IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 26 June 2022, accepted 9 July 2022, date of publication 19 July 2022, date of current version 26 July 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3192472

RESEARCH ARTICLE

Cyber Intrusion Detection System Based on a Multiobjective Binary Bat Algorithm for Feature Selection and Enhanced Bat Algorithm for Parameter Optimization in Neural Networks

WAHEED ALI H. M. GHANEM[1,2,3], SANAA ABDULJABBAR AHMED GHALEB[1,2,5], AMAN JANTAN[4], ABDULLAH B. NASSER[6], (Member, IEEE), SAMI ABDULLA MOHSEN SALEH[7], AMIR NGAH[3], ARIFAH CHE ALHADI[3], HUMAIRA ARSHAD[8], ABDUL-MALIK H. Y. SAAD[9], (Senior Member, IEEE), ABIODUN ESTHER OMOLARA[10], YOUSEF A. BAKER EL-EBIARY[5], (Member, IEEE), AND OLUDARE ISAAC ABIODUN[11]

[1]Faculty of Engineering, University of Aden, Aden, Yemen
[2]Faculty of Education-Aden and Saber, Aden University and Lahej University, Aden, Yemen
[3]Faculty of Ocean Engineering Technology and Informatics, Universiti Malaysia Terengganu, Terengganu 32030, Malaysia
[4]School of Computer Science, Universiti Sains Malaysia, Pinang 11800, Malaysia
[5]Faculty of Informatics and Computing, Universiti Sultan Zainal Abidin, Terengganu 21300, Malaysia
[6]School of Technology and Innovation, University of Vaasa, Vaasa 65200, Finland
[7]School of Electrical and Electronic Engineering, Universiti Sains Malaysia, Nibong Tebal, Pulau Pinang 14300, Malaysia
[8]Department of Computer Science, Islamia University of Bahawalpur, Bahawalpur 63100, Pakistan
[9]Division of Electronic and Computer Engineering, School of Electrical Engineering, Faculty of Engineering, Universiti Teknologi Malaysia, Johor 81310, Malaysia
[10]Department of Computer Science, University of Abuja, Gwagwalada 900110, Nigeria
[11]Department of Computer Science, Bingham University, Karu 961105, Nigeria

Corresponding authors: Waheed Ali H. M. Ghanem (waheed.ghanem@gmail.com) and Sanaa Abduljabbar Ahmed Ghaleb (sanaaghaleb.sg@gmail.com)

ABSTRACT The staggering development of cyber threats has propelled experts, professionals and specialists in the field of security into the development of more dependable protection systems, including effective intrusion detection system (IDS) mechanisms which are equipped for boosting accurately detected threats and limiting erroneously detected threats simultaneously. Nonetheless, the proficiency of the IDS framework depends essentially on extracted features from network traffic and an effective classifier of the traffic into abnormal or normal traffic. The prime impetus of this study is to increase the performance of the IDS on networks by building a two-phase framework to reinforce and subsequently enhance detection rate and diminish the rate of false alarm. The initial stage utilizes the developed algorithm of a proficient wrapper-approach-based feature selection which is created on a multi-objective BAT algorithm (MOBBAT). The subsequent stage utilizes the features obtained from the initial stage to categorize the traffic based on the newly upgraded BAT algorithm (EBAT) for training multilayer perceptron (EBATMLP), to improve the IDS performance. The resulting methodology is known as the (MOB-EBATMLP). The efficiency of our proposition has been assessed by utilizing the mainstream benchmarked datasets: NLS-KDD, ISCX2012, UNSW-NB15, KDD CUP 1999, and CICIDS2017 which are established as standard datasets for evaluating IDS. The outcome of our experimental analysis demonstrates a noteworthy advancement in network IDS above other techniques.

INDEX TERMS Intrusion detection system (IDS), bat algorithm (BAT), metaheuristic algorithm (MA), feature selection (FS), multi-objective optimization (MOO), multilayer perceptron (MLP).

The associate editor coordinating the review of this manuscript and approving it for publication was Bilal Alatas.

I. INTRODUCTION

There is a long list of network security techniques designed to protect computer networks. Confidentiality, integrity or

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

availability of network resources are what the protection involves so as to build defense against intrusions or compromise [1], [2]. Regardless of the proliferation of data compromise, individual technologies are yet in want of full protection against network infringement. Various technologies are engaged in a defense in-depth setting.

