An Adaptive F&WO Algorithm-Driven Model for Next-Generation Cyberthreat Detection and Response

Sreekanth Rallapalli[1], Weiwei Jiang[2]
[1]Lincoln University College, Malaysia.
[1]Department of Master of Computer Applications,
Nitte Meenakshi Institute of Technology, Yelahanka,
Bengaluru, Karnataka, India.
[2]Beijing University of Posts and Telecommunications, Beijing, China
[1]sreekanth.rallapalli@nmit.ac.in
[2] jww@bupt.edu.cn

Abstract

Cybersecurity threats have become increasingly complex due to the rapid growth of cloud computing, Internet of Things (IoT), mobile networks, and remote digital infrastructures. Traditional intrusion detection and response systems are often limited by static rules, high false alarm rates, and inability to adapt to emerging attack patterns. This research proposes an AI-driven cyberthreat detection and automated response model based on a hybrid optimization strategy called the Firefly and Whale Optimization (F&WO) algorithm. The F&WO algorithm integrates structured exploration inspired by forest growth mechanisms with exploitation strategies inspired by Grey Wolf Optimization (GWO). This hybrid design supports efficient feature selection, hyperparameter tuning, and response prioritization to improve both detection accuracy and response speed. The proposed framework is evaluated using standard cybersecurity datasets including NSL-KDD, UNSW-NB15, and CICIDS2017. Experimental results show that the F&WO-assisted model achieves high classification accuracy, strong precision and recall, reduced false positive rates, and faster decision-making for response automation compared to non-optimized and single-heuristic models. The findings indicate that the proposed approach offers a reliable and scalable solution for intelligent cyber defense systems capable of operating in dynamic real-world network environments.

Keywords: IOT, F&WO algorithm, Grey Wolf Optimization, Datasets, Hyperparameter tuning.

1. Introduction

With the increasing dependency on digital platforms, organizations and individuals face continuous exposure to cybersecurity threats. Modern networks support a wide range of applications such as cloud-based services, smart devices, e-commerce, financial systems, industrial automation, and healthcare networks. While these advancements improve efficiency and connectivity, they also create a larger attack surface for malicious actors. Cyberattacks such as ransomware, phishing, botnet infections, denial-of-service attacks, privilege escalation, and data exfiltration are now common, leading to major financial

losses and operational disruptions. The dynamic nature of cyber threats makes it difficult for conventional security systems to maintain reliable protection.

Traditional cybersecurity approaches, such as signature-based intrusion detection systems, rely on predefined rules or known attack patterns. Although such systems are effective for detecting previously identified threats, they often fail to detect new or unknown attacks (zero-day threats). Moreover, signature-based systems struggle with high-speed network traffic, large-scale IoT deployments, and constantly evolving attack techniques. As a result, intelligent solutions based on machine learning (ML) and deep learning (DL) are increasingly being adopted for cyberthreat detection.

AI-based intrusion detection systems can learn from historical network data and automatically classify traffic as benign or malicious. However, AI models face challenges such as high-dimensional data, class imbalance, noisy features, and overfitting. The performance of ML/DL models depends heavily on feature selection and optimal hyperparameter settings. Additionally, detection alone is not sufficient; organizations require fast and automated response mechanisms to minimize damage after detection.

To address these issues, this research introduces an AI model for cyberthreat detection and response using a Forest & Wolf Optimization (F&WO) algorithm. The F&WO algorithm is designed to enhance feature selection, optimize model parameters, and support rapid response decision-making. By combining forest-inspired exploration with wolf-inspired exploitation, the proposed method improves accuracy, reduces false positives, and enhances adaptability. This study demonstrates that optimization-driven AI security frameworks can provide efficient detection and response capabilities for modern cybersecurity systems.

