Al-Furat Journal of Innovations in Electronics and Computer Engineering (FJIECE)
ISSN -2708-3985

# Metaheuristic Optimization in Machine Learning for Cyber Attack Detection: A Review of Techniques and Applications

Roaa Safi Abed Alah[1], Sarah Riyadh Adnan[2], Aqeel Majeed Breesam[3*]

[1]Department of Intelligent Medical Systems, University of Information Technology and Communication, Baghdad, Iraq
rouaa.safi@uoitc.edu.iq
[2]High Institute for Infertility Diagnosis Assisted Reproductive Technologies, Al-Nahrain University, Baghdad, Iraq
sara.r.adnan@nahrainuniv.edu.iq
[3]Institute of Medical Technology/ Baghdad, Middle Technical University, Baghdad, Iraq
aqeelmajeed@mtu.edu.iq

**Article's Information**

Received: 15.01.2026
Accepted: 17.02.2026
Published: 31.03.2026

**Keywords:**
Intrusion Detection Systems
Cyber-attack detection
Metaheuristic optimization
Feature selection
Multi-objective optimization

**Abstract**

The speed of cyber-attacks and the increasing complexity of cyber theft has made intrusion detection a focal point in today's cybersecurity environment. The present paper is an overview of metaheuristic optimization techniques to detect cyber-attacks using machine learning. The purpose of this survey is to review the use of metaheuristic algorithms in the improvement of intrusion detection systems (IDSs) in terms of feature selection, parameter optimization, and multi-objective optimization. This survey covers the main work that uses single-objective and multi-objective metaheuristic algorithms such as evolutionary algorithms, swarm intelligence algorithms, and hybrid metaheuristic optimization approaches. The papers are reviewed in terms of their use for IDS tasks, use of single-objective and/or multi-objective optimization, and their performance using benchmarking datasets. The survey shows some of the trends: metaheuristic algorithms are highly effective for feature selection, classification performance, and a combination of detection rate and false alarm rate. And hybrid solutions that use metaheuristic algorithms and machine learning / deep learning algorithms, such as Convolutional Neural Networks (CNN) and Gradient Boosting, are more effective than single solutions. The advantages are clear, yet the research also intersects some of the challenges related to the methods, including scalability, efficiency, interpretability, and adversarial attack resistance. Based on these insights, future research will focus on developing adaptive and scalable optimisation approaches, integrating optimisation approaches into real-time and distributed systems, and designing interpretable and robust IDS. This survey offers a practical perspective on the metaheuristic optimisation for cyber-attack detection techniques, and the use of metaheuristic optimisation in designing efficient and scalable IDS.

https://doi.org/10.46649/fjiece.v5.1.16a.31.3.2026
*Corresponding author: aqeelmajeed@mtu.edu.iq

Al-Furat Journal of Innovations in Electronics and Computer Engineering (FJIECE)
ISSN -2708-3985

## 1. INTRODUCTION

Cyber-attacks are increasingly frequent, complex, and dynamic and pose a significant threat to existing digital systems. As networked systems are becoming more widespread in areas such as health, industry, engineering, monitoring, and defense, there is a demand for secure communication and data integrity [1, 2]. Intrusion Detection Systems (IDSs) play a critical role in detecting intrusions, but the rule-based systems are generally ineffective for the new and evolving types of attacks.

Machine learning (ML) techniques have been widely used in IDSs as they provide a means to learn patterns from complex and nonlinear data. While effective, ML-based intrusion detection models have several issues, including the high-dimensional feature space, redundant and/or irrelevant attributes, and parameter tuning. This affects the detection performance, computational cost, and generalisation power. Similar optimization problems have been extensively studied in other networked systems, such as Wireless Sensor Networks (WSNs), where tasks such as deployment, location, energy consumption, and clustering need to be optimized [38]. These similarities call for having effective optimization techniques in order to improve the performance of various systems.

The emergence of metaheuristic algorithms as a potent way of solving complex optimization problems where the deterministic approach has failed to work has been identified [9]. These algorithms are usually divided into single-objective (SO) algorithms, which maximize one performance criterion [10], and multi-objective (MO) algorithms, which maximize several conflicting objectives at the same time [11]. Metaheuristic methods are gradient-free and highly exploratory; therefore, they have been successfully exploited in other engineering and computational applications [12, 13]. They come in handy, especially in detecting cyber-attacks, feature selection, hyperparameter optimization, and classifier performance.

Although several studies have examined the use of metaheuristic algorithms in optimization problems, most research studies concentrate on the use of a single technique without giving a critical and in-depth comparison in the context of intrusion detection. The wider networked systems have also been analyzed in the past, which offers a hint on how to model the strategies and performance measurement [14]. However, a systematic review where metaheuristic optimization techniques are associated with their practical applicability in ML-based cyber-attack detection is still required.

Therefore, this article is a metaheuristic optimization methodology review in intrusion detection systems. It discusses some of the most important types of algorithms, their comparative roles in feature selection and model optimization, and the primary problems and outlook of future research. It is aimed at offering a better insight into how these methods can be used to develop precise, scalable, and resilient cyber-attack detection systems.

### *1.1. METAHEURISTIC TECHNIQUES*

Complex optimization problems are solved with the help of metaheuristic (MH) techniques because they can efficiently search large and nonlinear search spaces without the need to have gradient information [15]. This has made them very popular as they are flexible, easy to implement, and can produce high-quality solutions in a reasonable amount of computational time [16, 17]. These properties are especially useful in the context of cyber-attack detection, where intrusion detection models have to operate with high-dimensional data, and at the same time, they must be highly accurate and low in computation cost.

Metaheuristic algorithms are usually categorized according to the inspiration. They have been classified into four in this work: evolutionary algorithms, swarm intelligence methods, physics-inspired (based on natural phenomena), and human-inspired algorithms [18, 19]. This categorization is structural, as well as indicative of the variations in search behavior, convergence properties, and appropriateness to intrusion detection tasks.

Al-Furat Journal of Innovations in Electronics and Computer Engineering (FJIECE)
ISSN -2708-3985

Evolutionary algorithms (EAs) are based on biological evolution and use the process of selection, mutation, and crossover. Such representative methods are the Arithmetic Optimization Algorithm (AOA) [20], evolutionary programming [21], Genetic Algorithms (GA) [22, 23], Evolution Strategies (ES) [24], Differential Evolution (DE) [25], and Genetic Programming (GP) [26]. These algorithms are useful in global search and are commonly applied in feature selection in intrusion detection. However, they may be more computationally expensive since they might be an iterative population-based operation.

The Swarm intelligence (SI) methods are inspired by the social life of living organisms. They are Particle Swarm Optimization (PSO) [27], Salp Swarm Algorithm (SSA) [28], Marine Predators Algorithm (MPA) [29] and Whale Optimization Algorithm (WOA) [30]. These are the processes that are described by the fact of a quick convergence and simplicity of implementation. They have widely been used in optimization of IDS as they can moderate the exploration and exploitation although in few cases they may converge too early.

The third group consists of physics-inspired and natural phenomena-based algorithms, which include Water Cycle Algorithm (WCA) [31], Spiral Optimization (SO) [32], Wind-Driven Optimization (WDO) [33], Field of Force (FOF) [34], Electromagnetism Algorithm [35], Charged System Search (CSS) [36], Simulated Annealing [37], Gravitational Search Algorithm (GSA) [38], Aquila Optimizer (AO) [39], Optics- Unlike in the original presentation, these methods are here considered as a single category to prevent the overlap of concepts. They are robust modeling of physical processes to enhance search dynamics, although their ability to process noisy and high-dimensional data defines their ability to detect cyber-attacks.

