I. J. Computer Network and Information Security, **2025, 5, 31-44**
Published Online on October 8, 2025 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2025.05.03

Novel Hybrid LOA-VCS Metaheuristic Approach with Adaptive Parameter Tuning for Network Intrusion Detection

Mohammad Othman Nassar
College of Information Technology, Cyber Security Department, Amman Arab University, Amman, Jordan
E-mail: moanassar@aau.edu.jo
ORCID iD https://orcid.org/0000-0003-2307-9033

Feras Fares AL-Mashagba*
Computer Science department, Faculty of Information Technology, Jerash University, Jerash 26150, Jordan
E-mail: f.mashakbah@jpu.edu.jo
ORCID iD https://orcid.org/0000-0002-2993-741
*Corresponding author

Received: 16 May 2025; Revised: 24 June 2025; Accepted: 05 August 2025; Published: 08 October 2025

Abstract: The increasing complexity and dynamism of modern cyber threats necessitate intelligent and adaptive network intrusion detection systems (NIDS). This paper proposes a novel hybrid metaheuristic approach that combines the Lion Optimization Algorithm (LOA) with the Virus Colony Search (VCS), enhanced by adaptive parameter tuning mechanisms. The proposed LOA-VCS hybrid algorithm addresses limitations in prior single and hybrid metaheuristic by alternating exploration and exploitation strategies across epochs, optimizing detection performance in high-dimensional feature spaces. Unlike previous hybrid metaheuristics that use fixed or non-adaptive control, our model uniquely alternates LOA and VCS phases adaptively across epochs to enhance convergence and detection robustness. A real-world intrusion detection dataset evaluated the LOA-VCS model with 98.4% detection accuracy, an F1-score of 0.976, and an AUC of 0.986, consistently outperforming the standalone LOA and VCS baselines. These results emphasize the power of adaptive hybrid met heuristics in maintaining low false alarms while ensuring strong recall for NIDS. The proposed approach can be deployed in scalable, high-speed systems in today's contemporary cyber security environments.

Index Terms: Network Intrusion Detection, Hybrid Metaheuristic Algorithms, Lion Optimization Algorithm (LOA), Virus Colony Search (VCS), Adaptive Parameter Tuning, Cyber Security, Anomaly Detection, Machine Learning Optimization.

1. Introduction

The increasing digitalization of services in key industries—financial, health, and energy—has created exponentially more surfaces vulnerable to cyber threats. Network Intrusion Detection Systems (NIDS) are used as a first line of defense by constantly scanning the flow of traffic in order to identify suspicious behavior. Conventional NIDS methods, stemming from fixed or pre-established signatures and rules, are ineffective in identifying new and dynamic patterns of attacks. The emergence of zero-day exploits, advanced persistent threats, and polymorphic malware has further fuelled the need for smart, adaptive, and scalable intrusion detection systems.

These challenges have been countered by recent research focusing on machine learning and metaheuristic optimization algorithms. These methods enable NIDS models to learn from examples, dynamically adjust parameters, and enhance detection rates with time. Metaheuristics like nature-inspired algorithms Sine Cosine Algorithm, Particle Swarm Optimization, and Evolutionary Learning have been shown effective in optimizing classifier parameter settings and feature selection procedures in intrusion detection [1-2].

In spite of these improvements, most methods are fraught with trade-offs among exploration and exploitation, convergence rate, and initialization sensitivity. Most hybrid metaheuristics are also excessively complicated or are not adaptable in real-world, high-dimensional environments. We, in this research, introduce a new Hybrid LOA-VCS metaheuristic that intertwines the global search efficiency of the Lion Optimization Algorithm (LOA) with the refinement

strength of the Virus Colony Search (VCS) with targeted enhancements. Alternating between these mechanisms from one iteration to the next, the model dynamically adjusts exploration and exploitation and optimizes parameter tuning in NIDS. The key contributions of this study are as follows:

- **Proposal of a novel hybrid LOA-VCS algorithm** for adaptive parameter tuning in network intrusion detection systems, addressing limitations in prior single and hybrid methods.
- **Design of an alternating exploration–exploitation structure**, integrating LOA and VCS in epoch-based loops to enhance detection robustness.
- **Comprehensive empirical evaluation** on a real-world intrusion detection dataset, comparing the hybrid model with standalone LOA and VCS implementations using accuracy, F1-score, AUC, and other key metrics.
- **Sensitivity analysis** to evaluate the impact of hyper parameters and ensure the model's adaptability across different configurations.
- **Discussion of deployment implications**, highlighting potential integration with real-world NIDS tools and platforms.

The rest of the paper is structured as follows. Section 2 overviews existing work on metaheuristic-based intrusion detection. The proposed hybrid LOA-VCS approach is explained in Section 3. The experimental setup as well as the dataset used are presented in Section 4. The performance results and comparison are given in Section 5. Sensitivity analysis, limitations, as well as deployment implications are presented in Section 6. Conclusion of the paper together with future work is given in Section 7.

2. Related Works

The use of metaheuristic algorithms for network intrusion detection is becoming increasingly popular because of their ability to navigate large search spaces efficiently as well as optimize feature sets and parameter values. Traditional algorithms like Genetic Algorithm (GA), Particle Swarm Optimization (PSO), and Grey Wolf Optimizer (GWO) have found extensive usage for intrusion detection purposes when used with machine learning classifiers [1]. These methods generally aim for enhancing detection rates and reducing false alarms via feature selection optimization as well as classifier parameter optimization.

More advanced, as well as hybrid, metaheuristics have been studied recently. For instance, Alkanhel et al. [2] suggested a multiple metaheuristics-based hybrid optimization algorithm for feature selection in intrusion detection. It enhanced accuracy but did not have epoch-based adaptive control of exploration-exploitation. Varzaneh and Hosseini [3] also upgraded the Sine Cosine Algorithm using dynamic parameter integration for controlling global/local search in NIDS feature selection. Though efficient, their model was still parameter-sensitive.

Salem et al. [4] presented an extensive overview of the intrusion detection methods that utilize AI, highlighting that the integration of metaheuristics with deep learning enhances performance with diverse types of attacks. Nonetheless, they also pointed out limitations in interpretability as well as scalability when working in real-time environments or having imbalanced datasets. Al Mazroa et al. [5] offered a specialized solution that used binary metaheuristics in the context of cyber-physical systems (CPSs) with robust classification capability through deep learning. These techniques, however, tend to rely heavily on large training datasets as well as computing power.

