IEEE Access
Multidisciplinary ⁝ Rapid Review ⁝ Open Access Journal

Received 20 December 2023, accepted 8 January 2024, date of publication 10 January 2024,
date of current version 19 January 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3352568

RESEARCH ARTICLE

Enhancing Cybersecurity in the Internet of Things Environment Using Bald Eagle Search Optimization With Hybrid Deep Learning

LOUAI A. MAGHRABI[1], (Member, IEEE), SAHAR SHABANAH[2,3], TURKI ALTHAQAFI[4], DHEYAALDIN ALSALMAN[5], SULTAN ALGARNI[6], ABDULLAH AL-MALAISE AL-GHAMDI[4,6], AND MAHMOUD RAGAB[7,8,9]

[1]Department of Software Engineering, College of Engineering, University of Business and Technology, Jeddah, Saudi Arabia
[2]Computer Science Department, School of Engineering, Computing and Design, Dar Al-Hekma University, Jeddah 22246, Saudi Arabia
[3]Computer Science Department, Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah 21589, Saudi Arabia
[4]Information Systems Department, School of Engineering, Computing and Design, Dar Al-Hekma University, Jeddah 22246, Saudi Arabia
[5]Department of Cybersecurity, School of Engineering, Computing and Design, Dar Al-Hekma University, Jeddah 22246, Saudi Arabia
[6]Information Systems Department, Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah 21589, Saudi Arabia
[7]Information Technology Department, Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah 21589, Saudi Arabia
[8]Mathematics Department, Faculty of Science, Al-Azhar University, Naser City, Cairo 11884, Egypt
[9]Center of Research Excellence in Artificial Intelligence and Data Science, King Abdulaziz University, Jeddah 21589, Saudi Arabia

Corresponding author: Mahmoud Ragab (mragab@kau.edu.sa)

This research work was funded by Institutional Fund Projects under grant no. (IFPIP: 378-611-1443) and supported by the Ministry of Education and Deanship of Scientific Research (DSR), King Abdulaziz University (KAU), Jeddah, Saudi Arabia.

ABSTRACT Nowadays, the Internet of Things (IoT) has become a rapid development; it can be employed by cyber threats in IoT devices. A correct system to recognize malicious attacks at IoT platforms became of major importance to minimize security threats in IoT devices. Botnet attacks have more severe and common attacks and it is threaten IoT devices. These threats interrupt IoT alteration by interrupting networks and services for IoT devices. Several existing methods present themselves to determine unknown patterns in IoT networks for improving security. Recent analysis presents DL and ML methods for classifying and detecting botnet attacks from the IoT environment. Consequently, this paper develops a Bald Eagle Search Optimization with a Hybrid Deep Learning based botnet detection (BESO-HDLBD) algorithm in an IoT platform. The presented BESO-HDLBD approach aims to resolve the security issue by identifying the botnets in the IoT environment. To reduce the high dimensionality problem, the BESO-HDLBD method uses the BESO system for the feature selection process. For botnet detection purposes, the BESO-HDLBD algorithm uses HDL, which is an integration of convolutional neural networks (CNNs), bidirectional long short-term memory (BiLSTM), and attention concept. The desire for the HDL technique in botnet detection utilises the intricate nature of botnet attacks that frequently contain difficult and developing patterns. Combining CNNs permits for effectual feature extraction from spatial data, BiLSTM networks capture temporal dependencies, and attention mechanisms improve the model's capability to concentrate on fundamental patterns. The selection of hyperparameters of the HDL approach takes place using the dragonfly algorithm (DFA). The experimental analysis of the BESO-HDLBD system could be examined under a benchmark botnet dataset. The obtained outcome infers a better outcome of the BESO-HDLBD technique compared to the recent detection system with respect to distinct estimation measures.

INDEX TERMS Cybersecurity, Internet of Things, botnet attacks, machine learning, parameter tuning, smart environment.

I. INTRODUCTION

The increase in the Internet of Things (IoT) devices has caused a consistent rise in the quantity of IoT-based attacks.

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

The IoT botnet attack has been considered the major IoT threat, which attempts to commit actual, useful, and gainful cyber threats [1]. IoT botnets have been groups of Internet-linked IoT devices to are corrupted with malware and directed remotely by attackers [2]. Because of the rapid expansion of threats as well as miscellany in attack strategies, IoT systems have considerable challenging issues in providing methods to detect threats and security attacks. Since malware has been implemented, there is an enhanced count of developments in machine learning (ML) and deep learning (DL) based classification devices and methods that utilize entire time sequence information. There are significant issues in existing techniques to identify proper and efficient strategies to defend IoT devices from botnet attacks [3]. A botnet attack is known as a severe threat dispersed quickly among systems linked to the Internet. To keep IoT devices from botnet threats, there are key gaps in earlier tools for determining suitable and effectual procedures [4].

The intrusion detection system (IDS) is an effective performance to deal with botnet threats. It employs AI to find novel forms of botnet threats [5]. The IDS is classified into 2 kinds such as anomaly and misuse techniques. These kinds rely on existing signatures. Many IDSs exist, like Snort and Suricata. Furthermore, the previous classification would permit better IoT Botnet response solutions. Consequently, it minimizes the damage produced by probable threats. The dynamic analysis technique observes in what way malware communicates with its environment when it could be implemented [6]. The information is significant for Ml and DL types finding malware. The illustrative methods require constant sequence information gathering while the malware is executing. During this case, the malware effectively performed its objective of data system damage and completely showed its aggressive character [7]. There are presently existing classification methods for such phases, hence, once a DDoS attack done by an IoT Botnet has previously ensued, recognizing the DDoS threat and the IoT Botnet system alone at this place could not be too difficult [8].

Presently, artificial intelligence (AI) techniques are utilized to find IoT threats with additional guaranteed recognition [9]. AI techniques even can find changes in networks and approaches to threats. Several problems are posed by safety solutions to deal with IoT threats: attackers will make a few variations in earlier threats that safety solutions are not able to find. Recent studies have focused on the design of AI tools for the detection of attacks in the IoT environment [10]. DL and ML have been designed into safety devices to find such threats proficiently. DL is one of the AI developments are exist in numerous real-life applications for handling complex non-linear information.

