] G. Nassreddine, M. Nassereddine, and O. Al-Khatib, "Ensemble Learning for Network Intrusion Detection Based on Correlation and Embedded Feature Selection Techniques," *Computers*, vol. 14, no. 3, Feb. 2025, Art. no. 82, https://doi.org/10.3390/computers14030082.

[32] O. H. Abdulganiyu, T. Ait Tchakoucht, A. E. H. Alaoui, and Y. K. Saheed, "Attention-driven Multi-model Architecture for Unbalanced Network Traffic Intrusion Detection via Extreme Gradient Boosting," *Intelligent Systems with Applications*, vol. 26, June 2025, Art. no. 200519, https://doi.org/10.1016/j.iswa.2025.200519.