Cloud-Cyber Physical Systems: Enhanced Metaheuristics with Hierarchical Deep Learning-based Cyberattack Detection

Ahmad Taher Azar
College of Computer and Information Sciences, Prince Sultan University, Riyadh, Saudi Arabia | Automated Systems and Soft Computing Lab (ASSCL), Prince Sultan University, Riyadh, Saudi Arabia | Faculty of Computers and Artificial Intelligence, Benha University, Egypt
aazar@psu.edu.sa

Syed Umar Amin
Automated Systems and Soft Computing Lab (ASSCL), Prince Sultan University, Riyadh, Saudi Arabia | College of Computer and Information Sciences, Prince Sultan University, Riyadh, Saudi Arabia
samin@psu.edu.sa

Mohammed Abdul Majeed
Department of Cybersecurity and Cloud Computing Technical Engineering, Uruk University, Baghdad, Iraq
mmajeed91@uruk.edu.iq

Ahmed Al-Khayyat
College of Technical Engineering, The Islamic University of Najaf, Iraq | College of Technical Engineering, The Islamic University of Al Diwaniyah, Iraq | College of Technical Engineering, The Islamic University of Babylon, Iraq
ahmedalkhayyat85@gmail.com

Ibraheem Kasim Ibraheem
Department of Electrical Engineering, College of Engineering, University of Baghdad, Iraq
ibraheemki@coeng.uobaghdad.edu.iq (corresponding author)

Received: 3 July 2024 | Revised: 21 July 2024 | Accepted: 29 July 2024

ABSTRACT

Cyber-Physical Systems (CPS) integrate several interconnected physical processes, networking units, and computing resources, along with monitoring the processes of the computing system. The connection between the cyber and physical world creates threatening security problems, particularly with the growing complexities of transmission networks. Despite efforts to overcome this challenge, it remains challenging to analyze and detect cyber-physical attacks in CPS. This study mainly focuses on the development of Enhanced Metaheuristics with Hierarchical Deep Learning-based Attack Detection (EMHDL-AD) method in a cloud-based CPS environment. The proposed EMHDL-AD method identifies various types of attacks to protect CPS. In the initial stage, data preprocessing is implemented to convert the input dataset into a useful format. Then, the Quantum Harris Hawks Optimization (QHHO) algorithm is used for feature selection. An Improved Salp Swarm Algorithm (ISSA) is used to optimize the hyperparameters of the HDL technique to recognize several attacks. The performance of the EMHDL-AD algorithm was examined using two benchmark intrusion datasets, and the experimental results indicated improvements over other existing approaches.

Keywords-cyber-physical systems; hierarchical deep learning; attack detection; enhanced metaheuristics; feature selection

I. INTRODUCTION

Cyber-Physical Systems (CPS) exchange real-time data and information between physical and virtual systems [1]. CPS play a crucial role in the Internet of Things (IoT) related industries and have considerable financial potential. CPS are considered to be the communication of computing, physical, and network. They have progressed as an Internet of cyber-physical things, providing various services such as smart cities, e-commerce, smart homes, e-health, etc. [2]. Many industrial equipment is controlled wirelessly by implementing CPS, aiding in handling large and complicated industrial structures. Interconnected CPS elements are highly capable of remotely processing IoT-based objects, sensing the surroundings, and having the flexibility to alter processes at runtime with real-time computing [3]. A CPS can also be embedded in several schemes and used in different domains such as military, IT, healthcare, transport, etc. CPS enhance production efficiency and quality while exposing security problems. The transmission network acts as a connection between physical and information systems, which becomes a key to system security [4]. Attack detection of transmission networks can potentially maintain the privacy of the CPS structure. However, it is essential to consider the CPS features when setting up targeted attack detection approaches [5]. The continuous operation of CPS generates large network traffic datasets, increasing computation overhead. Software and networks are prone to attackers who try to infiltrate or damage CPS-based systems [6]. The executing process of control software in cyber systems is disrupted when attackers access the network or hold physical systems, causing failure or other manipulations [7]. Such assaults on CPS can cause havoc on industrialized equipment and processes.

In [8], Intrusion Detection Systems (IDSs) were studied, demonstrating the increased performance of Machine Learning (ML) methods [8]. Intrusion detection utilizes software and hardware to detect intrusions in networks. The deployment process of an established model allows for regulating security at the network level [9]. IDSs are of 2 types, host- and network-based. Online data have been employed to extract features for classification-based identification techniques [10]. ML techniques, which include unsupervised and supervised methods, in addition to Deep Learning (DL), are frequently used in ID systems. This study focuses primarily on the development of Enhanced Metaheuristics with a Hierarchical DL-based Attack Δetection (EMHDL-AD) approach in a cloud-based CPS environment. At first, data preprocessing was implemented to convert the input dataset into a useful format. The Quantum Harris Hawks Optimization (QHHO) algorithm was then used for Feature Selection (FS). Lastly, an Improved Salp Swarm Algorithm (ISSA) was used with the HDL classifier to detect attacks. The performance of the proposed EMHDL-AD method was examined using two benchmark datasets.

II. RELATED WORKS

Artificial intelligence is rapidly revolutionizing the world by improving efficiency, production, and decision-making across industries. It automates tedious processes, allowing people to focus on more strategic and creative work. Furthermore, its ability to rapidly and precisely evaluate large datasets drives advances in technology, healthcare, finance, and other fields [11-13]. AI can offer more personalized services, greater safety, and a smarter society with better infrastructure and quality of life. ML and DL are at the heart of these breakthroughs, with applications in healthcare, finance, retail, manufacturing, and beyond [14-17]. To greatly increase anomaly detection rates, improve industrial CPS performance, and resolve challenges, a knowledge distillation method was proposed in [18] based on a triplet CNN. A robust system loss function was considered during training to increase the training stability of the model, along with k-fold cross-validation to increase the performance of anomaly detection. In [19], an industrial CPS IDS was proposed based on the diffusion model (IDD). In [20], an ideal DBN-based distributed IDS (ODBN-IDSs) was presented to secure a CPS platform [20]. This study used a Binary Flower Pollination Algorithm (BFPA) to select features, which were then used in a DBN to detect intrusions. The hyperparameters of the DBN were fine-tuned using the Equilibrium Optimizer Algorithm (EOA). In [21], an AI-based Multi-Modal Fusion-based IDS (AIMMF-IDS) was proposed for industrial CPS, using an enhanced Fish Swarm Optimizer FS (IFSO-FS). Using the Levy Flight (LF) idea as the orthodox FSO process search method, this system could avoid getting stuck in local optima.

In [22], an IDS approach was presented based on cognitive computing to improve security in industrial CPS. Preprocessing was used to remove noise from the data. Next, a Binary Bacterial Foraging Optimizer (BBFO) was used for FS, and GRU was applied to detect intrusions. Lastly, the NADAM optimizer was used to fine-tune the hyperparameters of GRU and improve detection rates. In [23], a strong AD technique was devised based on a semi-supervised ML algorithm that enables near real-time attack detection. A DNN model was employed to detect anomalies based on reconstructed errors. In [24], DeepFed was proposed to detect cyber threats in CPS. A new DL-based identification model was designed for industrial CPS using a CNN and a GRU, and an FL structure was developed, building a complete detection method in a privacy-preserving way. DL and ML methods on cyber-physical attacks were investigated in [1, 5, 6, 9, 25-28], while works on intrusion detection in CPSs can be found in [3, 7, 8, 10, 29, 30]. In [31], a survey on security and privacy issues was presented. The application of swarm optimization algorithms in the detection of cyberattacks in cloud-cyber physical systems was studied in [28, 32-38]. Table I summarizes key studies.

TABLE I. SUMMARY OF KEY STUDIES REVIEWED

Study	Methodology	Findings
Forest-PA	Utilizes the forest algorithm with PA rules	Effective for certain types of attacks but prone to local optima
WISARD	Employs WISARD weightless neural network	Good initial results but lacks scalability
AE-RF	Combines autoencoder with random forest	Improved detection accuracy but suffers from low population diversity
LIB-SVM	Uses Support Vector Machine with LIBRARY optimizations	High accuracy with optimized hyperparameters but limited by static settings
FURIA	Fuzzy Unordered Rule Induction Algorithm	Flexible rule-based system but suboptimal feature selection

This study describes a novel cloud-based CPS intrusion detection method, called EMHDL-AD, to identify attacks on various platforms. Data preparation employs the QHHO method to select features. ISSA is used to optimize the hybrid deep-learning approach parameters for intrusion detection. Benchmark tests demonstrated that EMHDL-AD outperformed previous models in accuracy, recall, and F1 score, obtaining results up to 99.55%. The proposed approach showed better results with greater TRAC/VDAC but lower TRLS and VDLS. Most impressively, ISSA improved global search/classification performance while preventing local optima and increasing population diversity. This shows the potential of EMHDL-AD as a weapon against cyber attacks in CPS contexts, such as cloud-based systems.

