Journal
IJCSM

Iraqi Journal for Computer Science and Mathematics

Journal Homepage: http://journal.esj.edu.iq/index.php/IJCM
e-ISSN: 2788-7421 p-ISSN: 2958-0544

Hybrid Honey Badger Algorithm with Artificial Neural Network (HBA-ANN) for Website Phishing Detection

Muhammad Arif Mohamad[1]*, Muhammad Aliif Ahmad[2], Zuriani Mustaffa[1]

[1]Faculty of Computing, Universiti Malaysia Pahang Al Sultan Abdullah,
[2]Faculty of Computing, Universiti Teknologi Malaysia

*Corresponding Author: Muhammad Arif Mohamad

DOI: https://doi.org/10.52866/ijcsm.2024.05.03.041
Received April 2024; Accepted June 2024; Available online August 2024

ABSTRACT: Phishing is a sort of cyberattack that refers to the practice of fabricating fake websites that imitate authentic websites in order to trick users into disclosing private information. Identifying these fake sites is challenging due to their deceptive nature as they often mimic legitimate websites, making it difficult for users to distinguish between the real and fake ones. Artificial Neural Network (ANN) is one popular method for website phishing detection. ANN is capable of detecting phishing websites by identifying patterns and characteristics connected to phishing websites through a network training phase. Technically, in the network training phase of ANN, neurons on the network must be passed over. There are multiple techniques in training the network, one of which is training with metaheuristic algorithms. Metaheuristic algorithms that aim to develop more effective hybrid algorithms by combining the good and successful aspects of more than one algorithm are algorithms inspired by nature. Therefore, this study proposed a hybrid Honey Badger Algorithm with Artificial Neural Network (HBA-ANN) classification model. HBA as metahueristic algorithm is used to optimize the network training process of ANN to improve their performances. Three main steps made up the proposed HBA-ANN classification model: setting up the experiment, optimizing HBA for network training, and network testing. Lastly, the performance of the proposed HBA-ANN classification model is assessed in terms of recall, precision, F1-score, accuracy and error rate using the confusion matrix that was generated for analysis. The proposed hybrid HBA-ANN was found to be effective in identifying the phishing website after conducting an experimental and statistical analysis.

Keywords: Cybersecurity, Website Phishing Detection, Metaheuristic Optimization, Honey Badger Algorithm, Artificial Neural Network

1. INTRODUCTION

The internet serves as a platform that connects and exchanges data amongst large-scale networks, which include public, corporate, and academic organizations. The most common usage areas of the Internet are search, news, social networking, gaming, e-commerce, education, file and data transfer, communication, online services and remote work. Despite its benefits like accessibility and convenience, there are drawbacks as well. Some of these include cyberbullying, physical and mental health problems, inappropriate content, wasted time and internet fraud [1-2].

Internet fraud, which is growing day by day and causing economic damage, is a cybercrime that is carried out by using tools such as the internet, e-mail, SMS and malware etc. to seize and defraud people's information [3,4]. Trojans, identity theft, data breach, ransomware, denial of service, scareware, malware and phishing are some techniques used in internet fraud [5].

Phishing is one of internet fraud method, representing a form of social engineering attack through which malicious individuals, often cybercriminals, aim to deceive target users into divulging their private data, comprising credit card details, debit card information, social media accounts, and more [6]. Various phishing techniques are employed to trick people, such as imitation of an e-mail sent by a corporate firm, generating fake emails that appear to originate from social media platforms, and creating fake banking sites designed to mimic authentic ones [7].

In this study, an investigation on the websites phishing detection was conducted. In the website phishing technique, the victim is directed to the fake of the corporate site in various ways to obtain their information by malicious users [7]. The victim, who does not know about website phishing, very quickly believes the fake website and can transfer their information to cybercriminals. [8]. Furthermore, the advanced technologies employed in today's web development make it difficult for users to discern the authenticity of a website, contributing to the success of phishing attempts.

One of the approaches employed for websites phishing detection is blacklist method [8, 9]. This method relies on a list of websites known to pose phishing threats [10]. Cybercriminals often attempt to make URLs resemble legitimate sites to deceive victims effectively. By visually replicating the real webpage and associating it with a legitimate-looking

*Corresponding author: arifmohamad@umpsa.edu.my

URL, perpetrators increase the likelihood of victims trusting the fake site [10]. Another approach in websites phishing detection involves the use of Artificial Neural Networks (ANN). ANN one of machine learning used to make sense or detect trends from data that is too complex or imprecise to be noticed by humans or other computer techniques [11]. ANN can obtain a set of weights that reduces the classification error in order to obtain good performance in term of accuracy [12-16]. This illustrates the role of advanced machine learning techniques in bolstering the capabilities of phishing detection methods.

Various algorithms serve as learning techniques in the training of neural networks, with deterministic algorithms being as alternative approach. Deterministic algorithm represents an optimization approach applied in enhancing the performances of Artificial Neural Networks (ANN), providing results without uncertainty [17]. However, a drawback of deterministic approaches lies in their potential to slow down network training when additional hidden layers are introduced, and the risk of getting stuck in a local optimum based on the initial solution [18-20]. On the other hand, stochastic algorithms are employed as another technique in network training [21]. These algorithms introduce randomness, diminishing the likelihood of being trapped in a local minimum and reducing dependence on the initial solution [22]. Among stochastic algorithms, metaheuristic algorithms inspired by nature are notable. Metaheuristic algorithms offer advantages such as easy design, efficient resolution of real problems and functions, hybridization with multiple algorithms, and avoidance of being confined to local optimal values [23-25]. These characteristics make metaheuristic algorithms a versatile and effective choice in the training of neural networks. Indeed, the Butterfly Optimization Algorithm [26], Harris-hawk Optimization [27], Barnacle Mating Optimizer[28], Grasshopper Optimization Algorithm [29], Flower Pollination Algorithm [30], Honey Badger Algorithm [31] are among the popular and commonly used metaheuristic algorithm due too successfully applied in solving optimization problem across different domains.

2. LITERITURE REVIEW

In literature, various research has explored the application of metaheuristic algorithm for website phishing detection. Alshahrani et al. [32] proposed a metaheuristic approach in their research of website phishing detection which is Particle Swarm Optimization (PSO) was employed for optimizing the weighting of distinct website features, leading to improved accuracy in identifying phishing websites. According to this method, PSO is used to better weight different website features in order to achieve higher accuracy values when finding phishing websites. This intelligent method, which was developed according to the results obtained, achieved better results in detecting phishing compared to other machine learning techniques.

Ali et al. [33] stated that they used machine learning techniques for phishing detection. Researchers using URL-based phishing detection in their studies have tried to detect fake or legal websites with machine learning techniques. Researchers using GA for feature selection in machine learning found that the accuracy increased compared to the results without GA.