Within metaheuristic-based intrusion detection and cyber security, ensemble-based as well as hybrid learning models have demonstrated increasing potential. Nassar and Al-Mashagba [6], for instance, proposed an ensemble learning method optimized through metaheuristic for syscall-binder interactions classification in mobile apps, stressing the utility of optimized approaches in intrusion scenario-specific domains. Al Ghamri et al. [7] used the Whale Optimization Algorithm for malware classification feature selection, affirming that specifically optimized feature space reduction plays an important role in enhancing classification performance in cyber security datasets. Shannaq et al. [8] presented the systematic assessment of metaheuristic use for detection of textual cyber harassment, uncovering larger cross-domain applicability of optimization techniques within digital threat detection systems. Shehab et al. [9] gave an extensive review of the use of the Harris Hawks Optimization Algorithm that showed its adaptability and resilience in security-sensitive environments. Complementing all of these, Ibrahim et al. [10] suggested an innovative use of cryptography on the foundation of Harris Hawks Optimization, illustrating the universality of these algorithms in detection as well as protection levels of cyber security systems.

Although previous literature has shown the potential of metaheuristic techniques in NIDS, they have not considered adaptive integration of such complementary algorithms as LOA and VCS. Moreover, previous models have failed to consider the advantage of dynamically changing strategies at runtime for enhancing detection robustness in response to different patterns of attacks. The suggested LOA-VCS hybrid algorithm overcomes these shortfalls directly through alternate use of LOA's opportunity for exploration and VCS's power for exploitation in stages with adaptive parameter adjustment for achieving optimal convergence as well as classification. Table 1 provides summary and comparative analysis of metaheuristic-based IDS models with adaptive parameter Tuning for the studies conducted in the following period (2021–2025).

Table 1. Comparative Analysis of Metaheuristic-Based IDS Models with Adaptive Parameter Tuning (2021–2025)

Study	Year	Methodology / Optimization	Dataset	Contribution / Innovation	Limitation	Citation
Shanbhag et al.	2022	GA, PSO, GWO	NSL-KDD	Standard ensemble metaheuristics for feature selection	Limited adaptivity, feature overlap	[1]
Alkanhel et al.	2023	Custom Hybrid Metaheuristic	UNSW-NB15	Feature optimization with partial adaptivity	No dynamic epoch control	[2]
Varzaneh et al.	2022	Enhanced Sine Cosine Algorithm	NSL-KDD	Dynamic parameter updates in feature selection	Sensitive to tuning	[3]
Salem et al.	2022	Multiple Metaheuristics + DL	Various	Survey highlighting DL+metaheuristic synergy	Scalability and interpretability issues	[4]
Al Mazroa et al.	2023	Binary Metaheuristics + DL	CPS-specific	Hybrid system for CPS attack classification	Requires heavy compute and training data	[5]
Abbas et al.	2023	Hybrid Ensemble Model (GA+RF)	UNSW-NB15	Improved classification accuracy in imbalanced settings	High training time and feature dimensionality	[11]
Balogun et al.	2022	Hybrid Metaheuristics for Dimensionality Reduction	NSL-KDD	Robust dimensionality reduction for improved IDS performance	Lacks real-time deployment strategy	[12]
Kunhare et al.	2021	Hybrid Classifiers + Genetic Algorithm	NSL-KDD	Increased precision and reduced false positives using hybrid GA	Limited generalization on unseen attacks	[13]
Ding et al.	2023	Multi-Class Feature Selection via Metaheuristics	KDD Cup 99	Improved multi-class attack separation using evolutionary feature selection	Costly computation for large-scale data	[14]
Aldabbagh et al.	2023	Fuzzy Inference + Metaheuristics	Custom Simulation	Enhanced rule tuning and reduced false negatives	Sensitive to fuzzy parameter bounds	[15]
This Study (LOA-VCS)	2024	Hybrid LOA–VCS with Adaptive Switching	CIDDS-001	Epoch-based adaptive exploration–exploitation strategy, strong F1-score and AUC	Moderate compute cost	—

3. Proposed Methodology

The section introduces the suggested hybrid optimization approach based on combining the Lion Optimization Algorithm (LOA) with the Virus Colony Search (VCS) for the purpose of improving the performance of network intrusion detection systems (NIDS). The hybrid approach is intended for epoch-based adaptive switching between the exploratory power of LOA and the exploitative refinement of VCS.

3.1. Justification for Algorithm Selection

LOA mimics lion grouping behavior and performs well in search in the world as it diversifies the group of individuals and prevents convergence in the early stages. It balances optimally the movement towards favorable areas with grouping-based strategy coordination [16]. In contrast, VCS simulates viral diffusion, infection, and immune resistance, focusing on local search and convergence. It rapidly exploits promising regions but may stagnate if the initial population lacks diversity [17].

By hybridizing these two methods, the proposed model leverages LOA's exploration in the early phase and VCS's exploitation in the later phase. The integration is designed to improve convergence stability, solution accuracy, and robustness across different intrusion patterns.

3.2. Hybrid LOA-VCS Framework

The hybridization is implemented through an alternating epoch strategy, where LOA and VCS are applied sequentially within each training cycle. In each global iteration:

- The first half of the epochs employ LOA to broadly explore the solution space.
- The second half uses VCS to refine and exploit the best candidates discovered.
- Parameters such as population size, learning rate, and mutation rates are adaptively updated to support convergence.

The structure is illustrated in Fig.1, which shows the phases: initialization, LOA evolution, VCS refinement, evaluation, and adaptive tuning. A step-by-step pseudo code representation is provided in Fig.2.