Social, educational, or competitive behaviors are modeled by human-inspired algorithms. They include Teaching-Learning-Based Optimization (TLBO) [43], Volleyball Premier League Algorithm (VPL) [44], Seeker Optimization Algorithm (SOA) [45], Soccer League Competition (SLC) [46], and League Championship Algorithm (LCA) [47]. Although these methods present novel optimization methods, their use in intrusion detection must be considered in terms of quantifiable increases in detection accuracy and computational efficiency.

In general, this classification is a structured description, but the aim of this survey is not to list algorithms. Rather, it critically analyzes the contribution of these techniques to enhance machine learning-based cyber-attack detection.

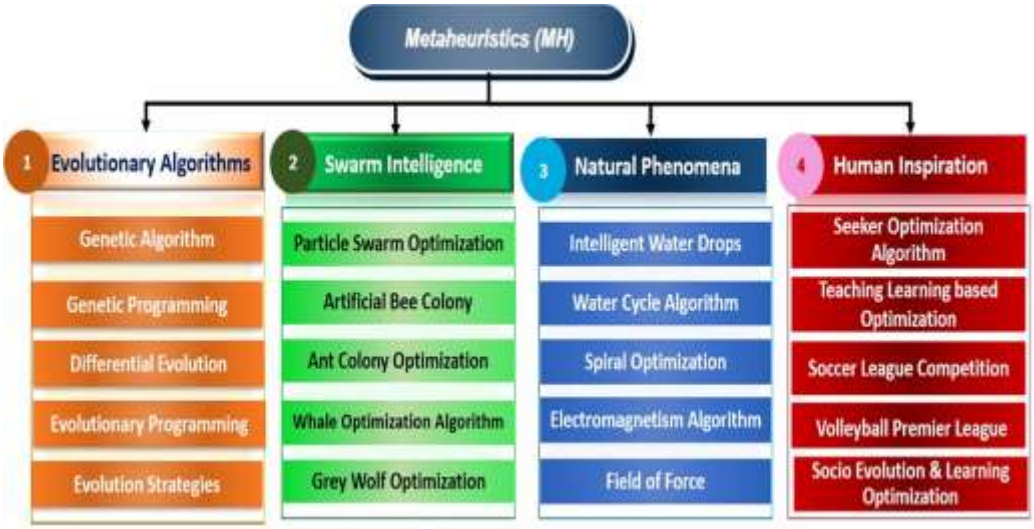


**Fig. 1. Classification of metaheuristic algorithms into evolutionary, swarm intelligence, physics-inspired, and human-inspired approaches, highlighting their relevance to optimization tasks in machine learning-based cyber-attack detection.**

Figure 1 represents the primary divisions of metaheuristic algorithms that were taken into account in this survey. Even though these categories vary in terms of the inspiration they use, and the way they are

used to detect cyber-attacks, they are important in detecting cyber-attacks because they can maximize the choice of features, enhance the performance of classifiers, and balance exploration and exploitation in high dimensional search space.

### *1.2. SINGLE-OBJECTIVE AND MULTI-OBJECTIVE METAHEURISTIC ALGORITHMS*

The metaheuristic optimization problems can be divided into single-objective (SO) and multi-objective (MO) ones, based on the number of optimization criteria. This difference is especially significant in cyber-attack detection, where the objectives of optimization can be different, such as maximizing detection accuracy or balancing a variety of performance measures.

Single-objective (SO) algorithms are aimed at maximizing one performance measure, e.g. classification accuracy, detection rate, or quality of feature subset. Such techniques are usually used in intrusion detection, whereby the ultimate goal is to enhance a given performance measure. Representative algorithms are Neural Network Algorithm (NNA) [48], combining optimization and neural structures, Artificial Electric Field Algorithm (AEFA) [49], which proves to be efficient with nonlinear optimization problems, and Seagull Optimization Algorithm (SOA) [50], which improves the trade-off between exploration and exploitation. Other algorithms like Artificial Ecosystem-Based Optimization (AEO) [51] and Artificial Gorilla Troops Optimizer (GTO) [52] show good performance in managing complex and high-dimensional search spaces. We also have algorithms like the Orca Predation Algorithm (OPA) [53] and Hunger Games Search (HGS) [54] that are directed at the improvement of convergence behavior and flexibility. Though SO algorithms have advantages with respect to particular optimization tasks, their greatest weakness is that they cannot be used to address multiple conflicting objectives simultaneously.

Multi-objective (MO) algorithms, in their turn, are the algorithms, which prefer to maximize two or more criteria simultaneously. This is often a trade-off to the accuracy of detection and the false alarm rates, the computational cost and the complexity of the model of cyber-attack detection. Other algorithms such as the Mayfly Algorithm (MA) [55], a hybrid of evolutionary and swarm-based algorithms to achieve improved convergence, MO Artificial Bee Colony (MOABC) [58] which has been demonstrated to effectively approximate Pareto-optimal solutions, and MO Artificial Immune Algorithm to Fuzzy Clustering (MOFC) [59] are focused on improving robustness and diversity of the Such algorithms as MO Grasshopper Optimization Algorithm (MOGOA) [62] and MO Grey Wolf Optimizer (MOGWO) [63] have shown a high level of performance in terms of maintaining the balance between the speed of convergence and the diversity of solutions, whereas MO Sine-Cosine Algorithm (MOSCA) [65] and MO Volleyball Premier League Approach (MOVPL) [72]. Such algorithms generate a set of Pareto-optimal solutions and, therefore, the decision-makers are free to select the most appropriate trade-off among conflicting objectives.

MO algorithms are more appropriate to the real-world intrusion detection systems that operate with multiple performance measures that need to be taken concurrently as compared to SO approaches. However, this advantage is accompanied by the fact that the level of computational complexity is high, and more advanced evaluation strategies are required.

The main features and uses of the representative SO and MO metaheuristic algorithms are summarized in Table 1. The two categories have a sharp difference that can be observed. SO algorithms are mainly applied to optimize single performance measures and are commonly assessed with reference to benchmark engineering problems. Instead, MO algorithms are concerned with the trade-off analysis and robustness between different objectives. This distinction is particularly notable in the context of cyber-attack detection since real-world applications of IDS have to trade off the detection accuracy, computation efficiency, and false alarms. Thus, SO algorithms are still appropriate to a set of optimization tasks, but MO approaches offer a more detailed framework to be applied to real-life.

Al-Furat Journal of Innovations in Electronics and Computer Engineering (FJIECE)
ISSN -2708-3985

