Cluster Computing (2024) 27:8655–8681
https://doi.org/10.1007/s10586-024-04388-5

Intrusion detection systems for IoT based on bio-inspired and machine learning techniques: a systematic review of the literature

Rafika Saadouni[1] · Chirihane Gherbi[1] · Zibouda Aliouat[1] · Yasmine Harbi[1] · Amina Khacha[1]

Received: 15 December 2023 / Revised: 13 February 2024 / Accepted: 26 February 2024 / Published online: 14 April 2024

Abstract
Recent technological advancements have significantly expanded both networks and data, thereby introducing new forms of attacks that pose considerable challenges to intrusion detection and network security. With intruders deploying increasingly diverse attack vectors, the need for robust Intrusion Detection Systems (IDSes) has become paramount. IDS serves as a crucial tool for monitoring network traffic to uphold the integrity, confidentiality, and availability of systems. Despite the integration of Machine Learning (ML) and Deep Learning (DL) algorithms into IDS frameworks, achieving higher accuracy levels while minimizing false alarms remains a challenging task, especially when handling large datasets. In response to this challenge, researchers have turned to bio-inspired algorithms as potential solutions to enhance IDS models. This paper undertakes a comprehensive literature review focusing on augmenting the security of Internet of Things (IoT) networks by integrating bio-inspired methodologies with ML and DL techniques. Among 145 published articles, 25 relevant studies were selected to address the defined research objectives. The findings underscore the efficacy of combining bio-inspired techniques with ML and DL approaches in enhancing IDS performance, highlighting their potential to bolster IoT network security. Furthermore, the review incorporates a comparative analysis of the selected articles, considering various factors, and outlines ongoing challenges and future directions in integrating bio-inspired techniques with ML and DL algorithms.

Keywords Intrusion detection systems (IDSes) · Internet of things (IoT) · Machine learning (ML) · Deep learning (DL) · Bio-inspired · SLR

1 Introduction

In today's rapidly evolving digital landscape, the security of computer networks is of paramount importance. With the proliferation of internet-based communication and the escalating complexity of cyber threats, safeguarding network environments' tasks against unauthorized access and malicious activities has grown considerably more intricate. Intrusion Detection Systems (IDS) have emerged as indispensable tools for monitoring and protecting network integrity, confidentiality, and availability [1]. These systems serve as a crucial defense against a large spectrum of attacks that can disrupt operations and compromise sensitive data. As confirmed in [2], they can detect both known and unknown (zero-day) attacks. Traditional IDS methodologies have predominantly relied on rule-based systems and signature-based detection methods to identify known attack patterns. As referenced in [3], the realm of IoT security is seeing the potential of incorporating various emerging technologies and techniques. However, the ever-evolving landscape of cyber threats demands more adaptive and sophisticated detection mechanisms. In response, the integration of advanced technologies in IoT, such as

✉ Rafika Saadouni
rafika.saadouni@univ-setif.dz

Chirihane Gherbi
chirihane.gherbi@univ-setif.dz

Zibouda Aliouat
zaliouat@univ-setif.dz

Yasmine Harbi
yasmine.harbi@univ-setif.dz

Amina Khacha
amina.khacha@univ-setif.dz

[1] LRSD Laboratory, Ferhat Abbas University of Setif 1, Setif, Algeria

Machine Learning (ML) [4] and Deep Learning (DL) [5], has gained significant attention. ML and DL algorithms can detect anomalies, even in the explicit attack signatures absence, by learning patterns from historical data.

Moreover, the fusion of bio-inspired techniques with ML and DL methodologies presents a promising avenue for further enhancing the capabilities of IDS. Inspired by natural processes, bio-inspired algorithms draw upon the efficiency and adaptability of biological systems to solve complex problems [6]. By mimicking the behaviors of organisms and ecosystems, these algorithms offer a novel approach to address the challenges posed by the evolving threat landscape.

The following subsection discusses related works to highlight the main differences between this survey from the previous ones on IoT security.

1.1 Related reviews

Balasaraswathi et al. [7] presented a comprehensive survey of feature selection methods for IDS, utilizing both non-bio-inspired and bio-inspired optimization algorithms. They evaluated two types of feature selection techniques. The first category was bio-inspired, which included ecology-based algorithms, swarm-based algorithms, and evolutionary algorithms. The second one involved non-Bio-Inspired techniques comparison, such as clustering approach, effect-based approach, correlation-based techniques, Support Vector Machine (SVM), Pulse-Coupled Neural Network (PCNN), Principal Component Analysis (PCA), Linear Discriminant Analysis (LDA), rough-set theory, and mutual information. These techniques were applied to two real datasets (KDD CUP99 and NSL KDD).

Alamiedy et al. [8] explained an overview of optimization algorithms utilized in feature selection, aiming to enhance machine learning classifier performance across diverse problem sets. They categorized these algorithms into two main groups. The initial category comprises non-bio-inspired algorithms, while the second category encompasses bio-inspired algorithms, which include swarm-based, evolutionary, and ecology-based classes.

Kumar et al. [9] conducted a thorough examination of intelligent intrusion detection techniques within the cloud computing environment. They executed a systematic literature review along with a meta-analysis. The study focused, particularly, on three distinct categories of intelligent IDS approaches: computational intelligence algorithms, Machine Learning algorithms and hybrid meta-heuristic algorithms. The authors compared the effectiveness of Machine learning-based IDS in cloud computing and reviewed the computational intelligence approaches, which include bio-inspired algorithms, computation algorithms, evolutionary, and swarm intelligence algorithms. The study also examined the hybridization of algorithms. The results of the study revealed that IDSs founded on hybrid meta-heuristic algorithms exhibited superior attributes. These included heightened accuracy, reduced false positivity rate, and improved detection rate when compared to alternative methodologies.

Di Mauro et al. [10] critically reviewed supervised feature selection techniques for network intrusion detection. They conducted experiments using ML-based engines, comparing feature selection algorithms, from classic rank search to modern bio-inspired ones like genetic search and ant colonies. The study focused on feature correlation, performance metrics and time complexity. Experiments were designed for automated interaction with ML engines.

Mahendran et al. [11] conducted a thorough examination of the security and privacy concerns related to the Internet of Things (IoT) and analyzed the various vulnerabilities and requirements for ensuring the security and privacy of IoT The authors discussed IoT technology, applications, security issues, and countermeasures to prevent attacks in four-layer IoT architecture. They also reviewed how cryptography, bio-inspired computing, and machine learning can secure IoT application's privacy.

Mohammed Ali et al. [12] introduced a comprehensive analysis of machine and deep learning techniques for IoT security. The authors examined a wide range of IoT security threats and attack surfaces, subsequently evaluating various machine and deep learning approaches that can be employed to mitigate these threats. Additionally, they explored the application of machine and deep learning methods to enhance security within the IoT context, illustrating the respective opportunities, advantages, and limitations of each approach. Finally, they concluded by emphasizing the existing challenges and constraints of these techniques and offering future recommendations for future, research endeavors in this domain.

Jan Lansky et al. [13] provided a systematic review of deep learning-based IDs. The authors reviewed a wide range of research articles and existing studies. They discussed the fundamental concepts and techniques of deep learning applied to intrusion detection. They also examined the different types of data used in these systems and analyzed the architectures of deep neural networks used in IDSs. The authors examined commonly used performance measures and assessed the advantages and limitations of these systems compared to traditional intrusion detection approaches. Finally, the article highlights the challenges and opportunities associated with using deep learning in intrusion detection, including data collection, feature selection, model robustness, and privacy, as well as future research directions.

Jeyavim et al. [14] explored the employing of bio-inspired algorithms for network intrusion detection. The

authors described how can bio-inspired algorithms, such as genetic algorithms, evolutionary algorithms, and swarm intelligence, be applied to intrusion detection by exploiting their ability to learn and adapt to new scenarios. They claimed that bio-inspired algorithms could improve intrusion detection in computer networks, but further research is required to understand their benefit and effectiveness in this context.

Saranya et al. [15] evaluated the effectiveness of various Machine Learning techniques used for detecting and preventing intrusions in computer networks. The authors examined a range of Machine Learning algorithms employed in IDS, including both traditional and advanced techniques. They discussed the characteristics, advantages, and limitations of each algorithm, along with their suitability for different types of network environments, and evaluated the performance of these algorithms based on several metrics, such as detection rate, false positive rate, accuracy, and computational efficiency. Finally, the review tackled the challenges and constraints linked to employing Machine Learning algorithms in IDS, including the handling of large-scale data, real-time processing requirements, and adaptability to evolving attack strategies.

Table 1 provides an overview of the current survey studies, emphasizing the significance of our research.

1.2 Motivations and contributions

Unlike other surveys, our work offers a comprehensive study of utilizing bio-inspired techniques within Machine Learning and Deep Learning methodologies, particularly within the realm of IoT security. This survey systematically identifies and contrasts the opportunities, advantages, and limitations of integrating bio-inspired methods with ML/DL techniques for IoT security. Due to the promising results achieved from this fusion in improving the performance of the model and efficiency of the IDS, this work aims to stimulate further investigation and innovation in the field of IoT security and enable researchers to understand the purpose of merging these intelligent approaches.

Our article distinguishes itself from other survey papers in three key ways:

a) We implemented a systematic process for selecting articles to focus on hybrid IDS incorporating ML and DL with bio-inspired elements in IoT networks. In contrast, previous studies [7, 8, 10–12, 14, 15] reviewed IDSs without a systematic approach. A SLR methodology gathers and analyzes information from relevant literature on specific research topics [16]. Its goal is to methodically identify,

Table 1 Related work comparison

Ref	Publication Year	Main contributions	Systematic review	Taxonomy and comparaison	Approach			
					ML	DL	BIT	Hybrid
[7]	2017	Feature selection methods for intrusion detection employing non-bio-inspired and bio-inspired optimization algorithms	✘	✔	✘	✘	✔	✘
[8]	2019	Feature selection for improved performance of machine learning classifiers in anomaly-based IDSs using various algorithms	✘	✔	✘	✘	✘	✔
[9]	2021	Three intelligent IDS approaches employed in the cloud computing environment including ML, computational intelligence, and hybrid meta-heuristics	✔	✔	✔	✘	✔	✔
[10]	2021	Evaluation of Supervised feature selection techniques for network intrusion detection	✘	✘	✘	✘	✔	✘
[11]	2022	Security privacy of IoT applications by using cryptography, bio-inspired computing, and ML	✘	✘	✔	✘	✔	✘
[12]	2020	ML and DL methods for IoT security	✘	✔	✔	✔	✘	✘
[13]	2021	Use of DL techniques for detecting and preventing intrusions in computer systems	✔	✔	✘	✔	✘	✘
[14]	2022	Effectiveness of applying bio-inspired algorithms to enhance network intrusion detection	✘	✔	✘	✘	✔	✘
[15]	2020	Effectiveness of ML algorithms in intrusion detection systems	✘	✔	✔	✘	✘	✘
Our survey	2023	Bio-inspired and ML integration for enhancing IoT security	✔	✔	✔	✔	✔	✔

DL: Deep Learning, ML: Machine Learning, BIT: Bio-Inspired Techniques

classify, and compare existing studies in a particular field, offering a comprehensive overview of the research landscape. Although studies [9] and [13] employed systematic literature review methodologies, the study [9] concentrated solely on IDS in cloud environments, and the study [13] exclusively utilized DL-based IDS.

b) Our study reviewed articles published between 2019 and 2023, ensuring an updated perspective and insights into the latest trends at the intersection of bio-inspired fusion with ML and DL for IDS.

c) A comprehensive comparison of recent IDS utilizing ML, DL, and bio-inspired approaches is conducted in our study, analyzing their methodologies, techniques, datasets, evaluation metrics, advantages, and drawbacks.

The primary contributions of this work include:

- Introduction of a novel taxonomy of IDSs based on bio-inspired, ML, and DL techniques, specifically tailored for IoT security.
- Conducting a comprehensive comparison between bio-inspired and ML-based IDS and bio-inspired and DL-based IDS.
- Identifying and emphasizing open issues and challenges associated with the integration of both bio-inspired with ML techniques and bio-inspired with DL techniques in the context of IoT security.
- Several potential research future directions of bio-inspired and ML for IoT security are presented.

1.3 Paper organization

Figure 1 illustrates the structure of this study. In Sect. 2, we provide a brief introduction to ML approaches, DL approaches, Bio-Inspired techniques, and IDS classification. Section 3 outlines the steps of the systematic literature review (SLR) methodology used in this research. In Sect. 4, we classify, analyze, and compare the selected articles. The study results, as well as the identified open issues and challenges, are discussed in Sect. 5. Our study is then concluded in Sect. 6.

2 Background

2.1 Machine learning techniques for IoT-IDS

Machine Learning forms a subset of Artificial Intelligence (AI), enabling systems to enhance their automated skills through experience, bypassing explicit programming Via mathematical models. ML techniques allow machines to learn, identify patterns, and make data-driven decisions autonomously [15]. There are four main categories of ML algorithms: supervised, unsupervised, semi-supervised, and reinforcement learning. These categories can be harnessed to detect sophisticated attacks and establish a sturdy IDS. As depicted in Fig. 2, the classification of ML techniques utilized in IDS for IoT environments can be discerned.

2.1.1 Supervised learning algorithms

Supervised learning deals with fully class-labeled data and focuses on finding the relationship between data and its corresponding classes. The objective of supervised learning is to minimize the discrepancy between predicted outputs and actual labels, enabling the model to recognize patterns and generalize its understanding when dealing with new, unseen data points. The process involves two main tasks: classification and regression.

Classification: involves two steps, training, and testing, where the algorithm uses labeled data to learn from the response variable and the output is a fixed such as [True, False], [Yes, No], or [normal, attack], among others. The upcoming sections will illustrate various classification learning approaches, encompassing Support Vector Machine (SVM), K-Nearest Neighbor (KNN), Random Forest (RF), Naive Bayes (NB), Decision Trees (DT), and Logistic Regression (LR).

