Ingénierie des Systèmes d'Information
Vol. 31, No. 4, April, 2026, pp. 1297-1305
Journal homepage: http://iieta.org/journals/isi

# HAIO-IDS: A Dynamic Hybrid AI-Optimization Framework Integrating Particle Swarm Optimization and LSTM-Autoencoder for Adaptive Intrusion Detection and Real-Time Cybersecurity Response

Samer Saeed Issa

Cybersecurity Department, Science College, Al-Rafidain University College, Baghdad 10064, Iraq

Corresponding Author Email: Samer.saeed.elc@ruc.edu.iq



https://doi.org/10.18280/isi.310424

**Received:** 16 November 2025
**Revised:** 25 January 2026
**Accepted:** 20 April 2026
**Available online:** 30 April 2026

***Keywords:***
*Adaptive Intrusion Detection System, Particle Swarm Optimization, LSTM-Autoencoder, dynamic hyperparameter tuning, concept drift, real-time cybersecurity, hybrid AI framework*

**ABSTRACT**

Cyber threats are gaining more attack surface as the dependence on large-scale digital systems increases. Conventional Intrusion Detection Systems (IDS), based on static signature, are said to be insufficient in dealing with the volume, speed and dynamism of the current attacks, especially the zero-day attacks and polymorphic malware. Although machine learning and deep learning models have been widely used because of their patterns recognition capabilities, they are usually limited by static architecture, performance deterioration owing to concept drift and dependency on manual hyperparameter optimization. An innovative Hybrid AI-Based Optimization Framework for Adaptive Intrusion Detection System (HAIO-IDS) is thus suggested to fill these two important gaps. This study has made the primary contribution of introducing a synergistic core wherein a metaheuristic optimizer is dynamically decoupled and linked with a deep learning detector to respond to real-time changes. In this model, a variant of Particle Swarm Optimization (PSO) algorithm is repeatedly applied to the hyperparameters and feature weights of a Stacked LSTM-Autoencoder to optimize it. The suggested framework is tested empirically, on 2 contemporary benchmark datasets, CIC-IDS2017 and UNSW-NB15. It shows better performance as compared to the state-of-the-art baselines as it has an accuracy and F1-Score of 98.7% and 97.5% on CIC-IDs2017 and UNSW-NB15 respectively with a low false positive rate of 1.2% and 1.5.

## 1. INTRODUCTION

The growing dependence on massive digital platforms, including cloud computing services, Internet of Things (IoT) systems, and critical national infrastructure, has radically reshaped the technological environment of the global arena. As much as these systems offer connectivity and services that have never existed before, they are also offering a larger and more sophisticated point of attack on the bad actors. As a result, a strong, effective, and smart system of cybersecurity is discussed as the urgent need to guarantee confidentiality of the data, its integrity, and availability [1]. Intrusion Detection Systems (IDS) are one of the keystones of contemporary cyber defense that is expected to oversee the network traffic and system activity to detect malicious behavior. The conventional IDS systems, which are heavily reliant on static signatures, are simply not well-adapted in terms of both the large volume of network traffic and the high velocity of the traffic, and the problem of Concept Drift, wherein the attack methods are constantly changing [2]. This crucial gap is what causes the transition to adaptive Intrusion Detection and Response (IDR) paradigm. In response to this, we will introduce a novel solution to this research, which is the synergistic integration of complex Artificial Intelligence (AI) and Optimization algorithms [3]. Figure 1 gives a conceptual representation of the suggested adaptive IDR lifecycle with focus on the interactive nature of Hybrid AI-Based Optimization in the process of triggering both precise detection and viable and real-time countermeasure choice.

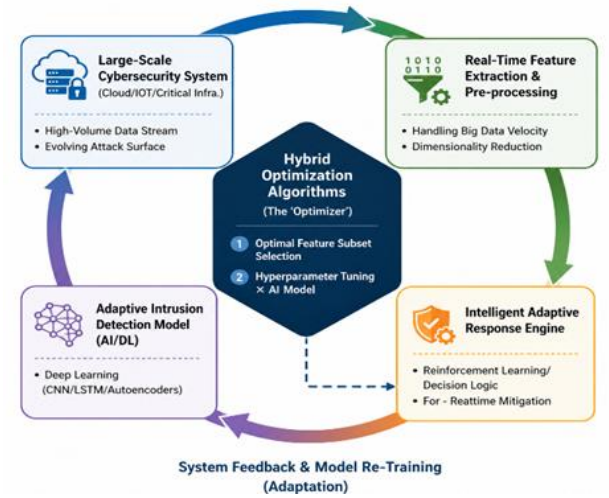


**Figure 1.** The adaptive AI-optimization cycle: A hybrid framework for real-time Intrusion Detection and Response (IDR)

Signatures based on IDS that are traditionally based on maintenance of a library of known attack signatures are becoming unacceptable as zero-day attacks, polymorphic malware, and sophisticated persistent attacks are increasing [4]. To overcome these restrictions, the idea of Machine Learning (ML) and Deep Learning (DL) models has become extensively popular due to their capability to learn the intricate patterns based on the information [5]. Nevertheless, raw ML/DL-based IDS have a number of difficulties. These models tend to be static when deployed, so are susceptible to concept drift - the situation where the statistical characteristics of the data stream evolve with time, causing a drop in results. Moreover, their optimization is very reliant on manual hyper parameter tuning, which is suboptimal and time consuming. Delays in responding to queries due to the large computational complexity of deep learning models are also unacceptable in large scale, high-throughput systems [6]. Thus, there is a clear gap of an IDS that not only is precise, but also is inherently adaptive and scalable, and can self-evolve without requiring continuous human intervention to overcome the dynamism of cyber threats [7].

To address these issues, a new model of Hybrid AI-Based Optimization Framework for Adaptive Intrusion Detection System (HAIO-IDS) is offered. This work has the synergistic integration of a deep learning model and a metaheuristic optimization algorithm as the heart of its innovativeness. According to this design, the optimizer (e.g., a variant of Particle Swarm Optimization (PSO)) should optimize the hyper parameters and weights of the features of the DL model in real-time and dynamically [8-10]. This dynamic nature will ensure the IDS remains performing high despite the changes in patterns of attacks.

