Development of an Enhanced Intrusion Detection System Framework Using Walrus Optimization Algorithm for Support Vector Machine Parameter Tuning

Michael Olugbenga ABOLARINWA[1], Olufemi Olayanju AWODOYE[2], Adegbola Isaac OLADIMEJI[3], Olajide Yusuf ADEBAYO[4]
[1]Department of Computer Science, Federal University of Agriculture and Developmental Studies, Iragbiji, Nigeria
[2]Department of Computer Engineering, Ladoke Akintola University, Ogbomosho, Nigeria
[3]Department of Information Technology and Health Informatics, Federal University of Health Sciences, Azare, Nigeria
[4]Department of Data Science, Osun State University, Osogbo. Nigeria
michael.abolarinwa@fuadsi.edu.ng, ooawodoye50@lautech.edu.ng, oladimeji.adegbola@fuhsa.edu.ng, olajide.adebayo@uniosun.edu.ng

Abstract: The intrusion detection system (IDS) plays a vital role in modern cybersecurity by identifying unauthorized activities on a network and supporting protective responses. However, traditional IDS approaches face difficulties when dealing with complex data and sophisticated attack methods, leading to lower detection accuracy and an increase in false positives. This study introduces a new framework that combines the Walrus Optimization Algorithm (WaOA) with Support Vector Machine (SVM) classifiers to enhance the performance of SVM-based IDS, which is very sensitive to both the choice of useful feature selection and hyperparameter optimization. Suboptimal feature selection and poor hyperparameters may lead to overfitting, higher computational cost, and poor detection results. By integrating the WaOA and SVM in order to optimize SVM hyperparameters, the framework aims to boost SVM efficiency while reducing computational complexity. The CICIDS2017 dataset will be used as our input data, while the implementation will be done using MATLAB programing language. The evaluation of the experiment will be done by comparing the results of the enhanced WaOA_SVM with those of the standard SVM. The study will investigate whether hyperparameter optimization using WaOA can improve classification performance and operational efficiency compared with a standard SVM.

Keywords: Accuracy, Cybersecurity, False Positives, Intrusion Detection System, Support Vector Machine.

INTRODUCTION

New and more complicated cyberattacks have emerged as a result of rapidly growing and proliferating network technologies, particularly the Internet of Things (IoT) (Ashraf, Aryal et al., 2025). With the increasing digitization of infrastructures, the frequency

https://doi.org/10.54851/v8i2y202605

and sophistication of cyberattacks are increasing, which poses a restriction on the use of traditional security mechanisms (Pinto, Herrera, Donoso, Gutierrez. 2023).

This study proposes an enhanced WaOA-SVM IDS framework in which WaOA will be employed specifically to optimize SVM hyperparameters rather than primarily performing feature selection. The objective of WaOA will therefore be not simply to train the SVM, but to search for a combination of SVM parameters that minimizes the classification error or maximizes a selected performance measure. The study will systematically investigate whether WaOA can identify a SVM configuration that improves IDS performance, reduces false-positive errors, and provides a favourable computational trade-off compared to standard SVM parameterization. The study will use the CICIDS2017 dataset for multiclass network attack detection and will also investigate whether the hybrid model can significantly outperform the standard SVM model approach, as the sample literature reveals that the use of metaheuristic optimization algorithms for the field of feature selection improve the work of the IDS is widely studied. Some of the methods have shown substantial improvements; however, they are trapped in local optima and premature convergence, such as Genetic Algorithm (GA), Particle Swarm Optimization (PSO), and Ant Colony Optimization (Geng, Y., Li, Y., and Deng, C., 2024)[3]. Thus, the research focus recently has been on the development of nature-inspired optimization methods that have a better exploration and exploitation ratio (Xie, J., Wu, H., and Zhao, Y., 2024).

An IDS is one of the most important ways to secure network infrastructure from malicious attacks by monitoring all traffic, detecting malicious activity, and alerting on it immediately. However, traditional IDS is not suitable for large and high-dimensional data and dynamism, which reduces detection accuracy and increases the false positive ratio (Mobolaji etal., 2025). These challenges have been tackled by the extensive implementation of ML-based methods. One of the ML methods is SVM, which has a good learning ability in classification, regression, and prediction. It has emerged as one of the top methods in ML due to its learning performance. SVM is based on statistical learning theory, a systematic approach to ML in the context of finite samples. It is based on Vapnik–Chervonenkis (VC) dimension theory and the structural risk minimization principle, and can effectively solve the curse of dimensionality problem by using a kernel function (Wang et al., 2017). But the effectiveness of SVM-based IDS is highly dependent on hyperparameter optimization. Poor hyperparameter optimization can result in overfitting, computation cost, and may give poor detection results (Isam et al 2026).