Intrusion Detection Systems (IDSs), firewalls, and Intrusion Prevention Systems (IPSs) are among the most popular network security technologies.

System administrators provided early warnings by IDS which furnishes the network with a degree of protection from any dubious action. The reason is because intrusion detection systems have the ability to detect different kinds of malicious actions. A second layer of protection is attractively formed in traditional firewalls which covers limitations of security policies [3]–[5].

In summary IDSs operations are as follows: monitor, analyse, detect, and stir alarms. The two classifications are: network-based IDS (NIDS), this discern computer threats at the layer of the network by assessing the traffic of the network and the other is the HIDS which refers to host-based IDS and detects traffic on the network host or computers. The two detection techniques used by IDS include: (1) Misuse detection, where attacks use signature databases containing designations of a known attack. (2) anomaly detection; assumes that the adversary's behaviour differs from that of the main user [6], [7].

IDS still suffer from performance problem even though they are mature technology. Performance in this context looks at the detection rate of actual treats while preventing errors in reporting potential ones. False positives infer the network incorrectly reports an attack [8], [9].

An IDS must embrace an anomaly-detection approach to curtail novel attacks. The approach is based on the argument that malicious behaviour is not the same as would be expected from normal user behaviour. Thus, by identifying activities that are anomalous, new threats can then be detected. This undertaking inherently points to a classification problem; which implies training the classifier model using a number of features to segregate at least two classes in a given set of observations. Among the successful classifiers, artificial neural networks (ANNs) turned out to be the most extensively utilized system for intrusion detection [10], [11].

Traditional ANN-based IDSs has twofold problem. One is the classifier's performance which relies on a set of parameters. Before an optimal set of values is settled, the parameters need to be learned. Regarding ANNs, these parameters are a set of weights and biases that label network edges feeding into the nodes [12]–[14].

The determination of these weights is achieved through a training process which in essence is an optimization problem in which the space of all possible weights is searched for the ideal combinations of values that will result in a classification of the best network packets. Regrettably, the search space for all weights is so large that classical learning algorithms, such as backpropagation, could only produce suboptimal values within certain time and computational resources. Conversely, an IDS manages enormous amounts of information containing unimportant and redundant features, which invariably makes the processes of training and testing slow, alongside utilization of high resource, and poor rate of detection [15]. Therefore, a rudimentary step in the construction of an IDS is feature selection (FS). A decline in the false alarm rate, an improved classification accuracy, alongside lesser time and computational costs are achieved when feature sets are optimized [16]–[18].

Since training classifiers on an optimal set of parameters and with a certain selection of features is essentially an optimization problem, the metaheuristic turns out to be a natural candidate for a solution. That's particularly true because traditional training algorithms are based on a gradient descent algorithm, which is quite limited in comparison to the methods available in artificial neural networks. There is a lot of research out there using metaheuristic algorithms (MA) in order to train neural networks (NNs) and address the feature selection problem for intrusion detection among many other applications [19]–[21].

The metaheuristic algorithms span evolutionary computations (EC) like the genetic algorithm (GA) and swarm intelligence (SI) for instance, particle swarm optimization (PSO). However, the nature of these algorithms leaves the room for much improvement since the most important challenge at the heart of any met heuristic optimization algorithm is the capability of balancing the exploitation and exploration activities in the search space to identify a global optimum solution [22], [23]. Nevertheless, the search for a proper exploration and exploitation trade-off remains a challenging task in any algorithm and can always be improved for a new application such as intrusion detection [24], [25]. This opportunity to used better metaheuristics to optimize IDS classifiers is the main driver of the research in this research.

This work expands on the basis that the impediments of existing FS and characterization techniques can be reduced, and their performance improved, by leveraging optimization systems that are metaheuristic-based. This optimization type has proven to be very effective in tackling complex issues that include multitude and evolving factors. The techniques encompass the task of the classifier's training in addition to selecting the ideal set of features which will perform the classification. Besides, feature selection is a multi-objective problem that involves several objectives [26], [27], leading to the need for multi-objective optimization (MOO), which is a serious challenge to be surmounted in this research as well.