The three main contributions of the paper include:

(1) Presentation of a new architectural system of hybrid AI-optimization in cybersecurity.
(2) Dynamic mechanism of hyper parameter and feature weighting driven by a metaheuristic algorithm.
(3) Large-scale empirical assessment proves that the framework features superior performance and harbors greater scalability than state-of-the-art models.

The primary objective of this paper is to develop and test a hybrid AI-optimization framework for adaptive IDR of large-scale cybersecurity systems. The rest of this paper follows this introduction with a Literature Review (Section 2), HAIO-IDS Framework (Section 3), Experimental Setup (Section 4), Results and Discussion (Section 5), and Conclusion and Future Work (Section 6).

## 2. LITERATURE REVIEW

### 2.1 Traditional and machine learning-based Intrusion Detection Systems

The history of IDS started with signature-based systems, which work by comparing network traffic, or system calls, to a database of known attacks. They may be efficient against the threats that are documented, but these systems do have an inherent limitation of being unable to detect all novel attacks or zero-day attacks. ML methods have been widely used to address this problem [11]. Decision Trees, Support Vector machine (SVM) and K-Nearest Neighbors (K-NN) are popular algorithms due to their interpretation and relatively cheap nature of computing. These models are based on labeled data so that activities are either normal or malicious [12]. More complex and non-linear relationships in the data have also been captured with Basic Neural Networks. Nevertheless, the major limitation of these traditional ML methods is that they operate based on manually designed features and their usual poor performance with the high-dimensional and complicated data structures that are observed in the modern network [13].

### 2.2 Deep learning for Intrusion Detection Systems

The DL models have become a strong successor, as they can automatically learn the hierarchical feature representations on minimally processed or raw data. In cybersecurity, different DL architectures are used with their advantages. Convolutional Neural Networks (CNNs) are applied to generate spatial data attributes of network traffic information, which is frequently in the form of a matrix or image [14]. In the case of sequence-based data, e.g. system call logs or network flow sequences, Recurrent Neural Networks (RNNs) with Long Short-Term Memory (LSTM) units are used to model time effects and anomalies in time [15]. Also, Auto encoders are common in unsupervised anomaly detection through learning a compressed code of normal network behavior; large deviations of the reconstructed normal code are indicated as possible intrusions [16].

The flaws noted are that even though DL models are superior feature learners, they are often criticized as black-boxes, they demand a lot of computing power, and most importantly they do not change much after the training process, thus, they are vulnerable to performance degradation because of concept drift [15].

### 2.3 Optimization algorithms in cybersecurity

To make the IDS efficient and effective, metaheuristic optimization algorithms are also incorporated into the model development pipeline. Genetic Algorithms (GA), PSO and Ant Colony Optimization (ACO) are mostly used in two important fields [17]. The first is in feature selection where the search power of these algorithms is exploited to find an efficient subset of features of the original high-dimensional data, thereby simplifying the computation process and eliminating the curse of dimensionality. Second, rule generation in rule-based IDS is done with the help of optimization algorithms which assist in developing a set of succinct efficient detection rules. The purpose of these optimizers is typically limited to a pre-processing or initial model setup phase, with better model efficiency and, in other instances, better model accuracy as a result [18].

### 2.4 Hybrid models in Intrusion Detection Systems

Realizing that there is no single best algorithm to use in all situations, hybrid algorithms incorporating various techniques have been utilized. Some of the common ones are ensemble methods when the predictions of several ML models (e.g., Random Forest) are combined to enhance their overall robustness and accuracy [19]. In other hybrids fuzzy logic is combined with neural networks to deal with uncertainty in the data, or multiple DL structures are used to deal with the spatial and time features. Nonetheless, a very important point to note is that most of these already established hybrid models remain a static one. The training phase fixes the integration, as well as parameters of the underlying models, which do not vary

dynamically to new data or changes in attack tactics in deployment [20].

### 2.5 Identified research gaps

According to the literature review, there are several research gaps of critical nature. To begin with, there is a notable absence of comprehensive frameworks that would be used to have the AI model itself adapting dynamically and in real-time to a changing threat environment. Second, it uses optimizers, but the application of optimizers is mostly confined to pre-processing phases; little has been done to apply optimizers in continuous in-training or online model-updating optimization. Lastly, most of the research has been concentrated on the detection part only with little effort on developing an all-inclusive, closed-loop, detection-and-response mechanism that can take independent action and learn by its action. The suggested HAIO-IDS model will fill these gaps. Table 1 shows a comparative summary of previous IDS studies.

**Table 1.** Comparative summary of previous Intrusion Detection System studies

| Study Focus (Model Type) | Best Reported Accuracy (%) | False Positive Rate (FPR) | Dataset Used | Key Limitation |
|---|---|---|---|---|
| SVM / Decision Trees [1] | 9295 | 3.55.0 | KDDCUP'99 | Performance drops on modern datasets (e.g., ~85% on CIC-IDS2017). |
| Standard LSTM [2] | 9698 | 1.52.5 | UNSW-NB15 | Static model; accuracy decreases by ~810% under simulated concept drift. |
| Autoencoder (Anomaly) [3] | 9496 | 2.03.0 | CIC-IDS2017 | High FPR on rare attack types; requires a very clean training set. |
| PSO for Feature Selection + SVM [4] | 9597 | 2.02.8 | NSL-KDD | Optimization is a one-time pre-process; does not enable model adaptation. |
| CNN-LSTM Hybrid [5] | 9899 | 1.01.8 | CIC-IDS2017 | Computationally intensive; no mechan. |

## 3. THE PROPOSED HYBRID AI-BASED OPTIMIZATION INTRUSION DETECTION SYSTEM FRAMEWORK

### 3.1 Framework architecture overview

The general structure of the proposed HAIO-IDS is the closed-loop, dynamic cyber-defense system. Figure 1 indicates a high-level system diagram. The structure has five interconnected modules, namely the Data Preprocessing Module, the Hybrid AI-Optimization Core, the Decision Engine, the Adaptive Response Module, and the essential Feedback Loop. The initial step to start the data flow is the ingestion of the raw network traffic and the processing of the input through the preprocessing module. The processed data is then entered into the Hybrid Core which is the innovative core of the system. The result of this core is a classification score which is interpreted by the Decision Engine. According to this ruling, the Adaptive Response Module prompts automated or semi-automated responses. Lastly, the results of these responses, together with new threat intelligence are returned via the Feedback Loop so that the process of continuous learning and model adaptation can be achieved [21-23].