WaOA is another recently developed bio-inspired metaheuristic, which simulates the social interaction of foraging and socializing of walruses (Wang et al., 2017). Therefore, WaOA is an effective solution to high-dimensional optimization problems and is developed to have adaptive search strategies to guarantee the convergence stability and the diversity of solutions (Geng et al., 2024). Empirical studies have shown that WaOA outperforms several of the classic optimization algorithms in feature selection, as well as the accuracy of classification in ML security applications (Bahmaid et al., 2024). A hybrid model of SVM and WaOA is proposed to overcome the drawbacks of both algorithms. This model is based on using WaOA_SVM to optimize its parameters to improve the accuracy of IDS and significantly reduce the false negative rate.

The remainder of the paper is organized as follows. The *Literature review* section presents related work on IDS and optimization-based methods. The *Proposed materials and methods* section describes the proposed architecture, including the dataset, preprocessing, SVM parameter optimization, and classification methodology. The *Expected results* section outlines the expected results of the experiment. Finally, the Conclusion

section summarizes the research findings and provides recommendations for future work.

LITERATURE REVIEW

IDS are integral components of cybersecurity that detect and thwart malicious behavior in networked systems. The accuracy and efficiency of IDS have been a subject of research interest, and several methods like ML, deep learning (DL), and optimization-based methods have been proposed and applied. Diana et al., (2025) present a survey of IDS technologies for network security; feature selection techniques, the SVM, and WaOA in IDS are covered. The researcher explores traditional and modern developments. It also includes a survey of the IDS architecture and types, major detection mechanisms, data and environment, and implementation in today's network environment, such as cloud computing, virtualized environment networks, Internet of Things, and industrial control systems. He also talks about the difficulties with IDS and a novel hybrid algorithm using ML. Osman et al., (2025) introduced a method to increase the precision of the model and classification. He applied the RF model to feature selection and SVM for final classification. The hybrid model was applied to complex data to measure the accuracy, precision, recall, and F1 score.

The performance evaluation indicates that the hybrid model has an accuracy of 99.89% and an F1 score and precision of 99.93%, respectively. This indicates that the RF-SVM model has great potential for optimizing predictive models and the decision-making process. Bahmaid and Ghaleb (2024) proposed a hybrid Intrusion Detection System that relies on a Chaotic Walrus Optimization-driven Convolutional Echo State Network (CWO-CESN) for IoT-assisted Wireless Sensor Networks (WSNs). The model is composed of Convolutional Neural Networks (CNNs) and Echo State Networks (ESNs), and its optimization was carried out using a chaotic map-based WaOA. The method's effectiveness in complex and resource-limited environments is demonstrated by the high detection accuracies of 99% and 99.5% in NSL-KDD and WSN-DS datasets, respectively, and 99.8% with the assistance of WaOA in the IoT-23 dataset. In (Ngueajio, et al., 2022), a comprehensive survey on SVM-based IDS has been conducted and tested on both NSL-KDD and KDD Cup 99 datasets. The paper provides a comparative discussion about different IDS models that have been implemented with SVM classifiers, including their performance indicators, advantages, and drawbacks. The results demonstrated the power and flexibility of SVM-based IDS and indicated some limitations in terms of scalability, feature selection, and computational efficiency, thus establishing the need for simplified and efficient architectures for hybrid detection.

Despite these advancements, there is limited research that has explored the combination of WaOA-SVM classification for IDS with modern-day datasets, which further emphasizes the Employment of WaOA specifically to optimize the principal SVM hyperparameters rather than primarily performing feature Selection

Benchmark Datasets for Intrusion Detection

Benchmark datasets are critical to the testing of the performance of IDSs. Some popular datasets are KDD Cup 99, NSL-KDD, CICIDS2017, and UNSW-NB15 (Pinto, A., Herrera, L., Donoso, Y., Gutierrez J. A., 2023) [2] etc. While KDD Cup 99 is widely used, it has problems of being redundant and strongly imbalanced. The NSL-KDD dataset overcomes some of these shortcomings by eliminating duplicate records and enhancing data distribution (Geng et al., 2024). More recent datasets, like CICIDS2017 and UNSW-NB15, contain realistic and up-to-date traffic scenarios, which are more appropriate for recent IDS research (Xie et al., 2024).

