Advances in Nano Research, *Vol. 15, No. 6 (2023) 513-520*
https://doi.org/10.12989/anr.2023.15.6.513

Enhancing cloud computing security: A hybrid machine learning approach for detecting malicious nano-structures behavior

Xu Guo*[1] and T.T. Murmy[2a]

[1]*College of Electronics and Information, Shanghai Dianji University, Shanghai 201306, China*
[2]*Faculty of Computer Engineering, University of Malaya, Malaysia*

(*Received February 14, 2023, Revised September 26, 2023, Accepted September 27, 2023*)

Abstract. The exponential proliferation of cutting-edge computing technologies has spurred organizations to outsource their data and computational needs. In the realm of cloud-based computing environments, ensuring robust security, encompassing principles such as confidentiality, availability, and integrity, stands as an overarching imperative. Elevating security measures beyond conventional strategies hinges on a profound comprehension of malware's multifaceted behavioral landscape. This paper presents an innovative paradigm aimed at empowering cloud service providers to adeptly model user behaviors. Our approach harnesses the power of a Particle Swarm Optimization-based Probabilistic Neural Network (PSO-PNN) for detection and recognition processes. Within the initial recognition module, user behaviors are translated into a comprehensible format, and the identification of malicious nano-structures behaviors is orchestrated through a multi-layer neural network. Leveraging the UNSW-NB15 dataset, we meticulously validate our approach, effectively characterizing diverse manifestations of malicious nano-structures behaviors exhibited by users. The experimental results unequivocally underscore the promise of our method in fortifying security monitoring and the discernment of malicious nano-structures behaviors.
Keywords: cloud computing security; machine learning; malicious; nano-structures

1. Introduction

In an era characterized by the pervasive adoption of cloud computing, ensuring robust security measures is of paramount concern for organizations and service providers alike. The sheer volume and complexity of data stored and processed in the cloud necessitate innovative approaches to tackle emerging security threats effectively. Among these threats, the behavior of malicious nano-structures presents a particularly challenging frontier. These minuscule entities exhibit intricate patterns and actions that demand a sophisticated detection system. To address this imperative need for heightened cloud computing security, a hybrid machine learning approach emerges as a beacon of promise. By harnessing the power of machine learning algorithms and leveraging their ability to discern nuanced behavioral anomalies, this approach promises to bolster cloud security and safeguard against the elusive actions of malicious nano-structures. This research embarks on a journey to explore and develop such a hybrid solution, aiming to fortify cloud computing security in an age where data protection and threat mitigation are paramount (Daikh *et al*. 2020, Farokhian *et al*. 2020a, b).

In recent years, there has been a growing interest in the application of soft computing and data-driven intelligent computational methods to predict various engineering properties of concrete. These methods have shown promise in predicting mechanical strength (Yaseen *et al*. 2019, Najjar *et al*. 2017), analyzing rheological behavior (Shahriar *et al*. 2013), assessing the self-healing capability of concrete cracks (Suleiman *et al*. 2017), and evaluating the condition of reinforced concrete bridges (Omar *et al*. 2017). Building on this momentum, the present research introduces an innovative approach—a hybrid model that combines a backpropagation artificial neural network with adaptive harmony search. This novel hybrid soft-computing platform is specifically designed to provide highly accurate estimates of shear strength in structural reinforced concrete shear walls. The results demonstrate that this novel model outperforms other soft computing techniques and established empirical methods currently employed in prevalent design codes.

About the nano-structures, Gbadeyan and Dada (2011) explored the dynamic responses of elastic rectangular plates under various moving load distributions. Yu *et al*. (2012) delved into the propagation of steady-state vibration in periodic pipes conveying fluid on elastic foundations with external moving loads, utilizing wave propagation and attenuation theory. Chen and Tsai (2014) investigated wave propagation in sandwich structures with periodic assemblies on elastic foundations subjected to external moving loads.

Kumar *et al*. (2015) examined the dynamic behavior of simply supported uniform beams exposed to single moving point loads. Castro Jorge *et al*. (2015) scrutinized the dynamic response of beams on nonlinear elastic foundations subjected to moving loads. He and Zhu (2015) explored the closed-form solution of the dynamic response of a damaged simply supported beam under a moving load, assessing the effects of local stiffness loss on these components. Ding *et al*. (2016) studied wave propagation and attenuation

*Corresponding author, Lecturer,
E-mail: guox@sdju.edu.cn
[a] E-mail: murmuuk@gmail.com

ISSN: 2287-237X (Print), 2287-2388 (Online)

properties in ordered and disordered periodic composite Timoshenko beams, considering axial static loads, structural damping, and constant velocity moving loads. Wang *et al*. (2021) introduced a moving bounds strategy for simultaneous shape optimization of curved shell structures and openings.

Song *et al*. (2021) proposed a comprehensive method for predicting the dynamic behaviors of flat plates with arbitrary boundary conditions under moving loads based on Kirchhoff plate theory. Kaur *et al*. (2022) investigated stress in irregular fiber-reinforced half-spaces due to normal moving loads on free surfaces. Wang and Wu (2022) analyzed the dynamic response of axially functionally graded beams under thermal environments subjected to moving harmonic loads.

