Science World Journal Vol. 21(No 1) 2026 https://dx.doi.org/10.4314/swj.v21i1.43
www.scienceworldjournal.org
ISSN: 1597-6343 (Online), ISSN: 2756-391X (Print)
Published by Faculty of Science, Kaduna State University

Full Length Research Article

AN IMPROVED GREY WOLF OPTIMIZATION ALGORITHM WITH CHAOTIC MAPPING FOR INTRUSION DETECTION IN NETWORKS

[1]Abakar Mahamat, [1]Mustapha Aminu Bagiwa, [1]Salisu Aliyu, *[1,2]Hassan Muhammad Yusuf

[1]Department of Computer Science, Ahmadu Bello University, Zaria, Nigeria
[2]Department of Computer Science, Division of Agricultural Colleges, Ahmadu Bello University, Zaria, Nigeria

*Corresponding Author Email Address: abuabdurrahman1101@gmail.com

ABSTRACT
Intrusion Detection Systems (IDS) play a vital role in safeguarding computer networks against increasingly sophisticated cyber threats. However, many optimization-based IDS models suffer from an imbalance between exploration and exploitation, leading to premature convergence, poor feature diversity, and high false alarm rates.
This study aims to develop an improved intrusion detection framework by enhancing the Modified Grey Wolf Optimization (MGWO) algorithm with a chaotic mapping to address the exploration-exploitation imbalance and enhance feature selection and detection performance. The proposed Intrusion Detection System integrates the Improved Modified Grey Wolf Optimization (IMGWO) algorithm with a deterministic chaotic position-update mechanism. Information Gain is employed to evaluate feature significance, while MinMax normalization ensures effective data scaling. The optimized feature subsets are used to train the classifier, and experiments were conducted using the UNSW-NB15 benchmark dataset. Performance is evaluated using standard metrics, including accuracy, F1 Score, False Positive Rate (FPR), Classification Error Rate (CER), and G-mean. Experimental results demonstrate that the proposed IMGWO-based IDS significantly outperforms existing approaches. The model achieved an accuracy of 98.07%, an F1-score of 97.51%, an FPR of 1.55%, a CER of 0.97%, and a G-Mean of 97.96%, indicating improved detection capability and reduced false alarms.

Keywords: Chaotic map, Grey Wolf Optimization, Information Gain, Intrusion Detection System, Extreme Learning Machine

INTRODUCTION

The rapid evolution of cyber threats in recent years has significantly increased the complexity of network security. Intrusion Detection Systems (IDS) serve as a critical line of defence by monitoring network traffic and system activities to detect anomalous behaviour and unauthorized access. Despite their importance, conventional IDS approaches often exhibit high false-positive rates, limited detection accuracy, and substantial computational inefficiencies when confronted with modern, sophisticated attack patterns. (Abdelkhalek et al., 2023). The increasing volume, velocity, and complexity of network traffic, coupled with the continuous emergence of novel attack vectors, have highlighted the need for more intelligent and adaptive intrusion detection techniques.

In this context, machine learning and nature-inspired optimization algorithms have demonstrated considerable potential in enhancing IDS performance by improving feature selection, classification accuracy, and system adaptability. (Zhang et al., 2025). Feature selection plays a crucial role in IDS effectiveness, as selecting only the most relevant attributes reduces data dimensionality while preserving essential information required for accurate detection. This process not only improves detection accuracy but also reduces computational overhead. Among nature-inspired optimization techniques, the Grey Wolf Optimization (GWO) algorithm has been widely adopted for feature selection due to its simplicity and ability to balance exploration and exploitation through its simulated hunting behaviour.

Despite its effectiveness, GWO is prone to premature convergence and can become trapped in local optima, particularly in complex, high-dimensional search spaces. (Rajeshwari & Anuradha, 2024).

To solve the problem of GWO, Alzaqebah et al. (2022) The Modified Grey Wolf Optimization (MGWO) algorithm improves upon the standard GWO by introducing an intelligent initialization phase and a faster classification method. While the standard GWO uses random initialization for its population, MGWO integrates filter- and wrapper-based initialization, allowing the algorithm to focus on the most relevant features early on. This hybrid approach accelerates convergence and improves optimization performance.

However, this approach causes a significant imbalance between exploration and exploitation during the search process. As the algorithm progresses, the heavy reliance on the initial population reduces its ability to explore new regions of the search space, leading to premature convergence and entrapment in local optima.

To overcome this challenge, this study introduces a chaotic mapping mechanism into the MGWO algorithm. Chaotic mapping introduces deterministic yet non-repetitive behaviour that enhances search diversity while maintaining convergence stability. By dynamically guiding the wolves' position updates, the chaotic mechanism improves the balance between exploration and exploitation, enabling the algorithm to escape local optima and identify higher-quality solutions.

