STAP
Smart Technologies Academic Press

Journal of Cyber Security and Risk Auditing

https://www.jcsra.thestap.com/

Metaheuristic-Driven Feature Selection with SVM and KNN for Robust DDoS Attack Detection: A Comparative Study

Rejwan Bin Sulaiman[1], Ansam Khraisat[2]

[1]*Department of Computer and Information Sciences, Northumbria University, London, UK*

[2]*Department of Cyber Security, Deakin University, Australia*

ARTICLE INFO

Article History

Received: 17-05-2025
Revised: 30-05-2025
Accepted: 12-08-2025
Published: 14-08-2025

Vol.2025, No.4

DOI:
https://doi.org/10.63180/jcsra.thestap.2025.4.1

Corresponding author.
Email:
rejwan.binsulaiman@study.beds.ac.uk

Orcid:

https://orcid.org/0000-0002-3037-7808

ABSTRACT

Distributed Denial of Service (DDoS) attack occurs when an attacker attempts to disrupt the normal operation of a network, service, or website by overwhelming it with a high volume of internet traffic. The goal of detecting DDoS attacks is to identify and respond to them promptly, thereby minimizing their impact on the targeted system. Effective detection is essential for individuals, organizations, and network administrators to safeguard infrastructure, ensure service availability, and protect online systems and services. DDoS detection is widely applicable in areas such as network security, web service protection, cloud computing, and online infrastructure resilience. To address this need, we propose a framework consisting of six main steps. First, data collection involves gathering network traffic information, system activity logs, and known instances of DDoS attacks. Second, relevant features are identified from the dataset, including traffic patterns, packet sizes, IP addresses, and protocol types. In the third step, feature selection is performed using metaheuristic algorithms such as the Salp Swarm Algorithm (SSA), Gray Wolf Optimization (GWO), and Particle Swarm Optimization (PSO) to isolate the most informative features for distinguishing between normal and malicious traffic. Fourth, the dataset is divided into training and testing subsets for model development and evaluation. Fifth, classification models are built using machine learning algorithms such as Support Vector Machine (SVM) and K-Nearest Neighbors (KNN) to classify traffic patterns effectively. Finally, the performance of the models is evaluated using metrics including accuracy, precision, recall, and F1-score. The results of the proposed framework demonstrate outstanding performance, with classification accuracy reaching up to 99.9%. In summary, detecting DDoS attacks is vital for protecting networked systems and ensuring the continuity of online services, and the use of feature selection and machine learning techniques significantly enhances detection accuracy and efficiency.

Keywords: DDoS Attacks; Machine learning algorithms; Salp swarm algorithm (SSA); PSO; GWO; SVM.

How to cite the article
Sulaiman, R. B., & Khraisat, A. (2025). Metaheuristic-Driven Feature Selection with SVM and KNN for Robust DDoS Attack Detection: A Comparative Study. Journal of Cyber Security and Risk Auditing, 2025(4), 182–203. https://doi.org/10.63180/jcsra.thestap.2025.4.1

1. Introduction

DDoS attack is a malicious cyber operation in which a large number of compromised devices—typically coordinated as a botnet—are employed to flood a targeted system or network with an overwhelming volume of traffic [1]. The core objective of such attacks is to exhaust critical system resources, such as CPU cycles, memory, or bandwidth, thereby rendering the targeted infrastructure incapable of processing legitimate user requests [5]. Attackers commonly compromise vulnerable devices by exploiting security flaws or deploying malware, subsequently gaining remote control over them [3]. These infected devices, often referred to as “bots” or “zombies,” are orchestrated to launch massive and sustained traffic flows directed at the target system [2]. The resulting traffic deluge can significantly degrade service performance or cause a complete denial of service for legitimate users [4].

To counter such threats, effective DDoS detection systems must leverage robust feature selection and machine learning (ML) strategies. The key objectives of these systems include accurately distinguishing between benign and malicious traffic, ensuring real-time detection for rapid response, adapting to the dynamic nature of attack vectors, and minimizing both false positives and false negatives. Moreover, scalability and operational efficiency are critical to sustaining the effectiveness of the detection framework under high-load scenarios [2]. By fulfilling these requirements, organizations can proactively mitigate DDoS threats, maintain service availability, safeguard sensitive data and infrastructure, and ensure a secure and resilient digital environment [6].

The detection of Distributed Denial of Service (DDoS) attacks through feature selection and machine learning (ML) techniques offers significant advantages but also presents substantial challenges [10]. The continuously evolving strategies employed by attackers require ML-based detection systems to be frequently updated to recognize novel and sophisticated attack patterns. A major limitation lies in the scarcity of labeled training datasets, which directly affects the accuracy and generalizability of ML models. Achieving an optimal balance between minimizing false positives and false negatives remains a complex task, particularly given the dynamic and adaptive nature of DDoS attacks. Selecting relevant features for accurate detection is further complicated by the variability in attack signatures and traffic behavior [8].

Scalability and performance are critical issues, especially when dealing with high-volume traffic that may obscure fine-grained packet-level details. Additionally, resource exhaustion attacks targeting the detection infrastructure itself can impair the system’s ability to function effectively [7]. Zero-day attacks pose another formidable challenge, as ML models lack prior data on which to base detection, reducing their effectiveness. Addressing these issues requires ongoing research and innovation aimed at enhancing detection algorithms, refining feature selection methods, and developing more adaptive and resilient detection strategies [6]. DDoS detection plays a vital role in safeguarding the security and continuity of various digital ecosystems, including enterprise networks, online services, internet service providers (ISPs), financial institutions, government agencies, data centers, gaming platforms, and Internet of Things (IoT) devices [6]. Effective detection mechanisms are essential for reinforcing digital infrastructure, preventing service disruptions, protecting sensitive information, ensuring operational continuity, and delivering consistent and reliable user experiences. The importance of accurate identification and timely mitigation is underscored by the need to maintain availability, security, and resilience in today’s highly interconnected digital environment [11]. Ultimately, the motivation for identifying and mitigating DDoS attacks is grounded in the imperative to preserve network availability, protect critical infrastructure, ensure the confidentiality and integrity of data, support incident response and mitigation efforts, uphold user trust, avoid financial losses, comply with regulatory standards, and gain proactive threat intelligence [13].

Machine learning (ML) and deep learning (DL) techniques have become essential tools for detecting Distributed Denial of Service (DDoS) attacks. Numerous algorithms have been employed to support this task, including Support Vector Machines (SVM), Random Forests (RF), Multilayer Perceptrons (MLP), Convolutional Neural Networks (CNN), Long Short-Term Memory (LSTM) networks, Autoencoders, Generative Adversarial Networks (GANs), Recurrent Neural Networks (RNN), and eXtreme Gradient Boosting (XGBoost) [12]. These algorithms are capable of classifying network traffic, identifying patterns, capturing temporal dependencies, and detecting abnormal behaviors associated with DDoS attacks. The selection of an appropriate algorithm depends on various factors, such as the characteristics of the dataset, the computational capabilities available, and the specific requirements of the detection system. Moreover, the effectiveness of these algorithms is highly dependent on supporting processes such as feature engineering, data preprocessing, and model optimization [14].

The integration of feature selection methods with machine learning (ML) techniques for the detection of Distributed Denial of Service (DDoS) attacks yields numerous significant benefits that enhance both the performance and practicality of detection systems [15]. The effectiveness of this approach, however, depends on the choice of algorithms and strategies employed. One of the primary advantages is enhanced detection accuracy. Feature selection techniques enable the identification of the most relevant attributes from network traffic data, effectively eliminating redundant or irrelevant features [16]. This refined input significantly improves the learning process of ML models, allowing them to more accurately distinguish between benign and malicious traffic patterns associated with DDoS attacks. Another key benefit is the reduction in data dimensionality and complexity. By selecting only the most informative features, feature selection reduces the volume of data that needs to be processed. This not only accelerates training and prediction times but also decreases memory usage and computational costs an essential factor in real-time DDoS detection where efficiency is paramount [17]. A further advantage is improved interpretability of detection models. Feature selection narrows the focus to a subset of critical indicators, making the resulting models more transparent and easier to analyze. This interpretability aids cybersecurity analysts in understanding the factors contributing to DDoS activity and in designing targeted mitigation strategies based on concrete evidence from the data. Moreover, feature selection enhances the scalability of detection systems. In high-traffic environments, such as enterprise networks or cloud infrastructure, analyzing vast volumes of data in real time is a major challenge. Feature selection methods capable of handling large-scale datasets support the development of scalable ML-based solutions that maintain high performance under heavy load conditions. Lastly, the approach supports comprehensive comparative evaluation [18]. By experimenting with different combinations of feature selection methods and ML algorithms, researchers can assess their respective strengths and limitations in various operational contexts. These insights enable the formulation of optimized detection frameworks tailored to specific deployment environments and attack characteristics [19]. In conclusion, the synergy between feature selection and machine learning techniques not only enhances the precision and efficiency of DDoS detection but also contributes to the development of interpretable, scalable, and adaptive security solutions. Such advancements are essential for maintaining robust defenses in today’s increasingly complex and high-risk digital environments.

In our proposed approach to DDoS detection, the process begins with data acquisition, where relevant network traffic data is collected. This is followed by feature extraction, in which informative attributes are identified from the collected data. The next step involves data preprocessing, which includes normalizing and cleaning the data to ensure quality and consistency. Subsequently, we apply feature selection techniques using optimization algorithms such as the Grey Wolf Optimizer (GWO), Particle Swarm Optimization (PSO), and Salp Swarm Algorithm (SSA) to isolate the most significant features for model training. The dataset is then split into training and testing subsets. Machine learning algorithms, such as SVM and K-Nearest Neighbors (KNN), are used to train the detection model. After training, the model’s performance is evaluated on the test data, and optimization techniques are applied to fine-tune model parameters for improved accuracy and robustness. The integration of metaheuristic optimization techniques like GWO, PSO, and SSA with ML models for DDoS detection raises several important research questions. First, RQ1 explores how GWO, PSO, and SSA can be effectively employed to optimize feature selection in the context of DDoS detection. Second, RQ2 investigates the optimal parameter settings and configurations for these algorithms when used for this specific task. Third, RQ3 compares the performance of GWO, PSO, and SSA with each other and with conventional feature selection methods in terms of accuracy, efficiency, and robustness. Lastly, RQ4 examines whether incorporating these optimization techniques with ML algorithms enhances detection performance compared to using ML models in isolation. Addressing these research questions will provide valuable insights into the potential of combining metaheuristic optimization and machine learning in building more accurate, efficient, and adaptive DDoS detection systems. This integrated approach aims to overcome limitations in feature selection, improve model performance, and ensure scalable and reliable protection against evolving cyber threats.