- **Support Vector Machine (SVM)**: is grounded on the concept of a hyperplane of maximum-margin separation in an n-dimensional feature set comprising two or more classes. It is adept at resolving both linear and nonlinear issues. The SVM algorithm discovers the splitting hyperplane through the maximal distance between the nearest data point of every class compared [17].
- **K-Nearest Neighbor (KNN)**: relies on the concept of similarity between features to predict the class of a given data sample. Specifically, the Euclidean distance metric is employed to measure the distance between neighboring instances, enabling the identification of new data points based on their proximity to already observed classes [18].
- **Random forest (RF)**: represents a specialized machine learning approach that leverages multiple Decision Trees (DTs) to establish a precise and resilient classification algorithm. The methodology involves the creation of a set of DTs, each constructed randomly, and collectively trained to yield classification outcomes through a process known as majority voting [19]. While DTs form the foundational components of RF, they differ in operation. DTs generate a rule set during training for subsequent classification, whereas RF

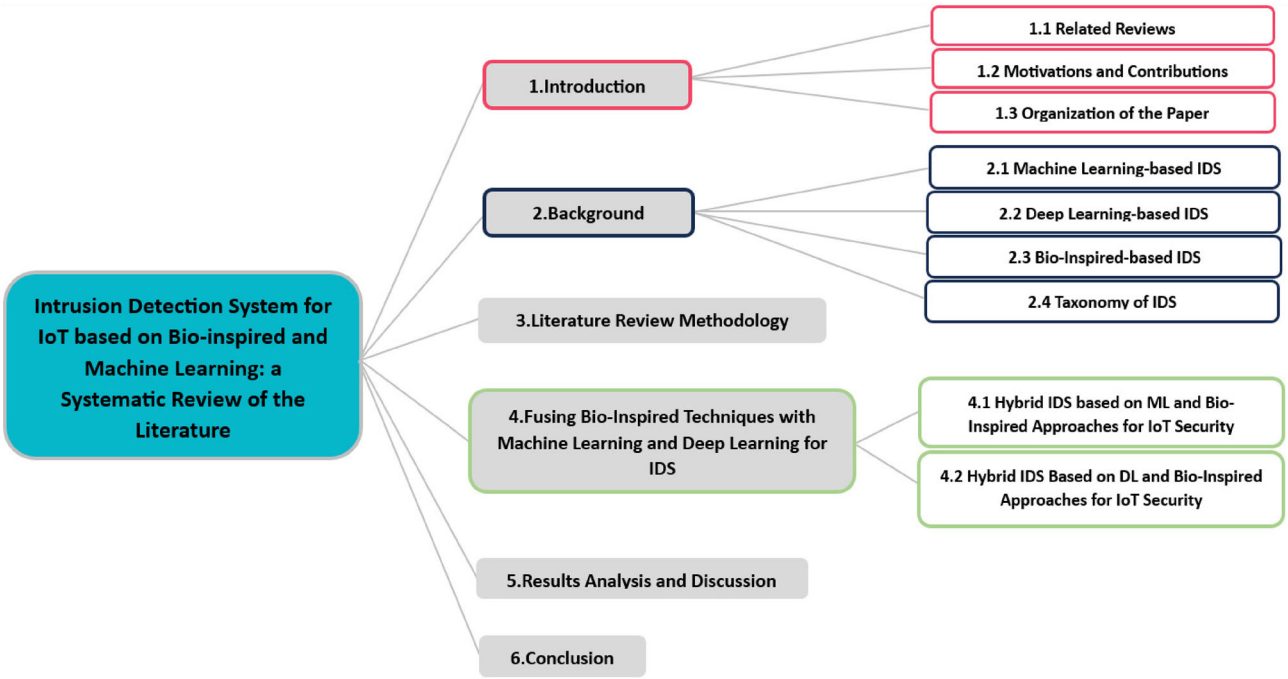

Fig. 1 Review's Structural Flow

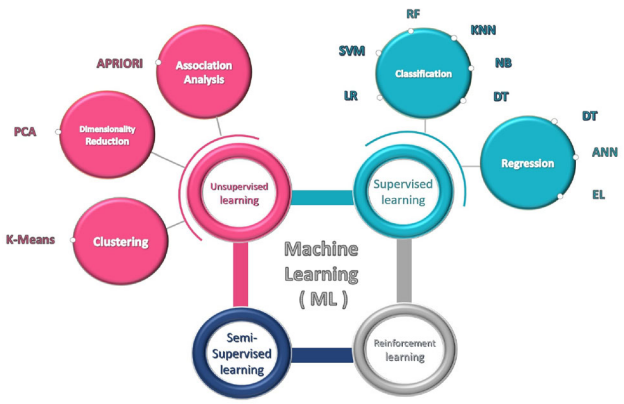

Fig. 2 Machine Learning Techniques for IoT-IDS

assembles a rule subset using the complete set of DTs. This approach contributes to a more robust and accurate classification output, effectively countering overfitting. Furthermore, RF requires fewer inputs and eliminates the necessity for the intricate process of feature selection [20].

– **Naïve Bayes (NB)**: is a form of Bayesian theorem used to predict event probabilities based on prior observations [21]. This supervised learning method is employed for classifying normal and abnormal behaviors using present data through Bayesian probability. NB is commonly utilized in IoT for intrusion detection and anomaly classification [22].
– **Logistic regression (LR)**: is a statistical method used for predictive analysis, especially effective in scenarios involving binary and linear classification tasks. It employs the sigmoid function to transform predicted values into probabilities that range between 0 and 1. As a classification model, it is characterized by its straightforward implementation and is particularly well-suited for situations where data classes can be separated linearly [23].

Regression: involves predicting a real number or a continuous value as the output based on input variables. Various regression techniques, including Artificial Neural Network (ANN), Decision Tree (DT), and Ensemble Learning (EL), are elaborated upon in the following subsections.

– **Artificial neural networks (ANNs)**: are inspired by the structure of the human brain, utilizing interconnected neurons. These neurons, organized into processing elements, establish connections that form the network. There are two primary categories in the NN algorithm: hierarchical and interconnected networks. These networks are defined by various functional layers of neurons, such as input, hidden, and output layers. The backpropagation algorithm is employed as a learning technique for training the ANN. The key benefit of utilizing ANN is its ability to reduce network response time, thereby enhancing IoT performance [24]. However, NNs are inherently computationally complex and

challenging to implement within a distributed IoT system [25].

- **Decision Trees (DTs)**: resemble trees with branches and leaves, where each branch represents an attribute or feature, and each leaf signifies a decision or classification. By traversing from the root node to the leaves, DT classifies samples based on their feature values using knowledge gained from prior datasets [26]. The foundation of DT lies in its root node, which identifies the feature that optimally splits the training samples. This branching process continues, allowing the tree to learn and classify data. Within ML, DT falls into two primary categories: classification and regression [27]. One of the strengths of DT algorithms is their ability to automatically select the most informative features for constructing the tree. To prevent overfitting, pruning techniques are employed to trim irrelevant branches. Prominent DT models include CART, C4.5, and ID [28]. In the realm of security applications, DTs provide significant utility as classifiers [22, 29].
- **Ensemble Learning**: refers to a collaborative learning approach where different classification techniques (either homogeneous or heterogeneous multi-classifiers) are employed in tandem to achieve accurate and robustly estimating outcomes [30]. Given that each classifier possesses distinct strengths and weaknesses, some excelling at detecting specific attack types while underperforming others, the ensemble strategy is designed to address these limitations by training multiple classifiers and constructing a robust classifier. Among the homogeneous methods, commonly utilized models include Bagging, Bagging Random Subspace, Rotation Forest, Tree Ensemble, and Dagging. On the other hand, in the realm of heterogeneous approaches, Stacking and Voting are the prevalent choices.

2.1.2 Unsupervised learning algorithms

Unsupervised learning is a branch of ML that can be applied in intrusion detection by training algorithms on unlabeled data, where explicit target variables or labels are absent during the training process. This is achieved through techniques like clustering, dimensionality reduction, and association analysis.

Clustering: involves grouping similar data points into distinct clusters, based on their shared characteristics or proximity in a feature space. K-means is a prominent method widely utilized in IDS, it forms small groups to categorize data samples into clusters by grouping highly similar data based on Euclidean distance from cluster centroids [31, 32]. It involves iteratively recalculating cluster centroids by averaging data points in each cluster, aiming to minimize distances within clusters and maximize distances between clusters through iterative optimization of an objective function [33, 34]. The process continues until no further cluster modifications can be made.

Dimensionality reduction: is a technique that aims to reduce the number of input features or variables while preserving as much relevant information as possible. A widely used method for this purpose is Principal Component Analysis (PCA), particularly prevalent in IDS. It is recognized as a feature reduction or feature selection technique, aimed at transforming a large dataset into a smaller version while retaining the same information content. The PCA's chosen feature sets can be coupled with other algorithms to detect anomalies and intrusions in IoT networks by reducing the system complexity [35].

Association analysis: refers to the process of identifying relationships or patterns among items within a dataset. Apriori is a notable example of such a method, extensively employed in IDS. It is developed by Agrawal and Sriknat [36], utilized for uncovering frequent item sets via Boolean rules. It stands out as a notable technique in the realm of association rule mining. In the context of IDS, the Apriori algorithm can be applied to uncover associations between different types of events or activities that might indicate potential security threats or anomalies [22].

2.1.3 Semi-supervised learning

The semi-supervised learning is a hybrid approach combining unsupervised and supervised learning. It utilizes both unlabeled data and a small amount of labeled data during training, enabling it to discover patterns in unlabeled data and improve predictive accuracy with limited labels. This makes semi-supervised learning promising in domains with scarce labeled data, addressing the challenges of fully unsupervised or supervised learning.

2.1.4 Reinforcement learning

Reinforcement Learning (RL) emulates human learning by allowing machines to interact with their environment and optimize feedback through action [37]. In network security, RL models are designed for cyberattack detection and prevention. These models learn from past experiences to identify attack indicators, triggering alerts for human intervention when suspicious patterns or behaviors are detected, ensuring thorough investigation if needed.

2.2 Deep learning techniques for IoT-IDS

Deep learning (DL) encompasses the use of deep neural networks, incorporating numerous hidden layers to capture intricate features within a deep network. It can be

categorized into three models: discriminative, generative, and hybrid. This section outlines the DL approaches employed for developing IDS solutions in the reviewed articles.

2.2.1 Discriminative mode

Discriminative (or supervised) architectures are primarily employed with labeled data to discern patterns for prediction tasks. The subsequent section outlines the prevalent discriminative deep learning architectures frequently utilized in the context of security.

- **Convolutional Neural Network (CNN)**: is a deep learning framework optimized for array-based data. It is recognized as a neural network capable of initially extracting finer-resolution features and subsequently refining them into more complex features at a broader resolution [5]. This architecture comprises an input layer, a sequence of convolutional and pooling layers for feature extraction, terminating with a fully connected layer, and a softmax classifier situated within the classification layer.
- **Recurrent Neural Network (RNN)**: is a type of neural network characterized by having a connection graph that includes at least one cycle [5]. The RNN is composed of input units, hidden units functioning as memory components, and output units. Each RNN unit leverages its current input and the previous output for decision-making. RNNs have been enhanced with diverse memory unit variations, with Long Short-Term Memory (LSTM) [38] and Gated Recurrent Unit (GRU) [39], standing out as the most notable options.
- **Deep Neural Network (DNN)**: forms a fundamental architecture in deep learning, facilitating learning through multiple layers commonly termed Multi-Layer Perceptrons (MLP). The structure of a DNN includes an input layer, an output layer, and multiple hidden layers. MLP represents a variant of a feedforward artificial neural network, known for its sequential arrangement of many layers [5].

2.2.2 Generative mode

Unsupervised deep learning architectures, often referred to as generative models, possess the ability to learn from unlabeled raw data for diverse task achievements autonomously. The subsequent list encompasses the prevalent architectures within this classification.

- **Restricted Boltzmann Machine (RBM)**: is a model comprising two layers; an input layer and a hidden layer, allowing data flow in both directions. These two layers are interconnected through a specific set of weights. Connections between units within the same layer are absent in RBM [5].
- **Deep Boltzmann Machine (DBM)**: is characterized by a network of symmetrically interconnected stochastic binary units. This network encompasses both visible units and a series of hidden unit layers [5]. The architecture of a DBM is derived from a broader concept known as a general Boltzmann machine (BM), which itself comprises units that make stochastic decisions to determine their active and inactive states [40].
- **Deep Belief Network (DBN)**: is a multi-layered belief network, with each layer being a RBM. In the context of DL, DBN is constructed by vertically stacking several RBMs, followed by a softmax classification layer. The DBN consists of visible units and hidden units. The visible units layer represents the data, while the hidden units layer learns to extract features [5, 41].
- **AutoEncoder (AE)**: is a popular DL technique that works in an Encoder-Decoder fashion. Its fundamental concept revolves around minimizing the gap between output and input by acquiring optimal features [42]. The architecture comprises input and output layers with matching dimensions, whereas the hidden layers typically possess smaller dimensions compared to the input layer. Notable variants of AE include Sparse AE, Stacked AE and Variational AE [43].

2.2.3 Hybrid mode

Hybrid structures combine generative and discriminative models, leveraging generative attributes in initial phases and discriminative attributes in later stages for effective data differentiation.

- **Generative Adversarial Network (GAN)**: represents a hybrid DL technique that uses both generative and discriminative models at the same time for training. This method involves the generative model predicting the dataset's distributions and sample origins, while the discriminative model verifies these predictions. In this interplay, the generative model strives to deceive by generating samples using random noise, while the discriminative model seeks to differentiate between authentic training data and the deceptive features generated by the generative model [44].
- Ensemble of DL Networks (EDLNs): involve employing multiple DL algorithms simultaneously by organizing them into an ensemble. This collaborative approach aims to generate improved outcomes compared to individual DL components [45]. Within EDLNs, diverse combinations of discriminative, generative,

and hybrid DL algorithms can be employed. Heterogeneous EDLNs incorporate classifiers from various genres, while homogeneous EDLNs employ classifiers of the same genre (Fig. 3).

2.3 Bio-inspired techniques

Bio-inspired refers to the design, concepts, or approaches that are inspired by biological systems, processes, or structures found in nature. Bio-inspired algorithms emulate biological patterns and behaviors to creatively tackle intricate optimization challenges, drawing insights from natural processes for innovative problem-solving approaches [6]. In the context of IDS, these systems derive inspiration from natural defense mechanisms to elevate the precision and efficiency of detecting potential threats within digital environments [46]. Figure 4 illustrates the bio-inspired algorithms, which are categorized into three distinct types of inspirations: evolutionary, swarm-based, and ecology.