III. MOTIVATION FOR EMHDL-AD

A. Limitations and Challenges of Existing Approaches

Existing approaches for attack detection on cloud-based CPS platforms, such as Forest-PA, WISARD, AE-RF, LIB-SVM, and FURIA models, exhibit several limitations that the proposed EMHDL-AD method aims to address:

- Local Optima Problem: Many traditional algorithms, such as Forest-PA and WISARD, often get trapped in local optima, reducing their effectiveness in finding the global optimum solution. EMHDL-AD incorporates chaotic sequences in the ISSA iterative mapping to enhance global search ability and avoid local optima.
- Population Diversity: Techniques such as AE-RF and LIB-SVM may suffer from low population diversity, which can limit their ability to effectively explore the search space. EMHDL-AD improves population diversity by using ISSA-based hyperparameter optimization, ensuring a more robust search process and better overall performance.
- Hyperparameter Optimization: Existing models like FURIA often rely on static or poorly optimized hyperparameters, which can limit their classification accuracy. EMHDL-AD employs ISSA for dynamic hyperparameter optimization, significantly enhancing attack detection performance.
- Feature Selection (FS): Many traditional methods do not efficiently select the most relevant features, leading to suboptimal performance. EMHDL-AD uses the QHHO algorithm for effective FS, which helps to identify the best subset of features for improved attack detection.
- Scalability: Traditional approaches may struggle with scalability when applied to large datasets. Advanced preprocessing and FS mechanisms ensure that it can handle large datasets more effectively.

By addressing these specific limitations and challenges, the proposed EMHDL-AD method offers a more robust and efficient solution for attack detection on cloud-based CPS platforms, showcasing superior performance compared to existing techniques.

B. Novelty and Contributions of EMHDL-AD

The proposed EMHDL-AD method introduces several novel contributions to the field of attack detection on cloud-based CPS platforms:

- Enhanced Population Diversity with ISSA: EMHDL-AD employs ISSA, which incorporates chaotic sequences into the iterative mapping process. This enhancement significantly improves global search ability and population diversity, preventing the algorithm from getting trapped in local optima.
- Dynamic Hyperparameter Optimization: Unlike existing methods that rely on static or poorly optimized hyperparameters, EMHDL-AD uses ISSA for dynamic hyperparameter optimization. This approach ensures that the hyperparameters are continuously optimized during the training process, leading to superior attack detection performance.
- Effective FS with QHHO: Integrating the QHHO algorithm for FS allows the method to efficiently identify the most relevant features, reducing data dimensionality and enhancing the accuracy and efficiency of the detection process.
- Scalability to Large Datasets: Advanced preprocessing and feature selection mechanisms ensure scalability when applied to large datasets. This ability is demonstrated by the EMHDL-AD method's performance on benchmark datasets such as CICIDS2017 and NSLKDD2015, where it exhibits superior detection results compared to existing approaches.
- Robust Performance Metrics: Comprehensive experimental results show that EMHDL-AD consistently outperformed traditional models, such as Forest-PA, WISARD, AE-RF, LIB-SVM, and FURIA, in terms of accuracy, precision, recall, and F1-score. This robust performance across various metrics highlights the efficacy of the proposed method in real-world attack detection scenarios.

C. Potential Impact and Real-World Applications of EMHDL-AD

The EMHDL-AD method has a significant potential impact and wide-ranging real-world applications in securing CPS environments. Some key areas of impact and application are:

- Industrial Control Systems (ICSs): The EMHDL-AD method can be applied to detect cyber-attacks in ICSs such as SCADA (Supervisory Control and Data Acquisition) and DCS (Distributed Control Systems). By ensuring real-time monitoring and detection of malicious activities, it helps prevent disruptions in critical infrastructure sectors such as power generation, water treatment, and manufacturing.
- Smart Grids: With the integration of advanced metering infrastructure and distributed energy resources, smart grids are highly susceptible to cyber-attacks. EMHDL-AD can enhance the security of smart grids by identifying and mitigating potential threats, ensuring the stability and reliability of the power supply.

- Healthcare Systems: The increasing adoption of CPS in healthcare, such as IoT-enabled medical devices and telemedicine platforms, requires robust security measures. EMHDL-AD can be employed to protect sensitive patient data and ensure the safe operation of medical devices, thus enhancing the overall security of healthcare systems.
- Transportation Systems: Modern transportation systems, including autonomous vehicles and intelligent transportation infrastructure, rely heavily on CPSs. EMHDL-AD can provide advanced threat detection capabilities to protect against cyber-attacks that could disrupt transportation services or compromise passenger safety.
- Smart Cities: As cities become smarter with the deployment of IoT devices and CPS for services such as traffic management, public safety, and utility management, EMHDL-AD can be instrumental in securing these systems against cyber threats, ensuring seamless and secure operation of smart city services.
- Cloud-Based CPS Platforms: EMHDL-AD is particularly suited for cloud-based CPS platforms, where scalability and efficient processing of large datasets are crucial. By providing robust attack detection mechanisms, it enhances the security of cloud-hosted CPS applications across various domains.

The practical relevance and importance of the EMHDL-AD method are underscored by its ability to provide a comprehensive and scalable solution to protect CPS environments against evolving cyber threats. This method not only improves detection accuracy and efficiency but also ensures the reliability and safety of critical systems in real-world applications.

IV. THE PROPOSED SYSTEM

This study proposes the EMHDL-AD method for cloud-based CPS platform attack detection consisting of four stages of operations, namely data preprocessing, QHHO-based FS, HDL-based attack detection, and ISSA-based hyperparameter optimization. Figure 1 represents the working process of the EMHDL-AD algorithm.

A. Data Preprocessing

Data preprocessing was performed to convert the input dataset into a useful format. The proposed method converts the input dataset to a suitable form using the min-max data normalization to scale feature ranges between 0 and 1.

$$v' = \frac{v - min_A}{max_A - min_A} \quad (1)$$

where min_A and max_A denote the maximum and minimum values of A and v and v' represent its original and normalized values.

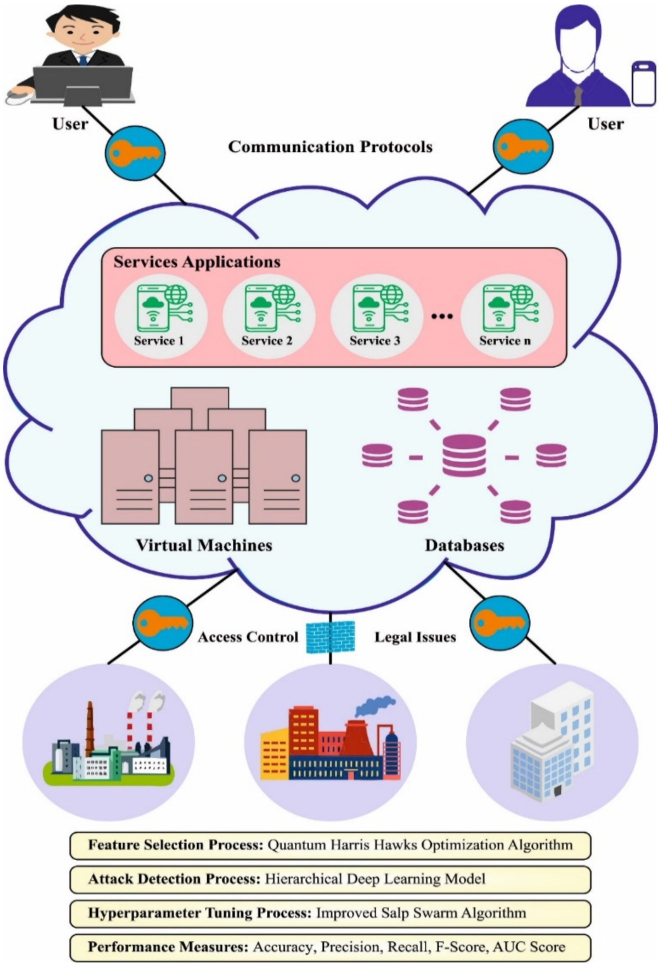
User
Communication Protocols
User
Services Applications
Service 1
Service 2
Service 3
Service n
Virtual Machines
Databases
Access Control
Legal Issues
Feature Selection Process: Quantum Harris Hawks Optimization Algorithm
Attack Detection Process: Hierarchical Deep Learning Model
Hyperparameter Tuning Process: Improved Salp Swarm Algorithm
Performance Measures: Accuracy, Precision, Recall, F-Score, AUC Score

Fig. 1. The overall process of EMHDL-AD.