In this study, ANN training approach based on metaheuristic algorithm has been proposed for the website phishing detection. The training part was executed utilizing Honey Badger Algorithm (HBA), leading to the development of a hybrid HBA-ANN algorithm, designed for website phishing detection. Selection of HBA for ANN network training is attributed to its status as a cutting-edge metaheuristic algorithm, recognized for its success in addressing benchmark problems [34]. Notably, HBA offers a balanced exploration and exploitation approach throughout the search process, resulting in higher convergences rate compared to another metaheuristic algorithm. The distinctive feature of HBA lies in its ability to effectively handle challenging optimization problems with multiple local solutions [35]. Given HBA's numerous advantages over another methods, it emerges as a preferred solution for various optimization scenarios. Additionally, HBA's simplicity in implementation and minimal susceptibility to overfitting are noteworthy due to the minimal parameter setup required during initialization [36]. Moreover, HBA is recognized for its versatility and expandability, allowing for easy adaptation to diverse optimization challenges.

2.1 Overview of HBA

Proposed by Hassim et al. [31], HBA was inspired by honey badger foraging behavior. HBA employs two main strategies to locate food: relying on their own sense of smell and following honeyguide birds, known for their proficiency in finding honey. Like honey badger's hunting approach, the algorithm involves a gradual and consistent movement while utilizing its sensing capabilities to locate the target. By engaging in digging activities, the algorithm simulates the process of identifying the target's location before making a capture. Interestingly, honey badgers encounter difficulties in finding beehives, despite their affinity for honey. To overcome this challenge, they form a symbiotic relationship with honeyguide birds, by leading the honey badger to beehives. Benefiting both parties as they share and enjoy the honey. This collaborative behavior serves as a model for the HBA in optimizing search processes.

$$x_i = lb_i + r_1 \times (ub_i - lb_i) \tag{1}$$

Here, r_1 as random value which is ranged from 0 to1, and ub_i and lb_i are the upper and lower bounds. Equation (1) is used to calculate the location of the honey badger x_i.

$$I_i = r_2 \times \frac{S}{4\pi d_i^2} \tag{2}$$

$$S = (x_i - x_{i+1})^2 \tag{3}$$

$$d_i = x_{prey} - x_i \tag{4}$$

Equations (3) and (4) are used to calculate S and d_i, which stand for the intensity of scent source and distances of honey badgers and its victim respectively. r_2 as random value which is ranged from 0 to 1. Intensity I_i is correlated with the victim's concentration strength and the distance. Inversely, if the scent is strong, the honey badger will move quickly in that direction toward its objective. The Equation (2) is used to determine smell intensity.

$$\alpha = C + exp\left(\frac{-t}{t_{max}}\right) \tag{5}$$

Equation (5), where n is the maximum numbers of iteration while C is constants, computes a density factors (α), which control time-varying arbitrariness in ensuring the smooth transitions of explorations to exploitations.

2.1.1 Digging Phase of HBA

When in digging mode, the badgers use their senses of smell to locate the victim and approach it. It starts digging to capture the victim.

$$x_{new} = x_{prey} + F * \beta * I * x_{prey} + F * r_3 * \alpha * d_i * |\cos(2\pi r_4) * (1 - \cos(2\pi r_5))| \tag{6}$$

where the target's location is represented by x_{prey}, its capacity to find food is represented by β, the distances between honey badgers and its victim represented by d_i, random number between 0 to 1, while F served as the flag in changing the search directions. Equation (6) illustrates the digging mode.

2.1.2 Honey Phase of HBA

The badger utilizes honeyguide birds to locate the honey beehive during the honey mode phase.

$$x_{new} = x_{prey} + F * r_7 * \alpha * d_i \tag{7}$$

where x_{prey} represents the target's location and x_{new} represents the honey badger's new position. Equation (7) is used by the honey badger to determine its new location. Given that it encompasses both the discovery and the utilization stages, it conducts a worldwide search. The HBA algorithm's operation is thoroughly illustrated in Figure 1.

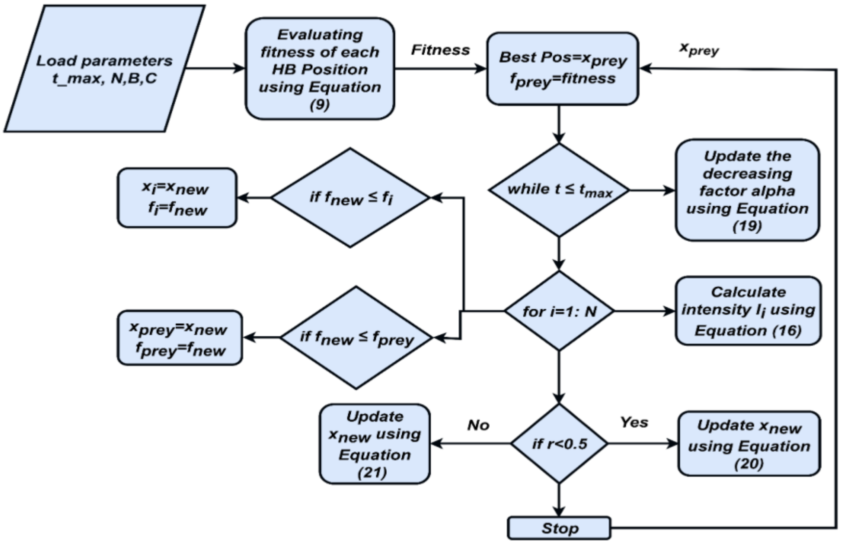

Load parameters t_max, N,B,C
Evaluating fitness of each HB Position using Equation (9)
Fitness
Best Pos=x_{prey} f_{prey}=fitness
x_{prey}
while $t \le t_{max}$
Update the decreasing factor alpha using Equation (19)
$x_i=x_{new}$ $f_i=f_{new}$
if $f_{new} \le f_i$
for i=1: N
Calculate intensity I_i using Equation (16)
$x_{prey}=x_{new}$ $f_{prey}=f_{new}$
if $f_{new} \le f_{prey}$
Update x_{new} using Equation (21)
No
if r<0.5
Yes
Update x_{new} using Equation (20)
Stop

FIGURE 1. Flowchart of HBA

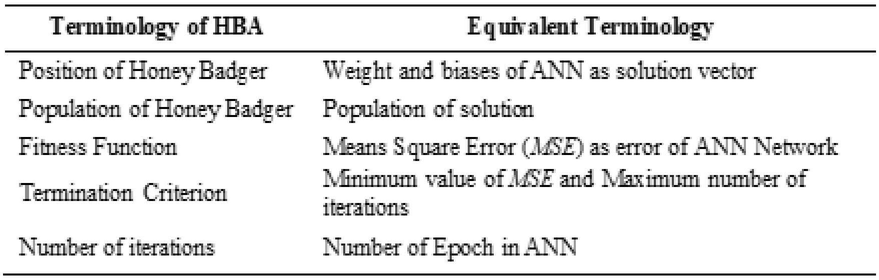
3. METHODOLOGY

This section focuses on the methodology which has been utilized in this study in order to develop and enhance ANN model of website phishing detection by optimizing with HBA. The HBA-ANN classification model consisted of three major processes namely experimental setup, HBA optimization in network training, and network testing. Figure 2 illustrates the procedures involved in developing the proposed HBA-ANN classification model for phishing website detection.