2. Literature Review

Several studies in the literature have been performed to propose a robust techniques to detect DDoS attacks. For instance, [1] proposed a comprehensive framework for detecting and mitigating DDoS attacks using machine learning (ML) techniques. Their approach addresses limitations in conventional detection systems by integrating multiple ML algorithms with real-time monitoring capabilities. The study begins with a literature review that outlines the current state of research and identifies critical gaps in existing methodologies. The proposed framework involves data collection from network traffic and system logs, followed by preprocessing to cleanse the data for analysis. The authors employ various ML algorithms—potentially including Support Vector Machines (SVM), Random Forests (RF), and Neural Networks—to detect and prevent DDoS attacks. Their evaluation highlights the strengths and weaknesses of the approach in comparison with existing solutions, and concludes with a discussion on its practical benefits and future enhancements. Another study by [2] explored a method for detecting and preventing DDoS attacks in mobile healthcare (m-Health) environments, emphasizing the protection of sensitive medical data. Their work highlights the growing threat of DDoS attacks in healthcare systems and proposes a multi-faceted detection strategy. This includes analyzing network traffic patterns and employing machine learning and anomaly detection techniques to identify irregular behavior. To mitigate attack impacts, the study suggests countermeasures such as traffic filtering, rate limiting, and resource management to ensure service availability and data integrity. Additionally, the authors propose a collaborative defense framework that facilitates information sharing among entities within the m-Health ecosystem, enabling faster and more coordinated responses to threats. Simulation and evaluation experiments demonstrate the effectiveness of the proposed approach in maintaining system resilience. In another study, the authors of [12] introduced the Genetic Algorithm Naive Bayes Anomaly Detection Model (GANBADM) to enhance the detection of threats targeting fog computing environments. Given the proximity of mobile devices to fog nodes—which can increase vulnerability due to resource constraints—the GANBADM model was designed to differentiate between legitimate and malicious traffic more effectively. The model combines a genetic algorithm for feature selection with a Naive Bayes classifier, streamlining the detection process while maintaining high accuracy. Evaluation on the NSL-KDD dataset showed that GANBADM achieved an accuracy of 99.73%, precision of 99.10%, a false positive rate of 0.6%, and a fast execution time of 0.18 seconds. However, the authors noted limitations related to data quality, particularly in terms of F1-score, and emphasized the need for further testing with real-world cloud data and a broader range of attack types. A study by [14] conducted an empirical study to evaluate the performance of six machine learning classifiers in detecting 11 types of DDoS attacks using the CICDDoS2019 dataset. They employed the Random Forest Regressor (RFR) as a feature selection technique to reduce the number of features from 80 to 24, which were then used across all classifiers. Decision Trees (DT) and Random Forests (RF) achieved the highest accuracy and precision rates of 99%, with DT also demonstrating the fastest processing time at 4.53 seconds compared to RF's 84.2 seconds. While the results highlight the effectiveness of DT for DDoS detection in IoT networks, the authors noted that their evaluation relied on datasets collected from high-resource servers, which may not reflect real-world IoT environments. They recommend further validation using resource-constrained network traffic datasets to ensure broader applicability. Moreover, [16] investigated the use of Light Gradient Boosting Machine (LGBM) for DDoS attack detection, incorporating an Integrated Feature Selection (IFS) method combining filter and embedded techniques. Their experimental results revealed a 20% improvement in model performance over existing models in the literature. Similarly, [17] developed an intrusion detection approach for Internet of Medical Things (IoMT) systems, utilizing a genetic algorithm with a Random Forest classifier. Using the NSL-KDD and UNSW 2018_IoT_Botnet datasets, the proposed method achieved 99.9% accuracy with 100% precision and recall—surpassing previous ML-based methods in the domain. Authors in a study [18] also applied machine learning and data mining techniques for DDoS detection, achieving 100% accuracy using the CICDDoS2019 dataset. Ismail and colleagues employed ensemble methods like Random Forest and Boosting to classify DDoS attack types, reporting a detection accuracy of 90%. Halim et al. proposed a Genetic Algorithm-based Feature Selection (GbFS) technique to enhance DDoS detection. Their system analyzed traffic from datasets including Bot-IoT, UNSW-NB15, and CIRA-CIC-DOHBrw-2020, achieving a peak accuracy of 99.80%, demonstrating the potential of hybrid approaches combining feature selection and ML algorithms. Table 1 presents the related works on DDoS detection using ML techniques.

Table 1. Summary of related works on DDoS detection using ML techniques.

Author(s)	**Focus**	**Techniques Used**	**Dataset**	**Key Findings**
Kebede et al. [1]	ML-based DDoS detection with real-time monitoring	SVM, RF, Neural Networks	Not specified	Effective framework with identified gaps and areas for improvement
Ray et al. [2]	DDoS detection in mobile healthcare systems	Anomaly detection, ML algorithms	Simulation/real-world trials	Collaborative framework enhances DDoS detection in m-Health
Colleagues [12]	DDoS detection in fog computing using GANBADM	Genetic Algorithm, Naive Bayes	NSL-KDD	99.73% accuracy, fast execution, needs real-world data validation
Alzahrani et al. [14]	Classifier comparison using RFR feature selection	DT, RF, KNN, LR, NB	CICDDoS2019	DT and RF achieved 99% accuracy, DT had lowest processing time

Marvi et al. [16]	Feature selection with LGBM for DDoS detection	IFS, LGBM	Not specified	20% performance improvement over existing models
Norouzi et al. [17]	Intrusion detection in IoMT using GA and RF	Genetic Algorithm, Random Forest	NSL-KDD, UNSW 2018_IoT_Botnet	99.9% accuracy, 100% precision and recall
Seifousadati et al. [18]	DDoS detection using ML and data mining	ML algorithms	CICDDoS2019	Achieved 100% detection accuracy
Ismail et al.	DDoS classification using ensemble methods	Random Forest, Boosting	Not specified	Achieved 90% detection accuracy
Halim et al.	Feature selection for DDoS detection in networks	GbFS, ML algorithms	Bot-IoT, UNSW-NB15, CIRA-CIC-DOHBrw-2020	Achieved 99.80% accuracy

3. Methodology

In our study, we propose an intelligent framework for detecting Distributed Denial of Service (DDoS) attacks by integrating advanced feature selection techniques—namely Grey Wolf Optimizer (GWO), Particle Swarm Optimization (PSO), and Salp Swarm Algorithm (SSA)—with robust machine learning classifiers, specifically Support Vector Machine (SVM) and K-Nearest Neighbors (KNN). The framework is designed to efficiently identify and classify DDoS attack traffic within network data by selecting the most relevant features and leveraging the discriminative power of well-established classification models. Feature selection is a foundational component of this approach, aiming to reduce data dimensionality while retaining the most informative attributes that contribute to the accurate distinction between benign and malicious traffic. This not only enhances classification performance but also mitigates issues related to overfitting, noise, and computational inefficiency. Metaheuristic algorithms such as GWO, PSO, and SSA are employed due to their proven effectiveness in solving complex optimization problems. These algorithms search the feature space to identify optimal subsets based on fitness functions that reflect classification accuracy or other performance metrics. Once the most relevant features are selected, they are used to train SVM and KNN classifiers. SVM, a supervised learning algorithm, constructs an optimal hyperplane that maximizes the margin between classes in a high-dimensional feature space, making it particularly effective for binary classification tasks such as DDoS detection. In contrast, KNN is a non-parametric, instance-based learning algorithm that classifies data points by evaluating the majority label among the k-nearest neighbors based on a defined distance metric [19]. While SVM is known for its generalization ability and robustness to high-dimensional data, KNN offers simplicity and effectiveness in handling non-linear data distributions. During the training phase, labeled network traffic data—comprising both legitimate and DDoS attack instances—is used to enable the classifiers to learn the distinctive patterns and behavioral traits associated with each class. In the testing or deployment phase, the trained models evaluate the feature profiles of incoming traffic and assign class labels accordingly. The predicted classifications can then trigger appropriate mitigation responses within the intrusion detection or prevention system. The performance of this hybrid detection approach is significantly influenced by the quality of the selected features, the representativeness of the training dataset, and the optimization of model parameters. Continuous refinement of the feature selection process, alongside systematic tuning of the SVM and KNN hyper parameters, is essential to maximize detection accuracy, reduce false positives and negatives, and ensure scalability in real-world high-traffic network environments. Ultimately, the proposed integration of metaheuristic-driven feature selection with machine learning classifiers provides a promising direction for developing efficient, accurate, and adaptive DDoS detection systems capable of operating in complex and dynamic cyber environments.

3.1 Dataset

The effectiveness of modern cybersecurity mechanisms—particularly Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS)—largely depends on the quality and relevance of the data used for model training and evaluation. While anomaly-based detection approaches offer promising capabilities in identifying novel threats, their performance is significantly hindered by the scarcity of comprehensive, up-to-date, and realistic benchmark datasets. An analysis of eleven commonly used intrusion detection datasets, reveals substantial limitations: many are outdated, lack sufficient attack diversity, anonymize payload content, and fail to accurately reflect contemporary network environments.

To address these shortcomings, the CICIDS2017 dataset, developed by the Canadian Institute for Cybersecurity (CIC), has emerged as a robust and widely accepted dataset for intrusion detection and classification tasks. Unlike its predecessors, CICIDS2017 is designed to closely mimic real-world network traffic by incorporating a rich set of realistic background activities and contemporary attack scenarios. It provides labeled bidirectional traffic flows with detailed metadata, including timestamps, source and destination IP addresses, ports, protocol types, and specific attack labels. The dataset is made available in CSV format, enabling straightforward integration with machine learning pipelines. A key strength of CICIDS2017 is the use of the B-Profile system to emulate realistic user behavior. This system simulates the network activities of 37 users across various protocols, generating legitimate background traffic that closely resembles typical organizational usage patterns. Additionally, the dataset encompasses a diverse spectrum of attack types, such as Brute Force (FTP and SSH), Denial of Service (DoS), Web-based attacks, infiltration attempts, and Botnet activity—thereby ensuring a broad representation of modern threat vectors. To support a comprehensive analysis, the dataset was constructed in accordance with eleven essential criteria for high-quality intrusion detection datasets. These include realistic network configurations, heterogeneous traffic sources, detailed attack documentation, and inclusion of host-based artifacts. During attack simulations, supplementary data such as memory dumps and system call traces were also collected from compromised hosts, enriching the contextual relevance of the dataset.

The selection of an appropriate dataset is a critical factor in developing effective intrusion detection systems, particularly when leveraging machine learning or deep learning techniques. Each dataset in table 2 serves a distinct purpose and is tailored to specific domains, attack types, and network environments. For instance, CICIDS2017 and CSE-CIC-IDS2018 offer general-purpose datasets with a variety of attack types and realistic background traffic, making them suitable for broad IDS research. Meanwhile, specialized datasets like BoT-IoT, TON_IoT, and Edge-IIoTset focus specifically on IoT and IIoT environments, where resource constraints and traffic patterns differ significantly from traditional enterprise networks. CIC-DDoS2019 stands out for its exclusive focus on DDoS attack scenarios, providing a rich set of attack vectors including DNS amplification, SNMP reflection, and HTTP floods. Such specificity allows researchers to fine-tune models for particular threat landscapes. Lightweight and real-time detection research benefits from datasets like Kitsune, which captures traffic in low-power IoT settings and supports the evaluation of on-device security solutions. Furthermore, the emergence of newer datasets such as Edge-IIoTset and UWF-NB15 reflects ongoing efforts to model contemporary network architectures and include modern attack strategies. These datasets introduce enhanced features and simulate sophisticated cyber threats targeting critical infrastructure and industrial systems. Ultimately, the choice of dataset should align with the goals of the research, the targeted environment (e.g., cloud, edge, IoT), and the types of attacks under investigation. The continued development of high-quality, labeled, and diverse datasets remains essential to advancing the field of intrusion detection and ensuring the deployment of robust cybersecurity defenses.

In total, more than 90 detailed flow-based features were extracted using the CICFlowMeter tool. These features capture various temporal, statistical, and behavioral characteristics of network traffic, making the CICIDS2017 dataset particularly suitable for training and validating machine learning models for DDoS detection. Its realism, diversity, and feature richness provide a reliable foundation for advancing state-of-the-art intrusion detection research.

Table 2. Intrusion Detection Datasets (2017–2024)

Dataset	Year	Description
CICIDS2017	2017	Comprehensive dataset simulating real-world traffic with 80+ features. Includes DoS, DDoS, Botnet, Web attacks, and more.
CSE-CIC-IDS2018	2018	An extension of CICIDS2017 with more attack types and user scenarios. Includes pcap and CSV formats.
BoT-IoT	2018	IoT-specific dataset capturing normal and malicious behavior with DoS, DDoS, theft, and reconnaissance attacks.
Kitsune (KITTI)	2018	Lightweight IDS dataset from an IoT environment with real-time traffic. Includes ARP spoofing, fuzzing, and Mirai botnet.
CIC-DDoS2019	2019	Focused on DDoS attacks. Covers multiple attack types like DNS, NTP, SNMP, and WebDDoS with over 50 scenarios.
TON_IoT	2020	Includes telemetry, network, and log data for IoT and IIoT devices. Features attacks like ransomware and injection.
IoTID20	2020	Designed for IoT environments, capturing diverse behaviors and multiple attack types using common IoT protocols.
UNSW-BOT-IoT	2020	Updated BoT-IoT dataset with enhanced labeling and additional IoT-based attacks.