**Table 1. The summary of features and applications of single- and multi-objective metaheuristic algorithms**

| Algorithm Type | Algorithm | Key Features and Applications |
|---|---|---|
| Single-Objective (SO) | Neural Network Algorithm (NNA) | Inspired by biological nervous systems, validated for Pressure vessel design, welded beam design, and gear train design. Demonstrates superior performance over competing methods [48]. |
| | Artificial Electric Field Algorithm (AEFA) | Based on Coulomb's law of electrostatic force, validated on CEC 2015 benchmark functions, excels in nonlinear optimization problems [49]. |
| | Seagull Optimization Algorithm (SOA) | Mimics seagull behaviors for enhanced search space Exploration and exploitation, applied to optical buffer design and tension/compression spring design [50]. |
| | Artificial Ecosystem-Based Optimization (AEO) | Models energy flow in ecosystems; works effectively on practical engineering challenges like multiple disk clutch brake systems and cantilever beams. [51]. |
| | Artificial Gorilla Troops Optimizer (GTO) | Inspired by the social intelligence of gorilla troops, effective in high-dimensional problems like spacecraft trajectory optimization [52]. |
| | Orca Predation Algorithm (OPA) | Mimics cooperative hunting behavior of orcas; excels in constrained problems like welded beam and three-bar truss designs [53]. |
| | Hunger Games Search (HGS) | Inspired by hunger-driven animal behaviors, scalable and adaptable for diverse engineering tasks [54]. |
| Multi-Objective (MO) | Mayfly Algorithm (MA) | Combines swarm intelligence with evolutionary algorithms; excels in discrete flow shop scheduling [55]. |
| | MO Artificial Bee Colony (MOABC) | Uses a grid-based approach for evaluating Pareto fronts; effective in solving MO challenges [58]. |
| | MO Artificial Immune Algorithm for Fuzzy Clustering (MAFC) | Enhances clustering accuracy through multi-kernel learning and optimization strategies [59]. |
| | MO Water Cycle Algorithm (MOWCA) | Simulates the natural water cycle; resilient in engineering design problems [60]. |
| | MO Spotted Hyena Optimizer (MOSHO) | Inspired by social and hunting behaviors of hyenas; employs a fixed-size archive and roulette wheel mechanism [61]. |
| | MO Grasshopper Optimization Algorithm (MOGOA) | Effective in MO challenges, surpassing traditional methods like MOEA/D and MOPSO [62]. |
| | MO Sine-Cosine Algorithm (MOSCA) | Applied in spring and welded beam designs; demonstrates significant improvements in MO challenges [65]. |
| | MO Volleyball Premier League Approach (MOVPL) | Addresses global optimization problems with complex objectives; outperforms existing MO models [72]. |
| Evaluation Criteria | Statistical Metrics | Includes mean, standard deviation, and statistical tests like the Wilcoxon rank-sum test to validate algorithm performance [68] [69]. |
| | Convergence Curves | Visualize the relationship between iterations and objective function performance; assess optimization dynamics [70]. |
| | Real-World Applications | Practical problems like welded beam and disk brake designs serve as benchmarks to test applicability [71]. |

 

## 2. RELATED WORK

The conventional rule-based network intrusion detection method of monitoring has gradually been supplanted by machine learning (ML) and deep learning (DL) techniques because the attack traffic currently is high-dimensional, dynamic, and inaccessible, and can only be identified by a combination of static signatures. As the review studies by Abraham and Bindu [73] and Ahmad et al. [77] have shown, the ML- and DL-based intrusion detection systems (IDSs) have become one of the main research directions as they can learn more complex traffic patterns and adapt to the changing attacks in a more efficient way than the traditional methods. Simultaneously, the secure system design is a fundamental issue. Karim et al. [74] stressed that downstream vulnerabilities could be minimized by considering security practices at the early stages of the software development life cycle, and Chandrashekar and Sahin [75] demonstrated that feature selection is a crucial component in high-dimensional classification problems since redundant attributes could raise the computational cost and decrease the effectiveness of the model.

The literature available can be divided into three broad directions, namely, deep learning-based IDS architectures, feature-selection and representation-learning approaches, and metaheuristic or bio-inspired hybrid frameworks. This organization offers a more analytical framework than a mere list of studies, and it is easier to find how the field has developed since the construction of classifiers to optimization-conscious intrusion detection models.

The former direction is concerned with deep learning-based IDS architectures. Zhang et al. [78] developed an intrusion detection model, which relied on the generation of features and a visualization plan, in which the primary improvement was better representation and separability of classes before classification, instead of a hybrid CNN-gcForest architecture. Yu et al. [79] proposed stacking dilated convolutional autoencoders, which showed that hierarchical unsupervised representation learning can enhance the extraction of features in network traffic. Karatas et al. [80] explored CNN-based packet classification and demonstrated that convolutional models are capable of learning discriminative patterns of packet data. Wu and Guo [76] introduced LuNet, a hierarchical CNN+RNN architecture that simultaneously encodes spatial and temporal traffic information and stated that it has high detection performance and reduced false-positive alarms compared to other approaches. Jiang et al. [81] introduced hybrid sampling with a deep hierarchical network, which is particularly relevant to the task of the class-imbalance problem that is prevalent in IDS datasets. Su et al. [82] created the BAT framework, which combines BiLSTM with an attention mechanism to capture sequential dependencies in network traffic more effectively. A deep-learning IDS with data visualization was introduced by Toldinas et al. [83], and a CNN-based model was suggested by Wu et al. [84] to detect intrusion in large networks. This work was further extended by Binbusayyis and Vaiyapuri [85] who used a convolutional autoencoder with a one-class support vector machine (SVM) to offer an unsupervised intrusion detection system that can be used with weakly labelled or never seen attacks. On the whole, these studies enhanced representation learning and classification performance, but most of them rely on large training sets, equal distributions of data, or computationally expensive training processes.

A second body of research is concerned with feature selection and feature representation reduction, which is still necessary since IDS data is usually noisy, redundant, and high-dimensional. An efficient feature reduction can be used to enhance efficiency as well as generalization by eliminating irrelevant attributes before classification. Li et al. [92] discussed the problem of anomaly detection through adaptive feature selection with deep sparse autoencoders, and demonstrated that small learned representations can enhance anomaly discrimination. Dwivedi et al. [93] used the Grasshopper Optimization Algorithm (GOA) in detecting anomalies that are based on the anomaly and demonstrated that the metaheuristic-driven optimization can enhance the quality of features and detection. Even though Nazir et al. [88] concentrated on Android malware detection as opposed to network intrusion detection, its wrapper-based feature-selection model is also methodologically applicable since it demonstrates how search-based selection can enhance cybersecurity classifiers in general. In comparison to purely end-to-end deep architectures, this

body of literature puts more of a focus on dimensionality control and preprocessing quality as the key performance drivers.

The third direction is the metaheuristic and bio-inspired hybrid models, which are the most relevant in the current survey. Sharma and Sahay [86] suggested a bio-inspired intrusion detection method and demonstrated that biologically inspired search can enhance the performance of the IDS. Jiang et al. [87] proposed the PSO-XGBoost, whereby the XGBoost is optimized by particle swarm optimization; their findings indicated that the model performed better than the comparison models, especially better on minority attack classes. Moghanian and Meybodi [89] suggested a hybrid PSO-GA that uses Naive Bayes, which demonstrates that the search diversity and quality of feature selection can be enhanced by using a hybrid optimizer, compared to a single optimizer. Pingale et al. [90] also applied a hybrid optimization framework to the IDS enhancement, which supports the tendency to integrate search mechanisms. Almomani [91] suggested a wider bio-inspired hybrid model, combining several metaheuristic algorithms, such as PSO, Multiverse Optimizer (MVO), Grey Wolf Optimizer (GWO), Moth-Flame Optimization (MFO), and Firefly Algorithm (FFA), to enhance network intrusion detection by optimizing feature selection and classification. These hybrid frameworks are more explicitly optimization-oriented, and more in line with the feature-selection and parameter-tuning problems that are the focus of this survey; but they also have the disadvantage of being more complex in algorithm and more challenging to tune the parameters.

A more recent direction of optimization is the Horse Herd Optimization Algorithm (HOA) and its variations. HOA is created to trade off exploration and exploitation in high dimensional search space and has demonstrated encouraging results in classification-based optimization problems. The works that you refer to as HOA in spam detection [94] and optimized deep-learning prediction in medical imaging [95] would, however, be viewed as evidence of the increased search power of the optimizer, but not as direct proof of network intrusion detection. This difference is significant in a review article, since the successful performance in other areas does not necessarily mean the same performance in the tasks of IDS. Therefore, the value of HOA in intrusion detection is yet to be determined, but it seems to be promising that it can be determined by direct comparison with the established IDS-oriented metaheuristics.