The primary objective of this research is to enhance the optimization capability of MGWO by addressing the limitations of existing initialization-based approaches. By integrating chaotic mapping into the MGWO framework and applying it to intrusion detection, this study is restricted to binary classification to establish a consistent basis for comparison with prior research that utilized the UNSW-NB15 dataset without incorporating multi-class classification. By limiting the problem to two classes, the classification task is simplified, thereby facilitating a more focused evaluation of the proposed model's effectiveness while ensuring methodological comparability with existing studies. Furthermore, time complexity is outside the scope of this

research, as the primary objective is to improve feature selection and classification accuracy using the Improved Modified Grey Wolf Optimization (IMGWO) algorithm. Considering the availability of sufficient computational resources within a cloud-based environment, the study emphasizes performance metrics such as accuracy and F1-score rather than execution time. Consequently, this deliberate methodological choice ensures a more focused and rigorous evaluation of the intrusion detection system's detection capabilities.

The major contributions of this study are detailed as follows:

i.I. Integrate a Chaotic mapping mechanism into the Modified Grey Wolf Optimization to enhance search diversity and dynamically update search agents' positions.

ii.A Hybrid feature selection process guided by Information Gain, combined with the Enhanced Grey Wolf Optimization Algorithm, was introduced to reduce data dimensionality while preserving salient features required for accurate detection.

iii.Comparative analysis was conducted with the model proposed by Alzaqebah et al. (2022) using different performance evaluation metrics to assess improvements in detection accuracy.

The rest of the study is structured as follows: Section 2 discusses related work. Section 3 details the proposed enhanced IDS model. Section 4 presents the experimental results and analysis of the proposed model. Finally, Section 5 concludes the study and suggests future research directions.

Feature-Selection-Based Intrusion Detection Systems

Feature selection is a critical component of Intrusion Detection Systems (IDS) as it reduces data dimensionality, improves classification accuracy, and lowers computational overhead. Several studies have demonstrated that selecting only the most informative features significantly enhances IDS performance.

Alzaqebah et al. (2022) proposed a Modified Grey Wolf Optimization (MGWO)-based IDS that integrates both filter-based and wrapper-based feature selection strategies. Information Gain (IG) was employed during a smart initialization phase to identify relevant features from the UNSW-NB15 dataset. The proposed model achieved an accuracy of 81% and an F1-score of 78%, while reducing false positives and crossover error rates. However, the study focused primarily on generic attacks and did not evaluate the model across diverse datasets or attack types, limiting its general applicability.

Similarly, Alqahtany et al., (2025) Combined Enhanced Grey Wolf Optimization (EGWO) with a Random Forest (RF) classifier for feature selection in IoT-based IDS. The approach reduced the feature set from 43 to 23 using the NF-ToN-IoT dataset and achieved 99.93% detection accuracy. Despite the strong performance, the reliance on a single dataset and potential computational cost when scaling to large IoT environments remain notable limitations.

Grey Wolf Optimization (GWO)-Based IDS

Grey Wolf Optimization (GWO) has gained popularity in IDS research due to its simplicity and ability to balance exploration and exploitation. However, classical GWO often suffers from premature convergence and limited search diversity.

Chidambaram et al., (2021) introduced an MGWO variant to reduce fuzzy rules in Cloud Intrusion Detection Systems (CIDS). By modifying the control parameter and incorporating weighted position updates, the proposed MGWO demonstrated improved convergence speed and solution quality compared to PSO, CS, and standard GWO. Nevertheless, the approach was evaluated only on benchmark functions and lacked real-time cloud deployment, leaving concerns about computational overhead unaddressed.

Yerriswamy & Gururaj, (2022) proposed a Genetic-Based Enhanced GWO (GB-EGWO), combining GWO with Genetic Algorithms to improve feature selection and detection accuracy. The model achieved 98.62% accuracy on the NSL-KDD dataset and performed well across multiple attack categories. Despite these results, the hybridization increased computational complexity, and the use of a single, outdated dataset limits its relevance to modern cyber threats.

Chaotic Maps in Optimization Algorithms

Chaotic maps have been increasingly integrated into metaheuristic algorithms to enhance search diversity and prevent stagnation in local optima. Unlike random processes, chaotic systems exhibit deterministic yet non-repetitive behavior, making them well-suited to improving the exploration–exploitation balance.

Several studies have shown that chaotic reverse learning and chaotic initialization can improve convergence speed and solution quality in optimization problems. (Lozi, 2023). These approaches introduce controlled randomness that enhances population diversity throughout the optimization process. However, most existing works apply chaotic maps only during initialization or in non-IDS domains, leaving their full potential in continuous feature-selection-driven IDS underexplored.

Hybrid and Quantum Metaheuristics for IDS

Hybrid and quantum-inspired optimization techniques have recently been explored to enhance IDS performance further. These approaches combine multiple metaheuristics or incorporate quantum computing principles to improve learning and optimization capabilities.

Alotaibi et al., (2025) proposed the Hybrid Grey Wolf Quantum Binary Bat Algorithm (GWQBBA) for feature selection and classification using the UNSW-NB15 dataset. The model reduced the feature set to 12 and achieved 98.5% accuracy with an RF classifier. While effective, the model's complexity and lack of real-time evaluation limit its practical deployment.

