A Systematic Review of Metaheuristics-Based and Machine Learning-Driven Intrusion Detection Systems in IoT

Mohammad Shamim Ahsan[1], Salekul Islam[2] and Swakkhar Shatabda[3*]
[1]Department of Computer Science and Engineering,
Bangladesh University of Engineering and Technology
[2]Department of Electrical and Computer Engineering, North South University
[3]Department of Computer Science and Engineering, BRAC University

This paper has been published in Swarm and Evolutionary Computation, available at https://doi.org/10.1016/j.swevo.2025.101984

Abstract

The widespread adoption of the Internet of Things (IoT) has raised a new challenge for developers since it is prone to known and unknown cyberattacks due to its heterogeneity, flexibility, and close connectivity. To defend against such security breaches, researchers have focused on building sophisticated intrusion detection systems (IDSs) using machine learning (ML) techniques. Although these algorithms notably improve detection performance, they require excessive computing power and resources, which are crucial issues in IoT networks considering the recent trends of decentralized data processing and computing systems. Consequently, many optimization techniques have been incorporated with these ML models. Specifically, a special category of optimizer adopted from the behavior of living creatures and different aspects of natural phenomena, known as metaheuristic algorithms, has been a central focus in recent years and brought about remarkable results. Considering this vital significance, we present a comprehensive and systematic review of various applications of metaheuristics algorithms in developing a machine learning-based IDS, especially for IoT. A significant contribution of this study is the discovery of hidden correlations between these optimization techniques and machine learning models integrated with state-of-the-art IoT-IDSs. In addition, the effectiveness of these metaheuristic algorithms in different applications, such as feature selection, parameter or hyperparameter tuning, and hybrid usages are separately analyzed. Moreover, a taxonomy of existing IoT-IDSs is proposed. Furthermore, we investigate several critical issues related to such integration. Our extensive exploration ends with a discussion of

*Correspondance:swakkhar.shatabda@bracu.ac.bd

promising optimization algorithms and technologies that can enhance the efficiency of IoT-IDSs.

Keywords: Internet of Things (IoT), Intrusion Detection Systems (IDS), Machine Learning (ML), Deep Learning (DL), Metaheuristic Algorithms, Cybersecurity, Optimization Techniques.

1 Introduction

The popularity of the Internet of Things devices has spread surprisingly in the last few years. Nowadays, it offers a scalable platform not only for industry, healthcare, and home applications but also for agriculture, vehicular settings, and ultra-sophisticated systems like drone technologies [1]. Alarmingly, this widespread adoption leads to unavoidable security issues as a negative side effect of close connectivity. Transferring susceptible information, such as personal data, patient data, and private business analysis makes such effects more severe and unimaginable. For example, millions of IoT and embedded devices (e.g., DVDs, printers, and IP cameras) were infected by a botnet in 2016, widely known as *Mirai botnet*[2]. Notably, the attack was spread to several nations and manufacturing organizations and affected around 65 thousand IoT devices within the first 20 hours. Another concerning incident occurred in 2020, where an ADT employee pled guilty to accessing the security cameras of 220 women over 9,600 times during four years [3]. The defendant routinely added his email address to customers' "ADT Pulse" accounts and got real-time access to the video feeds from their homes for sexual gratification. In such cases, an IoT-IDS can be used to detect and report on unique visitors, unauthorized access, and malicious activities.

Intrusion detection is one of the most crucial aspects of IoT security. An IDS typically identifies diverse attacks based on predefined rules or specific deviations from normal behavioral patterns. It can identify external and internal attacks on networks or computer systems, surpassing the performance of the traditional firewall. Typically, a firewall works on a set of specific rules, often based on IP addresses, port numbers, and protocols to check which packets are allowed to enter the network. Since firewalls filter packets relying on simple policies, they cannot detect internal or external attacks which require analyzing complex behavioral patterns. On the contrary, an IDS can identify malicious activities by observing the deviations from normal behaviors, which include both simple and complicated patterns. The entire IDS can be divided into two modules: feature engineering (mostly *feature selection*) and *classification* or detection. Feature selection aims to select a set of optimal features, discarding the least significant ones to efficiently and faster the classification process and reduce the computational overhead of the system. Feature selection methods can be categorized into three methods: *filter*, *wrapper*, and *hybrid* methods. In the filter method, all features are statistically examined and rated with the help of data (input and target variables). Then based on the rating, less ranked features or features rated below a specific threshold are eliminated before classification. Information gain and linear correlation coefficient [4] are well-known metrics used in filter methods. The wrapper techniques outperform filter methods by training and testing a machine-learning model using each subset of features, iteratively. Specifically, these methods rank subsets of features based on their prediction accuracy generated from the machine learning algorithms. However, they are more expensive and time-consuming than the filter approaches. Sequential forward selection, sequential backward selection, stepwise selection [5], hill climbing, etc. are popular wrapper methods. Though filter methods are proven simple, fast, and scalable, they consider feature dependencies to a certain extent, resulting in an inappropriate feature set. Besides, wrapper methods offer better feature sets than filters. But, they become much slower and computationally expensive for a large number of features [6].

A group of wrapper methods fall into the category of optimization-based techniques, known as *metaheuristics algorithms* that overcome the drawbacks of the prior methods. A metaheuristic is a general exploration method that applies to optimize an underlying heuristic. In the case of feature selection in ML, the optimal subset of features is searched in the feature space based on some heuristic or performance measure. Generally, a metaheuristic algorithm consists of two phases: exploitation and exploration. In the exploitation or intensification phase, the algorithm explores the neighborhood of an already promising solution in the search space. However, during exploration (a.k.a., diversification), the algorithm tries to traverse the unvisited regions of the search space. Although they do not make any hypothesis on the mathematical properties of the objective function, they gradually develop it through a continuous learning process. Among the major advantages, the utilization of parameters and comparatively faster convergence to the solutions are crucial. In addition, metaheuristics are efficient and effective in obtaining global optimal values, resulting in global optimal features. Moreover, even with large datasets, they perform significantly well [7]. However, metaheuristics are approximate and usually non-deterministic and do not guarantee the optimal (or, best) solution [8] like the exact algorithms (e.g., dynamic programming, branch and bound, branch and cut, linear programming, etc.). Still, they can provide near-optimal solutions in acceptable computing time (but the exact algorithms can not), which is highly essential for complex problems like detecting intrusions in dynamic environments. Interestingly, these techniques are mostly inspired by natural phenomena, including the instincts of living creatures. In addition to filter and wrapper techniques, a hybrid approach is another one that focuses on combining different aspects of existing feature selection methods [9].

Regarding attack or intrusion detection, traditional IDSs like statistical-driven (e.g., payload-based), rule-based, heuristics-based, etc. cannot detect the complex patterns of dynamic IoT systems. On the other hand, classical and deep machine learning models have been proven to generate notable results, even in heterogeneous environments such as IoT. The main purpose of using ML-based techniques is to handle large data sets and produce high accuracy, fast processing, and significant performance; thus enhancing security. However, they require high computational resources and a significant amount of time to achieve minor precision improvements [10]. Despite these improvements offered by machine learning, the era of big data and the increasing use of IoT introduce new problems with traditional centralized cloud-based data storage and processing systems. In particular, low throughput, high latency, and data privacy are the most serious issues [11]. In addition, IoT devices contain sensitive and private data, such as financial or patient information. To address these issues, edge computing technology has become widely accepted, especially in the IoT context. In this technology, data are processed, stored, and computed closer to the location of devices. Consequently, not only the data transmission time, response time, and latency are reduced but also higher scalability and decentralization are achieved. Regarding IDSs, when machine learning models are trained in edge servers with large datasets, the computing power and the adequacy of energy support become crucial challenges since edge servers can hardly meet these requirements [12].

Although researchers always rely on utilizing optimization techniques to mitigate such problems and improve the effectiveness of ML-oriented IoT-IDSs, metaheuristics-based optimization has been a notable focus in recent years. Considering the outstanding facilities offered by these optimizers, they can play a pivotal role in designing IoT-IDSs. Specifically, these algorithms can be utilized not only to select optimal feature sets — before being trained by an ML-based classifier — but also to optimize the parameters (e.g., weights and biases) and hyperparameters (e.g., learning rate, number of neurons, layers volume, and amount of epochs) of the models during training. For these reasons, numerous recent works [13, 14, 15, 16, 17] have employed them to select an optimal set of features; while others have used these techniques to tune parameters [18, 19] and hyperparameters [20, 21, 22] in ML-driven classifiers.

Scope of this Review and Contributions

Among existing related studies, almost all have focused on one aspect: metaheuristics or machine learning techniques; not both. Although very few surveys mention the integration of these two, their coverage and classifications are considerably inadequate. Moreover, in notable cases, the selected works are not IoT-specific. Most importantly, these studies do not analyze the connections of optimization techniques with machine learning algorithms while developing an IoT-IDS. Furthermore, no studies have analyzed the different applications of metaheuristics for such detection systems. To address these gaps in the literature, we analyze a diverse range of metaheuristics, from swarm-based, nature-inspired, and evolutionary algorithms to search-based, human-inspired, physics-based, mathematics-based, and hybrid ones. Regarding machine learning techniques, conventional methods such as classifications, artificial neural networks, and ensemble learning, along with advanced algorithms, for instance, autoencoder, deep belief networks, deep neural networks, recurrent neural networks, convolutional neural networks, etc. are explored. Another significant contribution of this work is the analysis of the various applications of metaheuristics in the IoT IDSs, such as feature selection, parameter optimization, hyperparameter tuning, and their hybrid usage. Moreover, the correlations among metaheuristics, machine learning, and datasets used for the IoT-IDSs are figured out that distinguish this work from others. In summary, the following contributions are made:

- We present an extensive review of the existing applications of metaheuristics algorithms to develop machine learning-based intrusion detection systems, especially for IoT. In addition, a large-scale taxonomy of metaheuristics and ML-integrated IoT-IDSs is introduced.

- Hidden correlations among top-notch metaheuristics, ML techniques, and the most commonly used datasets are analyzed, and some insightful findings are disclosed. Importantly, these results also reflect the effectiveness of such metaheuristic-ML integration considering different applications, especially feature selection, parameter or hyperparameter tuning, and hybrid cases.
- Several crucial challenges that may arise when integrating metaheuristic algorithms with machine learning techniques are outlined. Accordingly, the viability of a few emerging technologies is discussed. Finally, some possible integrations of metaheuristics and ML, and their feasibility in IoT-IDSs are explored.

The remainder of this paper proceeds as follows. Section 2 introduces the background, including the classification of intrusion detection systems, metaheuristics, and machine learning techniques. Section 3 provides the related surveys with their limitations, research gaps analysis, and differentiating aspects of our work. Then, in Section 4, we discuss our research objectives along with search strategy and data assessment. Next, Section 5 introduces the results of the systematic literature review, including the technical and extensive exploration of the existing relevant detection systems and many insightful findings. After that, in Section 6, our overall investigation with possible future challenges are summarized. Finally, Section 7 concludes our work. Along with them, an *Appendix* section at the end of the paper presents a performance tabulation of existing metaheuristics-based and ML-driven IoT-IDSs in tabulation form.

2 Background

In this section, intrusion detection methods, techniques, meta-heuristics, and machine learning-based models are briefly discussed.

2.1 Intrusion Detection Methods and Techniques in IoT

Methods. An intrusion detection system (IDS) is a software or hardware system that detects traces of malicious activities on a computer system or network. Primarily, IDS can be categorized into three types: host-based IDS (HIDS), protocol-based intrusion detection system (PIDS), and network-based IDS (NIDS). In HIDS, the system is dedicated to working for a specific host. As a result, any insider as well as outsider attack is seamlessly detected. The most crucial limitation here is the necessity of one IDS for each host. Regarding PIDS, the system concentrates on identifying malicious behaviors in a specific protocol. Usually, a PIDS is executed either within a single or among multiple hosts. For example, a PIDS may inspect TCP or HTTP traffic to trace malicious content. Similarly, it can monitor traffic between a web server and a database to detect any suspicious SQL queries. In NIDS, intrusions within the network are detected by monitoring the patterns and contents of the incoming and outgoing traffic. Consequently, the outside intrusions can be identified and all hosts are protected. However, it becomes expensive whenever there is too much traffic in the network.

Regarding the IoT, most of the intrusion detection systems are network-based since attackers can seamlessly misuse the heterogeneous and dynamic characteristics of the IoT environment. In the literature, NIDS is classified into the following four methods: Signature-based Intrusion Detection System (SIDS), Anomaly-based Intrusion Detection System (AIDS), Specification-based Intrusion Detection System (SpIDS), and Hybrid Intrusion Detection System (HyIDS). In SIDS, an intrusion signature is checked with the previously known intrusion patterns, stored in the database, to find significant matching. It is also known as knowledge-based detection or misuse detection. AIDS is a dynamic intrusion detection approach that monitors the activity log of a system and reports anomalies whenever it observes any deviations from normal behaviors. This method provides the capabilities to detect not only known and unknown attacks but also any insider attacks. In SpIDS, a set of rules and thresholds are defined for network modules like nodes, protocols, firewalls, etc. Utilizing these specifications, the system detects intrusions while observing any discrepancies from the acceptable behaviors [23]. On the other hand, Hybrid IDS incorporates the advantages of SIDS, AIDS, and SpIDS to detect both familiar and novel intrusions utilizing limited computational resources. The classification of NIDS is showed in Figure 1.

Techniques. Considering the resource and energy-constrained characteristics, AIDS and HyIDS are the most appropriate and feasible methods in IoT [24, 25]. Various machine Learning-based, statistical-driven (like payload-based), rule-based, and heuristics-based tech-

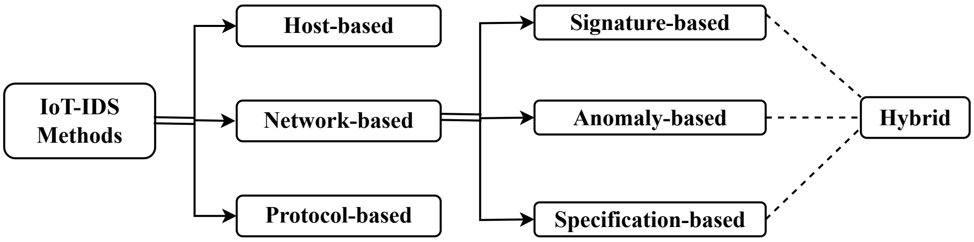

Figure 1: Categories of Intrusion Detection Methods in IoT.

niques are used to escalate the training process for AIDS. Recently, metaheuristics and hybrid approaches integrating different algorithms have been developed in this field, especially for IoT. In the next two Sections, some well-established techniques used in IoT-IDS are discussed. Figure 2 illustrates the classification of the existing IoT-IDS techniques as a whole.

2.2 Metaheuristic Algorithms

A metaheuristic is a general exploration (or diversification) method that can be applied to different problems in a similar way by visiting regions of the search space that are not already seen and evaluating candidate solutions. In general terms, metaheuristics are approximation algorithms that provide good or acceptable solutions within an acceptable computing time, that cannot be obtained with more specialized techniques, such as brute-force, linear programming, dynamic programming, randomization, quantum computation, exact algorithms, etc., but do not give formal guarantees about the quality of the solutions [26]. The main difference between heuristic and metaheuristic is that a heuristic algorithm utilizes some specially designed functions to explore the solution space intelligently; whereas, a metaheuristic is an iterative generation process that directs a supporting heuristic to explore and exploit the search space efficiently [8]. Moreover, heuristics can be applied to a specific problem; but, metaheuristics are more generalized and can be employed in the same way to many different problems. The metaheuristics algorithms can be classified into three groups as discussed below.

1. *Population-based metaheuristics:* This type of metaheuristic utilizes global exploration and local exploitation ability for searching in global search space to discover new promising solutions and to refine the already discovered solutions. In this study, these algorithms are divided into three classes: (i) Swarm-based, (ii) Nature-based, and (iii) Evolutionary Algorithms (EAs). Swarm-based metaheuristics (a.k.a. swarm in-

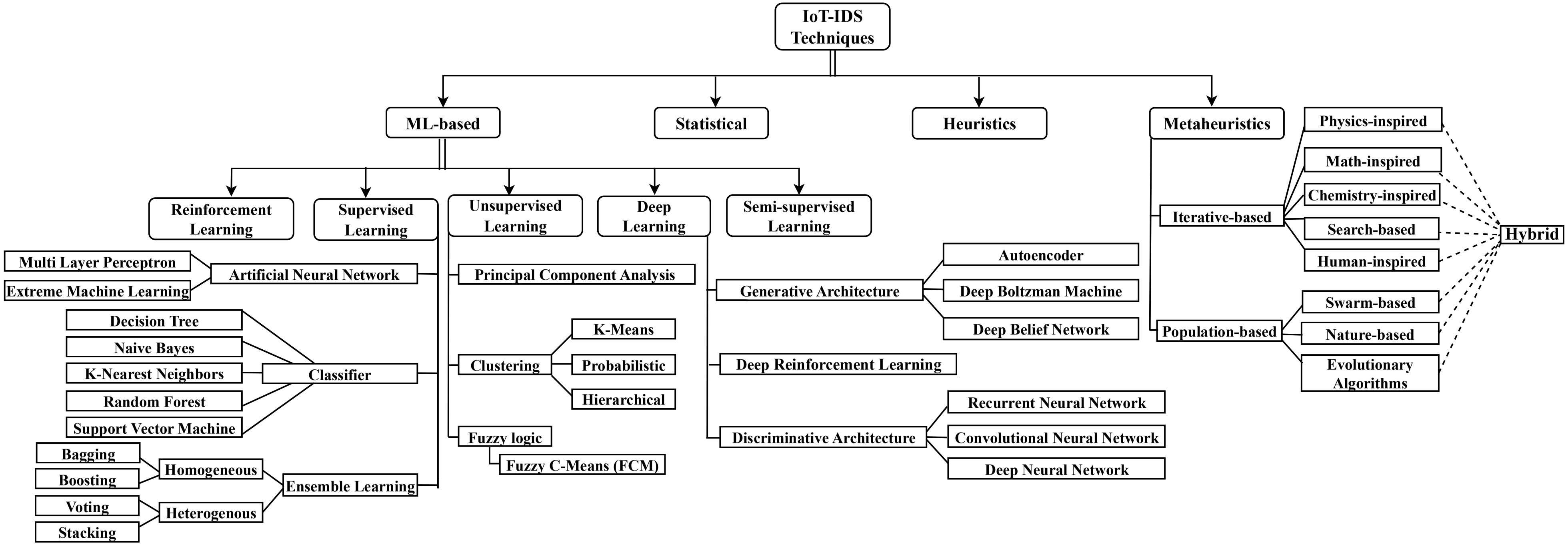

Figure 2: Classification of the existing IoT-IDS techniques.

telligence) are inspired by the social collective behavior of the birds, ants, bees, etc., where each animal (artificial agents) interacts with each other to achieve a particular goal in the environment [27]. Ant colony optimization (ACO), particle swarm optimization (PSO), Artificial bee colony (ABC), etc. are some of the most popular swarm-based metaheuristics. The second category is nature-inspired optimization, such as gorilla troops optimizer (GTO), crow search algorithm (CrSA), reptile search algorithm (RSA), butterfly optimization algorithm (BOA), moth–flame optimization (MFO), biogeography-based optimization (BBO), intelligent water drop (IWD), etc. Particularly, these algorithms mimic the successful characteristics of complex natural processes, including distinct animal behaviors, biological systems, natural calamities, etc. Though swarm intelligence also relies on nature, it specifically focuses on decentralized systems and collaborative behaviors; whereas, nature-inspired metaheuristics encompass diverse elements of nature, including the behavior of an individual animal. Another well-established population-based optimizations are evolutionary algorithms, which are based on the process of natural evolution like survival, reproduction, and mutation. Specifically, there are three important components of an EA: parent selection, variation operators (recombination/crossover and mutation), and replacement (evolution). Genetic algorithms (GAs), evolutionary programming (EP), and differential evolution (DE) are the most popular EAs in the literature.

2. *Iterative-based metaheuristics:* The second major group of metaheuristics is iterative-based. These algorithms are inspired by the laws of physics, mathematics, chemistry, or social human behavior. Particularly, physics-based metaheuristics are based on the concepts of physical laws and principles, for example, classical mechanics, thermodynamics, optics, etc. Gravitational search algorithm (GSA), simulated annealing (SA), multi-verse optimizer (MVO), etc. are the most popular physics-based optimization techniques. Similarly, math-based metaheuristics adopt mathematical concepts like number theory, geometry, and algebra, along with modern mathematics. Arithmetic optimization algorithm (AOA) [28] and sine cosine algorithm (SCA) [29] are prominent techniques in literature that are based on the arithmetic operators and sine/cosine mathematical functions, respectively. Other interesting iterative-based metaheuristics are inspired by human interaction, intelligence, learning processes, and experiences.

Some of these algorithms are teaching-learning-based optimization (TLBO), human-guided search (HGS) [30], and harmony search (HS). The rest algorithms in this category are search-based, for instance, local search (LS), tabu search (TS), neighborhood search (NS), etc.

3. *Hybrid metaheuristics:* Hybrid algorithms are integrated with different metaheuristics to utilize the advantages of distinct techniques for solving optimization problems. Algorithms in hybrid metaheuristics can focus on solving different problems simultaneously. For example, in hybridization with LS, global search is utilized to explore the search space, whereas LS is used to refine the areas of possible global optimum. On the other hand, the sub-metaheuristics within a hybrid approach can concentrate on optimizing different parts of the same problem, like a combination of PSO and GA, where PSO finds the optimal parameters used in GA.

2.3 Machine learning techniques

The relevant machine learning models are classified here. *Supervised Learning (SL)* is the model that is trained with labeled data (a set of inputs and correct outputs) to learn the corresponding features, followed by an execution engine to predict using the test data. Supervised learning is used when the target has a similar pattern to the trained data. Different classification techniques like decision tree (DT), random forest (RF), k-nearest neighbor (KNN), etc., collaborating of multiple classifiers a.k.a ensemble learning (EL), along with artificial neural networks (ANN) fall into this category. In *Unsupervised Learning (USL)* the desired outputs are not provided in the training phase. The main aim is to learn the similarity of the unlabeled data and further classify them into multiple groups. Some of the eminent algorithms are principal component analysis (PCA), and clustering techniques, such as k-means, probabilistic, and hierarchical clustering. *Semi-supervised Learning (SSL)* encompasses the mechanism of both supervised and unsupervised learning. Specifically, it utilizes a combination of unlabeled and labeled inputs. The purpose of this is to make better predictions in discovered patterns. *Reinforcement Learning (RL)* adopts the human learning process, especially learning from experiences. Particularly, it continuously optimizes feedback through actions after interaction with the environment. *Deep Learning (DL)* models originate from the concept of information processing and distribution in the human brain.