A. GOALS

The major objective of this study is to enhance the performance of IDS on computer networks. A detection system that handles the shortfall of IDS is put forward. Features that are significant in the network packets are extracted leveraging a MOO technique as the initial step. A machine learning (ML) model is trained utilizing the

enhanced metaheuristic algorithm (MA) in the subsequent step. The ML model can detect known and unknown attacks based on the features acquired from the initial stage.

The general goal can be split into the accompanying list of comprehensive objectives:

1. The development of a metaheuristic system that can be utilized to reinforce the performance of trained NN for the detection of malicious traffic in IDS. The explored approach shows better convergence and precision for resolving optimization issues that are single and constrained.

2. The adaptation of the developed system for training of Multi-Layer Perceptrons (MLPs). A fusion appropriate for data representation and ideal for fitness measure for classification tasks will be presented.

3. Design and implement a novel IDS which uses the potentialities of the proposed multi-objective binary bat algorithm (MOBBAT) for wrapper-based FS for selecting ideal features from the packets at the foremost phase. The subsequent phase passes these features into the MLP model from objective two for the detect network intrusions.

The enhanced Bat algorithm's remodeling for training the NN with the end goal of detecting intrusion precipitated into the corresponding training algorithm, EBATMPL. This covers the first two objectives. A multi-objective BAT algorithm for FS (MOBBAT) is provided as parts of the third aim. In conclusion, the objective incorporates the EBATMLP along with the optimal features identified by the MOBBAT to yield a novel IDS called MOB-EBATMLP.

B. ORGANISATION

This study's overview is given in Section II. Section III presents related research. Section IV discusses the methodology. The assessment of MOB-EBATMLP is depicted in Section V, alongside results and discussions. The conclusion is covered in Section VI.

II. BACKGROUND

A. BAT ALGORITHM (BAT)

BAT is motivated by swarms of bats utilizing echolocation to detect preys. The formulation of the steps and the attributes of bat echolocation is simplified as [28]:

- Echolocation is utilized by bats to detect distance, and likewise 'recognize' the contrast amongst obstacles and prey;
- To find a prey, bats fly at random using a velocity v_i with a frequency f_{min} alongside position x_i with varying wavelength λ and loudness A_0. Based on the closeness of their potential obstacle, they can spontaneously fine-tune the frequency of their discharged pulses and the pulse emission rate $r \in [0, 1]$;
- The assumption is based on the premise that loudness varies from a positive high A_0 to a minimal constant value A_{min}.

The first phase is the initialization of all the variables, as each bat is defined by a position $\boldsymbol{x}_i^t$, emission pulse rate $\boldsymbol{r}_i^t$, velocity $\boldsymbol{v}_i^t$, loudness $\boldsymbol{A}_i^t$ and frequency $\boldsymbol{f}_i^t$. In the search space at time t. The populace of bats is characterized arbitrarily as each bat constitutes a viable solution for the optimization problem. The second phase includes generating a new populace by the application of the alterations portrayed in the equations:

$$f_i = f_{min} + (f_{max} - f_{min})\,\beta, \tag{1}$$

where, $\beta \in [0, 1]$.

$$v_i^t = v_i^{t-1} + \left(x_i^t - x_*\right) f_i, \tag{2}$$

x_* Represents the current universal best location after contrasting all the solutions amongst the defined bats.

$$x_i^t = x_i^{t-1} + x_i^t, \tag{3}$$

Summarily, based on the problem in view, the frequency f is assigned to $f_{\min} = 0$ and $f_{\max} = 100$ in real-world use-cases. At first, an individual bat is arbitrarily specified with a frequency drawn at uniform $[f_{\min}, f_{\max}]$. As for the part of the local search, once a solution is chosen amongst the current best solutions, a new solution for individual bat is produced locally using random walk where $\varepsilon \in [-1, 1]$ is a scaling factor identified as a random number, while $A^t =< A_i^t >$ represents the average loudness of all bats at time t.

$$x_{new} = x_{old} + \varepsilon A^t \tag{4}$$

Additionally, updates of the loudness A_{i}, the rate r_{i} of pulse emission are performed as:

$$A_i^{t+1} = \alpha A_i^t,\ r_i^{t+1} = r_i^0\left[1 - exp\left(-\gamma t\right)\right], \tag{5}$$

α and γ are constants.