Prior to commencing the experiment, we conducted the experimental setup as the first process of the HBA-ANN development procedure. There are three steps in the experimental setup, firstly with the step of declared the dataset and input/output, secondly with the step of declared ANN parameter, and lastly with the step of declared HBA parameter. Details of experimental setup are discussed in the next subsection 3.1.

Secondly is HBA optimization in network training process. In the process of network training, the HBA has been hybridized with ANN model specifically during the ANN network is being trained. The following subsection 3.2 provides a brief discussion of the specifics of HBA optimization in the network training process. Prior to that, Table 1 lists the terms that are equivalent between HBA and ANN based on this study, helping to clarify the basic processes and terminologies of both.

Table 1. Basic process and terminologies HBA-ANN



Terminology of HBA	Equivalent Terminology
Position of Honey Badger	Weight and biases of ANN as solution vector
Population of Honey Badger	Population of solution
Fitness Function	Means Square Error (*MSE*) as error of ANN Network
Termination Criterion	Minimum value of *MSE* and Maximum number of iterations
Number of iterations	Number of Epoch in ANN

Thirdly, the process of network testing conducted where the trained network by HBA is used against the testing dataset as testing procedure to test the network. At the end of this development procedure of proposed HBA-ANN classification model, validation of the network is conducted to validate the network of HBA-ANN classification model, in term of error convergence, convergence time and learning iteration. Details of the training and validation process are present in the next subsection 3.3 and 3.4 respectively.

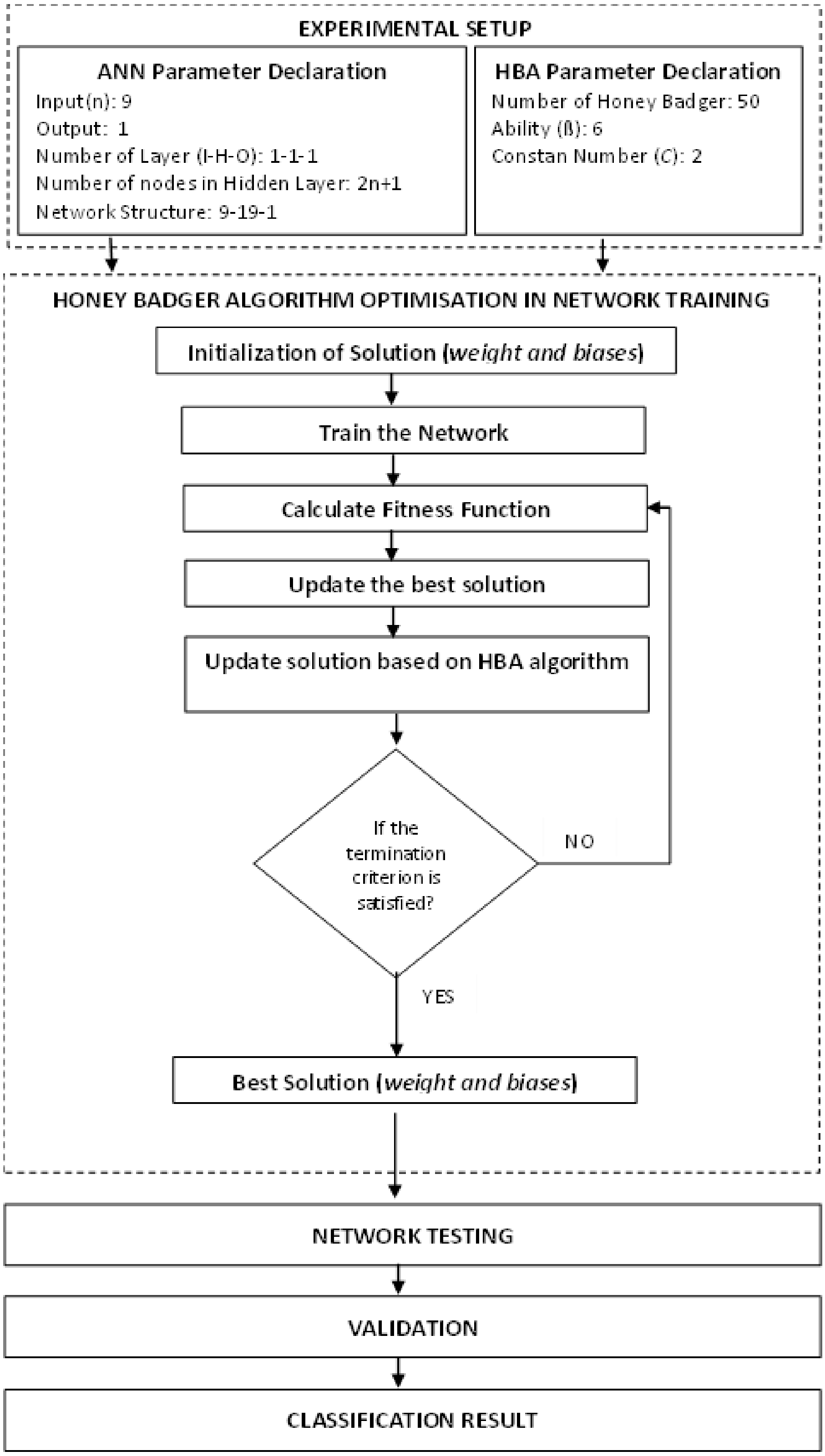
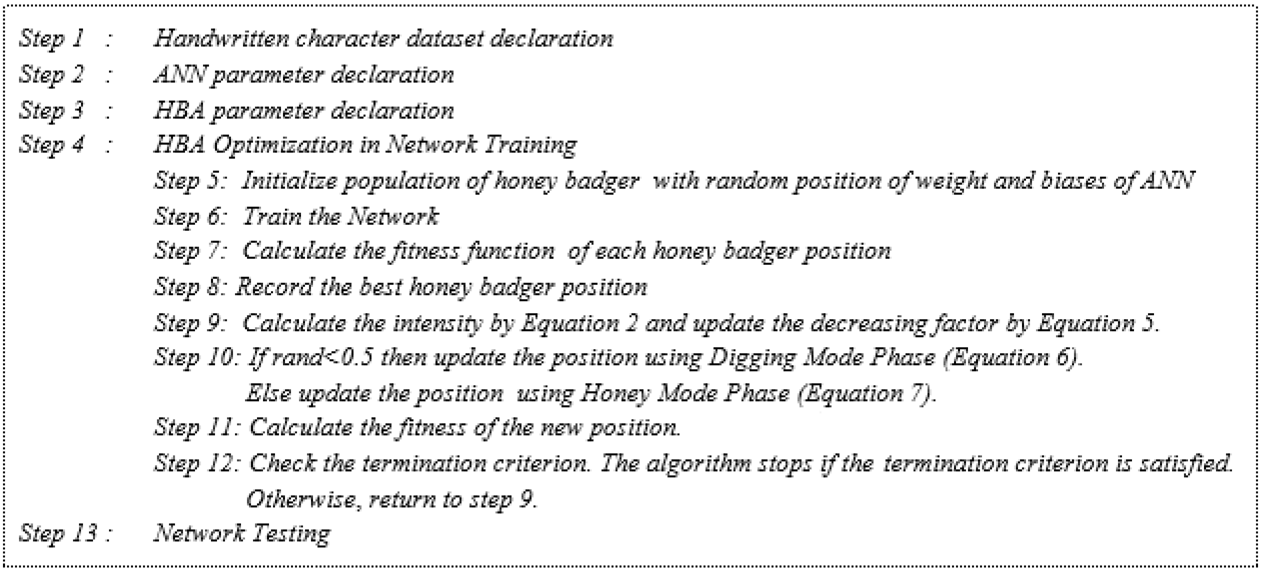