In brief, these types of architectures can be categorized into generative (unsupervised), discriminative (supervised), and deep RL architectures for IoT-IDSs.

3 Related Work

The systematic literature review (SLR) in [31] covers only a few population-based metaheuristics for intrusion detection in the IoT environment. Additionally, physical law-based, human-inspired, and hybrid optimization techniques are not discussed. Moreover, the authors do not concentrate solely on IoT. Rather, wireless, public networks, computer networks, Hadoop and MapReduce, and edge networks are also explored significantly. Furthermore, though they analyze the datasets used in developing the IDSs, no correlation is discovered among the metaheuristics, mostly used datasets and ML methods. Saadouni et al. [32] presents an SLR for IoT-IDS based on bio-inspired and ML-driven techniques. The authors vividly discuss the integration of ML methods with optimization algorithms. However, one of the most notable limitations of this work is the investigation of only 25 papers, whereas there are several well-established metaheuristics-assisted IDSs dedicated to IoT. Importantly, although the authors claim to study only IoT-based papers, we find that most of the articles are not focused on the IoT environment. In [33], the authors study population-based optimizations, specifically swarm intelligence devised for detecting intrusions in IoT. Besides, they analyze the datasets used and the performances of the existing systems. The main drawback of the SLR is the lack of covering all categories of metaheuristics-driven IDSs. Moreover, only basic ML algorithms are discussed in the SLR; whereas many crucial deep learning-based IDSs are sorted out in our study. Sharma et al. [34] aims to explore IoT-IDSs that rely on only multi-objective metaheuristics algorithms. Apart from this, they analyze different machine-learning models and popular datasets. However, the relation between these diverse techniques is still missing. Moreover, the study is not systematic. Heidari et al. [35] introduces an SLR containing rigid comparison and exploration of different IDSs in the IoT environment. The first and foremost limitation is the missing metaheuristics and ML-based systems, which we aim to cover in our study. Verma et al. [36] propose a survey on ML-driven IDSs for IoT applications. Regrettably, the study does not include any optimization algorithms, rather it intends to analyze the machine learning classifiers commonly utilized in intrusion detection. Hajiheida et al. [37] also do not study the metaheuristics algorithms that are extensively employed in the IoT-IDS. Importantly, rather than focusing on the metaheuristics or ML-based systems, they categorize and discuss different systems, such as SIDS, AIDS, SpIDS, and HyIDS.

The existing reviews either explore nature-inspired or ML-based IoT-IDS systems. Though there is only one survey [34] that discusses the integration of metaheuristics and machine learning techniques for the IoT environment, the coverage and analysis are too inadequate regarding the volume, significance, and diversity of the related IDSs in literature. Most importantly, no reviews analyze the correlation between the optimization algorithms and machine learning models while experimenting on a specific dataset. Apart from these, the existing works do not categorize the applications of different metaheuristics regarding intrusion detection in the IoT environment.

To address all these issues, a systematic literature review is presented, which extensively explores the existing metaheuristics and ML-integrated IDSs, specific to the IoT environment. Additionally, we analyze these systems based on different applications of metaheuristics algorithms, such as optimal feature selection, parameter tuning, hyperparameter tuning, etc. Moreover, the discovery of the connections among these algorithms, their outstanding performances, and the used datasets significantly distinguish this review from others. Furthermore, a new large-scale visualized taxonomy is demonstrated to provide researchers with an overview of the existing IoT-IDSs. Table 1 provides an in-depth comparison with the state-of-the-art reviews, highlighting the contributions of our work over others.

Table 1: Comparison with existing state-of-the-art surveys.

Work	**Year**	**SLR**	**# of articles**	**IoT-specific**	**Metaheuristics**				**Machine Learning Models**			**Usage of Datasets**	**Perfor. Analysis**	**Correlation Analysis**	**Application Analysis**
					EA	**SI**	**PhA**	**Others**	**Basic ML**	**DL**	**Hybrid**				
[31]	2024	✓	145	×	×	✓	×	×	×	×	×	×	✓	×	×
[32]	2024	✓	25	×	✓	✓	×	×	✓	✓	×	×	✓	×	×
[33]	2024	✓	101	×	×	✓	×	×	✓	×	×	✓	✓	×	×
[34]	2024	×	37	✓	✓	✓	×	✓	✓	✓	×	×	×	×	×
[35]	2023	✓	24	✓	×	×	×	×	×	×	×	×	✓	×	×
[36]	2020	×	25*	✓	×	×	×	×	✓	×	×	×	✓	×	×
[37]	2019	✓	43	✓	×	×	×	×	✓	✓	×	×	✓	×	×
Ours	2025	✓	111	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

*Not explicitly mentioned in the paper.

4 Review methodology

This section presents the review methodology used in this paper.

4.1 Objectives and Research Questions

This research aims to investigate the existing integration of metaheuristics and ML algorithms to detect intrusions in the IoT ecosystem. Besides, uncovering the hidden correlations among the top-performing optimization techniques and ML models, considering specific datasets is another goal of similar importance. To achieve these objectives, firstly, it requires understanding the necessity and exploring different applications of the metaheuristics-assisted ML architectures for developing IoT-IDSs. Secondly, an investigation is needed on the most popular datasets and evaluation metrics utilized to measure these detection systems. The next plan is to discover which optimization techniques and ML models come up with excellent performances, considering the tested datasets. After that, we plan to analyze and sort out the challenges and issues that arise because of the collaboration of these different conceptual techniques. Finally, the unexplored areas of metaheuristics and machine learning techniques need to be studied to facilitate future research. Table 2 outlines the specific research questions identified to achieve the objectives mentioned above.

RQ#	Research Questions	Objectives
RQ1	What are the need and existing applications of metaheuristics optimizations in developing ML-based IDS, especially for IoT?	To understand the necessity and explore the existing metaheuristics and ML algorithms, incorporated for developing IoT-IDSs.
RQ2	What are the most commonly used datasets and evaluation metrics for integrated IoT-IDS assessment?	To identify the well-known datasets and their coverages, and define the popular performance metrics.
RQ3	What are the relations between the optimization algorithms and classification methods with the datasets?	To find out the best-performing IoT-IDSs, analyze the metaheuristics and ML algorithms they used, and synthesize the outcomes.
RQ4	What are open issues raised by the integration of metaheuristics algorithms with ML?	To discuss the unavoidable challenges as well as possible solutions while combining machine learning with metaheuristics.
RQ5	What are the unexplored metaheuristics optimization algorithms for IDS in IoT?	To facilitate future research in this field, the undiscovered techniques need to be mentioned.

Table 2: Research questions and objectives.

4.2 Search strategy

In this review, we search relevant works in established and well-known online sources, such as IEEE Xplore Digital Library, ACM Digital Library, Elsevier, Springer, Nature, Wiley, Taylor & Francis, MDPI, and World Scientific. Initially, 765 articles are selected in total. For searching, specific keywords related to IoT-IDS which incorporate metaheuristics and ML have been used (See Table 3). Since we aim to cover the most recent techniques, we search and select only the relevant, effective, and scholarly papers that were published between 2020 and 2024. Importantly, this focused and extensive investigation differentiates our work from previous SLRs or surveys in the same field. Next, the papers that are deemed irrelevant and found to be duplicates are removed. Particularly, several research has been conducted on the metaheuristics and ML-driven detection systems that incorporate blockchain, fog computing, and supercomputing technologies, which are not relevant to this review. Moreover, several works focus on specific attack detection, for example, botnet, ransomware, malware, denial of service (DoS), etc. These articles are also removed from our dataset. Furthermore, intrusion detection systems that are not IoT-specific, are also eliminated since our concentration is solely on the IoT-IDSs. All of these keywords for exclusion are listed in Table 4. Apart from this, the related surveys are not included in the dataset. Additionally, the papers published in foreign languages are excluded from this study. Finally, 111 articles are chosen for this literature review.

Key	**Criteria**
Search string	(Metaheuristics-based) AND (Machine learning OR ML-based) AND (Intrusion Detection System OR IDS) AND (Internet of Things OR IoT)
Limiters	Article date between 2020 and 2024
Search modes	Search words occur either in the title, abstract, or in the introduction of the article

Table 3: Search criteria.

Excluded keywords		
Botnet detection	Malware detection	Ransomware detection
Data mining	Blockchain	Remote Sensing Images
Wireless Sensor Networks (in general)	DoS/DDoS detection	Fog Computing
Supercomputing	Selective forwarding attack	

Table 4: Exclusion keywords.

4.3 Data analysis

After applying the search strategy, a dataset consisting of 111 papers are collected, containing both conference and journal works on metaheuristics and ML-based intrusion detection systems for IoT. Among these, 90% are journal papers, and the rest are conference papers. According to Figure 3, in recent times, researchers have tended to give more attention to metaheuristics-assisted machine learning while developing IoT-IDS. It is also discovered that the highest number of quality articles was published in 2023 with 37 papers, followed by 31 papers in 2024, and 24 papers in 2022. Before 2021, metaheuristics were not studied in such a focused way as depicted in the Figure.

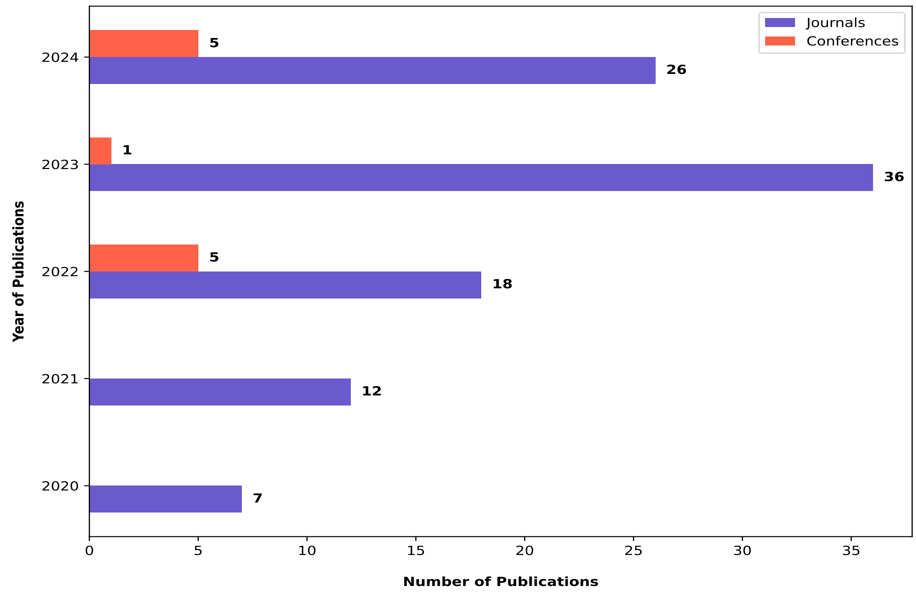

Figure 3: Year-wise publications for related IoT-IDSs, are included in this literature review.

4.4 Investigation of Journal Papers

We further analyze the 100 journal papers. Specifically, they are collected from 56 journals in total, where almost half of them are ranked as Q1 journals. Simultaneously, the amount of Q2 and Q3 journals is also significant, which indicates the inclusion of high-quality and well-established research in this literature review. A donut plot is drawn in Figure 4 to illustrate the percentage of different quartile journals studied in this work.

5 Results of the review

This section provides the results of the review answering each research question.

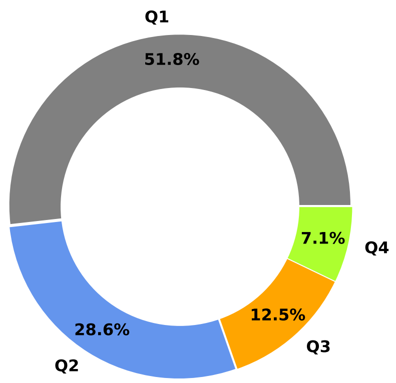

Figure 4: Percentile of different quartile journals included in this literature review [Q1=29, Q2=16, Q3=7, Q4=4].

5.1 *RQ1: What are the need and existing applications of metaheuristics optimization in developing ML and DL-based IDS, especially for IoT?*

Though machine learning algorithms offer high accuracy, enhanced security, and better performance, they require excessive computational power like high-performance GPUs (Graphics Processing Units), and a large volume of storage for generating, executing, and managing large datasets during training and testing phases. Undoubtedly, deep learning algorithms can seamlessly handle enormous datasets and offer fast processing; but, these require significant time to achieve minor precision improvements. Moreover, parameter-tuning is another unavoidable critical issue since adjusting the number of layers with the expected accuracy is entirely correlated [10]. In this regard, metaheuristics can be utilized to obtain near-optimal solutions in a shorter time than the exact algorithms. Specifically, a metaheuristic algorithm is an iterative generation process that guides a subordinate heuristic to explore and exploit the search space efficiently [8]. Besides, these algorithms terminate when specific conditions (e.g., the number of iterations, elapsed time, etc.) are satisfied. As a result, there is no possibility of running the algorithm for a long period; even the likelihood of being stuck in the local minima is negligible.

We discuss the existing integrated IoT-IDSs categorized into different metaheuristics algorithms. Besides, these optimization techniques are also analyzed by classifying them into diverse applications, such as future selection, parameter tuning, hyperparameter optimization, and hybrid applications. In this work, swarm intelligence techniques are differentiated from nature-based optimizations considering the vastness and significance of these two distinct categories of metaheuristics. Though swarm-based algorithms are also based on nature, they especially concentrate on decentralized systems and collaborative behaviors; contrarily, nature-inspired metaheuristics encompass diverse elements of nature, including the discrete behaviors of individual animals. The taxonomy of the existing metaheuristics and ML-integrated IoT-IDSs is illustrated in Figure 5.

5.1.1 Population-based Metaheuristics and ML

Swarm-based Metaheuristics. The well-known particle swarm optimization (PSO) technique is widely used in IoT-IDSs. Particularly, Elmasry et al. [38] leverage a double PSO to optimize features and hyperparameters. The efficiency of this metaheuristic is examined by discriminative and generative ML methods, especially CNN, LSTM, and DBN. Among these, DBN excels over others by 2% to 6% while testing on the NSL-KDD and CICIDS2017 datasets. In another paper, Saheed et al. [39] integrate an AE with PSO to optimally select features from the BoT-IoT and UNSW-NB15 datasets. After that, they also modify the inertia weight of PSO to optimize the hyperparameters of DNN, resulting in the efficient classification of attacks (an accuracy of 97.61% and 94.62% in BoT-IoT and UNSW-NB15, respectively). However, the combination of genetic self-adjusted PSO (GSAPSO) and EGB and KNN classifiers does not result in considerable performances [40].

Apart from these, bird swarm optimization (BSA), salp swarm algorithm (SSA), and golden jackal optimization algorithm (GJOA) are found to be reliable for detecting intrusions in IoT environments. In particular, a DBN-driven IoT-IDS is presented in [41], which offers 98.96% accuracy, 99.4% precision, and 98.87% recall on the NSL-KDD dataset when parameters are tuned by evaluated BSA (EBSA). Aljehane et al. [42] leverage GJOA to find the most significant features from the CICIDS-2017 dataset and SSA to optimize hyperparameters of the attention-driven bi-directional LSTM (A-BiLSTM). This dual usage of population-based optimizers secures 99.69% accuracy, 98.92% f1-score, and 98.74% MCC. Another variant of SSA, referred to as chaotic salp swarm optimization (CSSA) performs well with the incorporation of LightGBM, having an accuracy of 98.35%∼99.38% on the MC-IoT, MQTT-IoT-IDS2020, and MQTTset datasets [43]. However, adopting BSA and social group optimization algorithm (SCOA) for selecting features and optimizing parameters in kernel

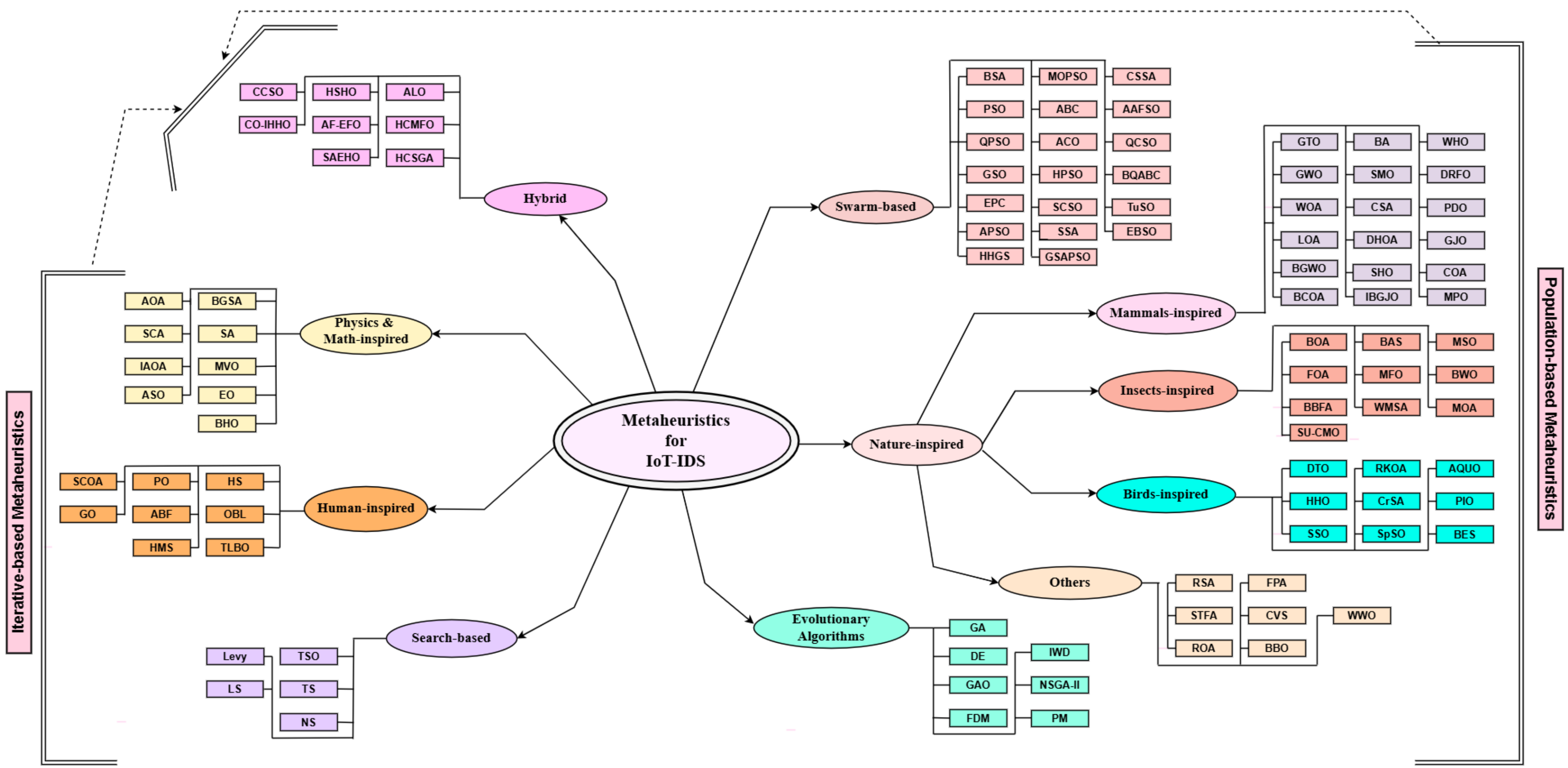

Figure 5: Taxonomy of the existing metaheuristics and ML-integrated IoT-IDSs.

extreme machine learning model (KELM) fails to deliver decent results across all metrics (99.45% accuracy, 80.26% precision, 82.67% recall, and 80.95% f1-score).

Interestingly, some detection systems demonstrate different performances in various datasets. For example, IDS with artificial bee colony (ABC) and extreme machine learning classifier performs well on CICIDS-2017; whereas significantly fails on UNSW-NB15 (accuracy 98.71% vs. 71.54%) [44]. Similar results appear in swarm-inspired sand cat swarm optimizer (SCSO) and ELM-based system [17]. However, integration of glow-swarm optimization (GSO) with PCA [45], chimp chicken swarm-based optimization (CCSO) with deep LSTM [46], and improved ACO with ensemble classifier (DDT, ANFIS and MDSVM) [47] does not result in considerable performance.

Nature-inspired Metaheuristics. These optimization techniques are extensively integrated with machine learning-based IoT-IDSs, especially Grey-Wolf Optimization (GWO) [48, 49, 50, 51, 52, 53], firefly optimization algorithm (FOA) [54, 55, 56], Capuchin Search Algorithm (CSA) [57, 58], and Whale Optimization Algorithm (WOA) [59, 19, 60, 61]. Regarding the GWO-based detection systems, [48, 51, 52, 53] utilize GWO for feature selection; whereas [49, 50] use for optimizing hyperparameters of quantum-based SVM classifier and EL method (comprised of DT, RF, KNN, and MLP), respectively. The former systems identify intrusions relying on XGBoost, elastic regularization-assisted contractive autoencoder (CAE), deep neural network (DNN), and SVM, respectively. Notably, all these IDSs come up with remarkable efficiency (e.g., 99%$\sim$100% accuracy). However, different datasets, preprocessing and other related techniques are employed within these IoT-IDSs. In [55, 56], FOA is integrated for selecting near-optimal features, and detection is conducted by classifiers, especially ensemble, and DT, respectively. Though [55] shows notable detection ability, [56] severely under-performs. In contrast, Savanovic et al. [54] improve the original FOA for tuning hyperparameters in classification techniques like KNN, and XGBoost. As a consequence, their IoT-IDS provides an accuracy of 99.98% and 99.6997%, respectively on UNSW-NB15 and IoT healthcare datasets. Turing to CSA-based detection systems, Kumar et al. [57] optimize parameters of a capsule autoencoder (HKCAE) and Elaziz et al. [58] select near-optimal features for CNN model using this metaheuristic. Importantly, in this case, parameter tuning turns to be more effective than feature selection since the former IDS offers outstanding accuracy on BoT-IoT and UNSW-NB15 datasets (99.9% and 99.7%); whereas the later system behaves inconsistently across various datasets (considerable for BoT-IoT, KDDCup-99, and CICIDS-2017; severe for NSL-KDD). Among the four WOA-based IDSs, [59] is the best-performing system with approximately 99.8% accuracy, precision, recall, f1-score, and specificity. The authors leverage this optimization technique to tune the hyperparameters of a gated recurrent unit (GRU). However, optimizing parameters of an LSTM using WOA also turns out to be effective (99.1%∼99.5% accuracy) [19].