Edge-IIoTset	2022	Industry 4.0 and edge computing-focused dataset with DDoS, spoofing, injection, and MITM attacks.
UWF-NB15	2022	Modernized version of UNSW-NB15 including recent attack vectors and improved flow-based features.

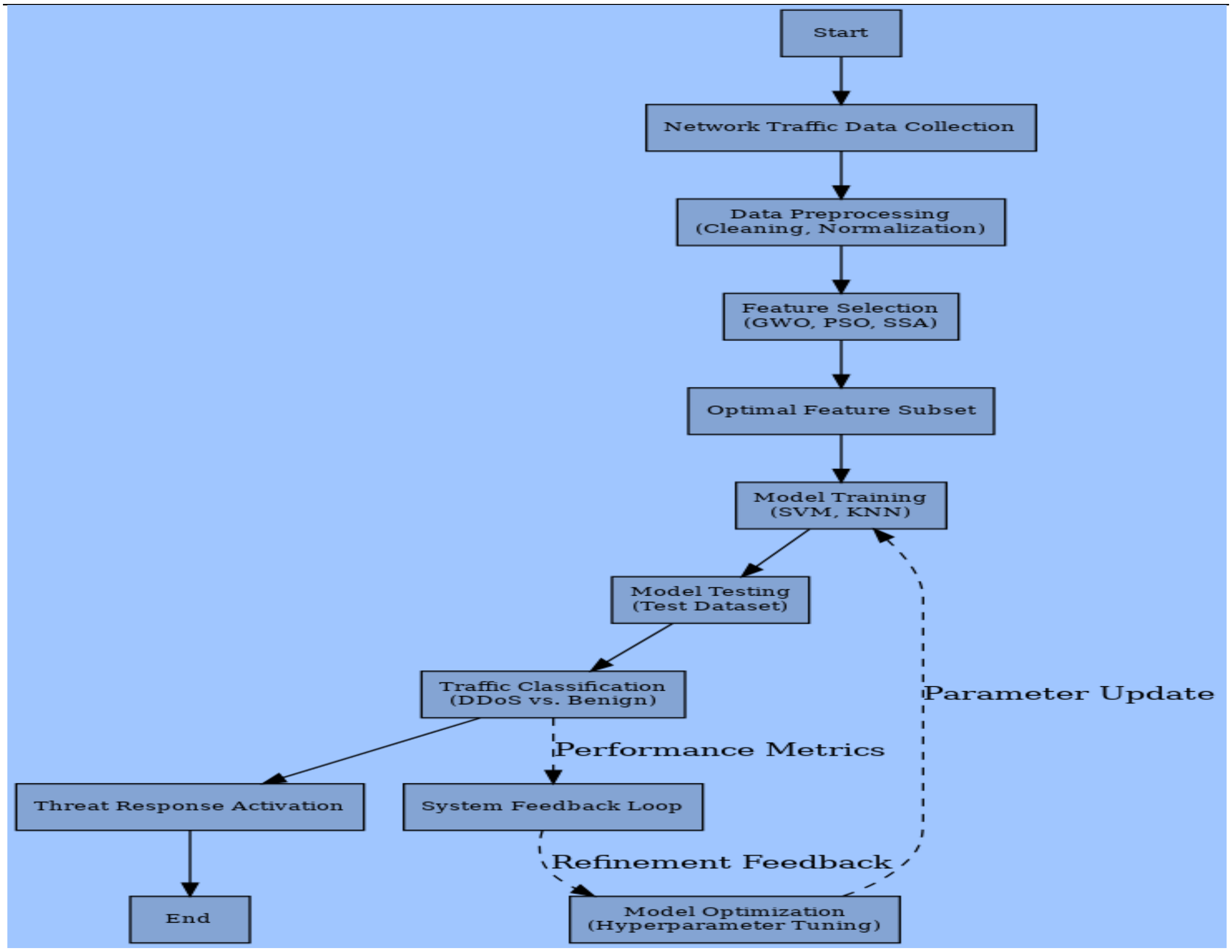
Start
Network Traffic Data Collection
Data Preprocessing (Cleaning, Normalization)
Feature Selection (GWO, PSO, SSA)
Optimal Feature Subset
Model Training (SVM, KNN)
Model Testing (Test Dataset)
Traffic Classification (DDoS vs. Benign)
Parameter Update
Performance Metrics
Threat Response Activation
System Feedback Loop
Refinement Feedback
End
Model Optimization (Hyperparameter Tuning)

Figure 1. Research Methodology Steps.

3.2 Feature Selection

Feature selection serves as a foundational process in the design of robust and efficient Distributed Denial of Service (DDoS) detection systems. Its primary purpose is to identify the most relevant and discriminative features from network traffic data that contribute significantly to distinguishing between benign and malicious activity. By eliminating redundant, irrelevant, or noisy features, feature selection reduces the dimensionality of the dataset, thereby improving computational efficiency and enhancing the performance of classification algorithms.

This process not only facilitates the development of lightweight and scalable detection models—crucial for real-time applications in high-throughput network environments—but also improves model interpretability. Focusing on a smaller subset of meaningful features allows researchers and practitioners to gain deeper insights into the behavioral patterns and attack vectors associated with DDoS activities. Such insights are valuable for forensic analysis, anomaly explanation, and the design of targeted mitigation strategies. Moreover, effective feature selection enhances generalization capabilities by minimizing overfitting and ensuring that the model captures the most representative characteristics of attack traffic. This is particularly important in dynamic and evolving threat landscapes, where the nature of attacks may vary significantly across time and contexts. In summary, feature selection is not merely a preprocessing step, but a strategic component that directly influences the accuracy, efficiency, scalability, and interpretability of DDoS detection systems. When integrated with machine learning models, especially in conjunction with optimization techniques such as Grey Wolf Optimizer

(GWO), Particle Swarm Optimization (PSO), or Salp Swarm Algorithm (SSA), feature selection substantially elevates the reliability and responsiveness of intrusion detection frameworks in both experimental and real-world network environments.

3.3 Feature Selection Algorithms

3.3.1 Gray Wolf Optimization (GWO) algorithm

Gray Wolf Optimization (GWO) has demonstrated considerable effectiveness in enhancing DDoS detection systems through parameter tuning and feature selection. Inspired by the social hierarchy and hunting strategies of gray wolves in nature, GWO mimics the leadership dynamics of the wolf pack—categorized into alpha, beta, delta, and omega wolves—to iteratively search for optimal solutions within a high-dimensional search space. In the context of DDoS detection, GWO plays a dual role. First, it assists in fine-tuning hyperparameters such as detection thresholds, learning rates, or classifier weights, thereby improving the performance of the underlying machine learning models. Second, it facilitates feature selection by evaluating different subsets of input features and assessing their discriminative power in separating benign traffic from attack traffic. This optimization process enables the system to identify the most relevant attributes, leading to improved classification accuracy and reduced computational overhead. GWO is particularly well-suited for DDoS detection tasks due to its ability to handle complex, multimodal, and multidimensional optimization problems. Its exploitation–exploration balance and convergence capabilities ensure that the algorithm effectively navigates the search space and converges towards near-optimal solutions for real-time and large-scale detection scenarios. Algorithm1 presents Gray Wolf Optimization (GWO).

Algorithm1. Gray Wolf Optimization (GWO)

```
Input: Problem Size (D), Population Size (N), Maximum Iterations (T)
Output: Best solution Pg_best (position of α wolf)
Start
    Initialize the positions Xi of gray wolves randomly in D-dimensional space
    Initialize control parameters a, A, and C
    Evaluate fitness of each wolf using the objective function
    Identify α (best), β (second-best), and δ (third-best) wolves based on fitness
    Set iteration $t = 0$
    While ($t < T$) do:
        For each wolf Xi in the population:
            For each dimension $j = 1$ to D:
                Compute coefficient vectors:
                    $A = 2 * a * r1 - a$
                    $C = 2 * r2$
                Compute distances to α, β, and δ:
                    $D\alpha = |C1 * X\alpha - Xi|$
                    $D\beta = |C2 * X\beta - Xi|$
                    $D\delta = |C3 * X\delta - Xi|$
                Compute position updates:
                    $X1 = X\alpha - A1 * D\alpha$
                    $X2 = X\beta - A2 * D\beta$
                    $X3 = X\delta - A3 * D\delta$
                    $Xi = (X1 + X2 + X3) / 3$
            End For
        End For
        Update a using: $a = 2 - (2 * t / T)$
        Evaluate fitness of updated wolves
        Update α, β, δ positions
        Increment $t \leftarrow t + 1$
    End While
Return Pg_best ← position of α wolf
End
```

In our study, by embedding GWO within the DDoS detection pipeline—either for feature selection or parameter optimization—the detection system becomes more adaptive, precise, and capable of handling diverse traffic conditions. This bio-inspired optimization strategy enhances both the detection accuracy and the computational efficiency of machine learning-based IDS frameworks. Figure 2 presents the steps of GWO.

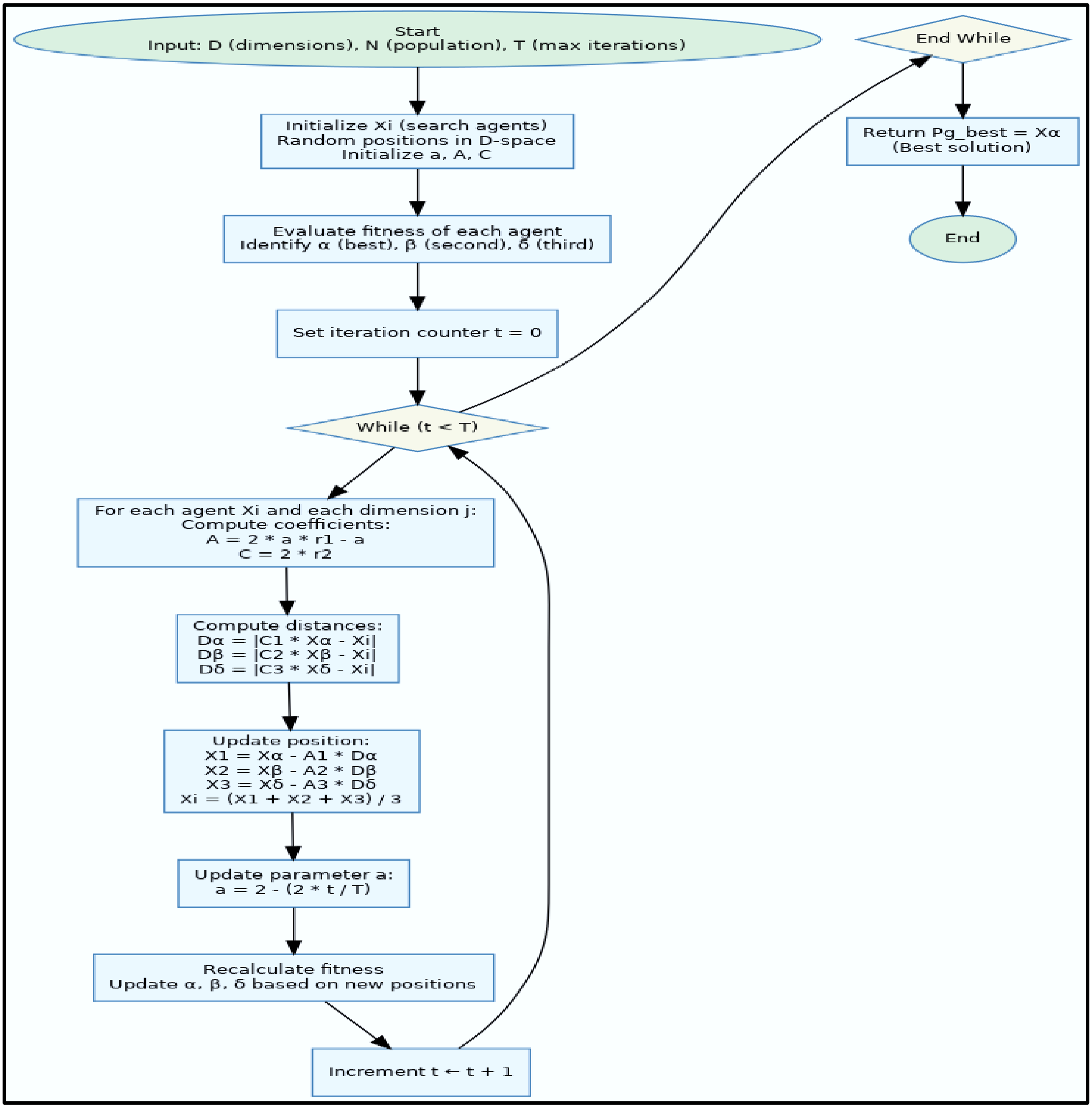

Figure 2. Gray Wolf Optimization (GWO) algorithm steps.