This study introduces a Bald Eagle Search Optimization with a Hybrid Deep Learning based botnet detection (BESO-HDLBD) technique in an IoT environment. The presented BESO-HDLBD technique aims to resolve the security issue by identifying the botnets in the IoT environment. To reduce the high dimensionality problem, the BESO-HDLBD technique uses the BESO method for the FS technique. For botnet detection purposes, the BESO-HDLBD system employs HDL, which is an integration of convolutional neural networks (CNNs), bidirectional long short-term memory (Bi-LSTM), and attention concept. Since manual hyperparameter tuning is a tedious and laborious process, metaheuristics-based dragonfly algorithm (DFA) can be used to select the hyperparameters of the HDL model. The simulation validation of the BESO-HDLBD system is determined under a benchmark botnet database. The key contribution is summarized as follows.

- An intelligent BESO-HDLBD technique is particularly adapted for IoT platforms, purpose of recognizing and mitigating botnet attacks effectively. It contains BESO-based feature subset selection, HDL-based detection, and DFA-based hyperparameter tuning established for botnet recognition. According to our perception, the BESO-HDLBD method does not exist in the works.
- To address the higher dimensionality problem, the BESO-HDLBD algorithm integrates the BESO system for feature selection. This stage supports decreasing the complexity of the database and concentrating on appropriate features for botnet recognition.
- Employs an HDL technique for botnet recognition that contains CNN, BiLSTM, and attention models, offering a widespread and effectual performance to identify difficult patterns connected with botnet attacks.
- Utilizes the DFA to adjust hyperparameters in the HDL methodology. This ensures that the DL approach is adjusted for optimum solution in botnet detection.

II. RELATED WORKS

Catillo et al. [11] developed a new IoT-driven cross-device technique that enables learning an individual IDS approach rather than numerous distinct methods on the traffic of various IoT systems. A semi-supervised method is used because of its broader suitability in unexpected threats. The result relies on an all-in-one DAE that contains training an individual DNN with usual traffic from several types of IoT systems. Popoola et al. [12] suggested an effective DL-based botnet threat recognition technique. Especially, SMOTE produces a extra few instances to attain class stability, although DRNN learns hierarchical feature representation in the stable network traffic data to execute differentiated categorization. In [13], one class classifier-based ML solution is introduced for the recognition of IoT botnets from heterogeneous surroundings. This technique is a lightweight approach that employs choosing the optimal feature using famous filter and wrapper techniques to select features. The suggested approach is assessed over several datasets.

Alshahrani et al. [14] developed an automated BDC-RSOD model to detect botnets. Primarily, the network data has pre-processing and the RSO technique is exploited for electing features. Moreover, the LSTM technique can be used for the detection of botnets. In [15], a DL structure of Bot detection called DeBot has been projected. DeBot utilizes a new Cascade Forward BPNN (CFBPNN) method with a subclass of features utilizing the Correlation-based FS (CFS) procedure. Hezam et al. [16] introduced the BiLSTM CNN model that combines bidirectional LSTM and CNN. This proposed technique applies the CNN model to process data and optimize features with the BiLSTM classifier.

Kirubavathi and Sridevi [17] devised a Botnet recognition approach to find a threat to real-time traffic. Next, the study relates and differentiates various ML and DL approaches for finding Botnets on the standard features. Then, the new packet-captured (pcap) documents from the Aposemat IoT 23 database are examined for threats. Then DL technique GRU can be applied to find the malware threats. In [18], an effective approach for botnet detection is presented. This was done by an innovative combination of the architectural CNN with the LSTM (CNN-LSTM) procedure to find 2 usual and severe IoT attacks.

Dakic et al. [19] examine a hybrid design, dubbed as HybNet that interchanges among DL and matched filter pathways depending on the supposed interference level. This supports the detector to work in a wider range of conditions, optimally leveraging either the matched filter or DL benefits. Presekal et al. [20] present a new technique for online cyber threats situational awareness that improves power grid resilience. It helps power system operators from the detection and localization of active attack places in Operational Technology (OT) networks from close real-time. In [21], an effectual and dependable DCNNBiLSTM approach for network intrusion detection depends on a realistic network traffic database has been presented. Al Sawafi et al. [22] examined an IDS technique utilizing the hybridization of supervised and semi-supervised DL for network traffic classifiers for known and unknown abnormal behaviours from the IoT platform.

III. THE PROPOSED MODEL

For accomplishing security in the IoT environment, this study has presented a novel BESO-HDLBD approach for automated botnet detection. The BESO-HDLBD method aims to resolve the security issue by identifying the botnets in the IoT environment. It encompasses three major processes namely BESO-based FS subset, HDL-based classification, and DFA-based hyperparameter tuning. Fig. 1 represents the workflow of the BESO-HDLBD method.

A. STAGE I: FEATURE SELECTION USING BESO ALGORITHM

Primarily, the BESO-HDLBD technique uses the BESO algorithm for the feature selection process. BESO algorithm is a new meta-heuristic optimization model whose main inspiration comes from the hunting behaviors of bald eagles (North American predatory birds) [23].

The core idea of BESO is to emulate the bald eagle's behaviors while fishing and flying. Bald eagles choose and locate the finest hunting area with respect to food quantity. These behaviors are quantitatively represented in the following.

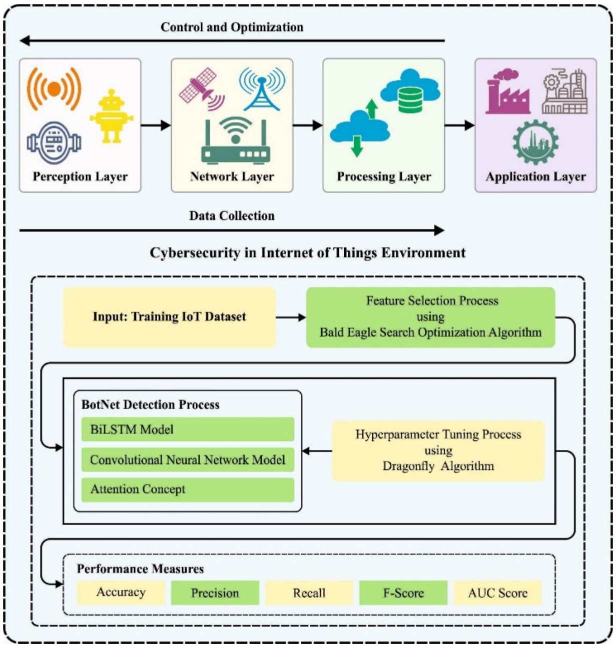

FIGURE 1. Workflow of BESO-HDLBD algorithm.