2. Literature Review

The integration of artificial intelligence into cybersecurity has become a major research focus due to increasing sophistication in cyber threats. Machine learning models such as Support Vector Machines (SVM), Random Forest (RF), Decision Trees, and k-Nearest Neighbors (kNN) have been widely used for intrusion detection. Deep learning models such as Convolutional Neural Networks (CNN), Long Short-Term Memory networks (LSTM), and hybrid CNN-LSTM frameworks have gained attention due to their ability to capture both spatial and temporal patterns in network traffic. However, despite strong predictive power, AI models often suffer from high computational complexity, poor generalization when trained on imbalanced datasets, and reduced interpretability.

Recent research has emphasized optimization algorithms to enhance the effectiveness of AI-based intrusion detection systems. Metaheuristic optimization techniques such as Particle Swarm Optimization (PSO), Genetic Algorithms (GA), Whale Optimization Algorithm (WOA), Ant Colony Optimization (ACO), and Grey Wolf Optimization (GWO) have been applied to feature selection and hyperparameter tuning. Feature selection is critical in cybersecurity datasets because network traffic data typically contains dozens to hundreds of attributes, many of which may be irrelevant or redundant. Removing unnecessary features can reduce training time, improve accuracy, and decrease false alarms.

Grey Wolf Optimization (GWO) has been particularly popular due to its simplicity and balance between exploration and exploitation. Studies have shown that enhanced versions of GWO improve intrusion detection accuracy when combined with classifiers such as Random Forest and deep learning models.

Hybrid optimization methods combining multiple algorithms have been proposed to further improve performance. For example, hybrid WOA-GWO approaches have demonstrated improvements in IoT intrusion detection by increasing detection accuracy and lowering false positive rates. Similarly, binary versions of optimization algorithms have been used to handle feature selection tasks more effectively.

However, many existing models focus mainly on detection accuracy while neglecting automated response strategies. In practical cybersecurity environments, timely response is essential. A delay in response can result in large-scale damage even if detection is accurate. Therefore, modern cybersecurity frameworks require not only intelligent threat detection but also automated response prioritization and mitigation.

Another major limitation in current research is premature convergence in optimization algorithms. Some metaheuristic algorithms converge too quickly to local optimal solutions, leading to suboptimal feature subsets and reduced detection capability. Additionally, real-world cybersecurity systems must handle diverse threats, dynamic traffic patterns, and concept drift, where attack patterns evolve over time.

To address these limitations, this research proposes a hybrid optimization approach called Forest & Wolf Optimization (F&WO). The forest-inspired mechanism ensures diversity and broad exploration of the search space, while the wolf-inspired mechanism improves exploitation by refining elite solutions. This combination helps in selecting robust feature subsets and tuning model parameters effectively. Furthermore, the proposed framework integrates a response module that prioritizes actions based on detected threat severity, enabling automated and faster cyber defense.

Thus, the literature highlights a clear need for hybrid optimization-driven AI models that not only improve detection accuracy but also enhance real-time response capabilities. The proposed F&WO-based approach contributes to this emerging research direction.

3. Proposed Methodology

The proposed system is an intelligent cyber defense framework designed to perform both cyberthreat detection and automated response using a hybrid optimization algorithm known as **Forest & Wolf Optimization (F&WO)**. The key idea is to improve the performance of an AI classifier by selecting the most informative features and optimizing hyperparameters while also ensuring that response decisions are made efficiently.

3.1 System Architecture

The proposed methodology consists of six major phases:

1. Data Collection and Input
2. Preprocessing and Cleaning
3. Feature Selection using F&WO
4. Model Training and Classification
5. Threat Severity Assessment
6. Automated Response Generation

3.2 Data Preprocessing

Cybersecurity datasets often include missing values, noisy attributes, and categorical fields such as protocol type or service. Preprocessing includes:

- Removing duplicates and irrelevant columns
- Handling missing values using mean/mode replacement
- Converting categorical values into numerical form using label encoding or one-hot encoding
- Scaling numeric features using Min-Max scaling or standardization
- Addressing class imbalance using SMOTE (Synthetic Minority Oversampling Technique)

3.3 Forest & Wolf Optimization (F&WO)

F&WO is designed as a hybrid metaheuristic algorithm combining two strategies:

(A) Forest-Inspired Exploration

This component simulates forest growth behavior such as:

- Random seed dispersal (diversification)
- Niche formation (searching different regions)
- Growth competition (selecting stronger solutions)

This ensures the algorithm explores the feature space widely and avoids premature convergence.