2.3.1 Evolutionary algorithms (EA)

Evolutionary algorithms (EA) draw inspiration from biological processes and intellectual methodologies. These algorithms utilize iterative refinement to leverage various collective phenomena within dynamic populations of problem solvers. This approach encompasses concepts akin to biological evolution, growth patterns, selection dynamics, reproduction strategies, and survival mechanisms present within a population [47]. Each algorithm starts with an initial feasible solution population, then i teratively advances across generations to converge upon the best solution [48]. Within this solution population, the EA algorithm employs fitness-based selection, favoring the

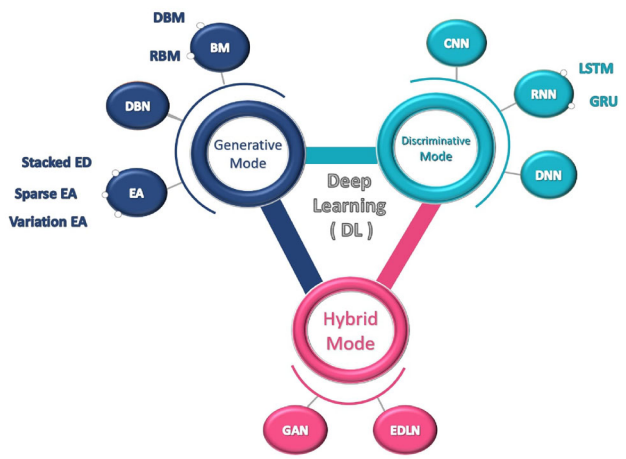

Fig. 3 Deep learning techniques for IoT-IDS

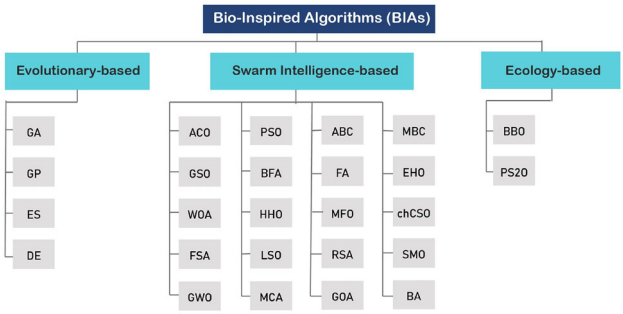

Fig. 4 Classification of bio-inspired Techniques

propagation of improved solutions to successive generations [43].

EAs are integral for optimizing classifier features or parameters in IDS attack classification. These algorithms treat dataset features as chromosomes, gauging feature importance through fitness evaluation. The chosen features subsequently integrate into the classification module, where diverse attack patterns drive effective classification [42].

2.3.2 Swarm intelligence algorithms

Swarm intelligence, also known as collective intelligence, pertains to the examination of how social insects demonstrate problem-solving skills in intricate situations. This includes scenarios like optimizing routes between nests and food sources [49]. Although lacking individual expertise, these insects achieve remarkable results by leveraging swarm behavior and communication. This allows them to collectively converge on global solutions for specific applications. Numerical optimization techniques have been harnessed to simulate the behavior of diverse swarms observed in activities such as hunting and mating [50].

Swarm Intelligence algorithms adhere to five fundamental principles: quality, proximity, diverse response, adaptability, and stability. These algorithms commence with an initialization phase to configure parameter values and persistently operate until specified termination conditions are met or a stop criterion is triggered. The fitness function is evaluated for each solution, leading to mathematical adjustments guided by the results. Assessing fitness functions for individual solutions or search agents in the swarm aids in proposing a taxonomy and identifying the most suitable solution for the problem [51].

2.3.3 Ecology-based algorithms

Comprising populations of individuals, these systems undergo growth through optimization strategies. Thus, individuals within each population are adjusted using

intensification and diversification mechanisms, featuring distinct initial parameters for each strategy. Ecology-based systems can manifest in two forms: homogeneous and heterogeneous. Under the homogeneous model, all populations evolve using the same optimization strategy and identical parameters. Conversely, within the heterogeneous model, strategies or parameters have the potential to vary among populations. [7].

Table 2 defines all abbreviations corresponding to bio-inspired algorithms shown in Fig. 4.

2.4 Proposed taxonomy of IDS for IoT

The classification of IDS based on bio-inspired and ML techniques is organized according to different aspects, including the detection strategy, the deployment strategy, and the evaluation strategy. Our proposed taxonomy of IDS for IoT is shown in Fig. 5.

a) **Detection strategy** Various elements are involved in the detection strategy of IDS, encompassing approaches, techniques, detection types, and classification types. These aspects are subdivided into different categories. Approaches are grouped into four classifications based on the analysis approach utilized for intrusion detection: signature-based IDS [75], anomaly-based IDS [76], specification-based IDS [77], and hybrid IDS [78]. Meanwhile, the detection techniques stem from diverse sources such as Deep Learning (DL), Machine Learning (ML), bio-inspired techniques, and hybrid methodologies. In terms of intrusion classification, it can either be binary, distinguishing between normal and abnormal behaviors, or multi-class, attributing the intrusion to a specific attack category. Moreover, the detection system's operation can fall into two categories: online operation, which is suitable for real-time systems, or offline operation.

b) **Deployement strategy** The deployment strategy can be divided into two main categories: one based on the level and the other based on the system architecture. From the perspective of the level-based strategy for Intrusion Detection Systems (IDS), they can be further classified into two subcategories: Network-Based IDS (NIDS), Host-Based IDS (HIDS), or a combination of the two in a hybrid setup [76, 79]. NIDS is deployed at the network level to safeguard all devices and the entire network against intrusions. NIDS continuously monitors network traffic, identifying potential security breaches and policy violations. On the other hand, HIDS is implemented on a single information host. Its role involves monitoring all activities on this specific host, scanning for any violations of its security policies, and detecting suspicious behaviors. The deployment architecture determines the configuration of IDS components, which can be categorized based on their architectural type: centralized, distributed, or hybrid. In a centralized architecture, data is collected from one or multiple sources and then all processing takes place at a central location. In a distributed architecture, IDS components are dispersed across various physical locations. A hybrid architecture combines elements of both centralized and distributed approaches.

c) **Evaluation strategy** The intended Intrusion Detection System (IDS) needs to meet both performance and security criteria. The confusion matrix stands out as the primary metric frequently employed in assessing the efficacy of IDS. A range of metrics, such as accuracy, precision, detection rate, recall, F-score, and false alarm rate (FAR), can be derived from this matrix. Additionally, assessing the efficiency of the IDS involves evaluating factors like

Table 2 Abbreviations of bio-inspired Techniques

Abbreviation	Definition	References
GA	Genetic Algorithm	[52]
GP	Genetic Programming	[53]
ES	Evolutionary Strategy	[54]
DE	Differentiated Evolution	[55]
ACO	Ant Colony Optimization	[56]
PSO	Particle Swarm Optimization	[57]
GSO	Glowworm Swarm Optimization	[58]
BFA	Bacterial Foraging Algorithm	[59]
FA	Firefly Algorithm	[60]
ABC	Artificial Bee Colony	[61]
EHO	Elephant Herding Optimization	[62]
WOA	Whale Optimization Algorithm	[63]
HHO	Harmony Search Algorithm	[64]
MBC	Modified Bee Colony algorithm	[59]
ChCSO	Chimp Chicken Swarm Optimization	[65]
MFO	Moth Flame Optimization	[29]
FSA	Flamingo Search Algorithm	[66]
RSA	Reptile SearchAlgorithm	[67]
LSO	Locust Swarm Optimization	[68]
SMO	Spider Monkey Optimization	[69]
GWO	Grey Wolf Optimization	[70]
MCA	Meerkat Clan Algorithm	[22]
GOA	Grasshopper optimization algorithm	[71]
BA	Bat Algorithm	[72]
BBO	Biogeography Based Optimization	[73]
PS2O	Symbiosis	[74]

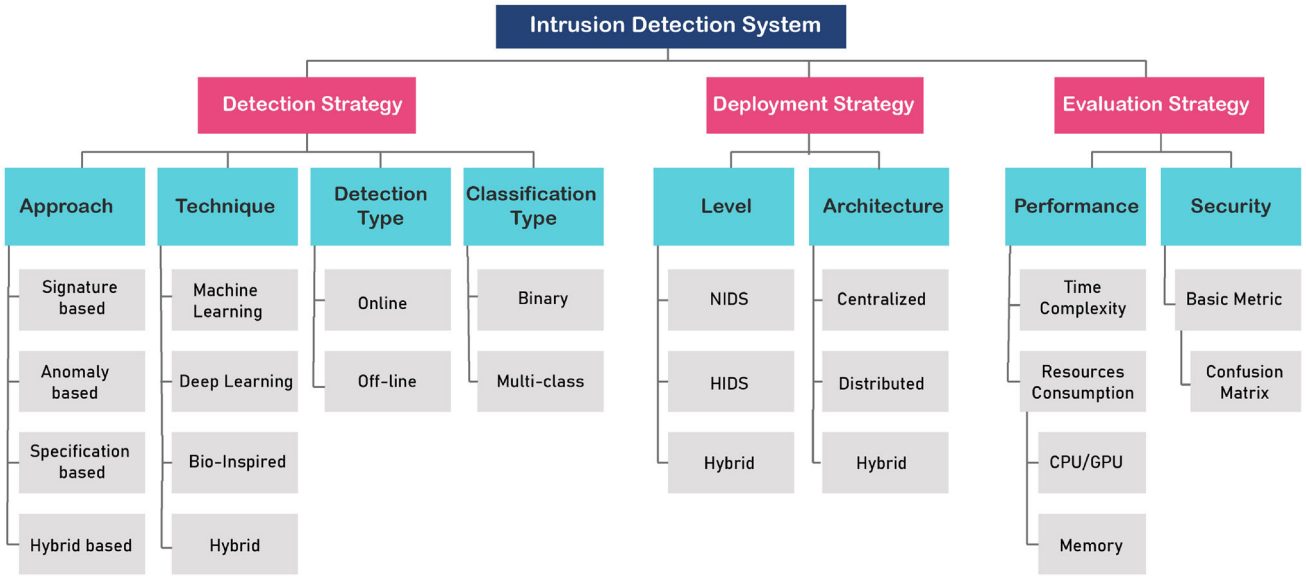

Fig. 5 Proposed Taxonomy of IDS in IoT

resource utilization (CPUGPU and memory) and the complexity of processing time [80].

2.5 Summary

Securing IoT systems presents a multifaceted challenge, demanding comprehensive solutions that leverage various approaches to capitalize on their respective advantages and establish robust security measures. Several promising technologies and techniques are explored, focusing on the most widely adopted models of Machine Learning and Deep Learning techniques for Intrusion Detection Systems in IoT environments. Additionally, a variety of bio-inspired algorithms, categorized into three distinct types of inspirations, offer innovative solutions for enhancing security. Finally, a proposed taxonomy of IDS for IoT is introduced, integrating these diverse approaches to furnish a structured framework for classifying and analyzing IDS solutions in IoT environments.

3 Literature review methodology

This research delves into the integration of bio-inspired algorithms with both Machine Learning (ML) and Deep Learning (DL) techniques to enhance the security of IoT networks. This investigation is conducted using a Systematic Literature Review (SLR) methodology. Our review methodology comprises five steps including review questions, data searching, initial selection, data filtering, and final selection.

First, the study establishes a set of research questions (RQs) that encompass the goals and scope of our inquiry. Table 3 outlines the precise research questions that have been identified to fulfill the stated objectives.

Secondly, the process of article retrieval involved employing targeted keywords related to the subject matter. We utilized the Boolean operator"AND"to combine key search terms, which encompassed"Machine Learning," "Deep Learning," "bio-inspired," "Hybrid Approaches,"and"Intrusion Detection System."Additionally, we employed the Boolean operator"OR"to encompass synonyms and alternative spellings of the primary keywords, such as"ML,""DL," "IDS,""Nature-Inspired,"or"algorithms."

To identify pertinent works, we conducted thorough searches across various digital databases, including IEEE Xplore, Elsevier, Springer, and IAES journals. In the initial screening, we selected a total of 145 research papers that had been published within the past five years (from 2019 to 2023). The distribution of research studies by each considered publisher is depicted in Fig. 6. Notably, a significant portion of the research articles, amounting to 32%, 20%, and 12% respectively, were published in the prominent databases: IEEE, Elsevier, and MDPI.

In the subsequent phase, we reexamined the titles, abstracts, and keywords of every article, employing the predefined inclusion and exclusion criteria outlined in Table 4. The process of refining our selection is depicted in Fig. 7, illustrating the stages of study selection guided by our inclusion and exclusion guidelines.

Initially, our search yielded 131 articles meeting these criteria. Subsequently, we removed Duplicated articles,

Table 3 Research questions

	Qestion	Objective
RQ1	Why is the combination of bio-inspired and ML techniques employed for IoT-IDS?	To inquire about the rationale behind the integration of these techniques to detect intrusions in the IoT systems
RQ2	How can the integration of bio-inspired techniques with ML contribute to enhancing the security of IoT systems?	To explore the potential ways through which these hybridization techniques can be used to improve the security of IoT systems
RQ3	What are the most commonly used datasets and evaluation metrics for hybrid IoT-IDS assessment considering security parameters?	To comprehend and be familiar with the frequently employed datasets and performance measures used to assess the efficacy of these hybrid IDS within the realm of the IoT, while considering security parameters
RQ4	What are the strengths and weaknesses of blending ML and bio-inspired techniques for IoT security?	To explore the potential benefits and drawbacks of combining these techniques to enhance security in the context of the IoT
RQ5	What is the impact of implementing the amalgamated approaches in real-world scenarios for IoT security?	To evaluate the effectiveness and implications of implementing amalgamated approaches for IoT security in real-world scenarios
RQ6	What are open issues raised by the integration of bio-inspired techniques with ML?	To identify and understand the unresolved challenges that emerge when combining bio-inspired techniques with both machine learning and deep learning

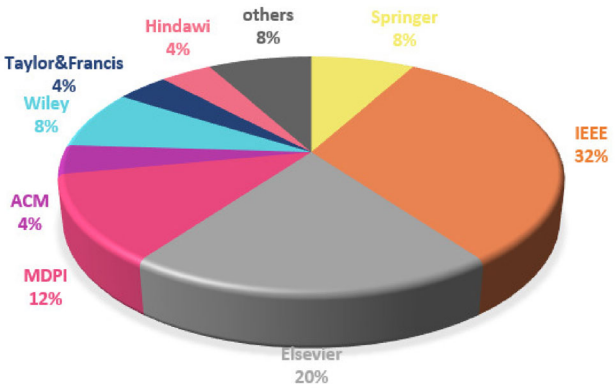

Fig. 6 Percentage of research studies by publisher

those lacking peer review, and studies exploring machine learning or deep learning-based IDS without a focus on their integration with bio-inspired techniques.

