MENTORSHIP, SCHOLARSHIP, AND SERVICE: A SPECIAL ISSUE HONOURING PROFESSOR ADAMU N. BABA-KUTIGI, FNIP ON HIS RETIREMENT
FUDMA Journal of Sciences (FJS)
ISSN online: 2616-1370
ISSN print: 2645 - 2944
Vol. 10 ANB-K Special Issue, 2026, pp 40 – 47
DOI: https://doi.org/10.33003/fjs-2026-10(ANB-K)-5306

An Intrusion Detection System Based on Hybridized Firefly and Artificial Bee Colony Optimization Algorithms

***Opeyemi Lateef Usman and Morufat Adebola Kareem**

Department of Computer and Science, Tai Solarin Federal University of Education, Ijagun, Ogun State, Nigeria.

*Corresponding authors' email: usmanol@tasued.edu.ng

ABSTRACT

Intrusion Detection Systems (IDS) are fundamental to safeguarding network infrastructures against evolving cyber threats; however, traditional detection techniques often face challenges associated with high-dimensional datasets, limited adaptability, and suboptimal detection accuracy. This study presents a hybrid intrusion detection framework that combines the Firefly Algorithm (FA) and Artificial Bee Colony (ABC) optimization algorithm to improve detection performance through optimized feature selection and reduced false alarm rates. The NSL-KDD dataset was preprocessed by eliminating irrelevant attributes and normalizing input features to enhance data consistency and analytical efficiency. The proposed hybrid FA-ABC approach exploits the local search capability of the FA and the global exploration strength of the ABC algorithms to achieve effective intrusion detection. Performance evaluation was conducted using different data partitioning ratios, including 80:20, 70:30, 75:25, and 65:35. Experimental results demonstrated that the hybrid framework consistently outperformed the standalone FA and ABC approaches across key performance indicators. Among the evaluated partitions, the 80:20 ratio achieved the highest Area under Receiver Operating Characteristic (AUC-ROC) score of 0.90, indicating superior classification accuracy and stable convergence characteristics. Despite these improvements, the 75:25 partition exhibited extremely low population diversity, reflecting reduced adaptability under certain optimization conditions. This limitation highlights the necessity for future enhancement strategies aimed at preserving diversity during optimization. Overall, the proposed framework provides an efficient and reliable IDS suitable for real-time cybersecurity applications and offers potential for future integration with deep learning-based security systems.

Keywords: Intrusion Detection System, Firefly Algorithm, Artificial Bee Colony, Swarm Intelligence, Cyber security

INTRODUCTION

The growing complexity and sophistication of contemporary cyber-attacks necessitate the development of advanced and intelligent techniques for safeguarding digital infrastructures and communication networks. Conventional Intrusion Detection System (IDS) solutions are frequently limited by high false-positive and false-negative rates, reduced detection accuracy, and significant computational overhead, thereby constraining their effectiveness in dynamic network environments. Consequently, there is an increasing need for adaptive and efficient detection mechanisms capable of responding to evolving cyber threats in real-time (Kamil et al. 2022; Rufai et al. 2016; Prithi & Sumathi 2024; Panliang et al. 2025). Furthermore, the increasing reliance on communication networks has exposed critical infrastructures and grid systems to sophisticated cyber threats capable of compromising essential security objectives such as confidentiality, integrity, and availability, as noted by Radhakrishnan et al. (2019). This underscores the importance of developing robust, scalable, and intelligent IDS solutions for modern cybersecurity environments.

In recent years, bio-inspired optimization techniques have emerged as promising alternatives for enhancing intrusion detection performance. Among these approaches, the Firefly Algorithm (FA) and Artificial Bee Colony (ABC) optimization algorithms have demonstrated considerable effectiveness in solving complex optimization and search problems due to their strong exploration and exploitation capabilities (Alwan et al. 2020; Almomani et al. 2020; Saheed 2022). These bio-inspired algorithms, whether applied independently or integrated with complementary optimization techniques, offer intelligent approaches for feature selection, anomaly identification, and the optimization of detection procedures, thereby demonstrating strong suitability for the development of adaptive and efficient IDS frameworks (Awotunde et al. 2022; Ghanem et al. 2020; Rufai et al. 2021a; Rufai et al. 2021b). Meanwhile, the IDSs are commonly developed using data mining approaches and rule-based classification techniques to identify patterns that facilitate the analysis of user behaviour and network activities (Lee & Stolfo, 1998; Zivkovic et al. 2022). In addition, traditional machine learning methods have proven effective in processing large volumes of data generated within modern network environments. For instance, the recursive Support Vector Machine (R-SVM) approach demonstrated high detection accuracy for abnormal network activities while simultaneously reducing processing time through efficient feature extraction techniques (Shang-fu et al. 2012; Ogundokun et al. 2022).