B. Feature Selection Using the QHHO Algorithm

QHHO is used to generate the best feature subset. The hunting habits of Harris hawks are used to mimic the HHO algorithm [39]. HHO uses two distinct strategies, exploration and exploitation, to simulate cooperative hunting.

$$E = 2E_0\left(1 - \frac{t}{T}\right) \quad (2)$$

where E denotes the prey's escape energy, and HHO understands the transition from the exploration to the exploitation stage based on it. E_0 indicates the prey's fundamental energy state, which varies arbitrarily in $[-1, 1]$ at each iteration. The mathematical equation is $E_0 = 2 * rand - 1$, where $rand$ represents a uniformly distributed random integer in the range of zero and one, and t and T specify the existing and the maximum amount of iterations.

1) Exploration Phase

If $|E| \geq 1$, hawks enter the exploration stage. They might monitor and stalk prey with their companions, or they might randomly perch in tall trees in search of prey. Assume that the location choice can be made between the two following approaches with equivalent probability:

$$X_{t+1}^{i,j} = \begin{cases} X_t^{rand,j} - r_1|X_t^{rand,j} - 2r_2X_t^{i,j}| & q \geq 0.5 \\ (X_t^{prey,j} - X_t^{av,j}) - r_3[LB^j + r_4(UB^j - LB^j)] & q < 0.5 \end{cases} \tag{3}$$

where $X_t^{i,j}$ and $X_{t+1}^{i,j}$ denote the present location of the i^{th} hawk at the j^{th} parameter and the location at the following iteration, respectively, $i \in [1, N_{pop}]$, $j \in [1, Dim]$. N_{pop} indicates the overall amount of hawks, and Dim denotes the dimension of the respective problem. $X_t^{rand,j}$ and $X_t^{prey,j}$ denote the location of the hawk and the prey that are chosen randomly at the j^{th} variable, correspondingly. r_1, r_2, r_3, r_4, and q denote five dissimilar random integers ranging from zero to one. LB^j and UB^j indicate the lower and upper boundaries of the search range at the j^{th} parameter, and $X_t^{av,j}$ indicates the present average location of hawks at the j^{th} variable as follows:

$$X_t^{av,j} = \frac{1}{N_{pop}} \sum_{i=1}^{N} X_t^{i,j} \tag{4}$$

C. Exploitation Phase

If $|E| < 1$, then hawks are in the exploitation stage. Here, they perform a raid, hunting on the observed prey observed. However, in the hunting process, the prey tries to escape from the hunt. Hence, Harris hawk adopts various pursuit methods for the escaping behavior of the prey. HHO develops a four-hunting tactic for stimulating the hunting and chasing behaviors, which exploits the escape probability r and the escape energy E for determining which strategy to adopt. The integration of escape probability E and escape energy r in EMHDL-AD involves a synergistic approach that leverages both parameters to enhance the overall optimization strategy:

- Early stages: At the early stages of the optimization, high E and r values promote extensive exploration, allowing the algorithm to search a wide array of potential solutions. This phase is crucial for identifying diverse regions of the search space that may contain global optima.
- Middle stages: As the process continues, E and r are gradually adjusted based on the convergence rate and the quality of solutions. This adjustment ensures a balanced approach where the algorithm can still explore new solutions while beginning to exploit promising areas.
- Final stages: In the final stages, lower E and r values concentrate the search around the most promising solutions, ensuring thorough exploitation and fine-tuning. This phase is essential for achieving high precision and accuracy in the final solution.

By adopting this strategy, EMHDL-AD effectively balances exploration and exploitation, leading to improved performance in FS and cyberattack detection. The dynamic adjustment of E and r ensures that the optimization process is both comprehensive and efficient, ultimately enhancing the robustness and reliability of the proposed method.

If both $|E|$ and r are less than 0.5, the prey will have enough energy to hop away at random, but not before the hawks have surrounded it. The hawk now employs gentle besiege to successfully hunt by taking advantage of the prey's physical strength. This tactic may be represented mathematically using:

$$X_{t+1}^{i,j} = \Delta X_t^j - E \times \left|JumpX_t^{prey,j} - X_t^{i,j}\right| \tag{5}$$

$$\Delta X_t^j = X_t^{prey,j} - X_t^{i,j} \tag{6}$$

$$Jump = 2(1 - r_5) \tag{7}$$

where ΔX_t^j denotes the distance between the prey's present location at the j^{th} parameter and the existing location of the i^{th} hawks, r_5 shows the randomly produced number within $[0, 1]$, and $Jump$ signifies random jump concentration that differs randomly within $[0, 2]$ at every iteration.

If $|E| < 0.5$ and $r \geq 0.5$, then they don't have adequate energy to escape. The hawk has surrounded the prey and chooses a hard besiege and faster raid hunt. The process description of this strategy is given below:

$$X_{t+1}^{i,j} = X_t^{prey,j} - E \times \left|\Delta X_t^j\right| \tag{8}$$

If $|E| \geq 0.5$ and $r < 0.5$, the prey has enough energy to escape the siege and moves in a zigzag pattern. Now, the Harris hawk continues to consume the energy of the prey and establishes a complete encircle.

$$X_{t+1}^{i,j} = \begin{cases} Y_{t+1}^{i,j} \; if \; f(Y_{t+1}^{i,j}) < f(X_t^{i,j}) \\ Z_{t+1}^{i,j} \; if \; f(Z_{t+1}^{i,j}) < f(X_t^{i,j}) \end{cases} \tag{9}$$

$$Y_{t+1}^{i,j} = X_t^{prey,j} - E \times \left|IumpX_t^{prey,j} - X_t^{i,j}\right| \tag{10}$$

$$Z_{t+1}^{i,j} = Y_{t+1}^{i,j} + S^j \times L^j \tag{11}$$

$$L^j \sim LP(\mu^j, \nu^j, \beta^j) \tag{12}$$

where S^j denotes a random integer, and $LP(\cdot)$ indicates the Lévy flight function:

$$LP(u^j, \nu^j, \beta^j) = 0.01 \times \frac{u^j \times \sigma}{|\nu^j|^{\frac{1}{\beta i}}} \tag{13}$$

$$\sigma = \left(\frac{\Gamma(1+\beta) \times \sin\left(\frac{\pi\beta}{2}\right)}{\Gamma\left(\frac{1+\beta}{2}\right) \times \beta \times 2^{\left(\frac{\beta-1}{2}\right)}}\right)^{\frac{1}{\beta}} \tag{14}$$

where u and ν are random values within $(0, 1, u \sim N(0, \delta^2)$, $\nu \sim N(0,1))$ default $\beta = 1.5$.

If $|E| < 0.5$ and $r < 0.5$, then the prey does not have adequate energy to escape. However, the hawks don't fully encircle them. Hence, they select these strategies to shorten and accelerate the average location distance between them. This model can be expressed as follows:

$$X_{t+1}^{i,j} = \begin{cases} Y_{t+1}^{i,j} & if \; f(Y_{t+1}^{i,j}) < f(X_t^{i,j}) \\ Z_{t+1}^{i,j} & if \; f(Z_{t+1}^{i,j}) < f(X_t^{i,j}) \end{cases} \tag{15}$$

$$Y_{t+1}^{i,j} = X_t^{prey,j} - E \times \left|JumpX_t^{prey,j} - X_t^{av,j}\right| \tag{16}$$

$$Z_{t+1}^{i,j} = Y_{t+1}^{i,j} + S^j \times L^j \tag{17}$$

The QHHO technique can be derived using the quantum computing concept to increase the performance of the HHO technique. Quantum computing uses concepts of quantum mechanisms such as entanglement, quantum gate, and state superposition. The building block in quantum computation is a Q-bit that ranges within $|1>$, $|0>$, or superposition state $|0>$ and $|1>$. It is formulated by the incorporation of states $|0> and\ 1>$:

$$|Q>=\alpha|0>+\beta|1> \text{ such that } |\alpha|^2+|\beta|^2=1 \qquad (18)$$

where α and β are complex numbers.