1) JUSTIFY THE CHOICE OF THE BAT ALGORITHM

The intrinsic advantage of BAT is that it has the benefits of combining single-based and population-based algorithms to improve convergence quality. The other benefits of the BAT that motivation researchers to adopt it to solve classification and time series prediction problems are as follows [20]:

- Frequency tuning: The BAT employs echolocation and frequency tuning during the process of problem solving. Although echolocation is not directly used to imitate the right function in the real world, frequency alterations are used.
- Automatic zooming: The BAT has the ability to automatically zoom into an area where potentially better solutions have found. This zooming is performed by the automatic shifting from explorative movement to local intensive exploitation. Therefore, the BAT has a fast convergence rate in the early stages of the iteration process.
- Parameter control: Most metaheuristic algorithms employ fixed Parameters which need to be tuned in advance. In contrast, the BAT used Parameter control, whereby the values of the Parameters (A and r) are differed as the iteration process. This helps to automatically direct the BAT to move from exploration to exploitation when the best solution is searching.

B. MULTI-OBJECTIVE OPTIMIZATION (MOO)

The need to make an ideal choice, particularly on account of the existence of tradeoffs between at least two varying objective functions makes the MOO very valuable. It can include boosting or limiting different varying objective functions [29]. The equation of an n-objective minimization challenge is derived as:

$$minimiseF\ (x) = [f1\ (x)\ ,f2\ (x)\ ,f3\ (x)\ ,\ldots\ ,fn\ (x)] \quad (6)$$

$$\text{Subject to}: \ g_i\ (x) \leq 0, \text{i} = 1, 2, 3, \ldots \text{m}, \text{h}_i(x) = 0, \quad \text{i} = 1, 2, 3, \ldots 1 \quad (7)$$

x constitutes a selection vector, the aggregate of the objective functions to be reduced is n. When n equals one, the model in (6) becomes a single-objective problem and the ideal answer minimizes the objective. Nevertheless, when $n > 1$, $\text{f}_i\ (x)$ represents the objective function, $g_i(\text{x})$ and $\text{h}_i(x)$ are the constraint/utility functions of the problem being maximized or minimized.

The nature of a solution in MOO is marked via the trade-off amongst the n varying goals. If the following conditions are met, then, x is domineering over y; all non-dominated arrangements are the ideal answers to the MOO problems. These solutions are referred to as Pareto set/front [29]:

$$\forall i{:}f_i\ (x) \leq f_i\ (y)\ \ and\ \exists j{:}f_i\ (x) < f_i\ (y) \quad (8)$$

MOOs are utilized to obtain a group of non-domineering solutions, drawback, or trade-off solutions. In the event that a solution does not dominate any other solution, then it is referred to as the Pareto-optimal solution. All the solutions delineate the trade-off surface known as the Pareto front [30].

Multi-objective metaheuristics are characterized into four major classes: scalar methodologies, criterion-based methodologies, dominance-based methodologies, and indicator-based methodologies. Figure 1 presents further details [31]. This figure likewise features the MOO technique that is adopted in our proposition.

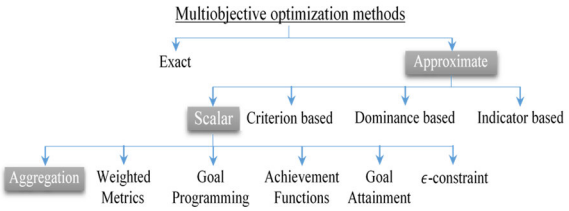

FIGURE 1. Classification of MOO algorithms, highlighting the methods used in this research.

1) SCALAR APPROACHES

The methodologies that mutate a MOO problem into an individual objective or cluster of such issues are contained in this category of MOO metaheuristics. The approach depicted in Section II is adjusted as a scalar methodology. The methodology incorporates the accumulation strategy, the weighted measurements technique, the goal programming technique, the achievement capacities, the goal achievement technique, and the ϵ-constraint technique. The rationale for the utilization of scalarization approaches is when Pareto ideal arrangements are produced. The scalar methodologies is a priori strategy, it requests that adequate inclination data is communicated before the solution process. The utility capacity strategy, goal programming, and lexicographic technique are common known instances of priori methods.

2) AGGREGATION METHOD

One of the foremost and widely utilized techniques for the generating Pareto optimal solutions is the aggregation (or weighted aggregation) method. In aggregate method, aggregation function is used to transform a MOO issue to a single-objective problem by joining several objective functions f_i into a single objective function f linearly:

$$f\ (x) = \sum_{i=1}^{n} \omega_i f_i\ (x) \quad (9)$$

where the weights $\omega_i \in [0\ldots1]$ and $\sum_{i=1}^{n} \omega_i = 1$.