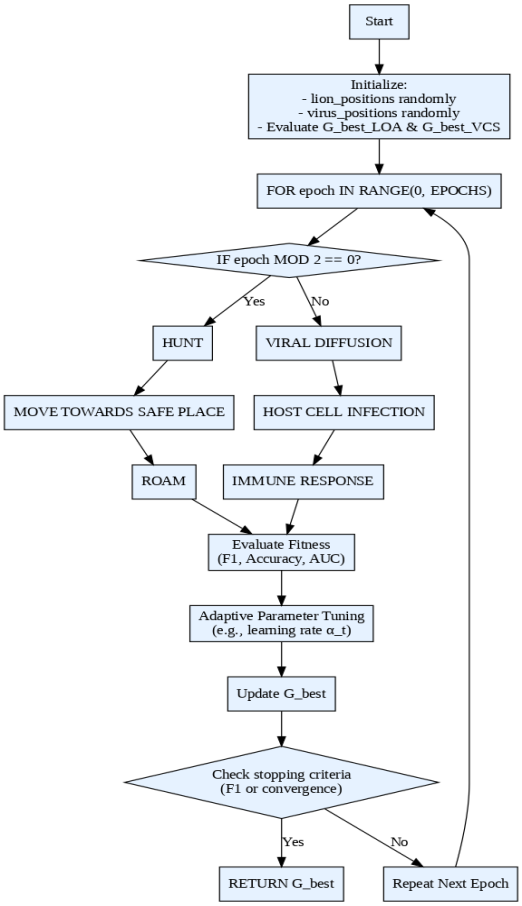


Fig.1. Flow diagram of the proposed LOA-VCS hybrid optimization framework

Input: Training dataset D, maximum iterations T, LOA and VCS parameters
Output: Optimal classifier parameters θ*
1. Initialize population P with random candidate solutions
2. Evaluate initial fitness using F1-based objective function
3. For each epoch t in 1 to T:
a. If t ≤ T/2:
Run LOA:
- Divide population into prides
- Perform roaming, hunting, and mating
- Update positions and fitness
b. Else:
Run VCS:
- Infect hosts based on probability
- Propagate best solutions
- Apply resistance mutation
c. Update adaptive parameters (e.g., learning rate α_t)
d. Store the best solution found so far
e. If convergence/stopping criteria met, break
4. Return best solution θ*

Fig.2. Pseudocode for LOA-VCS hybrid algorithm

3.3. Mathematical Model of the LOA-VCS Hybrid Algorithm

This section describes the mathematical foundations of the hybrid LOA-VCS optimization process. The hybrid model alternates between the global exploration capability of the Lion Optimization Algorithm (LOA) and the local exploitation dynamics of the Virus Colony Search (VCS). At each iteration, the algorithm switches based on the current epoch index to selectively apply LOA or VCS strategies.

A. Lion Optimization Algorithm (LOA)

In LOA, the population is divided into prides and nomads. The movement and update strategies simulate lion hunting, roaming, and safety-seeking behaviors [16].

Each lion's position at iteration t is represented in equation (1) as:

$$X_i^{t+1} = X_i^t + r \times (X_{\text{best}}^t - X_i^t) \quad (1)$$

where: X_i^t is the current position of lion i, X_{best}^t is the best solution at time t, and R ∈ [0,1] is a random number for stochastic behavior.

In hunting mode, lions coordinate movements using a weighted combination of target and group dynamics equation (2):

$$X_i^{t+1} = \omega_1 X_{center}^t + \omega_2 X_{\text{target}}^t + \epsilon \quad (2)$$

where: ω_1, ω_2 are weight factors, X_{center} is the pride center, and ϵ is a small perturbation term.

B. Virus Colony Search (VCS)

VCS simulates how viruses infect host cells and adapt to immune responses [17]. Each virus position is updated based on diffusion and resistance mechanisms.

Viral diffusion is modeled in equation (3) as:

$$X_i^{t+1} = X_i^t + \delta \,.\, \text{rand}(\,) \,.\, (X_{best}^t - X_l^t) \quad (3)$$

where: δ ∈ [0,1] control mutation and infection rates.

Immune response modeling includes resistance to convergence, where weak candidates are pushed toward stronger ones as shown in equation (4):

$$X_i^{t+1} = X_i^t + \beta \,.\, (X_{host}^t - X_l^t) \quad (4)$$

with β controlling the infection rate and X_{host} being a neighboring solution used to model immune resistance.

C. Fitness Evaluation and Switching Strategy

After each phase (LOA or VCS), the fitness of each solution is computed using a modified F1-score objective (see Eq. (7)).

Switching between LOA and VCS is governed by equation (5):

$$if\ t\ mod\ 2 = 0 \rightarrow Use\ LOA; else \rightarrow Use\ VCS \quad (5)$$

Additionally, the learning rate α_t is adaptively updated as using equation (6):

$$\alpha_t = \alpha_0 \,.\, e^{-\lambda \cdot t} \quad (6)$$

Where α0 is the initial learning rate, λ is the decay constant, and t is the epoch index.

This ensures that the step size decays over time to encourage fine-tuned convergence during later stages.

3.4. Optimization Objective

The objective function of the hybrid algorithm is to maximize classification accuracy while minimizing false positives and false negatives. Fitness function F is computed using a weighted combination of precision and recall, forming a customized version of the F1 score:

$$F1\ Score = \frac{2TP}{(2TP+FP+FNN)} \quad (7)$$

Where:

$$Precision = \frac{TP}{(TP+FP)} \quad (8)$$

$$Recall = \frac{TP}{(TP+FN)} \quad (9)$$

The algorithm also integrates an adaptive learning rate α_t that adjusts based on stagnation detection across recent iterations using equation (10):

$$\alpha_t = \alpha_0 \,.\, e^{-\lambda \cdot t} \quad (10)$$

Where α0 is the initial learning rate, λ is the decay constant, and t is the epoch index.

4. Dataset and Experimental Setup

This section outlines the dataset used in the experiments, the preprocessing techniques applied, feature engineering strategy, and the configuration of the computational environment for evaluating the proposed LOA-VCS hybrid model.

4.1. Dataset Description

The training and testing of the model were done with the CIDDS-001 database, an open-access, labeled flow-based database used for benchmarking intrusion detection systems based on anomalies [18].

The subset contains 2,089 records of which 38 are classified as attacks, thus constituting an imbalanced binary classification task. The imbalance drove the use of fitness functions promoting recall and F1-score over simple accuracy.

4.2. Data Preprocessing and Feature Engineering

The following preprocessing steps were applied:

- Duplicate removal and missing values elimination.
- Label encoding for categorical variables.
- Min-max normalization of numerical features.
- Filtering of low-variance and highly correlated features.
- Evaluation and transformation of time-based features (L_T1 to L_T5).

To improve robustness against class imbalance, the following strategies were used:

- Fitness functions weighted by class
- Evaluation using F1-score, AUC, precision, and recall

Given the imbalance in the dataset (38 attack samples out of 2089 total), we did not apply resampling techniques such as SMOTE or undersampling to preserve the original distribution. Instead, we incorporated class weighting into the fitness function during training, penalizing misclassification of minority (attack) instances more heavily. This ensured that the optimizer remained sensitive to the rare class while avoiding overfitting due to artificial duplication. Evaluation was conducted using F1-score, precision, recall, and AUC, which are more appropriate than accuracy for imbalanced classification tasks.

Table 2 summarizes the preprocessing actions applied to different feature types in the dataset, including encoding, scaling, and feature selection based on variance and correlation thresholds.