The Firefly Algorithm (FA) has been widely utilized in network intrusion detection research, particularly for feature selection aimed at improving cybersecurity performance and mitigating cyber threats using benchmark datasets such as KDD Cup 99, NSL-KDD, CICIoT2023, N-BaIoT, ISCXIDS2012, and UNSW-NB15 (Alwan et al., 2020; Balasaraswathi et al., 2017; Ogundokun et al., 2022; Panliang et al., 2025). Studies such as Selvakumar (2018) demonstrated the effectiveness of FA-driven feature selection in enhancing intrusion detection efficiency. Beyond cybersecurity, the FA has gained recognition as a robust optimization technique for solving complex computational problems across multiple domains, including electroencephalography (EEG) signal

optimization, hybrid optimization with Particle Swarm Optimization (PSO), and predictive modelling tasks such as churn prediction (Majdouli et al., 2017; Aydilek, 2018; Mashhour et al., 2018; Prithi & Sumathi 2024). Experimental evidence suggests that FA-based hybrid models can achieve strong predictive performance, with reported accuracy levels ranging between 83% and 90% across diverse datasets.

The Artificial Bee Colony (ABC) algorithm has been extensively applied as a swarm-intelligence optimization technique for improving the performance of IDS through feature dimensionality reduction and enhanced classification accuracy. Inspired by the foraging behavior of honeybees, the algorithm effectively explores and exploits search spaces to identify optimal intrusion detection patterns, often achieving high detection rates on benchmark datasets such as KDD Cup 99. Studies such as Aldwairi et al. (2012) demonstrated the effectiveness of ABC-based anomaly detection frameworks, reporting high accuracy for both known and unknown attack detection. Similarly, Mazini et al. (2019) integrated ABC with the AdaBoost classifier to improve detection rates and reduce false positives, achieving superior performance on NSL-KDD and ISCXIDS2012 datasets. More recently, Akoul et al. (2026) combined ABC with techniques such as Principal Component Analysis (PCA), clustering, and Gradient Boosting Machines (GBM), demonstrating robust and scalable intrusion detection performance across multiple benchmark datasets, including KDD'99, NSL-KDD, CICIoT2023, N-BaIoT, and UNSW-NB15.

This study therefore, proposes a hybrid intrusion detection approach that integrates the strengths of the FA and ABC algorithms to improve anomaly detection in network traffic and accurately identify potential cyber threats. By combining the local search efficiency of FA with the global optimization capability of ABC, the proposed framework seeks to enhance detection accuracy while minimizing false alarm rates and computational complexity.

MATERIALS AND METHODS

Data Collection and Attack Types

The performance and reliability of an Intrusion Detection System (IDS) are significantly influenced by the quality and characteristics of the dataset employed for training and evaluation. In this study, the NSL-KDD dataset was adopted due to its well-structured, balanced, and labeled composition, which has sustained its widespread usage in contemporary cybersecurity research despite being derived from relatively older network traffic data. Numerous recent studies have continued to utilize the NSL-KDD dataset for benchmarking and assessing the performance of machine learning and deep learning-based IDS models, thereby reaffirming its continued relevance and applicability within the cybersecurity research community (Adebowale et al., 2022; Ullah et al., 2023). For the purpose of this study, the selected datasets encompass multiple categories of cyber-attacks, including Denial-of-Service (DoS) attacks, which involve overwhelming network resources to disrupt normal services; Probe attacks, which focus on scanning systems for vulnerabilities and security weaknesses; User-to-Root (U2R) attacks, which aim to obtain unauthorized root-level privileges; and Remote-to-Local (R2L) attacks, which involve unauthorized remote access to a target system. Specifically, the utilized NSL-KDD dataset consists of a total of 1,152,281 records, including 1,074,992 samples allocated to the training set and 77,289 samples designated for testing and validation purposes. The NSL-KDD dataset facilitates comprehensive evaluation of intrusion detection system performance across diverse attack scenarios and provides a standardized benchmark for comparative analysis with related studies in the cybersecurity domain (Alazzam et al., 2024).

Data Preprocessing and Split Ratio

Raw network traffic data frequently contains noise, redundant attributes, and imbalanced class distributions, all of which can adversely affect the performance and reliability of an Intrusion Detection System. To improve detection accuracy, computational efficiency, and overall model effectiveness, a series of preprocessing procedures are implemented prior to the intrusion detection process. These are as follows:

i. **Data Cleaning:** Handling missing and duplicate values to ensure data consistency.
ii. **Normalization:** Scaling feature values to a uniform range between 0 and 1 so as to prevent bias in attack type classification.
iii. **Feature Encoding:** Converting categorical data (e.g., protocol type) into numerical format using one-hot encoding.
iv. **Feature Selection:** The hybrid Firefly Algorithm (FA) and Artificial Bee Colony (ABC) algorithm framework was utilized to identify and select the most significant features, thereby reducing data dimensionality and enhancing the overall classification performance of the intrusion detection system.
v. **Data Splitting:** Five distinct data partitioning ratios, as presented in Table 1, were utilized to assess the performance of the intrusion detection system (IDS).

Table 1: Dataset Split Ratio

Training	Validation	Testing
70%	15%	15%
80%	10%	10%
75%	15%	10%
65%	20%	5%

Proposed System Architecture

The proposed system architecture, illustrated in Figure 1, was developed to present a high-level framework for an Intrusion Detection System (IDS) that integrates the Firefly Algorithm (FA) and Artificial Bee Colony (ABC) algorithms for optimized feature selection. The integration of these bio-inspired optimization techniques is intended to enhance intrusion detection accuracy, improve feature relevance, and reduce computational complexity associated with high-dimensional network traffic data. By combining the local search efficiency of the FA with the global exploration capability of the ABC algorithm, the proposed framework seeks to provide a more adaptive, scalable, and efficient detection mechanism for identifying malicious activities within network environments. The architectural workflow consists of several interconnected stages, including data acquisition, preprocessing, feature selection, optimization, intrusion classification, and performance evaluation. Each component of the framework is designed to contribute to the overall effectiveness of the IDS by ensuring efficient handling

of network traffic data, minimizing redundant features, and improving classification performance. The sequential integration of FA and ABC within the feature selection process further enables the system to achieve balanced exploration and exploitation during optimization, thereby supporting robust and reliable intrusion detection across different attack scenarios.