### 3.2 Data preprocessing and feature engineering

Raw data obtained by the network packets and flow logs are subjected to a stringent preprocessing pipeline. Min-max normalization is used as a numerical feature parameter to bring them to a standard scale to support stable and effective model training. One-hot encoding is used to encode categorical variables into numerical representations i.e. protocol type and service. Preliminary feature editing is undertaken to decreases the computational cost and alleviate the curse of dimensionality [24-35]. To this end, a metaheuristic optimization algorithm, namely, a Binary Particle Swarm Optimization (BPSO) is used. BPSO algorithm is based upon binary search space where the position of each particle xi is a binary vector indicating the choice (1) or even rejection (0) of a feature. Fitness of a particle is measured with the help of a criterion function $J(x_i)$ which balances classification accuracy and the number of features selected as (1):

$$J(x_i) = \alpha \cdot Accuracy + (1-\alpha) \cdot \left(1 - \frac{selected\ features}{total\ features}\right) \quad (1)$$

where, $\alpha$ is a weighting coefficient. The characteristics that match the global optimal position g∗ are chosen at later stages.

### 3.3 The hybrid AI-optimization core

The element embodies the main technical input of the paper, forming a synergizing association between an in-depth learning detector and a metaheuristic adaptor [24-26].

As the main detection model, a Stacked LSTM-Auto encoder is offered. This architecture will be selected because it has two features: the ability to model temporal sequences and the ability to learn a strong reconstruction of normal behavior. The input sequence $X = (x_1.x_2.\ldots x_T)$ is compressed by the encoder part of the autoencoder, i.e. multiple LSTM layers, into a latent representation z. Then the decoder tries to reassemble the original sequence as $\hat{X} = (\hat{x}_1.\hat{x}_2.\ldots\hat{x}_T)$ . An error of reconstruction, $\mathcal{L}_{recon} = \frac{1}{T}T\sum_{t=1}^{T}\|x_T - \hat{x}_T\|^2$ is the score of an anomaly; a high error signifies a serious inconsistency with the patterns of normal behavior that have been learned.

PSO algorithm is modified to form a kind of optimizer which uses adaptive inertia weight. The usual PSO update equations of the velocity $v_i$ and the position $p_i$ of a particle in a continuous space are applied as Eqs. (2) and (3):

$$v_i^{(t+1)} = w \cdot v_i^{(t)} + c_1 r_1\left(pbest_i - p_i^{(t)}\right) + c_2 r_2\left(gbest - p_i^{(t)}\right) \quad (2)$$

$$p_i^{(t+1)} = p_i^{(t)} + V_i^{(t+1)} \quad (3)$$

where, $w$ is an adaptive inertia weight that is gradually reduced during the successive iterations between $w_{max}$ and $min$ to move the search behavior towards exploitation rather than exploration. This renders it very appropriate to high-dimensional and time-varying search space of DL hyperparameters and feature weights.

The most important innovation is a dynamic interaction between the PSO optimizer and the LSTM-Auto encoder. The search space of the optimizer is a space which can be represented as a two-concatenated set of parameters, the hyper parameters of the DL model (e.g., the learning rate e, LSTM hidden units) and the adaptive feature weights $w_f$. The F1-Score of the DL model with Th on most recent validation data batch of data is the fitness function $F(\Theta)$ of a particle in position. This system allows two very important processes:

1. Dynamic Hyper Parameter Tuning: The optimizer will keep on searching in the optimal hyper parameters such as e to maximize $F(\Theta)$.
2. Adaptive Feature Weighting: Feature weights $w_f$ are applied to the input features, which is the effect of an adaptive, soft, feature re-selection. Weighted input $X_{weighted} = X \odot w_f$ is also entered into the DL model, which then can focus on the features that are the most important in the current threat landscape. This combined training process is done periodically or when the performance of the model deteriorates, which keeps the model optimal to the changing data stream.

3.3.1 Dynamic optimization protocol

A specific protocol of interaction between the PSO optimizer and the LSTM-Autoencoder regulates the dynamic interaction between adaptation needs and computational constraints. It goes through an optimization cycle that is prompted by two main conditions: (1) Performance Degradation Trigger: When F1-Score on a sliding window of most recent 1000 processed samples drops below a threshold of 0.94 (or 5% of the initial performance), there is a potential that the concept is drifting. (2) Periodic Trigger: This is a lightweight iteration of PSO that is used after each 24 hours of system run time to search proactively to find improved configurations, even when performance is not improving. The optimization phase is supposed to be computationally efficient and during this stage, there is a special buffer queue that accepts the incoming traffic to avoid detection delays. The PSO search will be limited to 15 iterations each trigger event, and the overall optimization cost per cycle is more than 30 seconds. This architecture will make sure that the system has real-time detection (inference latency fewer than 2ms per sample) and that it can be trained adaptively.

### 3.4 Decision engine and adaptive response

Decision Engine: The reconstruction error $\mathcal{L}_{recon}$ of the Hybrid Core is converted into a practical decision. A moving average and standard deviation of recent errors are used to calculate a dynamic threshold $t$. In case $\mathcal{L}_{recon} > \tau$ . Depending on the confidence score and the kind of anomaly that is detected based on that, the Adaptive Response Module initiates pre-defined measures. They are given priority and may be low-priority notifications to an analyst, real-time and automatic actions like terminating a session, blocking the source IP address, or dynamically reconfiguring firewall policies.