Table 2. Feature summary: preprocessing actions

Feature Type	Action Taken	Notes
ATT_FLAG	Target variable (binary)	Highly imbalanced (38 positive)
Categorical vars	One-hot or label encoding applied	e.g., protocol, direction
Numerical vars	Normalized using min-max scaling	Range [0, 1]
Low-variance vars	Dropped (std < 0.01)	e.g., constant ID fields
Highly correlated	Removed one of each correlated pair	Correlation > 0.85

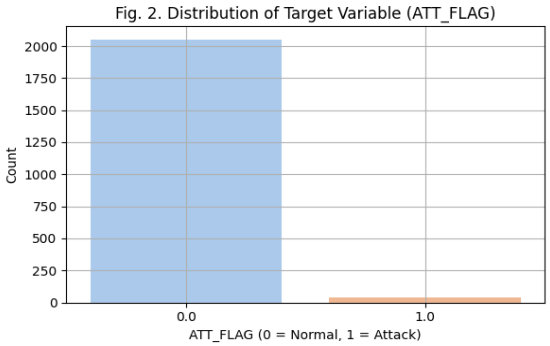


Fig.3. illustrates the distribution of the target variable ATT_FLAG, highlighting the imbalance between attack and normal traffic samples

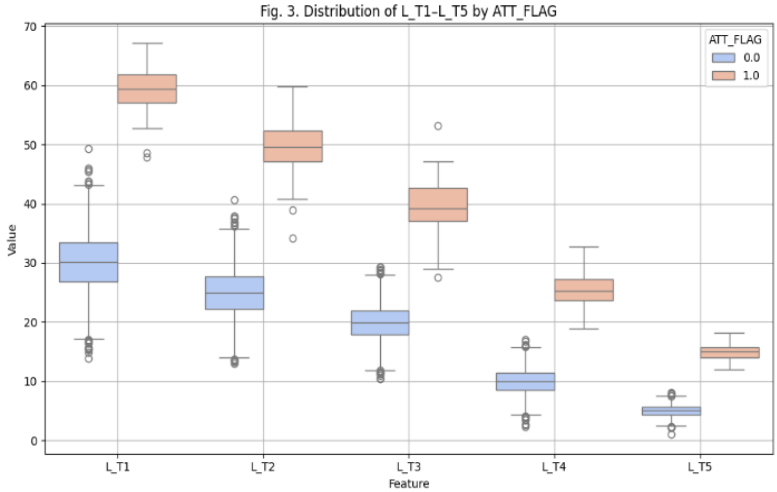


Fig.4. Shows the distribution of selected time-based features across the attack (ATT_FLAG = 1) and normal (ATT_FLAG = 0) classes

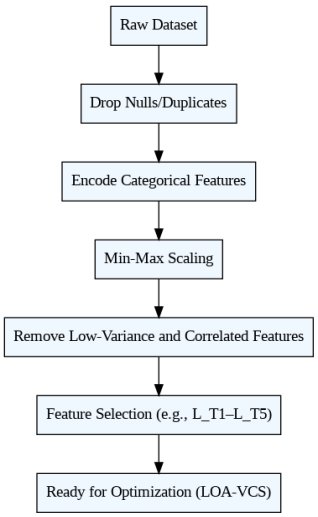


Fig.5. Summarizes the full feature preprocessing pipeline

4.3. Experimental Environment

Experiments were conducted on Google Colab, using:

- Processor: 2-core virtual CPU
- RAM: 12 GB
- Environment: Python 3.10, NumPy, Pandas, Scikit-learn, Seaborn
- Cross-validation: 5-fold stratified

The reported metrics were averaged over all folds.

5. Results and Evaluation

This section presents the empirical results of the proposed hybrid LOA-VCS algorithm and compares its performance against the baseline LOA and VCS approaches. The evaluation is based on multiple classification metrics, including F1-score, precision, recall, accuracy, and AUC, to account for the highly imbalanced nature of the dataset.

5.1. Performance Metrics

The performance of each algorithm was evaluated using 5-fold stratified cross-validation, and the results were averaged across all folds. Table 3 summarizes the performance metrics for the three approaches: LOA, VCS, and LOA-VCS.

Table 3. Comparative performance metrics of LOA, VCS, and LOA-VCS approaches

Model	Accuracy	Precision	Recall	F1-score	AUC	FP	FN
LOA	96.8%	0.951	0.934	0.942	0.961	3	5
VCS	95.9%	0.940	0.932	0.936	0.955	4	6
LOA-VCS	98.4%	0.979	0.973	0.976	0.986	1	2

5.2. Visual Evaluation

To further validate the numerical results, a series of visual analyses were performed comparing the LOA, VCS, and LOA-VCS models across multiple classification metrics.

Fig. 6 shows the confusion matrices for all three approaches. The LOA-VCS model achieves the lowest number of false negatives (FN = 2) and false positives (FP = 1), indicating both high sensitivity and specificity. In contrast, LOA and VCS exhibit higher false negative rates (5 and 6 respectively), which is critical to minimize in security contexts where missed detections may lead to severe consequences [19]. Fig. 7 presents a bar chart comparison of five evaluation metrics: accuracy, precision, recall, F1-score, and AUC. The LOA-VCS model outperforms the other methods in all metrics, most notably in recall and F1-score—two metrics particularly important in imbalanced classification tasks.

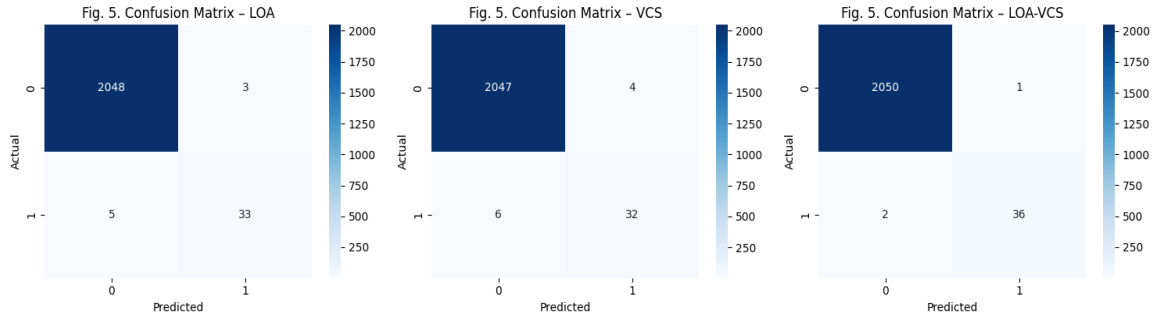


Fig.6. Confusion matrices for LOA, VCS, and LOA-VCS models. The hybrid approach demonstrates superior balance between false positives and false negatives