Consequently, we arrived at a final set of 25 research articles that precisely addressed the specific analytical queries identified in our systematic review.

3.1 Summary

In this section, we conducted a systematic literature review to select papers focusing on the integration of bio-inspired techniques with ML and DL. To guide our review process, we formulated specific research questions (RQs) and outlined their objectives. We established inclusion and exclusion criteria to streamline the selection process. From a pool of 145 papers, we meticulously evaluated each against our criteria, resulting in the final selection of 25 research articles. These chosen articles directly addressed the analytical queries outlined in our systematic review, providing a solid basis for our investigation into the integration of bio-inspired methodologies with ML and DL.

4 Fusing bio-inspired techniques with machine learning and deep learning for IDS

In this section, we provide a comprehensive overview of the chosen articles following the Systematic Literature Review (SLR) methodology. The selected articles fall into two classes: IDS based on Machine Learning (ML) with bio-inspired approaches, as depicted in Table 5, and IDS based on Deep Learning (DL) with bio-inspired approaches as summarized in Table 6. Researchers have devised these innovative approaches to enhance attack detection within IoT networks. Moreover, we are in the process of

Table 4 Inclusion and exclusion criteria of our work

Inclusion criteria	Exclusion criteria
Articles published between 2019 and 2023	Duplicated and non-available articles
Papers published in a reputable journal or conference proceeding	Articles not peer-reviewed
Articles focus on the fusion of bio-inspired with ML and DL for IoT security	Articles do not discuss the hybridization of bio-inspired approaches with ML or DL

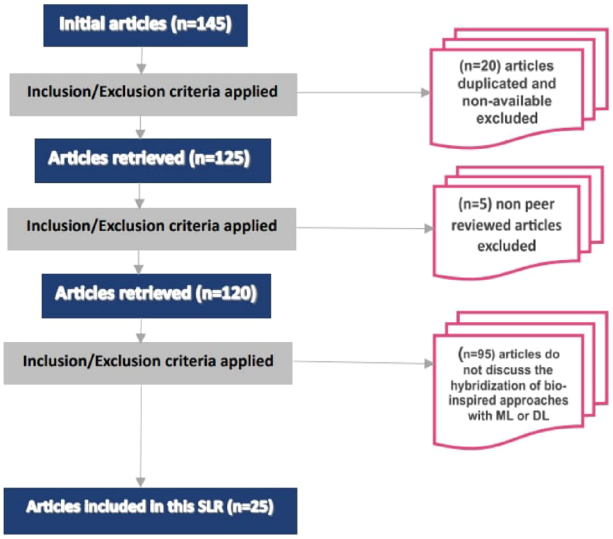

Fig. 7 Articles selection process

conducting a comparative analysis of the reviewed studies, taking into account various parameters including metrics, datasets, environment, tools, and programming language used in the implementation. Additionally, we highlight the respective strengths and limitations of each methodology.

4.1 Hybrid IDs based on ML and bio-inspired approaches for IoT security

Wathiq et al. [60] introduced a combination of the Firefly Algorithm (FA) and SVM to build a robust intrusion detection system. Their method utilized FA to reduce features by 76%, from 41 to 10. Subsequently, they utilized SVM as a classifier to evaluate this feature subset. Regarding performance, the proposed model generally achieved an accuracy level of approximately 78.89%, maintaining an acceptable false alarm rate of 2.5% when tested on the NSL-KDD dataset. However, the sensitivity to specific parameter choices in both SVM and FA parameters is notable. These parameters significantly influence the algorithm's performance, convergence, and behavior. Consequently, fine-tuning these parameters presents a significant challenge.

Vijayanand et al. [81] created a Wireless Mesh Networks (WMNs) specific IDS using the Whale Optimization Algorithm (WOA) and Genetic Operators for feature selection, aiming to pinpoint crucial features for an SVM-based IDS. Their enhanced WOA, integrating genetic algorithm operators, notably improved attack detection, achieving 95.91% accuracy on the CICIDS2017 dataset and 94.44% on the ADFA-LD dataset, outperforming standard WOA and other algorithms. Despite superior intrusion detection, their method extended training time due to the selection of more informative features.

Sweta et al. [35] devised an innovative IDS by amalgamating Principal Component Analysis (PCA), the firefly optimization algorithm, and XGBoost. Their evaluation utilized a dataset collected from Kaggle, initially preprocessed through One-Hot encoding for categorical-to-numeric conversion, followed by standard scaler normalization. Subsequently, PCA reduced dataset dimensionality, and the firefly optimization algorithm identified the most pertinent attributes. Finally, the XGBoost algorithm was trained on the selected attributes. Though lacking specifics on the classification type, dataset name, and encompassed attacks, their PCA-firefly-XGBoost model exhibited notable performance with exceptional accuracy (99.9%), sensitivity (93.1%), and specificity (99.9%) metrics compared to conventional machine learning methods.

Sydney et al. [82] explored an IDS for the Industrial Internet of Things (IIoT) using Genetic Algorithm (GA) combined with Random Forest (RF) for feature selection. The GA-RF method generated 10 feature vectors for binary classification and 7 for multiclass, each with varying attribute sets. The study employed the UNSW-NB15 dataset and evaluated several classifiers, such as RF, LR, NB, DT, ET, and XGB. In binary classification, RF classifier achieved the best results. For multi-class, Extra-Trees (ET) performed best. While the authors explored IDS for the Industrial Internet of Things, their study did not employ a dataset exclusively focused on IIoT. Despite promising results, they acknowledged the necessity for further experiments utilizing the TON-IoT dataset, consisting of traffic patterns predominantly generated by IIoT devices, to validate their proposed methodology.

Shubhra et al. [71]introduced EFSGO, an efficient intrusion detection system merging Ensemble Feature Selection (EFS) with the Grasshopper Optimization Algorithm (GOA). EFS initially trims redundant attributes, followed by GOA identifying significant features from the reduced set. The GOA, employing SVM as a fitness function, optimizes parameters for enhanced attack classification accuracy. Results in the NSL-KDD dataset showcased a 99.69% detection rate, 99.98% accuracy, and a 0.07 false alarm rate. In the KDD Cup 99 data, EFSGO achieved 99.26% detection, 99.89% accuracy, and a 0.097 false alarm rate. Despite effectiveness, using old datasets with limited attacks may not mirror real-world network scenarios accurately.

Arar et al. [29] presented a feature selection method for intrusion detection using the Moth Flame Optimization (MFO) algorithm alongside the decision tree (DT) classifier. MFO identified crucial features, reducing the feature count from 78 to 4 for DoS, BotNet, and Port Scan attacks.

Table 5 Summary of models integrating Bio-Inspired techniques and Machine Learning algorithms

Ref.	Year	Models	Classification Type	Dataset	Metrics	Simulators/ Tools	Language	Advantages	Disadvantages
[60]	2019	FA-SVM	Multi-class	NSL-KDD	Accuracy FAR	MATLAB	N/A	(+)Decrease training and testing time	(-)Sensitive to the selection of algorithm-specific parameters
[81]	2020	GA-WOA-SVM	Multi-class	CICIDS2017 ADFA-LD	Detection Rate Sensitivity Specificity Precision	Matlab 2014b	N/A	(+)Improve intrusion detection. (+)Reduce the classifier's computational complexity	(-)Training requires additional time
[35]	2020	PCA-firefly-XGBoost	N/A	collected from Kaggle	Accuracy Sensitivity Specificity	Google Colab	Python	(+)Time complexity reduction. (+)Efficiently addresses overfitting. (+)Proficient with missing values	(-)Lack of specificity regarding the classification type, dataset name, and included attacks
[82]	2021	GA-RF (RF, LR, NB, DT, ET, XGB)	Binary Multi-class	UNSW-NB15	Accuracy Precision Recall F1-Score	Scikit-Learn	Python	(+)Acceptable level of attack detection	(-)UNSW-NB15 lacks exclusive focus on Industrial Internet of Things (IIoT)
[71]	2021	EFS-GOA-SVM	Multi-class	NSL-KDD KDD CUP99	Accuracy Detection Rate FAR	MATLAB R2016a	N/A	(+)Decrease training time. (+)Enhance performance metrics	(-)Datasets outdated, attacks limited
[29]	2021	MFO-DT	Multi-class	CICIDS2017	Accuracy Detection Rate	Evolopy-master Weka Gui tool	Python Java	(+)Flexibility and robustness (+)Decrease training time	(-)Substantial reduction of features
[22]	2021	MIMCA-DT MIMCA-NB MIMCA Apriori	Binary	CICIDS2017	Accuracy Time	ORANGE	Python	(+)Minimize the time required	(-)Absence of Multi-Class Classification
[83]	2022	BMRF-RF	Multi-class	NSL-KDD CICIDS2017	Accuracy Precision Recall F-measure Execution time	Jupyter Notebook	Python	(+)Feature reduction capability. (+)Superior performance compared to other methods	(-)Slower execution times compared to other methods
[52]	2022	K-means-GA-SVM	N/A	NSL-KDD	Accuracy Detection Rate FAR	MATLAB	MATLAB	(+)High accuracy, low error. (+)Best training time compared other works	(-)Lacks specificity on classification type. (-)Single and dated dataset evaluation
[84]	2022	HHO-PSO-SVM	Binary	NSL-KDD	Accuracy Precision Sensitivity Specificity F1-Score	MATLAB R2021a	NA	(+)Ability to fine-tune SVM parameters. (+)Overcoming local optima problems. (+)Addressing early convergence issues	(-)Limited to detecting DDoS attacks in cloud computing. (-)Absence of Multi- Class Classification. (-)Single dataset evaluation

Table 5 (continued)

Ref.	Year	Models	Classification Type	Dataset	Metrics	Simulators/ Tools	Language	Advantages	Disadvantages
[85]	2023	(RFE-PSO-GWO-GA-RF	Multi-class	CSE-CIC-IDS-2018	Accuracy Precision Detection Rate F1-Score	Jupyter Notebook Google Colab	Python	(+)Feature reduction capability. (+)High accuracy	(-)Lower performance in Infiltration Attacks compared to others. (-)Single dataset evaluation
[56]	2023	ACO-PSO-SVM	N/A	image dataset	Accuracy Recall Precision F1-Score	N/A	Python	(+)Effective and lightweight model. (+)Ability to fine-tune SVM parameters	(-)Single dataset evaluation. (-)Absence of training and testing time discussion. (-)Lacks specificity on classification type
[57]	2023	IG-CS-PSO-RF	Multi-class	UNSW-NB15 Kyoto	Accuracy Recall Precision F1-Score FAR	Google Co-laboratory Pro	Python	(+)Feature reduction capability. (+)High level of attack detection. (+)Best training and testing time compared to other works	(-)Potential overfitting risk. (-)Possibility of underfitting due to overlooked important features

The study, based on the CICID2017 dataset, allocated 70% for training and 30% for testing. They evaluated the model using four metrics: accuracy, F1 score, sensitivity, and model-building time. For DoS and BotNet attacks, accuracy reached 99.9% and 99.94% respectively, with perfect f1 scores, sensitivity, and quick model-building times. While these results are promising, reducing the number of characteristics might risk excluding significant features.

Atheer et al. [22] conducted a study on NIDS, which incorporated the Mutual Information-Meerkat Clan Algorithm (MIMCA) from swarm intelligent algorithms for feature selection. The researchers employed four classification methods: Decision Tree (DT), Back-Propagation Neural Network (BP-NN), Naïve Bayes (NB), and the Apriori algorithm. The proposed algorithm is a wrapper feature selection technique that has demonstrated promising results in terms of accuracy while consuming minimal processing time. The evaluation was performed on two datasets, namely NSL-KDD and UNSW-NB15. However, the research centered on binary classification, yet the authors could have explored multiclass classification for a comprehensive assessment.

Ibrahim et al. [83] enhanced the Binary Manta-Ray Foraging (BMRF) Optimization Algorithm to build an intrusion detection system. They combined an adaptive S-shape function and the Random Forest (RF) classifier to identify crucial attributes and eliminate redundant elements from intrusion detection datasets. They compared their method to alternative techniques using well-known benchmark datasets: NSL-KDD and CIC-IDS2017. Results show the model's effectiveness. On the CIC-IDS2017 dataset, the model selected a set of 38 features, underwent training, and ultimately achieved an impressive precision of 99.6%, 94.3% recall, 96.9% F-measure, and 99.3% accuracy. Similarly, for the NSL-KDD dataset, the model identified 22 features and used them for training. The assessment results included a precision of 96.8%, recall of 96.2%, F-measure of 96.5%, and accuracy of 98.8%. However, the proposed method exhibited slower execution times compared to other methods.