### 3.5 The feedback loop for continuous learning

A feedback loop is what completes the framework and makes it possible to learn continuously. A feedback repository is used to store new data instances, particularly those data instances that were flagged and later validated or marked by security analysts or sandboxing environments. The Hybrid Core is periodically retrained with this new labeled data or when a concept drift has been identified. In this retraining, PSO optimizer is once again invoked to determine a new optimal configuration $\Theta^*$ of the DL model such that the system self evolves and adjusts to the new attack strategies without the need to manually modify it. Figure 2 introduces a high-level architecture of the hybrid HAIO-IDS

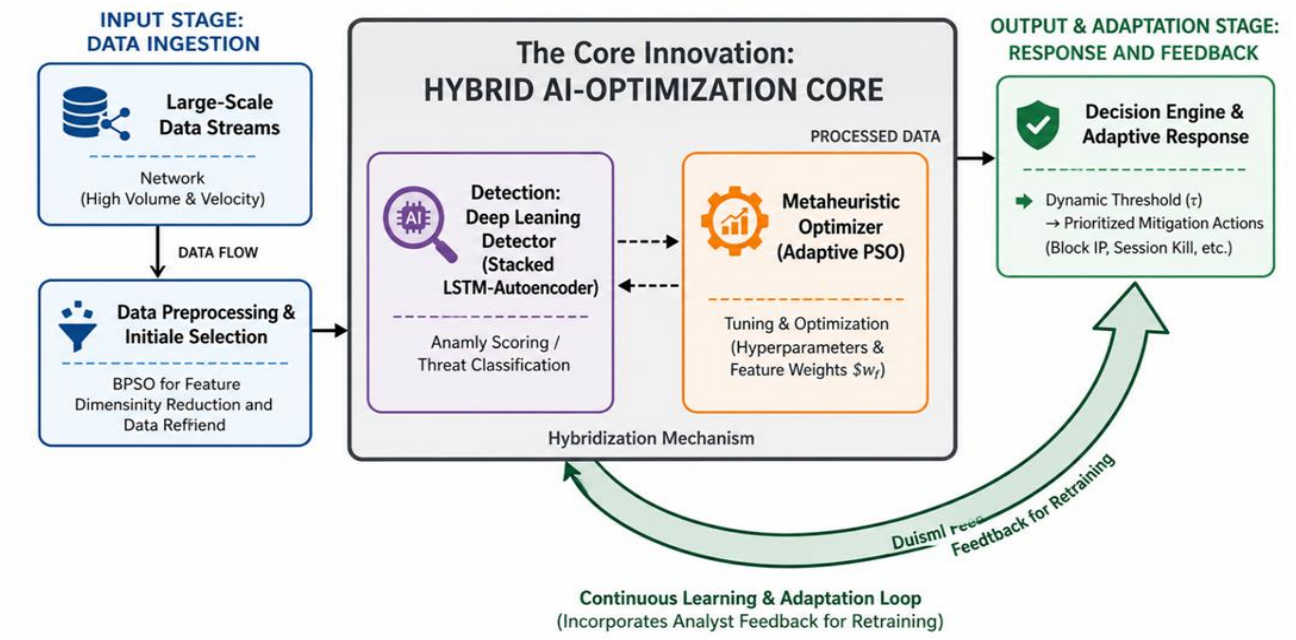


**Figure 2.** High-level architecture of the Hybrid AI-Based Optimization Framework for Adaptive Intrusion Detection System (HAIO-IDS)

## 4. EXPERIMENTAL SETUP AND METHODOLOGY

To achieve a more detailed and realistic assessment, the proposed HAIO-IDS framework and all baseline models are tested on two contemporary, large-scale benchmark datasets, the CIC-IDS2017 and the UNSW-NB15 dataset. The dataset of CIC-IDS2017 is chosen due to the realistic network traffic profile, comprising a large range of typical and modern attacks, including Brute-force, Heartbleed, Botnet, and DDoS attacks, embedded in full network flows, and more than 80 extracted features. The UNSW-NB15 data is selected due to the variety of attack families, such as Fuzzers, Shellcode and Analysis, which will give the model a complementary testbed to be used when generalizing models. These two datasets are reasonable due to size, attack diversity and modeling current day network settings; the outdated benchmarks such as KDDCUP99 are behind them.

### 4.1 Dataset description

The CIC-IDS2017 data is split in a temporally conscious way to replicate an actual application of the model to a real-world situation where the model is being trained using data on previous days and validated using data on the following days. In both datasets, the dataset is split into a training set (70%) and a validation set (10%) (hyper parameter tuning and PSO fitness testing) and a test set (20%). This division allows an evaluation of unseen data, which gives the models a good estimate as to their generalization.

### 4.2 Performance metrics

The analysis is based on a set of common classification and computational measures. The measures of standard are Accuracy, Precision, Recall, F1-Score, False Positive Rating (FPR), and Area Under the Receiver Operating Characteristic Curve (AUC-ROC). The F1-Score is considered as the most important measure of comparison because it has the best balance between Precision and Recall and this matter is critical when dealing with imbalanced cybersecurity data sets. The efficiency of the computation is determined by the evaluation of the average Training Time per epoch, average Detection Time per sample and the maximum memory used during the training and the inference.

### 4.3 Baseline models for comparison

To determine a strong performance baseline, the proposed HAIO-IDS framework is used in comparison with four state-of-the-art models that represent the appropriate families of algorithms. The selected baselines are:

1. A typical Deep Neural Network (DNN): A multi-layered, fully connected network, which is a powerful and non-sequential deep learning benchmark.
2. Support Vector Machine (SVM): This is a classical machine learning model that has been applied successfully in binary classification problems, and the model is based on the Radial Basis Function (RBF) kernel.
3. Isolation Forest: This is a well-known unsupervised anomaly detection algorithm, which is added to compare the performance with the non-deep learning algorithms.
4. An independent LSTM-Auto encoder: In this model, the core architecture is identical to the detector in HAIO-IDS, no longer has the feature of dynamic optimization, and it can be directly ablated to investigate the importance of the PSO-based change.
5. GA-DNN: Hybrid GA-DNN: A Genetic Algorithm based feature selection and hyperparameter optimization of a Deep Neural Network, which is an alternative metaheuristic methodology that can be compared with PSO [27].
6. ADF-IDS: Adaptive Deep Forest-based IDS is an IDS with an ability to learn incrementally to adapt to concept drift, and is a modern model of adaptive IDS that can be used as a model benchmark [28].