NEW TRENDS IN NETWORK SECURITY THREAT DETECTION.

IDS should never stand still since cyber threats are ever-changing. The advent of Adversarial Machine Learning (AML) has demonstrated that such attacks can be devised that are specifically targeted to evade an ML-based IDS, exposing its weaknesses in traditional detection models (Mobolaji et al., 2025). In an attempt to overcome these issues, newly developed studies investigated Federated Learning (FL) and blockchain-based IDS models as means of security and privacy protection, as well as demonstrating trust in a distributed setting (Xie et al., 2024). Those technologies can be used to achieve decentralized model training, secure data sharing, and collaborative threat intelligence, and minimize the risks of having centralized data processing. Combined, these trends suggest a rise in designs for IDS that are more resilient, more private, and more collaborative, with the ability to adequately address current cyber threats.

PROPOSED MATERIALS AND METHODS

The Intrusion Detection System framework will use the (WaOA) to optimize SVM hyperparameters for classification purposes. The CICIDS2017 Dataset will be utilized for the study. The following types of traffic will be considered in this research: BENIGN, DoS, DDoS, PortScan, Bot, and Brute Force. A stratified random sample of 1,500 instances will be selected to be large enough and representative in terms of computational efficiency and statistical representativeness. This kind of sampling will ensure that there is a proportional representation of each class of traffic and thus sampling error will be minimized by minimizing sampling bias. The study will improve an existing network IDS that gives a more discriminating characterization of cyberattacks. The study will also include an SVM classifier and WaOA in the optimization process for the detection of multiclass intrusion using the MATLAB programming language, as displayed in Figure 1. The problem will be formulated as a binary classification problem in the classification exercise, with the distinction between network traffic, normal traffic, and malicious traffic. Then all the types of positive attack classes (DoS, DDoS, PortScan, Bot, Brute Force) will be merged to form a total of 1,050 attack (positive) samples, while BENIGN normal traffic will amount to 450 samples. The composition of the class will provide a balanced learning structure that will enable the model to capture discriminative patterns (attack traffic vs. non-attack traffic) positively. The SVM classifier will be the detection engine since it has the key feature of high-dimensional feature space generalization. Nonetheless, the hyperparameters are very sensitive to the performance of SVM. To overcome automatic parameter tuning limitations, the most important SVM parameters will be tuned automatically using the WaOA. To determine the best combinations of parameters that can equip WaOA to achieve maximum detection accuracy with minimum false alarms, WaOA will undertake an iterative process of searching for the best parameter combinations. Finally, after optimization, the proposed WaOA-SVM model will be tested using the standard evaluation metrics of the IDS, such as accuracy, precision, recall, F1-score, and false-positive rate, to have a comprehensive overview of the ability of the IDS to detect malicious behavior in the network.

The main objectives of the system are to have the highest detection rate and the lowest false-positive rate. The overall proposed architecture of the IDS can be observed in Figure 1: The selected data set will be broken into parts, data preprocessing will be performed, the WaOA will optimize SVM hyperparameters, and then the performance will be evaluated.