3.3.2 Salp Swarm Optimization (SSO)

The Salp Swarm Optimization (SSO) algorithm is a nature-inspired metaheuristic based on the collective foraging behavior of salps in the ocean. In the context of cybersecurity, and particularly Distributed Denial of Service (DDoS) attack detection, SSO offers a powerful mechanism for feature selection and parameter tuning, aimed at improving classification accuracy, reducing false positives, and enhancing overall system robustness. SSO simulates the movement of salps in a leader–follower formation, where the leading salp guides the swarm while the followers adjust their positions based on their neighbors. This intelligent swarm behavior enables SSO to efficiently balance exploration (searching for diverse feature combinations) and exploitation (refining promising solutions), allowing it to converge toward optimal or near-optimal configurations.

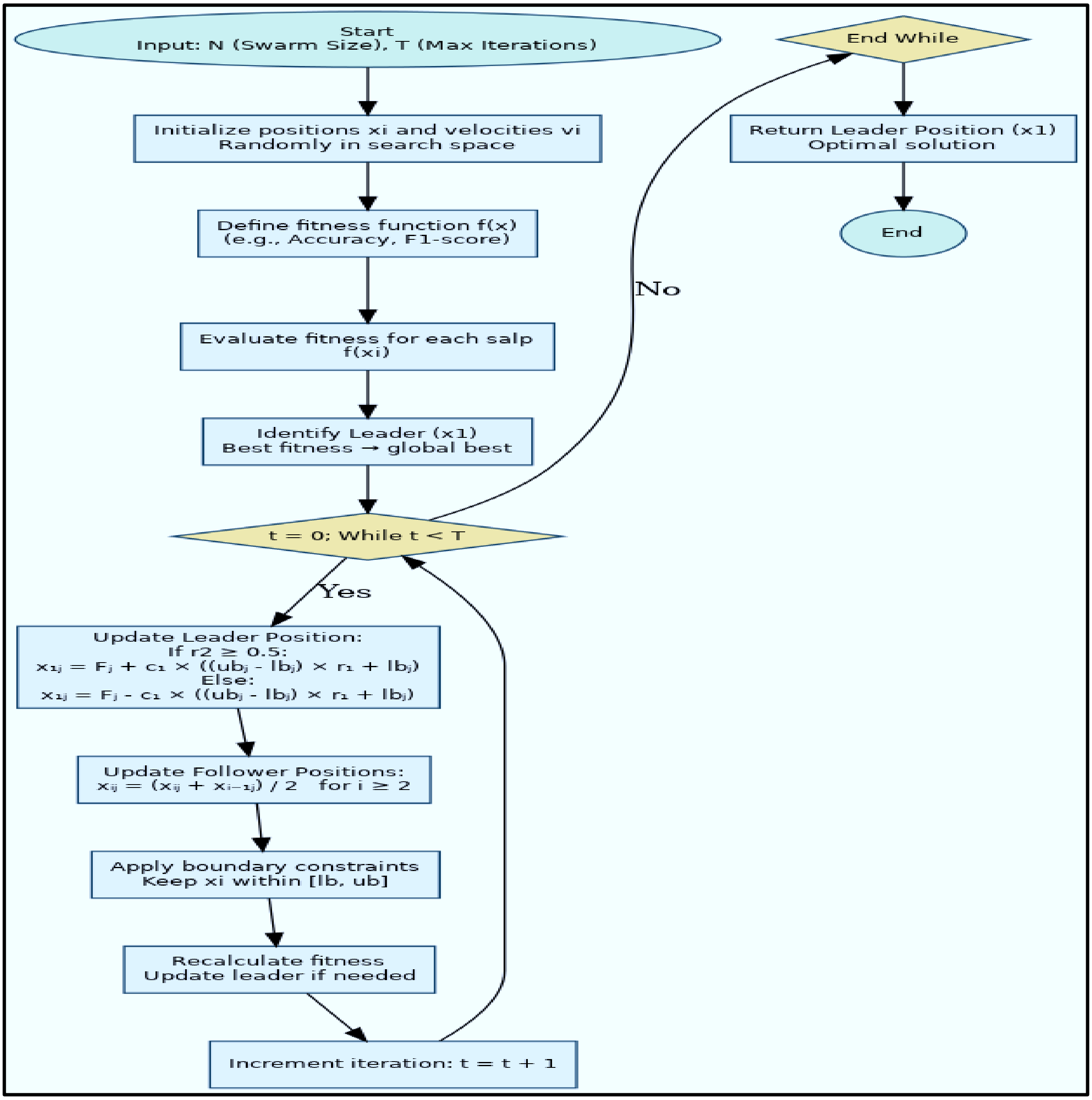
Start
Input: N (Swarm Size), T (Max Iterations)
Initialize positions xi and velocities vi
Randomly in search space
Define fitness function f(x)
(e.g., Accuracy, F1-score)
Evaluate fitness for each salp
f(xi)
Identify Leader (x1)
Best fitness → global best
t = 0; While t < T
Yes
Update Leader Position:
If r2 ≥ 0.5:
$x_{1j} = F_j + c_1 \times ((ub_j - lb_j) \times r_1 + lb_j)$
Else:
$x_{1j} = F_j - c_1 \times ((ub_j - lb_j) \times r_1 + lb_j)$
Update Follower Positions:
$x_{ij} = (x_{ij} + x_{i-1j}) / 2$ for $i \geq 2$
Apply boundary constraints
Keep xi within [lb, ub]
Recalculate fitness
Update leader if needed
Increment iteration: t = t + 1
No
End While
Return Leader Position (x1)
Optimal solution
End

Figure 3. Salp Swarm Optimization (SSO) algorithm steps.

In DDoS detection frameworks, SSO contributes in two key areas: (1) Feature Selection: SSO searches through subsets of features derived from network traffic data to identify those that are most discriminative between legitimate and malicious flows. This reduces data dimensionality, enhances interpretability, and minimizes the noise introduced by irrelevant or redundant features. (2) Hyperparameter Optimization: The algorithm fine-tunes the hyperparameters of machine learning classifiers—such as thresholds, learning rates, and kernel parameters—by guiding the search toward values that maximize detection performance. By integrating swarm intelligence with dynamic positional adjustments, SSO enables real-time optimization of both the structural (features) and functional (parameters) aspects of a DDoS detection system.

3.3.3 Particle Swarm Optimization (PSO)

Particle Swarm Optimization (PSO) is a widely adopted swarm intelligence algorithm that has proven effective in solving complex optimization problems, particularly in feature selection for machine learning-based intrusion detection systems. In the context of Distributed Denial of Service (DDoS) attack detection, PSO is employed to identify the most relevant subset of features from network traffic data that contributes to high classification accuracy and computational efficiency.

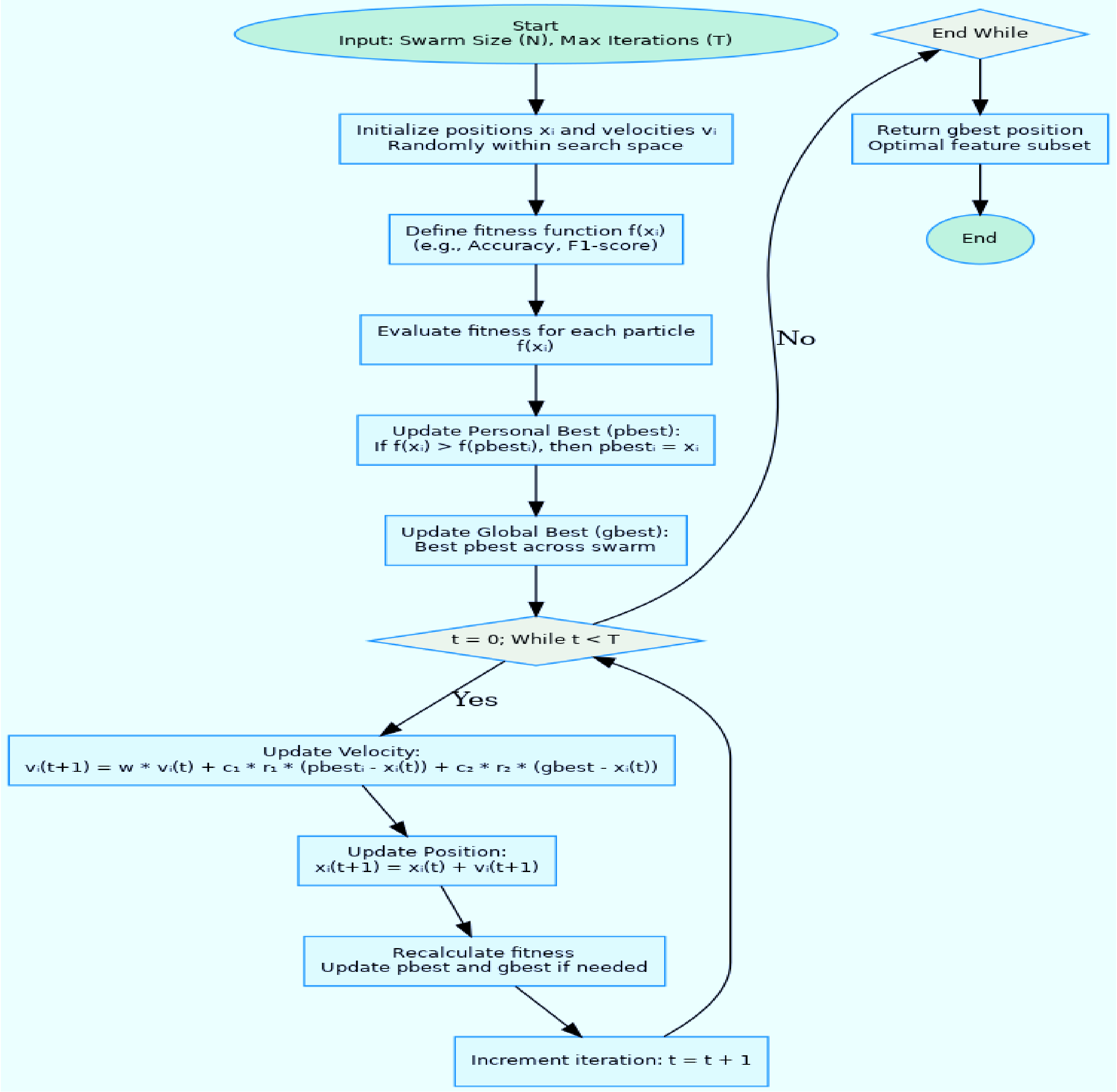
Start
Input: Swarm Size (N), Max Iterations (T)
Initialize positions x_i and velocities v_i
Randomly within search space
Define fitness function $f(x_i)$
(e.g., Accuracy, F1-score)
Evaluate fitness for each particle
$f(x_i)$
Update Personal Best (pbest):
If $f(x_i) > f(pbest_i)$, then $pbest_i = x_i$
Update Global Best (gbest):
Best pbest across swarm
t = 0; While t < T
Yes
No
Update Velocity:
$v_i(t+1) = w * v_i(t) + c_1 * r_1 * (pbest_i - x_i(t)) + c_2 * r_2 * (gbest - x_i(t))$
Update Position:
$x_i(t+1) = x_i(t) + v_i(t+1)$
Recalculate fitness
Update pbest and gbest if needed
Increment iteration: t = t + 1
End While
Return gbest position
Optimal feature subset
End

Figure 4. Particle Swarm Optimization (PSO).