$$P_{new,i} = P_{best} + \alpha \times r\left(P_{ave} - P_i\right) \tag{1}$$

In Eq. (1), the parameter α is used to manage variation in position that proceeds a value within 1.5 and 2. r is an arbitrary integer taking a value within [0, 1]. The eagles search for the nearby region to select an area according to intelligence that is now available during the search phase. P_{best} refers to the search area that the eagle selects based on the optimal location found during the search. During the searching phase, the eagle searches for the prey in the designated region, and moves in the spiral to quicken the hunt. The optimum location for the swooping can be a mathematical expression as in the following.

$$P_{i,new} = P_i + y(i) \times (P_i - P_{i+1}) + x(i) \times (P_i - P_{mean}) \tag{2}$$

$$x(i) = \frac{xr(i)}{\max(|xr|)}, y(i) = \frac{yr(i)}{\max(|yr|)} \tag{3}$$

$$xr(i) = r(i) \times \sin(\theta(i)), yr(i) = r(i) \times \cos(\theta(i)) \tag{4}$$

$$\theta(i) = a \times \pi \times rand \tag{5}$$

$$r(i) = \theta(i) + R \times rand \tag{6}$$

Here, the parameter a determines the corner between the point search at the center point, taking a value between 5 and 10, and the parameter R determines the number of search cycles, taking a value between 0.5 and 2 [23]. Bald eagles swoop towards the prey during the swooping phase. Each moves to the fittest location for the target.

$$P_{i,new} = rand \times P_{best} + x(i) \times (P_i - C_1 \times P_{mean}) + y_1(i) \times (P_i - C_2 \times P_{best})\, vec_1, c_2 \in [1, 2] \tag{7}$$

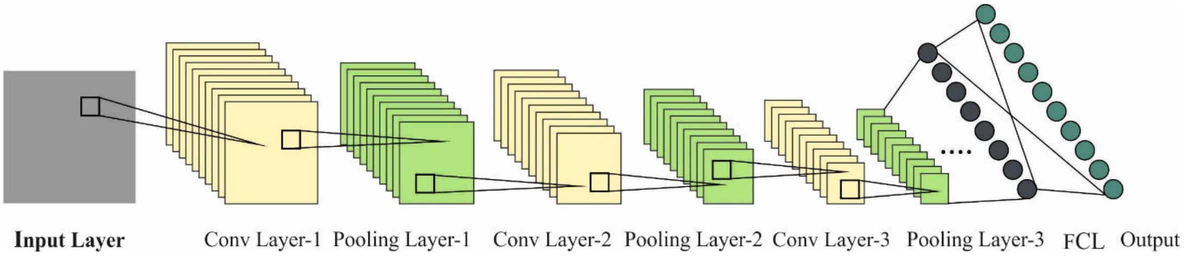

FIGURE 2. CNN structure.

$$x_1(i) = \frac{xr(i)}{\max(|xr|)}, y_1(i) = \frac{yr(i)}{\max(|yr|)} \tag{8}$$

$$r(i) = r(i) \times \sinh[(\theta(i))], yr(i) = r(i) \times \cosh[(\theta(i))] \tag{9}$$

$$\theta(i) = a \times \pi \times rand\ ver(i) = \theta(i) \tag{10}$$

During the BESO-FS methodology, the objectives can be integrated as a single main formula such that a present weight recognizes all the major significance [24]. In this condition, implemented an FF that adds these purposes of FS as represented in Eq. (11).

$$Fitness(X) = \alpha \cdot E(X) + \beta * \left(1 - \frac{|R|}{|N|}\right) \tag{11}$$

where,$|R|$ and $|N|$ denote the elected feature counts and the amount of novel features in the database, $Fitness(X)$ denotes the fitness value X, $E(X)$ stands for the classifier errors by utilizing the optimum feature in the X subset; α and β imply the classifier errors and reduced ratio, $\alpha \in [0, 1]$ and $\beta= (1-\alpha)$.

B. STAGE II: BOTNET DETECTION UTILIZING HDL

To accurately detect and classify botnets, the HDL model is applied. The Bi-LSTM is the optimum way to create synthetic well-log curves by taking the value of the good logs along depth as a systematic sequence into account because it can able to transmit data in neighboring depths with depth-term dependence and also capture data from a sequence of data [25]. In the meantime, the benefits of the attention mechanism and CNN in extracting the high-level features have been presented. The Bi-LSTM comprises 2 branches, where one utilizes CNN for capturing the features of well loggings and the other performs the FS by using a 2-layer Bi-LSTM with the attention module.

The X sequence matrix along depth is formulated by Eq. (12) for well logs measurement.

$$X = \begin{bmatrix} x_1^1 & x_1^2 & \cdots & x_1^n \\ x_2^1 & x_2^2 & \cdots & x_2^n \\ \vdots & \vdots & \vdots & \vdots \\ x_i^1 & x_i^2 & \cdots & x_i^n \\ \vdots & \vdots & \vdots & \vdots \\ x_d^1 & x_d^2 & \cdots & x_d^n \end{bmatrix} \tag{12}$$

where the attribute value of n well-logging at d depth is $\chi_d= (x_d^1, x_d^2, \ldots, x_d^n)$. The set $\chi^n= (x_{1,}^n x_{2,}^n \ldots, x_i^n, \ldots, x_d^n)$ represents the value of a specific well-log curve along the depth, namely GR, CNL, SP, and so on. $Y=(y_1, y_2, \ldots, y_i, \ldots, y_d)$ refers to the measurement of predicted well-logs. X and Y correspondingly have been the output and input of the CNN-BiLSTM-AT algorithm.

X is passed to the convolution operator in the CNN model. 1D convolution operator slides 128 filtering with a similar window dimension of 1 over depth sequence for capturing the lower level feature in the new well-loggings. Next, the max-pooling function has been used to decrease the size of feature mapping. A dropout function has been used to avoid the over-fitting of CNN. ReLu is applied as a non-linear activation function. Lastly, a dense layer with 100 neurons can employed to execute linear function and a fattened layer changes the direction of the dimension. Fig. 2 represents the substructure of CNN.