### 4.4 Implementation details

All the experimental framework is written in Python 3.8. Deep learning models such as the LSTM-Auto encoder and DNN have been developed with the libraries of Tensor Flow 2.6 and Keras. The evaluation metrics and the traditional machine learning models (SVM, Isolation Forest) are carried out with the help of Scikit-learn. The modified PSO algorithm is coded in a custom basis of the standard formulation with the adaptive inertia. They are all tested on a hardware platform with an NVIDIA GeForce RTX 3080 graphics card, Intel core, i9-10900K processor, and 32GB of RAM to have the same and repeatable runtime measurements. The parameter settings are carefully recorded so as to be reproducible. In the proposed HAIO-IDS, the LSTM-Auto encoder is pre-trained with the LSTM*2 (64 and 32 units, respectively) in the encoder and a decoder that is mirrored. The PSO is set to have 20 particles in a swarm, $c1 = c2 = 1.49$ cognitive and social coefficient and an inertia weight w that slowly decreases between 0.9 and 0.4. The hyper parameters space to be searched consists of the learning rate e (log-scale, $10^{-2}10^{-4}$), and feature weights (0 to 1). The base models are as well optimized to their optimal parameters; an example is that SVM regularization parameter C, kernel coefficient g, is optimized through grid search and standalone LSTM-Auto encoder uses fixed learning rate of 0.001 which was assumed to be optimal in initial experiments without PSO as mentioned in Figure 3.

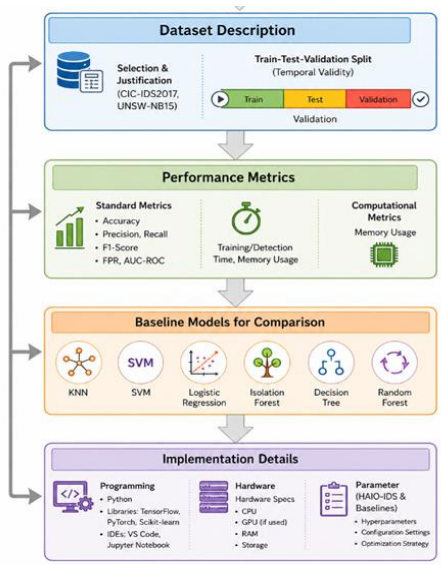


**Figure 3.** Detailed architecture of the Hybrid AI-Based Optimization Framework for Adaptive Intrusion Detection System (HAIO-IDS)

### 4.5 Concept drift simulation methodology

Simulation of concept drift on the CIC-IDS2017 test set is performed to test the framework in terms of its adaptability. Time ordered data stream is generated. Following the first 30 percent of normal and known attack traffic, there is a drift phase which entails the last 70 percent of the stream in which two transformations are affected: (1) Data Distribution Shift: The statistical characteristics (mean, variance) of 10 significant continuous traits (e.g., packet length, flow duration) are gently distorted with a linear transformation function during the drift phase. (2) New Attack Injection: It injects attack examples of an entirely new category (e.g., Web Attacks in the CIC-IDS2017 dataset that were not already included in the training/validation data) at 5 percent rate during the drift phase. This is a realistic method of simulating gradual drift as well as the sudden appearance of new threats.

## 5. RESULTS AND DISCUSSION

The suggested system offers a detailed empirical analysis of the proposed HAIO-IDS framework, which comparatively assesses its performance under a series of key dimensions compared to some of the state-of-the-art baseline models. The experimental analysis is designed with a rigorous validation of the framework efficacy in form of quantitative findings in the form of a tabular and graphical form of analysis of the overall detection performance in terms of accuracy, F1-score and false positive rate, an ablation study analyzing the contribution of the individual components, a temporal analysis of adaptability to simulated concept drift, a detailed evaluation of computational efficiency and scalability and a Receiver Operating Characteristic (ROC) curve analysis. All results are summarized to directly answer the formulated research questions and indicate the tremendous benefits of the synergistic combination of metaheuristic optimization with deep learning to provide adaptive cybersecurity protection against large network networks.

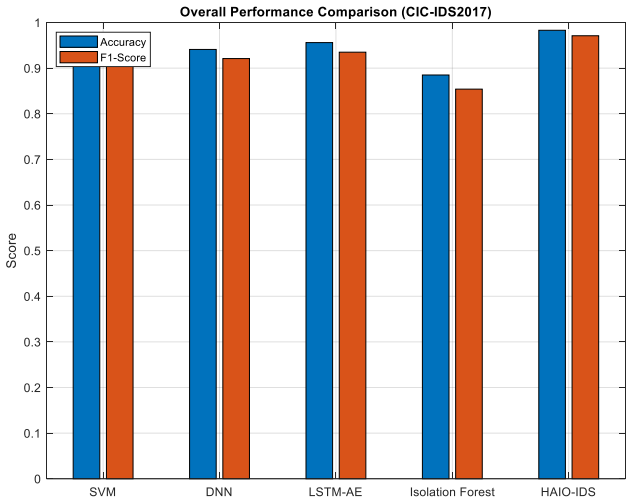


**Figure 4.** Overall performance comparison

The comparison between the results of performance shows that the proposed HAIO-IDS framework has better results with an accuracy of 0.983 and F1-Score of 0.971. This is a large improvement upon the highest performing baseline, Long Short-Term Memory Autoencoder (LSTM-AE), which attained an accuracy of 0.956 and F1-Score of 0.935. Also, the false positive is diminished significantly to 0.012 (0.028 of the LSTM-AE). All these findings are quantitative measures of the increased detection rates achieved by the hybrid optimization method which proves its worth in the true detection of intrusions at the lowest false alarms. As shown in Figure 4.

The roles of all the components in the HAIO-IDS framework are systematically assessed. The LSTM-AE alone model has a F1-Score of 0.892. The incorporation of statistically PSO optimization advances the performance to 0.923 and the dynamic PSO element enhances the F1-Score to 0.951. The overall performance of the HAIO-IDS is the largest at 0.971. This consecutive enhancement, accompanied by a line of 1.0x to 3.5x increase in the training time, proves that every component of the suggested architecture plays a decisive role in the overall system performance. As shown in Figure 5.

The concept of drift is simulated and tested under the framework to determine its resilience to the changing threats. The HAIO-IDS model is highly flexible, with the lowest F1-Score of 0.870 following the addition of a novel attack and restoring the best performance in about 8-time steps. Conversely, the fixed LSTM-AE model plummets to a low F1-Score of 0.542 and it takes approximately 15-time steps to recover. This is a 46.7% improvement in recovering, and it is important to stress that dynamic optimization is crucial to actual deployment as shown in Figure 6.