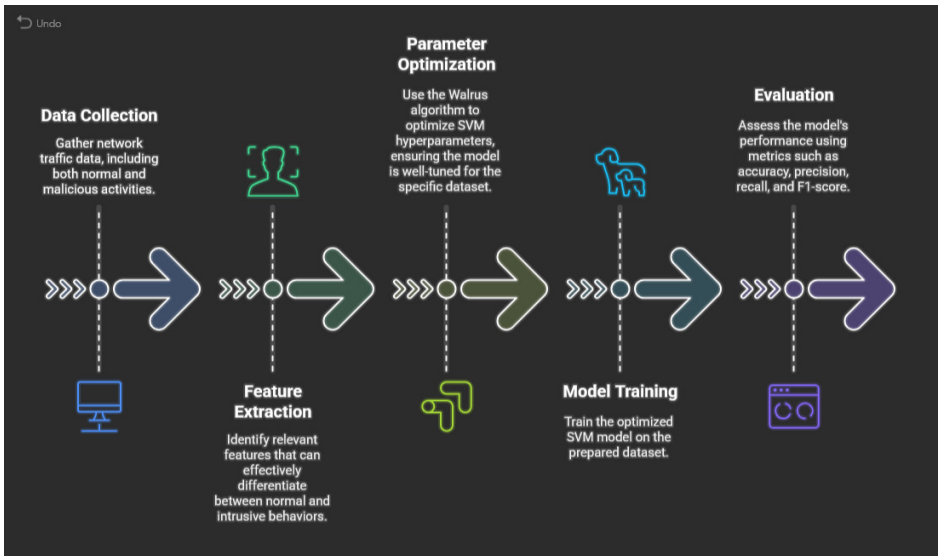


Figure 1. *Schematic Diagram of Walrus Optimized SVM for IDS Process*

The framework will be used to select and optimize malicious features in an IDS modeling process and provides a new methodological approach to solving the type of attack that was not previously addressed.

Dataset Description

The selection of the right dataset is crucial when evaluating IDS. Many benchmark datasets have been applied for IDS research, like KDD Cup 99, NSL-KDD, CICIDS2017, and UNSW-NB15. The CICIDS2017 dataset is chosen in this study because it includes the capability to simulate contemporary network traffic realistically and a variety of scenarios of contemporary cyberattacks. The wide variety of attack types offered by CICIDS2017 makes it suitable to evaluate IDS performance in real-life conditions, such as DoS, DDoS, PortScan, Bot, and Brute Force types of attacks. The dataset represents the network traffic of real user activities as well as attack activities; hence, it will offer a good reference point in the research of IDS. The broad coverage of features and the up-to-date attack patterns will ensure that the evaluation will be based on real-life applications.

The CICIDS2017 dataset is a descriptive characterization of network traffic, which is based on more than 80 flow-based attributes that are extracted from the bidirectional network flows. All these features are the statistical, temporal, and behavioral characteristics of network traffic and are widely employed in the analysis of IDS. Typical examples of the flow features are flow duration, total number of forward or backward packets, total packet length, average packet size, flow bytes per second, flow packets per second, number of TCP flags (SYN, ACK, FIN, RST), ratio of downlink/upstream, and protocol-specific features (with class labels). There are four types of features which can be extracted: (i) Basic flow features, providing basic statistics of traffic; (ii) Content-based features, related to interaction at the application-layer; e.g. HTTP and DNS behavior; (iii) Time-based features, modeling traffic dynamism in terms of rate-based measurements; (iv) Protocol level activities, defined by behavioral features, indicating protocol level activities based on TCP flag statistics. Although this rich feature set can be used to improve the detection capability, the high dimensionality

of the features and redundancy can cause the computational complexity to increase and low generalization performance when used directly by the ML classifiers. To solve this problem, the WaOA will be used to optimize the SVM classifier hyperparameters. The proposed IDS framework is a proposed methodology by the given optimisation process, which optimizes SVM hyperparameters to improve classification and enhances detection performance.

Data Preprocessing

Effective preprocessing of network traffic data is one of the crucial steps to improve the power and prediction ability of ML-based IDSs. The raw information of CICIDS2017 is noisy, with missing data, duplicate data, and features in different scales, which may affect the classification result. To address the above-mentioned issues, we will perform full preprocessing, which involves data cleaning, data normalization, and data balancing

Data Cleaning

The dataset will be exposed to a systematic data-cleaning process to improve the quality of data and ensure the reliability of subsequent model development. Missing values in the numerical attributes would be handled using median imputation, which will provide a robust estimate of the central tendency and is less sensitive to extreme values and outliers than mean-based imputation. In addition, duplicate and redundant records will be identified and removed to minimize potential sampling bias and prevent repeated observations from disproportionately influencing the learning process. These cleaning procedures help improve the integrity of the training data and enhance the model's ability to generalize effectively to previously unseen patterns of network traffic.

Feature Normalization

Minmax normalization will be used for all numerical features to achieve the same level of scale for features and enhance the convergence of the classifier using the following equation:

$$X' = «X\text{-}Xmin « / » Xmax\text{-}Xmin» \quad (1)$$

This normalization procedure will prevent elements from having big number ranges from dominating the learning procedure and boosts the working of SVM.

Data Balancing

The CICIDS2017 data set is imbalanced, with some classes having much fewer data samples than others. Imbalance can lead to classification bias where machine learning models tend to overlook the minority classes, which may lead to a decrease in the ability of the models to detect the minority attack categories. In order to avert this issue, the Synthetic Minority Oversampling Technique (SMOTE) method will be used to rebalance the training data. SMOTE creates synthetic samples for minority classes by interpolating between existing minority class samples, which adds samples to the classes without just copying observations. The technique was chosen because it is commonly applied in class imbalance problems in ML approaches for intrusion detection and can help the ML model to learn discriminative patterns from the minority classes in the attack classes. Importantly, SMOTE will be used only in the training dataset and not in the test set to avoid leakage and to keep the test set as an independent test set.