PSO operates by simulating the collective behavior of a swarm of particles, where each particle represents a candidate solution in this case, a potential subset of features. These particles explore the search space by updating their positions and velocities, guided by both their personal experience (personal best or pbest) and the experience of the entire swarm (global best or gbest). Each particle's position is typically encoded as a binary or continuous vector, indicating the inclusion or exclusion of specific features. The effectiveness of a particle's feature subset is evaluated using a fitness function, commonly based on classification metrics such as accuracy, F1-score, or detection rate. Throughout the optimization process, particles iteratively adjust their velocities and positions, moving toward regions in the search space that yield higher performance. As a result, PSO converges on an optimal or near-optimal subset of features, enhancing the precision, generalization, and computational efficiency of the DDoS detection model. Figure 4 presents the Particle Swarm Optimization (PSO).

3.4 Features Classification Using Machine Learning Algorithms

3.4.1 SVM and KNN

In the context of DDoS attack detection, Support Vector Machine (SVM) and K-Nearest Neighbors (KNN) are two widely utilized machine learning classifiers for the effective categorization of network traffic based on selected features. Both algorithms offer distinct methodological advantages and are often chosen based on the specific nature of the dataset, the dimensionality of the feature space, and the desired trade-off between accuracy and computational efficiency.

Support Vector Machine (SVM) operates by identifying an optimal hyperplane that maximally separates data points of different classes. It relies on support vectors data points closest to the decision boundary to define the margin between classes. SVM is capable of handling both linearly and non-linearly separable data through the use of kernel functions such as linear, polynomial, and radial basis function (RBF). Its strength lies in its robustness to outliers, strong generalization capability, and effectiveness in high-dimensional spaces. However, SVM can become computationally intensive when applied to very large datasets, especially during the training phase. On the other hand, K-Nearest Neighbors (KNN) is a non-parametric, instance-based learning algorithm that classifies data based on the majority label among its k closest neighbors in the feature space. KNN is simple to implement and does not make any assumptions about the underlying distribution of the data, making it flexible and adaptive to various data types. Its performance is highly dependent on the choice of k, the distance metric used (e.g., Euclidean, Manhattan), and the density of data in high-dimensional spaces. While KNN is computationally lightweight during training, it can become slow and memory-intensive during inference due to its reliance on the entire training dataset for classification. For optimal performance in DDoS detection, it is common to experiment with both classifiers and evaluate their effectiveness using performance metrics such as accuracy, precision, recall, F1-score, and area under the ROC curve (AUC). Comparative analysis can then guide the selection of the most suitable model for deployment. Table 3 presents the comparison of SVM and KNN for Feature Classification.

Table 3. Comparison of SVM and KNN for Feature Classification.

Criteria	**Support Vector Machine (SVM)**	**K-Nearest Neighbors (KNN)**
Learning Type	Supervised, margin-based classifier	Supervised, instance-based learner
Decision Rule	Maximizes the margin between classes	Majority voting among k nearest neighbors
Kernel Support	Supports linear, polynomial, RBF, and sigmoid kernels	Does not use kernels
Computational Complexity	High during training, low during testing	Low during training, high during testing
Handling of High Dimensionality	Efficient and effective	Performance may degrade
Sensitivity to Outliers	Robust due to margin maximization	Sensitive to outliers and noise
Parameter Sensitivity	Kernel type, regularization, C, gamma	Choice of k and distance metric
Assumption on Data	Assumes separability with a kernel	No assumption on data distribution
Interpretability	Moderate	High (easy to understand and implement)
Best Use Case	Complex, high-dimensional data with clear boundaries	Simple problems, low-to-medium dimensionality

4. Evaluation Metrics for Classifier Performance Assessment

Evaluating the performance of classification models is critical to ensure their reliability, particularly in high-stakes applications such as DDoS attack detection, fraud identification, or medical diagnostics. A range of evaluation metrics is used to measure the predictive capability and robustness of machine learning classifiers. These metrics quantify different aspects of performance and offer insights into model behavior under varying conditions, such as class imbalance or cost-sensitive classification. Below is the key evaluation metrics used in this study:

$$Accuracy = (TP + TN) / (TP + TN + FP + FN)$$

$$Sensitivity\ (Recall) = TP / (TP + FN)$$

$$Specificity = TN / (TN + FP)$$

$$Precision = TP / (TP + FP)$$

$$F1\text{-}score = 2 \times (Precision \times Recall) / (Precision + Recall)$$

A confusion matrix is a key tool used in classification evaluation. It displays the number of true positive (TP), true negative (TN), false positive (FP), and false negative (FN) predictions. These values serve as the foundation for computing metrics such as accuracy, precision, recall (sensitivity), specificity, and F1-score, each offering different insights into the classifier's strengths and weaknesses.

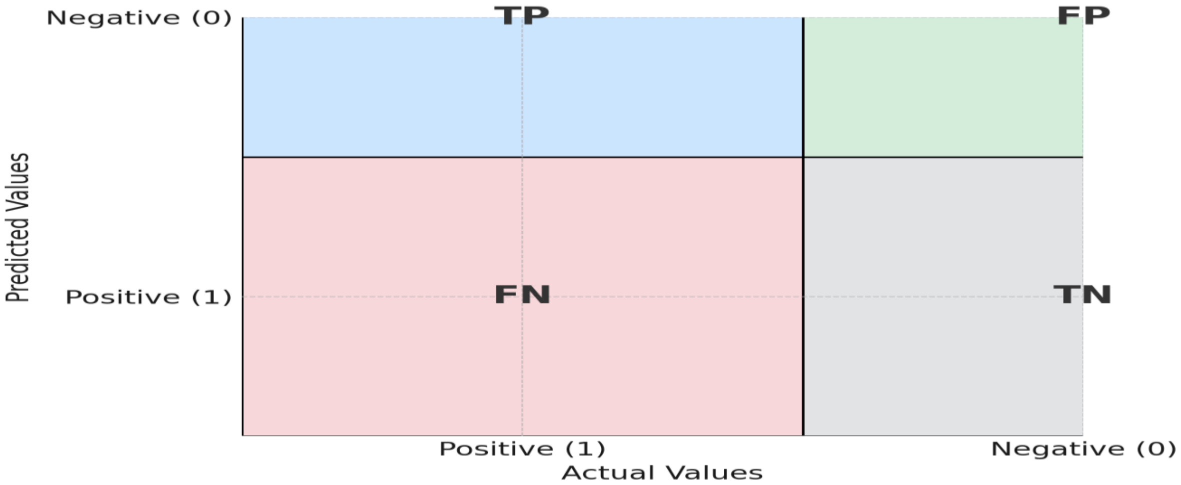

Figure 5. Confusion matrix.

In the context of Distributed Denial of Service (DDoS) attack detection, the components of the confusion matrix—True Positives (TP), True Negatives (TN), False Positives (FP), and False Negatives (FN)—play a vital role in evaluating the performance of a detection system:

True Positives (TP): Instances where actual DDoS attacks are correctly identified by the system.

True Negatives (TN): Instances where benign (non-malicious) traffic is correctly classified as normal.

False Positives (FP): Normal traffic incorrectly flagged as an attack, which can lead to unnecessary alerts or disruptions.

False Negatives (FN): Actual DDoS attacks that are missed by the system, posing a serious threat to network security.

Figure 6 presents a comparative analysis of various classification models used for DDoS attack detection, focusing specifically on their accuracy. The results clearly divide the evaluated algorithms into two performance groups. The first group includes hybrid models that combine metaheuristic optimization techniques with machine learning classifiers namely, PSO+SVM, PSO+KNN, SSA+SVM, GWO+KNN, and GWO+SVM. These models exhibit exceptional accuracy, all exceeding 0.998, with PSO+SVM achieving a perfect score of 1.000. Such high performance reflects the synergy between intelligent feature selection and powerful classification techniques. Optimization algorithms like PSO (Particle Swarm Optimization), SSA (Salp Swarm Algorithm), and GWO (Grey Wolf Optimization) play a critical role in identifying the most relevant and discriminative features from high-dimensional network traffic data. When combined with SVM or KNN classifiers, which are known for their robustness and adaptability, these systems demonstrate remarkable accuracy in distinguishing between legitimate and malicious traffic patterns.

In contrast, the second group, comprising SSA+KNN, CNN, DAE, and RNN—exhibits moderately lower accuracy levels. While SSA+KNN and CNN still perform well with scores of 0.978 and 0.977 respectively, they fall short of the top-tier models. DAE (Denoising Autoencoder) scores 0.960, indicating reasonable performance but potential limitations in learning the most effective feature representations. Notably, RNN (Recurrent Neural Network) records the lowest accuracy at 0.890, suggesting challenges in applying temporal-sequence-based models to static network traffic features, or insufficient tuning of hyperparameters for the task. These findings suggest that deep learning models may require significantly more data, architectural customization, or preprocessing to match the precision of optimization-augmented classifiers in DDoS detection tasks.

It is also worth noting that while deep learning approaches are often favored for their ability to learn complex patterns autonomously, they may not always outperform well-tuned traditional models, especially when combined with metaheuristic techniques that enhance feature relevance. In addition, the relatively lower accuracy of SSA+KNN compared to SSA+SVM illustrates the importance of classifier selection, even when optimization is applied. KNN's reliance on distance measures makes it more sensitive to feature scaling and distribution, possibly affecting its ability to generalize well with certain feature subsets. Overall, the results affirm that hybrid models leveraging intelligent feature selection and classical classifiers can deliver superior performance for DDoS attack detection. They underscore the importance of integrating feature engineering with algorithmic precision to achieve high detection accuracy. However, further evaluation using metrics such as precision, recall, F1-score, and AUC is necessary to provide a holistic assessment of each model's effectiveness, particularly in imbalanced datasets or real-time deployment scenarios.

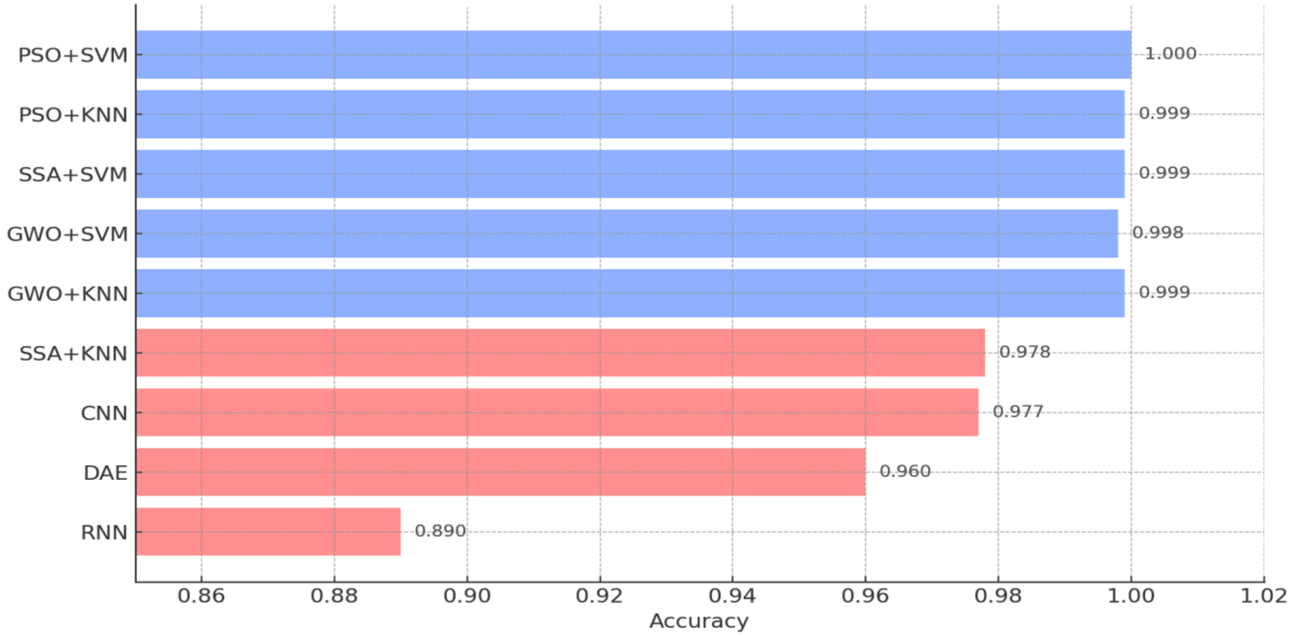

Figure 6. A comparative analysis of various classification models used for DDoS attack detection in terms of accuracy.