A Fitness Function (FF) is used to balance the classification accuracy (maximal) attained and the FS counts (minimal) in every solution (minimal). Equation (19) represents the FF used to estimate the solution.

$$Fitness=\alpha\gamma_R(D)+\beta\frac{|R|}{|C|} \qquad (19)$$

where $\gamma_R(D)$ indicates the classification error rate, $|R|$ denotes the cardinality of the subset chosen, $|C|$ shows the total quantity of features in the given data, and α and β represent the two parameters respective to the importance of classification quality and subset length. $a\in[1,0]$ and $\beta=1-\alpha$.

D. Optimal HDL-based Attack Detection

ISSA with HDL was used for attack detection. BiLSTM encompasses forward and backward LSTM [40]. The backward and forward LSTM hidden layers are used for backward and forward feature extraction. BiLSTM considers the effect of all the attributes before and after the sequence dataset. Therefore, wide-ranging feature data can be attained. The state of BiLSTM at t time involves backward and forward outputs.

$$h_t^{forward}=LSTM^{forward}(h_{t-1},x_t,C_{t-1}) \qquad (20)$$

$$h_t^{backJ\psi ard}=LSTM^{backward}(h_{t-1},x_t,C_{t-1}) \qquad (21)$$

$$H_t=\left[h_t^{fomard},h_t^{bacMard}\right] \qquad (22)$$

BiLSTM and CNN are representatives of DL. CNN feature extraction works in the spatial dimension. BiLSTM can preserve the context of past data for a longer time and realize the extraction of data features. The study integrated CNN with Bi-LSTM to extract features and create a deep hierarchical network system.

Simultaneously, temporal and spatial features are extracted by generating a hierarchical network structure that integrates CNN with BiLSTM. Since BiLSTM and CNN inputs have various types, the spatial feature extracted was tuned to the output of CNN to fulfill the Bi-LSTM input. The input size is set to 64, and the time step is fixed to 2 while being fed as an input layer of the BiLSTM. The output of the fully connected layer of CNN is 1×128. Both layers of the BiLSTM unit implement temporal feature extraction. The initial hidden layer uses 128 neurons and the following uses 64. The sigmoid activation function is applied to implement the nonlinear operation. The outcome of every recursive operation of the Bi-LSTM is a combination of each current and the previous features. One fully connected layer was interconnected after the output layer of Bi-LSTM, the formerly extracted feature was incorporated, and the output value of the final fully connected layer was distributed to softmax for classification.

E. Hyperparameter Tuning

Lastly, ISSA was used to optimize the hyperparameter of the HDL technique to recognize several attacks. Salps live in groups of smaller pelagic gelatinous chordates critical for greenhouse gas supply to the ocean [41], and a billion clusters collectively form a group called a salp chain. SSA mimics the swarm behaviors of salps. The leader and followers have two different roles in the salp chain. The leader leads the whole population, whereas the follower follows consecutively. This leadership strategy can be represented by

$$x_j^1\begin{cases}F_j+c_1\left((ub_j-lb_j)c_2+lb_j\right) & c_3\geq 0.5\\ F_j-c_1\left((ub_j-lb_j)c_2+lb_j\right) & c_3\leq 0.5\end{cases} \qquad (23)$$

where X_j^1 denotes the j^{th} parameter of the leader, F_j specifies the food source, and ub_j and lb_j indicate the upper and lower boundaries from the $j^{\text{ th}}$ parameter. Moreover, $c_2\in[0,1]$, $c_3\in[0,1]$, and c_1 are the key parameters to maintain the balance. This is expressed as

$$c_1=2e^{-(\frac{4FEs}{\text{Max}\,FEs})^2} \qquad (24)$$

where FEs represents the existing amount of calculations and $MaxFEs$ denotes the maximal amount of calculations. The followers can be represented as

$$X_j^i=\frac{\left(x_j^{i-1}+x_j^i\right)}{2} \qquad (25)$$

SSA is a metaheuristic approach that implements random initialization and can mitigate local optima problems, enhance the diversity of the population, make the algorithm find the optimum solution more rapidly, and improve global search ability. Chaotic sequences have randomness and outstanding ergodicity. Furthermore, their pseudo-randomness provides stronger uniformity and is equally distributed all over the search space. Therefore, as a form of a chaotic graph, in ISSA, Iterative Mapping (IM) is used in the initial phase of SSA to generate random solutions to improve global search ability and population diversity to avoid local optima. The IM definition can be given by

$$X_{i+1}=sin\left(\frac{b\pi}{\chi}\right) \qquad (26)$$

where b is randomly generated within $[0,1]$. Figure 2 demonstrates the steps included in ISSA.

```
Algorithm 1: Salp Swarm Algorithm
$Np$: population size
Initialize the location of the population;
Calculate the fitness of all individuals;
Set the better agent as FoodPosition ($F$)
and the better fitness as FoodFitness;
While $FEs \leq MaxFEs$
  Evaluate $c_1$;
  For $i = 1{:}Np$
    If $i \leq Np/2$
```

```
        Arbitrarily compute $r_1$ and $r_{2;}$
        Evaluate the leader;
      Else if $i < Np + 1$ && $i > Np/2$
        Evaluate the followers;
      End if
    End for
    Compute if the individuals are beyond
    the upper and lower boundaries;
    Assess the fitness of the population;
    Upgrade FoodPosition (F) and
    FoodFitness;
  End while
  Return $F$
```

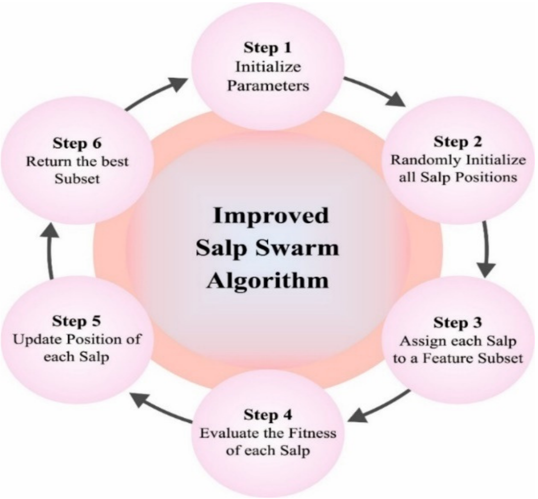
Step 1
Initialize Parameters
Step 2
Randomly Initialize all Salp Positions
Step 3
Assign each Salp to a Feature Subset
Step 4
Evaluate the Fitness of each Salp
Step 5
Update Position of each Salp
Step 6
Return the best Subset
Improved Salp Swarm Algorithm

Fig. 2. Steps involved in ISSA.

ISSA not only derives a fitness function to obtain a higher classification performance but also describes a positive integer to symbolize better outcomes for the solution candidate. The decline of the classifier error rate is taken as the fitness function.

$$fitness(x_i) = ClassifierErrorRate(x_i)$$
$$= \frac{number\ of\ misclassified\ samples}{Total\ number\ of\ samples} * 100 \qquad (27)$$

V. EXPERIMENTAL VALIDATION

The attack detection performance of the EMHDL-AD algorithm was examined using two datasets, as shown in Table I. The NSLKDD2015 dataset comprises 67,343 normal instances and 58,630 abnormal instances. Likewise, the CICIDS2017 dataset includes 50,000 normal and 50,000 abnormal instances.

TABLE II. DATASET DETAILS

Class	Number of Instances	
	NSLKDD 2015	CICIDS 2017
Normal	67343	50000
Anomaly	58630	50000
Total	**125973**	**100000**

Figure 3 and Table II show the attack detection results on the NSLKDD2015 dataset. The experimental results indicate that EMHDL-AD achieved enhanced performance in all aspects. On the total dataset, the EMHDL-AD approach attained average $accu_{bal}$ of 99.51%, $prec_n$ of 99.50%, $reca_l$ of 99.51%, F_{score} of 99.51%, and AUC_{score} of 99.51%. Meanwhile, on 70% of the training set (TR), EMHDL-AD achieved average $accu_{bal}$ of 99.49%, $prec_n$ of 99.49%, $reca_l$ of 99.49%, F_{score} of 99.49%, and AUC_{score} of 99.49%. On 30% of the test set (TS), EMHDL-AD achieved an average $accu_{bal}$ of 99.55%, $prec_n$ of 99.55%, $reca_l$ of 99.55%, F_{score} of 99.55%, and AUC_{score} of 99.55%. Figure 4 shows the EMHDL-AD approach's training accuracy (TRAC) and validation accuracy (VDAC) on the same dataset. Due to the higher TRAC and VDAC values, the results indicate that EMHDL-AD provides a better solution. Figure 5 shows the training loss (TRLS) and validation loss (VDLS) of EMHDL-AD on the same dataset, indicating how the proposed method achieves superior results with reduced TRLS and VDLS values. Figure 6 shows a clear precision-recall (PR) assessment of the proposed method on the NSLKDD2015, indicating PR values that were at their maximum across all classes.