In FS for intrusion detection systems, the trade-off includes three significant conflicting goals: classification error rate minimization, false alarm rate and feature's number. Thus, FS methodologies for IDSs is presented as a 3 objective minimization challenge. The FS process is optimized utilizing a number of procedures. However, the multi-objective binary bat algorithm for FS in IDS has not been explored as of recently, which has driven the examination of this specific strategy in this research [31].

III. RELATED WORK

These days, most of the IDSs are based on investigating all features in network packets for screening intrusion, interruption, and abuse patterns. FS method is viewed as perhaps the most essential technique which is applied in network security, especially in IDS. IDS is needed to manage tremendous volume of data that are likely made up of random, repetitive, and redundant features [32]. The main explanation behind the slowdown of the training and testing process can be because of logical inconsistency in features data, which brings about expanded resource consumption, just as in the decline of the execution of classification precision, and subsequently, rate of detection becomes low [33].

There exists a considerable amount of studies that encompass FS in the field of IDS. The studies focused on a decreased amount of features, removal of repetitive, unessential, and noisy data, and furthermore accelerate the results of IDS [34].

Numerous FS techniques have been applied in IDS. This section presents a rundown of past works on the utilization of FS techniques in IDS. Our study adds another technique, in view of the idea of MOO using the Bat algorithm. Details of the technique are introduced in the next sections.

In order to detect the generic attack Almomani and Omar [6] has developed a hybrid model for network IDS which includes two stages based on

hybridization bio-inspired metaheuristic algorithms. The first stage reduces the number of selected features for Network IDS, which is done via hybridization of bioinspired metaheuristic algorithms with each other in a hybrid model. There are many algorithms used in this stage that are mainly bat algorithm, grey wolf optimizer, whale optimization algorithm, moth-flame optimization, firefly algorithm, multiverse optimizer, and particle swarm optimization. The second stage employs random forest, support vector machine, and decision tree classifiers to detect generic attacks. The performance of this model was put to test using UNSW-NB15 dataset and based on the results the proposed model has achieved a 92.80% accuracy.

In [7] a new wrapper feature selection approach for IDS using Genetic Algorithm (GA) to select useful features, and Random Forest as classifier. The evolution-based feature selector uses an innovative fitness function to identify important features and reduce data dimensions, which raises the positive true rate and reduces the false positive rate at the same time. The proposed IDS performance analysis is evaluated using the NSL-KDD and UNSW-NB15 datasets. Based on the results of the experiment, the result in accuracy was 96.12%, 92.06% respectively.

In [8] proposed a hybrid model for network IDS that utilizes PSO and Random Forest (PSO-RF) algorithm to detect attacks. The PSO algorithm focuses on the applicability of a new cosmology inspired PSO algorithm in order to train random forest. The proposed IDS performance analysis has been evaluated using KDD-CUP 99 and UNSW-NB15 datasets, and it has achieved 97% and 75.94% accuracy on detecting the attacks, respectively.

In [9] developed two classification approaches for IDS based on the PSO algorithm that has been used for dimensionality reduction before employing the two classifiers for the classification procedure. The two classifiers employed are PSO and Decision Tree (PSO DT) and PSO and K-Nearest Neighbor (PSO KNN). Using KDD-CUP 99 dataset the proposed IDS has achieved 98.6, 89.6, and 1.1, in terms of accuracy, detection rate, and false alarm using the first proposed approach, and 99.6, 96.2, and 0.4, using the second proposed approach.

In [15] proposed a novel approach for IDS based on Multi-dimensional Feature Fusion and Stacking Ensemble Learning known as (MFFSEM). Comprehensive multi-feature datasets were prepared to meet the requirements for detecting abnormal behavior in real world. The multiple basic feature datasets are established considering different aspects of traffic information such as time, space, load, and the association and correlation among the basic feature datasets. Then, the stacking ensemble learning is performed on multiple datasets for overall features, thus an efficient global multidimensional model for anomaly detection is accomplished. We've evaluated the performance of the technique using KDD Cup 99, NSL-KDD, and UNSW-NB15 Datasets. Based on our results the accomplished accuracy was 92.48%, 84.33%, and 88.85% respectively.