Dalmaz et al., (2023) introduced GWOMFO, a hybrid GWO–Moth Flame Optimization algorithm evaluated on NSL-KDD, UNSW-NB15, and CIC IDS 2017 datasets. The model achieved high accuracy across datasets but required extensive parameter tuning and introduced additional computational complexity.

Elsedimy et al., (2024) proposed QSVM-IGWO, integrating an Improved GWO with a Quantum Support Vector Machine for IoT intrusion detection. Although the model outperformed classical classifiers, its reliance on quantum-inspired computation raises concerns regarding processing cost and real-world scalability.

Hybrid and quantum approaches show promising gains in accuracy but often suffer from increased complexity, scalability issues, and limited real-time validation.

Science World Journal Vol. 21(No 1) 2026 https://dx.doi.org/10.4314/swj.v21i1.43
www.scienceworldjournal.org
ISSN: 1597-6343 (Online), ISSN: 2756-391X (Print)
Published by Faculty of Science, Kaduna State University

Table 1: Summary of Research Gaps in Existing IDS Approaches

Authors	Methods	Results	Limitations
Alzaqebah et al. (2022)	**Modified Grey Wolf Optimization (MGWO)** algorithm for feature selection in Intrusion Detection System (IDS)	Achieved 81% accuracy, 78% F1-score, 84% G-mean on UNSW-NB15 dataset. It reduced FPR to 28%, CER to 27%, and Improved convergence speed and feature selection efficiency.	Limited to binary classification (focuses only on generic attacks), susceptible to suboptimal exploration-exploitation balance. Evaluated only on the UNSW-NB15 dataset, limiting generalizability. No comparison with deep learning.
Chidambaram et al. (2021)	**Modified Grey Wolf Optimizer (MGWO)** for **fuzzy rule reduction** in **Cloud Intrusion Detection Systems (CIDS)**	Improved **exploration and exploitation** of search space; outperformed **GWO, PSO, and CS** on 11 benchmark functions	High computational cost due to **complex modifications** in control parameters.
Yerriswamy & Murtugudde (2021)	**Genetic-Based Enhanced GWO (GB-EGWO)** for **feature selection in IDS**	Achieved **98.62% accuracy** on the **NSL-KDD dataset**; outperformed **classical GWO**	Needs further testing on **modern datasets** to validate performance on emerging cyber threats.
Alqahtany et al. (2025)	**Enhanced GWO (EGWO) + Random Forest (RF)** for **IoT IDS**	Improved **detection accuracy (99.93%)** on **NF-ToN-IoT dataset**, with **optimal feature selection (23 out of 43 features)**	Requires integration with **other metaheuristics** to enhance scalability.
Alotaibi et al. (2025)	**Hybrid Grey Wolf Quantum Binary Bat Algorithm (GWQBBA)** for **IDS feature selection and classification**	Reduced features to **12**, maintaining **98.5% accuracy** with **Random Forest** on **UNSW-NB15 dataset**	Computational complexity may increase with **larger datasets.**
Dalmaz et al. (2023)	**Hybrid GWO-Moth Flame Optimization (GWOMFO)** for **network attack detection**	High accuracy of **97.4% (NSL-KDD), 98.3% (UNSW-NB15), and 99.2% (CIC IDS 2017)**; validated on **13 benchmark functions**	Performance may vary depending on **dataset characteristics** and **feature selection strategies**
Elsedimy et al. (2024)	**Quantum SVM + Improved GWO (QSVM-IGWO)** for **IoT Intrusion Detection**	Outperformed **Logistic Regression, Decision Trees, and Random Forest** on the **Bot-IoT dataset**, improving **accuracy, precision, recall, F1-score, and ROC curve**	The complexity of **quantum computing integration** increases **hardware requirements**

Most existing IDS models either rely heavily on smart initialization or complex hybridization strategies, which often lead to premature convergence, increased computational cost, and limited generalization. Moreover, the use of chaotic mechanisms to dynamically balance exploration and exploitation throughout the optimization process remains insufficiently explored in IDS feature selection. This study addresses these gaps by introducing a chaotic-map-enhanced Improved Modified Grey Wolf Optimization algorithm for robust and efficient intrusion detection.

MATERIALS AND METHODS

Experimental setup

All experiments in this study were conducted in a Jupyter notebook environment hosted on the Kaggle cloud. The Kaggle environment has a maximum CPU RAM of 29 GB, a maximum disk space of 73.1GB, and a maximum GPU memory of 16 GB, which will enhance training speed by 12.5x according to the Kaggle cloud specifications. Python 3 was used to implement the proposed model. The libraries used are: random from the Python Standard Library, Seaborn, Matplotlib, NumPy, Pandas, Scikit-Learn, and PrettyTable.