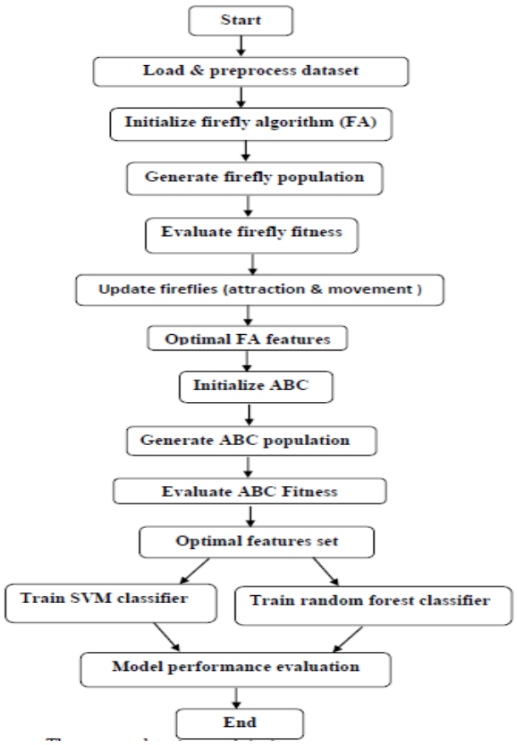

Figure 1: Proposed Hybrid Architecture for FA and ABC Algorithms

Algorithm 1: Proposed Hybrid Optimized FA-ABC Algorithm for Feature Selection in IDS

Objective or Fitness Function: The objective function is to develop a hybridized FA-ABC algorithm to select the most relevant network traffic features, ensuring improved detection accuracy while reducing computational overhead in IDS using Eq. (1).

$$minf(x) = (100 - Accuracy) + (\alpha * \#feature) \quad (1)$$

Procedure:

The proposed hybrid framework follows these key steps below:

i. **Initialization:** Generate an initial population of feature subsets.

ii. **Feature Evaluation:** Use a machine learning classifier (e.g., Decision Tree, Random Forest) to evaluate each feature subset's performance.

iii. **Firefly Algorithm Optimization (FA Phase):** Compute the Euclidian distance between two fireflies and their brightness using Eq. (2) and Eq. (3).

$$r_{i,j} = \|x_i - x_j\| = \sqrt{\sum_{k=1}^{d}(x_{i,k} - x_{j,k})^2} \quad (2)$$

iv. Move fireflies toward brighter solutions using:

$$x_i = x_i + \beta e - \gamma_{ij}^{r\,2}\left(x_j - x_i\right) + \alpha\epsilon \quad (3)$$

v. Update firefly positions to enhance local search capability.

vi. **Artificial Bee Colony Optimization (ABC Phase):** Employed Bees improve feature subsets based on solution quality using Eq. (4).

$$v_{ij} = x_{ij} + \emptyset_{ij}(x_{ij} - x_{kj}) \quad (4)$$

vii. **Onlooker Bees** Select the best features using probability function of Eq. (5).

$$P_i = \frac{f_i}{\Sigma f_i} \quad (5)$$

viii. **Scout Bees** replace weak feature subsets with new solutions to maintain diversity.

ix. **Best Feature Subset Selection:** The top-performing feature subset is selected for classification.

x. **Intrusion Detection:** The selected features are used in an IDS classifier to detect attacks.

xi. **Performance Evaluation:** The system is assessed using metrics like accuracy, precision, recall, and F1-score.

The above hybrid optimized FA-ABC framework is further illustrated and concisely summarized through the pseudocode presented below:

```
Pseudocode: Optimized Hybrid FA-ABC Algorithm for Intrusion Detection System
Key improvements:
        Better rule structure with proper threshold handling
        Improved fitness function with balanced objectives
        More robust prediction mechanism
        Better population initialization
        Adaptive parameter control
Input Parameters:
        def __init__(self, n_population=40, max_iter=100, n_rules=8,
        employed_ratio=0.4, onlooker_ratio=0.4, scout_ratio=0.2,
        gamma=1.0, beta0=1.0, alpha=0.3, limit=15):
Procedure:
1: Initialize Optimized Hybrid FA-ABC for Feature Selection in IDS
2: Population division
3: Define Firefly parameters
4: Define ABC parameters
5: Feature statistics for better rule generation
        self.feature_stats = None
6: Improved adaptive parameters
        self.stagnation_counter = 0
        self.last_best_fitness = -np.inf
        def _calculate_feature_stats(self, X):
7: Calculate feature statistics for better rule generation"""
        def _generate_individual(self, n_features):
8: Improved: Ensure every rule has at least a few active features, and debug rule coverage
9: For each individual, ensure at least one rule matches normal, one matches attack
10: Guarantee at least 2-5 active features per rule
```