In [16] proposed a novel machine learning for hybrid IDS based on Support Vector Machine (SVM) and Genetic Algorithm (GA) methodologies with an innovative fitness function developed to evaluate system accuracy. The performance of the approach has been tested using KDD Cup 99, NSL-KDD, and CICIDS2017 Datasets.

In [17] proposed a new cost-sensitive neural network method based on focal loss for network intrusion detection system. The proposal was applied using DNN and convolutional neural network to evaluate three benchmark datasets for Network Intrusion Detection Systems that suffer from imbalanced distributions: NSL-KDD, UNSW-NB15, and Bot-IoT.

In [18] developed IDS based on the ensemble of prediction and learning mechanisms to improve the accuracy of anomaly detection in a network penetration environment. The learning mechanism is based on automated machine learning, and the prediction model is based on the Kalman filter. The proposed IDS performance analysis has been evaluated using bothUNSW-NB15 and CICIDS2017 datasets and resulted in an accuracy rate of 98.80% and 97.02%, respectively.

In [32] developed a hybrid model for network IDS that includes a combined approach Principle Component Analysis and Deep Learning (PCA DL) to improve attack detection. By evaluating the method using KDD-CUP 99 dataset it has achieved a 92% accuracy in detecting the attacks.

In [33] proposed a lightweight supervised intrusion detection mechanism for IoT networks that uses optimized machine learning approaches through a combination of improvements including removal of multiple linear relationships, sampling, and dimensionality reduction. They tested their model using the CICIDS2017 and NSL-KDD datasets.

In [34] proposed a new Maximum correlation-based mutual information technique for efficient feature selection as the first stage and utilized the Kernel Extreme Learning Machine (KELM) based multiclass classifier for effective intrusion detection. they evaluated their framework by using the KDD cup 99, NSL-KDD, and UNSW NB15 datasets.

In [35] proposed the RL-NIDS that consists of two main modules, first learning module for unsupervised feature value representation that aims to explicitly learn feature interactions between categorical features, in the second module is supervised Neural Network for object Representation Learning which aims to learn the implicit interactions in the representation space. Accessible datasets inclusive of NSL-KDD and AWIDS were used to perform the experiment. The accuracy of the classification of datasets was 81.38% and 95.72%, respectively.

In [36] proposed a novel CNN model named RANet for NID automatically. In RANet, they not only introduce a Group-Gating module but also apply the overlapping method to the last max-pooling layer. and results showed that the proposed method achieved better classification outcome than the existing work of NID.

In [37] introduced for the first time the Jarvis-Patrick clustering algorithm in the field of anomaly detection and

proposed an extended JP clustering algorithm to overcome the shortcomings in the experimental process of JP clustering. Using the KDD CUP 99 dataset they proved that the detection rate of the extended JP clustering algorithm has greatly enhanced.

In [38] developed an adaptive and resilient model for NIDS based on deep learning architectures to improve the detection and classify network attacks. The focus is on how deep learning or Deep Neural Networks (DNNs) can facilitate flexible IDS with the ability to learn to detect recognized and new or zero network behavioral features, thereby taking out intrusive systems and reducing compromise risks. The proposed IDS performance analysis has been evaluated using the UNSW-NB15 datasets. Based on the results of the experiment, the accuracy and detection rate of the proposed model were 95.6%, 97.9% respectively.

In [39] proposed a hybrid model for network IDS which includes the adaptive particle swarm optimization and support vector machine (APSO-SVM) algorithm to correctly detect attacks. The APSO algorithm has been used to optimize SVM parameters. The proposed IDS performance analysis is evaluated using the KDD-CUP 99 dataset and has achieved 97.687% accuracy on detecting attacks.

In [40] proposed a new intrusion detection method (D-ONN) that uses a correlation tool and a random forest method to detect dominant independent variables to improve the neural-based attack classifier. To detect a malicious attack, a shallow neural network and an optimized neural-based classifier are presented. Their method, which used the KDDCUP99 dataset for evaluation, has demonstrated a very promising outcome. The results indicated that D-ONN has a higher outcome of 98% in terms of accuracy.