Dataset

The UNSW-NB15 dataset was used to train and evaluate the model. The UNSW-NB15 dataset is a modern network intrusion detection dataset developed by the Australian Centre for Cyber Security (ACCS) at the University of New South Wales in 2015. It contains a mix of normal and malicious traffic generated using the IXIA PerfectStorm tool, offering realistic network behaviour. The dataset includes 49 features and over 2.5 million labelled records, categorized into nine attack types, including DoS, Exploits, Fuzzers, and Reconnaissance, as well as normal traffic. It is widely used in cybersecurity research to evaluate and develop machine learning-based intrusion detection systems, addressing the shortcomings of older datasets such as KDD'99 by better reflecting contemporary threat scenarios.

Science World Journal Vol. 21(No 1) 2026 https://dx.doi.org/10.4314/swj.v21i1.43
www.scienceworldjournal.org
ISSN: 1597-6343 (Online), ISSN: 2756-391X (Print)
Published by Faculty of Science, Kaduna State University

Data Pre-processing

The dataset underwent comprehensive pre-processing to enhance its suitability for intrusion detection modelling. Redundant features such as IP addresses, timestamps, and IDs were removed to reduce noise and focus on impactful attributes. Missing or incomplete data rows were discarded to ensure data quality. Categorical features were encoded as numerical values using label encoding to enable compatibility with machine learning algorithms. Numerical features were then normalized using a MinMax scaler to ensure uniform scaling, thereby aiding efficient model convergence. Additionally, feature importance was assessed through Information Gain to identify the most relevant features, guiding the initial population of the optimization algorithm. Finally, the dataset was split into 70% for training and 30% for testing using stratified sampling, maintaining the proportions of normal and attack instances to ensure reliable evaluation.

The Proposed Model

Fig. 1 presents the detailed workflow of the proposed intrusion detection system. The process begins with data pre-processing, where the input dataset is cleaned by removing redundant features such as IP addresses and timestamps. Categorical attributes are encoded into numerical form, and numerical features are normalized to a uniform scale using the MinMax Scaler. The methodology computes Information Gain (IG) to evaluate each feature's relevance, which subsequently guides the initialization of the MGWO population.

The core contribution lies in integrating chaotic maps into the MGWO algorithm to update the wolves' positions, thereby introducing controlled randomness and enhancing population diversity during the search process. This chaotic mapping mechanism improves the algorithm's ability to escape local optima and achieve more effective feature subset selection. The system iteratively updates the search agents and selects the top three wolves (alpha, beta, and delta) to guide the optimization process.

To ensure the reliability and robustness of the results, the entire experimental procedure was repeated ten (10) times under the same conditions. The final model, optimized through these enhancements, is evaluated using a confusion matrix and standard classification metrics, with the reported results representing the aggregated performance across all runs. This novel integration of pre-processing and chaotic map-driven optimization demonstrates a significant improvement in feature selection and predictive performance.

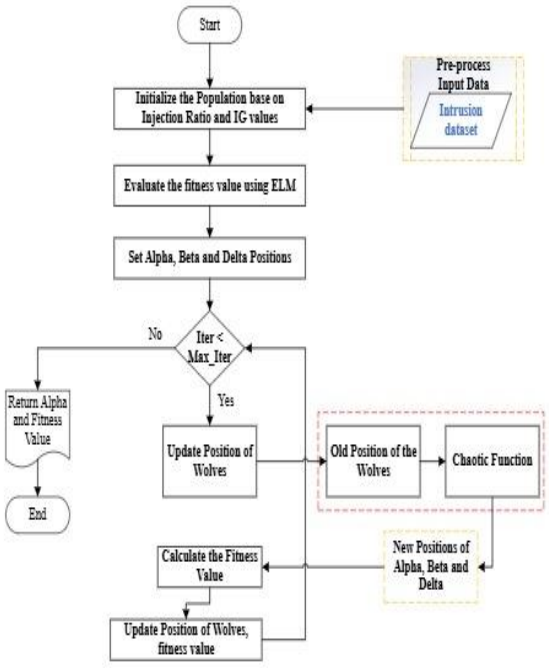

Figure 1: Workflow of the proposed model

Proposed Algorithm

Algorithm: IMGWO-ELM Intrusion Detection System (with IDS-specific enhancements)

Input:

file_paths ← Paths to the **IDS training and testing datasets**
population_size ← Number of wolves in the population
max_iterations ← Maximum number of iterations for optimization
injection_ratio ← Ratio of IG-based wolves injected into population (to bias towards high-relevance IDS features)

Output:

Best solution (feature subset), fitness score, and IDS performance metrics (e.g., F1-score, Detection Rate)