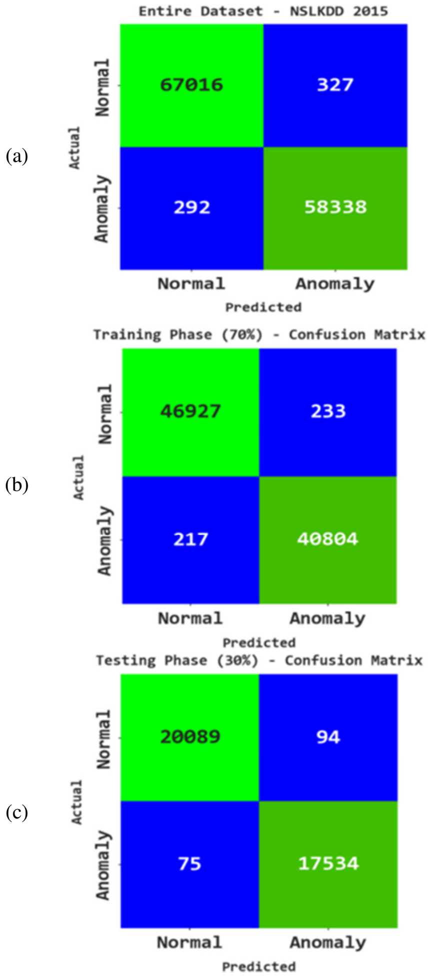

Fig. 3. Confusion matrices of EMHDL-AD on NSLKDD2015: (a) Entire, (b) 70% of TR set, and (c) 30% of TS set.

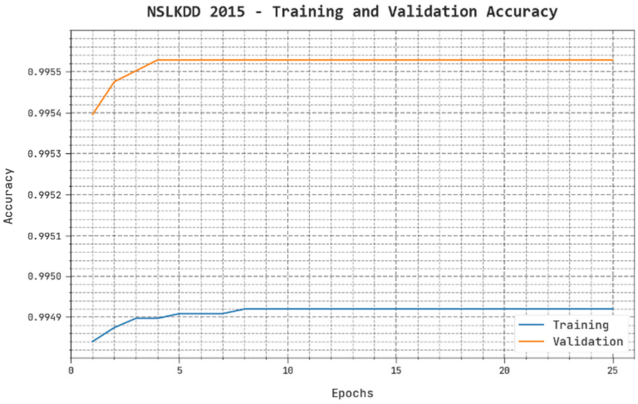

Fig. 4. EMHDL-AD results for TRAC and VDAC on NSLKDD2015.

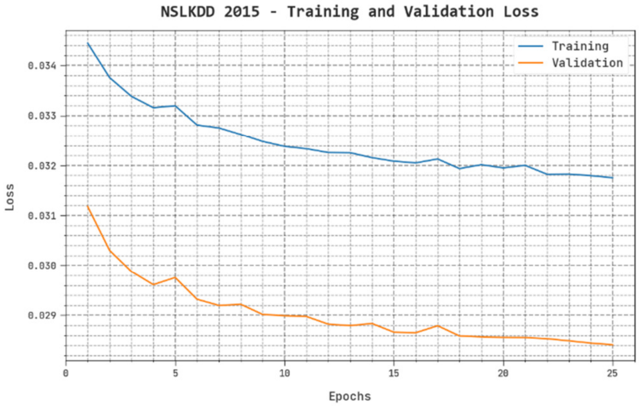

Fig. 5. EMHDL-AD results for TRLS and VDLS on NSLKDD2015.

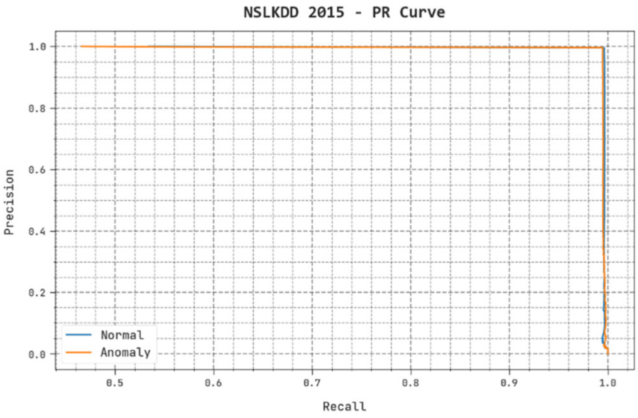

Fig. 6. PR analysis of EMHDL-AD on the NSLKDD2015.

Figure 7 shows the attack detection results achieved on the CICIDS2017 dataset. The confusion matrices show that the EMHDL-AD algorithm correctly recognized the normal and anomaly instances on the CICIDS2017 dataset. Table IV shows the EMHDL-AD method's classification results on the CICIDS2017 dataset, indicating that it performed better in all aspects. On the total database, EMHDL-AD accomplished average $accu_{bal}$ of 99.21%, $prec_n$ of 99.21%, $reca_l$ of 99.21%, F_{score} of 99.21%, and AUC_{score} of 99.21%. Meanwhile, on 70% of the TR set, EMHDL-AD attained average $accu_{bal}$ of 99.18%, $prec_n$ of 99.18%, $reca_l$ of 99.18%, F_{score} of 99.18%, and AUC_{score} of 99.18%. Furthermore, on 30% of the TS set, EMHDL-AD accomplished average $accu_{bal}$ of 99.27%, $prec_n$ of 99.27%, $reca_l$ of 99.27%, F_{score} of 99.27%, and AUC_{score} of 99.27%.

TABLE III. EMHDL-AD RESULTS ON NSLKDD2015

Class	$Accu_y$	$Prec_n$	$Reca_l$	F_{score}	AUC_{score}
Entire Dataset					
Normal	99.51	99.57	99.51	99.54	99.51
Anomaly	99.50	99.44	99.50	99.47	99.51
Average	**99.51**	**99.50**	**99.51**	**99.51**	**99.51**
Training Phase (70%)					
Normal	99.51	99.54	99.51	99.52	99.49
Anomaly	99.47	99.43	99.47	99.45	99.49
Average	**99.49**	**99.49**	**99.49**	**99.49**	**99.49**
Testing Phase (30%)					
Normal	99.53	99.63	99.53	99.58	99.55
Anomaly	99.57	99.47	99.57	99.52	99.55
Average	**99.55**	**99.55**	**99.55**	**99.55**	**99.55**

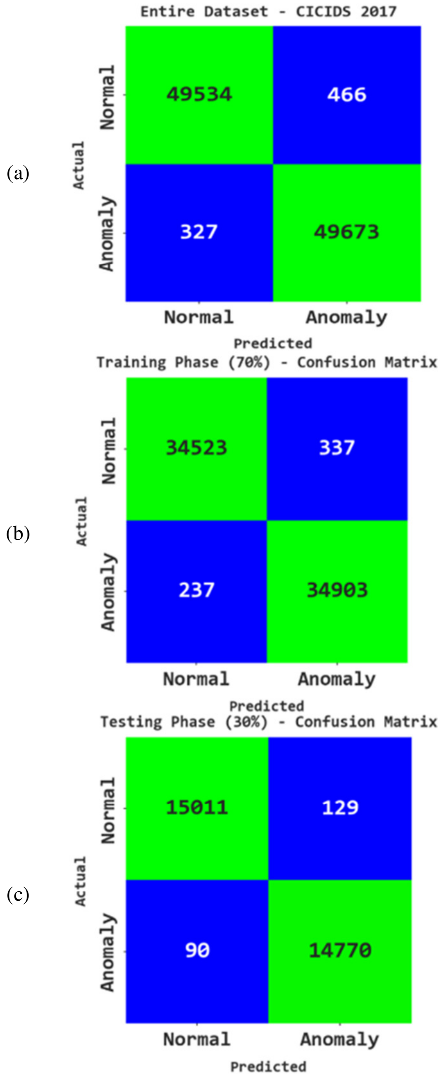

Fig. 7. Confusion matrices of EMHDL-AD on CICIDS2017: (a) Entire, (b) 70% of TR set, and (c) 30% of TS set.