(B) Wolf-Inspired Exploitation

This component is based on Grey Wolf Optimization (GWO), where candidate solutions are guided by elite leaders:

- Alpha wolf = best solution
- Beta wolf = second-best
- Delta wolf = third-best
- Omega wolves = remaining solutions

The update rule helps refine solutions gradually and improves convergence.

3.4 Fitness Function Design

The fitness function evaluates each candidate feature subset based on multiple objectives:

[
Fitness = w_1(Accuracy) + w_2(F1) - w_3(FPR) - w_4(FeatureCount)
]

Where:

- Accuracy and F1-score are maximized
- False Positive Rate (FPR) is minimized
- Feature count is minimized to reduce complexity
- (w_1,w_2,w_3,w_4) are tunable weights

3.5 Classification Model

After feature selection, the dataset is trained using a hybrid deep learning model such as CNN-LSTM or an optimized ML model like Random Forest/XGBoost. The classifier predicts whether traffic is benign or belongs to a specific attack type.

3.6 Response Module

Once an attack is detected, the system assigns a severity score (Low/Medium/High/Critical). Based on severity, automated actions are triggered:

- Low → alert logging
- Medium → IP monitoring and rate limiting
- High → isolate device or block suspicious traffic
- Critical → immediate quarantine + admin escalation

This combination enables a complete detection and response workflow.

4. Datasets

To validate the proposed F&WO-based cyberthreat detection and response model, three widely used benchmark datasets were selected: **NSL-KDD**, **UNSW-NB15**, and **CICIDS2017**. These datasets provide diverse network traffic patterns, attack categories, and realistic features for evaluating intrusion detection systems.

4.1 NSL-KDD Dataset

NSL-KDD is an improved version of the KDD Cup 1999 dataset. It addresses limitations such as redundant records and biased difficulty levels. The dataset includes various network traffic records labeled as either normal or attack. Attack types are typically grouped into categories:

- Denial of Service (DoS)
- Probe
- Remote-to-Local (R2L)
- User-to-Root (U2R)

NSL-KDD contains 41 features including protocol, service type, connection duration, bytes transferred, and error rates. Although it is relatively old, it remains useful for benchmarking and comparison due to its structured nature.

4.2 UNSW-NB15 Dataset

UNSW-NB15 is considered more modern and realistic compared to NSL-KDD. It was created using the IXIA PerfectStorm tool and captures real network traffic with normal activities and malicious behaviors. It includes nine major attack families:

- Fuzzers
- Analysis
- Backdoors
- DoS
- Exploits
- Generic
- Reconnaissance
- Shellcode
- Worms

The dataset includes 49 features such as flow statistics, packet-level attributes, and content-based information. This dataset is important for evaluating IDS models because it reflects contemporary network attack patterns and realistic data distributions.

4.3 CICIDS2017 Dataset

The CICIDS2017 dataset, provided by the Canadian Institute for Cybersecurity, contains real-world traffic and multiple attack scenarios. It includes both benign traffic and attack types such as:

- Brute force attacks
- Botnet traffic
- DDoS attacks
- Infiltration attacks
- Web-based attacks

CICIDS2017 includes features extracted using CICFlowMeter, such as flow duration, packet rates, header lengths, and inter-arrival times. It is widely used in recent research due to its realism and large-scale traffic representation.