Procedure: IMGWO_ELM_Intrusion_Detection(file_paths, population_size, max_iterations, injection_ratio)
Step 1: Preprocess Data for Intrusion Detection
Step 2: Compute Information Gain for IDS Feature Ranking
Step 3: Initialize Grey Wolf Population for Feature Subsets
Step 4: Evaluate a Wolf Using ELM for IDS Detection
Step 5: Update Wolf Positions Based on Chaotic Map value
Step 6: IMGWO Optimization Loop for IDS Feature Optimization
Step 7: Final Model Evaluation for IDS Detection Performance
Main Execution:
data ← PreprocessData(file_paths)
X ← data without 'labels'
y ← data['labels']
best_solution, best_fitness ← ImprovedModifiedGWO(X, y, population_size, max_iterations, injection_ratio)
Print best_fitness
conf_matrix ← EvaluateModel(X, y, best_solution)

Science World Journal Vol. 21(No 1) 2026 https://dx.doi.org/10.4314/swj.v21i1.43
www.scienceworldjournal.org
ISSN: 1597-6343 (Online), ISSN: 2756-391X (Print)
Published by Faculty of Science, Kaduna State University

Print conf_matrix
Print the number of selected features
Plot class distribution (Normal vs Attack)
End

Fitness Function Formulation

The fitness function is designed to simultaneously maximize classification performance and minimize the number of selected features. This multi-objective problem is converted into a single scalar fitness function using a weighted sum approach.
The fitness function is defined as:

$$\text{Fitness} = \alpha(1-\text{Accuracy}) + \beta\left(\frac{N_s}{N_t}\right) \quad (1)$$

where:

- Accuracy represents the classification accuracy obtained using the selected feature subset,
- $N_s$is the number of selected features,
- $N_t$is the total number of available features,
- α anbeta areeighting coefficients such that $\alpha + \beta = 1$.

In this study, greater emphasis is placed on classification accuracy to ensure reliable intrusion detection, while feature reduction is employed to improve computational efficiency. Therefore, the optimizer aims to minimize the fitness value by achieving high detection accuracy with a reduced feature subset.

Evaluation Metrics

To evaluate the performance of the proposed and existing models, the following quantitative measures were used: Accuracy score, F1-score, Precision score, and Recall score, False Positive Rate (FPR), False Negative Rate (FNR), Crossover Error Rate (CER), and Geometric Mean (G-Mean).

Accuracy

This measures the ratio of correct predictions (TP+TN) to the total number of predictions (TP+TN+FP+FN), and is calculated using equation 3.8.

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

Precision

Precision is the ratio of True Positive (TP) elements to the total number of positively predicted classes (TP + FP). The precision is calculated using equation 3.9.

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

Recall

The Recall measures the ratio of True Positive (TP) elements to the total number of positively and negatively classified elements (TP + FN). Which is calculated using equation 3.10.

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

F1-score

This is the harmonic Mean of precision and recall. This can be interpreted as the weighted average between precision and recall.

$$\boldsymbol{F1-score} = \frac{\boldsymbol{2*Precision*Recall}}{\boldsymbol{Precision+Recall}} \quad (5)$$

False Positive Rate (FPR)

This represents the number of elements that belong to the **Negative** class (Normal class) but are incorrectly predicted as the **Positive** class (Attack class). Which is calculated as:

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

False Negative Rate (FNR)

This represents the number of elements that belong to the **Positive** class (Attack class) but are incorrectly predicted as the **Negative** class (Normal class). Which is calculated as:

$$\boldsymbol{FNR} = \frac{\boldsymbol{FN}}{\boldsymbol{FN+TP}} \quad (7)$$

Crossover Error Rate (CER)

This is the absolute difference between the FNR and the FPR, which is calculated as:

$$\boldsymbol{CER} = |\boldsymbol{FPR} - \boldsymbol{FNR}| \quad (8)$$

Geometric Mean (G-Mean)

This is the square root of the Recall multiplied by the Precision. This can be calculated in the following equation:

$$\boldsymbol{G-Mean} = \sqrt{\boldsymbol{Recall*Precision}} \quad (9)$$

Chaotic Mapping in the IMGWOA-Based Intrusion Detection Model

Chaotic mapping has been widely applied in metaheuristic optimization algorithms to enhance population diversity and prevent premature convergence. Chaos theory describes deterministic nonlinear systems that exhibit pseudo-random behaviour due to their high sensitivity to initial conditions. These characteristics make chaotic sequences particularly well-suited to enhancing the exploration capabilities of optimization algorithms. In intrusion detection systems, incorporating chaotic mapping into optimization algorithms improves feature selection by enhancing the algorithm's search capability in high-dimensional feature spaces. (Jin et al., 2025).
In this study, chaotic mapping is integrated into the Improved Modified Grey Wolf Optimization algorithm to enhance the positions of the wolf in the proposed IDS model. The Logistic Chaotic Map was used to update the wolves' positions. (Bouteraa & Khishe, 2025).
The logistic chaotic map is mathematically expressed as:

$$x_{t+1} = \mu x_t\,(1 - x_t) \quad (10)$$

where:

- x_t is the chaotic variable at iteration t
- x_{t+1} is the chaotic value at the next iteration
- μ is the control parameter that determines the behaviour of the chaotic system
- $It\ represents$ the iteration index