The two-layer BiLSTM is used to capture the context data from the well-log. Bi-LSTM with 50 cell units gain the knowledge in the subsequent term of the present log sequence and learn the knowledge in the prior term of the present log point, hence the feature grabbed by the Bi-LSTM is considered as two representations of the well-log. During the attention layer, the attention model highlights the key feature of the log curve to decrease the influence of non-key features in the well-log. The attention layer comprises a softmax activation function and an FC unit with 100 neurons. In the Bi-LSTM layer, the tanh function can designated as the nonlinear activation function. The extraction feature in the Bi-LSTM is provided as the attention layer and later additional to the outcome of the FC unit. A single dense unit follows the attention layer. The output from Bi-LSTM-AT and the CNN branches have been concatenated before passed as the final dense layer with one neuron. At last, the predictive Y is generated in the CNN-BiLSTM-AT algorithm.

C. STAGE III: PARAMETER TUNING USING DFA

For the parameter tuning procedure, the DFA approach has been utilized in this work. DFA is the new SI optimization algorithm whose core motivation is the swarm behaviours of dragonflies (DFs) under migration and hunting [26]. Based on five crucial factors, the individual in the swarm changes their location as follows: cohesion, separation, alignment, distraction, and attraction. Alignment can be measured through an average of adjacent places, and cohesion was defined by variance among the current individual location and alignment. Attraction has been expressed by the distance to distraction, and food sources represent the total of the enemy as well as present different locations. Separation refers to the sum of distances of separate positions from other positions. The enemy is the worst performance, whereas the food source is one of the fittest solutions. The updating place of the individual swarm can be given as follows.

$$x_i^{t+1} = x_i^t + \Delta x_i^{t+1} \tag{13}$$

In Eq. (13), x_i^t is the existing location of i^{th} individuals, t shows iteration count, and Δx_i^{t+1} refers to the step vector:

$$\Delta x_i^{t+1} = (sS_i + aA_i + cC_i + fF_i + eE_i) + w\Delta x_i^t \tag{14}$$

In Eq. (14), F_i, S_j, A_j, E_i, and C_j indicate the attraction, separation, alignment, distraction, and cohesion values, correspondingly. w denotes the inertia weight. c, s, f, a, and e are cohesion, separation, attraction, alignment, and distraction coefficients correspondingly. The DFs have neighborhoods within a specific radius. In the iterations, the radius can augmented for exploring the global optima. When there are no other DFs in the neighborhood, then DFs exploit the random walking as given below:

$$x_i^{t+1} = x_i^t + Levy\,(d) \times x_i^t \tag{15}$$

In Eq. (15), d refers to the size of the searching space, and $levy(\cdot)$ denotes the Levy flight process. High alignment and Lower cohesion weight can be utilized by the smaller radius. At the iteration, the greater the cohesion, the lesser the alignment, and the larger the radius. Consequently, the parameter must be updated until the ending condition is satisfied.

The DFA methodology progresses an FF to realize a good classifier outcome. This describes a positive integer for implying the best outcome of the candidate outcomes. The decrease of the classifier errors could be determined to be FF, as represented in Eq. (16).

$$\begin{aligned} fitness\,(x_i) &= ClassifierErrorRate\,(x_i) \\ &= \frac{No.of\ misclassified\ instances}{Total\ No.\ of\ instances} * 100 \end{aligned} \tag{16}$$

IV. EXPERIMENTAL VALIDATION

In this section, the botnet detection outcome of the BESO-HDLBD system has been tested employing the CTU-13 dataset [27], comprising 20689 instances with two class labels as depicted in Table 1. The dataset comprises both normal and Botnet traffic. Normal Traffic contains the packets that are sent from a source to a destination and not deployed among the transmission. Botnet traffic comprises individual packets that are sent by a Botmaster or by a system that is in the mechanism of a Botmaster.

TABLE 1. Details on database.

Class	No. of Instances
Botnet	2554
Normal	18135
Total Instances	20689

Fig. 3 depicts the confusion matrices achieved through the BESO-HDLBD methodology under 80:20 and 70:30 of the TRPH/TSPH. The accomplished values indicated the efficient recognition of the Botnet and Normal samples with each class.

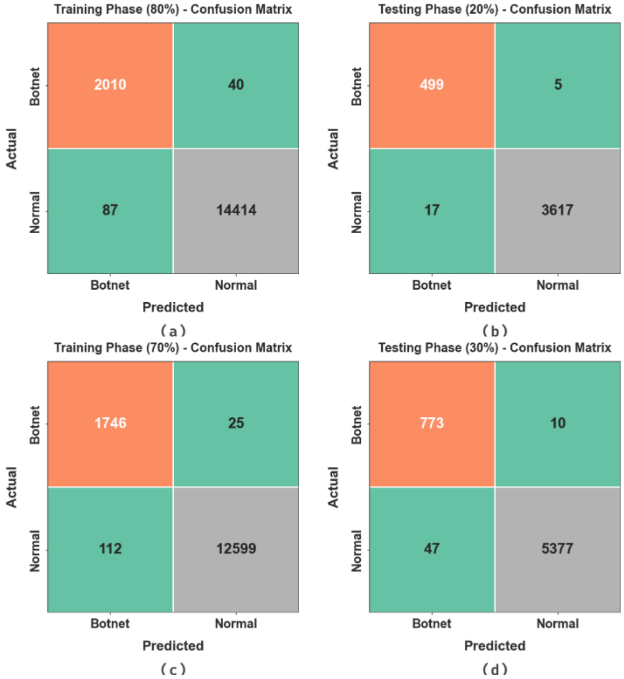

FIGURE 3. Confusion matrices of BESO-HDLBD model (a-c) TRPH of 80% and 70%; (b-d) TSPH of 20% and 30%.

The botnet detection analysis of the BESO-HDLBD system can be exhibited at 80:20 of TRPH/TSPH in Table 2 and Fig. 4. The experimental findings show the BESO-HDLBD approach identifies the botnet and normal samples. According to 80% of the TRPH, the BESO-HDLBD model offers average $accu_y$, $prec_n$, $reca_l$, F_{score}, and AUC_{score} values of 98.72%, 97.79%, 98.72%, 98.25%, and 98.72%. Also, based on 20% of the TSPH, the BESO-HDLBD algorithm offers average $accu_y$, $prec_n$, $reca_l$, F_{score}, and AUC_{score} values of 99.27%, 98.28%, 99.27%, 98.77%, and 99.27% correspondingly.