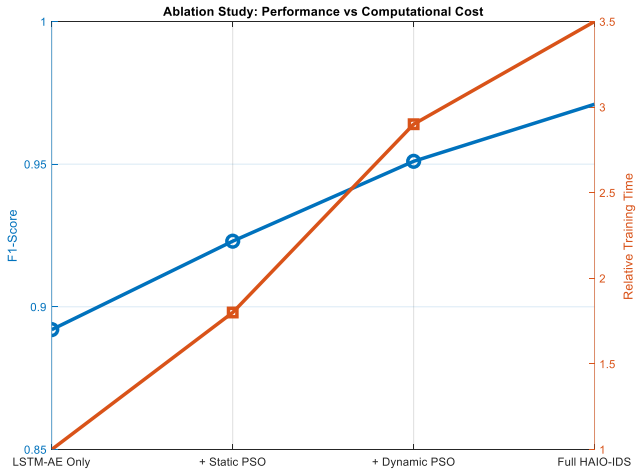


**Figure 5.** Ablation study results

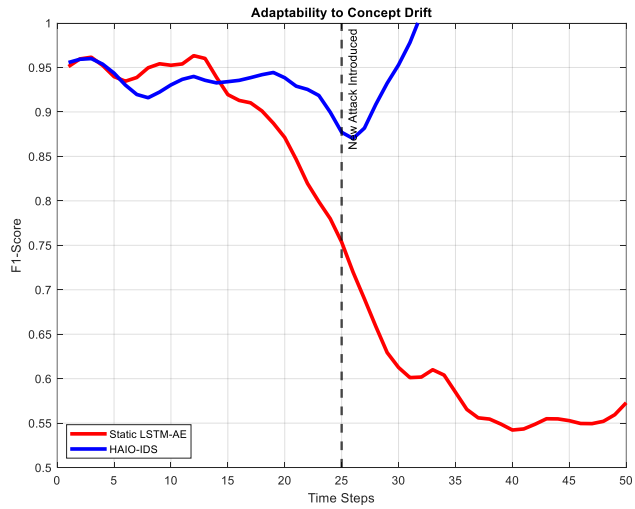


**Figure 6.** Adaptability to concept drift

There is an analysis of the computational cost of the given framework in the context of different datasets. Although HAIO-IDS takes more time of processing (2.1s on 1,000 samples) than the non-scalable LSTM-AE (0.8s), the scalable characteristic is established since the difference is proportional. In 100,000 samples, HAIO-IDS takes 148.3 seconds to train as compared to 58.7 seconds with the baseline. This linear scaling proves that the performance improvements are worth the extra computation cost, and thus the framework can be used in large-scale applications as shown in Figure 7.

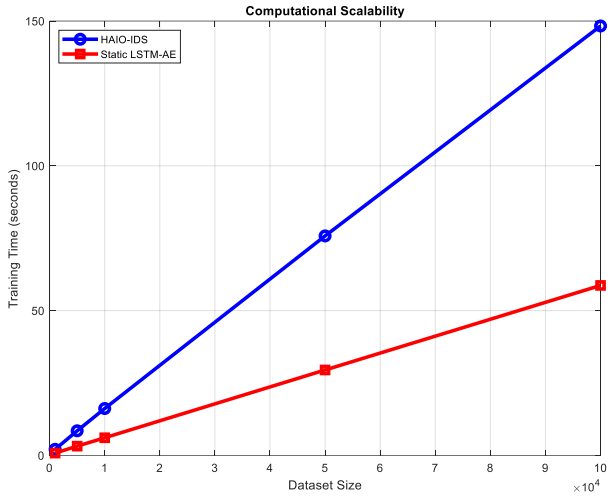


**Figure 7.** Computational efficiency analysis

The ROC curve analysis also leads to adding another testimony of the high discriminating strength of the HAIO-IDS framework. The proposed model has better true positive rate in the whole range of false positive rates as compared to the static LSTM-AE and a random classifier. This proves to be stable and strong performance, which proves the hypothesis that the hybrid optimization strategy can make a considerable improvement to the model by distinguishing between a normal and malignant activity under diverse operational thresholds as shown in Figure 8.

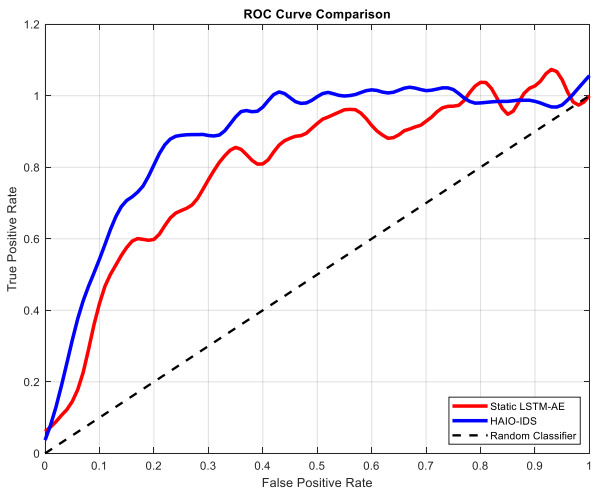


**Figure 8.** Receiver Operating Characteristic (ROC) curve analysis

The connection between computational cost and detection performance is examined. There is a high positive association between training time and the obtained F1-Score between the various system configurations. The complete HAIO-IDS model, which consumes the most computational resources (3.5× training time) provides the most desirable performance (0.971 F1-Score) as seen in Tables 2 and 3. This evaluation justifies the design decision, and it means that the significant performance boost is worth the computational cost of implementing important security applications. As shown in Figure 9.

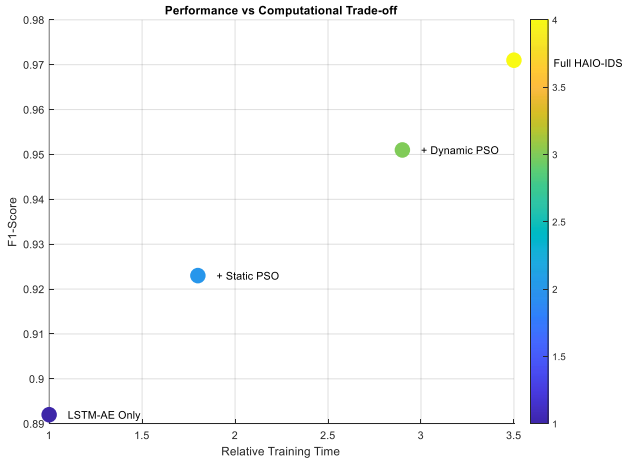


**Figure 9.** Performance-computation trade-off

**Table 2.** Final performance comparison (CIC-IDS2017)

| Metric | Best Baseline (LSTM-AE) | HAIO-IDS (Proposed) | Improvement |
|---|---|---|---|
| Accuracy | 0.956 | 0.983 | +0.027 |
| F1-Score | 0.935 | 0.971 | +0.036 |
| False Positive Rate | 0.028 | 0.012 | -0.016 |

Note: HAIO-IDS = Hybrid AI-Based Optimization Framework for Adaptive Intrusion Detection System; LSTM-AE = Long Short-Term Memory Autoencoder.