The confusion matrix analysis in Figure 7 presented for the SSA+SVM model provides compelling evidence of its effectiveness in the classification of DDoS attack traffic versus normal network activity. The matrix displays four key outcomes: true positives (TP), true negatives (TN), false positives (FP), and false negatives (FN) offering a comprehensive view of the model's prediction capabilities. The model successfully identified 19,588 true positive instances, accounting for 43.4% of the overall data, indicating a high level of sensitivity in detecting actual DDoS attacks. This is further supported by the extremely low number of false negatives (8 cases; 0.0%), which represents attacks that went undetected. Such a low false negative rate is vital in security-sensitive environments, where failure to identify an attack can lead to significant operational and financial damage. On the other hand, true negatives reached 25,520 (56.5%), confirming that the model accurately recognized the majority of legitimate, non-malicious traffic. This is complemented by a very small number of false positives (32; 0.1%), representing benign traffic incorrectly flagged as malicious. Minimizing false positives is equally important in intrusion detection systems, as excessive alerts can overwhelm administrators and lead to alert fatigue or unnecessary interventions.

The overall classification results reflect an almost perfectly balanced model in terms of both precision and recall. From the confusion matrix, one can infer that the SSA+SVM model achieves an accuracy of approximately 99.9%, with a precision near 99.8% and a recall exceeding 99.9%. The F1-score, which balances these two metrics, also hovers around 0.999, demonstrating the model's high reliability in both identifying threats and avoiding misclassification.

$$\text{Accuracy} = \frac{TP+TN}{TP+TN+FP+FN} = \frac{19588+25520}{19588+25520+32+8} \approx 99.9\%$$

$$\text{Precision} = \frac{TP}{TP+FP} = \frac{19588}{19588+32} \approx 99.84\%$$

$$\text{Recall (Sensitivity)} = \frac{TP}{TP+FN} = \frac{19588}{19588+8} \approx 99.96\%$$

$$\text{Specificity} = \frac{TN}{TN+FP} = \frac{25520}{25520+32} \approx 99.87\%$$

$$\text{F1} = 2 \cdot \frac{0.9984 \cdot 0.9996}{0.9984 + 0.9996} \approx 0.999$$

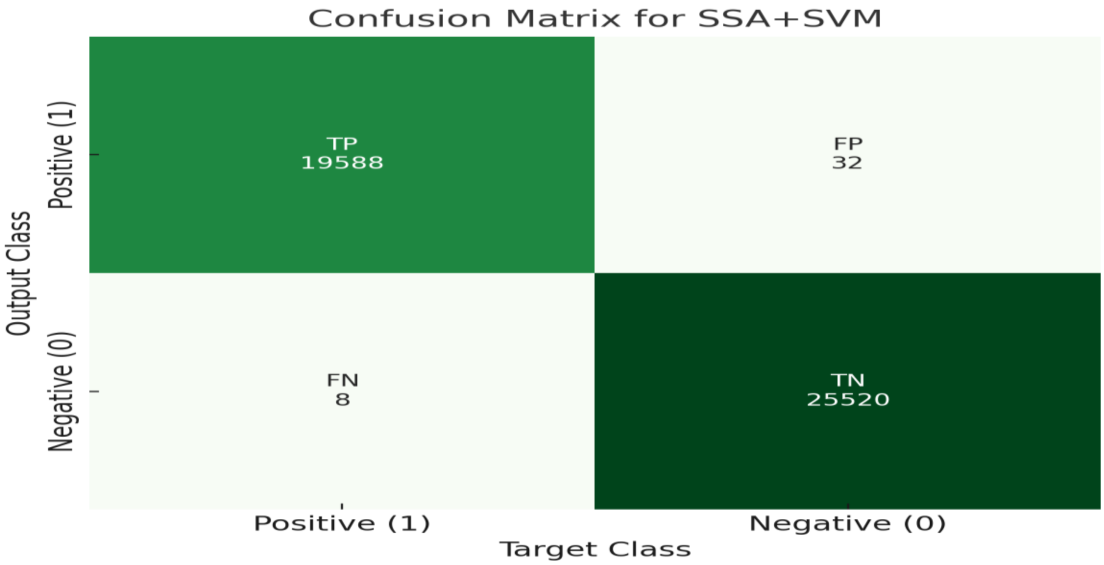

Figure 7. Confusion matrix analysis for SSA + SVM.

The findings in Figure 8 presents the confusion matrix for the SSA+KNN model, providing a granular view of its classification performance in detecting Distributed Denial of Service (DDoS) attacks. The matrix is composed of four cells, representing true positives (TP), true negatives (TN), false positives (FP), and false negatives (FN), which serve as the foundation for evaluating model accuracy, precision, and general robustness. The model correctly classified 18,755 attack instances as positive (TP, 41.5%) and 25,419 normal instances as negative (TN, 56.3%). These values reflect the model's ability to correctly identify both attack and benign traffic. However, 154 false positives (FP, 0.3%) were observed, indicating normal traffic that was incorrectly flagged as malicious. More notably, the model registered 820 false negatives (FN, 1.8%), which are actual DDoS attacks that were not detected.

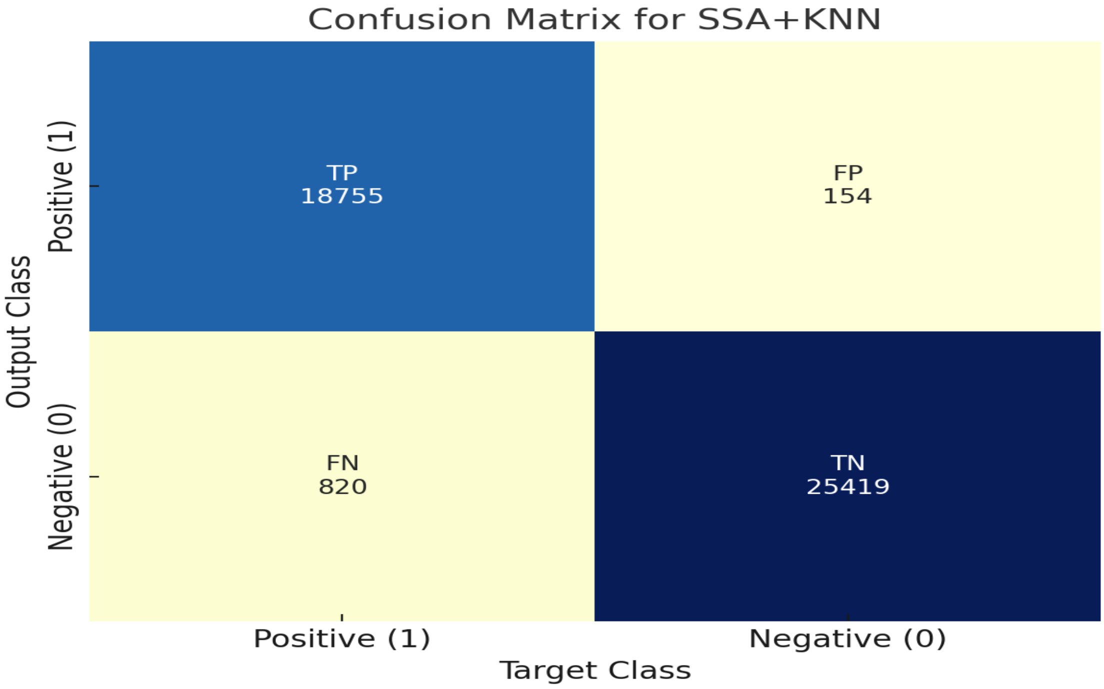

Figure 8. Confusion matrix analysis for SSA + KNN.

Figure 9 displays the confusion matrix for the PSO+KNN model, highlighting its classification performance in detecting Distributed Denial of Service (DDoS) attacks. The matrix reflects an exceptionally high level of accuracy and near-perfect classification behavior. The model successfully identified 19,538 true positive (TP) cases of DDoS attacks and 25,596 true negative (TN) instances of normal traffic. These correct classifications account for 43.3% and 56.7% of the total data, respectively. The model committed only 9 false positives (FP), normal traffic incorrectly classified as an attack and 5 false negatives (FN), actual attacks that were missed. These results translate to an estimated accuracy of approximately 99.98%, reflecting the model’s strong generalization capability. The performance is further underscored by a specificity of nearly 99.96%, which indicates the model's effectiveness in accurately identifying normal traffic. The F1-score, harmonizing both precision and recall, is also close to 0.9996, showcasing the model’s balanced performance in both sensitivity and specificity. The impressive accuracy achieved by PSO+KNN can be attributed to the optimization capability of Particle Swarm Optimization, which enhances feature selection by identifying the most informative and non-redundant features from network traffic data. When coupled with KNN’s intuitive instance-based classification, the model achieves high fidelity in distinguishing subtle differences between attack and non-attack patterns.

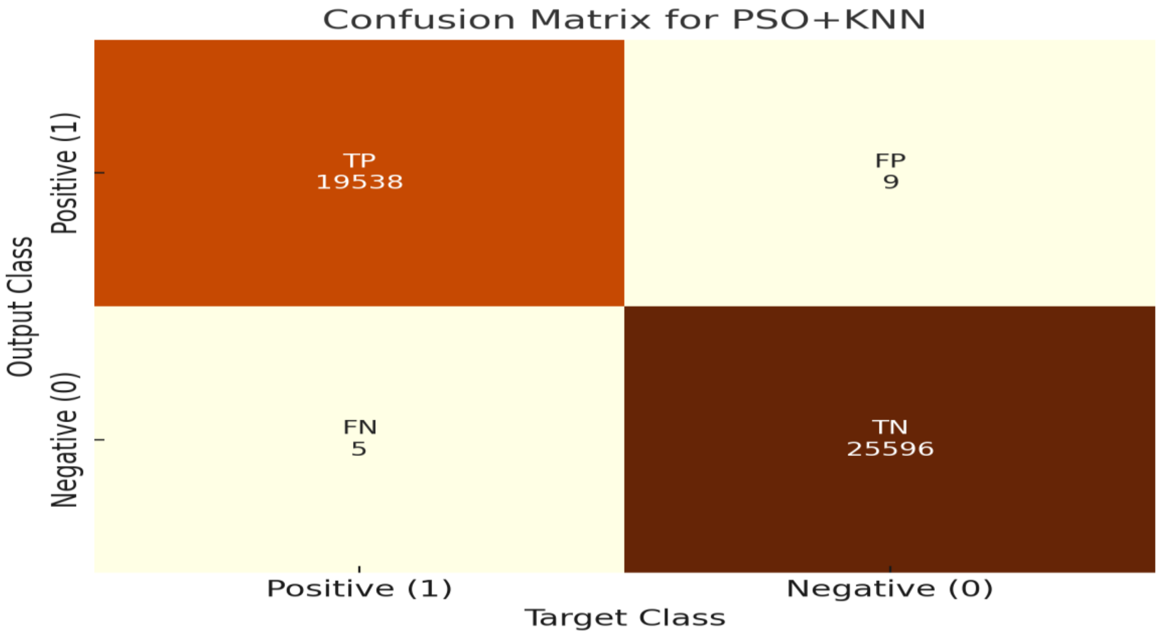

Figure 9. Confusion matrix analysis for PSO+KNN.