For chaotic behaviour, the parameter μ is is typically chosen in the interval:

$$3.57 < \mu \leq 4$$

In this research, the parameter is set as:

$$\mu = 4$$

Science World Journal Vol. 21(No 1) 2026 https://dx.doi.org/10.4314/swj.v21i1.43
www.scienceworldjournal.org
ISSN: 1597-6343 (Online), ISSN: 2756-391X (Print)
Published by Faculty of Science, Kaduna State University

Table 2: Variables and Parameters Used

x_t	chaotic variable at iteration t
x_{t+1}	$chaotic\ value\ at\ the\ next\ iteration$
t	$iteration\ index$
μ	Control parameter of the logistic chaotic map
x_i	Chaotic sequence value used for initialization

RESULTS AND DISCUSSION

Fig. 2 shows the distribution of the UNSW-NB15 dataset into training and test sets before pre-processing. It shows that 68% of the data, amounting to 175,341 records, was allocated to the training set, while the remaining 32%, totaling 82,332 records, was allocated to the test set. This proportion ensures that a larger portion of the data is used for model training while retaining a substantial portion for evaluating the model's performance.

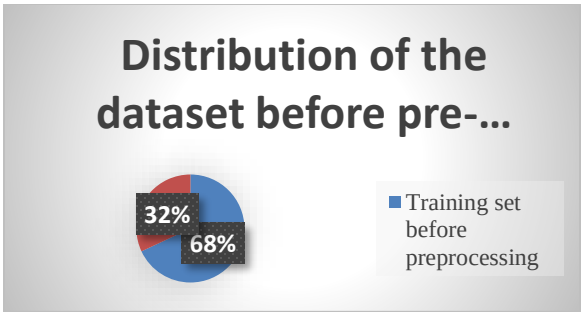

Figure 2: Percentage distribution of the dataset before pre-processing

Data distribution of training and testing sets

Fig. 3 shows the total number of the training set and the testing set after pre-processing. One of the most common attacks in the UNSW-NB15 dataset is the generic attack, which accounts for 58,871 data points. The original datasets training and testing set were first loaded as Data Frames and assigned binary labels: "Normal" as 0 and "Generic" as 1 while discarding other attack categories as our focus is on the generic and the normal categories. Redundant columns, such as IP addresses, ports, timestamps, and IDs, are removed to reduce noise as they do not contribute to the detection process. Rows with missing values are dropped to ensure data quality. Categorical columns are encoded into numeric form using label encoding. The feature set (X) and the target set (y) were then generated to simplify the splitting of the dataset into training and testing sets using the **train_test_spilt()** function from the **sklearn** library. The complete dataset was split into training and testing sets, with 70% for the training and 30% for the testing.

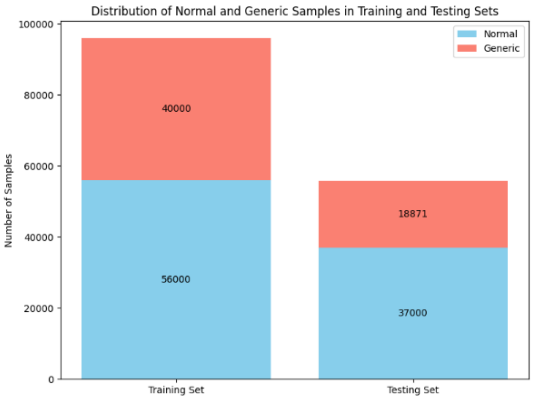

Figure 3: The distribution of Normal and Generic Samples in Training and Testing Sets

CLASSIFICATION RESULT

As clearly shown in Table 3, the proposed model (IMGWO) significantly outperforms the original MGWO in all metrics. The F1 Score, which balances precision and recall, is much higher for IMGWO (0.9751) than for MGWO (0.7808), indicating better overall classification performance. Similarly, the accuracy of IMGWO (98.07%) surpasses that of MGWO (80.93%), showing a substantial improvement in correct predictions. The FPR and CER, which reflect the rates of incorrect classifications, are drastically lower in IMGWO (0.0155 and 0.0097, respectively) than in MGWO (0.2808 and 0.2669), suggesting that IMGWO is more effective at minimizing both false alarms and misclassifications. Finally, the G-Mean, which measures the balance between sensitivity and specificity, is also higher in IMGWO (0.9796), affirming its robustness in handling imbalanced classification scenarios.

Table 3: Comparative analysis of the proposed model and the existing model.

Algorithm	**F1_Score (%)**	**Accuracy (%)**	**FPR (%)**	**CER (%)**	**G-Mean (%)**
Based model	78.08%	80.93%	28%	26%	84.03%
Proposed Model	**97.51%**	**98.07%**	**1.55%**	**0.97%**	**97.96%**

Number of Features selected and best Fitness Value

Fig. 4 shows a comparative analysis of the existing model, MGWO (Modified Grey Wolf Optimizer), and the proposed model, IMGWO (Improved Modified Grey Wolf Optimizer), based on two metrics: **fitness value** and **number of selected features**. The fitness value, shown by the blue bars and measured on the left y-axis, represents optimization performance, with lower values indicating better solutions. IMGWO shows a significantly lower fitness value (0.0048) compared to MGWO (0.0063), indicating that the improved model achieves a more optimal balance between feature relevance and redundancy. The red bars, representing the number of selected features and aligned with the right y-axis, show that IMGWO selects **20 features**, which is slightly more than the **17 features** selected by MGWO.