EXPERIMENTAL SETUP
ANN Parameter Declaration
Input(n): 9
Output: 1
Number of Layer (I-H-O): 1-1-1
Number of nodes in Hidden Layer: 2n+1
Network Structure: 9-19-1
HBA Parameter Declaration
Number of Honey Badger: 50
Ability (ß): 6
Constan Number (C): 2
HONEY BADGER ALGORITHM OPTIMISATION IN NETWORK TRAINING
Initialization of Solution (weight and biases)
Train the Network
Calculate Fitness Function
Update the best solution
Update solution based on HBA algorithm
If the termination criterion is satisfied?
NO
YES
Best Solution (weight and biases)
NETWORK TESTING
VALIDATION
CLASSIFICATION RESULT

FIGURE 2. Procedure of Development Hybrid HBA-ANN Classification model for Website Phishing Detection

Based on Figure 2, an algorithm for proposed hybrid HBA-ANN classification for website phishing detection is implemented as shown in Figure 3. There are thirteen steps in the algorithm namely the declaration of dataset, declaration of ANN parameter, declaration of parameter HBA, HBA optimization in network training, Initialize population of honey badger with random position of weight and biases of ANN, train network, calculation the fitness function, Record the best solution, Calculate the intensity by Equation 2 and update the decreasing factor by Equation 5, update the position using digging mode phase as Equation 6 or honey mode phase as Equation 7, calculation of fitness function for new position, check the termination criterion and network testing. Details of the process in each step are discussed in the next subsection.



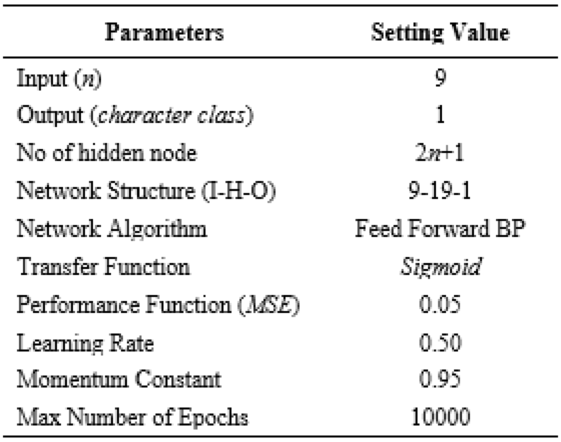
```
Step 1  :   Handwritten character dataset declaration
Step 2  :   ANN parameter declaration
Step 3  :   HBA parameter declaration
Step 4  :   HBA Optimization in Network Training
            Step 5:  Initialize population of honey badger  with random position of weight and biases of ANN
            Step 6:  Train the Network
            Step 7:  Calculate the fitness function  of each honey badger position
            Step 8: Record the best honey badger position
            Step 9:  Calculate the intensity by Equation 2 and update the decreasing factor by Equation 5.
            Step 10: If rand<0.5 then update the position using Digging Mode Phase (Equation 6).
                     Else update the position  using Honey Mode Phase (Equation 7).
            Step 11: Calculate the fitness of the new position.
            Step 12: Check the termination criterion. The algorithm stops if the  termination criterion is satisfied.
                     Otherwise, return to step 9.
Step 13 :   Network Testing
```

FIGURE 3. The algorithm of proposed hybrid HBA-ANN classification model for website phishing detection

3.1 EXPERIMENTAL SETUP

This subsection presents the experimental setup process of the proposed HBA-ANN. This process consists of declaration of dataset, ANN parameter and FA parameter which cover Step 1 until Step 3. The HBA-ANN is performed by using the dataset collected by UCI machine learning repository [37]. Subsequently, the declaration of ANN parameter values was conducted in term of declaration of input and output, determination of network layers, determination number of nodes, network construction, and network parameter initialization in term of network algorithm, network transfer function, momentum constant, learning rate, number of epoch and performance function. There are no training function and learning function declaration for this study because of the network training process is performed by HBA. Table 2 shows the details of ANN parameters declaration for this study. The initialization of the ANN parameters is based on guidelines given by [38].

Table 2. ANN parameter setting



Parameters	Setting Value
Input (*n*)	9
Output (*character class*)	1
No of hidden node	2*n*+1
Network Structure (I-H-O)	9-19-1
Network Algorithm	Feed Forward BP
Transfer Function	*Sigmoid*
Performance Function (*MSE*)	0.05
Learning Rate	0.50
Momentum Constant	0.95
Max Number of Epochs	10000

Third, the proposed algorithm's third step, the declaration of the HBA parameter. The number of honey badgers, their capacity to obtain food (*ß*), and their constant number (*C*) are the three parameters that are stated. Based on the recommended values by [36], the HBA parameter values are declared. Table 3 shows the HBA parameters declaration for this study.