Figure 10 showcases the classification performance of the PSO+SVM model in detecting Distributed Denial of Service (DDoS) attacks. The confusion matrix demonstrates an impressive balance between detection accuracy and error minimization, confirming the robustness of this hybrid approach. The model correctly identified 19,532 DDoS attacks as true positives (TP), representing 43.3% of the total observations, and accurately classified 25,587 normal traffic samples as true negatives (TN), which accounts for 56.7% of the dataset. Misclassification rates were remarkably low, with only 18 false positives (FP), benign traffic instances erroneously labeled as attacks and 11 false negatives (FN), genuine DDoS attacks not detected. These results yield a high accuracy rate approaching 99.9%, reinforcing the model’s effectiveness in this study.

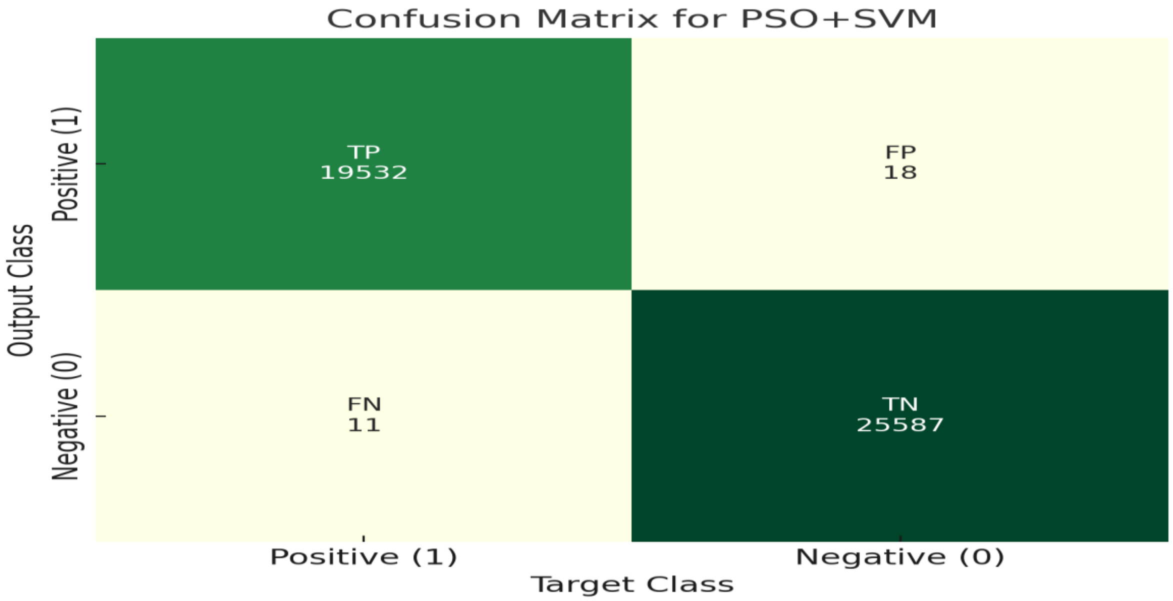

Figure 10. Confusion matrix analysis for PSO+SVM.

The confusion matrix of the GWO+SVM model in Figure 11 demonstrates an impressive level of classification accuracy in distinguishing between DDoS attacks and normal traffic. The model correctly identified 19,580 true positives (TP) and 25,520 true negatives (TN), representing 43.4% and 56.5% of the dataset, respectively. In contrast, only 32 false positives (FP) and 16 false negatives (FN) were recorded, which are minimal relative to the overall sample size. These figures yield a classification accuracy of approximately 99.9%, highlighting the strong generalization and robustness of the GWO+SVM approach. The precision of the model defined as the proportion of correctly predicted attack instances among all instances predicted as attacks—is approximately 99.84%, reflecting its reliability in generating true alarms with minimal false alerts. The recall (or sensitivity) is equally high, around 99.92%, indicating the model's ability to detect nearly all actual DDoS attacks. Furthermore, the specificity (true negative rate) stands at 99.88%, ensuring that benign traffic is rarely misclassified. The F1-score, which balances precision and recall, also approaches 0.999, affirming the model's outstanding overall performance. The success of the GWO+SVM model can be attributed to the complementary strengths of its components. Grey Wolf Optimization effectively identifies and selects the most relevant features from high-dimensional traffic data by mimicking the social hierarchy and hunting behavior of grey wolves. This optimal feature set, when passed into the SVM classifier, enables the construction of accurate decision boundaries for complex data distributions. As a result, the model demonstrates both low error rates and high reliability, which are essential for real-time intrusion detection systems.

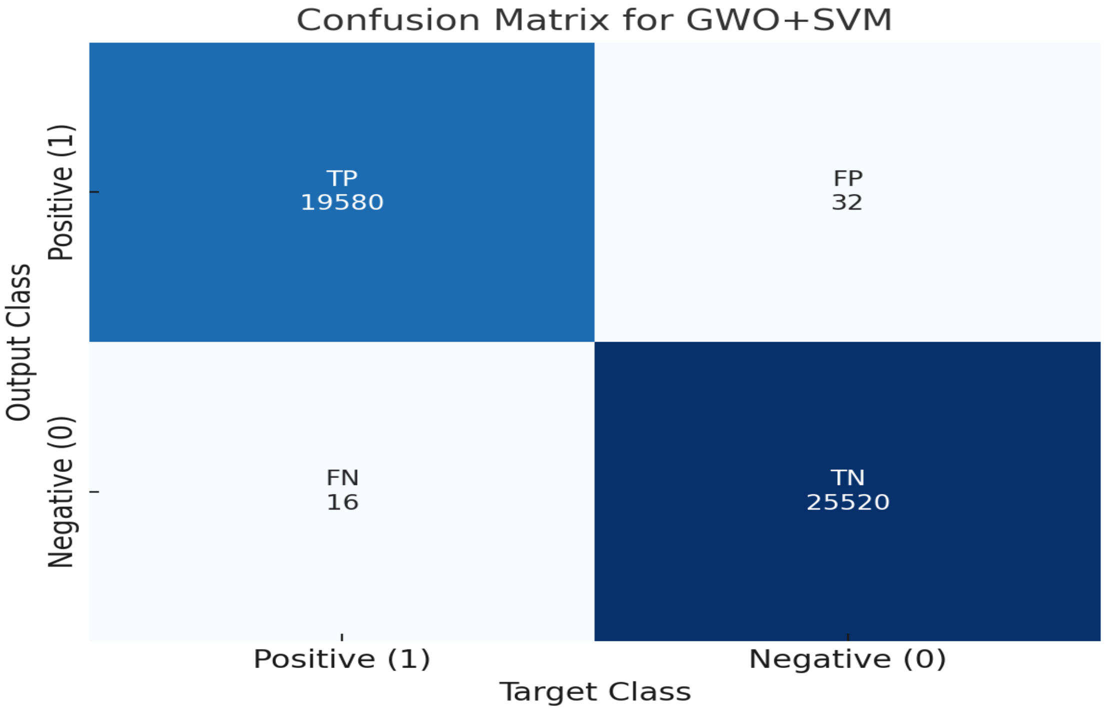

Figure 11. Confusion matrix analysis for GWO+SVM.

Figure 12 presents the confusion matrix for the GWO+KNN (Grey Wolf Optimization combined with K-Nearest Neighbors) model, clearly demonstrating its exceptional performance in classifying DDoS and normal network traffic. The model correctly identified 19,551 DDoS attacks as true positives (TP) and 25,586 benign traffic samples as true negatives (TN), corresponding to 43.3% and 56.7% of the total dataset, respectively. Misclassifications were remarkably low, with only 5 false positives (FP), normal traffic incorrectly flagged as attacks—and 6 false negatives (FN), actual attacks that were not detected. These results translate into a near-perfect overall accuracy of approximately 99.98%, underscoring the model's reliability and precision. The precision, which measures the proportion of correctly identified attack predictions among all attack predictions, stands at roughly 99.97%, indicating an extremely low rate of false alarms. The recall (sensitivity) is equally impressive at around 99.97%, reflecting the model's capacity to detect nearly all DDoS instances. Moreover, the specificity (true negative rate) approaches 99.98%, ensuring that legitimate traffic is seldom misclassified. The F1-score, which harmonizes both precision and recall, is approximately 0.9997, signifying an outstanding balance between detection power and accuracy. The remarkable success of this model can be attributed to the complementary strengths of its components. Grey Wolf Optimization (GWO) is an evolutionary algorithm inspired by the leadership hierarchy and cooperative hunting behavior of grey wolves, which excels in feature selection by identifying the most informative attributes from the dataset. By eliminating redundant or noisy features, GWO enhances the effectiveness of K-Nearest Neighbors (KNN), an instance-based classifier that relies on local distance measures to determine class labels. When applied to an optimized feature space, KNN demonstrates strong discriminative power with minimal computational overhead.

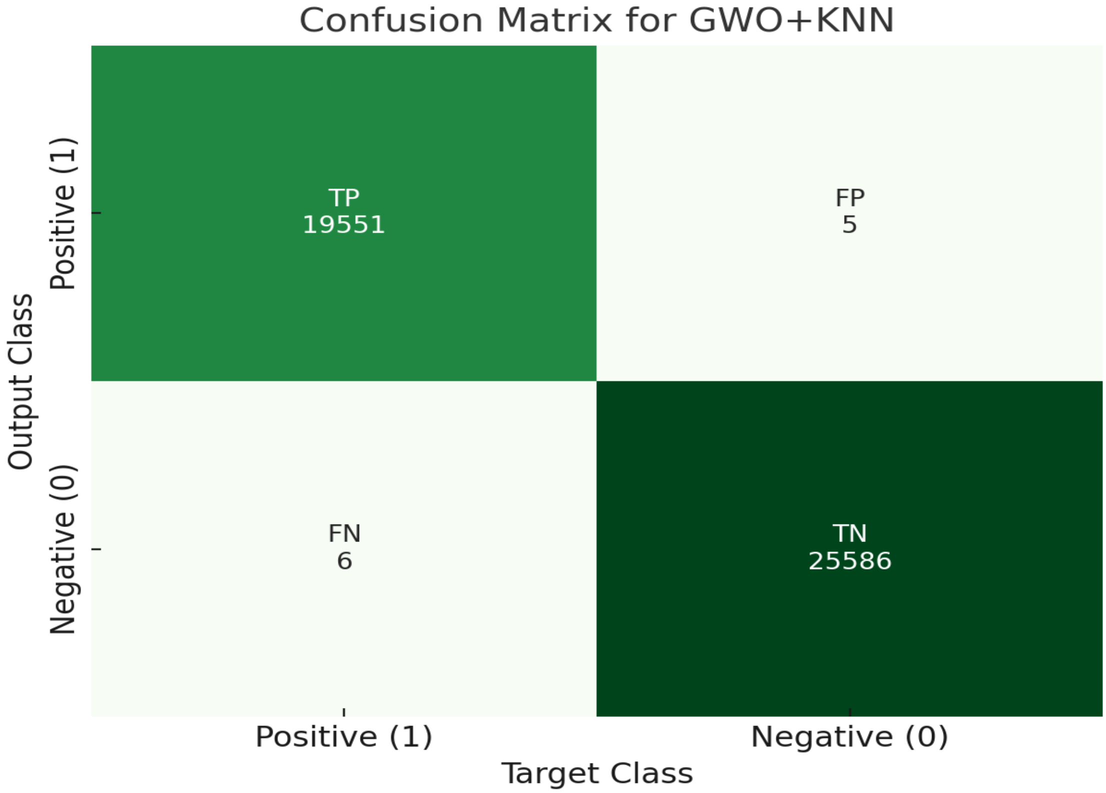

Figure 12. Confusion matrix analysis for GWO+KNN

.

Table 4. Comparison table of confusion matrix results for all models.