Yakub et al. [52] focused on creating an efficient hybrid approach that combines K-Means and Genetic Algorithm (GA) with Support Vector Machine (SVM) to improve a Cyber Intrusion Detection System. Their research aimed to detect both known and unknown attacks using a combination of supervised and unsupervised learning techniques. The k-means clustering algorithm was employed, utilizing 1-of-k coding on normalized data to differentiate between benign and normal network instances. To handle unnecessary and redundant data within the dataset, the researchers applied a genetic algorithm (GA) as a wrapper feature selection method. This approach resulted in the identification of eighteen significant attributes. Finally, the

Table 6 Summary of models integrating Bio-Inspired techniques and Deep Learning algorithms

Ref.	Year	Models	Classification Type	Dataset	Metrics	Simulators/ Tools	Language	Advantages	Disadvantages
[68]	2019	FNN-LSO	Binary	UNSW-NB15 NSL-KDD	Accuracy Precision F-measure Recall FAR	Visual Basic 2010	N/A	(+)Acceptable level of attack detection	(-)Absence of Multi- Class Classification. (-)Lack of training and testing time discussion
[70]	2019	ImGWO-ImCNN	Multi-class	DARPA'98 KDD'99	Accuracy Detection rate FPR F1-score	MATLAB R2016a	N/A	(+)Reduced error rate. (+)Feature reduction capability	(-)Datasets are outdated, and the range and variety of attacks are limited
[59]	2020	MBC-BFO-ANN MBC-BFO-Re NN MBC-BFO-RNN	Binary	KDDCUP	Accuracy Precision F-measure Recall FPR	N/A	Python	(+)Low error rate. (+)Feature reduction capability	(-)Long execution time. (-)Single, outdated dataset with limited range of attacks. (-)Absence of Multi-Class Classification
[69]	2020	SMO-DNN	Binary	NSL-KDD KDD Cup 99	Accuracy Precision F-measure Recall FPR	N/A	N/A	(+)Feature reduction capability. (+)Less training time than others. (+)Acceptable level of attack detection	(-)Absence of Multi-Class Classification. (-)Datasets are outdated, and attacks are limited
[64]	2023	HHO-ANN	Binary	AWID	Accuracy Precision Recall FPR	Google Colab scikit-learn	Python	(+)High level accuracy. (+)Feature reduction capability	(-)Absence of Multi-Class Classification. (-)Absence of training and testing time discussion. (-)Single dataset evaluation
[65]	2022	CNN-LSTM-ChCSO	Binary	BoT-IoT NSL-KDD	Accuracy Sensitivity Specificity	N/A	N/A	(+)Enhanced detection performance. (+)Feature extraction capability	(-)Absence of Multi-Class Classification. (-)Lacks information about the tool and implementation language. (-)Absence of training and testing time discussion
[86]	2021	GMGWO-ECAE	Binary Multi-class	BoT-IoT NSL-KDD	Accuracy Precision Recall F1-score FAR	Matlab 2020a	N/A	(+)Feature reduction capability. (+)High level of attack detection. (+)Best training time compared other models	(-)Neglect of crucial testing time metric
[67]	2022	CNN-RSA	Binary Multi-class	KDDCup-99 NSL-KDD CICIDS2017 BoT-IoT	Accuracy Presicion Recall F1-score FAR	Pytorch	N/A	(+)Feature reduction capability. (+)High level of attack detection	(-)Learning model time consumption
[87]	2023	CNN-COA	Multi-class	NSL-KDD	Accuracy Precision Recall F1-score	Keras 2.2	N/A	(+)Best training time compared other models	(-)Single and outdated dataset
[63]	2023	RWO-CNN-Deep Maxout Network-EA	Binary	NSL-KDD CICIDS-2018 UNSW-NB15	Accuracy Precision Recall F1-score	Python	Python	(+)Enhanced Detection Performance	(-)Lack of training and testing time citation. (-)Absence of Multi-Class Classification

Table 6 (continued)

Ref.	Year	Models	Classification Type	Dataset	Metrics	Simulators/ Tools	Language	Advantages	Disadvantages
[66]	2023	GA-FR-CNN	Multi-class	UNSW-NB 15 BOT-IoT	Accuracy Precision Recall F1-score	MATLAB 2019b	N/A	(+)Enhanced accuracy. (+)Reduced processing time	(-)Unbalanced datasets distribution
[88]	2023	1D-CNN-GA-PSO	Binary	UNSW-NB 15 CIC-IDS2017 NSL-KDD	Accuracy Precision Recall F1-score Loss	TensorFlow Keras NumPy	Python	(+)High level of accuracy, precision and recall. (+)Optimized hyperparameters	(-)Unbalanced datasets distribution. (-)Computational complexity. (-)Absence of Multi-Class Classification

input data, pre-processed by the GA predictors, underwent classification using an SVM. The experimental results demonstrated a high accuracy rate of 99% and a detection rate of 98.49% with a low False Alarm Rate (FAR) of 0.4. The training phase was executed in 51.98 s. The NSL-KDD dataset was utilized, with 75% of the data allocated for training the SVM classifier and 25% for testing purposes. Nevertheless, assessing the study's performance solely on one dataset might not offer a comprehensive conclusion. Additionally, using dated datasets with limited attack instances might not accurately reflect real-world network scenarios.

Sumathi et al. [84] proposed a model for IDS in cloud computing. Their approach incorporates a 10-fold cross-validation feature selection methodology to effectively detect Distributed Denial of Service (DDoS) attacks. The model, named SVM-HHO-PSO, employs hybrid optimization algorithms, namely the Harmony Search Algorithm (HHO) and Particle Swarm Optimization (PSO), to fine-tune the parameters of Support Vector Machines (SVM). To evaluate their model, they used the NSL-KDD dataset. The dataset was partitioned into 10-fold groups using the K-fold cross-validation technique, enabling efficient feature selection. The performance of SVM-HHO-PSO was compared with other classical algorithms such as C4.5, KNN, SVM, and existing algorithms from the literature. The results showcased the model's effectiveness, with SVM-HHO-PSO achieving a 97.05% detection accuracy, 97.62% precision for correctly classified DDoS attacks, 97.52% sensitivity for identifying actual attacks, 96.73% specificity for accurately classifying non-attack instances, and a 97.67% F1 score demonstrating its robust performance. The research focused solely on DDOS Attacks; however, it could have encompassed various types of cyber attacks beyond DDoS. This broader approach could offer a more comprehensive evaluation of different attack types and their characteristics. It might involve considering other cyber threats alongside DDoS attacks.

Amir et al. [56] introduced an innovative method to optimize IoT malware detection. Their approach employs visual network traffic representations and a model named ACO-PSO-SVM. This model combines ant colony optimization (ACO) for feature selection and particle swarm optimization (PSO) to improve the support vector machines (SVMs) classifier's performance. The method includes pre-processing, feature extraction, selection, and classification. The dataset consists of 858 PNG format Binvis images. These encompass various malware types such as trojans, botnets, IoT-related attacks, and backdoors. After parameter tuning via PSO, a linear function exhibited the best results. The method achieved an accuracy of 95.56%, recall of 96.43%, precision of 94.12%, and F1 score of 95.26%. However, the experiments were confined to a

single dataset, restricting the general applicability of the method to various datasets. There was limited exploration of diverse image-based datasets and an absence of training and testing time discussion.

Mhamad et al. [57] designed an IDS for cloud settings, blending hybrid feature selection with a supervised machine learning classifier. Their approach included preprocessing, feature selection, dataset balancing, and a random forest classifier. Feature selection combined information gain (IG), chi-square (CS) as filter methods, and particle swarm optimization (PSO). Selected features fed into the random forest (RF) classifier, enabling multi-class attack detection and classification. Using UNSW-NB15 and Kyoto datasets, they derived 21 features from UNSW-NB15's 48 and 10 from Kyoto's 23. Evaluation considered accuracy, precision, FAR, F1 measure, and recall. Notably, they achieved 98% and 99% accuracy, respectively. While these results are promising, the authors acknowledged that the feature selection method could potentially lead to overfitting if not executed correctly. Moreover, there's a risk of overlooking important features, potentially resulting in underfitting.

Zinia et al. [85] used a combined approach of bio-inspired techniques and machine learning for attack identification using the CSE-CIC-IDS-2018 dataset. Their model consists of two layers. The first layer employed Random Forest Recursive Feature Elimination (RF-based RFE) to select effective features. The second layer further refined selection using Particle Swarm Optimization (PSO), Genetic Algorithm (GA), and Grey Wolf Optimization (GWO). After feature selection, the dataset was divided into 70% training and 30% testing sets. They assessed the mechanism using a Random Forest Classifier, with most class labels showing impressive performance. However, infiltration attacks were an exception, where metrics like Accuracy, Precision, Detection Rate, and F1-score did not perform as well. Despite achieving good results, the study didn't specify training times. Utilizing diverse algorithms might further increase the overall processing time.

Table 5 provides an extensive comparison of hybrid IDS utilizing ML and bio-inspired approaches for IoT security.

4.2 Hybrid IDs based on DL and bio-inspired approaches for IoT security

Benmessahel et al. [68] have devised a cutting-edge intrusion detection system that integrates two models: Locust Swarm Optimization (LSO), a meta-heuristic optimization algorithm, and the Feed-Forward Neural Network (FNN). The accuracy and effectiveness of the system were confirmed through the utilization of two swarm optimizer-based trainers, Particle Swarm Optimization (PSO), and Genetic Algorithm (GA). The IDS framework comprises three essential modules: the data input module, the FNN network module, and the LSO module. To evaluate the proposed model, benchmark datasets, namely NSL-KDD and UNSW-NB15, were used. The evaluation metrics employed were accuracy, recall, and FAR. The obtained results for UNSW-NB15 were 95.42% accuracy, 99.33% recall, and 9.40% FAR. For NSL-KDD, the metrics were 94.02% accuracy, 89.83% recall, and 2.21% FAR. However, the model lacks Multi-Class Classification evaluation, and importantly, it overlooks any discussion concerning training and testing durations.

Kalaivani et al. [59] developed an IDS using Meta-heuristic Swarm Intelligence (MSI) through the MBC-BFO feature selection approach. This was coupled with three classification techniques: ANN, ReNN, and RNN. In this method, Bacterial Foraging Optimization (BFO) swarm behavior was integrated into the Modified Bee Colony (MBC) algorithm for local research. The process involved dataset splitting for preprocessing, feature selection, and classification. To assess performance, they used different proportions (10% and 100%) of the KDDCUP'99 dataset. Results indicated that the hybrid approach (MBC-BFO) along with RNN achieved high accuracy, precision, recall, F-Measures, and low FPR compared to existing methods with a 10% learning dataset. The study primarily focused on binary classification, overlooking the opportunity to delve into multiclass classification for a more comprehensive analysis. Its evaluation relying solely on a single dataset may result in biased conclusions, as old datasets with limited attacks may not faithfully represent real-world network scenarios. Furthermore, the model's prolonged execution time poses an additional limitation to its efficiency.

Neelu et al. [69] proposed an IDS called SMO-DNN for detecting network traffic intrusions. This system combines Spider Monkey Optimization (SMO) for dimensionality reduction and DNN for binary classification. The model was tested on NSL-KDD and KDD Cup 99 datasets, split 70% for training and 30% for testing. Results demonstrated SMO-DNN outperforming other methods in accuracy, precision, recall, F1 score, sensitivity, and specificity for both datasets. Notably, it achieved these results with reduced training time complexity. Nevertheless, it is crucial to conduct a comprehensive performance analysis of the proposed method across various datasets and incorporate multi-class classification scenarios.

Sahil et al. [70] developed a hybrid model called

ImGWO-ImCNN for anomaly detection in cloud environments. The model combines Improved Grey Wolf Optimization (ImGWO) for feature selection and Improved Convolutional Neural Network (ImCNN) for network anomaly classification. To evaluate the performance of the ImGWO-ImCNN model, the researchers used two

benchmark datasets, namely DARPA'98 and KDD'99, along with a Synthetic dataset. The results demonstrated that the proposed model outperformed existing schemes in various evaluation metrics. Specifically, for the DARPA'98 dataset, the ImGWO-ImCNN model exhibited superior performance in terms of False Positive Rate (FPR), accuracy, and F-score. Additionally, for the KDD'99 dataset, the model demonstrated better performance in terms of Detection Rate (DR) and F-score compared to other existing schemes. However, limitations persist as the datasets utilized are outdated and lack diverse attack scenarios, failing to accurately simulate real-world network environments.

Nation et al. [64] explored a WiFi intrusion detection framework named N-HHO. This framework employed artificial neurons (ANN) trained with Harris Hawks optimization (HHO), utilizing a bio-inspired optimization algorithm instead of a gradient descent algorithm for binary classification. By employing HHO, the model aimed to address issues like delayed convergence and local minima entrapment associated with artificial neurons during attack classification and detection. The AWID dataset evaluation showcased exceptional results, with the model achieving remarkable accuracy (99.16%), high recall (99.49%), precision (97.42%), a Low False Positive rate (FPR) of 01.27%, and an impressive F1 score of 98.28%. However, the analysis of the proposed method's performance overlooked crucial aspects like training and, notably, testing time.

Deore et al. [65] conducted a highly effective network intrusion detection study using a bio-inspired model combined with a hybrid deep learning approach. The proposed model, known as ChCSO-driven Deep LSTM, integrates three components: CNN, Chimp Chicken Swarm Optimization (ChCSO), and Deep LSTM. The entire process consists of four steps: preprocessing, dimension transformation, feature extraction, and intrusion detection classification. In the preprocessing step, redundant data is removed, and normalization is applied to prepare the data for subsequent processing. The output of this step serves as the input for dimension transformation, which relies on mutual information. The transformed data is then fed into the CNN model to extract relevant features. Finally, the data is classified using the LSTM model, which is trained using ChCSO to enhance the detection performance. The experimental evaluation involved two datasets, namely NSL KDD and BOT IoT. The performance of the ChCSO-driven Deep LSTM was assessed using three metrics: accuracy, sensitivity, and specificity. A comparative analysis was performed by evaluating the model's performance with and without attacks, achieved by altering the training data. However, the study primarily focused on binary classification, missing the opportunity to explore multiclass classification. To enhance effectiveness and comprehensively assess the model, the evaluation could have included training and, notably, testing time.

An IDS named GMGWO-ECAE was developed by Moizuddin et al. [86], which was based on combining a Generalized Mean Grey Wolf Algorithm (GMGWO) with an ElasticNet Contractive Auto Encoder. The GMGWO meta-heuristic algorithm was employed to select optimal features, while the ECAE, along with a softmax classifier, handled the classification and detection of attacks. Notably, the network achieved impressive classification metrics, with a notable accuracy of 99.9%. This exceptional performance was observed in both binary and multi-class classifications, using the NSL-KDD and BOT IoT datasets. Despite achieving high performance, their focus remained solely on training time, overlooking the crucial evaluation aspect of testing time necessary for assessing the model comprehensively.

Gokula et al. [87] developed a Hierarchical Network Model (HNM) named CNN-COA for NIDS. Their approach involved employing deep learning techniques, specifically a one-dimensional convolutional neural network (1D-CNN), in combination with a bio-inspired model, the Chimp optimization algorithm (COA), for effective feature extraction. To enhance the quality of their dataset, the authors employed preprocessing techniques. They utilized the One-Sided Selection (OSS) method to remove noise samples from the dataset. Additionally, to address the class imbalance, they applied the SMOTE Technique to create a more balanced dataset. The experimental results display an acceptable level of performance while minimizing training time. However, relying on a single outdated dataset with limited attacks might not accurately reflect real-world network scenarios.