Table 3. HBA parameter setting

Parameters	Setting Value
Number of Honey Badger	50
Ability of honey badger to get food, ß	6
Constant Number, C	2

3.2 TRAINING PROCEDURE

Network training is the fourth stage of the HBA-ANN algorithm, which uses HBA as an optimization approach and supervised training as a network training strategy. Each layer contains the input, hidden, and output layer. Each node in a layer that is connected to every other layer node is assigned a specific weight. The output of weight and desired weight were compared after the network processes the input. Once errors have spread throughout the system, the weights that govern the network are adjusted. The final network representation includes the optimized neuron and the weights vector that go with them is the output of the training.

Then, using the HBA optimization technique, these weight vectors are optimized. Up until the minimal error is reached, this process is repeated repeatedly. A minimum error of 0.05 or the completion of 10,000 iterations, or the Means sq\. Error (MSE) reaching that threshold, serve as the training's stopping criteria. To learn more about the network's behavior, the best error convergence rate is calculated throughout each iteration until the optimal solution is reached. The next subsection goes into detail about the network training and optimization process.

3.2.1 HBA OPTIMIZATION IN NETWORK TRAINING

The process of utilizing HBA to optimize the ANN network is depicted in Figure 4. As it relates to Steps 5 through 12 of the HBA-ANN algorithm, the figure depicts the process of optimizing the network of network training. Highlighting certain terms is necessary when designing the HBA to train the network:-

(a) Position of honey badger in population was represented the network's weights and biases

(b) As a fitness function, the network's minimum error of MSE is employed.

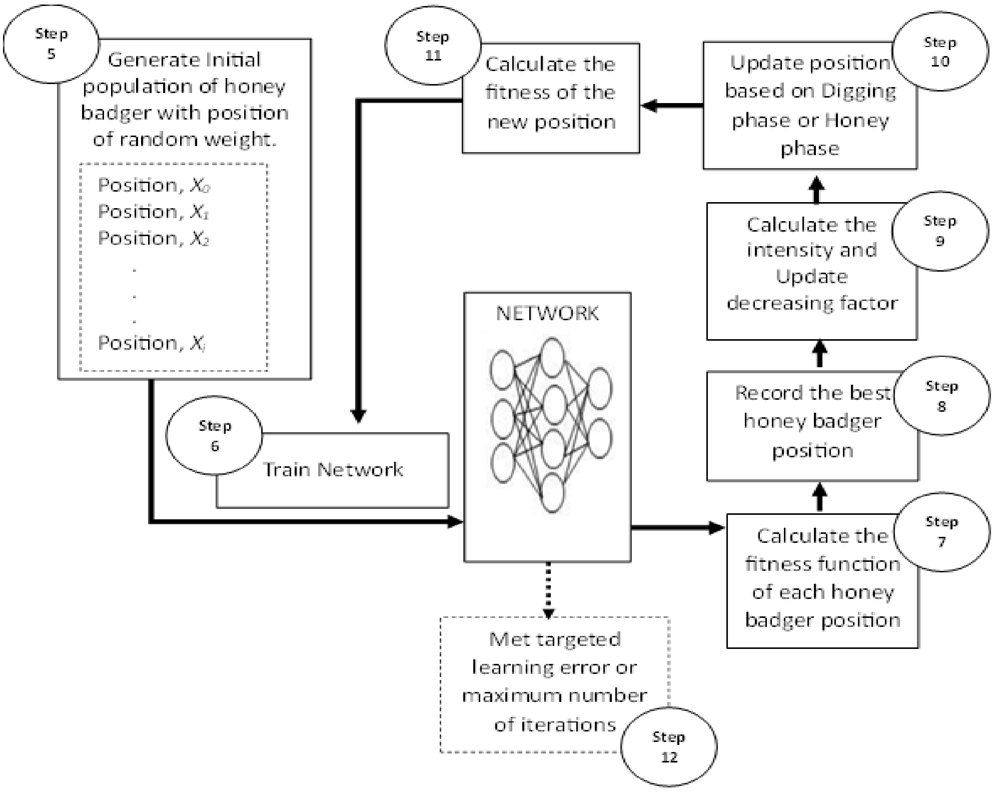

Step 5
Generate Initial population of honey badger with position of random weight.
Position, X_0
Position, X_1
Position, X_2
.
.
.
Position, X_i
Step 6
Train Network
NETWORK
Step 11
Calculate the fitness of the new position
Step 10
Update position based on Digging phase or Honey phase
Step 9
Calculate the intensity and Update decreasing factor
Step 8
Record the best honey badger position
Step 7
Calculate the fitness function of each honey badger position
Met targeted learning error or maximum number of iterations
Step 12

FIGURE 4. Illustration of Honey Badger Algorithm Optimization in Network Training

So, the optimization network training starts with generation of initial population of fireflies as Step 5 of the HBA-ANN algorithm. The population with a random set of weight and bias based on the population of honey badger position. Therefore, for this study, each position, X_i is characterized with a vector including two elements of weight, w_i and bias, b_i as follows.

$$X_i = [w_i, b_i] \tag{8}$$

Then the network of ANN is ready to be trained as Step 6 of HBA-ANN algorithm. The network is trained with the initial weight generated in the population. Given inputs ***x*** and current weights, the network computes an output ***O(x)***. It is necessary to finish this process in order for the intended output ***O*** to yield the same outcomes as the observed output ***y***. Once the network successfully trained, then the fitness function is calculated as Step 6 of the algorithm. In this study, MSE is utilized as the fitness function as shown in Equation 9.

$$E = \frac{1}{2}\sum_{l=1}^{L}\sum_{h=1}^{H}(o_{lh} - y_{lh})^2 \tag{9}$$

where,

L	input-output pair
H	output node

An error function as Equation 3.2 is applied in finding margin errors between the targeted output ***O*** and observed output *y*. So, the optimized weight means by obtained the minimum error. Therefore, a fitness function for HBA can be defined as minimum error of the network. So, the next step, record the best honey badger position according to fitness function as Step 8 of the algorithm. At this point, the best honey badger position means the position that could reach lower value of MSE of the network.

Consequently, Step 9 calculates the intensity and updates decreasing factor based on Equation 2 and Equation 5. Then, the next step is updating the position of honey badger based on digging mode phase or honey mode phase. Then, Step 11 calculates the new position of honey badger that has smaller MSE values for the new position. Lastly, check the termination criterion as Step 12 of the algorithm. The termination criterion must be met for the algorithm to terminate either target learning error (MSE) less than 0.05 or maximum number of iterations 10000. Otherwise, return to step 9.

3.3 TESTING PROCEDURE

Since the network is trained completely with the HBA optimization, the trained network is used against the testing dataset as a testing procedure to test the network as the last step of the proposed hybrid HBA-ANN algorithm. To examine the network's behavior, the percentage of correct results is then calculated by comparing the results that the network produced to the expected outcome. Additional analysis will be conducted using the simulation results obtained from the experiment.