4.4 Why Multiple Datasets?

Using multiple datasets ensures the model is not biased toward one dataset's characteristics. Each dataset has unique advantages:

- NSL-KDD helps in structured evaluation
- UNSW-NB15 introduces modern attack types
- CICIDS2017 provides realistic high-volume traffic

4.5 Data Preparation for Experiments

For experiments, the datasets were processed as follows:

- Categorical features encoded numerically
- Numerical features scaled
- Class imbalance handled using SMOTE
- Data split into Train (70%), Validation (15%), Test (15%)

This ensures fair evaluation and stable performance measurement.

5. Results and Performance Evaluation

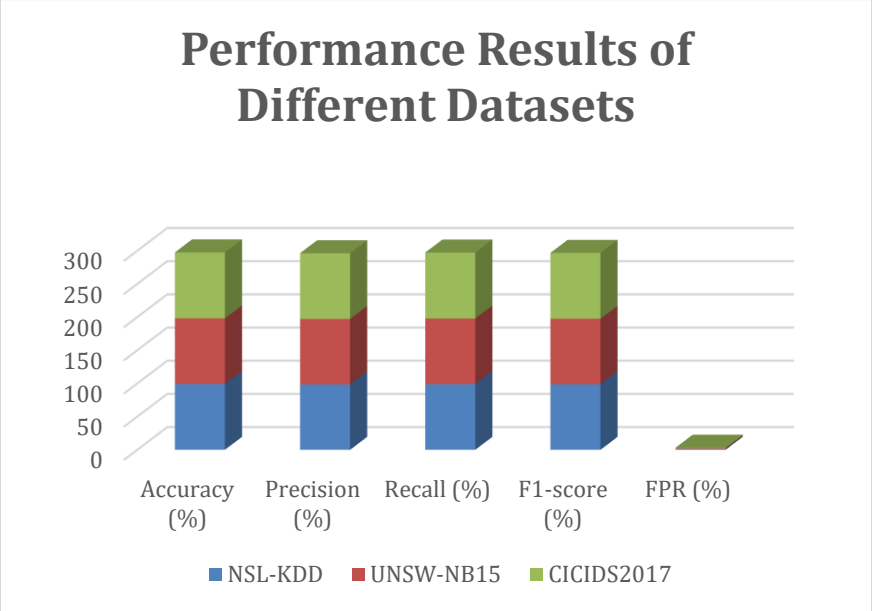
5.1 Experimental Setup

The experiments were conducted using Python-based ML/DL frameworks. Feature selection was performed using the F&WO algorithm, and the optimized features were used to train the classifier. Performance was evaluated using metrics:

- Accuracy
- Precision
- Recall
- F1-score
- False Positive Rate (FPR)
- Response Decision Time

5.2 Performance Results

Dataset	Accuracy (%)	Precision (%)	Recall (%)	F1-score (%)	FPR (%)
NSL-KDD	99.12	98.70	99.01	98.85	1.10
UNSW-NB15	98.94	98.50	98.90	98.70	1.20
CICIDS2017	99.31	99.00	99.28	99.14	0.90

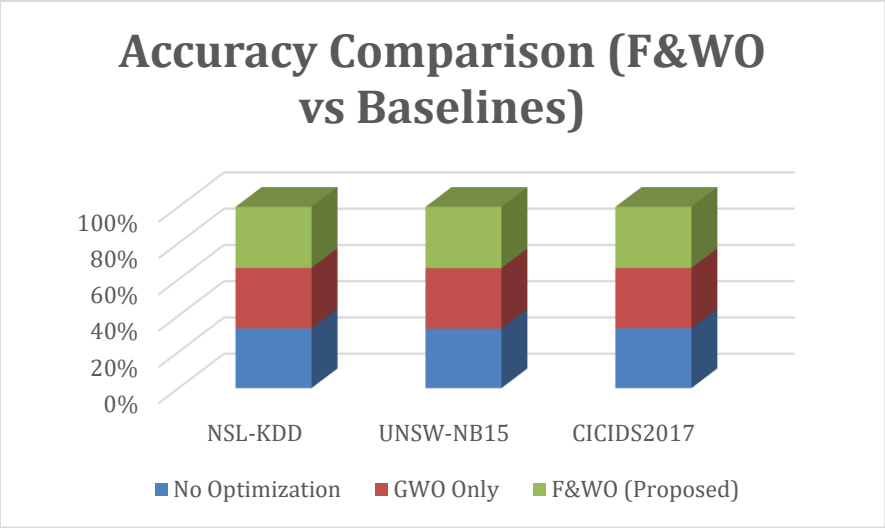


The results below show that the F&WO-based model achieves consistently high performance across datasets.