On the whole, there is an evident development of literature. Initial research was on the construction of classifiers and feature representation; subsequent research on dimensionality reduction, imbalance management, and anomaly-directed learning; and more recent research has been more and more using ML or DL models with metaheuristic optimization. However, the literature is still disjointed. Numerous papers have strong findings on single datasets, but comparatively few have systematic comparisons on the measures of detection accuracy, false alarm rate, computational cost, and robustness. This gap is the reason why the current survey has a narrower scope and is specifically interested in finding out the role of metaheuristic optimization in machine learning-based cyber-attack detection, and in which circumstances such methods are the most effective.

**Table 2. Summary of Networking and Intrusion Detection Systems, Their Features, and Applications**

| Category | Approach/ Reference | Main Contribution | Strengths | Limitations/ Comparative Insight |
|---|---|---|---|---|
| Networking | Security in network design [74] | Highlights the importance of integrating security into the software development lifecycle | Reduces vulnerabilities at early stages | Conceptual contribution; not directly applicable to IDS modeling |
| | ML/DL-based IDS review [73] | Provides an overview of machine learning and deep learning techniques for intrusion detection | Broad coverage of IDS approaches | Lacks detailed algorithm-level comparison |
| | Feature selection methods [75] | Explains the role of feature selection in high-dimensional classification | Strong theoretical foundation for preprocessing | General-purpose; not specific to IDS |

| | | | | |
|---|---|---|---|---|
| Intrusion Detection System | ML/DL-based IDS survey [77] | Reviews ML and DL methods for network intrusion detection | Provides a structured overview of IDS evolution | Limited focus on optimization techniques |
| | Feature generation with visualization [78] | Improves intrusion detection by enhancing feature representation using visualization strategies | Enhances class separability | Does not directly address optimization or scalability |
| | Stacking dilated convolutional autoencoders [79] | Learns hierarchical feature representations for intrusion detection | Effective unsupervised feature learning | Limited focus on feature selection or optimization |
| | CNN-based packet classification [80] | Applies CNNs to classify network traffic packets | Strong local feature extraction capability | Performance depends on dataset quality |
| | Hybrid sampling + deep hierarchical network [81] | Addresses class imbalance and improves feature learning | Effective on imbalanced datasets | Increased model complexity |
| | BAT (BiLSTM + attention) [82] | Captures temporal dependencies in network traffic | Strong sequence modeling capability | High computational cost |
| | Deep learning + visualization [83] | Combines deep learning with data visualization for IDS | Improves interpretability and feature representation | Additional preprocessing overhead |
| | CNN-based large-scale IDS [84] | Targets scalable intrusion detection for large datasets | Suitable for high-volume network traffic | Limited temporal modeling capability |
| | CAE + one-class SVM [85] | Provides an unsupervised intrusion detection framework | Effective for unknown attacks | Sensitive to feature representation quality |
| Feature Selection & Optimization | Wrapper-based feature selection (Android malware) [88] | Demonstrates search-based feature selection in cybersecurity | Improves classification performance | Not directly applied to network IDS |
| | Adaptive feature selection + deep autoencoders [92] | Learns compact representations for anomaly detection | Reduces dimensionality effectively | Limited IDS-specific evaluation |
| | GOA-based anomaly detection [93] | Uses the Grasshopper Optimization Algorithm for IDS | Improves feature selection and detection performance | Performance is dependent on the dataset characteristics |
| Metaheuristic & Hybrid IDS | Bio-inspired IDS model [86] | Applies bio-inspired optimization to intrusion detection | Enhances detection performance | Limited comparative benchmarking |
| | PSO-XGBoost model [87] | Uses PSO to optimize XGBoost for intrusion detection | Improves detection accuracy, especially for minority attacks | Requires careful parameter tuning |
| | PSO-GA + Naive Bayes [89] | Hybrid optimization for feature selection and classification | Improves search diversity and accuracy | Increased computational complexity |
| | Hybrid optimization IDS [90] | Combines optimization techniques for IDS improvement | Enhances detection efficiency | Model tuning complexity |
| | Bio-inspired hybrid metaheuristic model [91] | Integrates multiple optimizers (PSO, GWO, MFO, etc.) | Strong optimization capability | Reduced interpretability and higher complexity |
| Transferable Optimization Methods | HOA for spam detection [94] | Applies Horse Herd Optimization for classification tasks | Demonstrates strong search capability | Not validated on IDS datasets |
| | Optimized deep learning (medical domain) [95] | Uses optimization for prediction improvement | Shows general applicability of optimization | Not cybersecurity-specific |

## 3. CHALLENGES AND FUTURE WORK

Although the metaheuristic optimization has shown promising results in the detection of cyber-attacks based on machine learning, there are still several critical issues. These are not all the challenges that are pressing. According to the analyzed literature, scalability, ability to adapt to emerging threats, cost of computation, interpretability, resistance to adversarial attacks, and standardized evaluation are the most problematic areas.

Scalability is the first and most important challenge. Most of the metaheuristic approaches reviewed, such as swarm-based and hybrid optimization frameworks, are effective on benchmark datasets but have challenges when used in large-scale, high-dimensional, and real-time intrusion detection environments. With the increase in the volume and complexity of network traffic, optimization algorithms need to be able to process data efficiently without compromising detection accuracy. This is especially true of the methods based on iterative population-based search, as their computational cost is proportional to the size of the dataset and the number of features.

The second significant issue is adjustment to the changing cyber threats. The available optimization-based intrusion detection models are also designed and experimented with in relatively fixed conditions, but the real-world attacks are always changing in nature and behavior. The PSO-based, GOA-based, and other hybrid optimization models can be used to enhance feature selection and classifier tuning, yet they might still need retraining or re-optimization when the patterns of attacks vary. This reduces their responsiveness in dynamic environments. Future studies should then center on adaptive and self updating optimization frameworks capable of being more receptive to concept drift and novel attack vectors.

The third challenge is the complexity of the computation especially in hybrid and multi-objective models. Although hybrid metaheuristic approaches are likely to increase the detection accuracy, they also increase the complexity of algorithms, the training time, and parameter tuning. This issue is even more critical in real-time systems, where there is a need to make decisions as quickly as possible. In this regard, the next research should be aimed at the lightweight optimization strategies that will maintain the quality of detection and decrease the execution time and resource usage.

Another important issue is interpretability. Most of the reviewed techniques integrate machine learning models with metaheuristic optimization, yet the systems that are obtained are typically black boxes. This is particularly an issue in cybersecurity, where the analysts must be aware of why a sample is considered malicious and what characteristics affect the final decision. Even correct models can be opposed to practical implementation without interpretability. Future research should then explore explainable optimization-based IDS systems that offer clear feature importance, decision making and model behavior.

Stability to adversarial attacks is also a very important issue. The IDSs that utilize machine learning are susceptible to minor changes in the input data, which can cause misclassification or evasion. Even though feature selection and model tuning can be optimized, it does not necessarily imply that the model will be resistant to adversarial manipulation. This issue is directly connected with the shortcomings of the existing reviewed techniques, which are usually optimized to be accurate and not security-robust. Future studies ought to come up with adversarial robust metaheuristic models that expressly consider attack-conscious optimization goals.

The second issue is related to deployment in resource-constrained systems, including edge devices, Internet of Things (IoT), and distributed monitoring platforms. Most of the optimization methods that have been reviewed have been tested in traditional computing platforms and might not be directly applicable to low-power or latency-sensitive platforms. To be adopted practically, the energy-aware and resource-aware

optimization mechanisms should be included in future approaches. This is especially critical to the current cybersecurity systems, which are based on distributed and edge-based detection.

The other weakness is the fact that it is hard to integrate with the existing security infrastructures. Although the optimization-based IDS models can perform well in the laboratory, their implementation to the real world could still be challenging due to compatibility, maintenance cost, and the complexity of integrating them with the current network defense systems. Future work should then focus on implementation-oriented research, including modular architectures and interoperable optimization pipelines, which can be more easily tailored to real systems.