4. EXPERIMENTAL RESULT AND ANALYSIS

4.1 VALIDATION

This section discussed the result of the network training validation in terms of error convergence, convergence time and learning iteration. This experiment had two criterions for stopping conditions, either reached the MSE value equal to 0.005 or reach the maximum learning iteration which is 10000. The network is considered accepted if the network may converge less than the MSE value and maximum learning iteration. The experiment would be trapped in local minima and the convergence time would be slowed down if it ran for more than 10,000 iterations. It will take longer for the experiment to converge to minimum error. The HBA-ANN validation result is displayed in Table 4 with respect to learning iterations and convergence time.

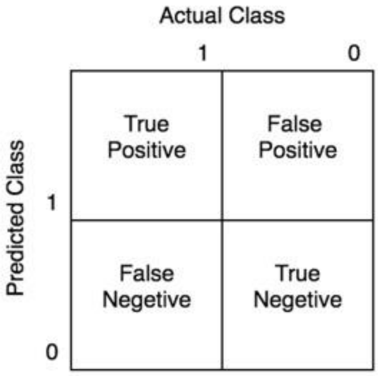
Table 4. Summary of convergence time and learning iterations of HBA-ANN

Validation	Value
Error Convergence	0.005
Learning Iteration	1689
Convergence Time (s)	528

The result shows that HBA-ANN is able to produce the minimum error with 0.00498 as it reached the minimum error. Moreover, HBA-ANN reached minimum error before reaching maximum iteration with 1689 of learning iteration. As conclusion, the HBA-ANN had been validated and can be applied to the testing dataset because it reaches the minimum error, without trapped in local minima and obtained convergence time with 528 second.

4.2 RESULT ANALYSIS AND EVALUATION

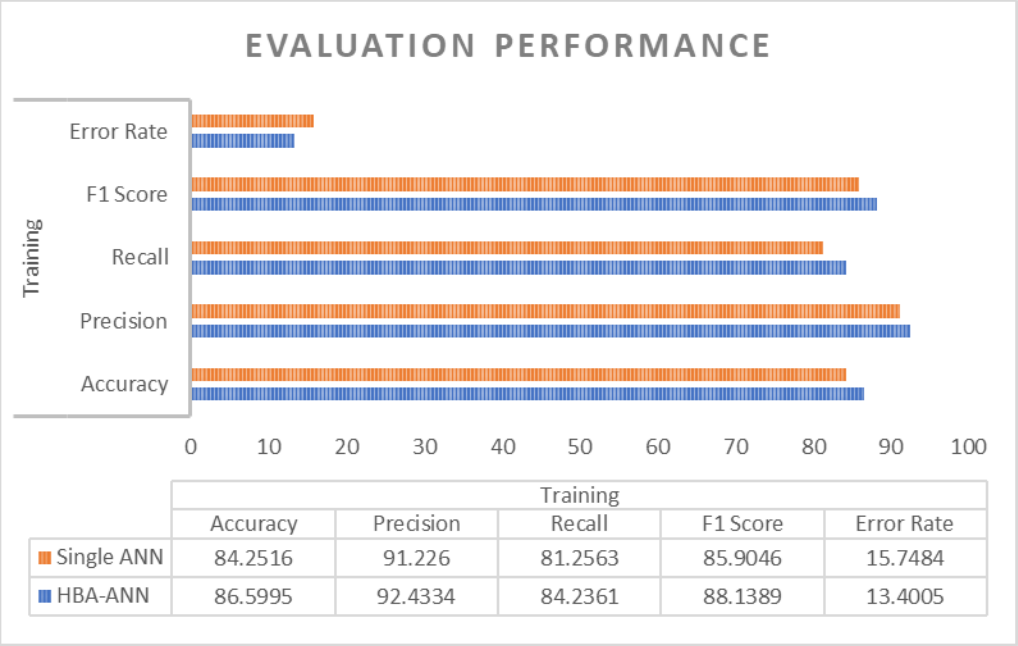
The classification results of the hybrid HBA-ANN algorithm for website phishing detection is recorded, analyzed, and evaluated based on the classification performances metrics. The result is presented in confusion matrix as shown in Figure 5 in terms of true positive, true negative, false positive and false negative. Additional performances evaluation in terms of recall, precision, F1-score, error rate and accuracy were measured based on the generated confusion matrix.



Predicted Class \ Actual Class	1	0
1	True Positive	False Positive
0	False Negetive	True Negetive

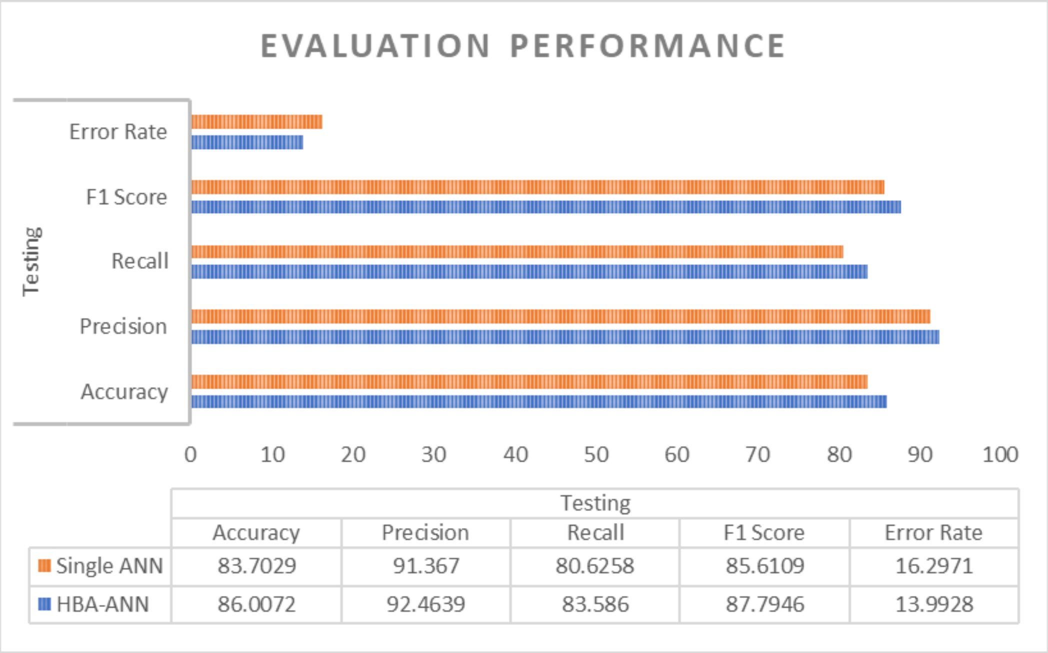
FIGURE 5. Confusion Matrix

Lastly the result is evaluated by comparing it with a single ANN algorithm according to performance evaluation measurements. The evaluation results of the proposed HBA-ANN and single ANN algorithms based on accuracy, recall, precision, F-score, and error rate for every phase of training and testing network of ANN were demonstrated in Figure 6 and Figure 7 respectively.