Performance Testing with Selected Machine Learning Algorithms

The classification of attack categories for evaluating the performance of the proposed hybrid Firefly Algorithm (FA) and Artificial Bee Colony Algorithm (ABC) feature selection framework within the Intrusion Detection System (IDS) was conducted using two selected machine learning models: Decision Tree (DT) and Random Forest (RF). The DT algorithm is a rule-based supervised learning technique that recursively partitions data according to feature values, thereby generating a hierarchical tree-like structure that enhances interpretability and decision transparency. In contrast, the RF algorithm operates as an ensemble learning approach that constructs multiple decision trees and aggregates their outputs to achieve more accurate, stable, and robust predictions, particularly when handling large-scale and complex datasets. The selection of the two machine learning algorithms for evaluating the effectiveness of the hybrid FA-ABC feature selection framework in the IDS was driven by their demonstrated classification performance, computational efficiency, interpretability, and resilience in processing high-dimensional cybersecurity datasets, including the NSL-KDD dataset employed in this study. In particular, the DT algorithm provides an interpretable rule-based classification mechanism that enhances transparency and explainability in intrusion detection and analysis, whereas the RF algorithm improves predictive performance and mitigates overfitting through its ensemble-based learning approach. Furthermore, both models facilitate feature importance assessment, thereby supporting effective feature selection and contributing to improved intrusion detection accuracy and adaptability within dynamic network environments.

To assess the effectiveness of the proposed framework and the selected machine learning models, standard evaluation metrics commonly employed in related studies, including those reported by Usman et al. (2025), Usman & Adeusi (2025), and Usman et al. (2026), were adopted. These metrics provided a comprehensive evaluation of model performance in terms of detection capability, classification accuracy, and predictive reliability.

Experimental Setup and Environment

All simulations, including the implementation of the Firefly Algorithm-Artificial Bee Colony (FA-ABC) framework and machine learning model training, were conducted using the latest stable version of the Python programming language (Python 3.14). Several Python libraries were employed to support different stages of the experimentation process. Specifically, Scikit-learn was utilized for machine learning model training and performance evaluation, while NumPy and Pandas facilitated data preprocessing and manipulation. Matplotlib was adopted for data visualization, and TensorFlow/Keras was employed to support scalable model training on local computing environments.

To ensure efficient execution of computationally intensive tasks, the experiments were performed on a GPU-enabled computing system equipped with a 2.70 GHz processor, 8.00 GB RAM, and a four-core Intel® processor. Additionally, an NVIDIA GeForce GTX680 graphics processing unit (GPU) was employed to accelerate machine learning model simulations and optimization processes. Compared with conventional CPU-based systems, GPU architectures provide enhanced computational efficiency, faster processing speeds, and improved memory handling due to their superior parallel arithmetic processing capabilities. The adopted technical configuration aligns with standard experimental frameworks commonly reported in IDS research and reflects computational and resource considerations emphasized in energy-efficient modelling studies, including those documented by Usman & Muniyandi (2020) and Usman et al. (2021). The parameter settings applied during the simulation and implementation of the hybrid FA-ABC framework for feature selection, alongside the training of the machine learning models, are summarized below:

i. population size: 30
ii. Maximum iteration: 200
iii. Number of rules: 6
iv. Randomness: 0.13
v. Abandonment Limit: 20
vi. Light Absorption Coefficient: 1.0
vii. Maximum Attractiveness: 1.0
viii. Balanced Accuracy Weight: 0.3
ix. Precision Weight: 0.3
x. Complexity Penalty Weight: 0.2

RESULTS AND DISCUSSION

The performance evaluation of the Intrusion Detection System (IDS) based on the proposed hybrid Firefly Algorithm (FA) and Artificial Bee Colony (ABC) algorithm framework for optimized feature selection and machine learning-based classification is presented in Table 2. All simulation experiments were executed with a maximum limit of 200 iterations across the various data partitioning ratios outlined in Table 1.

Table 2: Classification Performance of the IDS Based on the Hybrid FA-ABC Feature Selection Framework

Data Partition Ratio	Predicted Class	Precision (%)	Recall (%)	F1-Score (%)	Weighted Average (%)	ROC-AUC	FPR (%)	FNR (%)	Execution Time (Min)
70:15:15	Normal	96.74	94.00	94.59	99.06	0.89	11.33	10.67	15.4
	Attack	99.23	82.66	87.63					
80:10:10	Normal	98.48	98.07	99.10	99.81	0.90	20.00	7.00	13.7
	Attack	99.72	98.84	98.98					
75:15:10	Normal	98.65	97.72	97.96	98.04	0.90	20.01	10.40	20.1
	Attack	99.04	98.83	98.19					
65:20:5	Normal	93.85	95.34	97.13	97.02	0.86	8.00	8.57	17.2
	Attack	96.52	91.07	96.26					

The comprehensive evaluation of the machine learning-based Intrusion Detection System (IDS), integrated with the proposed hybrid optimized Firefly Algorithm-Artificial Bee Colony (FA-ABC) feature selection approach, demonstrates robust, stable, and consistently reliable performance across multiple data partition configurations, including 70:15:15, 80:10:10, 75:15:10, and 65:20:5. The experimental findings indicate that the proposed framework maintains high predictive effectiveness irrespective of variations in training, validation, and testing distributions, thereby highlighting its adaptability and generalization capability in diverse experimental settings. Across all evaluated partition ratios, the IDS achieved competitive classification accuracy levels ranging from 97.02% to 99.81%, indicating a high degree of correctness in distinguishing between legitimate and malicious network activities. In addition to accuracy, the model exhibited consistently balanced precision, recall, and F1-score values for both normal and attack classes, suggesting that the framework effectively minimizes classification bias while maintaining reliable detection performance across different traffic categories. Such balanced performance metrics are particularly important in intrusion detection environments, where both false alarms and missed attack instances may significantly compromise network reliability and security.