In [41] proposed IDS relying on an enhanced Multi-Objective Immune Algorithm (MOIA) for FS, and the NN was utilized for training the classification system leveraging appropriate feature chosen as subdivisions extracted by MOIA. The conventional MOIA was modified by the authors using a vector-based elite selection strategy, which can sustain individuals having favourable performance while differentiating greater than 5 class of attacks in IDS.

In [42] developed IDS that uses the ensemble classifier. This was built using Forest-based Penalizing Attributes and Random Forest. Their framework, which used the CIC-IDS2017 dataset for evaluation demonstrated a very high detection rate. The results indicated that CFSBA has a higher outcome of 96.76% in terms of accuracy, 94.04% rate of detection, and a lower false alarm rate of 2.38%.

In [43] presented a novel filter-based FS algorithm for IDS. It is based on a fusion of clustering approaches implemented by utilizing filter and wrapper approaches. The filter approach utilizes the cuttlefish algorithm (CFA) while the wrapper approach utilizes linear correlation coefficient method (FGLCC). In the work, decision tree was used as classifier and the performance was evaluated using KDD CUP 99 dataset. Detection rate, false positives and accuracy were used as the yardstick of assessment. The result showed a rate of detection of 95.23%, rate of false positive 1.65% and 95.03% of accuracy using the proposed FGLCC-CFA algorithm.

In [44] a light-weight system referred to as deep-full-range (DFR) used for the detecting advanced attacks was proposed by the authors. The framework utilizes deep learning (DL) for IDS and encrypted traffic classification.

In [45] put forward IDS which relies on a distributed DL system for examining and handling real-time data. The presented DNN model was used for intrusions and detection using network and host-based features collected in real time. Several experiments were conducted by the authors to compare the proposed system with available ML approaches. Accessible datasets inclusive of UNSW-NB15 and NSL-KDD was used to perform experiment. The results demonstrated that DNN surpasses different approaches for the binary classification. DNN with 5 layers gave a precision of 78.9% for binary classification for NSL-KDD. DNN with 5 layers produced a precision of 76.1% detection for UNSW-NB15.

In [46] implementation and evaluation of a DL algorithm for IDS in networks was carried out. The presented approach was trained on NSL-KDD and a deep NN. It introduced a vastly improved model fitting and an accuracy of 0.793 using 6 from the 41 features. The DL system gave a precision of 0.759 on the test set.

In [47] suggested IDS dependent on a DL technique utilizing a one-Dimensional Convolutional Neural Network (1DCNN). It was utilized for time-series supervised learning by serializing TCP/IP packets in a predetermined time range as an intrusion Internet traffic model for the IDS. Experiments was performed on the freely accessible UNSW-NB15 dataset. The outcomes indicated that the presented model performed better than different systems for classification with an accuracy of 0.9091 for the detection.

In [48] a new wrapper FS approach for IDS using Pigeon Inspired Optimizer (PIO) was put forward by Alazzam *et al.*. In the proposed PIO feature selection, the main features expected to develop an improved IDS was chosen, which guarantees a better rate of detection and false alarms decreased.

In [49] put forward a model which incorporates Multi-scale Convolutional Neural Network with Long Short-Term Memory (MSCNN-LSTM). An attempt was made to use MSCNN in analysing the data stream's spatial features. The LSTM system is utilized to activate the temporal features. In the end, the model leverages the spatial-temporal features for conducting the classification. Publicly available dataset UNSW-NB15 was used to conduct the experiments.

In [50] introduced a hybridized model for anomaly detection. The put forward model is a platform that detects malicious actions and sieves network traffic on the network. The filtering and extraction of distinctive features of the digital attacks were carried out using linear algorithms while the learning algorithms identify new types of cyber-attacks using these attributes and features.

In [51] presented a kernel analysis for reducing the dimensions, extracting the feature, combining differential evolution and gravitational search algorithm for optimizing the indicators of HKELM. KPCA-DEGSA-HKELM which is a novel IDS approach was attained afterwards.

In [52] presented another combination technique for anomaly network-based IDS (A-NIDS) utilizing an Artificial Bee Colony (ABC) technique (utilized for FS) and AdaBoost approach to acquire a detection rate that is high and a lower false-positive rate.

In [53] put forward a novel IDS method that utilized the multivariate control chart dependent on the quick Minimum Covariance Determinant (Fast-MCD) calculation for enhancing the capacities of the presented system to rapidly and precisely recognize the exceptions, and Kernel Density Estimation (KDE).