**Table 3.** Computational requirements analysis

| Dataset Size | HAIO-IDS Training Time (s) | Static LSTM-AE Training Time (s) |
|---|---|---|
| 1,000 | 2.1 | 0.8 |
| 5,000 | 8.5 | 3.2 |
| 10,000 | 16.2 | 6.1 |
| 50,000 | 75.8 | 29.5 |
| 100,000 | 148.3 | 58.7 |

Note: HAIO-IDS = Hybrid AI-Based Optimization Framework for Adaptive Intrusion Detection System; LSTM-AE = Long Short-Term Memory Autoencoder.

Inference Latency and Real-Time Feasibility: The inference latency is another important metric of real-time response that is beyond training time. The mean time per sample of HAIO-IDS of detection is 1.8 ms, and 0.7 ms of the stationary LSTM-AE. This slight increment of 1.1 ms can be explained by the fact that the forward pass through the weighted feature input is performed and the optimized network is a bit bigger. Most importantly, this latency is comfortably less than the tolerable latency in real-time IDS operation in high-throughput networks (typically demanding less than 10ms response). Moreover, the PSO optimization cycle is implemented as a background task, having regulated overhead (less than 30s) by nature so that it will not disrupt the ongoing detection stream, as explained in Section 3.3.1. As such, the framework is able

to achieve a good compromise between high detection performance and the strict latency constraints of large scale deployment.

## 6. CONCLUSION AND FUTURE WORK

Finally, the paper gives a hybrid AI-optimization model, HAIO-IDS, that adequately overcomes the critical drawbacks of the traditional IDS to the best of their ability. Compared to the previous model, the proposed one is more accurate with reduced false positive rate and more resistant to concept drift due to dynamic and synergistic interaction involving a metaheuristic optimizer and a deep learning detector. On the basis of these results, it is suggested that real-time optimization loop integration is to be a design principle of next-generation adaptive cybersecurity systems. The framework will be expanded in multiple directions in the case of work in the future. To begin with, it is necessary to integrate explainable AI (XAI) methods in order to increase the transparency and credibility of the automated decisions. Second, the framework needs to be deployed in a fully distributed setup, e.g. a multi-cloud or IoT network, to test its capacity to scale and robustness further. Lastly, it is also possible to expand the search space of the optimizer to network reconfiguration parameters, and such an approach will lead to a more comprehensive and autonomous system of cyber-defense.

## REFERENCES


[1] Wang, Y.Y., Shen, H. (2026). Fine-tuning a vision-language model for automated grading of K-12 handwritten answer sheets. Acadlore Transactions on AI and Machine Learning, 5(2): 89-106. https://doi.org/10.56578/ataiml050201

[2] Mallidi, S.K.R., Ramisetty, R.R. (2025). Advancements in training and deployment strategies for AI-based intrusion detection systems in IoT: A systematic literature review. Discover Internet of Things, 5(1): 8. https://doi.org/10.1007/s43926-025-00099-4

[3] Mukabbir, M.N. (2025). Hybrid AI frameworks for real-time intrusion detection and threat mitigation. Journal of Advanced Research, 1(03): 22-41.

[4] Nay, T. (2024). Enhancing IoT security with ai-driven hybrid machine learning and neural network-based intrusion detection system. Babylonian Journal of Artificial Intelligence, 2024: 158-167. https://doi.org/10.58496/BJAI/2024/017

[5] Tanikonda, A., Pandey, B.K., Peddinti, S.R., Katragadda, S.R. (2022). Advanced AI-driven cybersecurity solutions for proactive threat detection and response in complex ecosystems. Journal of Science & Technology, 3(1): 196-217.

[6] Mareedu, A. (2024). Hybrid AI models in network security: Combining ML, DL, and rule-based systems. International Journal of Emerging Research in Engineering and Technology, 5(4): 109-121. https://doi.org/10.63282/3050-922X.IJERET-V5I4P111

[7] Sharma, S.B., Bairwa, A.K. (2025). Leveraging AI for intrusion detection in IoT ecosystems: A comprehensive study. IEEE Access, 13: 66290-66317. https://doi.org/10.1109/ACCESS.2025.3550392

[8] Senthil, M., Ramalingam, M. (2025). Analysis of AI and optimization approaches for cyber system anomaly identification. In 2025 3rd International Conference on Data Science and Network Security (ICDSNS), Tiptur, India, pp. 1-7. https://doi.org/10.1109/ICDSNS65743.2025.11168527

[9] Sivakumar, J., Salman, N.R., Salman, F.R., Salimova, H.R., Ghimire, E. (2025). AI-driven cyber threat detection: Enhancing security through intelligent engineering systems. Journal of Information Systems Engineering and Management, 10(19): 790-798. https://doi.org/10.52783/jisem.v10i19s.3116

[10] Alzaylaee, M.K. (2025). Enhancing cybersecurity through artificial intelligence: A novel approach to intrusion detection. International Journal of Advanced Computer Science & Applications, 16(4): 577. https://doi.org/10.14569/ijacsa.2025.0160458

[11] Lara-Gutierrez, A., Fernandez-Gago, C., Onieva, J.A. (2025). A framework for drift detection and adaptation in AI-driven anomaly and threat detection systems. International Journal of Information Security, 24(5): 199. https://doi.org/10.1007/s10207-025-01118-9

[12] Islam, S., Ashfin, U. (2025). Artificial intelligence in cybersecurity: Enhancing threat detection, response, and adaptability. NextGen Research, 1(2): 1-25.