Classification

The proposed intrusion detection framework will be based on the classification stage, which uses an optimised Support Vector Machine (SVM) model, whose parameters

can be optimised using the WaOA. The most important aspect of the decision-making part of this optimised WaOA SVM model was its categorization of network traffic as either normal or malicious.

Support vector machine (SVM)

Supervised SVM is a ML technique that was widely used for binary and multi-class classifications because it has good generalization ability and has been found to be sensitive in high-dimensional feature spaces (Cortes et al., 1995). The SVM uses an optimal separating hyperplane, which is the closest plane to the maximum distance between the classes, which increases the accuracy of the classification and prevents overfitting.

SVM tries to solve an optimization problem to minimize the error of classification and maximize the margin between the classes, given a training sample set (x_i, y_i) where $x_i \in R^n$ is the input feature vector, and $\in \{-1,+1\}$ is the label of the classes. If the data are not linearly separable, the input data is mapped to a higher-dimensional feature space using kernel functions, which permits linear separation in the higher-dimensional space. Linear, polynomial, and radial basis function (RBF) kernels are quite common and can be used in a wide variety of applications.

In the proposed framework, the preprocessed feature set will be used to train the SVM classifier, while WaOA will be employed to optimize the selected SVM hyperparameters. Additionally, the important hyperparameters of SVM: the regularization parameter and parameters depending on the type of kernel, are automatically tuned with the aid of WaOA to make the detection more accurate and ensure a low rate of false positives. Through this integration, there will be better classification performance and computational efficiency in IDS tasks.

The dataset and all model parameters will be initialized in Algorithm 1; the feature vectors and corresponding class labels will be identified, and an initial population of walruses (candidate solutions) will be randomly generated. A single walrus will signify a possible solution that is an ensemble of SVM hyperparameters. The penalty factor C and the kernel function K will be set for the pre-defined search range. The main aim of the algorithm was to calculate the optimal SVM hyperparameters that will maximize classification accuracy and minimize computational complexity.

The WaOA is a nature-inspired search algorithm that is used to optimize the SVM hyperparameters. The SVM classifier is designed to create an optimal separating plane (hyperplane) with the greatest margin between different classes and a minimum classification error. For non-linearly separable data, it will employ kernel functions to map the input data into higher-dimensional feature spaces with improved class separability, such as Radial Basis Function (RBF), polynomial, and linear kernels. The optimization process requires solving the primal SVM problem (the one with the large number of parameters) by a dual approach, which can be optimally solved and guarantees an optimal decision boundary.

In order to do hyperparameter optimization, WaOA creates an initial population of candidate solutions pertaining to the various combinations of SVM parameters, mainly including the penalty factor C and parameters associated with the kernel. An SVM model will be learned and evaluated for each candidate solution, and the fitness of each solution is computed as the inverse of the classification accuracy. The fitness for the most suitable candidate solution is called the strongest walrus and will be used to guide the further optimization process. WaOA will be split into three consecutive optimization steps: Feeding Strategy, Migration and Escaping, and Fighting against predators. The candidate solutions update their positions at the Feeding Strategy (exploration phase), based on the most convincing walrus, thus promoting diversity and global search capability. The

Migration stage (combined exploration and exploitation) consists of moving walruses to areas of the search space where they might find better fitness values by adjusting hyperparameters. Lastly, the stage of Escaping and Fighting Against Predators (exploitation phase) conducts localized search operations to narrow down the hyperparameters in predetermined ranges.

This optimization process will then be repeated as long as the number of iterations is within the extremes. The fitness function will be achieved, or T will be reached. The ideal combination of the penalty factor C and kernel function, then K will be chosen, and the last SVM model will be trained with such optimised parameters.

The experimental evaluation will determine whether this approach can improve classification accuracy and reduce false positives compared with the standard SVM. The WaOA-SVM framework will combine WaOA with SVM, thus providing a superior IDS framework in real-time applications that will overcome standard SVM-based models, which depend on manual adjustments of the hyperparameters. The methodology proposed will be represented in Figure 2 through a graphic representation in the form of a flowchart that represents the main processes involved and how they relate to each other.