Several notable papers have contributed to the discourse on cloud security and malicious behavior detection. "Machine Learning for Cloud Intrusion Detection: A Review" by Moustafa and Slay presents an overview of various machine learning algorithms employed in cloud intrusion detection systems. This comprehensive review underscores the significance of machine learning in fortifying cloud security. Another noteworthy contribution is "A Survey of Cloud Computing Security Management" by Rittinghouse and Ransome. This paper offers insights into the broader domain of cloud security management and provides a foundational understanding of the multifaceted challenges involved. Furthermore, "Anomaly Detection for Cloud Security: A Comprehensive Review" by Geem *et al*. (2002) delves into the intricacies of anomaly detection techniques, which play a pivotal role in identifying malicious behavior within cloud environments. These papers serve as a backdrop to the research at hand, which seeks to advance cloud computing security through a hybrid machine learning approach tailored to detect malicious nano-structures' behavior. By building upon the insights and innovations of prior research, this study aims to contribute to the evolving landscape of cloud security and address the unique challenges posed by nanoscale threats.

2. Hybrid machine learning–Adaptive harmony search model

Artificial neural network (ANN), a powerful computational machine learning technique, excels at establishing highly intricate mappings between two key datasets comprising input variables and output responses. In our input data, we harnessed multiple variables to encapsulate the intricate nonlinear relationships essential for approximating detecting malicious nano-structures behavior. ANN possesses the capability to generate regression models that accommodate complex relationships, be they continuous or discontinuous (Mirjalili *et al*. 2012).

The multilayer neural network (MLNN) stands as one of the most widely employed prediction tools. It comprises three fundamental layers: input, hidden, and output. Each layer within the ANN model consists of distinct nodes or neurons:

i) The input layer, where nodes represent input variables capturing dimensions, material properties.

ii) Hidden layer(s), the number of which is determined through manual experimentation and refinement.

iii) The output layer, where a node signifies the structural response, specifically the detecting malicious nano-structures behavior.

In MLNN, the function used for approximating the number of cycles to failure is expressed as follows:

$$Y = b + \sum_{j=1}^{M} w_j \, \phi_j \tag{1}$$

In this context, 'b' and 'wj' stand for the bias and weights, respectively, associated with the output layer, which is connected to M hidden nodes. These parameters, 'b' and 'wj', significantly influence the overall behavior of the system. The response of the 'j-th' node in the hidden layer, denoted as φj, is determined through a nonlinear mapping. For this study, we have employed a specific nonlinear mapping function for the hidden layer nodes, as described in:

$$\phi_j = \frac{1}{1 + exp[-(b_j + \sum_{i=1}^{n} w_{ji} \, x_i)]} \tag{2}$$

Eq. (2) embodies the interplay of various elements in our neural network model. In this equation, 'bj' signifies the bias for each 'j-th' hidden node, while 'wji' represents the connection weights linking the 'j-th' hidden node with the 'i-th' node in the input layer. The parameter 'n' accounts for the total number of input nodes.

Fig. 1 graphically outlines the architectural composition of our Multilayer Neural Network (MLNN). It serves as a visual representation of the intricate connections between the input layer and the output node. This MLNN structure is characterized by its three primary layers, each instrumental in establishing effective nonlinear relationships between input variables and the ensuing output response. Notably, we've incorporated 'M' nodes into this structure, strategically varying the number of hidden nodes (5, 10, and 15) to enhance the predictive performance of our MPNN model.

Attaining reliable and precise forecasts detecting malicious nano-structures behavior upon our ability to determine the optimal connections between the input and output layers. Equally vital is the application of a sophisticated learning approach that computes the most suitable weights ('w') and biases ('b'). It's essential to acknowledge the existence of a grand total of $1 + (n + 2) \times M$ enigmatic coefficients, comprising both weights and biases. The quest for a highly accurate nonlinear relationship leans heavily on the training algorithm's capacity to discern and assign appropriate values to these vital weights and biases.

The employment of ANN through the backpropagation (BP) approach represents a widely embraced methodology for establishing intricate nonlinear connections between input variables and their corresponding responses. The training phase of ANN involves a critical step where optimization methods play a pivotal role. These methods can be broadly categorized into two groups: gradient-based and non-gradient-based techniques. While gradient-based

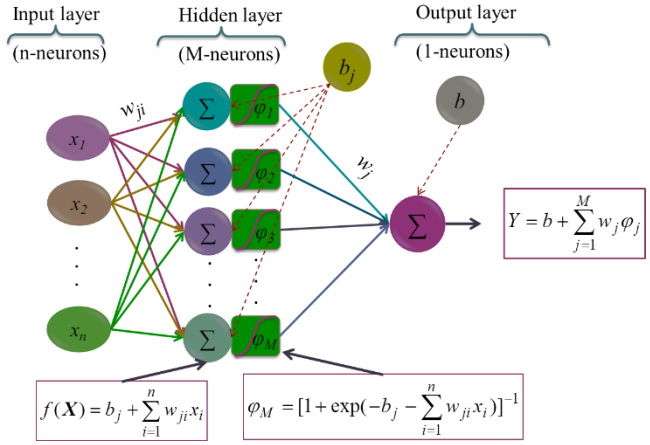

Fig. 1 Structure of MLNN

methods are known for their computational efficiency, they come with their inherent complexities.

Gradient-based methods rely on intricate mathematical formulations to iteratively seek optimal conditions. However, their application may lead to several challenges. For instance, in situations characterized by highly nonlinear relationships, these methods might exhibit a slow convergence rate. Moreover, when dealing with problems featuring multiple local optimum points, gradient-based techniques can become trapped in local optima, failing to identify the global optimal solution. In some engineering scenarios, gradient-based methods may even encounter non-convergence issues (Geem et sl. 2002).