	Training				
	Accuracy	Precision	Recall	F1 Score	Error Rate
▨ Single ANN	84.2516	91.226	81.2563	85.9046	15.7484
▨ HBA-ANN	86.5995	92.4334	84.2361	88.1389	13.4005

FIGURE 6. Comparison of training phase evaluation performance



	Testing				
	Accuracy	Precision	Recall	F1 Score	Error Rate
▨ Single ANN	83.7029	91.367	80.6258	85.6109	16.2971
▨ HBA-ANN	86.0072	92.4639	83.586	87.7946	13.9928

FIGURE 7. Comparison of testing phase evaluation performance

5. CONCLUSION

This study presents the development and evaluation of a hybrid HBA-ANN classification model for website phishing detection. The goal is to enhance the performance of the ANN using the metaheuristic approach, the HBA. Three primary processes comprise the development of the proposed hybrid HBA-ANN model, which are outlined in an algorithm comprising thirteen steps. These processes involve optimizing the network's learning process through the HBA, which modifies the weights of interconnections to minimize the network's error and improve its performance in detecting website phishing.

In the evaluation phase, the proposed hybrid HBA-ANN model is compared to a single ANN in terms of several performance metrics, including recall, precision, F1 score, error rate, and accuracy. The result demonstrated that the hybrid HBA-ANN model achieves 2.3 percent improvement in accuracy compared to the single ANN. As contributions, this study highlights the improvement of the ANN classification process through the optimized network learning process using the Honey Badger Algorithm. The proposed hybrid HBA-ANN classification model demonstrates better performance in detecting website phishing activity, showing promising results for website phishing detection.

Funding

None

ACKNOWLEDGEMENT

The authors honorably appreciate Soft Computing and Optimization Research Group (SCORE) for their support.

CONFLICTS OF INTEREST

The author declares no conflict of interest.

REFERENCES

[1] M. Mijwil, I. E. Salem, and M.M. Ismaeel, “The Significance of Machine Learning and Deep Learning Techniques in Cybersecurity: A Comprehensive Review,” *Iraqi Journal for Computer Science and Mathematics*, vol. 4, no. 1, pp 87-101. January 2023. https://doi.org/10.52866/ijcsm.2023.01.01.008

[2] A. D. Jasim, "A survey of intrusion detection using deep learning in internet of things," *Iraqi Journal for Computer Science and Mathematics*, vol. 3, no. 1, pp.83-93, January 2022. https://doi.org/10.52866/ijcsm.2022.01.01.009

[3] S. Mishra, and D. Soni, “SMS phishing and mitigation approaches,” *International Conference on Contemporary Computing*, pp. 1-5, August 2019. https://doi.org/10.1109/IC3.2019.8844920

[4] M. Mijwil, R. Doshi, K. K. Hiran, A. H. Al-Mistarehi, and M. Gök, "Cybersecurity Challenges in Smart Cities: An Overview and Future Prospects", *Mesopotamian Journal of CyberSecurity*, vol. 2022, pp. 1–4, January 2022. https://doi.org/10.58496/MJCS/2022/001

[5] M. Jasim and . L. E. George, "Phishing Attacks Detection by Using Artificial Neural Networks ", *Iraqi Journal for Computer Science and Mathematics*, vol. 4, no. 3, pp. 159–166, Aug. 2023. https://doi.org/10.52866/ijcsm.2023.02.03.013

[6] W. Syafitri, Z. Shukur, U. A. Mokhtar, R. Sulaiman and M. A. Ibrahim, "Social Engineering Attacks Prevention: A Systematic Literature Review," in IEEE Access, vol. 10, pp. 39325-39343, 2022. https://doi.org/10.1109/ACCESS.2022.3162594

[7] A. Mughaid, S. AlZu'bi, A. A. Hnaif, S. Taamneh, A. Alnajjar, and E. A. Elsoud, "An intelligent cyber security phishing detection system using deep learning techniques," *Cluster Computing*, vol. 25, no. 6, pp. 3819–3828, 2022, https://doi.org/10.1007/s10586-022-03604-4

[8] M. Alqahtani, "Phishing Websites Classification using Association Classification (PWCAC)," *International Conference on Computer and Information Sciences (ICCIS*), Sakaka, Saudi Arabia, 2019, pp. 1-6. https://doi.org/10.1109/ICCISci.2019.8716444

[9] M. Kathiravan, V. Rajasekar, S. J. Parvez, V. S. Durga, M. Meenakshi and S. Gowsalya, "Detecting Phishing Websites using Machine Learning Algorithm," *7th International Conference on Computing Methodologies and Communication (ICCMC)*, Erode, India, 2023, pp. 270-275. https://doi.org/10.1109/ICCMC56507.2023.10083999

[10] J. Hong, T. Kim, J. Liu, N. Park, and S. W. Kim. "Phishing url detection with lexical features and blacklisted domains," *Adaptive autonomous secure cyber systems*, pp. 253-267. February 2020. https://doi.org/10.1007/978-3-030-33432-1_12

[11] H. Apaydin, H. Feizi, M. T. Sattari, M. S. Colak, S. Shamshirband, and K.-W. Chau. "Comparative analysis of recurrent neural network architectures for reservoir inflow forecasting," *Water*, vol. 12, no. 5. pp. 1500. 2020. https://doi.org/10.3390/w12051500

[12] T. Vijayakumar, "Comparative study of capsule neural network in various applications," *Journal of Artificial Intelligence*, vol. 1, no. 1, pp. 19-27, September 2019. https://doi.org/10.36548/jaicn.2019.1.003

[13] F. Safara, A. S. Mohammed, M. Y. Potrus, S. Ali, Q. T. Tho, A. Souri, F. Janenia, M. Hosseinzadeh, "An Author Gender Detection Method Using Whale Optimization Algorithm and Artificial Neural Network," *IEEE Access*, vol. 8, pp. 48428-48437, February 2020. https://doi.org/10.1109/ACCESS.2020.2973509

[14] M. A. Awadallah, I. Abu-Doush, M. A. Al-Betar, and M. S. Braik, "Metaheuristics for optimizing weights in neural networks," *Comprehensive Metaheuristics*, pp. 359-377. Academic Press, 2023. https://doi.org/10.1016/B978-0-323-91781-0.00005-3

[15] S. Gulcu, "Training of the feed forward artificial neural networks using dragonfly algorithm," *Applied Soft Computing*, vol. 124, pp 109023, July 2022. https://doi.org/10.1016/j.asoc.2022.109023