Subhash et al. [63] explored an investigation into a novel intrusion detection system known as the Remora Whale Optimization (RWO) based Hybrid deep model. Their study encompassed several essential steps, starting with Z-score normalization for preprocessing, followed by holo-entropy-based dimension transformation. Feature extraction was accomplished through the utilization of a CNN model, complemented by feature selection using the Random Vector (RV) coefficient. Classification tasks were handled by a hybrid deep learning approach, specifically integrating Deep Maxout Network and Deep Auto Encoder (EA) architectures. The training of the Hybrid deep model involved a unique optimization algorithm, the RWO algorithm, which ingeniously combined the Remora Optimization Algorithm (ROA) and WOA. In terms of evaluation metrics, the team employed accuracy, precision, recall, and F1-score. The assessments were conducted on three distinct datasets: NSL-KDD, CICIDS-2018, and UNSW-NB15. Notably, the UNSW-NB15 dataset

showcased particularly high values, including 93.8% for accuracy, 92% for precision, 93.2% for recall, and 92.6% for the F1-score. However, The research centered on binary classification, yet the authors could have explored multi-class classification for a comprehensive assessment. Additionally, while the authors aimed to minimize the total training time, they omitted citing the training and testing durations in their results.

Anushiya et al. [66] introduced an IDS employing a deep learning technique coupled with swarm intelligence, termed GA-FR-CNN (Genetic Algorithm and Faster Recurrent Convolutional Neural Network). They harnessed Assimilated Artificial Fish Swarm Optimization (AAFSO) to optimize feature selection, thereby curtailing memory and computational expenses. The selected reduced features were then fed into the GA-FR-CNN algorithm for further processing and classification. Through the fusion of GA-FR-CNN and AAFSO, their model attained an accuracy of 99.89% in multi-class classification when evaluated on the UNSW-NB 15 dataset. Nevertheless, it yielded a slightly lower accuracy of 93.7756% when tested with the BOT-IoT dataset. Nevertheless, the model doesn't employ balanced datasets to enhance its performance.

Abdelghani et al. [67] developed an innovative IDS tailored for the IoT and cloud environments. This novel approach combines deep learning and metaheuristic optimization techniques. Specifically, they employed a CNN as a foundational feature extractor. Complementing this, the Reptile Search Algorithm (RSA), inspired by crocodile hunting behaviors, was used to select optimum features from the extracted set. The system's effectiveness was evaluated across diverse datasets, including KDDCup-99, NSL-KDD, CICIDS2017, and BoT-IoT. In these evaluations, the model achieved high performance in both classifications. Yet, the method's development encounters constraints, notably, its time-consuming nature attributed to model learning.

Dusmurod et al. [88] explored an intrusion detection system leveraging one-dimensional convolutional neural networks (1D-CNNs). Their approach involved employing PSO and GA to optimize and fine-tune hyper-parameters in the 1D-CNN model. The evaluation was conducted across three datasets: UNSW-NB15, CIC-IDS2017, and NSL-KDD, using metrics like accuracy, loss, precision, recall, and F1-score. While demonstrating remarkable performance in binary classification, the study revealed potential limitations. The authors admitted to overlooking the problem of class imbalance and computational complexity resulting from incorporating GA or PSO.

4.3 Summary

Blending bio-inspired algorithms with Machine Learning and Deep Learning is promising for creating robust intrusion detection systems (IDSs). This fusion strategy has the potential to augment accuracy, robustness, and adaptability in the face of evolving threats. Nonetheless, it is essential to acknowledge and address the challenges while ensuring proper design and implementation to maximize the benefits of these approaches.

Table 6 provides an extensive comparison of hybrid IDS utilizing DL and bio-Inspired approaches for IoT security.

5 Results analysis and discussion

The subsequent section displays the outcomes obtained from the analysis of each study, centering around the research questions established earlier in Sect. 3.

RQ1: Why is the combination of bio-inspired and ML techniques employed for IoT-IDS?

Intrusion Detection Systems are tasked with processing substantial volumes of network data. Their function revolves around analyzing patterns within this data to identify any anomalous activities. However, the wealth of information present in traffic data encompasses numerous features that can impede the efficacy of IDS detection. Relying only on a single type of Machine Learning or Deep Learning model falls short of capturing all pertinent features. As a result, the incorporation of bio-Inspired methods, such as swarm intelligence algorithms and evolutionary algorithms [88], presents promising approaches for intrusion detection. From the articles we reviewed, it's clear that over the last three years, researchers have been concentrating on combining bio-inspired and ML techniques, including DL methods, to design efficient and robust IDS systems, as illustrated in Fig. 8.

RQ2: How can the integration of bio-inspired techniques with ML contribute to enhancing the security of IoT systems?

The interplay of bio-inspired and ML techniques leverages the advantages of each algorithm by creating a hybrid approach that maximizes the strengths and minimizes the weaknesses through a collaborative effect. Several comprehensive studies, such as [57, 83, 85], have highlighted the effectiveness of bio-inspired methods in mitigating unnecessary and redundant features. Additionally, [56, 84] have thoroughly explored the efficacy of these methods in fine-tuning classifier parameters, emphasizing the crucial part they play in enhancing the performance of Machine Learning models. Furthermore, [88] extensively discusses the integration of bio-inspired

techniques in enhancing classifiers, specifically addressing challenges associated with deep learning (DL) like managing weights and optimizing intricate parameters. Across the spectrum of reviewed literature [59, 66, 67, 69, 70], these bio-inspired methodologies consistently demonstrate their impact by facilitating feature reduction within datasets, thereby alleviating the computational burden [66, 81]. They also showcase significant improvements in the overall performance of IDS, while notably reducing processing time [22, 29, 35, 60, 86, 87].

RQ3: What are the most commonly used datasets and evaluation metrics for hybrid IoT-IDS assessment considering security parameters?

The security metrics employed by researchers to evaluate their methodologies are illustrated in Figs. 9 and 10. It is observed that Detection Accuracy and Recall (Detection Rate) stand out as the predominantly employed measures for assessing hybrid models that integrate both ML and bio-inspired techniques. Robust network security requires certainly high accuracy and detection rates by the IDS. Therefore, these two metrics are fundamental in evaluating the efficiency of the proposed systems. When considering an IDS developed using DL and bio-inspired techniques, it becomes imperative to incorporate Accuracy, Precision, Recall, and F1-score as essential metrics, among others.

Benchmark datasets hold a pivotal role in assessing the efficacy of a proposed IDS. The assessment of utilizing publicly available datasets is depicted in Fig. 11. The data reveals that NSL-KDD and KDD Cup'99 were employed for testing and validation in 45% of cases. Despite their occurrence, these datasets remain widely favored by researchers due to the extensive results available in existing literature. In the context of developing IDS, it's evident that testing with antiquated datasets may result in sub-optimal real-world performance. A model that is trained and validated using the latest datasets is inherently positioned to exhibit superior performance when deployed in practical environments. This underlines the significance of utilizing up-to-date datasets rather than outdated datasets to ensure the efficiency and robustness of intrusion detection models in real-world scenarios.

In addition to performance improvements achieved by the combination of bio-inspired and ML techniques, understanding the types of attacks within each dataset allows us to evaluate their effectiveness in safeguarding critical security parameters: confidentiality, integrity, and availability (CIA). Table 7 represents the impacts of prevalent attacks on CIA. Breaching confidentiality involves unauthorized access to computer systems or data storage, while integrity breaches entail unauthorized alterations to information or system states. Attacks that disrupt resources lead to availability violations.

Consequently, effective IDSs rely on two primary components: the best-developed models and appropriate datasets to enhance performance and ensure service availability. The diverse range of attacks present in previous datasets underscores the importance of protecting various security parameters.

RQ4: What are the strengths and weaknesses of blending ML and bio-inspired techniques for IoT security?

Bio-inspired techniques hold great promise for enhancing IDS based on ML or DL as shown in Fig. 12. It can be applied effectively in various IDS scenarios, offering the following benefits:

+ Enhanced performance: significantly improved metrics like accuracy, precision, recall, and F1 score which have been demonstrated in recent studies [63, 65, 66, 71, 83], reflecting an enhanced performance.
+ Feature selection: enabling the identification and retention of the most relevant and informative features while eliminating redundant or irrelevant ones [63, 66].
+ Feature extraction: in [65, 67], allowing for the automatic generation of relevant and informative features from complex data.
+ Parameter optimization: enhances algorithm performance through optimized parameter settings [88].
+ Reduced complexity: in studies [66, 81], solutions with lower complexity have been provided, leading to streamlined processes
+ Time efficiency: contributes to reduced processing time, enabling faster results [57, 60, 86, 87].
+ Attack detection: by employing IDSs such as [64, 68, 82, 88], the system can swiftly and accurately identify and respond to malicious activities, enhancing attack detection.
+ Attack classification: by enhancing the system's capability to identify and categorize complex patterns and threats effectively [57, 67, 85, 86].
+ Fine-tuning parameter: Fine-tuning involves adjusting the weights of certain or all layers in a pre-trained model to suit a new task or dataset. Generally, the entire pre-existing model is adapted to the specifics of the new data during this process [56, 84].

However, several weaknesses remain in these combinations, specifically:

– Limited generalization: the improved performance observed on certain datasets might not necessarily generalize to other datasets.

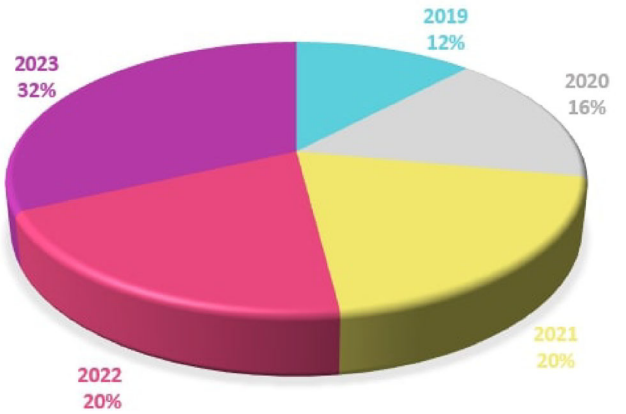

Fig. 8 Published articles based on bio-inspired and ML techniques for IoT-IDS per year

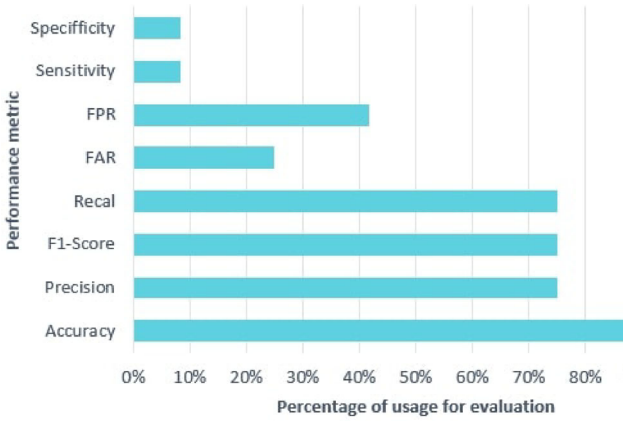

Fig. 10 Evaluation metrics used in hybrid IoT-IDS (DL and bio-inspired)

– Variable time reduction: not all combinations result in reduced processing time; some may even introduce additional computational overhead.
– Increased resource demand: combining more than two methods could necessitate greater computational resources, potentially resulting in escalated hardware and memory requirements.

RQ5: What is the impact of implementing the amalgamated approaches in real-world scenarios for IoT security?

The impact or significance of using the amalgamated approach becomes more apparent when we realize that there are no real-world examples or practical implementations discussed in the articles we reviewed. This absence highlights the challenge of translating theoretical discussions or concepts into actual applications in real-world settings. In real-world applications, the complexity and overlap of data pose significant challenges. When implementing an amalgamated approach for IoT security, particularly in the context of intrusion detection systems (IDS), the intricacies of real network scenarios must be taken into account. The data, encompassing both packet payload and packet header information, creates a dynamic environment where IDS models may exhibit varying performance levels. For instance, in the realm of"smart agriculture", implementing IDS solutions serves as a novel paradigm to mitigate agricultural production losses. IDS for Autonomous Agricultural Machinery or intelligent farms equipped with IDS play a pivotal role in ensuring the security of IoT systems by effectively mitigating potential attacks. This underscores the importance of amalgamating approaches to address the evolving challenges in IoT security effectively.

RQ6: What are open issues raised by the integration of bio-inspired techniques with ML?