The botnet detection outcome of the BESO-HDLBD approach is defined with 70:30 of the TRPH/TSPH in Table 3 and Fig. 5. The accomplished result implied that the BESO-HDLBD algorithm recognizes the botnet and normal instances. With 70% of the TRPH, the BESO-HDLBD method gains average $accu_y$, $prec_n$, $reca_l$, F_{score}, and AUC_{score} values of 99.05%, 96.89%, 98.85%, 97.84%, and 98.85% correspondingly. Moreover, on 30% of the TSPH, the BESO-HDLBD system reaches average $accu_y$, $prec_n$, $reca_l$,

TABLE 2. Botnet detection analysis of the BESO-HDLBD model at 80:20 of TRPH/TSPH.

Class	$Accu_y$	$Prec_n$	$Reca_l$	F_{score}	AUC_{score}
TRPH (80%)					
Botnet	98.05	95.85	98.05	96.94	98.72
Normal	99.40	99.72	99.40	99.56	98.72
Average	98.72	97.79	98.72	98.25	98.72
TSPH (20%)					
Botnet	99.01	96.71	99.01	97.84	99.27
Normal	99.53	99.86	99.53	99.70	99.27
Average	99.27	98.28	99.27	98.77	99.27

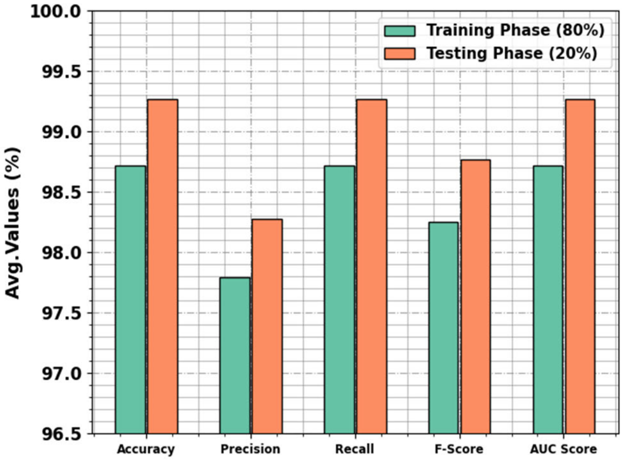

FIGURE 4. Average of BESO-HDLBD methodology under 80:20 of TRPH/TSPH.

TABLE 3. Botnet detection analysis of BESO-HDLBD system at 70:30 of TRPH/TSPH.

Class	$Accu_y$	$Prec_n$	$Reca_l$	F_{score}	AUC_{score}
TRPH (70%)					
Botnet	99.05	93.97	98.59	96.22	98.85
Normal	99.05	99.80	99.12	99.46	98.85
Average	99.05	96.89	98.85	97.84	98.85
TSPH (30%)					
Botnet	99.08	94.27	98.72	96.44	98.93
Normal	99.08	99.81	99.13	99.47	98.93
Average	99.08	97.04	98.93	97.96	98.93

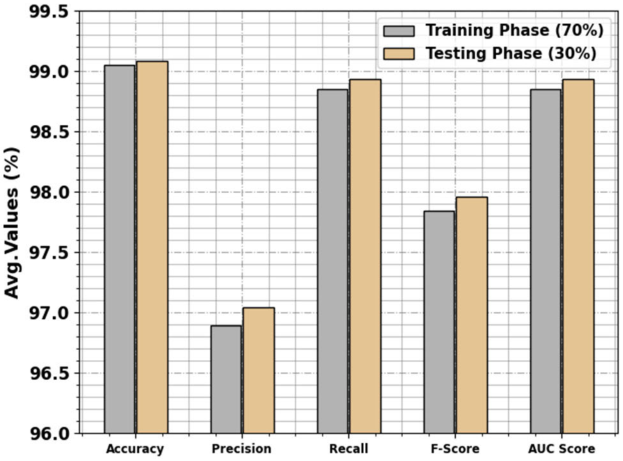

FIGURE 5. Average of BESO-HDLBD method with 70:30 of TRPH/TSPH.

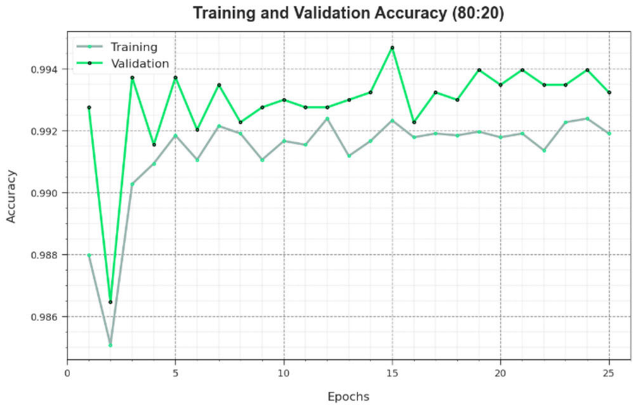

FIGURE 6. $Accu_y$ curve of BESO-HDLBD model on 80:20 of TRPH/TSPH.

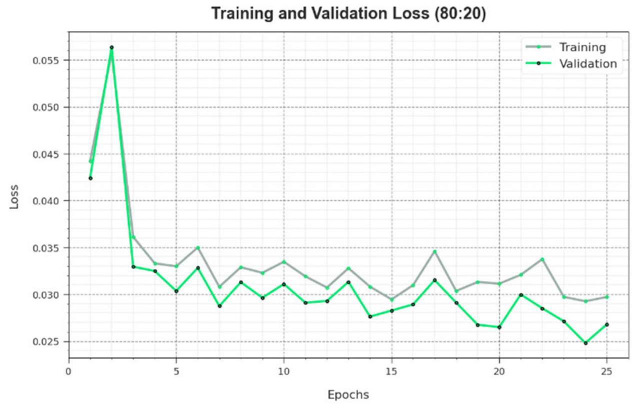

FIGURE 7. Loss curve of BESO-HDLBD technique on 80:20 of TRPH/TSPH.

F_{score}, and AUC_{score} values of 99.08%, 97.04%, 98.93%, 97.96%, and 98.93% correspondingly.