Science World Journal Vol. 21(No 1) 2026 https://dx.doi.org/10.4314/swj.v21i1.43
www.scienceworldjournal.org
ISSN: 1597-6343 (Online), ISSN: 2756-391X (Print)
Published by Faculty of Science, Kaduna State University

Despite selecting more features, IMGWO maintains superior optimization efficiency, as evidenced by the lower fitness value.

Figure 4: MGWO and IMGWO in terms of features selected and best fitness value

Statistical Analysis

From Table 4, the experimental results obtained from 10 independent runs demonstrate the robustness, stability, and high predictive capability of the proposed model across multiple evaluation metrics. The model achieved a mean accuracy of 0.9553 with a low standard deviation of 0.0097, indicating highly consistent classification performance despite variations in training initialization and data sampling. Similarly, the mean F1-score of 0.9430 reflects a strong balance between precision and recall, confirming the model's effectiveness in correctly identifying both positive and negative instances. The False Positive Rate (FPR) remains relatively low, with a mean value of 0.0421 and a standard deviation of 0.0095, suggesting that the model produces few false alarms and maintains reliable decision boundaries across runs. In addition, the Classification Error Rate (CER) averaged 0.0127, demonstrating a very small proportion of misclassified samples and highlighting the reliability of the predictive framework. The Geometric Mean (GMean), with a mean value of 0.9546 and a standard deviation of 0.0105, further confirms balanced performance across classes, which is particularly important when dealing with imbalanced datasets. Moreover, the relatively narrow gap between the best and worst results across all metrics indicates that the model maintains stable performance and is not significantly affected by stochastic variations during training. Thus, these results provide strong evidence that the proposed approach achieves high accuracy, balanced classification performance, low false-positive rates, and consistent performance across repeated experimental trials.

Table 4: Statistical performance of the proposed model over 10 independent runs, reporting mean, standard deviation, best, and worst values for key evaluation metrics.

S/N	Metric	Mean	Std	Best	Worst
0	Accuracy	0.955333	0.009731	0.976669	0.941574
1	F1-score	0.943031	0.012499	0.970158	0.924785
2	FPR	0. 042135	0. 009478	0. 054788	0. 022726
3	CER	0. 012747	0. 010666	0. 028574	0. 000793
4	GMean	0. 954574	0. 010508	0. 976496	0. 938285

Table 5 presents the 95% confidence intervals (CIs), which provide statistical evidence of the proposed model's effectiveness across the experimental runs. The accuracy confidence interval (0.9484–0.9623) indicates that the model's true population accuracy is highly likely to fall within this narrow range, confirming strong and consistent predictive performance. Similarly, the F1-score confidence interval (0.9341–0.9520) indicates a stable balance between precision and recall, suggesting that the model consistently maintains high classification performance across different experimental conditions. The False Positive Rate (FPR) confidence interval (0.0354–0.0489) remains relatively low, highlighting the model's ability to minimize false alarms while maintaining strong detection capability. In addition, the Classification Error Rate (CER) confidence interval (0.0051–0.0204) further confirms the low proportion of misclassified samples, reinforcing the overall reliability of the proposed framework. In summary, the narrow confidence intervals across all metrics indicate low variability and high statistical stability, demonstrating that the proposed model achieves consistent, reliable performance and that the reported results are unlikely to be due to random variation.

Table 5: 95% Confidence Intervals of the proposed model's performance metrics across 10 experimental runs.

Metric	Minimum Confidence	Maximum Confidence
Accuracy	0.9483723844600129	0.9622943992632655
F1-score	0.9340897206271925	0.9519725955897635
FPR	0.03535549332755719	0.04891550082029043
CER	0.005117172781808242	0.02037743356366274
GMean	0.947056551707286	0.9620904551142846

Conclusion and Future Work

This study proposes an enhanced Intrusion Detection System (IDS) that leverages an Improved Modified Grey Wolf Optimization algorithm with an integrated chaotic mapping to overcome the limitations of traditional GWO-based techniques. These limitations primarily include premature convergence and poor balance between exploration and exploitation during optimization. The methodology begins with thorough preprocessing steps, including data cleaning, feature normalization, and Information Gain (IG) analysis to select relevant attributes. The novel integration of chaotic mapping diversifies search-space traversal, enabling the algorithm to escape local optima and more effectively identify optimal feature subsets. Using the UNSW-NB15 dataset, a well-established benchmark in cybersecurity research, the model was trained and evaluated. The proposed Intrusion Detection System (IDS) achieved outstanding performance across all key metrics, including a notable F1-score of 0.9751 and an accuracy of 98.07%, significantly outperforming the baseline MGWO model. Future work should extend the IDS from binary to multi-class classification, enabling finer-grained detection across different attack categories. Additionally, future work should evaluate IMGWO on multiple, more recent datasets, including CICIDS and real-time traffic datasets, to assess its generalization and scalability.