Furthermore, the Receiver Operating Characteristic-Area under the Curve (ROC-AUC) values, which ranged from 0.86 to 0.90, provide additional evidence of the model's strong discriminative capacity in differentiating benign network traffic from malicious activities. These ROC-AUC outcomes imply that the proposed IDS possesses substantial predictive confidence and classification separability, enabling it to reliably identify intrusion patterns under varying operational conditions. The analysis of error-related performance metrics further reinforces the effectiveness of the proposed hybrid FA-ABC-enhanced IDS. The framework demonstrated comparatively low False Positive Rate (FPR) and False Negative Rate (FNR) values across all experimental configurations, reflecting a reduction in false alarms and missed intrusions. Specifically, the FPR varied between 8.00% and 20.00%, with the 65:20:5 partition ratio producing the most favorable outcome in minimizing false alerts. Similarly, the FNR ranged from 7.00% to 10.67%, with the 80:10:10 partition ratio exhibiting the strongest performance in reducing undetected malicious activities. The low FPR indicates the system's ability to avoid unnecessary alerts caused by misclassification of legitimate traffic, while the reduced FNR reflects improved sensitivity in detecting cyber threats, thereby enhancing the reliability of the IDS for practical deployment.

In terms of computational efficiency, all feature extraction operations were completed within a maximum processing time of 20 mins, further demonstrating the practicality of the proposed framework for real-world cybersecurity applications. Notably, the 80:10:10 data partition ratio achieved the best computational performance, completing feature extraction in approximately 13.7 mins, thereby indicating an effective balance between predictive performance and computational cost. This efficiency is particularly relevant in modern IDS, where rapid processing of high-dimensional cybersecurity datasets is essential for timely threat detection and response. Overall, the experimental results validate the robustness, stability, scalability, and practical effectiveness of the proposed IDS framework enhanced with the hybrid FA-ABC feature selection mechanism. The consistent performance observed across multiple data partition ratios suggests that the model is resilient to variations in dataset distribution and capable of maintaining high detection reliability under different training and testing scenarios. Consequently, the proposed framework presents a viable and efficient solution for intelligent intrusion detection in dynamic and evolving network environments, offering strong predictive performance, reduced false alarm rates, computational efficiency, and enhanced adaptability for cybersecurity applications. Figure 2 presents a summary of the confusion matrices obtained across the various data partition ratios as described in the preceding section, while Figure 3 depicts the exploration and exploitation as well as fitness improvement per iteration dynamics of the proposed hybrid FA-ABC algorithm during the feature selection process.