Classification

Optimised-WaOA_SVM will be employed for classification.

Algorithms of WaOA-SVM Optimisation

Algorithm 1. *Walrus Optimised Support Vector Machine Algorithm*

Step 1: Input - Dataset and Parameter Initialization

- Input: Dataset $D = \{(x_i, y_i)\}_{I_{-1}}^{m}$ with features $x_i \in R^n$ and labels $x_i \in \{-1, 1\}$
- Set the number of walruses *N* and the maximum iterations *T*
- Initialize walrus population (candidate solutions) with:
- Penalty factor (bounds: $C_{\min}, C_{\max}$)
- **Kernel function (RBF, Polynomial, Linear)

Step 2: Support Vector Machine (SVM) Formulation

SVM Objective Function

- SVM aims to find a hyperplane that maximizes the margin between classes. The objective function is:
- $\min_{w,b,\xi} \frac{1}{2}\|w\|^2 + C\sum_{i=1}^{m}\xi_i$
- subject to:
- $y_i(w^T x_i + b) \geq 1 - \xi, \xi_i \geq 0, \quad \forall i = 1, 2, ..., m$

where:

- $w \in R^n$: Weight vector of the separating hyperplane
- b: Bias term
- ξ_1: Slack variables (for soft-margin SVM)
- *C* : Penalty factor (regularization parameter, to be optimized)

Kernel Function (for Non-Linear SVM)

- SVM can use kernel functions to project data into a higher-dimensional space: $K(x_i, x_j) = \phi(x_i)^T \phi(x_j)$
- Common kernel functions:
- Linear kernel: $K(x_i, x_j) = x_i^T x_j$
- Polynomial kernel: $K(x_i, x_j) = (x_i^T x_j + 1)^d$
- RBF kernel: $K(x_i, x_j) = \exp f_0\left(-\frac{|x_i - x_j|^2}{2\sigma^2}\right)$

Dual Optimization Formulation

- Using Lagrange multipliers , the problem is rewritten as: $\max_{\alpha} \sum_{i=1}^{m} \alpha_i - \frac{1}{2} \sum_{i=1}^{m} \ddagger_{i=1} \alpha_i \alpha_j y_i y_j K(x_i, x_j)$

subject to: $\sum_{i=1}^{m} \alpha_i y_i = 0, \ 0 \le \alpha_i \le C$

where:

- α_4: Lagrange multipliers
- $K(x_i, x_j)$: Kernel function

Step 3: Walrus Optimization Algorithm (WaOA) for SVM

- Parameter Optimization
- Initialize Walrus Population
- Randomly generate candidate solutions:
- $W^{(0)} = \left\{ (C_j, K_j) \right\}_{j-1}^{N}$
- where:
- C_j is the penalty factor
- K_j is the kernel function

Step 4: Evaluate Fitness Function

- Train SVM for each candidate (C_j, K_j) using the inverse of classification accuracy as the fitness function:

where: $F_j = \frac{1}{\text{Accuracy}(C_j, K_j)}$

- Accuracy (C_j, K_j): Classification accuracy of SVM
- F_j: Fitness function (to minimize for best accuracy)

Step 5: Walrus Movement and Optimization

Phase 1: Feeding Strategy (Exploration)

- Calculate the new position of walrus *j*: $x_{i,j}^{(p_1)} = x_{i,j} + \text{rand}_{i,j}(SW_j - I_{i,j} \cdot x_{i,j})$

where:

- SW_j: Strongest walrus (best candidate solution)
- $I_{i,j}$: Interaction coefficient
- $x_{i,j}^{(p_1)}$: Updated position of the walrus
- Update walrus location: $X_i = \begin{cases} x_i^{(p_1)}, & if \quad F_i^{(p_1)} < F_i \\ X_i, & otherwise \end{cases}$

Phase 2: Migration (Exploration and Exploitation)

- Choose migration destination and calculate new location:

$$x_{i,j}^{(p_2)} = \begin{cases} x_{i,j} + rand_{i,j} \cdot (x_{k,j} - I_{i,j} \cdot x_{i,j}), & if \quad F_k < F_1 \\ x_{i,j} + rand_{i,j} \cdot (x_{i,j} - x_{k,j}), & otherwise \end{cases}$$

- Update walrus location: $X_i = \begin{cases} x_i^{(p_2)}, & if \ F_i^{(p_2)} < F_i \\ X_i, & otherwise \end{cases}$

Phase 3: Escaping and Fighting Against Predators (Exploitation)

- Calculate a new position using local bounds: $x_{i,j}^{(p_2)} = x_{i,j} + \left(lb_{(loman\, l_j)}^{t} + (ub_{(lan\, l_j, j)}^{t} - rand \cdot lb_{(lan\, l_j)}^{t}) \right)$
- Update walrus location: $X_i = \begin{cases} x_i^{(p_3)}, & if \ F_i^{(p_3)} < F_i \\ X_i, & otherwise \end{cases}$

Step 6: Convergence Check

- If maximum iterations *T* is reached or fitness function converges, stop.