REFERENCES

Abdelkhalek, A., Mashaly, M., Abdelkhalek, A., & Mashaly, M. (2023). Addressing the class imbalance problem in network intrusion detection systems using data resampling and deep learning. *The Journal of Supercomputing 2023 79:10*, *79*(10), 10611–10644. https://doi.org/10.1007/s11227-023-05073-x

Alotaibi, M., Mengash, H., … H. A.-A. E., & 2025, undefined. (n.d.). Hybrid GWQBBA model for optimized classification of attacks in an Intrusion Detection System. *ElsevierM Alotaibi, HA Mengash, H Alqahtani, AM Al-Sharafi, AE Yahya, SR Alotaibi, AO Khadidos, Alexandria Engineering Journal, 2025•Elsevier*. Retrieved March 8, 2026, from https://www.sciencedirect.com/science/article/pii/S1110016824016557

Alqahtany, S. S., Shaikh, A., & Alqazzaz, A. (2025). Enhanced Grey Wolf Optimization (EGWO) and a random forest-based mechanism for intrusion detection in IoT networks. *Scientific Reports*, *15*(1), 1916. https://doi.org/10.1038/s41598-024-81147-x

Bouteraa, Y., & Khishe, M. (2025). Fractal and chaotic map-enhanced grey wolf optimization for robust fire detection in deep convolutional neural networks. *Scientific Reports 2025 15:1*, *15*(1), 11495-. https://doi.org/10.1038/s41598-025-95519-4

Chidambaram, B., Subramaniam, S. E., & Varatharaj, A. (2021). An enhanced exploration and exploitation of the modified grey wolf optimizer for fuzzy rules reduction in a cloud intrusion detection system (CIDS). *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, *21*(6), 912–918. https://doi.org/10.17586/2226-1494-2021-21-6-912-918

Dalmaz, H., Erdal, E., Engineering, H. Ü.-C. M. in, & 2023, undefined. (n.d.). A new hybrid approach using GWO and MFO algorithms to detect network attacks. *Researchgate.NetH Dalmaz, E Erdal, H ÜnverComputer Modeling in Engineering & Sciences, 2023•researchgate.Net*. Retrieved March 8, 2026, from https://www.researchgate.net/profile/Erdal-Erdal/publication/368322038_A_New_Hybrid_Approach_Using_GWO_and_MFO_Algorithms_to_Detect_Network_Attack/links/63f793000cf1030a56461d1d/A-New-Hybrid-Approach-Using-GWO-and-MFO-Algorithms-to-Detect-Network-Attack.pdf

Elsedimy, E. I., Elhadidy, H., & Abohashish, S. M. M. (2024). A novel intrusion detection system based on a hybrid quantum support vector machine and improved Grey Wolf optimizer. *Cluster Computing*, *27*(7), 9917–9935. https://doi.org/10.1007/s10586-024-04458-8

Jin, X., Deng, H., & Jiao, X. (2025). Hybrid whale-gray wolf optimization for efficient intrusion detection in the Internet of Things. *Journal of Engineering and Applied Science 2025 72:1*, *72*(1), 144-. https://doi.org/10.1186/s44147-025-00711-y

Lozi, R. (2023). Survey of Recent Applications of the Chaotic Lozi Map. *Algorithms 2023, Vol. 16, 16*(10). https://doi.org/10.3390/a16100491

Rajeshwari, R., & Anuradha, M. P. (2024). Intrusion Detection Using Dynamic Feature Selection: An Adaptive Bacterial Foraging Method. *SN Computer Science 2024 5:6*, *5*(6), 679-. https://doi.org/10.1007/s42979-024-02975-2

Tejaswini, P., Singh, P., Ramchandani, M., Rathore, Y. K., & Janghel, R. R. (2022). Rice Leaf Disease Classification Using CNN. *IOP Conference Series: Earth and Environmental Science*, *1032*(1). https://doi.org/10.1088/1755-1315/1032/1/012017

Yerriswamy, T., & Gururaj, M. (2022). An Efficient Hybrid Protocol Framework for DDoS Attack Detection and Mitigation Using Evolutionary Technique. *Journal of Telecommunications and Information Technology*, *4*(4), 77–83. https://doi.org/10.26636/jtit.2022.165122

Zhang, C., Wang, N., … Y. H.-A. for C., & 2025, undefined. (2025). Machine Learning-based Intrusion Detection Systems: Capabilities, Methodologies, and Open Research Challenges. *Wiley Online LibraryC Zhang, N Wang, YT Hou, W LouAI for Cybersecurity: Research and Practice, 2025•Wiley Online Library*, 67–108. https://doi.org/10.1002/9781394293773.ch03