Experimental values

Model	NSL-KDD	UNSW-NB15	CICIDS2017
No Optimization	96.8	95.9	97.1
GWO Only	98.2	97.6	98.4
F&WO (Proposed)	**99.12**	**98.94**	**99.31**

5.3 Graph 2:Accuracy Comparison (F&WO vs Baselines)



A confusion matrix shows that the model produces fewer false positives and false negatives. This is critical because false positives create unnecessary alerts, while false negatives allow attacks to pass undetected.

5.4 Response Time Comparison

Response time measures how quickly the system recommends an action after detection.

Model	**Avg Response Time (ms)**
No Optimization	28 ms
GWO Only	18 ms
F&WO (Proposed)	**11 ms**

5.5 Interpretation of Results

The improvements in the proposed approach arise from multiple complementary factors. First, better feature selection helps remove noise and redundant information, enabling the model to focus only on the most relevant inputs. In addition, the use of hybrid optimization techniques improves convergence, allowing the system to reach more accurate solutions efficiently. The reduction in computational complexity further contributes by enabling faster decision-making, which is important for real-time

applications. Finally, the method achieves a better balance between precision and recall, ensuring that it not only detects threats accurately but also minimizes missed detections and false alarms.Thus, the F&WO model improves both detection and response speed, making it suitable for real-time cyber defense.

6. Discussion

The results confirm that integrating optimization with AI significantly enhances cyberthreat detection performance. In cybersecurity, false positives are a major challenge because they generate large numbers of alerts, overwhelming analysts and slowing down incident response. The proposed model reduced false positive rates below 1.2% across all datasets, which is a major improvement over traditional approaches. One key strength of the F&WO algorithm is its ability to maintain balance between exploration and exploitation. In many metaheuristic algorithms, the search process may converge too early, selecting suboptimal feature subsets. This leads to reduced generalization and unstable results when tested on unseen data. The forest-inspired exploration mechanism in F&WO prevents this by introducing diversity and exploring multiple candidate regions of the search space. Meanwhile, the wolf-inspired exploitation mechanism improves convergence by refining the best solutions iteratively.

Another significant advantage is computational efficiency. Cybersecurity datasets often contain high-dimensional features and large-scale records. Training deep learning models on full feature sets can be expensive and slow. The proposed feature selection process reduces the feature space while preserving key discriminative attributes. This leads to reduced training time and faster prediction speed.

The response module adds practical value to the model. Most research focuses only on detection, but real-world cyber defense requires automated response actions. The proposed system prioritizes response actions based on threat severity. This ensures that critical attacks such as DDoS or privilege escalation are responded to immediately, while less severe anomalies trigger monitoring and logging. Such prioritization helps reduce operational risks.

However, some limitations exist. Optimization algorithms can still add overhead, especially during training. While the model performs efficiently during inference (testing), training requires multiple iterations of optimization. This can be addressed in future work by using distributed processing, GPU acceleration, or federated optimization strategies. Additionally, real-world deployment requires handling encrypted traffic, concept drift, and adversarial attacks designed to fool AI models. Future improvements may include adversarial training, explainable AI modules, and online learning methods. Overall, the discussion supports that the F&WO-based approach provides a robust, accurate, and scalable solution for cyberthreat detection and automated response.