Lastly, the sector does not have standard benchmarking and evaluation procedures. Research papers under review often use different datasets, performance metrics, preprocessing pipelines and experimental settings and, therefore, it is not easy to directly compare them. As a result, it is not always clear that reported improvements are as a result of the optimization technique, or as a result of the variations in the evaluation configuration. The establishment of standardized benchmark infrastructures, universal measures of evaluation, and reproducible experimental protocols then should be considered a high-priority line of research.

According to these challenges, some future directions can be given priority. The most pressing requirement in the short-term is scalable and adaptive optimization frameworks, which can be used on large and dynamic intrusion datasets. Medium term Research should be done on computationally efficient, explainable, and adversarially robust models that can be applied in the real world. Over the long-term, metaheuristic optimization coupled with federated learning, edge intelligence, and standardized benchmarking frameworks can be very useful in enhancing the feasibility, privacy-consciousness, and comparability of intrusion detection systems.

Overall, metaheuristic optimization is a potentially effective way to enhance cyber-attack detection, although its practical effect will be determined by the effectiveness of future research on the elimination of these methodological and deployment-related constraints.

## 4. CONCLUSIONS

In this paper, the metaheuristic optimization methods in machine learning-based cyber-attack detection were thoroughly reviewed with special attention to their application in the selection of features, optimization of models, and improvement of performance. In contrast to traditional surveys where algorithms are mostly enumerated, this work presented a systematic study of metaheuristic types, such as evolutionary algorithms, swarm intelligence techniques, physics-inspired techniques and human-inspired techniques and discussed their applicability to intrusion detection systems. Moreover, the paper has differentiated between single-objective and multi-objective optimization models and explained how they are used in managing various intrusion detection needs. The main contribution of this survey is its comparative and application-based approach. The paper has identified the role of metaheuristic techniques in different phases of intrusion detection by categorizing the available literature into deep learning models, feature-selection techniques, and hybrid optimization frameworks. Specifically, it demonstrated that deep learning methods are more effective in representation learning, whereas metaheuristic algorithms are more effective in feature subset optimization, model parameter optimization, and trade-off optimization of competing goals, such as detection accuracy and false alarm rate. This difference gives a better insight into the application of metaheuristic optimization in cyber-attack detection systems, and when and how. It was

also found during the analysis that hybrid frameworks are one of the most promising paths towards the enhancement of the IDS performance. Practically, these frameworks are a combination of metaheuristic algorithms and machine learning or deep learning models. As an example, one can apply optimization methods like Particle Swarm Optimization (PSO) or Genetic Algorithms (GA) to select the best feature subsets to be used in training classifiers such as the Random Forest or XGBoost, thus dimensionality reduction and accuracy can be enhanced. Similarly, multi-objective optimization methods can be used in conjunction with deep learning models to minimize false alarms and optimize detection rates simultaneously. These practical arrangements show the way in which the hybrid models go beyond the theoretical improvements to the real implementation.

The alternative method of significance is development of explainable and interpretable models. The interpretability of the context of cyber-attack detection can be achieved by combining metaheuristic feature selection with the explainable AI techniques, e.g., ranking the feature importance or extracting the rule. Using smaller sets of important features and the aid of optimization methods, high performance and transparency can be achieved by applying interpretable classifiers (e.g., a decision tree or rule-based systems) as an example. This is necessary in the real world application where security analysts need to be in a position to understand the decision to make a detection. Moreover, real-time and scalable optimization models that can process large and dynamic network data are of interest to future research. This involves the incorporation of metaheuristic optimization and streaming data processing, edge computing, and a federated learning environment to enhance distributed and privacy preserving intrusion detection. The development of lightweight and adaptive optimization strategies will be significant to ensure that the IDS models are applicable in the real-world conditions. Lastly, the research suggests that one should have integrated assessment systems that would allow them to make similar comparisons between various optimization approaches. One of the weaknesses of the field is the inability to standardize datasets, measures and experimental designs. Standardized criteria and uniform assessment processes will need to be developed to foster research and identify the real effective practices. In conclusion, it is possible to state that the metaheuristic optimization techniques can be highly beneficial in enhancing machine learning-driven cyber-attack detection systems. They form a potent tool in the existing cybersecurity due to their ability to efficiently search complex search spaces and maximise the numerous characteristics of IDS models. In future research the current problems can be resolved by enhancing the efficiency and reliability of intrusion detection systems in more complex digital contexts by resolving the existing problems and moving to hybrid, interpretable and scalable solutions.

## REFERENCES

[1] M. A. Matin and M. M. Islam, “Overview of wireless sensor network,” in *Wireless Sensor Networks: Technology and Protocols*. Rijeka, Croatia: InTech, 2012. doi: https://doi.org/10.5772/49376

[2] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “A survey on sensor networks,” *IEEE Commun. Mag.*, vol. 40, no. 8, pp. 102–114, 2002. doi: https://doi.org/10.1109/MCOM.2002.1024422

[3] A. Sangwan and R. P. Singh, “Survey on coverage problems in wireless sensor networks,” *Wireless Pers. Commun.*, vol. 80, no. 4, pp. 1475–1500, 2015. doi: https://doi.org/10.1007/s11277-014-2092-3

[4] M. Rudafshani and S. Datta, “Localization in wireless sensor networks,” in *Proc. 6th Int. Symp. Inf. Process. Sensor Netw. (IPSN)*, 2007, pp. 51–60. doi: https://doi.org/10.1145/1236360.1236370

[5] E. H. Houssein, M. R. Saad, K. Hussain, W. Zhu, H. Shaban, and M. Hassaballah, “Optimal sink node placement in large scale wireless sensor networks based on Harris’ hawk optimization algorithm,” *IEEE Access*, vol. 8, pp. 19381–19397, 2020. doi: https://doi.org/10.1109/ACCESS.2020.2968740

[6] Z. Rezaei and S. Mobininejad, "Energy saving in wireless sensor networks," *Int. J. Comput. Sci. Eng. Surv.*, vol. 3, no. 1, pp. 23–37, 2012. doi: https://doi.org/10.5121/ijcses.2012.3103

[7] P. Subramanian, J. M. Sahayaraj, S. Senthilkumar, and D. S. Alex, "A hybrid grey wolf and crow search optimization algorithm-based optimal cluster head selection scheme for wireless sensor networks," *Wireless Pers. Commun.*, vol. 113, no. 2, pp. 905–925, 2020. doi: https://doi.org/10.1007/s11277-020-07318-7

[8] V. Prakash, D. Singh, S. Pandey, S. Singh, and P. K. Singh, "Energy-optimization route and cluster head selection using M-PSO and GA in wireless sensor networks," *Wireless Pers. Commun.*, 2024, pp. 1–26.