To determine the performance of the BESO-HDLBD system under 80:20 of TRPH/TSPH, TRA and TES $accu_y$ curves are determined, as illustrated in Fig. 6. The TRA and TES $accu_y$ curves show the effectiveness of the BESO-HDLBD method at numerous epochs. This figure gives important details approximately the generalization proficiencies and learning tasks of the BESO-HDLBD method. With increased epochs, it can be perceived that the TRA and TES $accu_y$ curves acquire enhanced. This can be evidenced by the BESO-HDLBD technique attaining improved TES $accu_y$ that has the possibility for recognizing the patterns from the data of TRA and TES.

Fig. 7 displays the wide-ranging TRA and TES loss values of the BESO-HDLBD system under 80:20 of the TRPH/TSPH across diverse epochs. The TRA loss illustrates the model loss gets lessened. Primarily, this can be modified

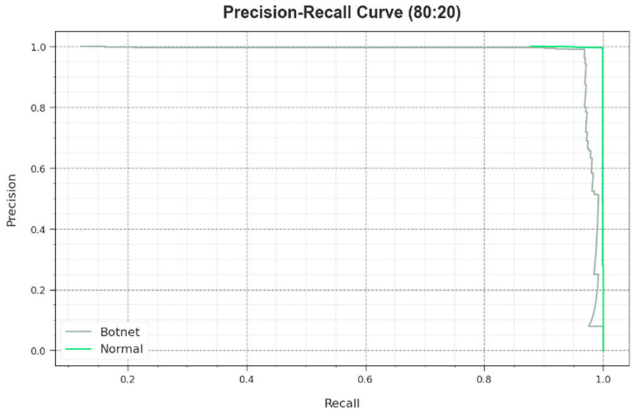

FIGURE 8. PR curve of BESO-HDLBD system at 80:20 of TRPH/TSPH.

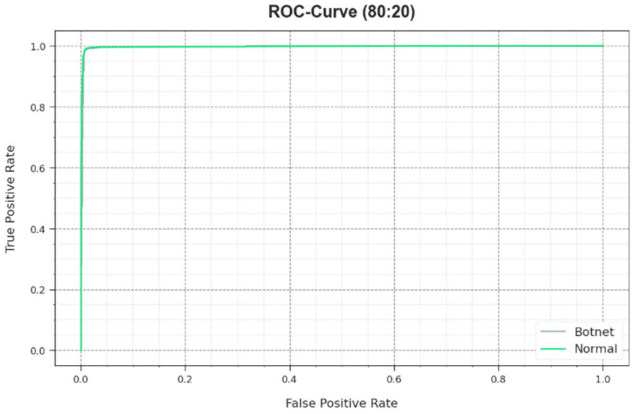

FIGURE 9. ROC curve of BESO-HDLBD algorithm at 80:20 of TRPH/TSPH.

the weight for minimising the classifier error under the TRA and TES data. These loss curves represent the level of a model that fits the data of TRA. This can be seen that the TRA and TES loss steadily minimalized as well as displayed that the BESO-HDLBD method efficaciously learns the patterns indicated in data of the TRA and TES. It can be observed that the BESO-HDLBD algorithm adapts the parameters to diminish the variance amongst the predictions and actual training labels.

The PR analysis of the BESO-HDLBD method at 80:20 of the TRPH/TSPH can be revealed in Fig. 8. The accomplished findings confirm that the BESO-HDLBD algorithm gets higher PR values with 2 classes. This represents the model for learning and recognizing different class labels. The BESO-HDLBD methodology gain improved experimental findings in the identification of positive instances with lessening of false positives.

The ROC analysis described by the BESO-HDLBD technique with 80:20 of the TRPH/TSPH can be illustrated in Fig. 9, it has been capabilities to the discrepancy of the classes. The figure identifies valued insights into the trade-off between the FPR and TPR through various classification epochs and thresholds. It reveals the correct predictions of the BESO-HDLBD system under the classification of numerous classes.

TABLE 4. Comparison analysis of the BESO-HDLBD system with other techniques [14], [28].

Methods	$Accu_y$	$Prec_n$	$Reca_l$	F_{score}
BESO-HDLBD	99.27	98.28	99.27	98.77
BDC-RSODL	99.12	96.91	99.18	98.00
P2P-BDS Model	94.50	95.61	96.67	94.66
MTC-CNN Model	95.00	95.87	97.77	96.16
DT	97.90	94.94	95.95	95.65
Host-based	92.90	95.34	96.84	96.59
FL-ANN Model	98.94	96.29	97.87	97.08

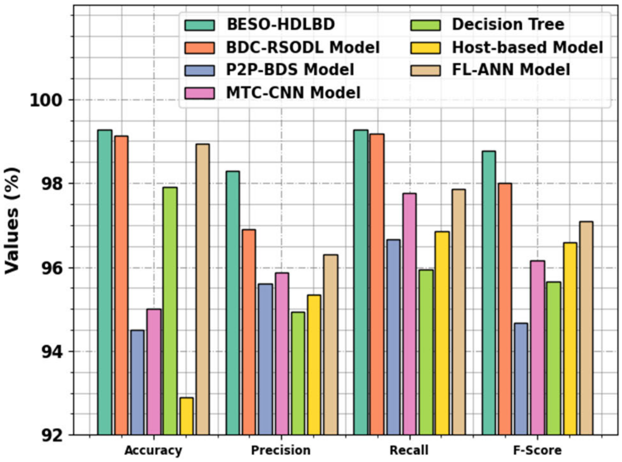

FIGURE 10. Comparison analysis of the BESO-HDLBD model with other systems.

In Table 4 and Fig. 10, a comparison analysis of the BESO-HDLBD algorithm with recent systems can be provided [14], [28]. The experimental values stated that the host-based approach accomplishes worse outcomes. Besides, the P2P-BDS and MTC-CNN approaches are stated to somewhat increase performances. Meanwhile, the DT and FL-ANN models accomplish reasonable performance. Although the BDC-RSODL model reaches considerable performance, the BESO-HDLBD technique exhibits supremacy over other methods with a maximum $accu_y$ of 99.27%, $prec_n$ of 98.28%, $reca_l$ of 99.27%, and F_{score} of 98.77%. Thus, the BESO-HDLBD technique can be employed for automated botnet detection.