[16] A. C. Cinar, "Training feed-forward multi-layer perceptron artificial neural networks with a tree-seed algorithm," *Arabian Journal for Science and Engineering*, vol. 45, no. 12, pp.10915-10938, December 2020. https://doi.org/10.1007/s13369-020-04872-1

[17] D. Devikanniga, K. Vetrivel, and N. Badrinath, "Review of meta-heuristic optimization based artificial neural networks and its applications," *Journal of Physics: Conference Series*, vol. 1362, no. 1, p. 012074. 2019. https://doi.org/10.1088/1742-6596/1362/1/012074

[18] S. Mandal, G. Saha, and R. K. Pal, "Neural network training using firefly algorithm," *Global Journal on Advancement in Engineering and Science*, vol 1, no. 1, pp. 7-11, 2015. https://doi.org/10.1145/3350532

[19] V. Nagori, "Fine tuning the parameters of back propagation algorithm for optimum learning performance," *2nd International Conference on Contemporary Computing and Informatics (IC3I)*, Greater Noida, India, 2016, pp. 7-12. https://doi.org/10.1109/IC3I.2016.7917926

[20] S. Y. S. Leung, Y. Tang, and W. K. Wong, "A hybrid particle swarm optimization and its application in neural networks," *Expert Systems with Applications*, vol. 39, no. 1, pp. 395-405, January 2021. https://doi.org/10.1016/j.eswa.2011.07.028

[21] Z. Lin, S. Du and A. Matta, "A New Partition-Based Random Search Method for Deterministic Optimization Problems," *Winter Simulation Conference (WSC)*, National Harbor, MD, USA, 2019, pp. 3504-3515. https://doi.org/10.1109/WSC40007.2019.9004850

[22] J. F. Chen, Q. H. Do, and H. N. Hsieh, "Training artificial neural networks by a hybrid PSO-CS algorithm," *Algorithms*, vol. 8, no. 2, pp. 292-308, June 2015. https://doi.org/10.3390/a8020292

[23] M. Kaveh, and M. S. Mesgari, "Application of meta-heuristic algorithms for training neural networks and deep learning architectures: A comprehensive review," *Neural Processing Letters*, vol. 55, no. 4, pp. 4519-4622, August 2023. https://doi.org/10.1007/s11063-022-11055-6

[24] S. Alsammarraie, and N. K. Hussein, "A new hybrid grasshopper optimization-backpropagation for feedforward neural network training," *Tikrit Journal of Pure Science*, vol. 25, no. 1, pp. 118-127, February 2020. http://dx.doi.org/10.25130/tjps.25.2020.018

[25] C. Berdjouh, M. C. E. Meftah, A. Laouid, M. Hammoudeh and A. Kumar, "Pelican Gorilla Troop Optimization Based on Deep Feed Forward Neural Network for Human Activity Abnormality Detection in Smart Spaces," *IEEE Internet of Things Journal*, vol. 10, no. 21, pp. 18495-18504, November 2023. https://doi.org/10.1109/JIOT.2023.3271831

[26] S. Arora, and S. Singh, "Butterfly optimization algorithm: a novel approach for global optimization," *Soft Computing*, vol. 23, pp. 715-734, February 2019. https://doi.org/10.1007/s00500-018-3102-4

[27] A. A. Heidari, S. Mirjalili, H. Faris, I. Aljarah, M. Mafarja, and H. Chen, "Harris hawks optimization: Algorithm and applications," *Future generation computer systems*, vol. 97, pp. 849-872, August 2019. https://doi.org/10.1016/j.future.2019.02.028

[28] M. H. Sulaiman, Z. Mustaffa, M. M. Saari, and H. Daniyal, "Barnacles mating optimizer: A new bio-inspired algorithm for solving engineering optimization problems," *Engineering Applications of Artificial Intelligence*, vol. 87, pp. 103330, January 2020. https://doi.org/10.1016/j.engappai.2019.103330

[29] S. Z. Mirjalili, S. Mirjalili, S. Saremi, H. Faris, and I. Aljarah, "Grasshopper optimization algorithm for multi-objective optimization problems," *Applied Intelligence*, vol. 48, pp. 805-820, April 2018. https://doi.org/10.1007/s10489-017-1019-8

[30] X. S. Yang, "Flower pollination algorithm for global optimization," *International conference on unconventional computing and natural computation*, pp. 240-249. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012. https://doi.org/10.1007/978-3-642-32894-7_27

[31] F. A. Hashim, E. H. Houssein, K. Hussain, M. S. Mabrouk, and W. Al-Atabany, “Honey Badger Algorithm: New metaheuristic algorithm for solving optimization problems,” *Mathematics and Computers in Simulation*, vol. 192, pp. 84-110, February 2022. https://doi.org/10.1016/j.matcom.2021.08.013

[32] Alshahrani, S.M., Khan, N.A., Almalki, J. and Al Shehri, W. “URL Phishing Detection Using Particle Swarm Optimization and Data Mining”. Computers, Materials & Continua, 73(3).2022. http://dx.doi.org/10.32604/cmc.2022.030982

[33] W. Ali, and A. A. Ahmed, “Hybrid intelligent phishing website prediction using deep neural networks with genetic algorithm-based feature selection and weighting,” *IET Information Security*, vol. 13, no. 6, pp. 659-669, November 2019. https://doi.org/10.1049/iet-ifs.2019.0006

[34] A. Fathy, H. Rezk, S. Ferahtia, R. M. Ghoniem, and R. Alkanhel, “An efficient honey badger algorithm for scheduling the microgrid energy management,” *Energy Reports*, vol. 9, pp.2058-2074. December 2023. https://doi.org/10.1016/j.egyr.2023.01.028

[35] R. Khajuria, S. Yelisetti, R. Lamba, and R. Kumar, “Optimal model parameter estimation and performance analysis of PEM electrolyzer using modified honey badger algorithm,”. *International Journal of Hydrogen Energy*, vol. 49, pp. 238-259, January 2024. https://doi.org/10.1016/j.ijhydene.2023.07.172

[36] S. N. Qasem, “A novel honey badger algorithm with multilayer perceptron for predicting COVID-19 time series data,” *The Journal of Supercomputing*, vol. 80, pp. 3943–3969. September 2023. https://doi.org/10.1007/s11227-023-05560-1

[37] D. Dua, and C. Graff, UCI Machine Learning Repository. Irvine, CA: University of California, School of Information and Computer Science. 2019

[38] G. Zhang, B. E. Patuwo, and M. Y. Hu, “Forecasting with Artificial Neural Networks: The State of Art,” *International Journal of Forecasting*. Vol. 14, pp. 35-62. 1998