Considering other IOT-IDSs of this category, most of the nature-inspired metaheuristics are leveraged for feature selection. Further examining of these systems reveal that various types of optimizers, such as Moth–Flame Optimization (MFO) [62], crow search algorithm (CrSA) [63], chaotic vortex search (CVS) [64], decisive red fox optimization (DRFO) [65], multi-objective prairie dog optimization (PDO [66], reptile search algorithm (RSA) [67], binary multi-objective Capuchin search algorithm (BMECapSA) [68], Aquila optimizer (AQUO) [69], BA [70], and Mayfly Optimization Algorithm (MOA) [71] are prominent. Among them, [62, 63, 64, 65, 66, 68] demonstrate higher efficiency while experimenting on diverse datasets. However, no common trend is found in terms of machine learning-based classifiers.

Other than these systems, a few IDSs utilize nature-centric optimization techniques for tuning parameters [72, 73, 74] or hyperparameters [22, 75] of the detection models; sometimes for hybrid applications [76, 77, 78]. Although in discrete cases, these systems show considerable results, their performances are not generally satisfactory.

Evolutionary Algorithms. Only a small number of IoT-IDSs have utilized evolutionary algorithms (EAs) and they do not significantly surpass other detection systems. The best-performing IDS of this type is proposed by Latif et al. [79], where hyperparameters of a CNN-based ensemble classifier are optimized by a genetic algorithm (GA). Ultimately, this system achieves 100% accuracy, precision, recall, f1-score, and Cohen's kappa score in the Edge_IIoTset dataset. Second best-performing IDSs presented in [80], where feature selection is accomplished by a non-dominated sorting genetic algorithm (NSGA) and classification is done using a support vector machine (SVM). Importantly, the system achieves a remarkable accuracy of 99.48% on the TON_IoT dataset. Gupta et al. [81] integrate an evolutionary algorithm intelligent water drop (IWD) and a nature-inspired biogeography-based optimization (BBO) technique with a feed-forward neural network (FNN). The IDS detects attacks more correctly when tested on CICIDS-2017 compared to the IoTID20 dataset (accuracy 98.2339% vs. 96.7414% and f1-score 99.0865% vs. 95.4901%). However, integration of an assimilated artificial fish swarm optimization (AAFSO) with genetic algorithm (GA)-tuned faster recurrent CNN (FRCNN) does not perform well across diverse datasets [82].

Population-based Hybrid Metaheuristics. Numerous works have employed more than one population-based metaheuristics to improve the performance of IoT-IDSs. In most cases, such hybridization is utilized to select an optimal set of features. Regarding traditional machine learning classifiers, KNN [83, 84, 13, 14] and RF [85, 86, 87, 88, 89] are widely used in these systems. Specifically, SSA+ALO [83], quantum-driven binary ABC+GA [84], gorilla troops optimizer (GTO)+birds swarm algorithm (BSA) [13], and GWO+dipper throated optimization (DTO) [14, 90] are integrated in these KNN-based detection systems. Notably, all these IDSs provide substantial performance in terms of accuracy, precision, recall, and other related metrics. On the other hand, RF-based IDSs utilize LOA+FOA [85], PSO+bat algorithm (BA) [86], spider monkey algorithm+hierarchical PSO [87], and PSO+GWO [88, 89] for feature selection purpose. These systems also demonstrate significant efficiency in classifying various attacks. In addition to these, hunger game search (HGS) and remora optimization algorithm (ROA) in [91], and GA and GWO are hybridized in [92] for selecting near-best features from AWID dataset for SVM classifier. Both of these combinations show notable performances with 99.1% accuracy and negligible FPR. Turning to deep learning-oriented IoT-IDSs, three works are found that applied a Look Ahead Artificial Neural Network (LAANN), recurrent neural networks (RNNs), and a deep learning-based hybrid neural network (DL-HCNN) respectively. Particularly, sea turtle foraging algorithm (STFA)+explorated PSO (EXPSO) [93], Harris hawk optimization (HHO)+fractional derivative mutation (FDM) [15], and Chicken Swarm Optimization (ChSO)+GA [94] are utilized in these systems to select optimal feature set. However, they fail to provide remarkable performance with 95%$\sim$98% considering all related metrics.

Apart from feature selection-based IDSs, a few research studies focus on tuning the parameters or hyperparameters of classification models. Khafaga et al. [95] propose an innovative whale optimization (WOA) regulated by DTO to optimize parameters of KNN, RF, and NN. Experimental evaluation using the RPL-NIDS17 dataset results in 99% AUC and 95.1% accuracy. In [96], SAEHO and SU-CMO are also proposed for adjusting the parameters of the two hybrid classifiers, particularly CNN+DBN and Bi-LSTM+GRU. The integration of SAEHO and hybrid classifier offers better accuracy than that of SU-CMO and hybrid classifier (91.6% vs 84.8%). Bahaa et al. [20] integrate adaptive PSO and WOA for hyperparameter optimization in their CNN-based detection system. However, the system achieves only 94.54% accuracy and 0.9 JSC. However, a small number of papers focus on employing hybrid population-based optimizers for accomplishing multiple purposes at a time [97, 98, 99]. One of the notable systems is introduced by Karthikeyan et al. [97], where GWO is leveraged to optimize parameters and FOA to choose the most suitable features for the SVM classifier in the IoT-WSN environment. The separate use of these two metaheuristics crucially influences the system's accuracy (99.29%). However, other such existing IoT-IDSs drastically fails, especially red kite optimization algorithm (RKOA)+Levy flight chaotic WOA with EL (LSTM, BiLSTM, and Bi-GRU) [98] and black widow optimization (BWO)+BES with hybrid deep learning (HDL) [99].

5.1.2 Iterative-based Metaheuristics and ML

Physics and Math-based Regarding math-inspired optimization techniques, the arithmetic optimization algorithm (AOA) is widely employed. In [100], AOA is utilized to select optimal feature sets for random forest and extra trees classifiers. Experimental evaluations on four public datasets reveal that the IDS produces a much less false positive rate (0.002%) for the tests conducted using the NF-ToN-IoT-v2 dataset. Makhadmeh et al. [101] also apply AOA for executing the same purpose using different classifiers, KNN. Interestingly, the accuracy of these two systems is almost identical (around 99.9%). Though AOA and quantum-driven PSO (QPSO) are utilized in [102] for different purposes, the deep wavelet neural network (DWNN)-based detection system does not secure substantial accuracy (98.21%). Turning to the physics-based IoT-IDSs, Atom Search Optimization (ASO) and Equilibrium Optimization (EO) techniques are utilized in [103] to select optimal features prior to applying K-means clustering. Importantly, this hybridization demonstrates remarkable performance on NSL-KDD, UNSW-NB15, and KDD-CUP99 datasets. In another paper [104], a black hole optimization technique is employed to select near-optimal features from the UNSW-NB15 and NSL-KDD datasets. Two CNNs are utilized in parallel to identify intrusion and result in around 97.5%∼99.89% efficiency in terms of common performance metrics.

Human-inspired. Considering the integration of metaheuristics adopted from human behaviors and their decision-making process, [105, 106, 107, 108] IoT-IDSs are the most notable ones. Specifically, the political optimizer (PO) utilized for parameter tuning in a cascade forward neural network (CFNN) model, compact SCA (CSCA) for adjusting the parameters of the KNN classifier, and modified growth optimizer (GO) for selecting near-best features before training by CNN are significantly performed well with an accuracy of 99.86%, 98.27%∼99.327%, and 99.941%), respectively. However, these groups of optimizers are not always effective, especially for intrusion detection in IoT environment [109, 21, 110].

Search-based Though IoT-IDSs of this category tend to bring significant performances, they are too rare in the literature. Only one of them is found [111], the authors utilize tabu search with the idea of cellular automata to succeed in the features selection task. Consequently, it results in accuracy, precision, and FPR of 99.5%, 97.92%, and 0.004%, respectively while classified using an ensemble learning method.

5.1.3 Hybrid Metaheuristics and ML

In the context of IoT intrusion detection systems, existing hybrid optimization algorithms can be categorized into 6 small groups: swarm+physics-based [112], nature+physics-inspired [113, 114], nature+math-inspired [115, 116], nature+human-based [117, 118], swarm+search-based [18], and nature+search-inspired [119, 120, 121]. Though utilizing physics-based techniques with nature-inspired ones (binary gravitational search (BGSA)+GWO [113], simulated annealing (SA)+shuffled shepherd optimization (SSO) [114]) prove to be effective, integrating with swarm-based optimizers (multi-object PSO+Lévy flight [112]) turns out to be inefficient. Regarding the third group, Rahmani et al. [115] employ grasshopper optimization (GAO) and AOA for parameters and hyperparameters tuning in a random neural network (RdNN), which generates an IDS having 99.56% precision and 99.37% detection rate. In another work [116], a binary chimp optimization algorithm (BCOA) is integrated with the sine cosine algorithm (SCA) for securing the IoT-WSN network. Although the IDS generates high accuracy and specificity (99.63% and 99.67%, respectively), the f1-score is not convincing (94.52%). The well-known human-based metaheuristic object-based learning (OBL) is hybridized with Harris Hawk Optimization (HHO) and Golden Jackal Optimization Algorithm (GJOA), respectively in [118] and [117] to select best possible features. These DT-based and LSTM-driven IoT-IDSs provide remarkable performances with 99.65%∼100% and 98.93% accuracy, respectively. Baniasadi et al. [18] adjust parameters of deep CNN (DCNN) utilizing neighborhood search (NS)-based PSO. They get a negligible amount of mean square error (0.00053%) with 98.86% accuracy and 95.32% specificity on the UNSW-NB15 and Bot-IoT datasets. Turning to the last group of this category, it can be concluded that selecting features using a combination of nature-inspired and search-based metaheuristics is not effective according to the results provided in [119, 120, 121]. It is worth mentioning that these IDSs use EL classifier, variational autoencoder (VAE), and deep RL, respectively.

Table 5 shows the list of works in the existing literature that leverage different metaheuristics-based techniques and ML algorithms. According to the table, most systems leverage nature-inspired optimization techniques to increase the efficiency of the classifiers. Besides, swarm-based, population-based hybrid, and hybrid metaheuristics are utilized significantly. Moreover, a thorough analysis of the IoT-IDSs based on different performance metrics, metaheuristics, their applications, ML algorithms, classification types, and datasets are presented in Appendix A (Table 11).

Metaheuristics	**Machine Learning Models**						
	SL			**USL**	**DL**		
	Classification	**EL**	**ANN**		**Generative**	**DRL**	**Discriminative**
Swarm-based	[122, 123, 124, 40]	[47, 43, 40]	[125, 44, 17, 73]	[45, 126]	[38, 41]		[38, 82, 21, 39, 42, 46]
Nature-inspired	[127, 128, 129, 130, 56, 49, 66]	[54, 63, 48, 55, 62, 76, 22, 50]	[131, 64, 73, 132, 60, 65, 81]		[120, 57, 72, 51, 78]		[52, 67, 68, 133, 134, 69, 59, 58, 19, 61, 74, 42, 70, 71, 135, 77, 136, 75]
EA-based	[122, 80]		[81, 79]				[82, 104]
Population-based hybrid	[13, 14, 95, 85, 90, 92, 91, 88, 86, 87, 89, 97, 83, 53, 84]		[95, 93]		[96]		[15, 96, 20, 98, 94, 137, 99, 75]
Phy/Math-based	[100, 101]			[103]			[102]
Human-inspired	[106, 16]		[105, 73]		[110]		[107, 109, 21, 110]
Search-based		[111]					
Hybrid	[114, 112, 118]	[113, 116, 119]	[115]		[120]	[121]	[138, 18, 117]

Table 5: List of existing IoT-IDSs based on different metaheuristics and ML models.

Analysis on Different Applications

We find that most of the existing IoT-IDSs solely utilize different metaheuristics algorithms for selecting an optimal set of features. Besides, some of the systems employ them distinctly for optimizing the parameters and hyperparameters of the machine learning models. However, a few works focus on *hybrid applications* by leveraging feature selection and parameter (FS-PT) or hyperparameter (FS-HPT) tuning in the same detection system. Figure 6 illustrates the percentage of different applications leveraged by the IDSs, and Table 6 shows the list of corresponding existing works.

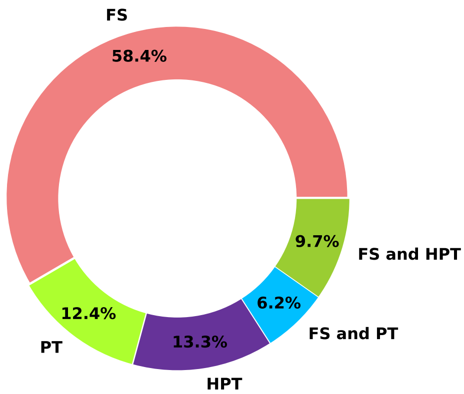

Figure 6: Percentile of different applications of metaheuristics algorithms.

Application	Ref.
FS	[13, 52, 14, 122, 131, 15, 80, 85, 113, 138, 67, 107, 100, 114, 45, 123, 90, 92, 91, 112, 88, 44, 128, 86, 47, 87, 68, 133, 89, 63, 124, 69, 17, 64, 93, 83, 48, 43, 111, 129, 55, 53, 119, 62, 94, 130, 126, 58, 137, 121, 60, 117, 118, 84, 56, 65, 66, 70, 71, 16, 51, 101, 81, 110, 136, 103, 104]
PT	[95, 105, 115, 96, 18, 73, 57, 19, 74, 41, 72, 135, 77, 46]
HPT	[54, 115, 109, 20, 73, 132, 21, 59, 61, 22, 49, 50, 77, 40, 79]
FS and PT	[125, 102, 116, 97, 134, 120, 75]
FS and HPT	[38, 127, 116, 98, 106, 82, 39, 76, 99, 42, 78]

Table 6: List of existing IoT-IDSs based on different applications of metaheuristics.

5.2 *RQ2: What are the most commonly used datasets and evaluation metrics for IoT-IDS assessment?*

In this study, we outline the most popular intrusion datasets used in the IoT context, specifically for testing metaheuristics and ML-driven systems. Interestingly, all works utilize public datasets, rather than creating on their own.

Our investigation reveals that the well-known NSL-KDD dataset [139] is extensively used by IoT-IDSs. It consists of 148,517 records extracted from the 5,209,458 samples of the oldest benchmark dataset, KDDCup-99 [140] by removing redundant records. Both of these datasets contain 41 features and 5 target classes. In 2015, the UNSW-NB15 dataset [141] was created having 49 features and 10 target classes. Importantly, since this dataset does not have any outdated features of attacks, researchers tend to test their works on this. Additionally, the BoT-IoT [142] and CICIDS-2017 [143] datasets are widely used as well. However, Table 7 states that CICIDS-2017 contains around 80 features and 8 classes; whereas BoT-IoT is a huge dataset with 73,360,900 records and 46 features and 7 classes. Several systems also utilize the TON-IoT [144] and N-BaIoT [145] datasets. TON-IoT is a large dataset with 22,339,021 records in total, of which 461,043 are dedicated to training and testing purposes. On the other hand, N-BaIoT consists of 23 features and 7,062,606 records. The proportion of each dataset used in the existing detection systems is shown in Figure 7. Apart from these mostly used datasets, the IoTID20 dataset [146] is used in 5 papers. Additionally, AWID [147], WSN-DS [148], and RPL-NIDDS17 [149] datasets are employed by three systems each; whereas, the rest of the works utilize distinct datasets.

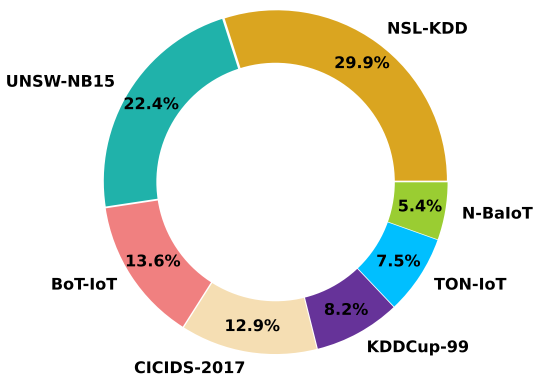

Figure 7: Percentile of the most used datasets for experimenting with the existing IoT-IDSs.

Evaluation metrics. The most prominent metrics widely used by the existing IoT-IDSs are enlisted here. These metrics include accuracy, precision, recall or sensitivity or true positive rate (TPR), f1-score, specificity or selectivity or true negative rate (TNR), false positive rate (FPR) or false alarm rate (FAR), area under curve (AUC), Matthew's correlation coefficient (MCC), and G-mean. Equations [1-9] denote their standard mathematical

Table 7: The most used datasets for experimenting with the existing IoT-IDSs.

Dataset (yr.)	**Target classes**	**Distribution (%)**	**# of features**	**# of training records**	**# of testing records**	**Total # of records**	**Imbalance**
NSL-KDD (2009) [139]	Benign, Probe, DoS, U2R, R2L	51.89 + 35.94 + 9.48 + 2.52 + 0.17	41	125,973	22,544	148,517	✓
UNSW-NB15 (2015) [141]	Benign, Fuzzers, Analysis, Backdoors, DoS, Exploits, Generic, Reconnaissance, Shellcode, Worms	87.36 + 0.95 + 0.11 + 0.09 + 0.64 + 1.75 + 8.48 + 0.55 + 0.06 + 0.01	49	175,341	82,332		✓
BoT-IoT (2019) [142]	Benign, DoS, DDoS, Reconnaissance, Information Theft	0.01 + 44.96 + 52.54 + 2.48 + 0.002	46	-	-	73,360,900	✓
CICIDS-2017 (2017) [143]	Benign, DoS Hulk, PortScan, DDoS, DoS GoldenEye, FTP-Patator, SSH-Patator, DoS slowloris, DoS Slowhttptest, Bot, Web Attack – Brute Force, Web Attack – XSS, Infiltration, Web Attack – SQL Injection, Heartbleed	83.34 + 8.16 + 5.61 + 1.48 + 0.36 + 0.28 + 0.21 + 0.20 + 0.19 + 0.07 + 0.05 + 0.02 + 0.00 + 0.00 + 0.00	80	-	-	2,830,743	✓
KDDCup-99 (1999) [140]	Benign, Probe, DoS, U2R, R2L	19.86 + 0.84 + 79.30 + 0.0 + 0.02	41	4,898,431	311,027	5,209,458	✓
TON-IoT (2021) [144]	Benign, Backdoor, DDoS, DoS, Injection, MITM, Password, Ransomware, Scanning, XSS	3.56 + 2.27 + 27.60 + 15.11 + 2.03 + 0.00 + 7.69 + 0.33 + 31.96 + 9.44	46	461,043		22,339,021	✓
N-BaIoT (2018) [145]	Benign, mirai_udp, gafgyt_udp, gafgyt_tcp, mirai_syn, mirai_ack, mirai_scan, mirai_udpplain, gafgyt_combo, gafgyt_junk, gafgyt_scan	7.87 + 17.41 + 13.40 + 12.17 + 10.38 + 9.11 + 7.62 + 7.41 + 7.29 + 3.71 + 3.61	23	-	-	7,062,606	moderately

representations, respectively.

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN} \tag{1}$$

$$\text{Precision} = \frac{TP}{TP + FP} \tag{2}$$

$$\text{Recall} = \frac{TP}{TP + FN} \tag{3}$$

$$\text{F1-score} = \frac{2 \times \text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}} \tag{4}$$

$$\text{Specificity} = \frac{TN}{TN + FP} = 1 - \text{FPR} \tag{5}$$

$$\text{FPR} = \frac{FP}{TN + FP} \tag{6}$$

$$\text{AUC} = \int_a^b f(x)\,dx \tag{7}$$

$$\text{MCC} = \frac{TP.TN - FP.FN}{\sqrt{(TN + FN) \times (TN + FP) \times (TP + FN) \times (TP + FP)}} \tag{8}$$

$$\text{G-Mean} = \sqrt{\text{Precision} \times \text{Recall}} \tag{9}$$

Here, true positive (TP) is the number of detected attacks that occurred indeed, and false positive (FP) is the number of predicted intrusions which are not truly occurred. Similarly, true negative (TN) is the number of correctly classified benign or normal instances, and false negative (FN) is the volume of events that are wrongly categorized as Benign. AUC is the curve of TPR against FPR which indicates the quality of a classification model. Particularly, this indicator gives an idea of the general accuracy of the classifier for all false positive detection rates. MCC is used to evaluate the quality of both binary and multi-class classifications. Specifically, it balances the measurement considering TP, TN, FP, and FN equally. G-mean is a balanced geometric mean calculated as the square root of the product of precision and recall. It aims to correctly measure the classifier performance on any imbalanced dataset. Depending on various requirements, several other metrics such as mean square error (MSE), Jaccard similarity coefficient (JSC) or Jaccard index, negative predictive value (NPV), and many more are also measured.

5.3 RQ3: What are the relations between the optimization algorithms and classification methods with the datasets?

To address this research question, we analyze the existing works and discover the best-performing IDSs tested using distinct highly-used datasets. All selected papers are published in Q1 or Q2 journals, indicating the correctness and effectiveness of our analysis.

5.3.1 Connecting dots among Metaheuristics, Datasets, and Machine Learning

NSL-KDD. Turning to the NSL-KDD dataset, different classification techniques are used in the assessments of IDSs. Among these classifiers, random forest (RF) remarkably demonstrates high performance in the top-performing IDSs with 99.66%∼99.98% accuracy and 99.85%∼99.96% f1-score (see Table 8). Notably, the RF algorithms are incorporated with population-based metaheuristics like GWO-PSO, LOA-FOA, and SMO-HPSO to select optimal features for the corresponding IDSs. Regarding deep learning algorithms, different discriminative methods like convolutional neural networks (CNNs), BiGRU, and LSTM are integrated to develop IoT intrusion detection systems. However, these models do not outperform RFs.

UNSW-NB15. Interestingly, from Table 8, it can be seen that the ensemble learning (EL) classification models are leveraged significantly in the tests conducted on the UNSW-NB15 dataset. The topmost systems generate an accuracy and f1-score of 99.41%∼100% and 99.33%∼99.99%, respectively. Importantly, these IDSs leverage metaheuristics for feature selection, parameter, and hyperparameter tuning in the machine learning models. In the majority of cases, EL techniques are integrated with either nature-based or population-based hybrid optimization algorithms, such as GWO, MFO, FOA, BGSA-BGWO, and LS-PIO. Besides, researchers also tend to explore diverse deep learning architectures though these systems are less effective than the previous ones.

BoT-IoT. Regarding the experiments on the BoT-IoT dataset, Table 8 illustrates that most of the best-performing IDSs employ discriminative architectures, specifically CNNs. However, these IDSs do not outperform EL, SVM, AE, and ANN-based systems (accuracy of 98.86%∼99.15% vs 99.68%∼99.98%). Further investigation of the metaheuristics uncovers that CNNs are tested by combining with diverse categories of optimization techniques (hybrid, SI, and nature-based); whereas, other machine learning algorithms are integrated with nature-based metaheuristics and exhibit better performance. Among these optimization algorithms, roughly half of them are used for feature selection and the other half are utilized for parameter and hyperparameter optimization.