[9] J. C. Spall, *Introduction to Stochastic Search and Optimization: Estimation, Simulation, and Control*. Hoboken, NJ, USA: Wiley, 2005. doi: https://doi.org/10.1002/0471722138

[10] K. Zielinski and R. Laur, "Constrained single-objective optimization using differential evolution," in *Proc. IEEE Int. Conf. Evol. Comput. (CEC)*, 2006, pp. 223–230. doi: https://doi.org/10.1109/CEC.2006.1688280

[11] R. Bowerman, B. Hall, and P. Calamai, "A multi-objective optimization approach to urban school bus routing: Formulation and solution method," *Transp. Res. Part A Policy Pract.*, vol. 29, no. 2, pp. 107–123, 1995. doi: https://doi.org/10.1016/0965-8564(94)00029-P

[12] D. Simon, *Evolutionary Optimization Algorithms*. Hoboken, NJ, USA: Wiley, 2013. doi: https://doi.org/10.1002/9781118659502

[13] E. H. Houssein, M. R. Saad, K. Hussain, H. Shaban, and M. Hassaballah, "A review of metaheuristic optimization algorithms in wireless sensor networks," in *Metaheuristics in Machine Learning: Theory and Applications*. Cham, Switzerland: Springer, 2021, pp. 193–217. doi: https://doi.org/10.1007/978-3-030-70542-0_9

[14] M. Iqbal, M. Naeem, A. Anpalagan, N. N. Qadri, and M. Imran, "Multi-objective optimization in sensor networks: Optimization classification, applications and solution approaches," *Comput. Netw.*, vol. 99, pp. 134–161, 2016. doi: https://doi.org/10.1016/j.comnet.2016.02.015

[15] L. Abualigah and A. Diabat, "Advances in sine cosine algorithm: A comprehensive survey," *Artif. Intell. Rev.*, vol. 54, pp. 2567–2608, 2021. doi: https://doi.org/10.1007/s10462-020-09849-7

[16] L. Abualigah and A. Diabat, "A comprehensive survey of the grasshopper optimization algorithm: Results, variants, and applications," *Neural Comput. Appl.*, vol. 32, pp. 15533–15556, 2020. doi: https://doi.org/10.1007/s00521-019-04166-9

[17] O. A. Alomari, A. Diabat, and Z. W. Geem, "A comprehensive survey of the harmony search algorithm in clustering applications," *Appl. Sci.*, vol. 10, no. 11, Art. no. 3827, 2020. doi: https://doi.org/10.3390/app10113827

[18] L. Abualigah, "Group search optimizer: A nature-inspired metaheuristic optimization algorithm with its results, variants, and applications," *Neural Comput. Appl.*, vol. 32, pp. 2949–2972, 2020. doi: https://doi.org/10.1007/s00521-019-04177-6

[19] L. Abualigah, "Multi-verse optimizer algorithm: A comprehensive survey of its results, variants, and applications," *Neural Comput. Appl.*, vol. 32, pp. 12381–12402, 2020. doi: https://doi.org/10.1007/s00521-019-04404-0

[20] L. Abualigah, A. Diabat, S. Mirjalili, M. Abd Elaziz, and A. H. Gandomi, "The arithmetic optimization algorithm," *Comput. Methods Appl. Mech. Eng.*, vol. 376, Art. no. 113609, 2021. doi: https://doi.org/10.1016/j.cma.2020.113609

[21] Y. Xin, L. Yong, and L. Guangming, "Evolutionary programming made faster," *IEEE Trans. Evol. Comput.*, vol. 3, no. 2, pp. 82–102, 1999.

[22] J. H. Holland, *Adaptation in Natural and Artificial Systems*. Ann Arbor, MI, USA: Univ. of Michigan Press, 1975.

[23] D. E. Goldberg and J. H. Holland, "Genetic algorithms and machine learning," *Mach. Learn.*, vol. 3, no. 2, pp. 95–99, 1988.
[24] Z. Michalewicz, *Genetic Algorithms + Data Structures = Evolution Programs*, 3rd ed. Berlin, Germany: Springer, 1996.
[25] R. Storn and K. Price, "Differential evolution: A simple and efficient heuristic for global optimization over continuous spaces," *J. Global Optim.*, vol. 11, no. 4, pp. 341–359, 1997. doi: https://doi.org/10.1023/A:1008202821328
[26] J. R. Koza, "Genetic programming as a means for programming computers by natural selection," *Stat. Comput.*, vol. 4, no. 2, pp. 87–112, 1994.
[27] R. Eberhart and J. Kennedy, "A new optimizer using particle swarm theory," in *Proc. 6th Int. Symp. Micro Mach. Human Sci. (MHS)*, 1995, pp. 39–43. doi: https://doi.org/10.1109/MHS.1995.494215
[28] S. Mirjalili, A. H. Gandomi, S. Z. Mirjalili, S. Saremi, H. Faris, and S. M. Mirjalili, "Salp swarm algorithm: A bio-inspired optimizer for engineering design problems," *Adv. Eng. Softw.*, vol. 114, pp. 163–191, 2017. doi: https://doi.org/10.1016/j.advengsoft.2017.07.002
[29] A. Faramarzi, M. Heidarinejad, S. Mirjalili, and A. H. Gandomi, "Marine predators algorithm: A nature-inspired metaheuristic," *Expert Syst. Appl.*, vol. 152, Art. no. 113377, 2020. doi: https://doi.org/10.1016/j.eswa.2020.113377
[30] S. Mirjalili and A. Lewis, "The whale optimization algorithm," *Adv. Eng. Softw.*, vol. 95, pp. 51–67, 2016. doi: https://doi.org/10.1016/j.advengsoft.2016.01.008
[31] H. Eskandar, A. Sadollah, A. Bahreininejad, and M. Hamdi, "Water cycle algorithm: A novel metaheuristic optimization method for solving constrained engineering optimization problems," *Comput. Struct.*, vols. 110–111, pp. 151–166, 2012. doi: https://doi.org/10.1016/j.compstruc.2012.07.010
[32] K. Tamura and K. Yasuda, "Primary study of spiral dynamics inspired optimization," *IEEJ Trans. Electr. Electron. Eng.*, vol. 6, no. s1, pp. S98–S100, 2011. doi: https://doi.org/10.1002/tee.20684
[33] Z. Bayraktar, M. Komurcu, J. A. Bossard, and D. H. Werner, "The wind driven optimization technique and its application in electromagnetics," *IEEE Trans. Antennas Propag.*, [UNVERIFIED / POSSIBLY INCORRECT from original conference citation].
[34] A. Kaveh, *Advances in Metaheuristic Algorithms for Optimal Design of Structures*. Cham, Switzerland: Springer International Publishing, 2014. doi: 10.1007/978-3-319-05527-4
[35] B. S. İlker and F. Shu-Cherng, "An electromagnetism-like mechanism for global optimization," *J. Global Optim.*, vol. 25, no. 3, pp. 263–282, 2003. doi: https://doi.org/10.1023/A:1022452626305
[36] A. Kaveh and S. Talatahari, "A novel heuristic optimization method: Charged system search," *Acta Mech.*, vol. 213, nos. 3–4, pp. 267–289, 2010. doi: https://doi.org/10.1007/s00707-009-0270-4
[37] S. Kirkpatrick, C. D. Gelatt, and M. P. Vecchi, "Optimization by simulated annealing," *Science*, vol. 220, no. 4598, pp. 671–680, 1983. doi: https://doi.org/10.1126/science.220.4598.671
[38] E. Rashedi, H. Nezamabadi-pour, and S. Saryazdi, "GSA: A gravitational search algorithm," *Inf. Sci.*, vol. 179, no. 13, pp. 2232–2248, 2009. doi: https://doi.org/10.1016/j.ins.2009.03.004
[39] L. Abualigah, D. Yousri, M. Abd Elaziz, A. A. Ewees, M. A. Al-qaness, and A. H. Gandomi, "Aquila optimizer: A novel metaheuristic optimization algorithm," *Comput. Ind. Eng.*, vol. 157, Art. no. 107250, 2021. doi: https://doi.org/10.1016/j.cie.2021.107250
[40] A. H. Kashan, "A new metaheuristic for optimization: Optics inspired optimization (OIO)," *Comput. Oper. Res.*, vol. 55, pp. 99–125, 2015. doi: https://doi.org/10.1016/j.cor.2014.10.011
[41] A. Y. S. Lam and V. O. K. Li, "Chemical-reaction-inspired metaheuristic for optimization," *IEEE Trans. Evol. Comput.*, vol. 14, no. 3, pp. 381–399, 2010. doi: https://doi.org/10.1109/TEVC.2009.2033580