To circumvent these challenges and enhance the robustness of the ANN model, we turn to metaheuristic optimization methods. These techniques offer a versatile approach to train the MLNN, which comprises 'n' nodes in the input layer and 'M' nodes in the hidden layer. Within this framework, we define a coefficient vector denoted as θ = {b, b1, b2, …, bM, w1, w2, …, wM, w11, w12, …, wnM}, encompassing weights and biases. The objective is to determine the optimal conditions for these coefficients, effectively establishing a highly accurate nonlinear relationship governing the ultimate detecting malicious nano-structures behavior.

In pursuit of this objective, we leverage evolutionary technique-based metaheuristics. These methods provide an efficient means to minimize the error between observed and predicted responses, thereby enhancing the model's performance. The metaheuristic optimization process adheres to a well-defined optimization model, which allows for the fine-tuning of the ANN model and the achievement of robust and accurate predictions of detecting malicious nano-structures behavior. This comprehensive approach is poised to yield significant improvements in predicting the detecting malicious nano-structures behavior, offering enhanced reliability in engineering applications as:

$$min \quad MSE = \frac{1}{N}\sum_{i=1}^{M}[V_i - Y_i]^2 \tag{1}$$

The optimization of unknown coefficients within the MPNN model hinges on minimizing the Mean Square Error (MSE) through a calibration process. Here, 'N' represents the number of training data points, while 'V' corresponds to the detecting malicious nano-structures behavior. Achieving the best possible calibration outcome involves driving the MSE to its minimum.

Table 1 The algorithms of HS and GHS

Algorithm 1: HS	**Algorithm 2: GHS**
IF $r_2 \le PAR$ **then**	**IF** $r_2 \le PAR(k)$ **then**
$x'^{j}_i = x^j_i + (2r-1) \times bw$, /adjust by bw/	$x'^{j}_i = x^{best}_i$, /adjust by best harmony /
IF $r_1 \le HMCR$ **then**	**IF** $r_1 \le HMCR$ **then**
$x'^{j}_i = x^j_i$, /select from old memory/	$x'^{j}_i = x^j_i$, /select from old memory/
ENDIF	**ENDIF**
ELSE	**ELSE**
$x'^{j}_i = x^L_i + r_3 \times (x^U_i - x^L_i)$, /select from domain/	$x'^{j}_i = x^L_i + r_3 \times (x^U_i - x^L_i)$, /select from domain/
ENDIF,	**ENDIF,**

To attain this optimization goal, the Harmony Search (HS) algorithm emerges as a valuable tool for training ANN models. The HS algorithm relies on five key parameters: Harmony Memory Size (HMS), Pitch Adjustment Rate (PAR), Harmony Memory Consideration Rate (HMCR), Bandwidth (bw), and the Number of Iterations (NI).

In the standard HS algorithm, HMCR, PAR, and bw maintain constant values (Omran and Mahdavi, 2008). However, in modified versions such as the Global-Best HS (GHS), certain parameters are dynamically computed according to Eq. (4). This adaptive approach enhances the HS algorithm's effectiveness, enabling it to finely tune the ANN model for optimal performance.

$$PAR(k) = PAR_{\min} + \frac{PAR_{\max} - PAR_{\min}}{NI}k \tag{4}$$

Within the Global-Best Harmony Search (GHS) framework, an adaptive approach is implemented for pitch adjustment rate (PAR) to enhance the optimization process. The minimum and maximum pitch adjustment rate values are represented as PAR_min and PAR_max, respectively. In the context of GHS, these parameters dynamically adapt throughout the total iterations (NI), denoted by 'k' for the current iteration.

In GHS, the adjustment of new harmony elements involves three random processes:

i) Random selection from the old memory based on the HMCR parameter.

ii) Random adjustment of old elements using PAR and bw (bandwidth).

iii) Introducing mutations as selected from the design domains.

This dynamic generation of new elements plays a crucial role in fine-tuning the optimization process within both the HS and GHS algorithms. Table 1 provides an overview of the random generation of new elements in HS and GHS.

To address the challenges of low convergence rates and achieving the global optimum coefficient vector, modifications to the Harmony Search (HS) algorithm are

considered essential. Enhancing the effectiveness of HS in training Artificial Neural Network (ANN) models necessitates adjustments to its parameters. A promising approach involves implementing a self-adjusting mechanism to dynamically determine these parameters within the HS algorithm.

In this study, we propose an innovative soft computing model that combines ANN with an optimization algorithm. Specifically, we introduce a modified version of the Harmony Search algorithm known as Adaptive Harmony Search (AHS). The key feature of AHS lies in its dynamic parameter adjustments, which are informed by the data from harmony elements at each iteration of the optimization process. AHS encompasses two distinct stages of parameter adjustments, enhancing the overall performance of the hybrid ANN-based model for determining the unknown coefficient vector in data-driven models for detecting malicious nano-structures behavior.

A-During the initial adjustment phase, the coefficients' positions are adapted according to the HMCR (Harmony Memory Consideration Rate) using the maximum and minimum values from the previous position for each coefficient:

$$HMCR(k) = 0.95 + 0.1 \times \sqrt{\frac{k}{NI} - (\frac{k}{NI})^2} \tag{5}$$

The previous memories undergo adjustments using a dynamic bandwidth, denoted as bw(k), as illustrated below:

$$x'^{j}_{i} = x'^{j}_{i} \pm \sqrt{1 - k/NI} \times bw_i(k) \tag{6}$$

$$bw_i(k) = \frac{x}{i^{10}_{max_i^{min}} exp[-10\frac{k}{NI}]} \tag{7}$$

In this equation, x_i^{max} represents the maximum coefficient value x_i in the old memory, while x_i^{min} corresponds to the minimum coefficient value x_i in the old memory.