Step 7: Output - Optimized SVM Parameters

- Optimal penalty factor C^*
- Optimal kernel function K^*
- Train the final SVM model using (C^*, K^*)

Evaluation Metrics

The metrics that were used to evaluate the performance of the proposed IDS include:

1. Accuracy (ACC): Tests the general correctness of classification.

$$ACC=\frac{TP+TN}{TP+TN+FP+FN} \quad (2)$$

2. Precision (P): This measures the percentage of attacks that were predicted correctly against the total number of attacks that were predicted.

$$P=\frac{TP}{TP+FP} \quad (3)$$

3. Recall (R) / Detection Rate (DR): Measures the rate of correctness of the attack detection.

$$R=\frac{TP}{TP+FN} \quad (4)$$

4. F1-Score: A weighted average of precision and recall.

$$F_1=\frac{2\times P\times R}{P+R} \quad (5)$$

5. False Positive Rate (FPR): Refers to the rate of misclassifying normal traffic as attacks.

$$FPR=\frac{FP}{FP+TN} \quad (6)$$

Flowchart

The proposed methodology is explained by means of a flowchart in Figure 2, which comprises the major processes involved and clearly shows the relationships and sequential interaction between the different methodological stages.

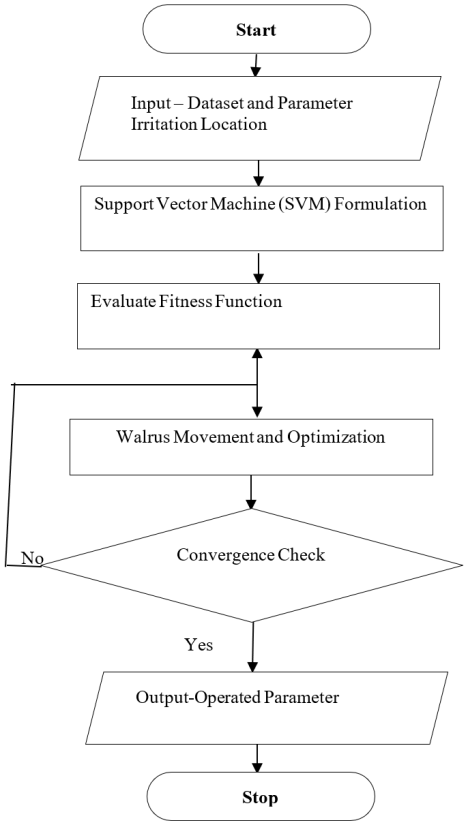


Figure 2. *Flowchart Diagram of Walrus Optimized SVM for IDS Process*

EXPECTED RESULTS

The result of the comparison of the WaOA-SVM with the standard SVM will produce these anticipated primary effects:

Enhanced Classification Accuracy: It is hypothesized that WaOA-SVM may achieve higher classification accuracy than the standard SVM. This hypothesis will be assessed experimentally using the defined evaluation metrics.

Reduced False Positive and False Negative Rates: The evaluation will examine whether WaOA-SVM can reduce FPR and FNR relative to the standard SVM. FAR levels below 2% stand as the necessary criterion to make this approach viable in operational settings.

CONCLUSION

Modern cybersecurity requires intrusion detection to be a fundamental element because cyber threats keep advancing in complexity. Traditional intrusion detection systems face limitations because they produce high false positive rates while having trouble with handling large volumes of network traffic. While the proposed WaOA-SVM framework has potential advantages, its actual performance remains to be established through experimental evaluation. WaOA will be employed to optimize the SVM hyperparameters, and the evaluation will determine whether this optimization improves classification accuracy and reduces FPR and FNR. Meanwhile, the performance of the SVM, including configurations using the RBF kernel, will be assessed for the classification of normal and malicious traffic.