CICIDS-2017 and KDDCup-99. Turning to the tests conducted on CICIDS-2017 and KDDCup-99 datasets, it can be observed that the same case as BoT-IoT concerning the utilization of deep learning techniques, that is, the abundant use of CNNs in the best-performing IDSs. On the CICIDS-2017 dataset, these algorithms work impressively since the accuracy and f1-score are between 99.77%$\sim$99.93%, and 99.72%$\sim$99.93%, respectively considering the topmost five IDSs. Table 8 depicts that these CNNs are consolidated with either hybrid (TSO-DE) or nature-based (RSA, AQUO, and CSA) metaheuristics. Notably, all of these algorithms are employed for selecting optimal features. On the contrary, when examined on the KDDCup-99 dataset, in most cases, CNNs do not surpass others in terms of f1-score. Other machine learning algorithms, specifically ANN and EL are synthesized with EXPSO-STFA and LS-PIO hybrid optimizers, respectively, which are also used for the optimal selection of the features.

TON-IoT. Investigation of the TON-IoT dataset reveals that both discriminative and generative-based models are leveraged to design IoT-IDSs. Distinctly, CNN and hybrid of AE-DNN models demonstrate higher performance with an accuracy of 99.99% and 99.888%, respectively. The corresponding f1-scores are almost identical. Concerning metaheuristics, these ML models incorporate binary multi-objective CSA (BMECapSA) and simulated annealing (SA), respectively, utilized for feature selection.

N-BaIoT. Similar to the experimental evaluations on the NSL-KDD dataset, plentiful use of classification algorithms, specifically RFs and KNN is noticed in the case of the N-BaIoT dataset. The accuracy and f1-score of these systems are satisfactory with 98.2%$\sim$99.86% and 99.4%$\sim$99.86%, respectively. However, the highest performance is achieved by the XGBoost technique. Importantly, KNNs tend to perform better when incorporated with a hybrid optimization algorithm, particularly SSO-SA. Regarding RF, it offers the same accuracy and f1-score when integrated with population-based hybrid metaheuristics (LOA-FOA and GWO-PSO). Notably, all these optimizers are employed for feature selection.

Table 8: The assessment of the best-performing IDSs in the IoT environment. Cells containing "-" indicate that the information is not explicitly mentioned in the related papers, and "N/A" denotes "not applicable" since those works optimize either parameters or hyper-parameters, rather than selecting features set. Besides, "Features count" is abbreviated as "FC", meaning the number of features selected by the corresponding metaheuristics.

Dataset	**Ref**	**Metaheuristics**	**Appli.**	**ML**	**FC**	**Acc(%)**	**F1(%)**	**Others(%)**	**Quar.**
NSL-KDD	[88]	GWO-PSO	FS	RF	-	99.97	99.96	-	Q2
	[85]	LOA-FOA	FS	RF	-	99.98	99.73	AUC=99.76	Q2
	[48]	BGWO	FS	EL (XG-Boost)	-	99.9427	99.9426	-	Q2
	[104]	BHO	FS	Parallel CNNs	-	99.8928	99.89		Q1
	[68]	BMECapSA	FS	CNN	18	99.85	99.85	FAR=0.0019, FNR=0.001	Q1
	[130]	SMO	FS	RF	-	99.675	99.9325	AUC=99.3025	Q2
	[89]	GWO-PSO	FS	RF	-	99.66	-	-	Q1
	[94]	HCSGA	FS	DLHNN	-	99.52	97.16	-	Q1
	[19]	WOA	PT	LSTM	N/A	99.5	-	Specificity=98.45	Q1
	[106]	Compact SCA	HPT	KNN	N/A	99.327	-	FAR=0.5848	Q2
	[97]	GWO,FOA	PT, FS	SVM	-	99.29	96.23	FAR=99.59, AUC=98.51	Q1
	[41]	EBSA	PT	DBN	N/A	98.96	99.13	-	Q2
	[87]	SMO-HPSO	FS	RF	22	98.98	98.59	AUC=99.81	Q1
	[117]	IBGJO	FS	LSTM	-	98.93	98.17	-	Q1
	[103]	ASO-EO, FOA	FS	k-means	-	98.9	100	-	Q1
	[63]	enhanced CrSA	FS	EL	11	99	98.14	-	Q1
UNSW-NB15	[54]	modified FOA	HPT	EL(XGBoost)	N/A	99.98	99.99	AUC-ROC=1	Q1
	[50]	GWO	HPT	EL	N/A	100	99.745	FAR=1.5, ROC=99.4	Q1
	[62]	MFO	FS	EL	14	100	99.75	-	Q1
	[57]	CSA	PT	HKCAE	N/A	99.7	98.9	Specificity=98.3	Q2
	[105]	PO	PT	CFNN	N/A	99.46	99.76	-	Q2
	[113]	BGSA-BGWO	FS	EL	4	99.41	99.33	FAR=0.03	Q2

Continued on next page

Table 8 – *Continued from previous page*

Dataset	Ref	Metaheuristics	Appli.	ML	FC	Acc(%)	F1(%)	Others(%)	Quar.
	[103]	ASO-EO, FOA	FS	k-means	-	99.1	99.4	-	Q1
	[19]	WOA	PT	LSTM	N/A	99.1	-	Specificity=98.99	Q1
	[61]	WOA	HPT	GRU	N/A	99	-	-	Q2
	[55]	FOA	FS	EL	-	98.89	98.91	AUC=99.79	Q2
	[65]	DRFO	FS	DBRBF	-	98.5	98.5	FAR=8.2	Q1
	[104]	BHO	FS	Parallel CNNs	-	97.7217	97.56		Q1
	[93]	EXPSO-STFA	FS	LAANN	-	95.65	95.64	Specificity=92.74, FNR=10.23, MCC=92.56	Q1
BoT-IoT	[50]	GWO	HPT	EL	N/A	99.98	99.955	FAR=1.3, ROC=99.99	Q1
	[57]	CSA	PT	HKCAE	N/A	99.9	98.2	Specificity=99.7	Q2
	[64]	CVS	FS	FLN-ANN	-	99.68	99.21	Specificity=99.83	Q1
	[58]	CSA	FS	CNN	-	99.15	98.806	-	Q1
	[49]	IGWO	HPT	QSVM	N/A	99.11	97.48	-	Q1
	[138]	TSO-DE	FS	CNN	-	99.042	99.042	FAR=0.00301	Q1
	[67]	RSA	FS	CNN	-	99.02	99.07	-	Q1
	[69]	AQUO	FS	CNN	10	98.926	98.904	-	Q1
	[18]	NS-BPSO	PT	DCNN	N/A	98.86	-	Specificity=95.32, MSE=0.00053	Q1
	[39]	HAEMPSO	FS, HPT	DNN	-	97.61	-	-	Q1
	[49]	IGWO	HPT	QSVM	N/A	99.11	97.48	-	Q1
	[46]	CCSO	PT	Deep LSTM	N/A	96.71	-	Specificity=91.985	Q1
CICIDS-2017	[138]	TSODE	FS	CNN	-	99.93	99.93	FAR=0.00009	Q1
	[67]	RSA	FS	CNN	-	99.911	99.888	-	Q1
	[69]	AQUO	FS	CNN	-	99.911	99.888	-	Q1
	[58]	CSA	FS	CNN	-	99.911	99.888	-	Q1
	[64]	CVS	FS	FLN-ANN	-	99.77	99.72	Specificity=99.92	Q1
	[117]	IBGJO	FS	LSTM	-	99.75	98.81	-	Q1
	[42]	GJOA,SSA	FS, HPT	A-BiLSTM	-	99.69	98.92	MCC=98.74	Q1
	[89]	GWO-PSO	FS	RF	-	99.66	-	-	Q1
	[75]	ALO, FPA	FS, HPT	CNN+LSTM	-	99.55	99.55	AUC=99.55	Q1
	[110]	IGC-SA	FS	AE-DNN	-	99.4	99.4	-	PAIS24
	[107]	MGO	FS	CNN	-	99.22	99.218	G-Mean=99.218	Q1
	[81]	IWD-BBO	FS	FNN	-	98.2339	99.0865	-	Q1
	[117]	IBGJO	FS	LSTM	-	99.75	98.81	-	Q1
KDDCup-99	[107]	MGO	FS	CNN	-	99.941	99.942	G-Mean=99.942	Q1

Continued on next page

Table 8 – *Continued from previous page*

Dataset	Ref	Metaheuristics	Appli.	ML	FC	Acc(%)	F1(%)	Others(%)	Quar.
	[69]	AQUO	FS	CNN	-	99.919	89.987	-	Q1
	[58]	CSA	FS	CNN	-	99.917	89.988	-	Q1
	[119]	LS-PIO	FS	EL	15	99.82	97.23	FAR=6.9, TPR=99.23, AUC=96.32	Q1
	[89]	GWO-PSO	FS	RF	-	99.66	-	-	Q1
	[103]	ASO-EO	FS	k-means	-	96.1	100	-	Q1
	[93]	EXPSO-STFA	FS	LAANN	-	95.65	95.64	Specificity=92.74, FAR=14.52, FNR=10.23, MCC=92.56	Q1
	[138]	TSODE	FS	CNN	-	92.064	90.007	FAR=0.01989	Q1
	[67]	RSA	FS	CNN	-	92.04	89.985	-	Q1
TON_IoT	[68]	BMECapSA	FS	CNN	12	99.99	99.99	FAR=0.0001, FNR=0.00002	Q1
	[110]	SA	FS	AE-DNN	-	99.888	99.875	-	PAIS24
	[74]	WHO	PT	fused CNN-BiGRU	N/A	99.71	99.05	-	Q1
	[78]	STFA,SpSO	FS, HPT	DBN	-	99.51	-	Specificty=99.36, MCC=60.36	Q1
	[111]	TS	FS	EL	13	99.5	-	FAR=0.004	Q1
N-BaIoT	[48]	BGWO	FS	EL (XG-Boost)	-	99.9941	99.9941	-	Q2
	[85]	LOA-FOA	FS	RF	-	99.86	99.86	-	Q2
	[88]	GWO-PSO	FS	RF	-	99.86	99.86	-	Q2
	[114]	SSO-SA	FS	KNN	-	98.7	99.8	-	Q2
	[123]	EPC	FS	KNN	-	98.2	99.4	-	Q1
	[20]	APSO-WOA	HPT	CNN	N/A	94.54	-	JCC= 0.9	Q1

Takeaway. According to the correlation analysis, the existing best IoT-IDSs have achieved 99.97%∼99.99% accuracy and 99.95%∼99.99% f1-score with NSL-KDD, UNSW-NB15, BoT-IoT, TON-IoT, and N-BaIoT datasets. Whereas, the performance slightly reduces while experimenting on the CICIDS-2017 and KDDCup-99 datasets (99.93%∼99.94% accuracy and f1-score). Overall, the metaheuristics and ML-integrated detection systems are effective in the IoT environment, irrespective of all widely used datasets. Another important observation is that existing intrusion detection datasets are extremely imbalanced since significant discrepancy is observed in data distribution between majority and minority classes (see Table 7).

Consequently, it is not difficult to get a remarkable accuracy from any ML classifier [150], which can mislead researchers. Therefore, "accuracy" should not be considered a trustworthy performance metric in such scenarios. In contrast, the F1-score is widely accepted as a reliable metric since it reflects the harmonic balance between precision and recall [151]. For this reason, almost all top-notch IoT-IDSs measure F1-score along with accuracy and others.

Regarding the algorithms reveals that the classification techniques, especially RF and ensemble learning, and discriminative architectures, particularly CNN models are utilized in the top-performing IoT-IDSs, considering all the datasets as a whole. We find that most of the best-performing systems employ discriminative models to identify intrusions in IoT. Additionally, classification and EL strategies are also utilized on a notable scale. Turning to metaheuristics, nature-inspired techniques are likely to be the most suitable ones since they are leveraged in more than half of the top-notch systems. However, hybridization of metaheuristics also proves to be effective in detecting intrusions in IoT. Concerning the application of these optimization techniques, in most cases, they are integrated for selecting optimal features, except in some cases of parameter and hyperparameter tuning. Figure 8 and 9 demonstrate the usage of these techniques with corresponding percentages.

Further investigation in ensemble learning classifiers reveals the efficiency of using both traditional and deep machine learning algorithms. A significant portion of these classifiers are based on classic and deep ML, such as KNN+SVM+LSTM+MLP [55], RF+DT+MLP+KNN [50], and SVM+KNN+RF+LSTM [63]. In addition, a combination of classic ML classifiers is also observed, especially RFs [111], LR+RF+XGBoost [62], DT+AdaBoost+RF [113], and OC-SVM+IF+LOF [119]. Interestingly, Latif et al. [79] leveraged a CNN-based bootstrap ensemble classifier (Generic CNN+Xception+Inception+InseptionResntV2+EffcientNetV2L). Regarding optimization techniques, there is a consistent trend of employing nature-inspired metaheuristics, specifically FOA [54, 55], MFO [62], BGWO [48], CrSA [63], GWO [50], and GA [79]. In addition to these, search-based TS [111] along with hybrid metaheuristics BGSA-BGWO [113] and LS-PIO [119] are efficient in IoT-IDS. Moreover, almost all metaheuristics are used to select features; except in [54], where modified FOA tunes hyperparameters of the XGBoost classifier.

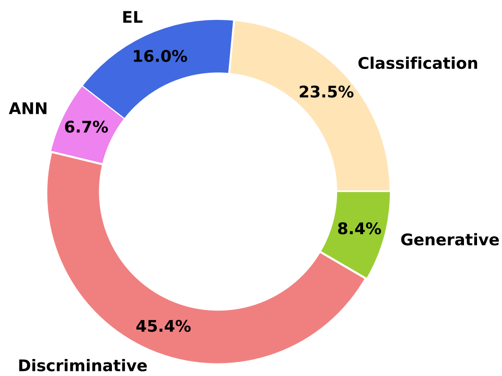

Figure 8: Usage of ML methods by the best performing IoT-IDSs.

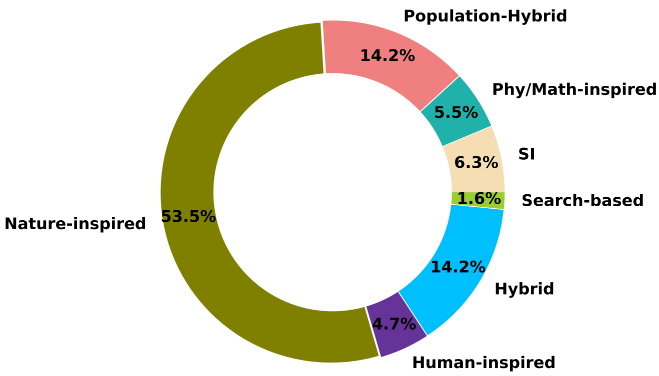

Figure 9: Usage of metaheuristics algorithms by the best performing IoT-IDSs.

5.3.2 Delve Into the Parameter and Hyperparameter Tuning Application

An in-depth analysis is conducted on the parameter and hyperparameter tuning, which are the minority but crucial applications of the metaheuristics optimization algorithms. Simultaneously, we analyze the hybrid applications too.

Parameter Tuning Takeaway. Investigating the 20 articles that employ metaheuristics algorithms for optimizing parameters of the ML models (including hybrid applications), we find that most of the systems utilize nature-inspired and swarm intelligence techniques. Interestingly, several works leverage math-inspired optimizers, especially SCA, as well as a few systems rely on human-inspired techniques like PO and SCOA. Regarding ML architectures, deep learning-based models, such as DBN, LSTM, CNN, AE, GRU are mainly employed.

However, the best performances are generated when nature-based optimizations are integrated with deep ML models (see Table 9). Specifically, CSA+HKCAE [57], and WHO+fused CNN-BiGRU [74] come up with highest accuracies (99.7%$\sim$99.9%, and 99.71%, respectively) as well as f1-scores (98.2%$\sim$98.9%, and 99.05, respectively). Apart from these IDSs, the human-inspired PO and CFNN-driven model [105] produces 99.46% accuracy and 99.76% f1-score. Importantly, all of these detection systems utilize distinct metaheuristics only for tuning the parameters. No other metaheuristics-assisted optimization is performed for feature selection or hyperparameter tuning.

Table 9: The best IoT-IDSs that have used metaheuristics for tuning parameters and hyperparameters of the machine learning models.

Parameter Optimization						Hyperparameter Optimization					
Ref	**Dataset**	**Meta.**	**ML**	**Acc (%)**	**F1 (%)**	**Ref**	**Dataset**	**Meta.**	**ML**	**Acc (%)**	**F1 (%)**
[57]	UNSW-NB15	CSA	HKCAE	99.7	98.9	[54]	UNSW-NB15	modified FOA	EL	99.98	99.99
	BoT-IoT			99.9	98.2	[50]	UNSW-NB15	GWO	EL	100	99.745
[74]	TON_IoT	WHO	fused CNN Bi-GRU	99.71	99.05		BoT-IoT			99.99	99.955
[105]	UNSW-NB15	PO	CFNN	99.46	99.76	[42]	CICIDS-2017	SSA	A-BiLSTM	99.69	98.92

Hyperparameter Tuning Takeaway. We examine the 27 works that leverage metaheuristics algorithms for optimizing the hyperparameters of the deep learning models, including hybrid applications. The hyperparameters optimized in the papers are shown in Table 10, including the leveraged metaheuristics and ML models. From the table, it can be seen that four IDSs ([115, 116, 73, 77]) utilize metaheuristics for optimizing both parameters and hyperparameters in the ML models, at a time.

Interestingly, Regarding best-performing systems, two nature-inspired and swarm-based metaheuristics are at the top. Particularly, modified FOA+EL(XGBoost) [54], GWO+EL (DT,RF,KNN, and MLP) [50], and SSA+A-BiLSTM [42] demonstrate highest accuracies (99.98%, 99.9%∼100%, and 99.69% respectively) and f1-scores (99.99%, 99.745%∼99.955%, and 98.92% respectively).

Importantly, according to Table 9, the first and second IDSs utilize the metaheuristics techniques only for hyperparameter tuning; whereas the last system simultaneously employs another nature-inspired optimizer (GJOA) to select an optimal feature set (hybrid application). Thus we observe hyperparameter tuning as a separate and hybrid application of the metaheuristics utilized in the top-performing IoT-IDSs. Another interesting finding is that the hybrid optimization technique is applied to a discriminative deep learning architecture; whereas the standalone hyperparameter tuning is employed to the ensemble classifiers.

Table 10: List of hyperparameters optimized by the metaheuristics in the related works. "—" indicates that hyperparameters are not explicitly stated in the papers.

Ref	Hyperparameters	ML	Metaheuristics
[54]	learning rate, min_child_weight, subsample, collsample_bytree, max_depth, gamma	KNN, XGBoost	modified FOA
[38]	learning rate, momentum, decay, dropout rate, number of hidden layers, numbers of neurons of hidden layers, number of epochs, batch size, optimizer, initialization function, layer type, activation function	DNN, LSTM-RNN, DBN	double PSO
[115]	(PT+HPT) number of hidden layers, neurons of each layer, weights	RdNN	GAO-AOA
[127]	Gamma (kernel coefficient parameter), C (the amount of regularization applied to the data)	SVM	GWO
[109]	—	IoT2Vec	ABF

Continued on next page

Table 10 – *Continued from previous page*

Ref	Hyperparameters	ML	Metaheuristics
[20]	number of convolutional kernels, length of convolutional filter, activation functions in the convolutional layer, probability of nodes used between the convolutional and second layers, number of second-layer neurons, activation functions in the second layer, number of third-layer neurons, activation functions in the third layer, batch sample size, learning rate	CNN	APSO-WOA
[116]	(PT+HPT) number of hidden nodes, input weighted, biases, C^+ for minority positive instances, C^- for most negative instances	CCR-ELM	SCA
[98]	learning rate, number of epochs, batch size	EL	LCWOA
[106]	k (Number of Neighbors), distance weight (w_k)	kNN	Compact SCA
[73]	(PT+HPT) weights, biases, regularization value, number of neurons, type of activation function	RWNN	GWO, PSO, MVO
[82]	batch size, learning rate	FR-CNN	GA
[132]	number of hidden neurons	ANN	SHO
[21]	—	CRNN	HS
[59]	earning rate, number of hidden layers, input weights, epochs	GRU	WOA
[39]	learning rate, input units, batch size, dropout, epochs, activation function, layers number, optimizer, units of hidden layer	DNN	modified PSO
[76]	number of suitable hidden neurons of DNN, iterations of Adaboost, number of suitable bootstrap in the random forest	HR-OELM	AF-EFO
[61]	learning rate, sample sampling rate (subsample), maximum depth of the tree	XGBoost	WOA
[22]	—	EL	TuSO
[99]	—	HDL	Enhanced BWO
[49]	num_wolves, min range, max range, initial population, crossover rate, num_qubits, depth, max fun, shots	QSVM	Improved GWO (IGWO)
[50]	—	EL	GWO
[42]	learning rate, activation, epochs, dropout rate, batch size	A-BiLSTM	SSA
[77]	(PT+HPT) weights and training parameters	DMN	ROA
[78]	learning rate, dropout, batch size, epoch count, activation function	DBN	SpSO
[40]	(XGBoost): learning rate, min child weight, subsample, colsample by tree, max depth, gamma (KNN): k, weights, distance	XGBoost and KNN	GSAPSO

Continued on next page

Table 10 – *Continued from previous page*

Ref	Hyperparameters	ML	Metaheuristics
[79]	optimizer, activation function, dense units, dropout, fine-tune layers, epochs	EL	GA
[75]	—	CNN+LSTM	ALO, FPA

5.4 *RQ4: What are open issues raised by the integration of metaheuristics with ML in IoT-IDS?*

Though metaheuristics and ML-integrated algorithms bring about significant evolution in the development of detection systems, there are still some issues and challenges that have to be addressed soon.

- **Resource-constrained issue of IoT devices.** The most critical issue in the development of the IoT-IDS is the dynamic and heterogeneous characteristics of its ecosystem. IoT supports different large-scale networks with distinct communication protocols and applications, which have individual abilities and conditions. Moreover, the data has various degrees of complexities ranging from a simple sensor for observing blood pressure to a complex full-duplex video feed. Moreover, some devices build up with multiple sensors, for example, a smartphone has sensors like GPS, camera, fingerprinting, etc. Consequently, ensuring the security of this diverse IoT environment is an extremely challenging task. Even, there is no such evidence that the integration of metaheuristics and ML methods always guarantees to protect against all types of attacks. Besides, the hybridization of multiple methods imposes a severe effect on the computational power and energy resources. Additionally, though a few works are dedicated to healthcare and industrial IoT, the amount is too insufficient considering the importance of sensitive data protection and the new era of "Industry 4.0". Moreover, it is indeed necessary to design unique IDSs for ITS, Internet of Medical Things (IoMT), Internet of Agriculture (IoA), Internet of Vehicle (IoV), and Internet of Done (IoD) by employing optimization-assisted ML techniques.