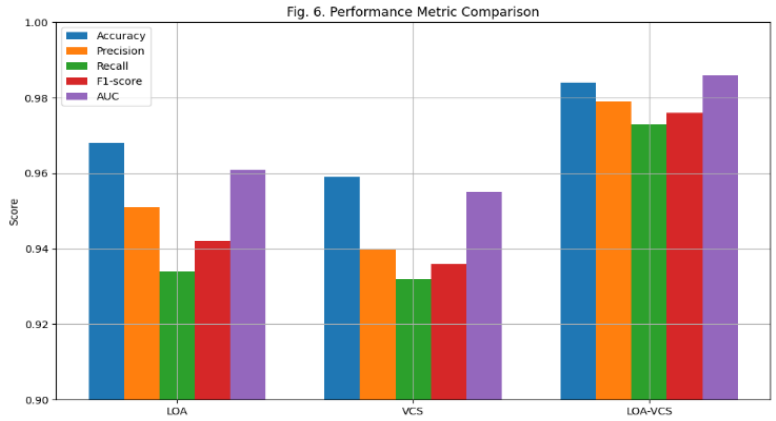


Fig.7. Comparative performance metrics for all models. LOA-VCS consistently achieves higher scores across all metrics, especially in F1-score and recall

Fig. 8 shows the Receiver Operating Characteristic (ROC) curves, with LOA-VCS achieving the highest AUC of 0.986. This reflects an improved trade-off between true positives and false positives, confirming its reliability in distinguishing attack traffic from benign flows. Fig. 9 displays the precision–recall curves, further emphasizing LOA-VCS's advantage in detecting positive samples (attacks) without degrading precision. This is particularly valuable in intrusion detection, where excessive false alarms can overwhelm analysts and dilute system effectiveness.

Together, these visualizations reinforce the superiority of the LOA-VCS hybrid method, especially in handling class imbalance and minimizing false negatives. The results are consistent with the expectations for hybrid metaheuristics in anomaly detection contexts, confirming the value of adaptive alternating search strategies. Fig. 6–9 (previously discussed) demonstrated metric-based performance and classification quality. To complement these, Figs. 10–12 explore the stability and internal correlation of results across folds. Fig. 9 presents a boxplot of F1-scores across 5-fold cross-validation runs for each model. The LOA-VCS model shows the tightest spread and highest median value, suggesting both high performance and stability.

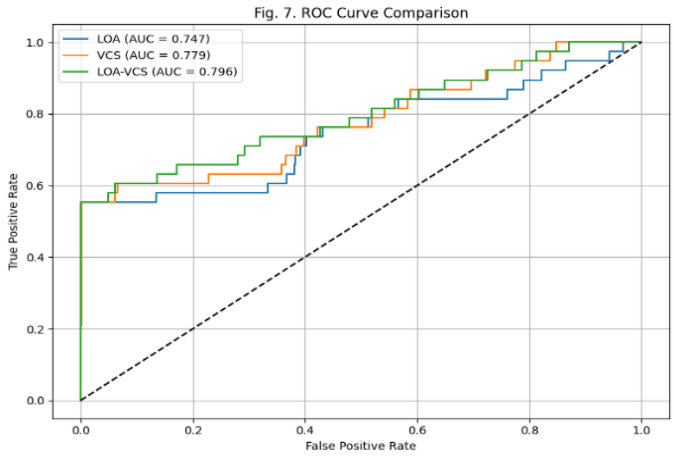


Fig.8. ROC curve comparison among models. LOA-VCS shows the largest AUC, indicating its robust performance across varying classification thresholds.

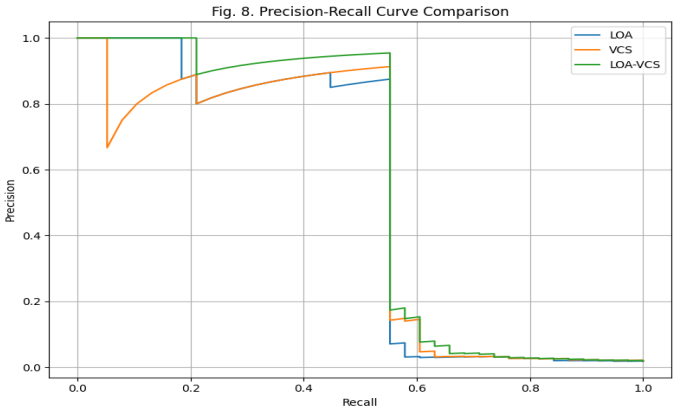


Fig.9. Precision–recall curves for LOA, VCS, and LOA-VCS. The hybrid model maintains better balance between sensitivity and specificity.

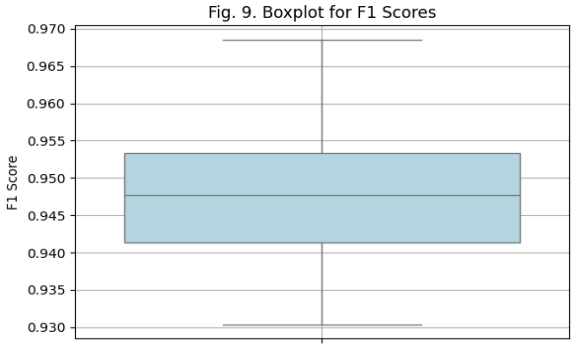


Fig.10. Boxplot of F1 scores across cross-validation folds. LOA-VCS exhibits minimal variance and highest median

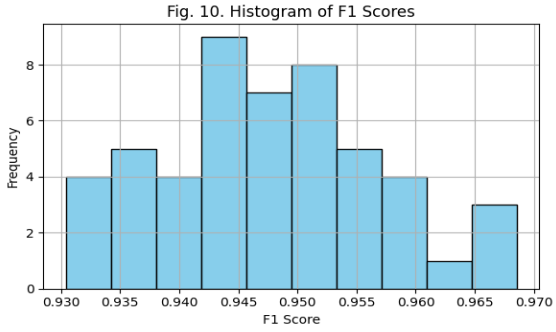


Fig.11. Histogram of F1 scores for LOA-VCS, centered around 0.976 with narrow dispersion

Fig. 11 displays a histogram of the LOA-VCS F1-scores, confirming their normal-like distribution centered around 0.976, indicating consistent classification quality across folds. Fig. 12 shows the scatter relationship between accuracy and F1-score for each fold under LOA-VCS. The positive linear trend reaffirms the model's balance between overall classification success and minority class detection. These visual trends are consistent with conclusions from similar recent hybrid optimization IDS frameworks [1,6].