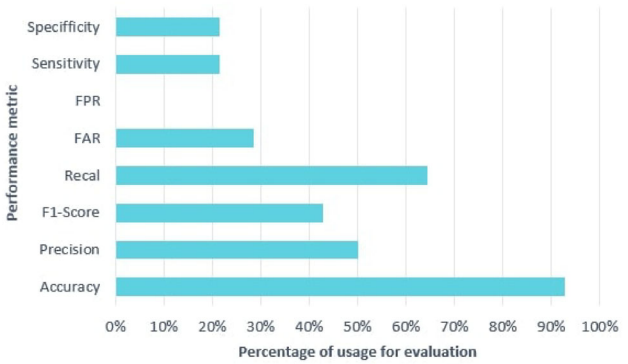

Fig. 9 Evaluation metrics used in hybrid IoT-IDS (ML and bio-inspired)

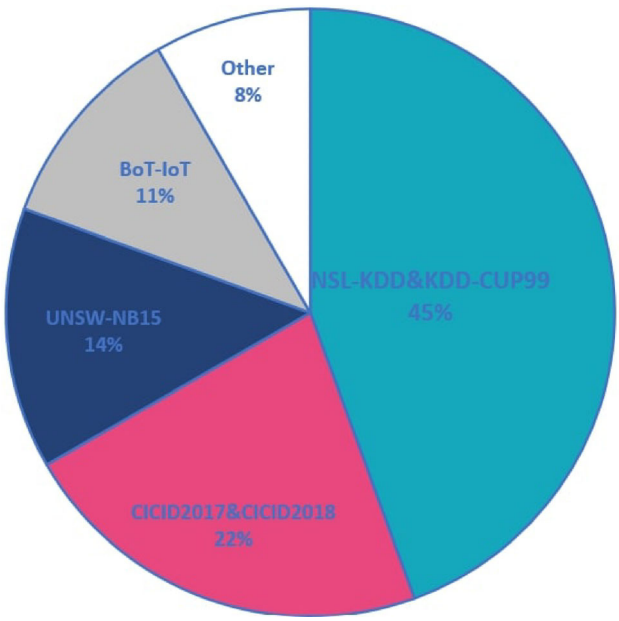

Fig. 11 Datasets distribution for IoT-IDS

The combination of bio-inspired techniques with ML or DL provides a range of issues and challenges, which can be outlined as follows:

- Dataset choice: To develop an effective IDS, the choice of intrusion detection dataset holds paramount importance. Updating these datasets is imperative to enhance the performance of IDS. Existing datasets like KDD CUP'99 and DARPA have limitations as they do not accurately represent real-world network situations. Utilizing such datasets to construct a hybrid IDS model might yield varying results in realistic network environments.
- Real-world performance evaluation: a significant IDS research challenge is assessing their effectiveness in actual environments. Most proposed methods are tested and validated using public datasets in controlled settings, not real-world scenarios. None have been tested in genuine contexts, leaving their practical performance uncertain. Many still use outdated datasets for testing. Thus, the main challenge is replicating laboratory efficiency. After laboratory validation, real-world testing is essential to confirm effectiveness in modern networks.
- Parameters choice: The fusion of bio-inspired techniques with ML and DL algorithms is extensively employed to enhance classifier performance. Nonetheless, the selection of suitable parameters presents a crucial challenge, whether for parameter optimization or feature selection.
- Quantity and quality of features: The efficiency of a classifier in detecting and classifying attacks is deeply tied to the quantity and quality of features used. However, establishing a clear relationship between

Table 7 Comparison of Attacks Across Datasets Based on Affected Security Parameters

Dataset	Year	Realistic traffic	Attack type	Affected Parameters		
				Confidentiality	Integrity	Availability
KDD Cup 1999	1999	✘	DOS	✘	✘	✔
			R2L	✔	✘	✘
NSL-KDD	2009	✘	U2R	✔	✘	✘
			probing	✔	✘	✘
UNSW-NB15	2015	✔	Fuzzers	✘	✔	✘
			Analysis	✘	✔	✘
			Backdoors	✔	✘	✘
			DoS	✘	✘	✔
			Exploits	✔	✔	✔
			Generic	✔	✔	✔
			Reconnaissance	✔	✘	✘
			Shellcode	✘	✔	✘
			Worms	✔	✘	✘
CICIDS 2017	2017	✔	Botnet	✘	✘	✔
			DoS	✘	✘	✔
			DDoS	✘	✘	✔
CSE-CIC-IDS2018	2018	✔	Brute Force	✔	✘	✘
			Infiltration	✔	✘	✘
			Web Attack	✔	✘	✘
BoT-IoT	2018	✔	Service scanning	✔	✘	✘
			OS Fingerprinting	✔	✘	✘
			DoS	✘	✘	✔
			DDoS	✘	✘	✔
			Information Thef	✔	✘	✘
			Data Theft	✔	✘	✘
			Keylogging	✔	✘	✘

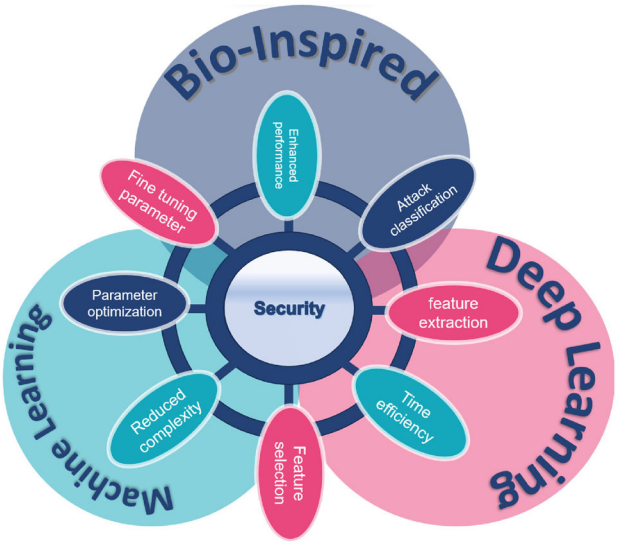

Fig. 12 Security enhancement with triad approaches for IoT systems

network flow features and attack categories poses a significant challenge. While reducing the number of characteristics might seem like a solution, it also introduces the risk of discarding crucial features that contribute to accurate detection and classification of attacks. Balancing the quantity and quality of features becomes pivotal for optimizing classifier performance in this context.

- Limited guidance on fusion methods: There is often a lack of clear guidelines on which bio-inspired algorithms work best with specific ML/DL methods for IDS applications. Selecting the right combination can be challenging.
- Limited resources of IoT devices: The limitations of IoT devices, including constrained computational power, memory, and energy resources, pose a significant challenge. These devices struggle to accommodate sophisticated models due to these constraints, making direct implementation impractical. Additionally, the energy demands of training and operating complex models may surpass IoT device capabilities, impacting their performance and lifespan.
- Adversarial machine learning (AML): is a technique utilized to create adversarial samples that involve deliberately crafted alterations in input, which can significantly impact the predictions and classifications of a model during both training and testing phases. AML presents significant cybersecurity threats across various sectors utilizing machine learning-based classification systems. This includes the potential of deceiving IDS to misclassify network packets.

6 Future directions

In the previous section, we explored the open issues stemming from integrating bio-inspired techniques with ML. In this section, we will delve into future directions and potential solutions aimed at overcoming these limitations:

- Advocate for the creation and utilization of datasets that accurately represent real-world IoT network situations.
- Establish collaborative partnerships with industry stakeholders to conduct real-world deployment trials of IDS solutions, ensuring practical validation in operational environments and gaining insights into performance, scalability, and usability in diverse network scenarios.
- Shift the research focus in IDS studies towards comprehensive evaluation, emphasizing metrics such as time complexity, energy consumption, and accuracy. This aims to guide the development of IDS solutions that are accurate and optimized for minimal time and energy impact in resource-constrained IoT environments.
- Investigate the hybridization of different bio-inspired algorithms to leverage their complementary strengths.
- Explore the practical efficacy of the latest bio-inspired techniques in feature selection for intrusion detection systems, particularly focusing on their adaptability and efficiency in IoT environments.
- Evaluate the potential of bio-inspired approaches in optimizing functions beyond traditional feature selection, such as hyperparameter tuning and model architecture selection, aiming to enhance the adaptability and performance of learning techniques in intrusion detection systems for IoT environments.
- Investigate transfer learning methods that can effectively adapt intrusion detection models to diverse IoT deployment scenarios with varying network characteristics and threat landscapes.
- Consider the adoption of transfer learning. By leveraging its ability to tap into pre-existing knowledge from related domains, transfer learning can greatly enhance the efficacy of intrusion detection systems in IoT environments, outperforming traditional machine learning and deep learning approaches.

7 Conclusion

This study conducted a systematic literature review focusing on intrusion detection within IoT environments, employing three distinct techniques: Machine Learning (ML), Deep Learning (DL), and bio-inspired methodologies. From an initial pool of articles, 25 research articles

were selected based on predefined inclusion and exclusion criteria. Furthermore, a comprehensive comparison was conducted, considering metrics, datasets, advantages, and limitations. Additionally, this study extensively addressed pertinent challenges and unresolved issues concerning the incorporation of bio-inspired methodologies alongside both ML and DL techniques for IoT networks. It also emphasized future directions aimed at enhancing IoT security.

As a result, this paper serves as a valuable resource for researchers seeking insights into the current state-of-the-art of security in IoT and offers a contemporary review of IDS applications using these three distinct approaches.

Author contributions CG, ZA, and YH organized the paper's structure, while AK created figures 4 and 5, and RS conducted the writing and the implementation. All authors contributed to reviewing the manuscript.

Funding No funding was received for this work.

Data availability No datasets were generated or analysed during the current study

Research data policy Data supporting the results and analysis of this study are available on request from the corresponding author.

Declarations

Conflict of interest None.

References

1. Ahmad, Z., Shahid Khan, A., Wai Shiang, C., Abdullah, J., Ahmad, F.: Network intrusion detection system: a systematic study of machine learning and deep learning approaches. Trans. Emerg. Telecommun. Technol. **32**(1), e4150 (2021)
2. Khan, I.A., Moustafa, N., Pi, D., Sallam, K.M., Zomaya, A.Y., Li, B.: A new explainable deep learning framework for cyber threat discovery in industrial iot networks. IEEE Internet Things J. **9**(13), 11604–11613 (2021)
3. Harbi, Y., Aliouat, Z., Refoufi, A., Harous, S.: Recent security trends in internet of things: a comprehensive survey. IEEE Access **9**, 113292–113314 (2021)
4. Gherbi, C., Senouci, O., Harbi, Y., Medani, K., Aliouat, Z.: A systematic literature review of machine learning applications in IoT. Int. J. Commun. Syst. **36**(11), e5500 (2023)
5. Ferrag, M.A., Maglaras, L., Moschoyiannis, S., Janicke, H.: Deep learning for cyber security intrusion detection: approaches, datasets, and comparative study. J. Inf. Secur. Appl. **50**, 102419 (2020)
6. Darwish, A.: Bio-inspired computing: algorithms review, deep analysis, and the scope of applications. Future Comput. Inform. J. **3**(2), 231–246 (2018)
7. Balasaraswathi, V.R., Sugumaran, M., Hamid, Y.: Feature selection techniques for intrusion detection using non-bio-inspired and bio-inspired optimization algorithms. J. Commun. Inf. Netw. **2**, 107–119 (2017)
8. Alamiedy, T.A., Anbar, M., Al-Ani, A.K., Al-Tamimi, B.N.,Faleh, N.: Review on feature selection algorithms for anomaly-based intrusion detection system. In Recent Trends in Data Science and Soft Computing: Proceedings of the 3rd International Conference of Reliable Information and Communication Technology (IRICT 2018), pages 605–619. Springer, 2019
9. Kumar, S., Gupta, S., Arora, S.: Research trends in network-based intrusion detection systems: A review. IEEE Access **9**, 157761–157779 (2021)
10. Di Mauro, M., Galatro, G., Fortino, G., Liotta, A.: Supervised feature selection techniques in network intrusion detection: a critical review. Eng. Appl. Artif. Intell. **101**, 104216 (2021)
11. Mahendran, A., et al.: Issues and solution techniques for iot security privacy-a survey. Int. J. Comput. Digital Syst. **12**(1), 909–928 (2022)
12. Al-Garadi, M.A., Mohamed, A., Al-Ali, A.K., Du, X., Ali, I., Guizani, M.: A survey of machine and deep learning methods for internet of things (iot) security. IEEE Commun. Surv. Tutor. **22**(3), 1646–1685 (2020)
13. Lansky, J., Ali, S., Mohammadi, M., Majeed, M.K., Karim, S.H., Rashidi, S., Hosseinzadeh, M., Rahmani, A.M.: Deep learning-based intrusion detection systems: a systematic review. IEEE Access **9**, 101574–101599 (2021)
14. RC, J.S., Parkavi,K: Investigations on bio-inspired algorithm for network intrusion detection–a review. Evol. Intell. 9 (2022)
15. Saranya, T., Sridevi, S., Deisy, C., Chung, T.D., Khan, M.A.: Performance analysis of machine learning algorithms in intrusion detection system: a review. Procedia Comput. Sci. **171**, 1251–1260 (2020)
16. Keele, S. et al.: Guidelines for performing systematic literature reviews in software engineering (2007)
17. Tong, S., Koller, D.: Support vector machine active learning with applications to text classification. J. Mach. Learn. Res. **2**, 45–66 (2001)
18. Li,Wenchao, Yi,Ping, Wu,Yue ,Pan,Li, Li,Jianhua. et al. A new intrusion detection system based on knn classification algorithm in wireless sensor network. Journal of Electrical and Computer Engineering, 2014, 2014
19. Breiman, L.: Random forests. Mach. Learn. **45**, 5–32 (2001)
20. Cutler, D.R., Edwards, T.C., Jr., Beard, K.H., Cutler, A., Hess, K.T., Gibson, J., Lawler, J.J.: Random forests for classification in ecology. Ecology **88**(11), 2783–2792 (2007)
21. D'Agostini, G.: A multidimensional unfolding method based on bayes' theorem. Nucl. Instrum. Methods Phys. Res. Sect. A **362**(2–3), 487–498 (1995)
22. Muhsen, A.R., Jumaa, G.G., Al Bakri, N.F., Sadiq, A.T.: Feature selection strategy for network intrusion detection system (nids) using meerkat clan algorithm. Int. J. Interact. Mob. Technol. (2021). https://doi.org/10.3991/ijim.v15i16.24173
23. Churcher, A., Ullah, R., Ahmad, J., Ur Rehman, S., Masood, F., Gogate, M., Alqahtani, F., Nour, B., Buchanan, W.J.: An experimental analysis of attack classification using machine learning in IoT networks. Sensors **21**(2), 446 (2021)
24. Saritas, M.M., Yasar, A.: Performance analysis of ANN and Naive Bayes classification algorithm for data classification. Int. J. Intell. Syst. Appl. Eng. **7**(2), 88–91 (2019)
25. Bangyal, W.H., Ahmad, J., Rauf, H.T., Shakir, R.: Evolving artificial neural networks using opposition based particle swarm optimization neural network for data classification. In 2018 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT), pages 1–6. IEEE, 2018
26. Abd Jalil, K., Kamarudin, M.H, Masrek, M.N.: Comparison of machine learning algorithms performance in detecting network intrusion. In 2010 international conference on networking and information technology, pages 221–226. IEEE, 2010