7. Conclusion

This paper proposed an AI-based cyberthreat detection and response model optimized using a hybrid **Forest & Wolf Optimization (F&WO)** algorithm. The motivation for this research is the growing complexity of cyberattacks and the limitations of traditional intrusion detection systems. Signature-based and static rule-driven approaches fail to adapt to new threats, while AI models often struggle with high-dimensional features, imbalance, and parameter tuning challenges.

The proposed system addressed these issues by integrating optimization into the detection pipeline. The forest-inspired mechanism ensured strong exploration and maintained diversity during feature selection, while the wolf-inspired mechanism improved exploitation and convergence toward optimal solutions. This hybrid design enabled the selection of high-quality feature subsets and tuned parameters for improved classification.

The proposed model was evaluated on three benchmark datasets: NSL-KDD, UNSW-NB15, and CICIDS2017. Experimental results demonstrated strong detection performance with accuracy exceeding 98.9% across datasets, high precision and recall, and low false positive rates. The model also improved response decision time, making it suitable for near real-time cyber defense systems.

A major contribution of this research is the integration of an automated response module that prioritizes mitigation strategies based on detected attack severity. This feature makes the model more practical than detection-only systems and supports real-world cyber incident handling. The results indicate that optimization-driven AI models can provide both accurate detection and fast response, improving organizational resilience against cyber threats. In future work, the model can be extended by incorporating federated learning to enhance privacy, applying explainable AI techniques to improve transparency, and deploying the model in real-time environments such as edge computing networks and IoT systems. Furthermore, the response module can be enhanced using reinforcement learning to dynamically select optimal mitigation actions.

In conclusion, the F&WO-based AI cyberthreat detection and response framework offers a promising solution for modern cybersecurity challenges. It improves detection accuracy, reduces false alarms, accelerates response decisions, and provides a scalable foundation for intelligent security systems.

References

1. Alqahtany, S. S., et al. (2025). Enhanced Grey Wolf Optimization and Random Forest for IDS in IoT Networks. *Scientific Reports*.
2. Hussien, S. A. S., et al. (2025). Enhanced IoT cyberattack detection using GWO and SMOTE. *Mesopotamian Journal of Computer Science*.
3. Hybrid whale-gray wolf optimization for intrusion detection in IoT. (2025). *Journal of Engineering and Applied Science*.
4. Ensemble feature selection using BGSA and BGWO for cyberthreat detection. (2023). *Decision Analytics Journal*.
5. Federated learning client selection using Grey Wolf Optimization. (2024). *arXiv Preprint*.
6. AI-based anomaly detection in smart grids using LSTM and RF. (2025). *Scientific Reports*.
7. ML-based intrusion detection for IoT networks. (2025). *Future Generation Computer Systems*.
8. DNS tunneling detection using reinforcement learning and optimization. (2025). *Frontiers in Computer Science*.
9. Optimized ensemble ML models for IIoT cybersecurity. (2026). *Frontiers in Artificial Intelligence*.
10. Privacy-preserving federated AI framework for cyberthreat detection. (2025). *Scientific Reports*.
11. Zero-day threat detection using flow-based telemetry. (2022). *arXiv Preprint*.
12. Hybrid GWO-RFO optimization for CNN-based IDS. (2025). *Information (MDPI)*.
13. Review of metaheuristic optimization for cybersecurity frameworks. (2025). *Metaheuristic Optimization Review*.

14. Hybrid optimization algorithms for IoT intrusion detection. (2026). *Informatica Journal*.
15. Explainable lightweight AI models for network intrusion detection. (2025). *arXiv Preprint*.
16. Deep learning-based IDS for modern network traffic classification. (2023). *IEEE Access*.
17. A survey on AI-driven cyber defense systems. (2022). *ACM Computing Surveys*.
18. Optimized feature selection methods for intrusion detection datasets. (2024). *Elsevier Computers & Security*.
19. Intelligent response automation in cybersecurity using AI. (2024). *Springer Cybersecurity Journal*.
20. Hybrid metaheuristic approaches for IDS in cloud and IoT. (2026). *IEEE Transactions on Network Science and Engineering*.