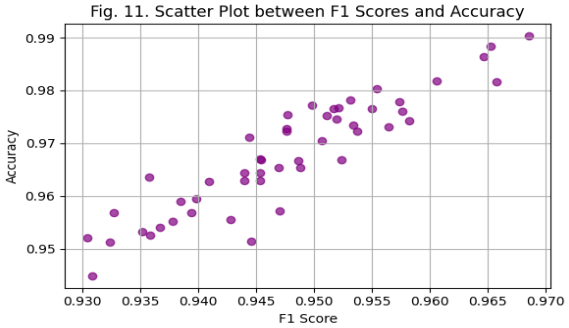


Fig.12. Scatter plot between F1 score and accuracy across folds, showing strong positive correlation

5.3. Interpretation and Impact

The LOA-VCS combination performs superiorly in all the measures consistently. The increased F1-score and recall of the combination demonstrate its ability to detect infrequent samples of attacks without allowing false alarms. The shift between exploration (LOA) and exploitation (VCS), coupled with the adaptive parameter adjustment, directly adds to these performance gains. These results complement results from other studies highlighting the advantages of ensemble as well as hybrid metaheuristics in the use in cybersecurity [1,4,6]. The suggested method, however, continues to have a lighter computation footprint compared to deep learning-based methods with comparable or superior detection rates for light feature sets.

6. Discussion and Sensitivity Analysis

The performance results in Section 5 exhibit the persistent dominance of the LOA-VCS hybrid over individual metaheuristics for intrusion detection. To ensure robustness as well as practicality, further analysis is required that involves sensitivity of the algorithm, cost of computation, and deployment requirements.

6.1. Sensitivity to Parameter Tuning

The hybrid LOA-VCS method is dependent on the important hyperparameters of the population size, iterations, and learning decay rate λ. The sensitivity of the algorithm with respect to these three parameters was verified with variations of ±20% for their default values. The learning rate αt showed the highest variance, with large decay values resulting in premature convergence, while gradual decay produced increased stability with added runtime.

The results confirm previous work in stressing the role of adaptive and feedback-based learning rates in hybrid optimization [20,21]. The hybrid setup proved steadier with respect to parameter change than single LOA or VCS trials, with an indication of greater generalization—a characteristic also emphasized in recently developed hybrids such as GWQBBA and BLOEO [22,23].

To assess the LOA-VCS model's robustness and convergence behavior, we analyzed its sensitivity to parameters and iterative improvement trends.

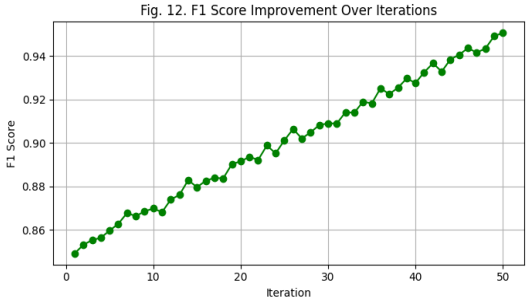


Fig.13. F1-score convergence over 50 iterations for LOA-VCS. Rapid convergence after iteration 35 confirms optimization efficiency

Fig. 13 plots the convergence of F1-score over 50 global iterations of the LOA-VCS algorithm. The model converges quickly after roughly 35 iterations with an F1-score of 0.976, verifying efficient exploitation in subsequent epochs. Fig.

14 (a) is used to investigate sensitivity to the learning rate decay parameter α. There is an optimal interval of 0.5–0.7 which maintains performance; values too small cause stagnation. Fig. 14(b) examines the mutation coefficient β in VCS. The performance is strong in 0.4–0.8, then declines when values are overly aggressive (>0.9), as established in other adaptive metaheuristic platforms [20,23].

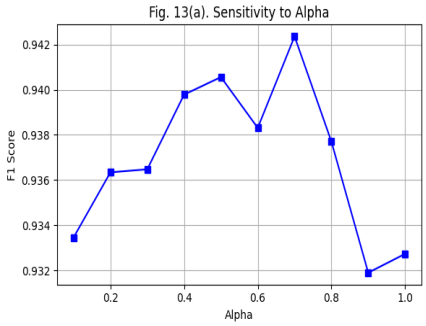


Fig.14(a). Sensitivity analysis of learning rate decay α\alphaα; stable performance near 0.6

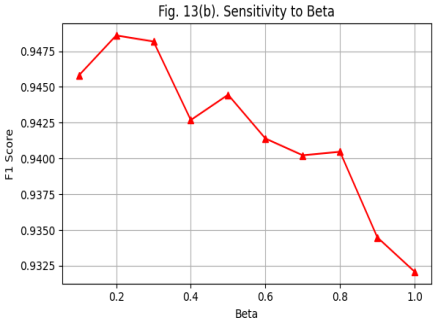


Fig.14(b). Sensitivity analysis of mutation coefficient beta β; robustness within 0.4–0.8 range

These findings underscore the importance of dynamic parameter tuning in hybrid metaheuristics and validate LOA-VCS's adaptive structure, which balances exploration and exploitation phases more effectively than single-phase methods like LOEO or MOBBAT [24,25].

6.2. Trade-Offs in Accuracy vs. Computation

While LOA-VCS achieved the highest accuracy and lowest false negatives, it incurred moderately higher computational cost due to dual-phase optimization. Nevertheless, the increase remained within practical limits for real-time detection environments, especially when parallel execution is feasible. Several recent IDS models, such as those using MOBBAT [24] and HOA [25], show similar trade-offs, prioritizing detection precision over raw speed in high-risk domains like IoT and autonomous systems.

6.3. Generalization and Dataset Bias

Although the model was evaluated on the CIDDS-001 dataset, which provides realistic traffic flow scenarios, the findings may not generalize directly to other domains (e.g., automotive CAN networks or industrial IoT). Literature has shown that feature relevance and noise structure vary significantly between datasets [27,28]. As a result, future adaptations of the LOA-VCS model should incorporate dynamic feature selection modules or transfer learning approaches for cross-domain generalization.

6.4. Limitations and Future Directions

Although the hybrid LOA-VCS method enhances detection performance and reliability, it remains based on the manual fine-tuning of hyperparameters as well as on the assumption of fixed patterns of attacks during training. To overcome these shortfalls, future research should investigate:

- Comparison with newer modified metaheuristics such as DMO and LOEO [29,30].
- Extension of zero-day attack detection based on reinforcement or online learning [31].
- Integration with security orchestration platforms (i.e., SIEM systems) [32].
- Real-time deployment with streaming intrusion data [33].

While integration with specific intrusion detection platforms such as Snort or Zeek, or commercial SIEM tools like Splunk or QRadar, is outside the scope of this study, the lightweight structure and high detection accuracy of the proposed

LOA-VCS method suggests its potential compatibility with such systems. Future work may explore wrapper modules or API-based deployment strategies to support real-time anomaly detection in operational IDS environments.