TABLE IV. EMHDL-AD RESULTS ON CICIDS2017

Class	$Accu_y$	$Prec_n$	$Reca_n$	F_{score}	AUC_{score}
Entire Dataset					
Normal	99.07	99.34	99.07	99.21	99.21
Anomaly	99.35	99.07	99.35	99.21	99.21
Average	**99.21**	**99.21**	**99.21**	**99.21**	**99.21**
Training Phase (70%)					
Normal	99.03	99.32	99.03	99.18	99.18
Anomaly	99.33	99.04	99.33	99.18	99.18
Average	**99.18**	**99.18**	**99.18**	**99.18**	**99.18**
Testing Phase (30%)					
Normal	99.15	99.40	99.15	99.28	99.27
Anomaly	99.39	99.13	99.39	99.26	99.27
Average	**99.27**	**99.27**	**99.27**	**99.27**	**99.27**

Figure 8 describes the TRAC and VDAC of EMHDL-AD on CICIDS2017, showing high values. Figure 9 shows the TRLS and VDLS of the EMHDL-AD method on the same dataset, indicating higher performance with reduced TRLS and VDLS values. Figure 10 shows a clear PR examination of the proposed approach on the same dataset, showing increased PR values for the two classes.

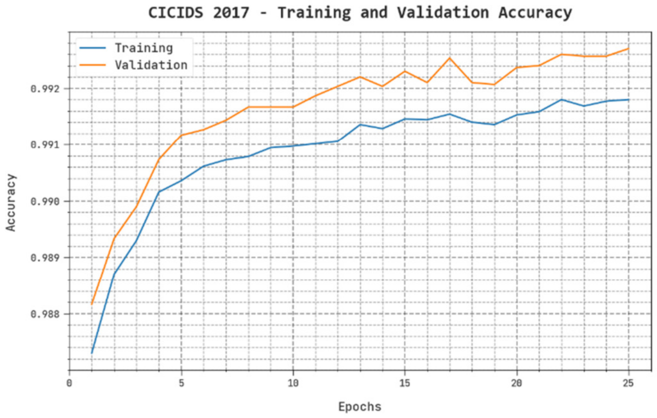

Fig. 8. TRAC and VDAC results of EMHDL-AD on CICIDS2017.

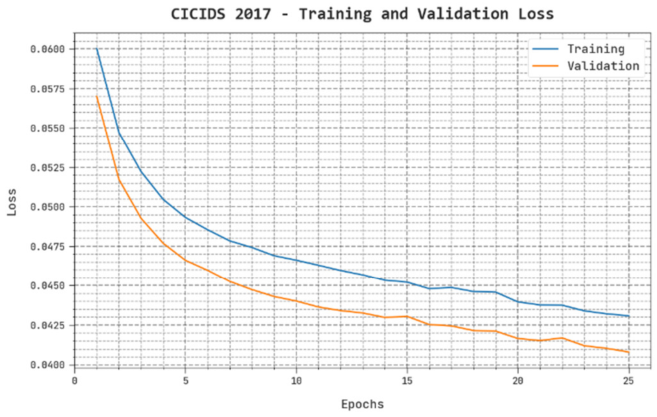

Fig. 9. TRLS and VDLS results of EMHDL-AD on CICIDS2017.

The superior performance of EMHDL-AD can be illustrated by the comparison in Table IV and Figure 11 [42]. This comparison shows the least efficiency of the Forest-PA and WISARD techniques. The AE-RF, LIB-SVM, and FURIA models achieve reasonably closer attack detection results. However, EMHDL-AD achieved superior outcomes over existing techniques with maximum $prec_n$ of 99.55%, $reca_l$ of 99.55%, $accu_y$ of 99.55%, and $F1_{score}$ of 99.55%.

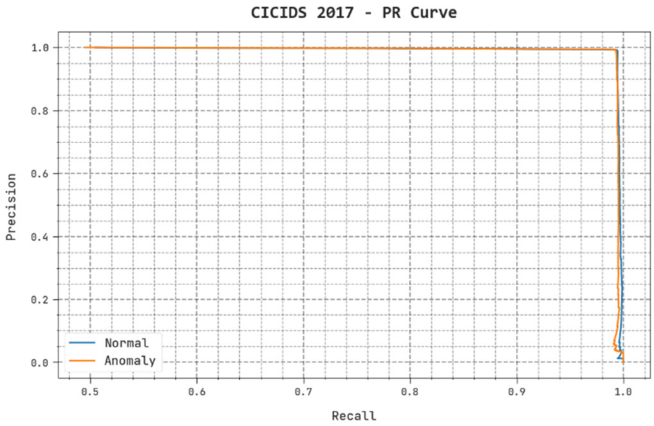

Fig. 10. PR results of EMHDL-AD on CICIDS2017.

TABLE V. COMPARISON OF EMHDL-AD WITH OTHER RECENT METHODS

Methods	$Prec_n$	$Reca_l$	$Accu_y$	$F1_{score}$
EMHDL-AD	99.55	99.55	99.55	99.55
FURIA Model	97.51	97.35	99.21	98.95
GSAE Model	96.69	99.48	97.93	97.45
AE-RF Model	97.59	98.92	97.43	97.85
LIB-SVM Model	97.53	98.09	97.21	98.15
Forest-PA Model	97.75	97.06	96.47	98.61
WISARD Model	97.39	96.95	96.09	99.48

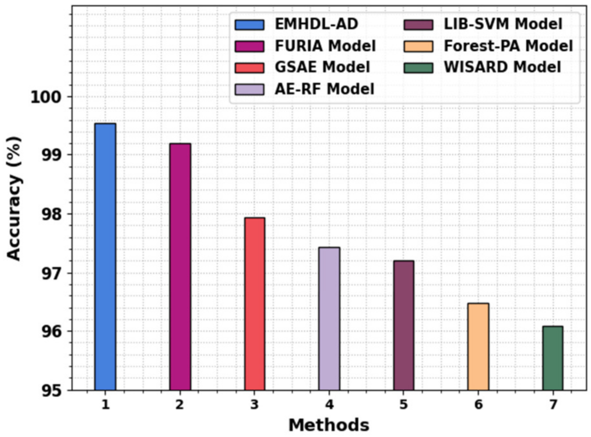

Fig. 11. $Accu_y$ comparison of EMHDL-AD with other recent techniques.

VI. FUTURE TRENDS AND RESEARCH DIRECTIONS IN CPS SECURITY

The field of CPS security is rapidly evolving, driven by the increasing integration of CPSs into various sectors and the corresponding increase in cyber threats. Future research on CPS security is expected to focus on several key areas:

- AI and ML: The application of AI and ML techniques for real-time threat detection and response will continue to be a major trend. Advances in DL, reinforcement learning, and anomaly detection will enhance the capability of CPSs to autonomously detect and mitigate threats.

- Blockchain Technology: Blockchain offers a decentralized and tamperproof solution to secure data transactions in CPSs. Future research will likely explore the integration of blockchain with CPS to ensure data integrity, authentication, and secure communication.
- Quantum Computing: As quantum computing becomes more accessible, its impact on CPS security will be significant. Research should focus on developing quantum-resistant cryptographic algorithms and leveraging quantum computing for enhanced security measures.
- Edge and Fog Computing: The shift towards edge and fog computing in CPS aims to reduce latency and improve real-time processing. Future research should address the security challenges associated with decentralized data processing and develop robust security frameworks for such computing environments.
- IoT Security: The proliferation of IoT devices within CPS requires comprehensive security solutions. Future trends should involve the development of lightweight encryption algorithms, secure boot mechanisms, and robust device authentication protocols.
- Standardization and Policy Development: As CPSs become more ubiquitous, the need for standardized security protocols and policies will grow. Research should focus on creating universally accepted security standards and guidelines to ensure consistent protection across different CPS implementations.
- Human Factors and Usability: Understanding human factors in CPS security, including user behavior, awareness, and training, is crucial. Research should aim to develop user-friendly security mechanisms that do not compromise usability while ensuring robust protection.
- Cross-Domain Security Solutions: CPSs are often part of larger, interconnected systems spanning multiple domains (e.g., smart cities, healthcare, transportation). Future research should focus on developing cross-domain security solutions that provide holistic protection for integrated CPS environments.