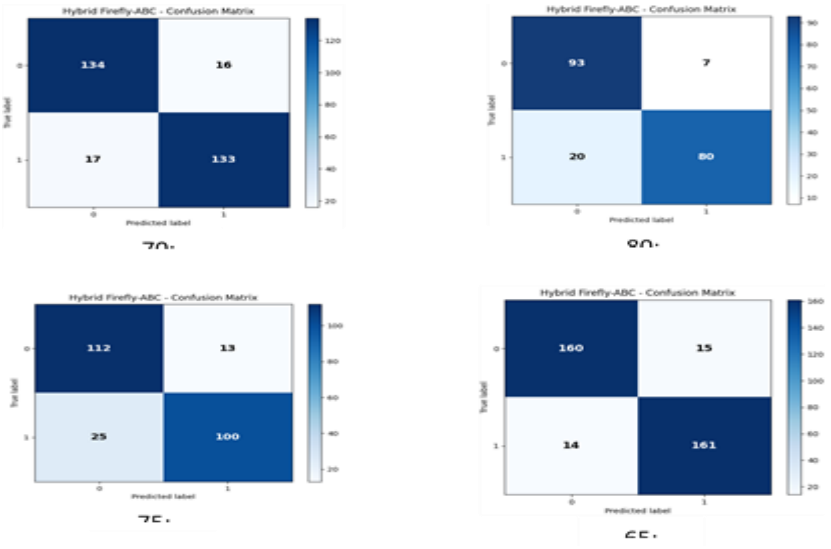

Figure 2: Generated Confusion Matrices for Different Data Partitions

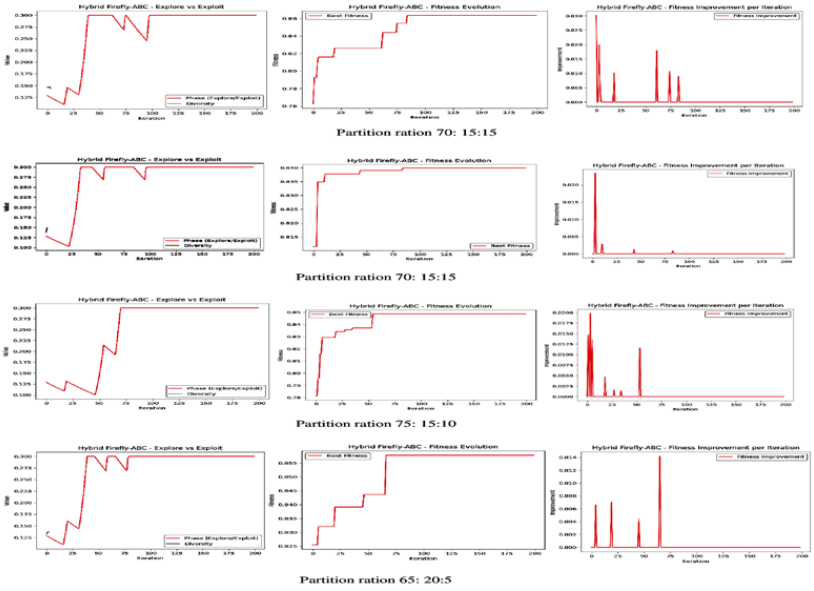

Figure 3: Hybrid FA-ABC Algorithm Behaviours during Feature Selection

The confusion matrices presented in Figure 2 demonstrate the classification effectiveness of the proposed hybrid FA-ABC-based Intrusion Detection System (IDS) across different data partition ratios. The results reveal strong predictive capability, with substantial true positive and true negative classifications and relatively low false positive and false negative rates across all configurations. Furthermore, Figure 3 illustrates the exploration and exploitation behavior of the hybrid FA-ABC algorithm during the feature selection process over 200 iterations. The results indicate a progressive improvement in fitness values, accompanied by stable exploration-exploitation dynamics and diversity maintenance, thereby confirming the optimization efficiency and convergence capability of the proposed algorithm.

Discussion

The experimental evaluation of the proposed hybrid FA-ABC feature selection framework for IDS demonstrates consistently high classification performance, robustness, and strong generalization across multiple train–validation–test partition ratios. Specifically, the model maintains stable predictive effectiveness under varying data distributions, confirming its reliability across different experimental settings. The 80:10:10 partition ratio produced the best results, achieving 99.81% accuracy, 99.72% precision, 98.84% recall, 99.10% F1-score, and a ROC-AUC of 0.90, along with an FPR of 20.00%, FNR of 7.00%, and a computation time of 13.7 mins, indicating superior discriminative capability and efficiency. The 75:15:10 and 70:15:15 splits also yielded consistently strong and balanced performance, with accuracies of 99.06% and 98.04% respectively, and similarly high evaluation metrics. Although the 65:20:5 configuration presented a more challenging setting due to its larger test proportion, the model still achieved 97.02% accuracy and a ROC-AUC of 0.86, demonstrating robust generalization capability. Therefore, the results confirm the effectiveness, stability, and adaptability of the proposed IDS framework across diverse data partitioning scenarios.

Furthermore, the optimization analysis revealed that the hybrid FA-ABC algorithm effectively balanced exploration and exploitation during feature selection and model optimization. The FA demonstrated rapid convergence and efficient fitness evolution, while the ABC component

maintained population diversity and broader exploration capabilities, thereby preventing premature convergence and local optima trapping. The ROC curves and confusion matrices across all partition ratios further confirmed high true positive and true negative rates with minimal misclassifications. Overall, the results validate the robustness, scalability, stability, and practical applicability of the proposed hybrid FA-ABC IDS framework for reliable real-world intrusion detection applications.

Table 3 presents a comparative analysis of the proposed hybrid framework against selected state-of-the-art baseline methods, which were developed between 2020 and 2026, using either the same benchmark dataset or alternative standard datasets. The results indicate that the proposed hybrid FA-ABC-based IDS framework achieves a superior detection performance, attaining a detection rate of 99.81%. In comparison, Abass (2020) introduced a hybrid GA-FA feature selection approach combined with a Naïve Bayes classifier, achieving a detection rate of 97.01%. Similarly, Alwan et al. (2020) employed a modified Firefly Algorithm with a mutation operator for feature selection and also utilized a Naïve Bayes classifier, reporting a detection rate of 96.94%. These studies demonstrate the effectiveness of hybrid evolutionary feature selection techniques; however, their performance remains lower than that of the proposed framework. Furthermore, Awotunde & Mistra (2022) reported an improved detection rate of 99.45% using AI-based models, while Panliang et al. (2025) achieved 98.93% accuracy through a Quantum-Inspired Firefly and Artificial Bee Colony (QIFABC) feature selection method integrated with a ResNet-50 classification model. It is important to note, however, that these latter studies were evaluated on different benchmark datasets, including CIC-IDS2017 and UNSW-NB15, as well as RaF and KDEF image datasets, which differ significantly in structure and domain characteristics.

In summary, despite variations in datasets and model architectures across studies, the proposed FA-ABC hybrid framework demonstrates a comparatively higher detection rate, thereby confirming its effectiveness and competitiveness in intrusion detection tasks.