- **Issues regarding datasets.** Most of the datasets, used in the existing papers, were created before 2020 (NSL-KDD: 2009, UNSW-NB15: 2015, BoT-IoT: 2019, CICIDS-2017: 2017, and KDDCup-99: 1999), which lack the features of the latest sophisticated attacks. Consequently, a question arises whether the existing techniques that integrate metaheuristics and ML, can detect these new intrusions or not. Alarmingly, there are not sufficient IoT-IDS datasets that contain the features or attributes of new intrusions, especially those generated after 2020. Moreover, the well-known widely used intrusion detection datasets are imbalanced, which can severely affect machine learning models. Furthermore, in the papers, experiments are conducted in lab settings. As a result, the correctness and effectiveness of the existing algorithms in real-world scenarios are arguably a critical issue.

- **Amount and quality of the selected features.** Surprisingly, most of the IoT-IDS papers have not clearly stated the features that are selected by the metaheuristics. As a result, it becomes much more difficult to analyze the correctness and effectiveness of the optimization techniques. Additionally, introducing these features would give an intuition on which features are crucial for developing a generalized IDS in IoT. Moreover, though the ultimate classification results are supposed to indicate the validity of the algorithms, it does not necessitate proof of whether these optimization techniques have any impact or not. A possible solution could be the analysis of individual IDSs with and without applying those metaheuristics. Regrettably, these tactics are almost missing in the literature. Furthermore, maintaining a decent balance between the quality and quantity of the selected features is another vital issue in the IoT context.

- **Appropriate selection of parameters and hyperparameters.** The optimization of the parameters, in both classical ML and deep learning architectures, is another important thing of consideration while implementing an IoT-IDS. Especially, in neural networks, the optimal choice of parameters like weights and biases plays a pivotal role in enhancing the performance of the detection system. Additionally, a few works also utilized tuning the hyperparameters, such as learning rate, number of layers, neuron volume, number of epochs, regularization value, type of activation function, etc. of different deep neural networks, such as DBN, RNN, GRU, CNN, and LSTM. Therefore, working with inappropriate and less significant variables can result in utmost failure of classifying attacks. Although several works claimed to generate excellent accuracy through optimizing these parameters and hyperparameters, there is a crucial lack of dedicated analysis on them.

- **Issues regarding ML methods.** To improve classification performance, combining the advantages of multiple ML algorithms can be a promising approach. Though some research has already utilized this, more advanced techniques must be applied to keep the computational overhead in control, maintaining all security requirements since IoT devices can only operate with low power and limited resources. Another challenging thing is to make the proposed IDSs capable of analyzing real-time traffic. Alarmingly, most of the models in the literature are typically offline, that is, they are trained on different datasets and are tested on real-time data. Consequently, they need to retrain periodically, which is time-consuming and expensive. Considering the IoT environment, where the data are diverse and dynamically evolve over time, these traditional static IDSs are not sufficient in real-world big-data applications, especially at the enterprise level. In this case, incremental learning can be a viable solution [152], where the system dynamically learns continuously added features that were previously unknown. In [153], an online IDS is proposed for the dynamic distributed network. Specifically, at first, a local parameterized detection model is constructed in each node using the online Adaboost algorithm. Then, all of the local models are combined using PSO-based and SVM-driven algorithms to generate a global detection model, which achieves 99.99% accuracy and 0.37% FAR. Wahab et al. [154] devise a technique to adjust the size of the DNN's hidden layers in an online manner so that the model can continuously learn and adapt new intrusions, and update predictions dynamically. The experimental evaluation states that their online DNN surpasses the static one in terms of false positives and false negatives by 6% and 4.5%, respectively.

5.5 *RQ5: What are the unexplored metaheuristics optimization algorithms for IDS in IoT?*

In this section, some possible optimization techniques are discussed that can be utilized for either feature selection, parameter, or hyperparameter optimization.

- **Microbiology-inspired metaheuristics.** These types of optimization techniques rely on the life cycle, immune system, social behavior, and collective behavior of viruses, bacteria, and other microorganisms. For example, the bacterial foraging optimization algorithm (BFOA) [155], bacterial swarming algorithm (BSA), bacterial-GA foraging (BF), and quantum-inspired bacterial swarming optimization (QBSO) are some popular techniques of this category. Interestingly, a few metaheuristics are based on the replication and herd immunity concept of the coronavirus, known as coronavirus herd immunity optimizer (CHIO) [156], and coronavirus optimization algorithm (COVIDOA). Other well-known microbiology-driven techniques are sperm swarm optimization algorithm (SSO), swine influenza models-based optimization (SIMBO), and symbiosis organisms search (SOS). No IoT-IDS is found to utilize any of these algorithms. However, a chaotic bacterial colony optimization (CBCO) technique is utilized for tuning the weights, biases, and number of neurons of the Elman recurrent neural network (ERNN), hence generalizing the model's performance [157]. As a result, the proposed IoT DDoS attack detection system surpasses other related systems. In [158], an improved bacterial foraging optimization is employed for feature selection in the smart city anomaly detection system. Specifically, the classic BFOA is enhanced using the simulated annealing technique by incorporating decisions based on probability to achieve better convergence to the global optima and to handle the local extrema. However, a Bayesian optimization algorithm is applied to tune the hyperparameters of the multiplicative long short-term memory (MLSTM) model. The experimental evaluations show that IBFOA provides better classification accuracy with less computational complexity. Since these works are related to the intrusion detection system, microbiology-inspired metaheuristics can be a good choice to test in the IoT-IDS environment with diverse ML models.

- **Chemistry-based metaheuristics.** Though many physics and math-based metaheuristics are utilized for developing robust IoT-IDSs, we find no chemistry-inspired algorithms, adopting the concepts of chemical reactions and laws, such as molecular reaction, motion, radiation, etc. Kinetic gas molecules optimization (KGMO) [159], artificial chemical reaction optimization algorithm (ACROA), and ions motion optimization algorithm (IMOA) are well-established optimization algorithms of this category. Intuitively, these algorithms can produce excellent performances like physics and math-inspired ones. However, these metaheuristics have been applied to other domains, such as cyber-physical systems [160], clustering and routing algorithms in WSN [161], clustering in big data environment [162], etc. Asha and Gowrishankar

[161] utilize glowworm swarm optimization (GSO) and kinetic gas molecule optimization (KGMO) to increase network lifetime and number of transmissions in WSN. This hybrid energy-efficient algorithm outperforms the existing PSO-PSO-WSN and PSO-GSO-WSN. Moreover, KGMO generally offers fast convergence and is suitable for complex real-world optimization tasks. In [162], an extended CRO (real-coded CRO) is employed to find the optimal clusters for fuzzy clustering. Consequently, the false negative activities are reduced significantly compared to the earlier models (e.g., SVM, NB, DT, RF, and FCM). Besides, the accuracy and convergence speed are improved, especially in the big data environment. based on these remarkable outcomes in various domains, chemistry-based metaheuristics can be integrated into IoT-IDSs.

- **Miscellaneous metaheuristics.** Some other popular metaheuristics are inspired by the sunflower behavior to find the best orientation towards the sun (sunflower optimization (SFO) [163]), players' intelligence to find the best position to score a goal (football game optimization (FGO)), optimization inspired from mother's care for her children [164] and the trading method of the stock exchanges (exchange market algorithm (EMA) [165]). Recently, Prashanth et al. [166] have devised an efficient routing technique for wireless sensor networks through load balancing by an SFO. While compared with the existing approaches (e.g., CRCGA, GECR, OMPFM, and GADA-LEACH), the optimization demonstrates better results considering packet delivery ratio, packet loss, throughput, average residual energy, and delay. Taking the similar characteristics (like resource-constrainedness) of both WSN and IoT, this variant of optimization algorithms can be a suitable solution for IoT-IDSs.

- **Metaheuristics and GAN-based Detection Systems.** Generative Adversarial Network (GAN) is one of the most popular detection methods regarding the development of an IDS [167]. Particularly, it facilitates synthetic data creation and better learning of the minority classes. Moreover, it can generate samples faster than DL methods, and is capable of identifying zero-day attacks in IoT since it learns from a wide range of attack scenarios [168]. Ferdowsi and Saad [167] develop a GAN-based distributed IDS to identify malicious activities, independent of a centralized controlling process. They utilize different ANNs for both the generator and discriminator. Recently, Rahman et al. [169] propose a GAN-based NIDS, called SYN-GAN, aiming to handle the disproportion in the existing imbalance datasets and mimic the real-world network intrusion data. Notably, the model demonstrates 91%, 84%, and 100% accuracy in the UNSW-NB15, NSL-KDD, and BoT-IoT datasets, respectively. However, GAN faces difficulties while training with high dimensional data since the developed generator and discriminator are often complex and unstable [170]. Incorporating metaheuristics with GAN can be a promising solution to resolve these issues since these optimizers have already proved efficient in feature selection, parameter optimization, and hyperparameter tuning phases. Researchers, focusing on implementing IoT-IDSs, can get insight from the work [171, 172], where GAN is integrated with different optimization techniques like war strategy optimization (WSO), gazelle optimization algorithm (GOA), and archerfish hunting optimizer (AHOA), etc. for parameter tuning and feature selection, resulting in an improved performance in the attack classification process. Though these works integrate GAN and metaheuristics in WSN and cloud, they do not solely focus on the IoT environment. Considering the scale, uniqueness, and difficulties of the IoT ecosystem, as well as the necessity of the metaheuristics and ML-integrated IoT-IDSs (as described in Section 1), we recommend applying GAN and these optimization techniques to develop IoT-IDSs.

6 Discussions

The Internet of Things (IoT) environment consists of a diverse range of sensitive and private data from various devices and sensors. Besides, the wide variety of protocols, technologies, and platforms make IoT more heterogeneous, complicated, and dynamic. Traditional intrusion detection systems, relying on specific rules, statistics, or heuristics often fail to identify these complex patterns of the IoT ecosystem. To overcome these problems, researchers have focused on machine learning-driven IDSs, especially for IoT. However, these methods come up with new problems, such as the requirement of high computational resources and significant time consideration for a small precision improvement. Moreover, the emerging trend of de-centralized edge computing technology-based IoT-IDSs faces challenges, for example, limited computing power and inadequate energy support, which are unavoidable requirements for the training and testing of ML models using large datasets. For these reasons, in recent years, a growing trend of utilizing optimization techniques, especially metaheuristics algorithms can be seen to select optimal features and tune parameters or hyperparameters in the ML-based IoT-IDSs.

Considering the recent trends and the significance of leveraging optimization and ML techniques, this study presents a systematic literature review on the metaheuristics and machine learning-integrated intrusion detection systems for IoT. The review includes 111 relevant papers, of which 96 are high-quality journal articles (51.8% Q1 and 28.6% Q2), and covers almost every recent optimization technique utilized for IoT-IDSs. The distinct analysis of different applications, such as feature selection, parameter, and hyperparameter tuning as well as hybrid applications has technically enriched this work. Our extensive investigation reveals that the majority of the systems (74.3%) apply these optimizers for selecting an optimal set of features from the popular public datasets. Simultaneously, a notable amount of works focus on tuning different parameters (e.g., weights and biases) of machine learning models and hyperparameters like learning rate, batch size, number of hidden layers, number of neurons, number of epochs, dropout rate, activation function, etc. are also optimized by some systems.

Apart from these, we also discover that most of the high-performing relevant detection systems leverage hybrid metaheuristics. Moreover, well-established ML classifiers like RF, KNN, and EL are employed significantly to identify various types of attacks. Regarding deep learning models, different discriminative architectures, for instance, CNN, DBN, and LSTM have demonstrated remarkable results. One of the severe drawbacks of these systems is the use of comparatively older and imbalanced datasets. Consequently, they lack the features of the latest attacks. Furthermore, the majority of the articles in the literature lack a dedicated analysis of the selected features, parameters, and hyperparameters that influence IDSs' performance; even in most of the cases, the selected or optimized set are not mentioned explicitly. Moreover, the existing systems operate in offline mode with specific datasets, which may drastically fail in real-world scenarios where traffic behaviors are extremely varied. To address these challenges, the dynamically updated features need to be trained continuously as done in the incremental learning. Moreover, we suggest integrating metaheuristics with GAN to perform optimum feature selection, keeping the IoT constraints and security conditions consistent.

Multimodal data processing has gained significant momentum with the advent of alignment models, particularly vision-language models, which excel at creating efficient vector-based data structures for storage, retrieval, and utilization. This is especially beneficial in IoT applications where resources such as processing power and memory are limited. Real-time detection leveraging edge and fog computing has also advanced, providing scalable solutions while minimizing latency. Multimodal approaches are crucial for managing diverse datasets and reducing false positives [173, 174, 175]. Emerging research directions include privacy-preserving federated learning, which enables decentralized model training while safeguarding data privacy, and explainable AI, which enhances trust by making IDS outputs interpretable. Additionally, quantum-inspired optimization is being explored for faster convergence, and multi-objective optimization aims to balance detection accuracy, latency, and energy efficiency in IoT environments. In addition, metaheuristic algorithms can provide an alternative to the neural architecture search algorithms for constructing hybrid novel deep learning models, handling multi-objective optimization problems, etc.

7 Conclusion

Considering the importance and recent widespread use of metaheuristics algorithms in developing machine learning-based intrusion detection systems, we aim to technically analyze the existing integrated IoT-IDS models in this study. Specifically, we have investigated the metaheuristics-assisted and machine learning-driven systems, categorizing them into various applications like feature selection, parameter optimization, and hyperparameter tuning. One of the significant findings of this review is the establishment of hidden relations between top-notch optimization techniques and ML architectures concerning the most used datasets. Moreover, the introduction of a large-scale visualized taxonomy of these integrated IoT-IDSs, also adds value to the literature. In the end, several technical issues of metaheuristics and ML integration are discussed and some insightful directions are proposed to address these challenges in the coming days.

List of Acronyms

Abbr.	Elaboration	Abbr.	Elaboration
AAFSO	Assimilated Artificial Fish Swarm Optimization	ABC	Artificial Bee Colony
ABF	Activity-based Footprinting	A-BiLSTM	Attention-based Bidirectional LSTM
ACO	Ant Colony Optimization	AE	Auto Encoder
ALO	Ant Lion Optimization	ANN	Artificial Neural Network
AOA	Arithmetic Optimization Algorithm	APSO	Adaptive Particle Swarm Optimization
AQUO	Aquila optimizer	ASO	Atom Search Optimization
BA	Bat algorithm	BAS	Beetle Antenna Search
BBFA	Binary Bee Foraging Algorithm	BBO	Biogeography-based Optimization
BCOA	Binary Chimp Optimization Algorithm	BES	Bald Eagle Search
BGSA	Binary Gravitational Search Algorithm	BGWO	Binary Grey Wolf Optimization
BHO	Black Hole Optimization	Bi-GRU	Bidirectional Gated Recurrent Unit
BiLSTM	Bidirectional Long-Short Term Memory	BOA	Butterfly Optimization Algorithm
BQABC	Binary Quantum-inspired ABC	BSA	Bird Swarms Algorithm
BWO	Black Widow Optimization	CCSO	Chimp Chicken Swarm Optimization
CD	Canberra Distance	CFNN	Cascade Forward Neural Network
ChSO	Chicken Swarm Optimization	CNN	Convolutional Neural Network
COA	Chimp Optimization Algorithm	CRNN	Cascaded Recurrent Neural Network
CrSA	Crow Search Algorithm	CSA	Capuchin Search Algorithm
CSSA	Chaotic Salp Swarm Optimization	CVS	Chaotic Vortex Search
DBN	Deep Belief Network	DBRBF	Descriptive Back Propagated RBF
DCNN	Deep CNN	DDT	Distance Decision Tree
DE	Differential Evaluation	DFWA	Dynamic Search Fireworks Optimization
DHOA	Deer Hunting Optimization Algorithm	DL	Deep Learning
DLHNN	Deep Learning-based Hybrid NN	DMN	Deep Maxout Network
DRFO	Decisive Red Fox Optimization	DT	Decision Tree
DTO	Dipper Throated Optimization	DWNN	Deep Wavelet Neural Network
EA	Evolutionary Algorithm	EBSA	Evaluated Bird Swarm Optimization
EFO	Electric Fish Optimization	EGB	Extreme Gradient Boosting
EL	Ensemble Learning	ELM	Extreme Learning Machine
EO	Equilibrium Optimization	EPC	Emperor Penguin Colony
ET	Extremely Randomized Trees or Extra Trees	FDM	Fractional Derivative Mutation
FL	Federated Learning	FLN	Fast-Learning Network
FNN	Feed-forward Neural Network	FOA	Firefly Optimization Algorithm
GA	Genetic Algorithm	GAO	Grasshopper Optimization
GJOA	Golden Jackal Optimization Algorithm	GO	Growth Optimizer
GRU	Gate Recurrent Unit	GSO	Glow-Worm Swarm Optimization

Abbr.	**Elaboration**	**Abbr.**	**Elaboration**
GTO	Gorilla Troops Optimizer	GWO	Grey-Wolf Optimization
HCSGA	Hybrid Chicken Swarm Genetic Algorithm	HDL	Hybrid Deep Learning
HHO	Harris Hawk Optimization	HKCAE	Capsule AE with a Hybrid Kernel function
HMS	Human Mental Search	HNM	Hierarchical Network Model
HPSO	Hierarchical Particle Swarm Optimization	HR-OELM	High Ranking-based Optimized EL
HS	Harmony Search	HSHO	Harmony Search Hawks Optimization
IAOA	Improved Arithmetic Optimization Algorithm	IBGJO	Improved Binary Golden Jackal Optimization
IGC	Information Gain Calculation	IoT	Internet of Things
IDS	Intrusion Detection System	ITS	Intelligent Transportation Systems
IWD	Intelligent Water Drop	KELM	Kernel Extreme Machine Learning Model
KNN	K-Nearest Neighbor	LAANN	Look Ahead Artificial Neural Network
LCWOA	Lévy-fight Chaotic Whale Optimization Algorithm	LOA	Lion Optimization Algorithm
LR	Linear Regression	LS	Local Search
LSTM	Long Short-Term Memory	MDSVM	Mahalanobis Distance SVM
MFO	Moth–Flame Optimization	ML	Machine Learning
MOA	Mayfly Optimization Algorithm	MOPSO	Multi-Objective Particle Swarm Optimization
MPO	Marine Predator Optimization	MSO	Moth Search Optimization
MVO	Multi-Verse Optimizer	NS	Neighborhood Search
OBL	Opposition-based Learning	PCA	Principal Component Analysis
PDO	Prairie Dog Optimization	PIO	Pigeon-inspired Optimization
PO	Political Optimizer	PM	Polymorphic Mutation
PSO	Particle Swarm Optimization	QCSO	Quantum Cat Swarm Optimization
QPSO	Quantum Behaved Particle Swarm Optimization	QSVM	Quantum Support Vector Machine
RBFNN	Radial Basis Function Neural Network	RBM	Restricted Boltzmann machine
RdNN	Random Neural Network	RF	Random Forest
RKOA	Red Kite Optimization Algorithm	RL	Reinforcement Learning
RNN	Recurrent Neural Network	ROA	Remora Optimization Algorithm
RSA	Reptile Search Algorithm	RWNN	Random Weight Neural Network
SA	Simulated Annealing	SAEHO	Seagull Adapted Elephant Herding Optimization
SCA	Sine Cosine Algorithm	SCOA	Social Group Optimization Algorithm
SCSO	Sand Cat Swarm Optimizer	SHO	Spotted Hyena Optimization
SMO	Spider Monkey Optimization	SpSO	Sparrow Search Optimization
SSA	Salp Swarm Algorithm	SSO	Shuffled Shepherd Optimization
STFA	Sea Turtle Foraging Algorithm	SU-CMO	Self-Upgraded Cat and Mouse Optimizer
SVM	Support Vector Machine	TLBO	Teaching-Learning-based Optimization

Abbr.	Elaboration	Abbr.	Elaboration
TS	Tabu Search	TSO	Transient Search Optimization
TuSO	Tuna Swarm Optimization	VAE	Variational Autoencoder
WHO	Wild Horse Optimization	WMSA	Water Moth Search algorithm
WOA	Whale Optimization Algorithm	WWO	Water Wave optimization

References

[1] Laith Abualigah, Ali Diabat, Putra Sumari, and Amir H Gandomi. Applications, deployments, and integration of internet of drones (iod): a review. *IEEE Sensors Journal*, 21(22):25532–25546, 2021.

[2] Manos Antonakakis, Tim April, Michael Bailey, Matt Bernhard, Elie Bursztein, Jaime Cochran, Zakir Durumeric, J Alex Halderman, Luca Invernizzi, Michalis Kallitsis, et al. Understanding the mirai botnet. In *26th USENIX security symposium (USENIX Security 17)*, pages 1093–1110, 2017.

[3] Erin Dooley. Adt technician pleads guilty to hacking home security footage. https://www.justice.gov/usao-ndtx/pr/adt-technician-pleads-gu- ilty hacking-home-security-footage.

[4] Heba F Eid, Aboul Ella Hassanien, Tai-hoon Kim, and Soumya Banerjee. Linear correlation-based feature selection for network intrusion detection model. In *Advances in Security of Information and Communication Networks: First International Conference, SecNet 2013, Cairo, Egypt, September 3-5, 2013. Proceedings*, pages 240–248. Springer, 2013.

[5] Trevor Hastie, Robert Tibshirani, and Ryan J Tibshirani. Extended comparisons of best subset selection, forward stepwise selection, and the lasso. *arXiv preprint arXiv:1707.08692*, 2017.

[6] Yap Bee Wah, Nurain Ibrahim, Hamzah Abdul Hamid, Shuzlina Abdul-Rahman, and Simon Fong. Feature selection methods: Case of filter and wrapper approaches for maximising classification accuracy. *Pertanika Journal of Science & Technology*, 26(1), 2018.

[7] Tansel Dokeroglu, Ayça Deniz, and Hakan Ezgi Kiziloz. A comprehensive survey on recent metaheuristics for feature selection. *Neurocomputing*, 494:269–296, 2022.

[8] Sachin Desale, Akhtar Rasool, Sushil Andhale, and Priti Rane. Heuristic and meta-heuristic algorithms and their relevance to the real world: a survey. *Int. J. Comput. Eng. Res. Trends*, 351(5):2349–7084, 2015.