These emerging trends and research directions will shape the future of CPS security, ensuring that systems remain resilient against evolving cyber threats while maintaining operational efficiency and reliability.

VII. CONCLUSION

This study proposed the EMHDL-AD method for securing cloud-based CPS. The proposed method combines data preprocessing, QHHO for FS, and ISSA with a hierarchical DL classifier for effective cyberattack detection. The proposed EMHDL-AD method was evaluated using two benchmark intrusion datasets, and the results demonstrated significant improvements over existing approaches. The method achieved high accuracy, precision, recall, and F1-score, indicating its robustness and effectiveness in detecting various types of cyberattacks. Despite the promising results, the study has certain limitations:

- Dataset Diversity: Evaluation was carried out using specific benchmark datasets, which may not cover all possible attack scenarios. Future research should include a broader range of datasets to validate the method's generalizability.
- Computational Complexity: The proposed method involves complex computations for FS and hyperparameter optimization, which can result in increased processing time and resource consumption. Optimizing the computational efficiency of the method is a potential area for future work.
- Real-world Deployment: The method was tested in a controlled experimental environment. Real-world deployment may present additional challenges, such as handling noisy data, adapting to evolving attack patterns, and integrating with existing security infrastructure.

The findings of this study have several important implications for the security of CPS:

- Enhanced Security Measures: The improved detection capabilities of the EMHDL-AD method can significantly enhance the security of CPS in various domains, including industrial control systems, smart grids, healthcare systems, and smart cities.
- Adaptive Detection: The dynamic hyperparameter optimization and effective FS mechanisms make the method adaptable to different attack types, ensuring robust and reliable security in CPS environments.
- Scalability: The method's ability to handle large datasets efficiently makes it suitable for deployment in cloud-based CPS platforms, where scalability is crucial.

Future research should focus on addressing the identified limitations and exploring the following areas:

- Expand Dataset Coverage: Incorporate more diverse datasets to test the method's performance across different attack scenarios and CPS environments.
- Optimize Computational Efficiency: Develop techniques to reduce computational complexity and improve processing speed.
- Real-world Applications: Implement and test the proposed method in real-world CPS environments to evaluate its practical applicability and effectiveness.

In conclusion, the EMHDL-AD method presents a promising approach to enhance the security of cloud-based CPS, offering robust detection capabilities and adaptability to various attack scenarios. Continued research and development in this domain could further strengthen the security and reliability of CPS in the face of evolving cyber threats.

ACKNOWLEDGMENTS

This paper is derived from a research grant funded by the Research, Development, and Innovation Authority (RDIA) - Kingdom of Saudi Arabia - with grant number (13382-psu-2023-PSNU-R-3-1-EI-). The authors would like to thank Prince Sultan University, Riyadh, Saudi Arabia, for support with the article processing charges (APC) of this publication. The authors specially acknowledge the Automated Systems and Soft Computing Lab (ASSCL) at Prince Sultan University, Riyadh, Saudi Arabia.

REFERENCES

[1] A. Presekal, A. Ştefanov, V. S. Rajkumar, and P. Palensky, "Attack Graph Model for Cyber-Physical Power Systems Using Hybrid Deep Learning," *IEEE Transactions on Smart Grid*, vol. 14, no. 5, pp. 4007–4020, Sep. 2023, https://doi.org/10.1109/TSG.2023.3237011.

[2] K. Bitirgen and Ü. B. Filik, "A hybrid deep learning model for discrimination of physical disturbance and cyber-attack detection in smart grid," *International Journal of Critical Infrastructure Protection*, vol. 40, Mar. 2023, Art. no. 100582, https://doi.org/10.1016/j.ijcip.2022.100582.

[3] A. E. Ibor, O. B. Okunoye, F. A. Oladeji, and K. A. Abdulsalam, "Novel Hybrid Model for Intrusion Prediction on Cyber Physical Systems' Communication Networks based on Bio-inspired Deep Neural Network Structure," *Journal of Information Security and Applications*, vol. 65, Mar. 2022, Art. no. 103107, https://doi.org/10.1016/j.jisa.2021.103107.

[4] B. Cassottana, M. M. Roomi, D. Mashima, and G. Sansavini, "Resilience analysis of cyber-physical systems: A review of models and methods," *Risk Analysis*, vol. 43, no. 11, pp. 2359–2379, 2023, https://doi.org/10.1111/risa.14089.

[5] V. Ravi, R. Chaganti, and M. Alazab, "Recurrent deep learning-based feature fusion ensemble meta-classifier approach for intelligent network intrusion detection system," *Computers and Electrical Engineering*, vol. 102, Sep. 2022, Art. no. 108156, https://doi.org/10.1016/j.compeleceng.2022.108156.

[6] J. Zhang, L. Pan, Q. L. Han, C. Chen, S. Wen, and Y. Xiang, "Deep Learning Based Attack Detection for Cyber-Physical System Cybersecurity: A Survey," *IEEE/CAA Journal of Automatica Sinica*, vol. 9, no. 3, pp. 377–391, Mar. 2022, https://doi.org/10.1109/JAS.2021.1004261.

[7] H. Mittal, A. K. Tripathi, A. C. Pandey, M. D. Alshehri, M. Saraswat, and R. Pal, "A new intrusion detection method for cyber–physical system in emerging industrial IoT," *Computer Communications*, vol. 190, pp. 24–35, Jun. 2022, https://doi.org/10.1016/j.comcom.2022.04.004.

[8] S. Thakur, A. Chakraborty, R. De, N. Kumar, and R. Sarkar, "Intrusion detection in cyber-physical systems using a generic and domain specific deep autoencoder model," *Computers & Electrical Engineering*, vol. 91, May 2021, Art. no. 107044, https://doi.org/10.1016/j.compeleceng.2021.107044.

[9] C. Comert *et al.*, "Secure Design of Cyber-Physical Systems at the Radio Frequency Level: Machine and Deep Learning-Driven Approaches, Challenges and Opportunities," in *Artificial Intelligence for Cyber-Physical Systems Hardening*, I. Traore, I. Woungang, and S. Saad, Eds. Cham, Switzerland: Springer International Publishing, 2023, pp. 123–154.

[10] R. Colelli, F. Magri, S. Panzieri, and F. Pascucci, "Anomaly-Based Intrusion Detection System for Cyber-Physical System Security," in *2021 29th Mediterranean Conference on Control and Automation (MED)*, Puglia, Italy, Jun. 2021, pp. 428–434, https://doi.org/10.1109/MED51440.2021.9480182.

[11] A. M. Anter, A. T. Azar, A. E. Hassanien, N. El-Bendary, and M. A. ElSoud, "Automatic computer aided segmentation for liver and hepatic lesions using hybrid segmentations techniques," in *2013 Federated Conference on Computer Science and Information Systems*, Krakow, Poland, 2013, pp. 193–198.

[12] A. Rehman, T. Saba, U. Tariq, and N. Ayesha, "Deep Learning-Based COVID-19 Detection Using CT and X-Ray Images: Current Analytics and Comparisons," *IT Professional*, vol. 23, no. 3, pp. 63–68, May 2021, https://doi.org/10.1109/MITP.2020.3036820.

[13] G. Atteia *et al.*, "Adaptive Dynamic Dipper Throated Optimization for Feature Selection in Medical Data," *Computers, Materials & Continua*, vol. 75, no. 1, pp. 1883–1900, 2023, https://doi.org/10.32604/cmc.2023.031723.

[14] A. Rehman, T. Sadad, T. Saba, A. Hussain, and U. Tariq, "Real-Time Diagnosis System of COVID-19 Using X-Ray Images and Deep Learning," *IT Professional*, vol. 23, no. 4, pp. 57–62, Jul. 2021, https://doi.org/10.1109/MITP.2020.3042379.

[15] E. Emary, H. M. Zawbaa, A. E. Hassanien, G. Schaefer, and A. T. Azar, "Retinal vessel segmentation based on possibilistic fuzzy c-means clustering optimised with cuckoo search," in *2014 International Joint Conference on Neural Networks (IJCNN)*, Beijing, China, Jul. 2014, pp. 1792–1796, https://doi.org/10.1109/IJCNN.2014.6889932.

[16] T. Saba, M. A. Khan, A. Rehman, and S. L. Marie-Sainte, "Region Extraction and Classification of Skin Cancer: A Heterogeneous framework of Deep CNN Features Fusion and Reduction," *Journal of Medical Systems*, vol. 43, no. 9, Jul. 2019, Art. no. 289, https://doi.org/10.1007/s10916-019-1413-3.