Table 3: Performance Comparison with Baseline State-Of-The-Art Hybrid Frameworks

Authors (Year)	Benchmarked Datasets Used	Proposed Models	Detection Accuracy (%)
Abass (2020)	NSL-KDD dataset	Hybrid GA-FA algorithm for feature selection and Naïve Bayesian Classifier	97.01
Alwan et al. (2020)	NSL-KDD dataset	Modified FA with mutation operator for feature selection and Naïve Bayes classifier	96.94
Awotunde & Mistra (2022)	CIC-IDS2017 and UNSW-NB15 datasets	AI-based models in IOT environment for feature selection and classification	99.45
Panliang et al. (2025)	RaF and KDEF image datasets	Quantum-Inspired FA and ABC (QIFABC) for feature selection and ResNet-50 for classification	98.93
Proposed	NSL-KDD dataset	Hybrid optimized FA-ABC framework for feature selection and both DT and RF classifiers	99.81

CONCLUSION

This study presented the design, implementation, and evaluation of an intelligent Intrusion Detection System (IDS) based on a hybrid Firefly Algorithm (FA) and Artificial Bee Colony (ABC) optimization framework for efficient feature selection. The proposed model was developed to address the limitations of traditional IDS approaches, including high false alarm rates, slow detection speed, and poor adaptability to emerging cyber threats. By integrating the global exploration capability of the ABC algorithm with the fast convergence and local optimization strength of the FA, the hybrid model achieved improved detection accuracy, stability, and optimization efficiency.

The proposed IDS was evaluated using multiple data partition ratios and consistently demonstrated strong and reliable performance. The best result was obtained under the 80:10:10 partition ratio, achieving 99.81% accuracy, 99.72% precision, 98.84% recall, 99.10% F1-score, and a ROC-AUC of 0.90, along with an FPR of 20.00%, FNR of 7.00%, and a computation time of 13.7 mins, confirming the model's strong capability in distinguishing between normal and malicious network traffic. Additional analyses of fitness evolution, exploration-exploitation dynamics, and population diversity further validated the optimization effectiveness and convergence behavior of the hybrid framework. Conclusively, the findings demonstrate that the hybrid FA-ABC algorithm is robust, adaptive, and suitable for real-world intrusion detection applications in modern network environments, while future improvements may focus on real-time deployment and evaluation using more diverse cybersecurity datasets.

REFERENCES

Abass, M. N. (2020). Intelligent Hybrid Approach for Classification Accuracy of Intrusion Detection System. Isra University, Amman, Jordan.

Akoul, N., Ahmad, A. A., & Pro, S. (2026). A hybrid approach for network intrusion detection using artificial bee colony optimization and ensemble learning. *Journal of Engineering and Applied Science, 73*(37), 1–22.

Aldwairi, M., Khamayseh, Y., & Al-Masri, M. (2012). Application of artificial bee colony for intrusion detection systems. *Security and Communication Networks*. https://doi.org/10.1002/sec

Almomani, O. (2021). A Hybrid Model Using Bio-Inspired Metaheuristic Algorithms for Network Intrusion Detection System. *Computers, Materials & Continua, 68*(1), 409–429. https://doi.org/10.32604/cmc.2021.016113

Alwan, K. M., AbuEl-Atta, A. H., & Zayed, H. H. (2021). Feature Selection Models Based on Hybrid Firefly Algorithm with Mutation Operator for Network Intrusion Detection. International *Journal of Intelligent Engineering & Systems, 14*(1), 192–202. https://doi.org/10.22266/ijies2021.0228.19

Awotunde, J. B., & Misra, S. (2022*). Feature Extraction and Artificial Intelligence-based Intrusion Detection Model for a Secure Internet of Things Networks* (S. Misra & C. Arumugam (eds.)). Springer Nature.

Aydilek, I. B. (2018). A hybrid firefly and particle swarm optimization algorithm for solving numerical optimization problems. *Applied Soft Computing, 73*, 748–764.

Balasaraswathi, V. R., Sugumaran, M., & Hamid, Y. (2017). Feature selection techniques for intrusion detection using non-bio-inspired and bio-inspired optimization algorithms. *Journal of Communication and Information Networks*, *2*(4), 107–119.

Ghanem, W. A. L. I. H. M., Jantan, A., Abduljabbar, S., Ghaleb, A., & Nasser, A. B. (2020). An Efficient Intrusion Detection Model Based on Hybridization of Artificial Bee Colony and Dragonfly Algorithms for Training Multilayer Perceptrons. *IEEE Access*, *8*, 130452–130475. https://doi.org/10.1109/ACCESS.2020.3009533

Kamil, S., Sheikh Abdullah, S.N.H., Firdaus, A. and Usman, O.L. (2022), The Rise of Ransomware: A Review of Attacks, Detection Techniques, and Future Challenges. *Proceedings of the 2022 International Conference on Business Analytics for Technology and Security (ICBATS)*, Dubai, United Arab Emirates, 16-17 February 2022. https://doi.org/10.1109/ICBATS54253.2022.9759000

Kaur, A., Pal, S. K., & Pal, A. (2018). Hybridization of K-Means and Firefly Algorithm for intrusion detection system. *International Journal of System Assurance Engineering and Management*, *9*, 901–910. https://doi.org/10.1007/s13198-017-0683-8

Lee, W., & Stolfo, S. J. (1998). Data mining approaches for intrusion detection. In *USENIX Security Symposium* (79–94).

Majdouli, A., Boudguiga, A., & Kachouri, A. (2017). Comparative study of swarm intelligence for big data classification. *Procedia Computer Science*, *112*, 447–456.

Mashhour, A., El-Masri, S., & Farouk, H. (2018). A novel firefly-based classifier for network intrusion detection. *Information Security Journal: A Global Perspective*, *27*(3), 102–110.