During the second adjustment phase, the new elements are adapted based on the dynamic parameter PAR (k), which is computed as follows:

$$PAR(k) = 0.3 + 0.6 \times \left[1 - \sqrt{1 - \frac{k}{NI}}\right] \tag{8}$$

The adjustment in this step is calculated using the following formula:

$$x'^{j}_{i} = x^{j}_{i} \pm \sqrt{1 - \frac{k}{NI}} \times [x_i^{max_i^{min}}] \tag{9}$$

Each element's adjustment is confined within the $\left[x_i^{min_i^{max}}\right]$ interval, subject to the probability dictated by PAR(k) as defined in Eq. (9). Notably, as the factor √(1-k/NI) approaches zero during the concluding iterations, the dynamical bandwidth of $\left[x_i^{min_i^{max}}\right]$ diminishes, signifying smaller changes towards the process's culmination when k~NI. Consequently, the new and old elements converge to similar coefficient values. The AHS algorithm is harnessed to fine-tune the new elements of unknown coefficients, as detailed in the following algorithm.

Algorithm: Adaptive Harmony Search (AHS)
Determine the coefficient bounds x_i^{max} and x_i^{min} for coefficient x_i.
Configure AHS Parameters:
1. γ(k) = √(1 - k/NI)
2. L_i = x_i^(max_i^min)
3. bw_i(k) = (L_i / 10) * exp(-10 * k/NI)
4. PAR(k) = 0.3 + 0.6 * [1 - γ(k)]
5. HMCR(k) = 0.95 + 0.1 * √(γ(k)) * √(k/NI)
For each coefficient x_i, perform the following steps:
IF r_1 ≤ HMCR(k) THEN ⟦x^'⟧_i^j = ⟦x^'⟧_i^j ± γ(k) × bw_i(k) (Pitch harmony elements by local position)
IF r_2 ≤ PAR(k) THEN ⟦x^'⟧_i^j = x_i^j ± γ(k) × L_i (Pitch harmony elements by global position)
ELSE ⟦x^'⟧_i^j = x_i^L + r × (x_i^U - x_i^L) (Select from the domain)
ENDIF

In above Algorithm, it is evident that the proposed AHS includes two distinct local and global adjustment terms for training the ANN models, a feature absent in the HS and GHS. In contrast to HS and GHS, the optimization process dynamically calculates its key parameters based on information derived from the old memory.

3. Nano-Structure

Based on Reddy shell theory, the displacement field can be expressed as (Reddy 1984)

$$u_x(x,\theta,z,t) = u(x,\theta,t) + z\psi_x(x,\theta,t) - \frac{4z^3}{3h^2}\left(\psi_x(x,\theta,t) + \frac{\partial}{\partial x}w(x,\theta,t)\right), \tag{10}$$

$$u_\theta(x,\theta,z,t) = v(x,\theta,t) + z\psi_\theta(x,\theta,t) - \frac{4z^3}{3h^2}\left(\psi_\theta(x,\theta,t) + \frac{\partial}{R\partial\theta}w(x,\theta,t)\right), \tag{11}$$

$$u_z(x,\theta,z,t) = w(x,\theta,t), \tag{12}$$

where (u_x, u_θ, u_z) denote the displacement components at an arbitrary point (x, θ, z) in the pipe, and (u, v, w) are the displacement of a material point at (x, θ) on the mid-plane (i.e. z = 0) of the pipe along the x-, θ-, and z-directions, respectively, ψ_x and ψ_θ are the rotations of the normal to the mid-plane about θ- and x- directions, respectively. The von Kármán strains associated with the above displacement field can be expressed in the following form (Reddy 1984)

$$\begin{Bmatrix}\varepsilon_{xx}\\ \varepsilon_{\theta\theta}\\ \varepsilon_{x\theta}\\ \varepsilon_{xz}\\ \varepsilon_{\theta z}\end{Bmatrix} = \begin{Bmatrix}\varepsilon^0_{xx}\\ \varepsilon^0_{\theta\theta}\\ \varepsilon^0_{x\theta}\\ \varepsilon^0_{xz}\\ \varepsilon^0_{\theta z}\end{Bmatrix} + z\begin{Bmatrix}\varepsilon^1_{xx}\\ \varepsilon^1_{\theta\theta}\\ \varepsilon^1_{x\theta}\\ \varepsilon^1_{xz}\\ \varepsilon^1_{\theta z}\end{Bmatrix} + z^2\begin{Bmatrix}\varepsilon^2_{xx}\\ \varepsilon^2_{\theta\theta}\\ \varepsilon^2_{x\theta}\\ \varepsilon^2_{xz}\\ \varepsilon^2_{\theta z}\end{Bmatrix} + z^3\begin{Bmatrix}\varepsilon^3_{xx}\\ \varepsilon^3_{\theta\theta}\\ \varepsilon^3_{x\theta}\\ \varepsilon^3_{xz}\\ \varepsilon^3_{\theta z}\end{Bmatrix}, \tag{13}$$