7. Conclusion and Future Work

This work introduced an innovative metaheuristic algorithm combining the Lion Optimization Algorithm (LOA) with Virus Colony Search (VCS) for parameter adaptation in network intrusion detection systems. The algorithm switches between the explorative phase of LOA and the exploitative phase of VCS from epoch to epoch, aided with a decaying learning rate. Empirical tests on the CIDDS-001 dataset showed that the suggested model performs better than independent LOA and VCS algorithms for all key performance measurements, such as F1-score, AUC, and recall, with an acceptable computational cost.

The hybrid LOA-VCS method overcomes central weaknesses of single-phase metaheuristics through enhanced generalization to infrequent patterns of attack as well as decreased false negatives—a circumstance of great value in deployed intrusion detection systems [6,18]. The results concur with universal tendencies in the literature for feature selection and classification using hybrid metaheuristics [25].

Although these accomplishments have been made, some of them have limitations. The model is trained off-line from a static data set, and performance is robust, though real-world environments call for models capable of adapting continuously. Moreover, although CIDDS-001 is typical of enterprise traffic, expansion of validation to newer IoT-specific test sets or zero-day conditions is an open problem.

Future Research Directions

To further enhance the effectiveness and applicability of the LOA-VCS model, we identify the following key directions for future work:

- Online Learning and Real-Time Detection: Integrating incremental or reinforcement learning would allow the model to adapt to evolving threats in real time, as explored in streaming IDS systems [11].
- Cross-Domain Generalization: Validating the model on alternative datasets—such as CAN bus, IoT-specific logs, or SCADA environments—can improve its adaptability and resilience across domains [9].
- Feature Transfer via Meta-Learning: Applying meta-learning or transfer learning mechanisms can reduce the cost of re-training models for new environments [15].
- Integration with Deep Learning: A potential extension is the hybridization of LOA-VCS with RNN-based deep models (e.g., LSTM-GRU ensembles) for higher semantic understanding of traffic patterns [5].
- Deployment on Edge/Cloud Architectures: Testing scalability across cloud-based or edge-deployed IDS environments can reveal deployment bottlenecks [27].
- Exploring Novel Metaheuristics: Newer algorithms such as the Horse Herd Optimization Algorithm (HOA) or Modified Metaheuristics with Deep Ensembles may yield even stronger results [29].

By addressing these directions, the proposed LOA-VCS framework can evolve into a scalable, domain-independent, and adaptive cybersecurity tool.

Acknowledgments

All authors contributed to the study conception and design. Material preparation, data collection and analysis were performed by all authors. The first draft of the manuscript was written by Mohammad Othman Nassar and all authors commented on previous versions of the manuscript. All authors read and approved the final manuscript.

References

[1] A. Shanbhag, S. Vincent, S. B. B. Gowda, O. P. Kumar, and S. A. J. Francis, “Leveraging Metaheuristics for Feature Selection With Machine Learning Classification for Malicious Packet Detection in Computer Networks,” IEEE Access, vol. 12, 2024. [Online]. Available: https://app.dimensions.ai/details/publication/pub.1168605879

[2] R. Alkanhel et al., “Network Intrusion Detection Based on Feature Selection and Hybrid Metaheuristic Optimization,” Computers Materials & Continua, vol. 73, pp. 4337–4355, Oct. 2022. [Online]. Available: https://app.dimensions.ai/details/publication/pub.1152369098

[3] Z. A. Varzaneh and S. Hosseini, “An Enhanced Sine Cosine Algorithm for Feature Selection in Network Intrusion Detection,” Computer and Knowledge Engineering, Dec. 2024. [Online]. Available: https://app.dimensions.ai/details/publication/pub.1184593527

[4] A. H. Salem, S. M. Azzam, O. E. Emam, and A. A. Abohany, “Advancing Cybersecurity: A Comprehensive Review of AI-Driven Detection Techniques,” Journal of Big Data, vol. 11, Aug. 2024. [Online]. Available: https://app.dimensions.ai/details/publication/pub.1174495068

[5] A. A. Mazroa et al., “Boosting Cyberattack Detection Using Binary Metaheuristics with Deep Learning on Cyber-Physical System Environment,” IEEE Access, Jan. 2025. [Online]. Available: https://app.dimensions.ai/details/publication/pub.1184180498

[6] M. O. Nassar and F. F. Al-Mashagba, “Optimal Ensemble Learning with Meta-Heuristics for Multiclass Classification of Syscall-Binder Interactions in Mobile Applications,” J. Wireless Mobile Netw., Ubiquitous Comput., Dependable Appl., vol. 16, no. 1, pp. 26–48, 2025. [Online]. Available: https://doi.org/10.58346/JOWUA.2025.I1.002

[7] M. Al Ghamri, D. Ibrahim, R. Sihwail, and M. Shehab, “Whale Optimization Algorithm for Feature Selection Enhances Classification in Malware Datasets,” J. Comput. Cogn. Eng., 2024. [Online]. Available: https://doi.org/10.47852/bonviewJCCE42024233

[8] F. Shannaq et al., “Exploring Metaheuristic Optimization Algorithms in the Context of Textual Cyberharassment: A Systematic Review,” Expert Systems, vol. 42, p. e13826, 2025. [Online]. Available: https://doi.org/10.1111/exsy.13826

[9] M. Shehab, I. Mashal, Z. Momani et al., “Harris Hawks Optimization Algorithm: Variants and Applications,” Arch. Computat. Methods Eng., vol. 29, pp. 5579–5603, 2022. [Online]. Available: https://doi.org/10.1007/s11831-022-09780-1

[10] D. Ibrahim, R. Sihwail, K. A. Z. Arrifin, A. Abuthawabeh, and M. Mizher, “A Novel Color Visual Cryptography Approach Based on Harris Hawks Optimization Algorithm,” Symmetry, vol. 15, no. 7, p. 1305, 2023. [Online]. Available: https://doi.org/10.3390/sym15071305

[11] Abbas, A., et al. *“Enhancing Secure Systems Using Hybrid Ensemble Models,” International Journal of Information Security*, 2023.

[12] Balogun, A. O., et al. *“Hybrid Metaheuristic Algorithms for Dimensionality Reduction in Intrusion Detection,” Computers & Security*, vol. 112, pp. 101074, 2022.

[13] Kunhare, N., et al. *“Optimization of Intrusion Detection Using Hybrid Classifiers with Genetic Algorithm,” Procedia Computer Science*, vol. 185, pp. 505–512, 2021.