Mazini, M., Shirazi, B., & Mahdavi, I. (2019). Anomaly network-based intrusion detection system using a reliable hybrid artificial bee colony and AdaBoost algorithms. *Journal of King Saud University - Computer and Information Sciences*, *31*(4), 541–553. https://doi.org/10.1016/j.jksuci.2018.03.011

Ogundokun, R. O., Misra, S., Bajeh, A. O., Okoro, U. O., & Ahuja, R. (2022). *An Integrated IDS using ICA-based Feature Selection and SVM Classification Method* (S. Misra & C. Arumugam (Eds.)). Springer Nature.

Panliang, M., Madaan, S., Ahmed, S., Ali, B., Gowrishankar, J., & Khatibi, A. (2025). Enhancing feature selection for multi-pose facial expression recognition using a hybrid of quantum inspired firefly algorithm and artificial bee colony algorithm. *Scientific Reports*, *15*(4665), 1–23.

Prithi, S., & Sumathi, S. (2024). A technical research survey on bio-inspired intelligent optimization grouping algorithms for finite state automata in intrusion detection system. *MultiCraft International Journal of Engineering, Science and Technology*, *16*(2), 48–67. https://doi.org/10.4314/ijest.v16i2.6

Radhakrishnan, S., Aljawarneh, P., & Kumar, V. (2019). Snort – Lightweight intrusion detection for networks. In *Proceedings of the 13th USENIX Conference on System Administration (LISA '99)*, 229–238.

Rufai, K.I., Usman, O.L., Muniyandi, R.C. and Oyinkanola, L.O.A. (2021a), Modelling Credit Card Payment Fraud Detection System for Financial Institutions in Nigeria Using an Improved Firefly Algorithm. *International Journal of Information Processing and Communication (IJIPC)*, *11*(1): 9-25. A Publication of Faculty of Communication and Information Sciences, University of Ilorin, Kwara State, Nigeria.

Rufai, K. I., Usman, O. L., Olusanya, O. O. and Adedeji, O. B. (2021b), Solving Travelling Salesman Problem using an Improved Ant Colony Optimization Algorithm. *University of Ibadan Journal of Science and Logics in ICT Research (UIJSLICTR)*, *6*(2): 158-170.

Rufai, K.I., Muniyandi, R. C., and Usman, O.L. (2016), Tacking the Course of Dimensionality in Intrusion Detection Systems: Membrane Computing Approach. *Proceedings of the 2nd TASUED-UCC International Conference, Tai Solarin University of Education*, Nigeria, August 22nd -25th, 2016, pp. 1539-1549.

Saheed, Y. K. (2022). *A Binary Algorithm based Feature Selection Method on High Dimensional Intrusion Detection Data* (S. Misra & C. Arumugam (Eds.)). Springer Nature.

Shang-fu, Z., Zhao, X., Li Y., & Chen, W. (2012). An improved intrusion detection algorithm based on classification. *Journal of Software*, *7*(7), 1549–1556.

Usman, O. L. (2025). Identifying Significant Structural Factors associated with Knee Pain Severity in Patients with Osteoarthritis using Hybrid Bio-BERT Bi-LSTM CNN Model. *Journal of Science and Information Technology (JOSIT)*, *19*(2): 18-28.

Usman O.L, & Adeusi O.O. (2025). Optimization of an efficient net-based transfer learning model for automated pneumonia detection from chest x-ray images. *Dutse Journal of Pure and Applied Sciences*, *11*(4a), 397–411. Retrieved from https://www.ajol.info/index.php/dujopas/article/view/311486

Usman, O. L. & Muniyandi, R. C. (2020). CryptoDL: Predicting Dyslexia Biomarkers from Encrypted Neuroimaging Dataset Using Energy-Efficient Residue Number System and Deep Convolutional Neural Network. Symmetry MDPI-Basel, 12(836), 1–24. https://doi.org/10.3390/sym12050836

Usman, O. L., Muniyandi, R. C., Omar, K., & Mohamad, M. (2021). Advanced machine learning methods for dyslexia biomarker detection: A review of implementation details and challenges. *IEEE Access*, *9*, 36879–36894. https://doi.org/10.1109/ACCESS.2021.3062709

Usman, O. L., Adeusi, O. O., Kareem, M. A., Owoade, A. A., Muniyandi, R. C. (2026). Quantitative Study on Impact of EfficientNet-based Deep Transfer Learning Model for Pneumonia Detection with Explainable Artificial Intelligence using Chest Radiographs. *Zamfara International Journal of Science, Technology, Education & Mathematics (ZIJSTEM)*, 3(1). 1-11.

Yinka-Banjo, C., Alli, P., Misra, S., Oluranti, J., & Ahuja, R. (2022). *Intrusion Detection using Anomaly Detection Algorithm and Snort* (S. Misra & C. Arumugam (Eds.)). Springer Nature.

Zivkovic, M., Tair, M., Venkatachalam, K., Bacanin, N., & Trojovský, P. (2022). Novel hybrid firefly algorithm : an application to enhance XGBoost tuning for intrusion detection classification. *PeeJ Computer Science*, *8*(e956), 1–38. https://doi.org/10.7717/peerj-cs.956

©2026 This is an Open Access article distributed under the terms of the Creative Commons Attribution 4.0 International license viewed via https://creativecommons.org/licenses/by/4.0/ which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is cited appropriately.