V. CONCLUSION

For accomplishing security in the IoT platform, this article presented an innovative BESO-HDLBD system for automated botnet detection. The BESO-HDLBD method aims to resolve the security issue by identifying the botnets in the IoT environment. It encompasses 3 main functions such as BESO-based FS subset, HDL-based classification, and DFA-based hyperparameter tuning. To reduce the high dimensionality problem, the BESO-HDLBD technique uses the BESO system for the FS. For botnet detection purposes, the BESO-HDLBD model uses HDL which is a BiLSTM, CNN, and attention concept. Finally, the parameter selection of the HDL model is performed by the design of the DFA. The experimental analysis of the BESO-HDLBD method could be determined under a benchmark botnet database. The obtained findings infer a better solution of the BESO-HDLBD technique compared to recent detection approaches in terms of different evaluation measures.

ACKNOWLEDGMENT

The authors gratefully acknowledge technical and financial support provided by the Ministry of Education and Deanship of Scientific Research (DSR), King Abdulaziz University (KAU), Jeddah, Saudi Arabia.

REFERENCES

[1] C. Joshi, R. K. Ranjan, and V. Bharti, "ACNN-BOT: An ant colony inspired feature selection approach for ANN based botnet detection," *Wireless Pers. Commun.*, vol. 132, no. 3, pp. 1999–2021, Oct. 2023.

[2] C. Li, Y. Zhang, W. Wang, Z. Liao, and F. Feng, "Botnet detection with deep neural networks using feature fusion," in *Proc. Int. Seminar Comput. Sci. Eng. Technol. (SCSET)*, Jan. 2022, pp. 255–258.

[3] R. K. V. Penmatsa, S. K. R. Mallidi, and R. R. Muni, "A wrapper based feature selection using grey wolf optimization for botnet attack detection," *Int. J. Sensors, Wireless Commun. Control*, vol. 11, no. 9, pp. 951–956, Nov. 2021.

[4] S. D. A. Rihan, M. Anbar, and B. A. Alabsi, "Approach for detecting attacks on IoT networks based on ensemble feature selection and deep learning models," *Sensors*, vol. 23, no. 17, p. 7342, Aug. 2023.

[5] K. Saurabh, A. Singh, U. Singh, O. P. Vyas, and R. Khondoker, "GANIBOT: A network flow based semi supervised generative adversarial networks model for IoT botnets detection," in *Proc. IEEE Int. Conf. Omni-Layer Intell. Syst. (COINS)*, Aug. 2022, pp. 1–5.

[6] H. Alkahtani and T. H. H. Aldhyani, "Botnet attack detection by using CNN-LSTM model for Internet of Things applications," *Secur. Commun. Netw.*, vol. 2021, pp. 1–23, Sep. 2021.

[7] M. A. Haq, "DBoTPM: A deep neural network-based botnet prediction model," *Electronics*, vol. 12, no. 5, p. 1159, Feb. 2023.

[8] H. Wasswa, T. Lynar, and H. Abbass, "Enhancing IoT-botnet detection using variational auto-encoder and cost-sensitive learning: A deep learning approach for imbalanced datasets," in *Proc. IEEE Region Symp. (TENSYMP)*, Sep. 2023, pp. 1–6.

[9] S. I. Popoola, B. Adebisi, R. Ande, M. Hammoudeh, and A. A. Atayero, "Memory-efficient deep learning for botnet attack detection in IoT networks," *Electronics*, vol. 10, no. 9, p. 1104, May 2021.

[10] M. W. Nadeem, H. G. Goh, Y. Aun, and V. Ponnusamy, "Detecting and mitigating botnet attacks in software-defined networks using deep learning techniques," *IEEE Access*, vol. 11, pp. 49153–49171, 2023.

[11] M. Catillo, A. Pecchia, and U. Villano, "A deep learning method for lightweight and cross-device IoT botnet detection," *Appl. Sci.*, vol. 13, no. 2, p. 837, Jan. 2023.

[12] S. I. Popoola, B. Adebisi, R. Ande, M. Hammoudeh, K. Anoh, and A. A. Atayero, "SMOTE-DRNN: A deep learning algorithm for botnet detection in the Internet-of-Things networks," *Sensors*, vol. 21, no. 9, p. 2985, Apr. 2021.

[13] K. Malik, F. Rehman, T. Maqsood, S. Mustafa, O. Khalid, and A. Akhunzada, "Lightweight Internet of Things botnet detection using one-class classification," *Sensors*, vol. 22, no. 10, p. 3646, May 2022, doi: 10.3390/s22103646.

[14] S. M. Alshahrani, F. S. Alrayes, H. Alqahtani, J. S. Alzahrani, M. Maray, S. Alazwari, M. A. Shamseldin, and M. Al Duhayyim, "IoT-cloud assisted botnet detection using rat swarm optimizer with deep learning," *Comput., Mater. Continua*, vol. 74, no. 2, pp. 3085–3100, 2023.

[15] P. L. S. Jayalaxmi, G. Kumar, R. Saha, M. Conti, T.-H. Kim, and R. Thomas, "DeBot: A deep learning-based model for bot detection in industrial Internet-of-Things," *Comput. Electr. Eng.*, vol. 102, Sep. 2022, Art. no. 108214.

[16] A. A. Hezam, S. A. Mostafa, Z. Baharum, A. Alanda, and M. Z. Salikon, "Combining deep learning models for enhancing the detection of botnet attacks in multiple sensors Internet of Things networks," *JOIV : Int. J. Informat. Visualizat.*, vol. 5, no. 4, pp. 380–387, Dec. 2021.

[17] G. Kirubavathi and U. K. Sridevi, "Detection of IoT botnet using machine learning and deep learning techniques," Tech. Rep., 2023, doi: 10.21203/rs.3.rs-2630988/v1.

[18] M. Y. Alzahrani and A. M. Bamhdi, "Hybrid deep-learning model to detect botnet attacks over Internet of Things environments," *Soft Comput.*, vol. 26, no. 16, pp. 7721–7735, Aug. 2022.

[19] K. Dakic, B. Al Homssi, M. Lech, and A. Al-Hourani, "HybNet: A hybrid deep learning-matched filter approach for IoT signal detection," *IEEE Trans. Mach. Learn. Commun. Netw.*, vol. 1, pp. 18–30, 2023.

[20] A. Presekal, A. Stefanov, V. S. Rajkumar, and P. Palensky, "Attack graph model for cyber-physical power systems using hybrid deep learning," *IEEE Trans. Smart Grid*, vol. 14, no. 5, pp. 4007–4020, Jan. 2023.