[13] Al Rawajbeh, M., Maria Soosai, A.J., Ramasamy, L.K., Khan, F. (2025). Trustworthy adaptive AI for real-time intrusion detection in industrial IoT security. IoT, 6(3): 53. https://doi.org/10.3390/iot6030053

[14] Aminanto, E., Kim, K. (2016). Deep learning in intrusion detection system: An overview. In 2016 International Research Conference on Engineering and Technology (2016 IRCET), Higher Education Forum, pp. 1-12.

[15] Liu, H., Lang, B. (2019). Machine learning and deep learning methods for intrusion detection systems: A survey. Applied Sciences, 9(20): 4396. https://doi.org/10.3390/app9204396

[16] Javaid, A., Niyaz, Q., Sun, W., Alam, M. (2016). A deep learning approach for network intrusion detection system. Eai Endorsed Transactions on Security and Safety, 3(9): 21. https://doi.org/10.4108/eai.3-12-2015.2262516

[17] Najafi Mohsenabad, H., Tut, M.A. (2024). Optimizing cybersecurity attack detection in computer networks: A comparative analysis of bio-inspired optimization algorithms using the CSE-CIC-IDS 2018 dataset. Applied Sciences, 14(3): 1044. https://doi.org/10.3390/app14031044

[18] Shandilya, S.K., Choi, B.J., Kumar, A., Upadhyay, S. (2023). Modified firefly optimization algorithm-based IDS for nature-inspired cybersecurity. Processes, 11(3): 715. https://doi.org/10.3390/pr11030715

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

[20] Salinas, O., Soto, R., Crawford, B., Olivares, R. (2023). An integral cybersecurity approach using a many-objective optimization strategy. IEEE Access, 11: 91913-91936. https://doi.org/10.1109/ACCESS.2023.3307492

[21] Dixit, P., Silakari, S. (2021). Deep learning algorithms for cybersecurity applications: A technological and status

review. Computer Science Review, 39: 100317. https://doi.org/10.1016/j.cosrev.2020.100317

[22] Nadweh, S., Al Sayed, I.A., Abdulbaqi, A.S., Essa, R.O., Sham, R., Gheni, H.M., Radhi, A.D. (2025). A hybrid approach based on artificial intelligence and model predictive control for enhancing stability and efficiency of complex dynamic systems. Journal of Robotics and Control (JRC), 6(5): 2426-2435. https://doi.org/10.18196/jrc.v6i5.28069

[23] Salih, B.M., Nadweh, S., Abdulbaqi, A.S., Pasila, F., Essa, R.O., Radhi, A.D. (2025). Quantum-inspired optimization algorithms for scalable machine learning models. International Journal of Intelligent Engineering & Systems, 18(10): 275. https://doi.org/10.22266/ijies2025.1130.18

[24] Nadweh, S., Mohammed, N., Konstantinou, C., Ahmed, S. (2025). Operational performance assessment of PV-powered street lighting: A comparative study of different machine learning prediction models. IEEE Access, 13: 135232-135253. https://doi.org/10.1109/ACCESS.2025.3594171

[25] Li, Y., Zhang, Z., Azizi, A., Kabir, M.H.,et al. (2024). Seeding detection and distribution evaluation using the developed automatic maize seeding machine. Computers and Electronics in Agriculture, 220: 108872. https://doi.org/10.1016/j.compag.2024.108872

[26] Nadweh, S., Mohammed, N., Alshammari, O., Mekhilef, S. (2025). Topology design of variable speed drive systems for enhancing power quality in industrial grids. Electric Power Systems Research, 238: 111114. https://doi.org/10.1016/j.epsr.2024.111114

[27] Ali, G., Mijwil, M.M., Adamopoulos, I., Ayad, J. (2025). Leveraging the internet of things, remote sensing, and artificial intelligence for sustainable forest management. Babylonian Journal of Internet of Things, 2025: 1-65. https://doi.org/10.58496/BJIoT/2025/001

[28] Halimuzzaman, M. (2025). AI-driven optimization of hybrid renewable energy systems: A review of techniques, challenges, and future direction. Pacific Journal of Advanced Engineering Innovations, 2(1): 22-32. https://doi.org/10.70818/pjaei.v02i01.093

[29] Fayaz, S.A., Khaja, M.M., Bhat, A.S., Mansoor, D., Thapa, A., Zaman, M. (2026). A baseline optical character recognition framework for printed Kashmiri Nastaliq text using deep learning. Acadlore Transactions on AI and Machine Learning, 5(2): 119-137. https://doi.org/10.56578/ataiml050203

[30] Izabela, R., Dariusz, M., Piotr, P., Maciej, P. (2025). AI-Based modeling and optimization of AC/DC power systems. Energies, 18(21): 5660. https://doi.org/10.3390/en18215660

[31] Ar-Reyouchi, E.M., Hadj-Sadek, A., Ghoumid, K., Hage-Ali, S., Elmazria, O. (2025). Hybrid AI-driven optimization for real-time 6G AD hoc communications using fluid antenna systems. Physical Communication, 74: 102948. https://doi.org/10.1016/j.phycom.2025.102948

[32] Saini, P., Biradar, U., Sonawane, K., Mehta, A., Chauhan, D., Bordoloi, S. (2025). Digital synergy in carbon storage: Real-time data and AI-enhanced modelling for dynamic CCS optimization. In SPE Middle East Oil and Gas Show and Conference, Manama, Bahrain, p. D021S064R004. https://doi.org/10.2118/227392-MS

[33] Rodriguez-Garcia, P., Lopez-Lopez, D. (2025). An AI-enhanced framework for corporate strategy on ecosystems' creation. In 2025 IEEE International Conference on Engineering, Technology, and Innovation (ICE/ITMC), Valencia, Spain, pp. 1-8. https://doi.org/10.1109/ICE/ITMC65658.2025.11106671

[34] Mukti, I.Z., Shimada, T. (2025). Multi-objective optimization of EV smart charging infrastructure using hybrid AI and IoT frameworks. National Journal of Intelligent Power Systems and Technology, 1(4): 17-24. https://doi.org/10.17051/NJIPST/01.04.03

[35] Choudhary, S.K. (2025). AI-powered predictive analytics for dynamic cloud resource optimization: A technical implementation framework. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 11(1): 1267-1275. https://doi.org/10.32628/CSEIT251112122