[42] L. Abualigah, M. Shehab, M. Alshinwan, S. Mirjalili, and M. A. Abd Elaziz, "Ant lion optimizer: A comprehensive survey of its variants and applications," *Archives of Computational Methods in Engineering*, vol. 28, no. 3, pp. 1397–1416, 2021. doi: 10.1007/s11831-020-09441-7
[43] V. R. Rao, V. J. Savsani, and D. P. Vakharia, "Teaching-learning-based optimization: A novel method for constrained mechanical design optimization problems," *Comput.-Aided Des.*, vol. 43, no. 3, pp. 303–315, 2011. doi: https://doi.org/10.1016/j.cad.2010.12.015
[44] M. Reza and S. Khodakaram, "Volleyball premier league algorithm," *Appl. Soft Comput.*, vol. 64, pp. 161–185, 2018. doi: https://doi.org/10.1016/j.asoc.2017.12.043
[45] C. Dai, Y. Zhu, and W. Chen, "Seeker optimization algorithm," in *Computational and Information Science*, Berlin, Germany: Springer, 2006, pp. 167–176. doi: https://doi.org/10.1007/11805828_19
[46] N. Moosavian and B. Kasaee Roodsari, "Soccer league competition algorithm: A novel meta-heuristic algorithm for optimal design of water distribution networks," *Swarm Evol. Comput.*, vol. 17, pp. 14–24, 2014. doi: https://doi.org/10.1016/j.swevo.2014.04.005
[47] A. H. Kashan, "League championship algorithm: A new algorithm for numerical function optimization," in *Proc. Int. Conf. Soft Comput. Pattern Recognit.*, 2009, pp. 43–48. doi: https://doi.org/10.1109/SoCPaR.2009.16
[48] A. Sadollah, H. Sayyaadi, and A. Yadav, "A dynamic metaheuristic optimization model inspired by biological nervous systems: Neural network algorithm," *Appl. Soft Comput.*, vol. 71, pp. 747–782, 2018. doi: https://doi.org/10.1016/j.asoc.2018.07.039
[49] A. Yadav, "AEFA: Artificial electric field algorithm for global optimization," *Swarm Evol. Comput.*, vol. 48, pp. 93–108, 2019. doi: https://doi.org/10.1016/j.swevo.2019.03.013
[50] G. Dhiman and V. Kumar, "Seagull optimization algorithm: Theory and its applications for large-scale industrial engineering problems," *Knowl.-Based Syst.*, vol. 165, pp. 169–196, 2019. doi: https://doi.org/10.1016/j.knosys.2018.11.024
[51] W. Zhao, L. Wang, and Z. Zhang, "Artificial ecosystem-based optimization: A novel nature-inspired meta-heuristic algorithm," *Neural Comput. Appl.*, vol. 32, no. 13, pp. 9383–9425, 2020. doi: https://doi.org/10.1007/s00521-019-04452-6
[52] B. Abdollahzadeh, F. S. Gharehchopogh, and S. Mirjalili, "Artificial gorilla troops optimizer: A new nature-inspired metaheuristic algorithm for global optimization problems," *Int. J. Intell. Syst.*, vol. 36, no. 10, pp. 5887–5958, 2021. doi: https://doi.org/10.1002/int.22535
[53] Y. Jiang, W. Qing, S. Zhu, and L. Zhang, "Orca predation algorithm: A novel bio-inspired algorithm for global optimization problems," *Expert Syst. Appl.*, vol. 188, Art. no. 116026, 2022. doi: https://doi.org/10.1016/j.eswa.2021.116026
[54] Y. Yang, H. Chen, A. A. Heidari, and A. H. Gandomi, "Hunger games search: Visions, conception, implementation, deep analysis, perspectives, and towards performance shifts," *Expert Syst. Appl.*, vol. 177, Art. no. 114864, 2021. doi: https://doi.org/10.1016/j.eswa.2021.114864
[55] K. Zervoudakis and S. Tsafarakis, "A mayfly optimization algorithm," *Comput. Ind. Eng.*, vol. 145, Art. no. 106559, 2020. doi: https://doi.org/10.1016/j.cie.2020.106559
[56] A. Shabani, B. Asgarian, M. A. Salido, and S. A. Gharebaghi, "Search and rescue optimization algorithm: A new optimization method for solving constrained engineering optimization problems," *Expert Syst. Appl.*, vol. 161, Art. no. 113698, 2020. doi: https://doi.org/10.1016/j.eswa.2020.113698
[57] M. Ghasemi, I. F. Davoudkhani, E. Akbari, A. Rahimnejad, S. Ghavidel, and L. Li, "A novel and effective optimization algorithm for global optimization and its engineering applications: Turbulent flow of water-based optimization (TFWO)," *Eng. Appl. Artif. Intell.*, vol. 92, Art. no. 103666, 2020. doi: https://doi.org/10.1016/j.engappai.2020.103666

[58] R. Akbari, R. Hedayatzadeh, K. Ziarati, and B. Hassanizadeh, "A multi-objective artificial bee colony algorithm," *Swarm Evol. Comput.*, vol. 2, no. 1, pp. 39–52, 2012. doi: https://doi.org/10.1016/j.swevo.2011.08.001

[59] R. Shang, W. Zhang, F. Li, L. Jiao, and R. Stolkin, "Multi-objective artificial immune algorithm for fuzzy clustering based on multiple kernels," *Swarm Evol. Comput.*, vol. 50, Art. no. 100485, 2019. doi: https://doi.org/10.1016/j.swevo.2019.100485

[60] A. Sadollah, H. Eskandar, and J. H. Kim, "Water cycle algorithm for solving constrained multi-objective optimization problems," *Appl. Soft Comput.*, vol. 27, pp. 279–298, 2015. doi: https://doi.org/10.1016/j.asoc.2014.11.046

[61] G. Dhiman and V. Kumar, "Multi-objective spotted hyena optimizer: A multi-objective optimization algorithm for engineering problems," *Knowl.-Based Syst.*, vol. 150, pp. 175–197, 2018. doi: https://doi.org/10.1016/j.knosys.2018.03.008

[62] S. Z. Mirjalili, S. Mirjalili, S. Saremi, H. Faris, and I. Aljarah, "Grasshopper optimization algorithm for multi-objective optimization problems," *Appl. Intell.*, vol. 48, no. 4, pp. 805–820, 2018. doi: https://doi.org/10.1007/s10489-017-1019-7

[63] S. Mirjalili, S. Saremi, S. M. Mirjalili, and L. dos S. Coelho, "Multi-objective grey wolf optimizer: A novel algorithm for multi-criterion optimization," *Expert Syst. Appl.*, vol. 47, pp. 106–119, 2016. doi: https://doi.org/10.1016/j.eswa.2015.10.039

[64] E. H. Houssein, M. A. Mahdy, D. Shebl, A. Manzoor, R. Sarkar, and W. M. Mohamed, "An efficient slime mould algorithm for solving multi-objective optimization problems," *Expert Syst. Appl.*, vol. 187, Art. no. 115870, 2022. doi: https://doi.org/10.1016/j.eswa.2021.115870

[65] M. A. Tawhid and V. Savsani, "Multi-objective sine-cosine algorithm (MO-SCA) for multi-objective engineering design problems," *Neural Comput. Appl.*, vol. 31, no. 2, pp. 915–929, 2019. doi: https://doi.org/10.1007/s00521-017-2992-8

[66] H. Hemmatian, A. Fereidoon, and E. Assareh, "Optimization of hybrid laminated composites using the multi-objective gravitational search algorithm (MOGSA)," *Eng. Optim.*, vol. 46, no. 9, pp. 1169–1182, 2014. doi: https://doi.org/10.1080/0305215X.2013.831513

[67] I. R. Kumawat, S. J. Nanda, and R. K. Maddila, "Multi-objective whale optimization," in *TENCON 2017 - 2017 IEEE Region 10 Conf.*, 2017, pp. 2747–2752. doi: https://doi.org/10.1109/TENCON.2017.8228310

[68] J. J. Liang, B. Y. Qu, and P. N. Suganthan, "Problem definitions and evaluation criteria for the CEC 2014 special session and competition on single objective real-parameter numerical optimization," Tech. Rep., Zhengzhou Univ. and Nanyang Technological Univ., 2013.