[17] E. Emary, H. M. Zawbaa, A. E. Hassanien, G. Schaefer, and A. T. Azar, "Retinal blood vessel segmentation using bee colony optimisation and pattern search," in *2014 International Joint Conference on Neural Networks (IJCNN)*, Beijing, China, Jul. 2014, pp. 1001–1006, https://doi.org/10.1109/IJCNN.2014.6889856.

[18] Z. Wang, Z. Li, D. He, and S. Chan, "A lightweight approach for network intrusion detection in industrial cyber-physical systems based on knowledge distillation and deep metric learning," *Expert Systems with Applications*, vol. 206, Nov. 2022, Art. no. 117671, https://doi.org/10.1016/j.eswa.2022.117671.

[19] B. Tang, Y. Lu, Q. Li, Y. Bai, J. Yu, and X. Yu, "A Diffusion Model Based on Network Intrusion Detection Method for Industrial Cyber-Physical Systems," *Sensors*, vol. 23, no. 3, Jan. 2023, Art. no. 1141, https://doi.org/10.3390/s23031141.

[20] P. Ramadevi, K. N. Baluprithviraj, V. Ayyem Pillai, and K. Subramaniam, "Deep Learning Based Distributed Intrusion Detection in Secure Cyber Physical Systems," *Intelligent Automation & Soft Computing*, vol. 34, no. 3, pp. 2067–2081, 2022, https://doi.org/10.32604/iasc.2022.026377.

[21] M. A. Alohali, F. N. Al-Wesabi, A. M. Hilal, S. Goel, D. Gupta, and A. Khanna, "Artificial intelligence enabled intrusion detection systems for cognitive cyber-physical systems in industry 4.0 environment," *Cognitive Neurodynamics*, vol. 16, no. 5, pp. 1045–1057, Oct. 2022, https://doi.org/10.1007/s11571-022-09780-8.

[22] M. M. Althobaiti, K. Pradeep Mohan Kumar, D. Gupta, S. Kumar, and R. F. Mansour, "An intelligent cognitive computing based intrusion detection for industrial cyber-physical systems," *Measurement*, vol. 186, Dec. 2021, Art. no. 110145, https://doi.org/10.1016/j.measurement.2021.110145.

[23] A. K. Dutta, R. Negi, and S. K. Shukla, "Robust Multivariate Anomaly-Based Intrusion Detection System for Cyber-Physical Systems," in *Cyber Security Cryptography and Machine Learning*, Be'er Sheva, Israel, 2021, pp. 86–93, https://doi.org/10.1007/978-3-030-78086-9_6.

[24] B. Li, Y. Wu, J. Song, R. Lu, T. Li, and L. Zhao, "DeepFed: Federated Deep Learning for Intrusion Detection in Industrial Cyber–Physical Systems," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 8, pp. 5615–5624, Aug. 2021, https://doi.org/10.1109/TII.2020.3023430.

[25] K. Bitirgen and Ü. B. Filik, "A hybrid deep learning model for discrimination of physical disturbance and cyber-attack detection in smart grid," *International Journal of Critical Infrastructure Protection*, vol. 40, Mar. 2023, Art. no. 100582, https://doi.org/10.1016/j.ijcip.2022.100582.

[26] M. A. Alsheikh, S. Lin, D. Niyato, and H.-P. Tan, "Machine Learning in Wireless Sensor Networks: Algorithms, Strategies, and Applications," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 4, pp. 1996–2018, 2014, https://doi.org/10.1109/COMST.2014.2320099.

[27] G. Luo, "A review of automatic selection methods for machine learning algorithms and hyper-parameter values," *Network Modeling Analysis in Health Informatics and Bioinformatics*, vol. 5, no. 1, May 2016, Art. no. 18, https://doi.org/10.1007/s13721-016-0125-6.

[28] A. L. Buczak and E. Guven, "A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 2, pp. 1153–1176, 2016, https://doi.org/10.1109/COMST.2015.2494502.

[29] H. J. Liao, C. H. Richard Lin, Y. C. Lin, and K. Y. Tung, "Intrusion detection system: A comprehensive review," *Journal of Network and Computer Applications*, vol. 36, no. 1, pp. 16–24, Jan. 2013, https://doi.org/10.1016/j.jnca.2012.09.004.

[30] R. Doriguzzi-Corin, S. Millar, S. Scott-Hayward, J. Martinez-del-Rincon, and D. Siracusa, "Lucid: A Practical, Lightweight Deep Learning Solution for DDoS Attack Detection," *IEEE Transactions on Network and Service Management*, vol. 17, no. 2, pp. 876–889, Jun. 2020, https://doi.org/10.1109/TNSM.2020.2971776.

[31] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A Survey on Security and Privacy Issues in Internet-of-Things," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1250–1258, Oct. 2017, https://doi.org/10.1109/JIOT.2017.2694844.

[32] M. Schranz *et al.*, "Swarm Intelligence and cyber-physical systems: Concepts, challenges and future trends," *Swarm and Evolutionary Computation*, vol. 60, Feb. 2021, Art. no. 100762, https://doi.org/10.1016/j.swevo.2020.100762.

[33] M. H. Nasir, S. A. Khan, M. M. Khan, and M. Fatima, "Swarm Intelligence inspired Intrusion Detection Systems — A systematic literature review," *Computer Networks*, vol. 205, Mar. 2022, Art. no. 108708, https://doi.org/10.1016/j.comnet.2021.108708.

[34] M. Devarajan, N. S. Fatima, S. Vairavasundaram, and L. Ravi, "Swarm intelligence clustering ensemble based point of interest recommendation for social cyber-physical systems," *Journal of Intelligent & Fuzzy Systems*, vol. 36, no. 5, pp. 4349–4360, Jan. 2019, https://doi.org/10.3233/JIFS-169991.

[35] B. Acharya, S. Panda, and N. K. Ray, "Multiprocessor Task Scheduling Optimization for Cyber-Physical System Using an Improved Salp Swarm Optimization Algorithm," *SN Computer Science*, vol. 5, no. 1, Jan. 2024, Art. no. 184, https://doi.org/10.1007/s42979-023-02517-2.

[36] N. Yi, J. Xu, L. Yan, and L. Huang, "Task optimization and scheduling of distributed cyber–physical system based on improved ant colony algorithm," *Future Generation Computer Systems*, vol. 109, pp. 134–148, Aug. 2020, https://doi.org/10.1016/j.future.2020.03.051.

[37] M. H. Almusawy, "Improved Arithmetic Optimization with Deep Learning Driven Traffic Congestion Control for Intelligent Transportation Systems in Smart Cities," *Journal of Smart Internet of Things*, vol. 2022, no. 1, pp. 81–96, Dec. 2022, https://doi.org/10.2478/jsiot-2022-0006.

[38] A. Sinha, P. Jha, B. Kumar, A. Mishra, V. Ujjwal, and A. Singh, "Blockchain-Based Smart Home Network Security through ML," *Journal of Smart Internet of Things*, vol. 2022, no. 1, pp. 1–9, Dec. 2022, https://doi.org/10.2478/jsiot-2022-0001.

[39] Y. Sun, Q. Huang, T. Liu, Y. Cheng, and Y. Li, "Multi-Strategy Enhanced Harris Hawks Optimization for Global Optimization and Deep Learning-Based Channel Estimation Problems," *Mathematics*, vol. 11, no. 2, 2023, https://doi.org/10.3390/math11020390.

[40] K. Jiang, W. Wang, A. Wang, and H. Wu, "Network Intrusion Detection Combined Hybrid Sampling With Deep Hierarchical Network," *IEEE Access*, vol. 8, pp. 32464–32476, 2020, https://doi.org/10.1109/ACCESS.2020.2973730.

[41] S. Hao *et al.*, "Salp swarm algorithm with iterative mapping and local escaping for multi-level threshold image segmentation: a skin cancer dermoscopic case study," *Journal of Computational Design and Engineering*, vol. 10, no. 2, pp. 655–693, Mar. 2023, https://doi.org/10.1093/jcde/qwad006.

[42] M. A. Duhayyim *et al.*, "Evolutionary-Based Deep Stacked Autoencoder for Intrusion Detection in a Cloud-Based Cyber-Physical System," *Applied Sciences*, vol. 12, no. 14, 2022, https://doi.org/10.3390/app12146875.