[21] V. Hnamte and J. Hussain, "DCNNBiLSTM: An efficient hybrid deep learning-based intrusion detection system," *Telematics Informat. Rep.*, vol. 10, Jun. 2023, Art. no. 100053.

[22] Y. Al Sawafi, A. Touzene, and R. Hedjam, "Hybrid deep learning-based intrusion detection system for RPL IoT networks," *J. Sensor Actuator Netw.*, vol. 12, no. 2, p. 21, Mar. 2023.

[23] S. Kankılıç and E. Karpat, "Optimization of multilayer absorbers using the bald eagle optimization algorithm," *Appl. Sci.*, vol. 13, no. 18, p. 10301, Sep. 2023.

[24] M. Mafarja, T. Thaher, M. A. Al-Betar, J. Too, M. A. Awadallah, I. A. Doush, and H. Turabieh, "Classification framework for faulty-software using enhanced exploratory whale optimizer-based feature selection scheme and random forest ensemble learning," *Int. J. Speech Technol.*, vol. 53, no. 15, pp. 18715–18757, Aug. 2023.

[25] L. Shan, Y. Liu, M. Tang, M. Yang, and X. Bai, "CNN-BiLSTM hybrid neural networks with attention mechanism for well log prediction," *J. Petroleum Sci. Eng.*, vol. 205, Oct. 2021, Art. no. 108838.

[26] E. Kaya, C. B. Kaya, E. Bendeş, S. Atasever, B. Öztürk, and B. Yazlık, "Training of feed-forward neural networks by using optimization algorithms based on swarm-intelligent for maximum power point tracking," *Biomimetics*, vol. 8, no. 5, p. 402, Sep. 2023.

[27] S. García, M. Grill, J. Stiborek, and A. Zunino, "An empirical comparison of botnet detection methods," *Comput. Secur.*, vol. 45, pp. 100–123, Sep. 2014.

[28] C. Joshi, R. K. Ranjan, and V. Bharti, "A fuzzy logic based feature engineering approach for botnet detection using ANN," *J. King Saud Univ. Comput. Inf. Sci.*, vol. 34, no. 9, pp. 6872–6882, Oct. 2022.

LOUAI A. MAGHRABI (Member, IEEE) received the B.Sc. degree in computer science from Lebanese American University, Beirut, Lebanon, the M.Sc. degree in information technology from the University of West of England, Bristol, U.K., and the Ph.D. degree in cybersecurity from Kingston University, London, U.K. He is currently an Assistant Professor with the Department of Software Engineering, College of Engineering, University of Business and Technology, Jeddah, Saudi Arabia. His research interests include cybersecurity, risk assessment, cryptography, artificial intelligence, machine learning, IoT, blockchain, drones, metaverse, quantum computing, and game theory. He received the best research paper award in 2021.

SAHAR SHABANAH is currently an Assistant Professor in computer science with King Abdulaziz University. Her research interests include computer graphics topics, including modeling, simulation and animation, data mining techniques, such as classification of multi labels data streams, the computer visualization of algorithms and medical and scientific data, computer games design of all types, such as educational, serious, training and simulations, multimedia and user interface design, special needs applications, image processing and objects detection, algorithms and data structures visualization, virtual reality, web and mobile applications development, and computer science education.

TURKI ALTHAQAFI received the double master's degree majoring in information technology and business information systems from Monash University, and the Ph.D. degree from the School of Information Technology, Monash University, specialized in information systems. He is currently pursuing the bachelor's degree in computer science with Umm Al-Qura University. He has recently joined Dar Al-Hekmah University as an Assistant Professor with the School of Engineering, Computer Science and Informatics. His research interest includes the area of information systems ranging from theory to design. His experience varies from academia and industry as he was working in the banking industry in the field of business continuity.

DHEYAALDIN ALSALMAN received the Bachelor of Arts degree majoring in information systems, human resources management, and management and leadership from Portland State University, Portland, OR, USA, the Master of Science degree in information systems with a concentration in enterprise security management from Lawrence Technological University, Southfield, MI, USA, and the Ph.D. degree in information systems with a specialization in information assurance and computer security from Dakota State University, Madison, SD, USA. He is currently an Assistant Professor in cybersecurity with Dar Al-Hekma University, Jeddah, Saudi Arabia. His research interests include phishing attacks and cybersecurity.

SULTAN ALGARNI received the bachelor's degree (Hons.) in computer science from King Abdulaziz University (KAU), Saudi Arabia, in 2008, the master's degree in information technology from the University of New South Wales (UNSW), Australia, in 2014, and the Ph.D. degree in computer science from KAU, in 2022. He is currently an Assistant Professor with the Faculty of Computing and Information Technology, KAU. His research interests include information security, networking, the IoT, SDN, and artificial intelligence.

ABDULLAH AL-MALAISE AL-GHAMDI received the Ph.D. degree in computer science from George Washington University, USA, in 2003. He is currently a Professor in software and systems engineering and AI, and associated with the Faculty of Computing and Information Technology (FCIT), King Abdulaziz University (KAU), and School of Engineering, Computing and Design, Dar Al-Hekma University, Jeddah, Saudi Arabia. He is a member of the Scientific Council and the Secretary General of Scientific Council, KAU. In addition, he is the Head of Consultant's Unit, the Vice-President for Development Office, and a Consultant to the Vice-President for Graduate Studies and Scientific Research, KAU. Previously, he was the Head of the IS Department, the Vice Dean for Graduate Studies and Scientific Research, and the Head of the Computer Skills Department, FCIT. His main research interests include software engineering and systems, artificial intelligence, data analytics, business intelligence, and decision support systems.

MAHMOUD RAGAB received the Ph.D. degree from the Faculty of Mathematics and Natural Sciences, Christian-Albrechts-University (CAU), Kiel, Schleswig-Holstein, Germany. He is currently a Professor in data science with the Department of Information Technology, Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah, Saudi Arabia, and Mathematics Department, Faculty of Science, Al Azhar University, Cairo, Egypt. He worked in different research groups at many universities, such as the Combinatorial Optimization and Graph Algorithms Group (COGA), Faculty II Mathematics and Natural Sciences, Berlin University of Technology, Berlin, Germany, The British University in Egypt (BUE), and Automation, Integrated Communication Systems Group, Ilmenau University of Technology (TU Ilmenau), Thuringia, Germany. His research interests include AI algorithms, deep learning, sorting, optimization, mathematical modeling, data science, neural networks, time series analysis, and decision support systems.