27. Kotsiantis, S.B.: Decision trees: a recent overview. Artif. Intell. Rev. **39**, 261–283 (2013)
28. Rai, K., Devi, M.S., Guleria, A.: Decision tree based algorithm for intrusion detection. Int. J. Adv. Netw. Appl. **7**(4), 2828 (2016)
29. Al Tawil, A., Sabri, K.E.: A feature selection algorithm for intrusion detection system based on moth flame optimization. In 2021 International Conference on Information Technology (ICIT), pages 377–381. IEEE, 2021
30. Woźniak, M., Grana, M., Corchado, E.: A survey of multiple classifier systems as hybrid systems. Inf. Fusion **16**, 3–17 (2014)
31. Jain, A.K.: Data clustering: 50 years beyond k-means. Pattern Recog. Lett. **31**(8), 651–666 (2010)
32. Hartigan, J.A., Wong, M.A.: Algorithm as 136: a k-means clustering algorithm. J. R. Stat. Soc. Ser. C **28**(1), 100–108 (1979)
33. Kumari, R., Singh, M.K., Jha, R., Singh, N.K., et al.: Anomaly detection in network traffic using k-mean clustering. In: 2016 3rd international conference on recent advances in information technology (RAIT), pages 387–393. IEEE, 2016
34. Li, Z., Li, Y., Xu, L.: Anomaly intrusion detection method based on k-means clustering algorithm with particle swarm optimization. In: 2011 international conference of information technology, computer engineering and management sciences, volume 2, pages 157–161. IEEE, 2011
35. Bhattacharya, S., S, S.R., Maddikunta, P.K., Kaluri, R., Singh, S., Gadekallu, T.R., Alazab, M.: Tariq UA novel pca-firefly based xgboost classification model for intrusion detection in networks using gpu. Electronics **9**(2), 219 (2020)
36. Agrawal, R., Srikant, R., et al.: Fast algorithms for mining association rules. In: Proc. 20th int. conf. very large data bases, VLDB, volume 1215, pages 487–499. Santiago, Chile (1994)
37. Mnih, V., Kavukcuoglu, K., Silver, D., Rusu, A.A., Veness, J., Bellemare, M.G., Graves, A., Riedmiller, M., Fidjeland, A.K., Ostrovski, G., et al.: Human-level control through deep reinforcement learning. Nature **518**(7540), 529–533 (2015)
38. Hochreiter, S., Schmidhuber, J.: Long short-term memory. Neural Comput. **9**(8), 1735–1780 (1997)
39. Chung, J., Gulcehre, C., Cho, K.H., Bengio, Y.: Empirical evaluation of gated recurrent neural networks on sequence modeling. arXiv preprint arXiv:1412.3555, 2014
40. Deng, L.: A tutorial survey of architectures, algorithms, and applications for deep learning. APSIPA Trans. Signal Inf. Process. **3**, e2 (2014)
41. Hinton, G.E.: A practical guide to training restricted Boltzmann machines. In: Neural Networks: Tricks of the Trade: Second Edition, pp. 599–619. Springer (2012)
42. Binitha, S., Siva Sathya, S., et al.: A survey of bio inspired optimization algorithms. Int. J. Soft Comput. Eng. **2**(2), 137–151 (2012)
43. Goodfellow, I., Bengio, Y., Courville, A.: Deep Learning. MIT Press, Cambridge (2016)
44. Goodfellow, I., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., Courville, A., Bengio, Y.: Generative adversarial nets. Adv. Neural Inf. Process. Syst. **27** (2014)
45. Ganaie, M.A., Hu, M., Malik, A.K., Tanveer, M., Suganthan, P.N.: Ensemble deep learning: a review. Eng. Appl. Artif. Intell. **1**(115), 105151 (2022)
46. Husain, M.S.: Nature inspired approach for intrusion detection systems. Design and analysis of security protocol for communication, pp. 171–182 (2020)
47. Atashpaz-Gargari, E., Lucas, C.: Imperialist competitive algorithm: an algorithm for optimization inspired by imperialistic competition. In: 2007 IEEE Congress on Evolutionary Computation, pp. 4661–4667. IEEE (2007)
48. Krishnanand, K.R., Nayak, S.K., Panigrahi, B.K., Rout, P.K.: Comparative study of five bio-inspired evolutionary optimization techniques. In: 2009 World Congress on Nature & Biologically Inspired Computing (NaBIC), pages 1231–1236. IEEE (2009)
49. Elsayed, S., Sarker, R., Essam, D.: Survey of uses of evolutionary computation algorithms and swarm intelligence for network intrusion detection. Int. J. Comput. Intell. Appl. **14**(04), 1550025 (2015)
50. Roy, S., Biswas, S., Chaudhuri, S.S.: Nature-inspired swarm intelligence and its applications. Int. J. Mod. Educ. Comput. Sci. **6**(12), 55 (2014)
51. Raj, M.G., Pani, S.K.: A meta-analytic review of intelligent intrusion detection techniques in cloud computing environment. Int. J. Adv. Comput. Sci. Appl. (2021). https://doi.org/10.14569/ijacsa.2021.0121023
52. Saheed, Y.K., Arowolo, M.O., Tosho, A.U.: An efficient hybridization of k-means and genetic algorithm based on support vector machine for cyber intrusion detection system. Int. J. Electr. Eng. Inform. **14**(2), 426–442 (2022)
53. Crosbie, M., Spafford, G., et al.: Applying genetic programming to intrusion detection. In: Working Notes for the AAAI Symposium on Genetic Programming, pages 1–8. Cambridge, MA: MIT Press (1995)
54. Back, T.: Evolutionary Algorithms in Theory and Practice: Evolution Strategies, Evolutionary Programming, Genetic Algorithms. Oxford University Press, Oxford (1996)
55. Popoola, E., Adewumi, A.O.: Efficient feature selection technique for network intrusion detection system using discrete differential evolution and decision. Int. J. Netw. Secur. **19**(5), 660–669 (2017)
56. El-Ghamry, A., Gaber, T., Mohammed, K.K., Hassanien, A.E.: Optimized and efficient image-based iot malware detection method. Electronics **12**(3), 708 (2023)
57. Bakro, M., Kumar, R.R., Alabrah, A., Ashraf, Z., Ahmed, M.N., Shameem, M., Abdelsalam, A.: An improved design for a cloud intrusion detection system using hybrid features selection approach with ML classifier. IEEE Access **11**, 64228–64247 (2023)
58. Almomani, O.: A hybrid model using bio-inspired metaheuristic algorithms for network intrusion detection system. Comput. Mater. Contin. (2021). https://doi.org/10.32604/cmc.2021.016113
59. Kalaivani, S., Gopinath, G.: Modified bee colony with bacterial foraging optimization based hybrid feature selection technique for intrusion detection system classifier model. ICTACT J Soft Comput. (2020)
60. Al-Yaseen, W.L.: Improving intrusion detection system by developing feature selection model based on firefly algorithm and support vector machine. IAENG Int. J. Comput. Sci. **46**(4), 534–540 (2019)
61. Mazini, M., Shirazi, B., Mahdavi, I.: Anomaly network-based intrusion detection system using a reliable hybrid artificial bee colony and adaboost algorithms. J. King Saud Univ. **31**(4), 541–553 (2019)
62. Xu, H., Cao, Q., Fu, H., Fu, C., Chen, H., Su, J.,: Application of support vector machine model based on an improved elephant herding optimization algorithm in network intrusion detection. In Artificial Intelligence: Second CCF International Conference, ICAI 2019, Xuzhou, China, August 22-23, 2019, Proceedings 2, pages 283–295. Springer, 2019
63. Pingale, S.V., Sutar, S.R.: Remora based deep maxout network model for network intrusion detection using convolutional neural network features. Comput. Electr. Eng. **110**, 108831 (2023)
64. Narengbam, L., Dey, S.: Wifi intrusion detection using artificial neurons with bio-inspired optimization algorithm. Procedia Comput. Sci. **218**, 1238–1246 (2023)
65. Deore, B., Bhosale, S.: Hybrid optimization enabled robust cnn-lstm technique for network intrusion detection. IEEE Access **10**, 65611–65622 (2022)

66. Anushiya, R., Lavanya, V.S.: A new deep-learning with swarm based feature selection for intelligent intrusion detection for the internet of things. Meas. Sens. **26**, 100700 (2023)
67. Dahou, A., Abd Elaziz, M., Chelloug, S.A., Awadallah, M.A., Al-Betar, M.A., Al-Qaness, M.A., Forestiero, A.: Intrusion detection system for iot based on deep learning and modified reptile search algorithm. Comput. Intell. Neurosci (2022). https://doi.org/10.1155/2022/6473507
68. Benmessahel, I., Xie, K., Chellal, M., Semong, T.: A new evolutionary neural networks based on intrusion detection systems using locust swarm optimization. Evol. Intell. **12**, 131–146 (2019)
69. Khare, N., Devan, P., Chowdhary, C.L., Bhattacharya, S., Singh, G., Singh, S., Yoon, B.: Smo-dnn: Spider monkey optimization and deep neural network hybrid classifier model for intrusion detection. Electronics **9**(4), 692 (2020)
70. Garg, S., Kaur, K., Kumar, N., Kaddoum, G., Zomaya, A.Y., Ranjan, R.: A hybrid deep learning-based model for anomaly detection in cloud datacenter networks. IEEE Trans. Netw. Serv. Manag. **16**(3), 924–35 (2019)
71. Dwivedi, S., Vardhan, M., Tripathi, S.: Building an efficient intrusion detection system using grasshopper optimization algorithm for anomaly detection. Clust. Comput., pp.1-20 (2021)
72. Ghanem, W.A., Ghaleb, S.A., Jantan, A., Nasser, A.B., Saleh, S.A., Ngah, A., Alhadi, A.C., Arshad, H., Saad, A.M., Omolara, A.E., El-Ebiary, Y.A., et al.: Cyber intrusion detection system based on a multiobjective binary bat algorithm for feature selection and enhanced bat algorithm for parameter optimization in neural networks. IEEE Access **10**, 76318–76339 (2022)
73. Simon, D.: Biogeography-based optimization. IEEE Trans. Evol. Comput. **12**(6), 702–713 (2008)
74. Chen, H., Zhu, Y.: Optimization based on symbiotic multi-species coevolution. Appl. Math. Comput. **205**(1), 47–60 (2008)
75. Liu, C., Yang, J., Chen, R., Zhang, Y., Zeng, J.: Research on immunity-based intrusion detection technology for the internet of things. In: 2011 Seventh International conference on natural computation, volume 1, pages 212–216. IEEE (2011)
76. Garcia-Teodoro, P., Diaz-Verdejo, J., Maciá-Fernández, G., Vázquez, E.: Anomaly-based network intrusion detection: techniques, systems and challenges. Comput. Secur. **28**(1–2), 18–28 (2009)
77. Zarpelão, B.B., Miani, R.S., Kawakani, C.T., de Alvarenga, S.C.: A survey of intrusion detection in internet of things. J. Netw. Comput. Appl. **84**, 25–37 (2017)
78. Bostani, H., Sheikhan, M.: Hybrid of anomaly-based and specification-based ids for internet of things using unsupervised opf based on mapreduce approach. Comput. Commun. **98**, 52–71 (2017)
79. Mukkamala, S., Janoski, G., Sung, A.: Intrusion detection using neural networks and support vector machines. In: Proceedings of the 2002 International Joint Conference on Neural Networks. IJCNN'02 (Cat. No. 02CH37290), volume 2, pp.1702–1707. IEEE (2002)
80. Milenkoski, A., Vieira, M., Kounev, S., Avritzer, A., Payne, B.D.: Evaluating computer intrusion detection systems: a survey of common practices. ACM Comput. Surv. **48**(1), 1–41 (2015)
81. Vijayanand, R., Devaraj, D.: A novel feature selection method using whale optimization algorithm and genetic operators for intrusion detection system in wireless mesh network. IEEE Access **8**, 56847–56854 (2020)
82. Sydney, M.K.: An advanced intrusion detection system for iiot based on ga and tree based algorithms. IEEE Access **9**, 113199–113212 (2021)
83. Hassan, I.H., Abdullahi, M., Aliyu, M.M., Yusuf, S.A., Abdulrahim, A.: An improved binary manta ray foraging optimization algorithm based feature selection and random forest classifier for network intrusion detection. Intell. Syst. Appl. **16**, 200114 (2022)
84. Sokkalingam, S., Ramakrishnan, R.: An intelligent intrusion detection system for distributed denial of service attacks: a support vector machine with hybrid optimization algorithm based approach. Concurr. Comput. Pract. Exp. **34**(27), e7334 (2022)
85. Anzum Tonni, Z., Mazumder, R.: A novel feature selection technique for intrusion detection system using rf-rfe and bio-inspired optimization. In: 2023 57th Annual Conference on Information Sciences and Systems (CISS), pages 1–6. IEEE (2023)
86. Moizuddin, M.D., Victor Jose, M.: A bio-inspired hybrid deep learning model for network intrusion detection. Knowl. Based Syst. **238**, 107894 (2022)
87. Kaviarasan, S., Geetha, A.: Network intrusion detection based on one-dimensional cnn with chimp optimization algorithm. J. Theor. Appl. Inf. Technol. 101(10) (2023)
88. Kilichev, D., Kim, W.: Hyperparameter optimization for 1d-cnn-based network intrusion detection using ga and pso. Mathematics **11**(17), 3724 (2023)

Rafika Saadouni achieved her Master's degree in Network and Distributed Systems from the University of Ferhat Abbas Setif-1, Algeria, in 2022. Currently, she is pursuing her Ph.D. in Computer Science at the same university, with research interests primarily centered around Cybersecurity, Machine Learning, Deep Learning, and IoT systems.

Chirihane Gherbi obtained her PhD in Computer Science from Larbi Ben Mhidi University, OEB, Algeria, in 2017. She is currently an associate professor at the College of Science, Computer Science Department, Ferhat Abbas University, and a member of the Network and Distributed Systems Laboratory (LRSD). Her principal areas of interest in research are wireless sensor networks (WSN), routing protocols in wireless communication, fault tolerance, security in the Internet of Things (IoT), and machine learning.

Zibouda Aliouat obtained her engineer diploma in 1984 and MSc in 1993 from Constantine University. She received her PhD from Setif 1 University of Algeria. She was an assistant professor at Constantine University from 1985 to 1994. Currently, she is a professor in Computer Engineering Department at Setif 1 University of Algeria. Her research interests are in the areas of computer networks and communication modeling and simulation, wireless sensor networks (WSN), fault tolerance of embedded systems and security and privacy in the Internet of Things (IoT), Internet of vehicles (IoV), and Nanonetworks communication. Specifically, it focused on clustering routing protocols in wireless communication and MAC layer.

Yasmine Harbi received the Ph.D. degree in Computer Science from Ferhat Abbas University Setif 1, Algeria. She is an associate professor at Computer Science Department, Ferhat Abbas University Setif 1, Algeria. Her main research interests include security and privacy in Internet of Things, blockchain, machine learning, and applied cryptography.

Amina Khacha completed her Bachelor's degree in 2020 and her Master's degree in 2022, demonstrating a profound comprehension of computer science principles and emerging trends. Currently, she is pursuing her Ph.D. in Computer Science at the University of Ferhat Abbas Setif-1, Algeria, specializing in security within the Internet of Things (IoT) and the utilization of Artificial Intelligence techniques for enhancing security measures.