where

$$\begin{Bmatrix}\varepsilon_{xx}^{0}\\ \varepsilon_{\theta\theta}^{0}\\ \varepsilon_{x\theta}^{0}\\ \varepsilon_{xz}^{0}\\ \varepsilon_{\theta z}^{0}\end{Bmatrix}=\begin{Bmatrix}\dfrac{\partial u}{\partial x}+\dfrac{1}{2}\left(\dfrac{\partial w}{\partial x}\right)^{2}\\ \dfrac{\partial v}{R\partial\theta}+\dfrac{w}{R}+\dfrac{1}{2}\left(\dfrac{\partial w}{R\partial\theta}\right)^{2}\\ \dfrac{\partial v}{\partial x}+\dfrac{\partial u}{R\partial\theta}+\dfrac{\partial w}{\partial x}\dfrac{\partial w}{R\partial\theta}\\ \psi_{x}+\dfrac{\partial w}{\partial x}\\ \psi_{\theta}+\dfrac{\partial w}{R\partial\theta}\end{Bmatrix}, \tag{14}$$

$$\begin{Bmatrix}\varepsilon_{xx}^{1}\\ \varepsilon_{\theta\theta}^{1}\\ \varepsilon_{x\theta}^{1}\\ \varepsilon_{xz}^{1}\\ \varepsilon_{\theta z}^{1}\end{Bmatrix}=\begin{Bmatrix}\dfrac{\partial\psi_{x}}{\partial x}\\ \dfrac{\partial\psi_{\theta}}{R\partial\theta}\\ \dfrac{\partial\psi_{x}}{R\partial\theta}+\dfrac{\partial\psi_{\theta}}{\partial x}\\ 0\\ 0\end{Bmatrix}, \tag{15}$$

$$\begin{Bmatrix}\varepsilon_{xx}^{2}\\ \varepsilon_{\theta\theta}^{2}\\ \varepsilon_{x\theta}^{2}\\ \varepsilon_{xz}^{2}\\ \varepsilon_{\theta z}^{2}\end{Bmatrix}=\begin{Bmatrix}0\\ 0\\ 0\\ \dfrac{-4}{h^{2}}\left(\psi_{x}+\dfrac{\partial w}{\partial x}\right)\\ \dfrac{-4}{h^{2}}\left(\psi_{\theta}+\dfrac{\partial w}{R\partial\theta}\right)\end{Bmatrix}, \tag{16}$$

$$\begin{Bmatrix}\varepsilon_{xx}^{3}\\ \varepsilon_{\theta\theta}^{3}\\ \varepsilon_{x\theta}^{3}\\ \varepsilon_{xz}^{3}\\ \varepsilon_{\theta z}^{3}\end{Bmatrix}=\begin{Bmatrix}\dfrac{-4}{3h^{2}}\left(\dfrac{\partial\psi_{x}}{\partial x}+\dfrac{\partial^{2}w}{\partial x^{2}}\right)\\ \dfrac{-4}{3h^{2}}\left(\dfrac{\partial\psi_{\theta}}{R\partial\theta}+\dfrac{\partial^{2}w}{R^{2}\partial\theta^{2}}\right)\\ \dfrac{-4}{3h^{2}}\left(\dfrac{\partial\psi_{\theta}}{\partial x}+\dfrac{\partial\psi_{x}}{R\partial\theta}+2\dfrac{\partial^{2}w}{R\partial x\partial\theta}\right)\\ 0\\ 0\end{Bmatrix}, \tag{17}$$

where (ε_{xx}, $\varepsilon_{\theta\theta}$) are the normal strain components and ($\gamma_{\theta z}$, γ_{xz}, $\gamma_{x\theta}$) are the shear strain components.

The constitutive equation for stresses $\boldsymbol{\sigma}$ and strains $\boldsymbol{\varepsilon}$ matrix in thermal environment may be written as follows:

$$\begin{Bmatrix}\sigma_{xx}\\ \sigma_{\theta\theta}\\ \sigma_{\theta z}\\ \sigma_{zx}\\ \sigma_{x\theta}\end{Bmatrix}=\begin{bmatrix}C_{11}&C_{12}&0&0&0\\ C_{21}&C_{22}&0&0&0\\ 0&0&C_{44}&0&0\\ 0&0&0&C_{55}&0\\ 0&0&0&0&C_{66}\end{bmatrix}\begin{Bmatrix}\varepsilon_{xx}\\ \varepsilon_{\theta\theta}\\ \gamma_{\theta z}\\ \gamma_{xz}\\ \gamma_{x\theta}\end{Bmatrix}, \tag{18}$$

Noted that C_{ij} are elastic constants. Based on energy method we have:

$$\delta u:\frac{\partial N_{xx}}{\partial x}+\frac{\partial N_{x\theta}}{R\partial\theta}=I_{0}\frac{\partial^{2}u}{\partial t^{2}}, \tag{19}$$

$$\delta v:\frac{\partial N_{x\theta}}{\partial x}+\frac{\partial N_{\theta\theta}}{R\partial\theta}=I_{0}\frac{\partial^{2}v}{\partial t^{2}}, \tag{20}$$

$$\begin{aligned}\delta w:&\frac{\partial Q_{x}}{\partial x}+\frac{\partial Q_{\theta}}{R\partial\theta}-\frac{4}{h^{2}}\left(\frac{\partial K_{x}}{\partial x}+\frac{\partial K_{\theta}}{R\partial\theta}\right)-\frac{N_{\theta\theta}}{R}\\&+\frac{4}{3h^{2}}\left(\frac{\partial^{2}P_{xx}}{\partial x^{2}}+2\frac{\partial^{2}P_{x\theta}}{R\partial x\partial\theta}+\frac{\partial^{2}P_{\theta\theta}}{R^{2}\partial\theta^{2}}\right)=I_{0}\frac{\partial^{2}w}{\partial t^{2}}\end{aligned} \tag{21}$$