[9] Naoual El Aboudi and Laila Benhlima. Review on wrapper feature selection approaches. In *2016 International Conference on Engineering & MIS (ICEMIS)*, pages 1–5, 2016.

[10] Subrato Bharati and Prajoy Podder. Machine and deep learning for iot security and privacy: applications, challenges, and future directions. *Security and communication networks*, 2022(1):8951961, 2022.

[11] Haochen Hua, Yutong Li, Tonghe Wang, Nanqing Dong, Wei Li, and Junwei Cao. Edge computing with artificial intelligence: A machine learning perspective. *ACM Computing Surveys*, 55(9):1–35, 2023.

[12] Wei Yu, Fan Liang, Xiaofei He, William Grant Hatcher, Chao Lu, Jie Lin, and Xinyu Yang. A survey on the edge computing for the internet of things. *IEEE access*, 6:6900–6919, 2017.

[13] Saif S Kareem, Reham R Mostafa, Fatma A Hashim, and Hazem M El-Bakry. An effective feature selection model using hybrid metaheuristic algorithms for iot intrusion detection. *Sensors*, 22(4):1396, 2022.

[14] Reem Alkanhel, El-Sayed M El-kenawy, Abdelaziz A Abdelhamid, Abdelhameed Ibrahim, Manal Abdullah Alohali, Mostafa Abotaleb, and Doaa Sami Khafaga. Network intrusion detection based on feature selection and hybrid metaheuristic optimization. *Computers, Materials & Continua*, 74(2), 2023.

[15] P Sanju. Enhancing intrusion detection in iot systems: A hybrid metaheuristics-deep learning approach with ensemble of recurrent neural networks. *Journal of Engineering Research*, 11(4):356–361, 2023.

[16] Ajay Kaushik and Hamed Al-Raweshidy. A novel intrusion detection system for internet of things devices and data. *Wirel. Netw.*, 30(1):285–294, aug 2023.

[17] Dijana Jovanovic, Marina Marjanovic, Milos Antonijevic, Miodrag Zivkovic, Nebojsa Budimirovic, and Nebojsa Bacanin. Feature selection by improved sand cat swarm optimizer for intrusion detection. In *2022 International Conference on Artificial Intelligence in Everything (AIE)*, pages 685–690. IEEE, 2022.

[18] Sahba Baniasadi, Omid Rostami, Diego Martín, and Mehrdad Kaveh. A novel deep supervised learning-based approach for intrusion detection in iot systems. *Sensors*, 22(12):4459, 2022.

[19] B Jothi and M Pushpalatha. Wils-trs—a novel optimized deep learning based intrusion detection framework for iot networks. *Personal and Ubiquitous Computing*, 27(3):1285–1301, 2023.

[20] Ahmed Bahaa, Abdalla Sayed, Laila Elfangary, and Hanan Fahmy. A novel hybrid optimization enabled robust cnn algorithm for an iot network intrusion detection approach. *Plos one*, 17(12):e0278493, 2022.

[21] Mohammed Basheri and Mahmoud Ragab. Quantum cat swarm optimization based clustering with intrusion detection technique for future internet of things environment. *Computer Systems Science & Engineering*, 46(3), 2023.

[22] P Vijayan and S Sundar. Original research article iot intrusion detection system using ensemble classifier and hyperparameter optimization using tuna search algorithm. *Journal of Autonomous Intelligence*, 7(2):1–10, 2024.

[23] Robert Mitchell and Ing-Ray Chen. A survey of intrusion detection techniques for cyber-physical systems. *ACM Computing Surveys (CSUR)*, 46(4):1–29, 2014.

[24] Yulong Fu, Zheng Yan, Jin Cao, Ousmane Koné, and Xuefei Cao. An automata based intrusion detection method for internet of things. *Mobile Information Systems*, 2017(1):1750637, 2017.

[25] Daniele Midi, Antonino Rullo, Anand Mudgerikar, and Elisa Bertino. Kalis—a system for knowledge-driven adaptable intrusion detection for the internet of things. In *2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS)*, pages 656–666. IEEE, 2017.

[26] Bastien Chopard and Marco Tomassini. *An introduction to metaheuristics for optimization*. Springer, 2018.

[27] Zhavat Sherinov and Ahmet Ünveren. Multi-objective imperialistic competitive algorithm with multiple non-dominated sets for the solution of global optimization problems. *Soft Computing*, 22(24):8273–8288, 2018.

[28] Laith Abualigah, Ali Diabat, Seyedali Mirjalili, Mohamed Abd Elaziz, and Amir H Gandomi. The arithmetic optimization algorithm. *Computer methods in applied mechanics and engineering*, 376:113609, 2021.

[29] Seyedali Mirjalili. Sca: a sine cosine algorithm for solving optimization problems. *Knowledge-based systems*, 96:120–133, 2016.

[30] Gunnar W Klau, Neal Lesh, Joe Marks, and Michael Mitzenmacher. Human-guided search. *Journal of Heuristics*, 16:289–310, 2010.

[31] Wengui Hu, Qingsong Cao, Mehdi Darbandi, and Nima Jafari Navimipour. A deep analysis of nature-inspired and meta-heuristic algorithms for designing intrusion detection systems in cloud/edge and iot: state-of-the-art techniques, challenges, and future directions. *Cluster Computing*, pages 1–27, 2024.

[32] Rafika Saadouni, Chirihane Gherbi, Zibouda Aliouat, Yasmine Harbi, and Amina Khacha. Intrusion detection systems for iot based on bio-inspired and machine learning techniques: a systematic review of the literature. *Cluster Computing*, pages 1–27, 2024.

[33] Dukka Karun Kumar Reddy, Janmenjoy Nayak, HS Behera, Vimal Shanmuganathan, Wattana Viriyasitavat, and Gaurav Dhiman. A systematic literature review on swarm intelligence based intrusion detection system: past, present and future. *Archives of Computational Methods in Engineering*, 31:1–68, 03 2024.

[34] Shubhkirti Sharma, Vijay Kumar, and Kamlesh Dutta. Multi-objective optimization algorithms for intrusion detection in iot networks: A systematic review. *Internet of Things and Cyber-Physical Systems*, 4:258–267, 2024.

[35] Arash Heidari and Mohammad Ali Jabraeil Jamali. Internet of things intrusion detection systems: a comprehensive review and future directions. *Cluster Computing*, 26(6):3753–3780, 2023.

[36] Abhishek Verma and Virender Ranga. Machine learning based intrusion detection systems for iot applications. *Wireless Personal Communications*, 111(4):2287–2310, 2020.

[37] Somayye Hajiheidari, Karzan Wakil, Maryam Badri, and Nima Jafari Navimipour. Intrusion detection systems in the internet of things: A comprehensive investigation. *Computer Networks*, 160:165–191, 2019.

[38] Wisam Elmasry, Akhan Akbulut, and Abdul Halim Zaim. Evolving deep learning architectures for network intrusion detection using a double pso metaheuristic. *Computer Networks*, 168:107042, 2020.

[39] Yakub Kayode Saheed, Aisha Abubakar Usman, Favour Dirwokmwa Sukat, and Muftahu Abdulrahman. A novel hybrid autoencoder and modified particle swarm optimization feature selection for intrusion detection in the internet of things network. *Frontiers in Computer Science*, 5:997159, 2023.

[40] Pavle Dakic, Miodrag Zivkovic, Luka Jovanovic, Nebojsa Bacanin, Milos Antonijevic, Jelena Kaljevic, and Vladimir Simic. Intrusion detection using metaheuristic optimization within iot/iiot systems and software of autonomous vehicles. *Scientific Reports*, 14(1):22884, 2024.

[41] A Biju and S Wilfred Franklin. Evaluated bird swarm optimization based on deep belief network (ebso-dbn) classification technique for iot network intrusion detection. *Automatika*, 65(1):108–116, 2024.

[42] Nojood O Aljehane, Hanan Abdullah Mengash, Majdy M Eltahir, Faiz Abdullah Alotaibi, Sumayh S Aljameel, Ayman Yafoz, Raed Alsini, and Mohammed Assiri. Golden jackal optimization algorithm with deep learning assisted intrusion detection system for network security. *Alexandria Engineering Journal*, 86:415–424, 2024.

[43] C Prajisha and AR Vasudevan. An efficient intrusion detection system for mqtt-iot using enhanced chaotic salp swarm algorithm and lightgbm. *International Journal of Information Security*, 21(6):1263–1282, 2022.

[44] Milos Stankovic, Milos Antonijevic, Nebojsa Bacanin, Miodrag Zivkovic, Marko Tanaskovic, and Dijana Jovanovic. Feature selection by hybrid artificial bee colony algorithm for intrusion detection. In *2022 International Conference on Edge Computing and Applications (ICECAA)*, pages 500–505. IEEE, 2022.

[45] Chintam Anusha, A Sravani, Jetti Anusha, Choudari Lakshmi, and Gantla Santoshi Kumari. Intrusion detection system in iot network by using metaheuristic algorithm with machine learning dimensional reduction technique. In *2022 3rd International Conference on Computing, Analytics and Networks (ICAN)*, pages 1–6. IEEE, 2022.

[46] Bhushan Deore and Surendra Bhosale. Hybrid optimization enabled robust cnn-lstm technique for network intrusion detection. *Ieee Access*, 10:65611–65622, 2022.

[47] S Vanitha and P Balasubramanie. Improved ant colony optimization and machine learning based ensemble intrusion detection model. *Intelligent Automation & Soft Computing*, 36(1), 2023.

[48] Bayi Xu, Lei Sun, Xiuqing Mao, Ruiyang Ding, and Chengwei Liu. Iot intrusion detection system based on machine learning. *Electronics*, 12(20):4289, 2023.

[49] EI Elsedimy, Hala Elhadidy, and Sara MM Abohashish. A novel intrusion detection system based on a hybrid quantum support vector machine and improved grey wolf optimizer. *Cluster Computing*, pages 1–19, 2024.

[50] Yakub Kayode Saheed and Sanjay Misra. A voting gray wolf optimizer-based ensemble learning models for intrusion detection in the internet of things. *International Journal of Information Security*, 23(3):1557–1581, 2024.

[51] MD Moizuddin and M Victor Jose. A bio-inspired hybrid deep learning model for network intrusion detection. *Knowledge-based systems*, 238:107894, 2022.

[52] Swarna Priya RM, Praveen Kumar Reddy Maddikunta, M Parimala, Srinivas Koppu, Thippa Reddy Gadekallu, Chiranji Lal Chowdhary, and Mamoun Alazab. An effective feature engineering for dnn using hybrid pca-gwo for intrusion detection in iomt architecture. *Computer Communications*, 160:139–149, 2020.

[53] Azam Davahli, Mahboubeh Shamsi, and Golnoush Abaei. A lightweight anomaly detection model using svm for wsns in iot through a hybrid feature selection algorithm based on ga and gwo. *Journal of Computing and Security*, 7(1):63–79, 2020.

[54] Nikola Savanović, Ana Toskovic, Aleksandar Petrovic, Miodrag Zivkovic, Robertas Damaševičius, Luka Jovanovic, Nebojsa Bacanin, and Bosko Nikolic. Intrusion detection in healthcare 4.0 internet of things systems via metaheuristics optimized machine learning. *Sustainability*, 15(16):12563, 2023.

[55] Rekha Gangula, Murali Mohan Vutukuru, and M Ranjeeth Kumar. Intrusion attack detection using firefly optimization algorithm and ensemble classification model. *Wireless Personal Communications*, 132(3):1899–1916, 2023.

[56] Yasmine Harbi, Salsabyl Merat, Zibouda Aliouat, and Saad Harous. Bio-inspired intrusion detection system for internet of things networks security. In *Proceedings of the Cognitive Models and Artificial Intelligence Conference*, pages 14–19, 2024.

[57] Chandra Umakantham Om Kumar, Jeyakumar Durairaj, Samsu Aliar Ahamed Ali, Y Justindhas, and Suguna Marappan. Effective intrusion detection system for iot using optimized capsule auto encoder model. *Concurrency and Computation: Practice and Experience*, 34(13):e6918, 2022.

[58] Mohamed Abd Elaziz, Mohammed AA Al-qaness, Abdelghani Dahou, Rehab Ali Ibrahim, and Ahmed A Abd El-Latif. Intrusion detection approach for cloud and iot environments using deep learning and capuchin search algorithm. *Advances in Engineering Software*, 176:103402, 2023.

[59] Kadiyala Ramana, A Revathi, A Gayathri, Rutvij H Jhaveri, CV Lakshmi Narayana, and B Naveen Kumar. Wogru-ids—an intelligent intrusion detection system for iot assisted wireless sensor networks. *Computer Communications*, 196:195–206, 2022.

[60] Mouaad Mohy-eddine, Azidine Guezzaz, Said Benkirane, Mourade Azrour, and Kamal Bella. A whale optimization algorithm feature selection model for iot detecting intrusion in environments. In *The International Conference on Artificial Intelligence and Smart Environment*, pages 413–419. Springer, 2023.

[61] Soumya Bajpai, Kapil Sharma, and Brijesh Kumar Chaurasia. A hybrid meta-heuristics algorithm: Xgboost-based approach for ids in iot. *SN Computer Science*, 5(5):1–16, 2024.

[62] Thippa Reddy Gadekallu, Neeraj Kumar, Thar Baker, Deepa Natarajan, Prabadevi Boopathy, and Praveen Kumar Reddy Maddikunta. Moth–flame optimization based ensemble classification for intrusion detection in intelligent transport system for smart cities. *Microprocessors and Microsystems*, 103:104935, 2023.

[63] D Jayalatchumy, Rajakumar Ramalingam, Aravind Balakrishnan, Mejdl Safran, and Sultan Alfarhood. Improved crow search-based feature selection and ensemble learning for iot intrusion detection. *IEEE Access*, 2024.

[64] R Geetha, A Jegatheesan, Rajesh Kumar Dhanaraj, K Vijayalakshmi, Anand Nayyar, V Arulkumar, J Velmurugan, and Rajendran Thavasimuthu. Cvs-fln: a novel iot-ids model based on metaheuristic

feature selection and neural network classification model. *Multimedia Tools and Applications*, pages 1–35, 2024.

[65] Osama Bassam J Rabie, Shitharth Selvarajan, Tawfiq Hasanin, Abdulrhman M Alshareef, CK Yogesh, and Mueen Uddin. A novel iot intrusion detection framework using decisive red fox optimization and descriptive back propagated radial basis function models. *Scientific Reports*, 14(1):386, 2024.

[66] Shubhkirti Sharma, Vijay Kumar, and Kamlesh Dutta. Multi-objective prairie dog optimization algorithm for iot-based intrusion detection. *Internet Technology Letters*, page e516.

[67] Abdelghani Dahou, Mohamed Abd Elaziz, Samia Allaoua Chelloug, Mohammed A Awadallah, Mohammed Azmi Al-Betar, Mohammed AA Al-Qaness, and Agostino Forestiero. Intrusion detection system for iot based on deep learning and modified reptile search algorithm. *Computational Intelligence and Neuroscience*, 2022(1):6473507, 2022.

[68] Hossein Asgharzadeh, Ali Ghaffari, Mohammad Masdari, and Farhad Soleimanian Gharehchopogh. Anomaly-based intrusion detection system in the internet of things using a convolutional neural network and multi-objective enhanced capuchin search algorithm. *Journal of Parallel and Distributed Computing*, 175:1–21, 2023.

[69] Abdulaziz Fatani, Abdelghani Dahou, Mohammed AA Al-Qaness, Songfeng Lu, and Mohamed Abd Elaziz. Advanced feature extraction and selection approach using deep learning and aquila optimizer for iot intrusion detection system. *Sensors*, 22(1):140, 2021.

[70] H Kanakadurga Bella and S Vasundra. Intrusion detection using bat optimization algorithm and densenet for iot and cloud based systems. *International Journal on Artificial Intelligence Tools*, 33(02):2350065, 2024.

[71] Sanjaikanth E Vadakkethil, Kiran Polimetla, Zaid Alsalami, Piyush Kumar Pareek, and Deepak Kumar. Mayfly optimization algorithm with bidirectional long-short term memory for intrusion detection system in internet of things. In *2024 Third International Conference on Distributed Computing and Electrical Circuits and Electronics (ICDCECE)*, pages 1–4. IEEE, 2024.

[72] Aswathy K Cherian, M Vaidhehi, M Arshey, Serin V Simpson, J Briskilal, and Astitva Singh. An iot-based deep belief network in intrusion detection system using butterfly optimization. In *2024 10th International Conference on Communication and Signal Processing (ICCSP)*, pages 1588–1593. IEEE, 2024.

[73] Raneem Qaddoura and Hossam Faris. Evolving random weight neural networks based on oversampled-segmented examples for iot intrusion detection. *The Journal of Supercomputing*, pages 1–35, 2024.

[74] Keerthi Kethineni and G Pradeepini. Intrusion detection in internet of things-based smart farming using hybrid deep learning framework. *Cluster Computing*, 27(2):1719–1732, 2024.

[75] Hayam Alamro, Radwa Marzouk, Nuha Alruwais, Noha Negm, Sumayh S Aljameel, Majdi Khalid, Manar Ahmed Hamza, and Mohamed Ibrahim Alsaid. Modeling of blockchain assisted intrusion detection on iot healthcare system using ant lion optimizer with hybrid deep learning. *IEEE Access*, 11:82199–82207, 2023.

[76] B Gopalakrishnan and P Purusothaman. A new design of intrusion detection in iot sector using optimal feature selection and high ranking-based ensemble learning model. *Peer-to-Peer Networking and Applications*, 15(5):2199–2226, 2022.

[77] Subhash V Pingale and Sanjay R Sutar. Remora based deep maxout network model for network intrusion detection using convolutional neural network features. *Computers and Electrical Engineering*, 110:108831, 2023.

[78] José Escorcia-Gutierrez, Margarita Gamarra, Esmeide Leal, Natasha Madera, Carlos Soto, Romany F Mansour, Meshal Alharbi, Ahmed Alkhayyat, and Deepak Gupta. Sea turtle foraging algorithm with hybrid deep learning-based intrusion detection for the internet of drones environment. *Computers and Electrical Engineering*, 108:108704, 2023.

[79] Shahid Latif, Wadii Boulila, Anis Koubaa, Zhuo Zou, and Jawad Ahmad. Dtl-ids: An optimized intrusion detection framework using deep transfer learning and genetic algorithm. *Journal of Network and Computer Applications*, 221:103784, 2024.

[80] Arun Kumar Dey, Govind P Gupta, and Satya Prakash Sahu. Hybrid meta-heuristic based feature selection mechanism for cyber-attack detection in iot-enabled networks. *Procedia Computer Science*, 218:318–327, 2023.

[81] Huma Gupta, Sanjeev Sharma, and Sanjay Agrawal. Artificial intelligence-based anomalies detection scheme for identifying cyber threat on iot-based transport network. *IEEE Transactions on Consumer Electronics*, 70(1):1716–1724, 2024.

[82] R Anushiya and VS Lavanya. A new deep-learning with swarm based feature selection for intelligent intrusion detection for the internet of things. *Measurement: Sensors*, 26:100700, 2023.

[83] Ruba Abu Khurma, Iman Almomani, and Ibrahim Aljarah. Iot botnet detection using salp swarm and ant lion hybrid optimization model. *Symmetry*, 13(8):1377, 2021.

[84] Afsaneh Mahanipour and Hana Khamfroush. Enhancing iot security: A novel feature engineering approach for ml-based intrusion detection systems. *arXiv preprint arXiv:2404.19114*, 2024.

[85] ES Phalguna Krishna and Arunkumar Thangavelu. Attack detection in iot devices using hybrid metaheuristic lion optimization algorithm and firefly optimization algorithm. *International Journal of System Assurance Engineering and Management*, pages 1–14, 2021.

[86] Tarek Gaber, Joseph B Awotunde, Sakinat O Folorunso, Sunday A Ajagbe, and Esraa Eldesouky. Industrial internet of things intrusion detection method using machine learning and optimization techniques. *Wireless Communications and Mobile Computing*, 2023(1):3939895, 2023.

[87] Sandhya Ethala and Annapurani Kumarappan. A hybrid spider monkey and hierarchical particle swarm optimization approach for intrusion detection on internet of things. *Sensors*, 22(21):8566, 2022.

[88] Ediga Sathyanarayana Phalguna Krishna and Thangavelu Arunkumar. Hybrid particle swarm and gray wolf optimization algorithm for iot intrusion detection system. *International Journal of Intelligent Engineering & Systems*, 14(4), 2021.

[89] Pankaj Kumar Keserwani, Mahesh Chandra Govil, Emmanuel S Pilli, and Prajjval Govil. A smart anomaly-based intrusion detection system for the internet of things (iot) network using gwo–pso–rf model. *Journal of Reliable Intelligent Environments*, 7(1):3–21, 2021.

[90] Reem Alkanhel, Doaa Sami Khafaga, El-Sayed M El-kenawy, Abdelaziz A Abdelhamid, Abdelhameed Ibrahim, Rashid Amin, and BM El-den. Hybrid grey wolf and dipper throated optimization in network intrusion detection systems. *CMC-COMPUTERS MATERIALS &CONTINUA*, 74(2):2695–2709, 2023.

[91] Ravinder Kumar, Amita Malik, and Virender Ranga. An intellectual intrusion detection system using hybrid hunger games search and remora optimization algorithm for iot wireless networks. *Knowledge-Based Systems*, 256:109762, 2022.

[92] Azam Davahli, Mahboubeh Shamsi, and Golnoush Abaei. Hybridizing genetic algorithm and grey wolf optimizer to advance an intelligent and lightweight intrusion detection system for iot wireless networks. *Journal of Ambient Intelligence and Humanized Computing*, 11(11):5581–5609, 2020.

[93] M Jeyaselvi, Rajesh Kumar Dhanaraj, M Sathya, Fida Hussain Memon, Lalitha Krishnasamy, Kapal Dev, Wang Ziyue, and Nawab Muhammad Faseeh Qureshi. A highly secured intrusion detection system for iot using expso-stfa feature selection for laann to detect attacks. *Cluster Computing*, 26(1):559–574, 2023.

[94] Subham Kumar Gupta, Meenakshi Tripathi, and Jyoti Grover. Hybrid optimization and deep learning based intrusion detection system. *Computers and Electrical Engineering*, 100:107876, 2022.

[95] Doaa Sami Khafaga, Faten Khalid Karim, Abdelaziz A Abdelhamid, El-Sayed M El-kenawy, Hend K Alkahtani, Nima Khodadadi, Mohammed Hadwan, and Abdelhameed Ibrahim. Voting classifier and metaheuristic optimization for network intrusion detection. *Computers, Materials & Continua*, 74(2), 2023.

[96] Amit Sagu, Nasib Singh Gill, Preeti Gulia, Pradeep Kumar Singh, and Wei-Chiang Hong. Design of metaheuristic optimization algorithms for deep learning model for secure iot environment. *Sustainability*, 15(3):2204, 2023.