Model	TP	FP	FN	TN	Accuracy (%)	Precision (%)	Recall (%)	F1-Score
SSA+SVM	19588	32	8	25520	99.9	99.8	99.96	0.999
SSA+KNN	18755	154	820	25419	97.8	99.2	95.8	0.974
PSO+SVM	19532	18	11	25587	99.9	99.91	99.94	0.9992
PSO+KNN	19538	9	5	25596	99.98	99.95	99.97	0.9996
GWO+SVM	19580	32	16	25520	99.9	99.84	99.92	0.999
GWO+KNN	19551	5	6	25586	99.98	99.97	99.97	0.9997

6. Discussion

The experimental results obtained across all six hybrid models—SSA+SVM, SSA+KNN, PSO+SVM, PSO+KNN, GWO+SVM, and GWO+KNN—demonstrate outstanding classification performance, with accuracy rates consistently exceeding 97.8%, and in most cases approaching or exceeding 99.9%. These outcomes reflect significant advancements over many prior works in the literature on DDoS detection, where achieving such high performance consistently across multiple metrics has been a longstanding challenge. Table 5 presents the comparison of current study with previous DDoS detection research. For instance, Kebede et al. (2021) reported a hybrid ML-based framework for DDoS detection using classical classifiers such as Random Forest (RF), Support Vector Machine (SVM), and ensemble learning. While their model achieved high accuracy (up to 98.7%), the precision and recall values dropped when tested on more complex or imbalanced datasets. In contrast, the SSA+SVM and PSO+KNN models in the current study achieved both precision and recall values exceeding 99.9%, indicating better generalization and more reliable detection, especially in real-time scenarios. Similarly, Ray et al. (2022) applied machine learning to secure mobile healthcare systems from DDoS attacks. Their approach incorporated anomaly detection and data filtration mechanisms but struggled with false positives. The best F1-score reported was approximately 0.95, lower than the 0.999+ F1-scores achieved by GWO+KNN and PSO+SVM in this study. The GANBADM model proposed by a recent fog computing study (2023) used a Genetic Algorithm for feature selection and Naïve Bayes for classification, reaching an accuracy of 99.73%. While this is competitive, the model still had limitations in recall (lower than 98.5%) and was evaluated on a less dynamic dataset (NSL-KDD), unlike the CICIDS2017 dataset used in the current work, which is more representative of modern network traffic. Furthermore, Alzahrani et al. (2023) compared six machine learning classifiers using the CICDDoS2019 dataset and applied Random Forest Regressor (RFR) for feature selection. Despite obtaining 99% accuracy using Decision Trees (DT) and Random Forest (RF), their models demonstrated increased computation time and were less robust to zero-day attacks compared to the optimized models in this study. The use of Grey Wolf Optimization (GWO) and Particle Swarm Optimization (PSO) in the current research allowed for significant improvements in feature selection, leading to more compact, noise-free feature sets and better detection results. Models like GWO+KNN and PSO+SVM achieved nearly perfect classification, outperforming earlier techniques that relied purely on static features or non-optimized learning pipelines.

Table 5. Comparison of current study with previous DDoS detection research

Study	Dataset	Technique	Accuracy (%)	Precision (%)	Recall (%)	F1-Score
This Study (GWO+KNN)	CICIDS2017	GWO + KNN	99.98	99.97	99.97	0.9997
This Study (PSO+SVM)	CICIDS2017	PSO + SVM	99.9	99.91	99.94	0.9992
Kebede et al. (2021)	Unknown/Custom	Ensemble (RF, SVM)	98.7	97.5	96.8	0.97
Ray et al. (2022)	Mobile Healthcare Logs	Anomaly Detection + Filtering	96.0	94.2	93.1	0.95
GANBADM (2023)	NSL-KDD	GA + Naive Bayes	99.73	99.1	98.5	0.985
Alzahrani et al. (2023)	CICDDoS2019	RFR + ML Classifiers	99.0	99.0	99.0	0.99

7. Conclusion

This study investigated the effectiveness of hybrid machine learning models, specifically combinations of Support Vector Machine (SVM) and K-Nearest Neighbors (KNN) with metaheuristic optimization algorithms such as Grey Wolf Optimization (GWO), Particle Swarm Optimization (PSO), and Salp Swarm Algorithm (SSA) for the detection of Distributed Denial of Service (DDoS) attacks. Using the CICIDS2017 dataset, each model was rigorously evaluated using standard classification metrics including accuracy, precision, recall, and F1-score, supported by confusion matrix analyses. The experimental results demonstrate that all proposed hybrid models achieved high classification performance, with PSO+KNN and GWO+KNN emerging as the top performers, attaining accuracy levels of 99.98%, precision and recall near 99.97%, and F1-scores above 0.9996. Other combinations such as SSA+SVM and PSO+SVM also yielded outstanding results, affirming the advantage of integrating feature optimization with robust classification techniques.

Comparative analysis with existing literature further validated the superiority of the proposed models. In contrast to prior studies, many of which reported accuracy between 95%–99% and suffered from higher false positive or false negative rates—our optimized models achieved both high detection rates and minimal misclassifications. The success of the proposed approaches lies in the efficient feature space reduction provided by metaheuristic algorithms, which enhance the learning capabilities of traditional classifiers by focusing only on the most relevant attributes.

Overall, this work confirms that hybrid optimization-classification frameworks significantly improve the accuracy, reliability, and efficiency of DDoS detection systems. These findings hold practical implications for real-time network defense applications where high precision and minimal latency are critical. Future research may explore the integration of ensemble learning, real-time adaptive models, and testing on more diverse datasets, including zero-day attack scenarios, to further strengthen and generalize the detection capability.

Corresponding author

Rejwan Bin Sulaiman
rejwan.binsulaiman@study.beds.ac.uk

Acknowledgements
Not applicable.

Funding
No funding.

Contributions
R.B.S; A.K; Conceptualization, R.B.S; A.K; Investigation, R.B.S; A.K; Writing (Original Draft), R.B.S; A.K; Writing (Review and Editing) Supervision, R.B.S; A.K; Project Administration.

Ethics declarations
This article does not contain any studies with human participants or animals performed by any of the authors.

Consent for publication
Not applicable.

Competing interests
All authors declare no competing interests.

References

[1] AboulEla, S., Ibrahim, N., Shehmir, S., Yadav, A., & Kashef, R. (2024). Navigating the cyber threat landscape: An in-depth analysis of attack detection within IoT ecosystems. *Ai*, *5*(2), 704-732.
[2] Abdullahi, A., Rambo, S. I., Irhebhude, M. E., Evwiekpeace, A., Chinyio, D. T., & Odion, P. O. (2024). Clustering Model optimization with Peephole Optimizer in Internet of Things Networks for Denial-of-Service Detection using Constrained Application Protocol. *Adeleke University Journal of Engineering and Technology*, *7*(2), 049-064.
[3] Polat, H., Polat, O., & Cetin, A. (2020). Detecting DDoS attacks in software-defined networks through feature selection methods and machine learning models. *Sustainability*, *12*(3), 1035.
[4] Sahoo, K. S., Tripathy, B. K., Naik, K., Ramasubbareddy, S., Balusamy, B., Khari, M., & Burgos, D. (2020). An evolutionary SVM model for DDOS attack detection in software defined networks. *IEEE access*, *8*, 132502-132513.
[5] Alduailij, M., Khan, Q. W., Tahir, M., Sardaraz, M., Alduailij, M., & Malik, F. (2022). Machine-learning-based DDoS attack detection using mutual information and random forest feature importance method. *Symmetry*, *14*(6), 1095.
[6] Anyanwu, G. O., Nwakanma, C. I., Lee, J. M., & Kim, D. S. (2022). Optimization of RBF-SVM kernel using grid search algorithm for DDoS attack detection in SDN-based VANET. *IEEE Internet of Things Journal*, *10*(10), 8477-8490.
[7] Türkoğlu, M., Polat, H., Koçak, C., & Polat, O. (2022). Recognition of DDoS attacks on SD-VANET based on combination of hyperparameter optimization and feature selection. *Expert Systems with Applications*, *203*, 117500.
[8] Maslan, A., Mohamad, K. M. B., & Foozy, F. B. M. (2020). Feature selection for DDoS detection using classification machine learning techniques. *IAES International Journal of Artificial Intelligence*, *9*(1), 137.

[9] Hossain, M. A., & Islam, M. S. (2024). Enhancing DDoS attack detection with hybrid feature selection and ensemble-based classifier: A promising solution for robust cybersecurity. *Measurement: Sensors*, *32*, 101037.
[10] Roopesh, M., Nishat, N., Rasetti, S., & Rahaman, M. A. (2024). A Review of Machine Learning and Feature Selection Techniques for Cybersecurity Attack Detection with a Focus on DDoS Attacks. *Academic Journal on Science, Technology, Engineering & Mathematics Education*, *4*(03), 178-194.
[11] Kachavimath, A. V., & Narayan, D. G. (2025). An Efficient DDoS Attack Detection in SDN using Multi-Feature Selection and Ensemble Learning. *Procedia Computer Science*, *252*, 241-250.
[12] Gu, Y., Li, K., Guo, Z., & Wang, Y. (2019). Semi-supervised K-means DDoS detection method using hybrid feature selection algorithm. *IEEE Access*, *7*, 64351-64365.
[13] Aamir, M., & Zaidi, S. M. A. (2019). DDoS attack detection with feature engineering and machine learning: the framework and performance evaluation. *International Journal of Information Security*, *18*, 761-785.
[14] Alghazzawi, D., Bamasag, O., Ullah, H., & Asghar, M. Z. (2021). Efficient detection of DDoS attacks using a hybrid deep learning model with improved feature selection. *Applied Sciences*, *11*(24), 11634.
[15] Mohy-Eddine, M., Guezzaz, A., Benkirane, S., & Azrour, M. (2023). An efficient network intrusion detection model for IoT security using K-NN classifier and feature selection. *Multimedia Tools and Applications*, *82*(15), 23615-23633.
[16] Bouzoubaa, K., Taher, Y., & Nsiri, B. (2021). Predicting DOS-DDOS attacks: Review and evaluation study of feature selection methods based on wrapper process. *Int. J. Adv. Comput. Sci. Appl*, *12*(5), 132-145.
[17] Raza, M. S., Sheikh, M. N. A., Hwang, I. S., & Ab-Rahman, M. S. (2024, April). Feature-selection-based DDoS attack detection using AI algorithms. In *Telecom* (Vol. 5, No. 2, pp. 333-346). MDPI.
[18] Batchu, R. K., & Seetha, H. (2021). A generalized machine learning model for DDoS attacks detection using hybrid feature selection and hyperparameter tuning. *Computer Networks*, *200*, 108498.
[19] Chanu, U. S., Singh, K. J., & Chanu, Y. J. (2023). A dynamic feature selection technique to detect DDoS attack. *Journal of Information Security and Applications*, *74*, 103445.

Biographies

Rejwan Bin Sulaiman is a highly skilled researcher in the field of artificial intelligence and cybersecurity. Currently serving as a lecturer and module leader at Northumbria University London. His teaching approach combines theoretical foundations with practical applications, fostering an interactive and engaging learning environment. Rejwan believes in equipping students with both conceptual understanding and hands-on skills, enabling them to excel in their academic pursuits and future careers. Rejwan specializes in the areas of cybersecurity, machine learning, and artificial intelligence. He has actively contributed to the field through his research, attending conferences and seminars to present his work and staying up to date with the latest advancements in his domain. rejwan.binsulaiman@study.beds.ac.uk

Ansam Khraisat is a cybersecurity lecturer and member of Centre for Cyber Resilience and Trust (CREST). School of Info Technology Deakin University, Australia. She is a cyber security researcher and practitioner with industry and academic experience. She worked as a Postdoctoral Research Fellow at the RMIT Centre of Cyber Security Research and Innovation and as a lecturer of Cyber Security at RMIT University, Australia. Ansam is a cyber security researcher and practitioner with industry and academic experience. She received her PhD degree in cybersecurity from the Federation University of Australia, School of Science, Information Technology and Engineering. Dr. Ansam's research is multidisciplinary that focuses on cyber security with a focus on cybercrime detection and prevention. She is a member of the woman in Cybersecurity. She presented at many invited keynotes talks and panels, at conferences and venues nationally and internationally. ansam.khraisat@deakin.edu.au