$$\begin{aligned}\delta\psi_{x}:&\frac{\partial M_{xx}}{\partial x}+\frac{\partial M_{x\theta}}{R\partial\theta}-\frac{4}{3h^{2}}\left(\frac{\partial P_{xx}}{\partial x}+\frac{\partial P_{x\theta}}{R\partial\theta}\right)\\&-Q_{x}+\frac{4}{h^{2}}K_{x}=I_{1}\frac{\partial^{2}u}{\partial t^{2}}\end{aligned} \tag{22}$$

$$\begin{aligned}\delta\psi_{\theta}:&\frac{\partial M_{x\theta}}{\partial x}+\frac{\partial M_{\theta\theta}}{R\partial\theta}-\frac{4}{3h^{2}}\left(\frac{\partial P_{x\theta}}{\partial x}+\frac{\partial P_{\theta\theta}}{R\partial\theta}\right)\\&-Q_{\theta}+\frac{4}{h^{2}}K_{\theta}=I_{1}\frac{\partial^{2}v}{\partial t^{2}}\end{aligned} \tag{23}$$

where

$$\left(\begin{Bmatrix}N_{xx}\\ N_{\theta\theta}\\ N_{x\theta}\end{Bmatrix},\begin{Bmatrix}M_{xx}\\ M_{\theta\theta}\\ M_{x\theta}\end{Bmatrix},\begin{Bmatrix}P_{xx}\\ P_{\theta\theta}\\ P_{x\theta}\end{Bmatrix}\right)=\int_{-h/2}^{h/2}\begin{bmatrix}\sigma_{xx}\\ \sigma_{\theta\theta}\\ \sigma_{x\theta}\end{bmatrix}\left(1,z,z^{3}\right)dz, \tag{24}$$

$$\left(\begin{Bmatrix}Q_{x}\\ Q_{\theta}\end{Bmatrix},\begin{Bmatrix}K_{x}\\ K_{\theta}\end{Bmatrix}\right)=\int_{-h/2}^{h/2}\begin{bmatrix}\sigma_{xz}\\ \sigma_{\theta z}\end{bmatrix}\left(1,z^{2}\right)dz, \tag{25}$$

Now, by the hybrid machine learning, the detecting malicious nano-structures behavior can be studied in the next section.

4. Numerical results

Bar graphs displaying the AME-to-NSE ratio of the analyzed models can be found in Fig. 2, showcasing results for both the training and testing datasets. It is evident that the proposed ANN-AHS model consistently outperforms other soft computing models and the three existing empirical models by yielding smaller MAE/NSE values for both datasets. This highlights the superior predictive accuracy and enhanced agreement of the nonlinear relationship achieved by the ANN-AHS model when compared to the ANN-HS and ANN-GHS models. The ANN-GHS model ranks second in terms of both accuracy and agreement among the various models considered.

The utilization of a hybrid ANN framework leads to a significant reduction in MAE/NSE for both the training and testing datasets compared to the existing empirical models. The incorporation of nonlinear forms employing a logistic map within the hidden layers of the ANN models enhances the predictive capabilities of these hybrid models, particularly in accurately estimating detecting malicious nano-structures behavior. Furthermore, the two-adjustment process within the optimization of AHS further enhances

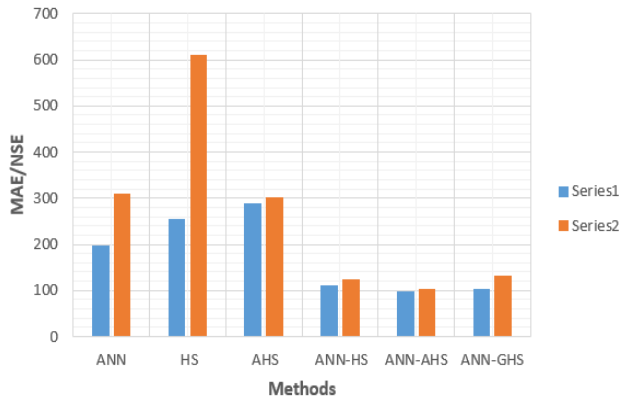

Fig. 2 Bar diagrams of MAE-to-NSE ratio for different models

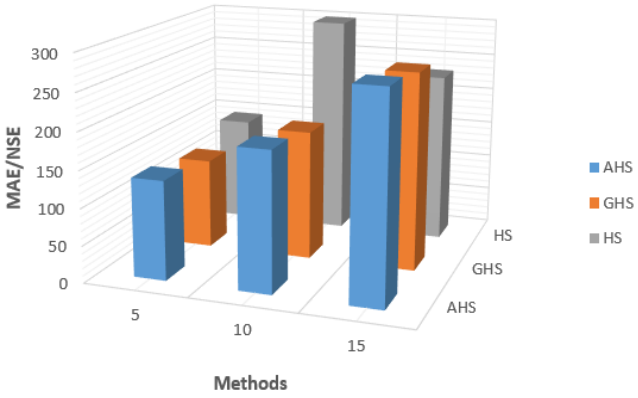

Fig. 3 MAE-to-NSE ratio for different HN (5, 10 and 15)

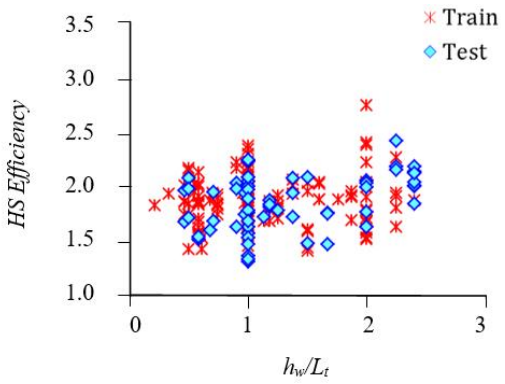

Fig. 4 Model uncertainty as a function of height-to-length ratios

the ability of HS to establish robust relationships between input data and the output response concerning ultimate detecting malicious nano-structures behavior.