[97] M Karthikeyan, D Manimegalai, and Karthikeyan RajaGopal. Firefly algorithm based wsn-iot security enhancement with machine learning for intrusion detection. *Scientific Reports*, 14(1):231, 2024.

[98] Fahad F Alruwaili, Mashael M Asiri, Fatma S Alrayes, Sumayh S Aljameel, Ahmed S Salama, and Anwer Mustafa Hilal. Red kite optimization algorithm with average ensemble model for intrusion detection for secure iot. *IEEE Access*, 11:131749–131758, 2023.

[99] Rua Y Aburasain. Enhanced black widow optimization with hybrid deep learning enabled intrusion detection in internet of things-based smart farming. *IEEE Access*, 2024.

[100] Salam Fraihat, Sharif Makhadmeh, Mohammed Awad, Mohammed Azmi Al-Betar, and Anessa Al-Redhaei. Intrusion detection system for large-scale iot netflow networks using machine learning with modified arithmetic optimization algorithm. *Internet of Things*, 22:100819, 2023.

[101] Sharif Naser Makhadmeh, Yousef Sanjalawe, and Hussam N Fakhouri. Intrusion detection system using modified arithmetic optimization algorithm for large-scale iot. In *2024 2nd International Conference on Cyber Resilience (ICCR)*, pages 1–6. IEEE, 2024.

[102] Areej A Malibari, Saud S Alotaibi, Reem Alshahrani, Sami Dhahbi, Rana Alabdan, Fahd N Al-wesabi, and Anwer Mustafa Hilal. A novel metaheuristics with deep learning enabled intrusion detection system for secured smart environment. *Sustainable Energy Technologies and Assessments*, 52:102312, 2022.

[103] Mahdieh Maazalahi and Soodeh Hosseini. K-means and meta-heuristic algorithms for intrusion detection systems. *Cluster Computing*, pages 1–43, 2024.

[104] Peiyu Li, Hui Wang, Guo Tian, and Zhihui Fan. A cooperative intrusion detection system for the internet of things using convolutional neural networks and black hole optimization. *Sensors*, 24(15):4766, 2024.

[105] Mohammed I Alghamdi. A hybrid model for intrusion detection in iot applications. *Wireless Communications and Mobile Computing*, 2022(1):4553502, 2022.

[106] Jeng-Shyang Pan, Fang Fan, Shu-Chuan Chu, Hui-Qi Zhao, and Gao-Yuan Liu. A lightweight intelligent intrusion detection model for wireless sensor networks. *Security and communication Networks*, 2021(1):5540895, 2021.

[107] Abdulaziz Fatani, Abdelghani Dahou, Mohamed Abd Elaziz, Mohammed AA Al-Qaness, Songfeng Lu, Saad Ali Alfadhli, and Shayem Saleh Alresheedi. Enhancing intrusion detection systems for iot and cloud environments using a growth optimizer algorithm and conventional neural networks. *Sensors*, 23(9):4430, 2023.

[108] Yazan Otoum and Amiya Nayak. As-ids: Anomaly and signature based ids for the internet of things. *Journal of Network and Systems Management*, 29(3):23, 2021.

[109] Agostino Forestiero. Metaheuristic algorithm for anomaly detection in internet of things leveraging on a neural-driven multiagent system. *Knowledge-Based Systems*, 228:107241, 2021.

[110] Sarra Cherfi, Ammar Boulaiche, and Ali Lemouari. Enhancing iot security: A deep learning approach with autoencoder-dnn intrusion detection model. In *2024 6th International Conference on Pattern Analysis and Intelligent Systems (PAIS)*, pages 1–7, 2024.

[111] Anjum Nazir, Zulfiqar Memon, Touseef Sadiq, Hameedur Rahman, and Inam Ullah Khan. A novel feature-selection algorithm in iot networks for intrusion detection. *Sensors*, 23(19):8153, 2023.

[112] Maria Habib, Ibrahim Aljarah, and Hossam Faris. A modified multi-objective particle swarm optimizer-based lévy flight: An approach toward intrusion detection in internet of things. *Arabian Journal for Science and Engineering*, 45(8):6081–6108, 2020.

[113] Arun Kumar Dey, Govind P Gupta, and Satya Prakash Sahu. A metaheuristic-based ensemble feature selection framework for cyber threat detection in iot-enabled networks. *Decision Analytics Journal*, 7:100206, 2023.

[114] Mohammed Alweshah, Saleh Alkhalaileh, Majdi Beseiso, Muder Almiani, and Salwani Abdullah. Intrusion detection for iot based on a hybrid shuffled shepherd optimization algorithm. *The Journal of Supercomputing*, 78(10):12278–12309, 2022.

[115] Parisa Rahmani, Mohamad Arefi, Seyyed MohamadSaber Seyyed Shojae, and Ashraf Mirzaee. Improvement of intrusion detection in iot networks using a hybrid machine and metaheuristic algorithm. 2024.

[116] Mohammed Aljebreen, Manal Abdullah Alohali, Muhammad Kashif Saeed, Heba Mohsen, Mesfer Al Duhayyim, Amgad Atta Abdelmageed, Suhanda Drar, and Sitelbanat Abdelbagi. Binary chimp optimization algorithm with ml based intrusion detection for secure iot-assisted wireless sensor networks. *Sensors*, 23(8):4073, 2023.

[117] Amir Vafid Hanafi, Ali Ghaffari, Hesam Rezaei, Aida Valipour, and Bahman Arasteh. Intrusion detection in internet of things using improved binary golden jackal optimization algorithm and lstm. *Cluster Computing*, 27(3):2673–2690, 2024.

[118] Richa Singh and RL Ujjwal. Intrusion detection system based on chaotic opposition for iot network. *International journal of electrical and computer engineering systems*, 15(2):121–136, 2024.

[119] Orieb Abu Alghanam, Wesam Almobaideen, Maha Saadeh, and Omar Adwan. An improved pio feature selection algorithm for iot network intrusion detection system based on ensemble learning. *Expert Systems with Applications*, 213:118745, 2023.

[120] M Anuradha, G Mani, T Shanthi, NR Nagarajan, P Suresh, and C Bharatiraja. Intrusion detection system for big data analytics in iot environment. *Computer Systems Science & Engineering*, 43(1), 2022.

[121] PG Om Prakash, Balajee Maram, Ganapathi Nalinipriya, and Rajan Cristin. Harmony search hawks optimization-based deep reinforcement learning for intrusion detection in iot using nonnegative matrix factorization. *International Journal of Wavelets, Multiresolution and Information Processing*, 19(04):2050093, 2021.

[122] Sohail Saif, Priya Das, Suparna Biswas, Manju Khari, and Vimal Shanmuganathan. Hiids: Hybrid intelligent intrusion detection system empowered with machine learning and metaheuristic algorithms for application in iot based healthcare. *Microprocessors and Microsystems*, page 104622, 2022.

[123] Mohammed Alweshah, Abdelaziz Hammouri, Saleh Alkhalaileh, and Omar Alzubi. Intrusion detection for the internet of things (iot) based on the emperor penguin colony optimization algorithm. *Journal of Ambient Intelligence and Humanized Computing*, 14(5):6349–6366, 2023.

[124] Asima Sarwar, Salva Hasan, Waseem Ullah Khan, Salman Ahmed, and Safdar Nawaz Khan Marwat. Design of an advance intrusion detection system for iot networks. In *2022 2nd international conference on artificial intelligence (ICAI)*, pages 46–51. IEEE, 2022.

[125] Thavavel Vaiyapuri, Shabbab Algamdi, Rajan John, Zohra Sbai, Munira Al-Helal, Ahmed Alkhayyat, and Deepak Gupta. Metaheuristics with federated learning enabled intrusion detection system in internet of things environment. *Expert Systems*, 40(5):e13138, 2023.

[126] A Vinodh Kannan. Intrusion detection in internet of things using ant colony optimisation. *ICTACT journal on data science and machine learning*, 1(3):88–91, 2020.

[127] Hamed Ghasemi and Shahram Babaie. A new intrusion detection system based on svm–gwo algorithms for internet of things. *Wireless Networks*, pages 1–13, 2024.

[128] Zhengnan Lv, Hongzhi Guo, Jing Hu, Zhicheng Zhang, and Zhiyang Wu. A binary bee foraging algorithm based feature selection approach for iot intrusion detection. *IEEE Internet of Things Journal*, 2023.

[129] Taief Alaa Alamiedy, Mohammed Anbar, Zakaria NM Alqattan, and Qusay M Alzubi. Anomaly-based intrusion detection system using multi-objective grey wolf optimisation algorithm. *Journal of Ambient Intelligence and Humanized Computing*, 11(9):3735–3756, 2020.

[130] Ethala Sandhya and Annapurani Kumarappan. Enhancing the performance of an intrusion detection system using spider monkey optimization in iot. *International Journal of Intelligent Engineering & Systems*, 14(6), 2021.

[131] Ya Li, Seyed-mohsen Ghoreishi, and Alibek Issakhov. Improving the accuracy of network intrusion detection system in medical iot systems through butterfly optimization algorithm. *Wireless Personal Communications*, 126(3):1999–2017, 2022.

[132] Archana Bathula, Samya Muhuri, Suresh Merugu, and Suneet K Gupta. Designing framework for intrusion detection in iot based on spotted hyena-based ann. In *ICDSMLA 2020: Proceedings of the 2nd International Conference on Data Science, Machine Learning and Applications*, pages 1615–1629. Springer, 2022.

[133] T Jayasankar, R Kiruba Buri, and P Maheswaravenkatesh. Intrusion detection system using metaheuristic fireworks optimization based feature selection with deep learning on internet of things environment. *Journal of Forecasting*, 43(2):415–428, 2024.

[134] Nenavath Chander and Mummadi Upendra Kumar. Metaheuristic feature selection with deep learning enabled cascaded recurrent neural network for anomaly detection in industrial internet of things environment. *Cluster Computing*, 26(3):1801–1819, 2023.

[135] S Kaviarasan and ABOTHU Geetha. Network intrusion detection based on one-dimensional cnn with chimp optimization algorithm. *J. Theor. Appl. Inf. Technol*, 101(10), 2023.

[136] Youcef Djenouri, Asma Belhadi, Gautam Srivastava, Jerry Chun-Wei Lin, and Anis Yazidi. Interpretable intrusion detection for next generation of internet of things. *Comput. Commun.*, 203(C):192–198, apr 2023.

[137] Nagamani H Shahapure, M Punitha, et al. Water moth search algorithm-based deep training for intrusion detection in iot. *Journal of Web Engineering*, 20(6):1781–1812, 2021.

[138] Abdulaziz Fatani, Mohamed Abd Elaziz, Abdelghani Dahou, Mohammed AA Al-Qaness, and Songfeng Lu. Iot intrusion detection system using deep learning and enhanced transient search optimization. *IEEE Access*, 9:123448–123464, 2021.

[139] Mahbod Tavallaee, Ebrahim Bagheri, Wei Lu, and Ali A Ghorbani. A detailed analysis of the kdd cup 99 data set. In *2009 IEEE symposium on computational intelligence for security and defense applications*, pages 1–6. Ieee, 2009.

[140] KDD Cup 1999. Available on: https://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html (Last accessed: November, 2024).

[141] Nour Moustafa and Jill Slay. Unsw-nb15: a comprehensive data set for network intrusion detection systems (unsw-nb15 network data set). In *2015 military communications and information systems conference (MilCIS)*, pages 1–6. IEEE, 2015.

[142] Nickolaos Koroniotis, Nour Moustafa, Elena Sitnikova, and Benjamin Turnbull. Towards the development of realistic botnet dataset in the internet of things for network forensic analytics: Bot-iot dataset. *Future Generation Computer Systems*, 100:779–796, 2019.

[143] Iman Sharafaldin, Arash Habibi Lashkari, Ali A Ghorbani, et al. Toward generating a new intrusion detection dataset and intrusion traffic characterization. *ICISSp*, 1:108–116, 2018.

[144] Nour Moustafa. A new distributed architecture for evaluating ai-based security systems at the edge: Network ton_iot datasets. *Sustainable Cities and Society*, 72:102994, 2021.

[145] Yair Meidan, Michael Bohadana, Yael Mathov, Yisroel Mirsky, Asaf Shabtai, Dominik Breitenbacher, and Yuval Elovici. N-baiot—network-based detection of iot botnet attacks using deep autoencoders. *IEEE Pervasive Computing*, 17(3):12–22, 2018.

[146] Imtiaz Ullah and Qusay H Mahmoud. A scheme for generating a dataset for anomalous activity detection in iot networks. In *Canadian conference on artificial intelligence*, pages 508–520. Springer, 2020.

[147] Constantinos Kolias, Georgios Kambourakis, Angelos Stavrou, and Stefanos Gritzalis. Intrusion detection in 802.11 networks: Empirical evaluation of threats and a public dataset. *IEEE Communications Surveys & Tutorials*, 18(1):184–208, 2015.

[148] Iman Almomani, Bassam Al-Kasasbeh, and Mousa Al-Akhras. Wsn-ds: a dataset for intrusion detection systems in wireless sensor networks. *Journal of Sensors*, 2016(1):4731953, 2016.

[149] Abhishek Verma and Virender Ranga. Evaluation of network intrusion detection systems for rpl based 6lowpan networks in iot. *Wireless Personal Communications*, 108:1571–1594, 2019.

[150] Akila Somasundaram and U Srinivasulu Reddy. Data imbalance: effects and solutions for classification of large and highly imbalanced data. In *international conference on research in engineering, computers and technology (ICRECT 2016)*, pages 1–16, 2016.

[151] Saptarshi Bej, Narek Davtyan, Markus Wolfien, Mariam Nassar, and Olaf Wolkenhauer. Loras: An oversampling approach for imbalanced datasets. *Machine Learning*, 110:279–301, 2021.

[152] Jiye Liang, Feng Wang, Chuangyin Dang, and Yuhua Qian. A group incremental approach to feature selection applying rough set technique. *IEEE transactions on knowledge and data engineering*, 26(2):294–308, 2012.

[153] Weiming Hu, Jun Gao, Yanguo Wang, Ou Wu, and Stephen Maybank. Online adaboost-based parameterized methods for dynamic distributed network intrusion detection. *IEEE Transactions on Cybernetics*, 44(1):66–82, 2013.

[154] Omar Abdel Wahab. Intrusion detection in the iot under data and concept drifts: Online deep learning approach. *IEEE Internet of Things Journal*, 9(20):19706–19716, 2022.

[155] Chen Guo, Heng Tang, Ben Niu, and Chang Boon Patrick Lee. A survey of bacterial foraging optimization. *Neurocomputing*, 452:728–746, 2021.

[156] Mohammed Azmi Al-Betar, Zaid Abdi Alkareem Alyasseri, Mohammed A Awadallah, and Iyad Abu Doush. Coronavirus herd immunity optimizer (chio). *Neural Computing and Applications*, 33:5011–5042, 2021.

[157] MI Thariq Hussan, G Vinoda Reddy, PT Anitha, A Kanagaraj, and P Naresh. Ddos attack detection in iot environment using optimized elman recurrent neural networks based on chaotic bacterial colony optimization. *Cluster Computing*, pages 1–22, 2023.

[158] Manal M Khayyat. Improved bacterial foraging optimization with deep learning based anomaly detection in smart cities. *Alexandria Engineering Journal*, 75:407–417, 2023.

[159] Sara Moein and Rajasvaran Logeswaran. Kgmo: A swarm optimization algorithm based on the kinetic energy of gas molecules. *Information Sciences*, 275:127–144, 2014.

[160] Paul Tavolato, Hubert Schölnast, and Christina Tavolato-Wötzl. Analytical modelling of cyber-physical systems: Applying kinetic gas theory to anomaly detection in networks. *Journal of Computer Virology and Hacking Techniques*, 16(1):93–101, 2020.

[161] GR Asha and Gowrishankar. An efficient clustering and routing algorithm for wireless sensor networks using gso and kgmo techniques. In *Smart Computing Paradigms: New Progresses and Challenges: Proceedings of ICACNI 2018, Volume 2*, pages 75–85. Springer, 2020.

[162] Weiping Ding, Janmenjoy Nayak, Bighnaraj Naik, Danilo Pelusi, and Manohar Mishra. Fuzzy and real-coded chemical reaction optimization for intrusion detection in industrial big data environment. *IEEE Transactions on Industrial Informatics*, 17(6):4298–4307, 2020.

[163] Mohammad Ehteram, Akram Seifi, and Fatemeh Barzegari Banadkooki. *Application of Machine Learning Models in Agricultural and Meteorological Sciences*. Springer Nature, 2023.

[164] Ivana Matoušová, Pavel Trojovskỳ, Mohammad Dehghani, Eva Trojovská, and Juraj Kostra. Mother optimization algorithm: A new human-based metaheuristic approach for solving engineering optimization. *Scientific Reports*, 13(1):10312, 2023.

[165] Naser Ghorbani and Ebrahim Babaei. Exchange market algorithm. *Applied soft computing*, 19:177–187, 2014.

[166] VS Prasanth, A Mary Posonia, and A Parveen Akhther. Effective ensemble based intrusion detection and energy efficient load balancing using sunflower optimization in distributed wireless sensor network. *Multimedia Systems*, 30(4):223, 2024.

[167] Aidin Ferdowsi and Walid Saad. Generative adversarial networks for distributed intrusion detection in the internet of things. In *2019 IEEE Global Communications Conference (GLOBECOM)*, pages 1–6. IEEE, 2019.

[168] Tim Salimans, Ian Goodfellow, Wojciech Zaremba, Vicki Cheung, Alec Radford, and Xi Chen. Improved techniques for training gans. *Advances in neural information processing systems*, 29, 2016.

[169] Saifur Rahman, Shantanu Pal, Shubh Mittal, Tisha Chawla, and Chandan Karmakar. Syn-gan: A robust intrusion detection system using gan-based synthetic data for iot security. *Internet of Things*, 26:101212, 2024.

[170] Balaji Lakshminarayanan, Alexander Pritzel, and Charles Blundell. Simple and scalable predictive uncertainty estimation using deep ensembles. *Advances in neural information processing systems*, 30, 2017.

[171] N Anusha, BR Tapas Bapu, A Vijayaraj, C Ramesh Kumar, and Raji P. Cyber intrusion detection using dual interactive wasserstein generative adversarial network with war strategy optimization in wireless sensor networks. *Multimedia Tools and Applications*, pages 1–31, 2024.

[172] G Senthilkumar, K Tamilarasi, and JK Periasamy. Cloud intrusion detection framework using variational auto encoder wasserstein generative adversarial network optimized with archerfish hunting optimization algorithm. *Wireless Networks*, 30(3):1383–1400, 2024.

[173] Yinong Li, Jianbo Li, Zhiqiang Lv, Haoran Li, Yue Wang, and Zhihao Xu. Gasto: A fast adaptive graph learning framework for edge computing empowered task offloading. *IEEE Transactions on Network and Service Management*, 20(2):932–944, 2023.

[174] Zhihao Xu, Zhiqiang Lv, Benjia Chu, and Jianbo Li. A fast spatial-temporal information compression algorithm for online real-time forecasting of traffic flow with complex nonlinear patterns. *Chaos, Solitons & Fractals*, 182:114852, 2024.

[175] Boyang Li, Yuhang Yang, Ziyu Zhao, Xin Ni, and Diyang Zhang. A novel ensemble learning approach for intelligent logistics demand management. *Journal of Internet Technology*, 25(4):507–515, 2024.

Appendices

***Appendix A.* Performances tabulation of the existing metaheuristics-based and ML-driven IoT-IDSs studied in this SLR.**

Though recall and detection rate can be used interchangeably, some papers explicitly mention DR rather than recall. Therefore, we use these two terms separately in this study to avoid conflict and confusion.

Table 11: Analysis of the IoT-IDSs based on different performance metrics, metaheuristics, applications, ML algorithms, datasets, and classification types. Here, “FC” and “CLT” represent selected feature count and classification types, respectively.