[69] Q. Zhang, A. Zhou, S. Zhao, P. N. Suganthan, W. Liu, and S. Tiwari, "Multiobjective optimization test instances for the CEC 2009 special session and competition," Tech. Rep., Univ. of Essex and Nanyang Technological Univ., 2008.

[70] S. K. Azad, "Monitored convergence curve: A new framework for metaheuristic structural optimization algorithms," *Struct. Multidiscip. Optim.*, vol. 60, no. 2, pp. 481–499, 2019. doi: https://doi.org/10.1007/s00158-019-02231-z

[71] R. Mailler and V. Lesser, "Solving distributed constraint optimization problems using cooperative mediation," in *Proc. 3rd Int. Joint Conf. Auton. Agents Multiagent Syst.*, 2004, pp. 438–445. doi: https://doi.org/10.1109/AAMAS.2004.10070

[72] R. Moghdani, K. Salimifard, E. Demir, and A. Benyettou, "Multi-objective volleyball premier league algorithm," *Knowl.-Based Syst.*, vol. 196, Art. no. 105781, 2020. doi: https://doi.org/10.1016/j.knosys.2020.105781

[73] J. A. Abraham and V. Bindu, "Intrusion detection and prevention in networks using machine learning and deep learning approaches: A review," in *2021 Int. Conf. Advancements in Electrical, Electronics, Communication, Computing and Automation (ICAECA)*, 2021.
[74] N. S. A. Karim, A. Albuolayan, T. Saba, and A. Rehman, "The practice of secure software development in SDLC: An investigation through existing model and a case study," *Security and Communication Networks*, vol. 9, no. 18, pp. 5333–5345, 2016. doi: 10.1002/sec.1708
[75] G. Chandrashekar and F. Sahin, "A survey on feature selection methods," *Comput. Electr. Eng.*, vol. 40, no. 1, pp. 16–28, 2014. doi: https://doi.org/10.1016/j.compeleceng.2013.11.024
[76] P. Wu and H. Guo, "LuNET: A deep neural network for network intrusion detection," in *2019 IEEE Symp. Ser. Comput. Intell. (SSCI)*, 2019, pp. 617–624. doi: https://doi.org/10.1109/SSCI44817.2019.9003126
[77] Z. Ahmad, A. S. Khan, C. W. Shiang, J. Abdullah, and F. Ahmad, "Network intrusion detection system: A systematic study of machine learning and deep learning approaches," *Trans. Emerg. Telecommun. Technol.*, vol. 32, no. 1, Art. no. e4150, 2021. doi: https://doi.org/10.1002/ett.4150
[78] J. Zhang *et al.*, "A novel intrusion detection system based on feature generation with visualization strategy," *Future Gener. Comput. Syst.*, vol. 95, pp. 156–171, 2019. doi: https://doi.org/10.1016/j.future.2018.12.042
[79] S. Yu *et al.*, "Network intrusion detection through stacking dilated convolutional autoencoders," *Secur. Commun. Netw.*, vol. 2020, Art. no. 8820707, 2020.
[80] G. Karatas *et al.*, "Effective packet classification for network intrusion detection using CNN," *IEEE Access*, vol. 8, pp. 64683–64694, 2020. doi: https://doi.org/10.1109/ACCESS.2020.2984761
[81] K. Jiang, L. Wang, Y. Wu, and S. Wang, "Network intrusion detection combined hybrid sampling with deep hierarchical network," *IEEE Access*, vol. 8, pp. 32464–32476, 2020. doi: https://doi.org/10.1109/ACCESS.2020.2973730
[82] T. Su *et al.*, "BAT: Deep learning methods on network intrusion detection using NSL-KDD dataset," *IEEE Access*, vol. 8, pp. 29575–29585, 2020. doi: https://doi.org/10.1109/ACCESS.2020.2972307
[83] J. Toldinas *et al.*, "A novel intrusion detection system based on deep learning and data visualization," *Electronics*, vol. 10, no. 5, Art. no. 556, 2021. doi: https://doi.org/10.3390/electronics10050556
[84] Y. Wu *et al.*, "A novel intrusion detection model for a massive network using convolutional neural networks," *IEEE Access*, vol. 8, pp. 57044–57056, 2020. doi: https://doi.org/10.1109/ACCESS.2020.2981810
[85] A. Binbusayyis and T. Vaiyapuri, "Unsupervised deep learning approach for network intrusion detection combining convolutional autoencoder and one-class SVM," *Appl. Intell.*, vol. 51, no. 10, pp. 7094–7108, 2021. doi: https://doi.org/10.1007/s10489-021-02254-9
[86] S. Sharma and S. K. Sahay, "A bio-inspired approach for intrusion detection," *J. Inf. Secur. Appl.*, vol. 46, pp. 1–11, 2019.
[87] H. Jiang, Z. He, G. Ye, and H. Zhang, "Network intrusion detection based on PSO-XGBoost model," *IEEE Access*, vol. 8, pp. 58392–58401, 2020. doi: https://doi.org/10.1109/ACCESS.2020.2983075
[88] M. Nazir, M. A. Khan, A. Hussain, A. Rehman, and T. Saba, "A wrapper-based feature selection technique for malware detection in Android applications," *Comput. Electr. Eng.*, vol. 89, Art. no. 106903, 2021. doi: https://doi.org/10.1016/j.compeleceng.2020.106903
[89] A. Moghanian and M. R. Meybodi, "A novel intrusion detection system using a hybrid of PSO and GA algorithms with naive Bayes classifier," *J. Ambient Intell. Humaniz. Comput.*, vol. 11, pp. 5581–5597, 2020. doi: https://doi.org/10.1007/s12652-020-01704-6
[90] S. Pingale, S. Patil, and P. Patil, "An efficient intrusion detection system using hybrid optimization algorithm," *J. King Saud Univ. Comput. Inf. Sci.*, 2022.

[91] O. Almomani, "A hybrid model using bio-inspired metaheuristic algorithms for network intrusion detection system," *Comput. Mater. Contin.*, vol. 68, no. 1, pp. 409–429, 2021. doi: https://doi.org/10.32604/cmc.2021.016920

[92] Y. Li, Y. Zhang, S. Wang, and Y. Zhang, "Anomaly detection via adaptive feature selection with deep sparse autoencoders," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 33, no. 3, pp. 1052–1064, 2022. doi: https://doi.org/10.1109/TNNLS.2020.3027734

[93] S. Dwivedi, M. Vardhan, and S. Tripathi, "Building an efficient intrusion detection system using grasshopper optimization algorithm for anomaly detection," *Cluster Comput.*, 2021.

[94] A. Hosseinalipour and R. Ghanbarzadeh, "A novel approach for spam detection using horse herd optimization algorithm," *Neural Comput. Appl.*, vol. 34, no. 15, pp. 13091–13105, 2022. doi: https://doi.org/10.1007/s00521-021-06849-2

[95] M. Rajeshwari, C. N. Kumar, and K. S. Kumar, "Skin cancer severity prediction using optimized deep learning model," *J. Ambient Intell. Humaniz. Comput.*, vol. 13, pp. 1–12, 2022.