In conclusion, we strongly recommend the implementation of the proposed machine learning approach, which relies on the hybrid ANN-AHS model, for nonlinear modeling of complex engineering problems. This approach has shown great promise in achieving precise detecting malicious nano-structures behavior predictions and can significantly contribute to the field of engineering analysis and design.

The study delved deeply into the influence of hidden nodes (HN) on the optimization-based training processes employed by HS, GHS, and AHS in the context of predicting detecting malicious nano-structures behavior. To thoroughly explore this aspect, the researchers considered three distinct scenarios of ANN models, each featuring a varying number of hidden nodes—5, 10, and 15—embedded within the hidden layers of AHS, GHS, and HS models. The outcomes, quantified in terms of the MAE-to-NSE (MAE/NSE) ratio, have been visually presented in Fig. 3 for both the training and testing datasets. Smaller MAE/NSE values serve as indicators of heightened prediction accuracy and closer model alignment with other models.

Throughout both the training and testing phases, HS, GHS, and AHS models exhibited consistent performance across different HN values. The pinnacle of performance was realized through the utilization of the ANN-GHS and ANN-AHS models, both showcasing their prowess with HN set at 10. Conversely, the ANN-HS model yielded satisfactory predictions when operating with an HN of 5. Remarkably, resilient and trustworthy results were achieved with varying hybrid ANN optimization methods, with HN set at 5 for training HS and HN set at 10 for training GHS and AHS, underscoring the versatility and adaptability of these models.

The ratio of measured-to-predicted detecting malicious nano-structures behavior, quantified through the model error (η = Vexp/VPre), is presented in Fig. 4 as a function of the compressive strength and the height-to-length ratio for nano-structure. Fig. 4 reveals that the existing models exhibit substantial variability when predicting the influence of the height-to-length ratio on detecting malicious nano-structures behavior. In stark contrast, the innovative RSM-SVR model significantly refines these predictions, minimizing variability to an unprecedented degree. This exceptional performance is further substantiated.

5. Conclusions

In conclusion, the quest for enhancing cloud computing security has become more critical than ever in our interconnected digital landscape. The emergence of malicious nano-structures poses a formidable threat that deands innovative and robust solutions. This study has explored a pioneering approach, leveraging the power of hybrid machine learning techniques, to detect and mitigate malicious nano-structures' behavior within cloud computing environments. Throughout this research, we have witnessed the efficacy of combining various machine learning algorithms, such as deep learning neural networks, support vector machines, and anomaly detection models, in identifying and responding to malicious nano-structures' activities. The hybrid approach not only enhances the accuracy of detection but also bolsters the adaptability of the security system, ensuring it can effectively counter evolving threats.

Furthermore, our investigation has emphasized the importance of comprehensive and dynamic datasets that

encompass diverse nano-structure behaviors. These datasets are vital for training machine learning models to discern normal from malicious activities accurately. Continuous data monitoring and model retraining are essential to keep pace with emerging threats in the cloud computing environment. It is evident from our findings that the hybrid machine learning approach holds great promise in fortifying cloud computing security. By proactively identifying and neutralizing malicious nano-structures, cloud service providers and users can significantly reduce the risk of data breaches, downtime, and cyberattacks.

Nonetheless, it is crucial to acknowledge that the field of cloud security is continually evolving, and so are the tactics employed by malicious actors. Therefore, ongoing research, development, and collaboration between the cybersecurity community and cloud computing experts are imperative to stay one step ahead of threats. In summary, this study highlights the potential of a hybrid machine learning approach as a pivotal tool in the ongoing battle to enhance cloud computing security and protect sensitive data from the ever-evolving landscape of threats posed by malicious nano-structures. By embracing innovative technologies and collaborative efforts, we can fortify our defenses and ensure the integrity and confidentiality of cloud-based systems.

Acknowledgments

This work was supported by Shahid Rajaee Teacher Training University under grant number 4951.

References

Castro Jorge, P., Simões, F.M.F. and Pinto da Costa, A. (2015), "Dynamics of beams on non-uniform nonlinear foundations subjected to moving loads", *Comput. Struct.*, **148**, 24-34. https://doi.org/10.1016/j.compstruc.2014.11.002

Gbadeyan, J.A. and Dada, M.S. (2011), "A comparison of dynamic responses of three versions of moving load problem involving elastic rectangular plates", *J. Vib. Control*, **17**, 903-915. https://doi.org/10.1177/1077546310377910

Chen, J.S. and Tsai, S.M. (2016), "Sandwich structures with periodic assemblies on elastic foundation under moving loads", *J. Vib. Control*, **22**, 2519-2529. https://doi.org/10.1177/1077546314548470

Daikh, A.A., Drai, A., Houari, M.S.A., Eltaher, M.A.J.S. and Structures, C. (2020), "Static analysis of multilayer nonlocal strain gradient nanobeam reinforced by carbon nanotubes", *Steel Compos. Struct.*, **36**(6), 643-656. https://doi.org/10.12989/scs.2020.36.6.643