Ref.	**Meta.**	**App^n**	**FC**	**ML**	**Dataset used**	**CLT**	**IoT-IDS Performance (%)**							
							Acc	**Prec**	**Rec**	**F1**	**Speci**	**DR**	**FPR**	**Others**
[13]	GTO-BSA	FS	-	KNN	NSL-KDD		95.5		91.4		97.4			
[52]	hybrid PCA-GWO	FS	-	DNN	CICIDS2017		98.7		97.3		99.7			
					UNSW-NB15		81.5		81.5		87.7			
					BoT-IoT		81.5		99.3		96.2			
					Kaggle dataset		99.9		95.4		100			
[95]	new WOA, guided by DTO	PT	N/A	KNN, RF, NN	RPL-NIDS17		95.1							AUC=99.0, MSE=2.50E-08
[122]	PSO, GA, and DE	FS	8-10	KNN,DT	NSL-KDD		95.71							
[131]	BOA	FS	-	ANN	NSL-KDD		93.27		94.37		92.68			
[15]	HHO-FDM	FS	-	LSTM +GRU = RNNs	IoT-23		98.12	98.06	98.31	98.18				AUC-ROC=99.82
[54]	modified FOA	HPT	N/A	KNN, XGBoost	UNSW-NB15		99.98	99.99	99.98	99.99				AUC-ROC=100
					IoT-healthcare-security-dataset		99.6997	99.6998	99.6997	99.6996				
[125]	BSA, SCOA	FS, PT	-	FL, KELM	-		99.45	80.26	82.67	80.95				
[102]	IAOA, QPSO	FS+ PT	-	DWNN	CICIDS2017		98.21	96.53	98.22	97.92				
[80]	NSGA-II	FS	13	SVM	TON-IoT		99.48							
					NSL-KDD		99.98	99.87	100	99.73				AUC=99.76

Table 11 – *Continued from previous page*

Ref.	Meta.	App^n	FC	ML	Dataset used	CLT	IoT-IDS Performance (%)							
							Acc	**Prec**	**Rec**	**F1**	**Speci**	**DR**	**FPR**	**Others**
[85]	LOA-FOA	FS	-	RF	NBaIoT		99.86	99.94	99.94	99.86				FN=7, FP=2
[113]	BGSA and BGWO	FS	4	DT and EL (AdaBoost and RF)	UNSW-NB15		99.41	99.92		99.33		99.09	0.03	
[138]	TSODE	FS	-	CNN	KDDCup-99	M	92.064	89.943	92.064	90.007			0.01989	
						B	92.451	94.32	92.451	92.851			0.07527	
					NSL-KDD	M	75.751	78.988	75.751	71.692			0.05868	
						B	77.381	83.637	77.381	77.08			0.19223	
					BoT-IoT	M	99.042	99.042	99.042	99.042			0.00301	
						B	99.992	99.992	99.992	99.992			0.00007	
					CICIDS-2017	M	99.93	99.93	99.93	99.93			0.00009	
						B	99.996	99.996	99.996	99.996			0.000029	
[67]	RSA	FS	-	CNN	KDDCup-99	M	92.04	89.684	92.04	89.985				
						B	92.344	94.335	92.344	92.763				
					NSL-KDD	M	76.107	82.171	76.107	71.731				
						B	77.814	83.83	77.814	77.545				
					CICIDS-2017	M	99.911	99.907	99.911	99.888				
						B	99.997	99.997	99.997	99.997				
					BoT-IoT	M	99.02	99.098	99.038	99.07				
						B	99.993	99.99	99.993	99.99				
[38]	double PSO	FS+HPT	10	DNN, LSTM-RNN, and DBN	NSL-KDD		98.77	98.1	92.29	95.11				
					CICIDS2017		95.81	95.82	95.81	95.81				
					KDDCup-99		99.941	99.947	99.936	99.942				G-Mean=99.942

Table 11 – *Continued from previous page*

Ref.	Meta.	App^n	FC	ML	Dataset used	CLT	Acc	Prec	Rec	F1	Speci	DR	FPR	Others
[107]	MGO, using WOA	FS	-	CNNs	NSL-KDD		92.04	90.841	91.04	90.941				G-Mean=90.941
					BoT-IoT		76.725	83.105	76.672	79.759				G-Mean=79.824
					CICIDS-2017		99.22	99.188	99.248	99.218				G-Mean=99.218
[100]	AOA	FS	7	RF and ET	NF-CSE-CIC-IDS2018-v2	M	99.52	99.51		99.4				
						B	99.54	99.54		99.54				
					NF-ToN-IoT-v2	M	97.21	97.15		97.16		99.52	3.27	
						B	99.99	99.99		99.99		99.54	3.26	
					NF-UNSW-NB15-v2	M	98.76	98.8		98.77		97.17	0.32	
						B	99.69	99.7		99.69		99.99	0.02	
					NF-BoT-IoT-v2	M	98.52	98.53		98.52		98.76	3.71	
						B	99.98	99.98		99.98		99.69	4.08	
[105]	PO	PT	N/A	CFNN	NSL-KDD++		99.86	99.89	99.58	99.72				
					UNSW-NB15		99.46	99.75	99.62	99.76				
					CIDCC-2017		99.38	99.69	99.66	99.69				
[114]	SSO-SA1 and SSO-SA2	FS	39.11	KNN	N-BaIoT		0.987	0.997	0.996	0.998				
[45]	GSO	FS	-	PCA	NSL-KDD		93.35	91.9	94.02			95.12	2.97	
[123]	EPC	FS	38.27	KNN	N-BaIoT		98.2	99.7	99.2	99.4				
[115]	GAO-AOA	PT+HPT	N/A	RdNN	TON_IOT			99.56				99.37	4	
[127]	GWO	FS+HPT	-	SVM	NSL-KDD		98	97	99	98				
					TON_IOT		81	82	84	83.57				

Table 11 – *Continued from previous page*

Ref.	Meta.	App^n	FC	ML	Dataset used	CLT	IoT-IDS Performance (%)							
							Acc	Prec	Rec	F1	Speci	DR	FPR	Others
[96]	SAEHO, SU-CMO	PT	N/A	CNN+DBN and Bi-LSTM+GRU	UNSW-NB15		92.8			81				MCC=0.786, Rand Index = 0.998 (dataset-2)
[90]	GWO-DTO	FS	-	KNN	RPL-NIDS17		98.1	97.8	99.4	98.6	97.8			
[109]	ABF	HPT	N/A	IoT2Vec	CASAS dataset					92.98				avg entropy= 0.7478
[20]	APSO-WOA	HPT	N/A	CNN	N-BaIoT		94.54	95.2						kappa= 0.936, hamming loss= 0.944 , JSC= 0.9
[92]	GA-GWO	FS	92	SVM	AWID		99.1	96.03		97.64		99.32	0.69	
[91]	HHGS-ROA	FS	-	SVM	AWID		99.16	99.76	99.4	99.58			0.2	MCC=99.97
[112]	MOPSO-Lévy	FS	44.33	KNN	N-BaIoT		97.06	88.69					1.66	TPR=0.7506, TNR=0.9834, G-mean=0.8317, AUC =0.867
					NSL-KDD	M	99.97	99.95	99.97	99.96				
						B	99.98	99.87	100	99.73				

Table 11 – *Continued from previous page*

Ref.	Meta.	App^n	FC	ML	Dataset used	CLT	IoT-IDS Performance (%)							
							Acc	**Prec**	**Rec**	**F1**	**Speci**	**DR**	**FPR**	**Others**
[88]	PSO-GWO	FS	-	RF	N-BaIoT		99.86	99.94	99.94	99.86				
[44]	a hybrid ABC	FS	14.8, 11.9	ELM	CICIDS-2017		98.71		96.17					
					UNSW-NB15		71.54		80.58					
[18]	NSBPSO	PT	N/A	DCNN	UNSW-NB15 and Bot-IoT		98.86	99.03			95.32			MSE=0.00053
[116]	BCOA, SCA	FS, PT+HPT	-	CCR-ELM	WSN-DS		99.63		97.91	94.52	99.67			
[128]	BBFA	FS	23	SVM	N-BaIoT		99.2					99	0.006	
[86]	PSO-BA	FS	16	RF	WUSTL-IIOT-2021		99.99	99.6	99.6	99.6				
[47]	IACO	FS	-	EL using DDT, ANFIS and MDSVM	UNSW-NB15		97.375					92.365	6.67	
[98]	RKOA, LCWOA	FS,HPT	-	EL using LSTM, BiLSTM, and BiGRU	WSN-DS		98.94		75.33	79.52	75.33			AUC=85.48
[87]	SMO-Hierarchical PSO(HPSO)	FS	22	RF	UNSW-NB		99.18	94.19	93.32	94.12			0.15	AUC=99.78, MCC=0.19
					NSL-KDD	M	98.98	98.76	97.89	98.59				AUC=99.81
						B	98.31	98.61	98.41	98.56			0.21	AUC=99.87, MCC=0.17
[68]	BMECapSA	FS	12,18	CNN	NSL-KDD		99.85	99.85	99.85	99.85			0.0019	FNR=0.001
					TON-IoT		99.99	99.99	99.99	99.99			0.0001	FNR=0.00002
[133]	DFWA	FS	-	ODRNN	IDS dataset		96.11	96.11		97.21		97.31	3.03	
[89]	GWO-PSO	FS	-	RF	KDDCup-99, NSL–KDD, CICIDS-2017	M	99.88, 99.25, 99.87							

Table 11 – *Continued from previous page*

Ref.	Meta.	App^n	FC	ML	Dataset used	CLT	Acc	Prec	Rec	F1	Speci	DR	FPR	Others
[97]	GWO, FOA	PT, FS	-	SVM	NSL-KDD		99.29		98.12	96.23	99.59			AUC=98.51
[63]	enhanced CrSA	FS	11,7	EL	NSL-KDD		99	98.38	98.02	98.14				
					UNSW-NB15		97.75	83.57	83.39	81.66				
[134]	new DHOAF, SpSO	FS,PT	-	CRNN	UNSW-NB15		99.31	67.09	60.33	60.35				
					UCI SECOM		97.88	92.42	89.87	91.1				
[124]	PSO	FS	17 83 (M)	RF	IoTID20		98 (B),							
[69]	AQUO	FS	10	CNN	CICIDS-2017	M	99.911	99.91	99.91	99.888				
						B	99.997	99.997	99.997	99.997				
					NSL-KDD	M	76.002	81.719	76.002	71.602				
						B	77.382	83.692	77.382	77.077				
					BoT-IoT	M	98.926	98.905	98.904	98.904				
						B	99.994	99.992	99.993	99.992				
					KDDCup-99	M	99.919	89.824	92.042	89.987				
						B	99.922	94.283	92.256	92.683				
[17]	SCSO	FS	14.5,11.7	ELM	UNSW-NB15		71.54		80.58					
					CICIDS-2017		98.7		96.17					
[64]	CVS	FS	-	FLN, an ANN	CIC IDS-2017		99.77	99.6		99.72	99.92	99.81		
					BoT-IoT		99.68	99.3		99.21	99.83	99.11		
[106]	Compact SCA	HPT	N/A	kNN	NSL-KDD		99.327					99.206	0.5848	
					UNSW-NB15		98.27					97.94	5.82	
[73]	GWO, PSO, MVO	PT+HPT	N/A	RWNN	IoTID20									G-mean=0.7283

Table 11 – *Continued from previous page*

Ref.	Meta.	App^n	FC	ML	Dataset used	CLT	IoT-IDS Performance (%)							
							Acc	**Prec**	**Rec**	**F1**	**Speci**	**DR**	**FPR**	**Others**
[93]	EXPSO-STFA	FS	-	LAANN	KDDCup-99, NSL-KDD, CIDDS-001, and UNSW-NB15		95.65	94.74	93.54	95.64	92.74		14.52	FNR=10.2 MCC=92.56
[83]	SSA–ALO	FS	-	KNN	N-BaIoT								0.029	TPR=0.991, G-mean=0.984
[48]	BGWO	FS	-	XGBoost	N-BaIoT	M	99.9941	99.9941	99.9941	99.9941				
						B	99.997	99.997	99.997	99.997				
					NSL-KDD	M	99.9427	99.9426	99.9427	99.9426				
						B	99.9427	99.9427	99.9427	99.9427				
					WUSTL-IIOT-2021	M	100	100	100	100				
					WUSTL-EHMS-2020	M	98.897	98.8923	98.897	98.8846				
[43]	ECSSA	FS	-	LightGBM	MC-IoT		99.38	99.25	98.8	98.76				
					MQTT-IoT-IDS2020		98.91	98.8	98.36	97.16				
					MQTTset		98.35	97.38	97.68	98.56				
[111]	TS	FS	13	EL using RF	TON_IoT		99.5	97.92					0.004	
[129]	multi-objective GWO	FS	4	SVM	NSL–KDD		87.59							
[55]	FOA	FS	-	EL using KNN,SVM,LSTM,MLP	UNSW-NB15	B	98.89	99.68	99.32	98.91				AUC=99.79
					NSL-KDD	M	92.3	91.32	78.47	81.435			0.95	AUC=90.2, MCC=0.45
						B	98.41	98.68	98.46	98.68			0.24	AUC=99.79, MCC=0.26
[53]	GABGWO	FS	94	SVM	AWID and KDDCup-99		99.09	96.31	99.3	97.84			0.68	

Table 11 – *Continued from previous page*

Ref.	Meta.	App^n	FC	ML	Dataset used	CLT	Acc	Prec	Rec	F1	Speci	DR	FPR	Others
[119]	LS-PIO	FS	15,10,8,3	EL	BoT-IoT		97.37			94.88			2.05	TPR=98.78, AUC=95.68
					UNSW-NB15		94.45			91.35			30.73	TPR=98, AUC=89.52
					NLS-KDD		94.7			89.1			21.33	TPR=95.7, AUC=87.63
					KDDCup-99		99.82			97.23			6.9	TPR=99.23, AUC=96.32
[120]	HCMFO,BAS	FS,PT	24,15	VAE	UNSW-NB15		97.39	89.17	96.4	91.53				
					NSL-KDD		95.25	87.16	95.4	90.56				
[57]	CSA	PT	N/A	HKCAE	BoT-IoT		99.9	98.7	99.7	98.2	99.7			
					UNSW-NB15		99.7	99.6	99.6	98.9	98.3			
[82]	AAFSO,GA	FS,HPT	-	FR-CNN	UNSW-NB15		94.488	94.2942	94.5631	94.4284				
					BoT-IoT		93.7756	86.6687	95.874	91.0393				
[62]	MFO	FS	14	EL using LR, RF and XG-Boost	UNSW-NB15		100	99.5	100					
[94]	HCSGA	FS	-	DLHNN	NSL-KDD		99.52	97.55		97.16		96.78		
[130]	SMO	FS	-	RF	NSL-KDD		99.675	99.955	99.9425	99.9325				AUC=99.3025
[126]	ACO	FS	-	PCA	KDDCup-99							91	1.8	
[132]	SHO	HPT	N/A	ANN	KDDcup99		98.16	98.06	98.03	98.04	98.27		1.73	FNR=1.97, NPV=98.27, MCC=96.30

Table 11 – *Continued from previous page*

Ref.	Meta.	App^n	FC	ML	Dataset used	CLT	IoT-IDS Performance (%)							
							Acc	**Prec**	**Rec**	**F1**	**Speci**	**DR**	**FPR**	**Others**
					IoTID20		98.83	99.79	98.96	99.38	96.67		3.33	FNR=1.04, NPV=96.67, MCC=90.20
					IoT Botnet		97.87	100	97.75	98.86	100		0	FNR=2.25, NPV=100, MCC=96.30
[21]	QCSO, HS	Clustering, HPT	N/A	CRNN	KDDCup-99							92.04	6.86	
[59]	WOA	HPT	N/A	GRU	WSN-DS		99.804	99.868	99.83	99.866	99.826			
[58]	CSA	FS	-	CNN	NSL-KDD	M	76.011	81.737	76.011	71.461				
						B	77.205	83.594	77.205	76.892				
					BoT-IoT	M	99.15	98.807	98.806	98.806				
						B	99.994	99.993	99.993	99.992				
					KDDCup-99	M	99.917	89.875	92.044	89.988				
						B	99.935	94.349	92.318	92.743				
					CICIDS-2017	M	99.911	99.91	99.91	99.888				
						B	99.997	99.997	99.997	99.997				
[39]	HAEMPSO,modified PSO	FS,HPT	-	DNN	BoT-IoT		97.61					97.81		
					UNSW-NB15		94.62					93.8		
[19]	WOA	PT	N/A	LSTM	CIDDS-001		99.3		98.3		99			
					UNSW-NB15		99.1		98		98.99			
					NSL-KDD		99.5		98.7		98.45			
[137]	WWO-MSO (WMSA)	FS	-	DRNN	BoT-IoT		96		96		97.3			
					KDDCup-99		94.5		92.9		96.4			

Table 11 – *Continued from previous page*

Ref.	Meta.	App^n	FC	ML	Dataset used	CLT	Acc	Prec	Rec	F1	Speci	DR	FPR	Others
							IoT-IDS Performance (%)							
[121]	HSHO	FS	-	DRL			96.925							TPR=96.9, TNR=97.92
[76]	AF-EFO	FS+PT	-	HR-OELM using DNN,RF,Adaboost	NSL- KDD		95.6	98.3	92.2	95.2	98.6		0.4	FNR=7.8, NPV=98.6, MCC=91.3
					Botnet		95	97.6	95.3	96.4	53.1		4.2	FNR=4.7, NPV=53.1, MCC=40.5
					CICIDS-2017		95.4	99.9	95.1	97.5	99.7		0	FNR=4.8, NPV=99.7, MCC=74.8
					CICIDS-2018		95.3	99.7	90.8	94.9	83.6		1.5	FNR=05.7, NPV=83.6, MCC=065.4
[60]	WOA	FS	-	RBFNN	NF-ToN-IoT		96.83							MCC=89.74
					NF-Bot-IoT		98.43							MCC=57.71
					Merged		95.93							MCC=82.68
[61]	WOA	HPT	N/A	XGBoost (EGB)	IoTID20		98.86	98.67	99.91	99.30				AUC=98.91
					UNSW-NB15		99.73	99.05	99.00	99.03				AUC=99.01
[117]	GJO-OBL (IBGJO)	FS	32,20	LSTM	CICIDS2017		99.75	98.52	99.1	98.81				
					NSL-KDD		98.93	97.98	98.37	98.17				
[74]	WHO	PT	N/A	a fused CNN model with Bi-GRU	APA-DDoS		99.35	99.9		99.08		98.99		
					ToN-IoT		99.71	99.89		99.05		99.02		
[118]	CO-IHHO	FS	-	DT and KNN	BoT-IoT		100(B), 99.65(M)							

Table 11 – *Continued from previous page*

Ref.	Meta.	App^n	FC	ML	Dataset used	CLT	Acc	Prec	Rec	F1	Speci	DR	FPR	Others
							IoT-IDS Performance (%)							
[84]	hybrid BQABC-GA	FS	11,10.6,10.33	KNN	NSL-KDD		98.89		97.03		98.76		1.24	
					UNSW-NB15		90.22		94.83		88.06		11.94	
					BoT-IoT		98.49		99.79		99.27		0.73	
[22]	TuSO	HPT	N/A	EL combining RF, XG-Boost, LightGBM (LGBM), and CatBoost	MQTT dataset		99.12	97.89	95.24	96.37				
[99]	Enhanced BWO, BES	HPT,FS	-	HDL	ToN-IoT		98.81	90.84	78.95	79.49				
					Edge-IIoTset		98.35	84.85	80.95	82.79				
[56]	a modified FOA	FS	39	DT	Edge-IIoT		79.64							
[65]	DRFO	FS	-	DBRF	IoTID-20		99.8							
					NetFlow-BoT-IoT-v2			99.17	99	99.1				
					NF-ToN-IoT-v2		99.9	99.9	99.8	99.8			0.001	
					NSL-KDD							99.52		
					UNSW-NB 15		98.5	99	99	98.5			8.2	
[49]	Improved GWO (IGWO)	HPT	N/A	QSVM	BoT-IoT		99.11	99.45	99.34	97.48				
[41]	EBSA	PT	N/A	DBN (RBMs,MLPs)	NSL-KDD		98.96	99.4	98.87					
[50]	GWO	HPT	N/A	EL (DT,RF,KNN,MLP)	BoT-IoT		99.98	99.94				99.97	1.3	ROC=99.99
					UNSW-NB15		100	99.59				99.9	1.5	ROC=99.4
[66]	multi-objective PDO	FS	10-9,11-15,12	SVM,KNN	NSL-KDD	SVM	97.842		97.921				0.012	
						KNN	98.975		99.959				0.002	
					CIC-IDS2017	SVM	71.673		75.992				0.093	
						KNN	97.234		93.171				0.007	
					IoTID20	SVM	99.788		99.819				0.027	
						KNN	99.402		99.386				0.006	
[72]	BOA	PT	N/A	DBN	UNSW-NB15		97.77	96.62	93.85	91.77				MCC=91.23

Table 11 – *Continued from previous page*

Ref.	Meta.	App^n	FC	ML	Dataset used	CLT	IoT-IDS Performance (%)							
							Acc	Prec	Rec	F1	Speci	DR	FPR	Others
[42]	a new GJOA, SSA	FS, HPT	-	A-BiLSTM	CICIDS-2017		99.69	98.92	98.92	98.92				MCC=98.74
[70]	BOA	FS	-	DenseNet	UNSW-NB15		98.89							
					NSL-KDD		98.4							
[71]	MOA	FS	-	BiLSTM	NSL-KDD		99.25	99.41	99.34	98.96				
					ToN-IoT		89.61	83.57	89.56	85.72				
					UNSW-NB15		99.35	98.49	99.28	98.64				
[16]	TLBO	FS	-	RF	UNSW-NB15		86.5							
[51]	Generalized Mean GWO	FS	15,5	ElasticNet Contractive AE	NSL-KDD	M	99.9	99.06	99.79	99.41			0.95	MCC=99.39
						B	99.84	99.68	99.94	99.81				MCC=99.67
					BoT-IoT	M	99.99			99.5				AUC=100, MCC=99.51
[135]	COA	PT	N/A	1D-CNN+COA (creating a HNM)	NSL-KDD		87.19	88.28	89.49	91.19				
[77]	ROA	FS,PT+HPT		DMN	NSL-KDD		92.1	92.3	92.9	93.4				
					CICIDS-2018		94.5	93.1	93.9	93.2				
[46]	CCSO	PT	N/A	Deep LSTM	NSL-KDD		94.635		96.64		96.02			
					BoT-IoT		96.71		96.35		91.985			
[101]	modified AOA	FS	-	KNN	BoT-IoT		99.998							
[81]	fuzzy and GA: IWD and BBO	FS	-	FNN	IOTID20		96.7414	91.3695	100	95.4901				
					CICIDS-2017		98.2339	99.4831	98.6334	99.0865				
[110]	combination of IGC and SA	FS	-	an AE with DNN	UNSW-NB15		76.93	88.24	66.83	76.06				
					TON-IOTwin7		99.9	99.89	99.89	99.89				
					TON-IOTwin10		99.86	99.86	99.86	99.86				
					CICIDS2017		99.4	99.47	99.34	99.4				

Table 11 – *Continued from previous page*

Ref.	Meta.	App^n	FC	ML	Dataset used	CLT	IoT-IDS Performance (%)							
							Acc	**Prec**	**Rec**	**F1**	**Speci**	**DR**	**FPR**	**Others**
[78]	STFA,SpSO	FS,HPT	-	DBN	UNSW-NB15		98.85		59.06	58.64	99.36			MCC=60.36
					TON_IoT		99.51		99.73					
[136]	MPO	FS	-	RNN	NSL-KDD									TNR=94, TPR=94
[103]	ASO-EO	FS	-	k-means	KDDCup-99		96.1			100	99.3		0.6	NPV=0.989, FNR=0.003, TNR=0.996, PPV=0.989, MCC=0.934, AUC=0.989
					UNSW-NB15		99.1			99.4	98.5		0.9	NPV=98.5, FNR=0.4, TNR=99.5, PPV=98.5, MCC=96.3, AUC=97.2
					NSL-KDD		98.9			100	99.1		99.1	NPV=98.9, FNR=0.3, TNR=99.7, PPV=99.1, MCC=97.1, AUC=98.8
[40]	GSAPSO	HPT	N/A	XGBoost and KNN	CAN dataset	(EGB)	79.11	82.5267	79.1132	70.9564				
						(KNN)	79.10	82.9847	79.0996	70.8823				

Table 11 – *Continued from previous page*

Ref.	Meta.	App^n	FC	ML	Dataset used	CLT	IoT-IDS Performance (%)							
							Acc	Prec	Rec	F1	Speci	DR	FPR	Others
[79]	GA	HPT	N/A	EL (CNNs-based)	Edge_IIoTset	M	100	100	100	100				Cohen's Kappa score=100
[104]	BHO	FS	-	Parallel CNNs	UNSW-NB15		97.7217	97.41	97.72	97.56				
					NSL-KDD		99.8928	99.89	99.89	99.89				
[75]	ALO, FPA	FS, HPT	-	CNN+LSTM	CICIDS-2017		99.55	99.55	99.55	99.55				AUC=99.55
					ToN-IoT		99.31	99.31	99.31	99.31				AUC=99.31
[108]	HMS	clustering	N/A	LightNet, Deep Q-learning	NSL-KDD				96.6		96.8	96.9		