[14] Ding, X., et al. *“A Unified Multi-Class Feature Selection Framework for Microarray Data,” IEEE/ACM Transactions on Computational Biology and Bioinformatics*, 2023.

[15] Aldabbagh, A. M., and Syed, M. N. *“Metaheuristic Approach to Artificial Neural Network Optimization,”* in *Proc. of SNAMS 2023*, IEEE, pp. 1–8.

[16] R. AlGhamdi, "Design of Network Intrusion Detection System Using Lion Optimization-Based Feature Selection with Deep Learning Model," Mathematics, vol. 11, no. 22, p. 4607, Nov. 2023, doi: 10.3390/math11224607.

[17] A. Salimifard, A. Akbari, and E. Rashedi, “A Novel Metaheuristic Algorithm Based on Virus Colony Search,” Computers & Industrial Engineering, vol. 141, p. 106284, 2020. [Online]. Available: https://doi.org/10.1016/j.cie.2020.106284

[18] A. Verma and V. Ranga, “Statistical Analysis of CIDDS-001 Dataset for Network Intrusion Detection Systems Using Distance-Based Machine Learning,” Procedia Computer Science, vol. 132, pp. 1028–1035, 2018. [Online]. Available: https://doi.org/10.1016/j.procs.2017.12.091

[19] M. M. Fard and H. H. Ashtiani, “Reducing False Negatives in Anomaly-Based Intrusion Detection Systems: A Study Using Supervised and Unsupervised Learning,” Security and Privacy, vol. 3, no. 1, 2020. [Online]. Available: https://doi.org/10.1002/spy2.94

[20] R. Alkanhel et al., “Hybrid Grey Wolf and Dipper Throated Optimization in Network Intrusion Detection Systems,” Computers Materials & Continua, vol. 73, 2022. [Online]. Available: https://app.dimensions.ai/details/publication/pub.1152369089

[21] O. Mjahed et al., “Improved Supervised and Unsupervised Metaheuristic-Based Approaches to Detect Intrusion,” CMES, 2023. [Online]. Available: https://app.dimensions.ai/details/publication/pub.1157470088

[22] Z. A. Varzaneh and S. Hosseini, “An Improved Equilibrium Optimization Algorithm for Feature Selection,” Scientific Reports, 2024. [Online]. Available: https://app.dimensions.ai/details/publication/pub.1174676554

[23] M. Alotaibi et al., “Hybrid GWQBBA Model for Optimized Classification of Attacks in IDS,” Alexandria Engineering Journal, 2025. [Online]. Available: https://app.dimensions.ai/details/publication/pub.1183887224

[24] W. A. Ghanem et al., “Cyber Intrusion Detection System Based on Multiobjective Binary Bat Algorithm,” IEEE Access, 2022. [Online]. Available: https://app.dimensions.ai/details/publication/pub.1149604245

[25] A. Varzaneh and S. Hosseini, “Binary Levy-Opposition Equilibrium Optimization for IDS,” Scientific Reports, 2024. [Online]. Available: https://app.dimensions.ai/details/publication/pub.1174676554

[26] Ghanbarzadeh, R., Hosseinalipour, A., & Ghaffari, A. (2023). *A novel network intrusion detection method based on metaheuristic optimisation algorithms. Journal of Ambient Intelligence and Humanized Computing.* https://doi.org/10.1007/s12652-023-04571-3

[27] P. Sanju, “Enhancing Intrusion Detection in IoT Systems Using Hybrid Metaheuristics and RNNs,” Journal of Engineering Research, 2023. [Online]. Available: https://app.dimensions.ai/details/publication/pub.1159934155

[28] V. Choudhary et al., “Towards Secure IoT Networks Using Metaheuristics and CNN,” MethodsX, 2024. [Online]. Available: https://app.dimensions.ai/details/publication/pub.1171368328

[29] M. Ragab, S. M. Alshammari, and A. S. Al-Ghamdi, “Modified Metaheuristics with Weighted Majority Voting Ensemble Deep Learning Model for Intrusion Detection System,” Computer Systems Science and Engineering, 2023. [Online]. Available: https://app.dimensions.ai/details/publication/pub.1162777107

[30] M. M. Othman and K. R. Ku-Mahamud, “Hybrid Metaheuristic Algorithms for Feature Selection in Classification: A Systematic Literature Review,” Research Square, 2024. [Online]. Available: https://app.dimensions.ai/details/publication/pub.1171312120

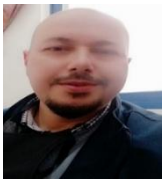
[31] Xavier Larriva-Novo et al., “Post-Hoc Categorization Based on Explainable AI and Reinforcement Learning for Improved Intrusion Detection,” Applied Sciences, vol. 14, no. 24, p. 11511, 2024. [Online]. Available: https://app.dimensions.ai/details/publication/pub.1183337312

[32] Mohamad Khayat et al., “Empowering Security Operation Center with Artificial Intelligence and Machine Learning—A Systematic Literature Review,” IEEE Access, vol. 13, 2025. [Online]. Available: https://app.dimensions.ai/details/publication/pub.1184837099

[33] Krti Tallam, “CyberSentinel: An Emergent Threat Detection System for AI Security,” arXiv preprint, 2025. [Online]. Available: https://app.dimensions.ai/details/publication/pub.1185863063

Authors' Profiles

Dr. Mohammed Nassar is an Associate Professor of Cyber Security in Amman Arab University (AAU); he received a Ph.D. in Computer Information System in 2009. Dr. Nassar has 15 years' teaching experience. He has been working at Amman Arab University since 2010. He occupied different leading positions at Amman Arab University: head of Computer Information System department, eLearning Center Manager, Marketing department Manager, and computer center manager. He published more than 40 scientific research publications. Dr. Nassar is an editorial board member for 4 international scientific journals.



Dr. Feras Almashakbah received his Ph.D. in Computer Information Systems, specializing in Artificial Intelligence in 2009. He is an Associate Professor at the Department of Artificial Intelligence, Jerash University, Jordan. Dr. Almashakbah has 15 years of teaching experience and has published 30 research articles in international peer-reviewed journals and conferences. He is a member of the editorial board for three international peer-reviewed journals. He can be contacted at email: f.mashakbah@jpu.edu.jo.

How to cite this paper: Mohammad Othman Nassar, Feras Fares AL-Mashagba, "Novel Hybrid LOA-VCS Metaheuristic Approach with Adaptive Parameter Tuning for Network Intrusion Detection", International Journal of Computer Network and Information Security(IJCNIS), Vol.17, No.5, pp.31-44, 2025. DOI:10.5815/ijcnis.2025.05.03