Ding, L., Zhu, H.P. and Wu, L. (2016), "Effects of axial load and structural damping on wave propagation in periodic Timoshenko beams on elastic foundations under moving loads", *Phys. Lett. A*, **380**, 2335-2341. https://doi.org/10.1016/j.physleta.2016.05.023

Farrokhian, A. (2020a), "Buckling response of smart plates reinforced by nanoparticles utilizing analytical method", *Steel Compos. Struct.*, **35**(1), 1-12. https://doi.org/10.12989/scs.2020.35.1.001

Farrokhian, A. (2020b), "The effect of voltage and nanoparticles on the vibration of sandwich nanocomposite smart plates", *Steel Compos. Struct.*,, **34**(5), 733-742. https://doi.org/10.12989/scs.2020.34.5.733

Geem, Z.W., J.H. Kim, and G. Loganathan, (2002), "Harmony search optimization, application to pipe network design", *Int. J. Model. Simul.*, **22**(2), 125-133. https://doi.org/10.1080/02286203.2002.11442233

He, W.Y. and Zhu, S. (2016), "Moving load-induced response of damaged beam and its application in damage localization", *J. Vib. Control*, **22**, 3601-3617. https://doi.org/10.1177/1077546314564587

Kaur, T., Singh, A.K., Chattopadhyay, A. and Sharma, S.K. (2022), "Dynamic response of normal moving load on an irregular fiber-reinforced half-space", *J. Vib. Control*, **22**, 77-88. https://doi.org/10.1177/1077546314528525

Mirjalili, S., S.Z.M. Hashim, and H.M. Sardroudi, (2012), "Training feedforward neural networks using hybrid particle swarm optimization and gravitational search algorithm", *Appl. Math. Comput.*, **218**(22), 11125-11137. https://doi.org/10.1016/j.amc.2012.04.069

Najjar, M.F., Nehdi, M.L., Azabi, T.M., Soliman, A.M. (2017), "Fuzzy inference systems-based prediction of engineering properties of two-stage concrete", *Comput. Concr.*, **22**(2), 133-152. https://doi.org/10.12989/cac.2017.19.2.133

Omar, T., Nehdi, M.L. and Zayed, T. (2017), "Integrated condition rating model for reinforced concrete bridge decks", *Comput. Concr.*, **28**(5), 23-44. https://doi.org/10.12989/cac.2017.28.5.023

Omran, M.G. and M. Mahdavi, (2008), "Global-best harmony search", *Appl. Math. Comput.*, **198**(2), 643-656. https://doi.org/10.1016/j.amc.2007.09.004

Reddy, J.N. (1984), "A simple higher order theory for laminated composite plates", *J. Appl. Mech.*, **51**, 745-752. https://doi.org/10.1115/1.3167719

Suleiman, A.R. and Nehdi, M.L. (2017), "Modeling self-healing of concrete using hybrid genetic algorithm - artificial neural network", *Materials*, **15**(135), 88-91. https://doi.org/10.3390/ma10020135

Shu, C., Chew, Y.T. and Richards, E. (1995), "Generalized differential and integral quadrature and their application to solve boundary layer equations", *Int. J. Numeric. Meth. Fluids*, **21**, 723-733. https://doi.org/10.1002/fld.1650210903

Shahriar, A. and Nehdi, M.L. (2013), "Modeling rheological properties of oil well cement slurries using multiple regression analysis and artificial neural networks", *J. Mater. Sci.*, **5**(1), 126-144.

Simsek, M. and Kocatu¨rk, T., (2009), "Nonlinear dynamic analysis of an eccentrically prestressed damped beam under a concentrated moving harmonic load", *J. Sound Vib.*, **320**, 235-253. https://doi.org/10.1016/j.jsv.2008.07.012

Song, Q., Shi, J., Liu, Z. and Wan, Y. (2021), "Dynamic analysis of rectangular thin plates of arbitrary boundary conditions under moving loads", *Int. J. Mech. Sci.*, **117**, 16-29. https://doi.org/10.1016/j.ijmecsci.2016.08.005

Sudheesh Kumar, C.P., Sujath, C. and Shankar, K. (2015), "Vibration of simply supported beams under a single moving load, A detailed study of cancellation phenomenon", *Int. J. Mech. Sci.*, **99**, 40-47. https://doi.org/10.1016/j.ijmecsci.2015.05.001

Wang, D., Zhang, W. and Zhu, J. (2021), "A moving bounds strategy for the parameterization of geometric design variables in the simultaneous shape optimization of curved shell structures and openings", *Finite Elem. Anal. Des.*, **120**, 80-89. https://doi.org/10.1016/j.finel.2016.07.002

Wang, Y. and Wu, D. (2022), "Thermal effect on the dynamic response of axially functionally graded beam subjected to a moving harmonic load", *Acta Astronaut.*, **127**, 117-181. https://doi.org/10.1016/j.actaastro.2016.05.030

Yaseen, Z.M., Keshtegar, B., Hwang, H.J., Nehdi, M.L. (2019),

"Predicting reinforcing bar development length using polynomial chaos expansions", *Eng. Struct.*, **195**, 524-535. https://doi.org/10.1016/j.engstruct.2019.06.012

Yu, D., Wen, J., Shen, H. and Wen, X. (2012), "Propagation of steady-state vibration in periodic pipes conveying fluid on elastic foundations with external moving loads", *Phys. Lett. A*, **376**, 3417-3422. https://doi.org/10.1016/j.physleta.2012.09.041

CC