LIMITATIONS AND FUTURE WORK

While the proposed WaOA-SVM framework has potential advantages, its actual performance remains to be established through experimental evaluation:

1. **Computational Complexity**: Although optimized SVM Hyperparameters will reduce dimensionality, the optimization process itself can be computationally intensive for very large datasets. Future research can explore hybrid optimization techniques to further enhance efficiency.

2. **Real-Time Adaptability**: The proposed model will be evaluated on benchmark datasets, but real-time intrusion detection in dynamic network environments remains an open challenge. Future work should focus on real-time deployment and adaptive learning models.

3. **Handling of Adversarial Attacks**: Although the proposed model is intended to enhance intrusion detection, adversarial machine-learning techniques may still pose challenges. Future studies can integrate adversarial defense mechanisms to further improve system resilience.

REFERENCES LIST

Ashraf, U. M., Arya.l S., Bouadjenek, M. R., Al-Hawawreh M., & Talukder, M. A., (2025).
Hierarchical classification for intrusion detection system: Effective design and empirical analysis. *Ad Hoc Networks,* 178(2025), ISSN 1570-8705. https://doi.org/10.1016/j.adhoc.2025.103982.
Bahmaid, S., & Ghaleb S. A. M., (2024). Intrusion Detection System Using Chaotic Walrus
Optimization-based. Proceedings of SAI Intelligent Systems Conference, IntelliSys 2022*, Intelligent Systems and Applications, 236-252*. https://orcid.org/0000-0003-4737-6876
Cortes, C., & Vapnik, V., (1995). Support-vector networks. *Machine Learning*. 20 (1995): 273-297. *https://doi.org/10.1007/s13369-019-03970-z*
Diana, L., Dini, P., & Paolini, D., (2025). Overview on Intrusion Detection Systems for Computers Networking Security. *Computers*, *14*(3), 87. https://doi.org/10.3390/computers14030087
Geng, Y., Li, Y., & Deng, C., (2024). An Improved Binary Walrus Optimizer with Golden Sine

Disturbance and Population Regeneration Mechanism to Solve Feature Selection Problems. *Biomimetics*, 9(8), 501. DOI: 10.3390/biomimetics9080501.

Isam, B. Al., Abdullahi, A. I., & Saadaldeen R. A., (2026). An Intelligent Multi-Stage GA–SVM

Hybrid Optimization Framework for Feature Engineering and Intrusion Detection in Internet of Things Networks, Computers, Materials and Continua, 87(1).

Mobolaji, O., Oluwatobi A. A., & Olanrewaju, A., (2025). Machine Learning Methods for

Intrusion Detection: A Comprehensive Survey. *International Journal of Scientific Research and Management (IJSRM),* 13(7), 2446-2456) DOI: 10.18535/ijsrm/v13i07.ec07

Ngueajio, M. K., Washington G., Rawat, D. B., & Ngueabou, Y., (2022). Intrusion Detection

Systems Using Support Vector Machines on the KDDCUP'99 and NSL-KDD Datasets. A Comprehensive Survey. Proceedings of SAI Intelligent Systems Conference, IntelliSys 2022*, Intelligent Systems and Applications, 609-629*. https://doi.org/10.48550/arXiv.2209.05579

Osman, B. M., Jirow M. S. A., & Aser D. A., (2025). A Novel Hybrid Approach to Machine

Learning for Enhanced Model Precision and Classification. *SSRG International Journal of Electrical and Electronics Engineering* 12(2), 91-101, https://doi.org/10.14445/23488379/IJEEE-V12I2P111

Pinto, A., Herrera, L., Donoso, Y., & Gutierrez J. A., (2023). Survey on Intrusion Detection Systems Based on Machine Learning Techniques for the Protection of Critical Infrastructure. *Sensors* (Basel). 23(5): 2415. doi: 10.3390/s23052415.

Wang H., Xiong J., Yao Z., Lin M., & Ren J., (2017). Research Survey on Support Vector

Machine. In Proceedings of EAI International Conference on Mobile Multimedia Communications, Chongqing, People's Republic of China, July 2017 (10th), 9. DOI: 10.475/123 4.

Xie, J., Wu, H.,& Zhao, Y., (2024). An Enhanced IDS Framework Combining LSTM and Walrus

Optimization Algorithm for Cybersecurity in Smart Cities. *IEEE Internet of Things Journal*, 11(2), 983–997. DOI: 10.1109/JIOT.2024.105106321.



This is an open access article distributed under the terms and conditions of the
Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License.