In [54] developed a hybrid IDS model that includes two stages based on hybridization the optimization of Quantum Beetle Swarm Algorithm (QBSA) for extreme learning machine to detect the generic attack. First, the QBSA is proposed. The precept of quantum mechanics is introduced to combine the BSA with the PSO algorithm. It is proposed that the LSQR decomposition set of rules is used to optimize the intense studying machine, it may reduce the amount of computation and increase the speed of convergence. Secondly, the QBSA algorithm is designed to understand the joint optimization of the weights and thresholds of the improved ELM. Finally, the QBSA-IELM model is applied to the field of intrusion detection. The performance of this model was evaluated on the CICIDS2017 dataset the accuracy achieved was 94.55%.

This studies presented an IDS system created utilizing another metaheuristic, MOBBAT, in view of the binary and multi-objective BAT algorithm, with the end goal of multi-objective FS. This approach utilizes the wrapper method of FS and utilizes the most encouraging improved bat model to train the MLP, as the wrapper classifier, the upgraded BAT is accustomed to tackling the issues experienced by the MLPs. The outcome of our tests revealed that our new methodology outperforms the wide range of various procedures in literature.

IV. METHODOLOGY OF THE STUDY

The methodology of this research is split into two as demonstrated in Figure 2: (1) the design of the two (2) principal modules of the presented method, which incorporate the FS procedure and a metaheuristic system for training the NN, (2) deployment of the presented system, coordinating the two prior modules in a connected framework, and (3) the assessment of the novel methodology and appraisal of the outcome by comparing it with different methodologies.

The critical target of this study is the selection of the significant features from individual network packet which can be accomplished by the EBAT-based optimization as the wrapper classifier. The optimization depends on utilizing

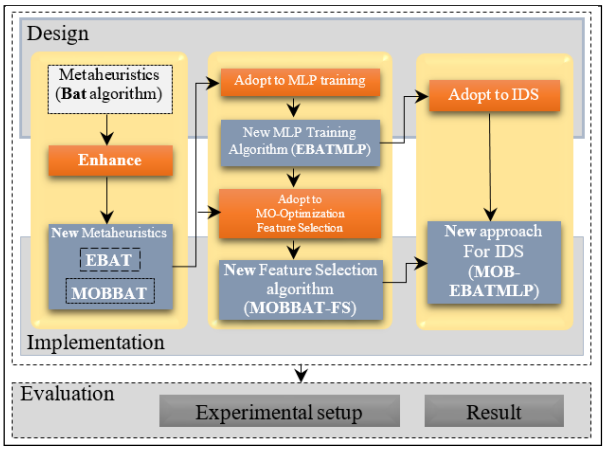

FIGURE 2. Research methodology.

a multi-objective and binary variation of the BAT system. An ideal subset of the features which is the output of this step is forwarded to the EBATMLP system. Hence, leading to an improved detection capacity to detection capacity.

Finally, the presented system is tested and assessed in the last step advance, in view of its efficacy for an increase in detection accuracy and a diminished false alarm rate. Five famous benchmark datasets were used to assess the performance of the system: KDD CUP 1999, ISCX2012, NLS-KDD, CICIDS2017, and UNSW NB15.

A. TRAINING OF MLP MODEL WITH THE EBat ALGORITHM

The model is categorized into four (4) fundamental phases: parameter initialization, data input, NN training, and the EBAT module.

In the preceding phase, initialization of the parameters of the EBAT system and the NN model are conducted. There are numerous variables in the EBAT algorithm, including Populace Size (NP), which addresses the amount of solutions in the population. Each solution ($i = 1, 2\ldots, D$) addresses a D-dimensional vector where D is the sum total of decision factors.

Solution Memory (SM) is a grid of the supreme solution vectors attained until this point. It is an increased matrix of size NP $\times$ D. The FS size is adjusted preceding executing the procedure. Every solution vector is additionally connected with a good value in light of the objective function f(x). Figure 3 depicts the algorithm.

In the subsequent stage, the data input component is the significant phase of data input. It depends on the processing, filtering, and extracting the features from the raw data. A pivotal step is the division of the raw data to the training and testing sets. It is utilized as input data in the next component. Preceding feeding the data into the NN model, the approaching data sources ought to fit into the scale from 0 to 1. For the training in the following module this normalization process is significant.

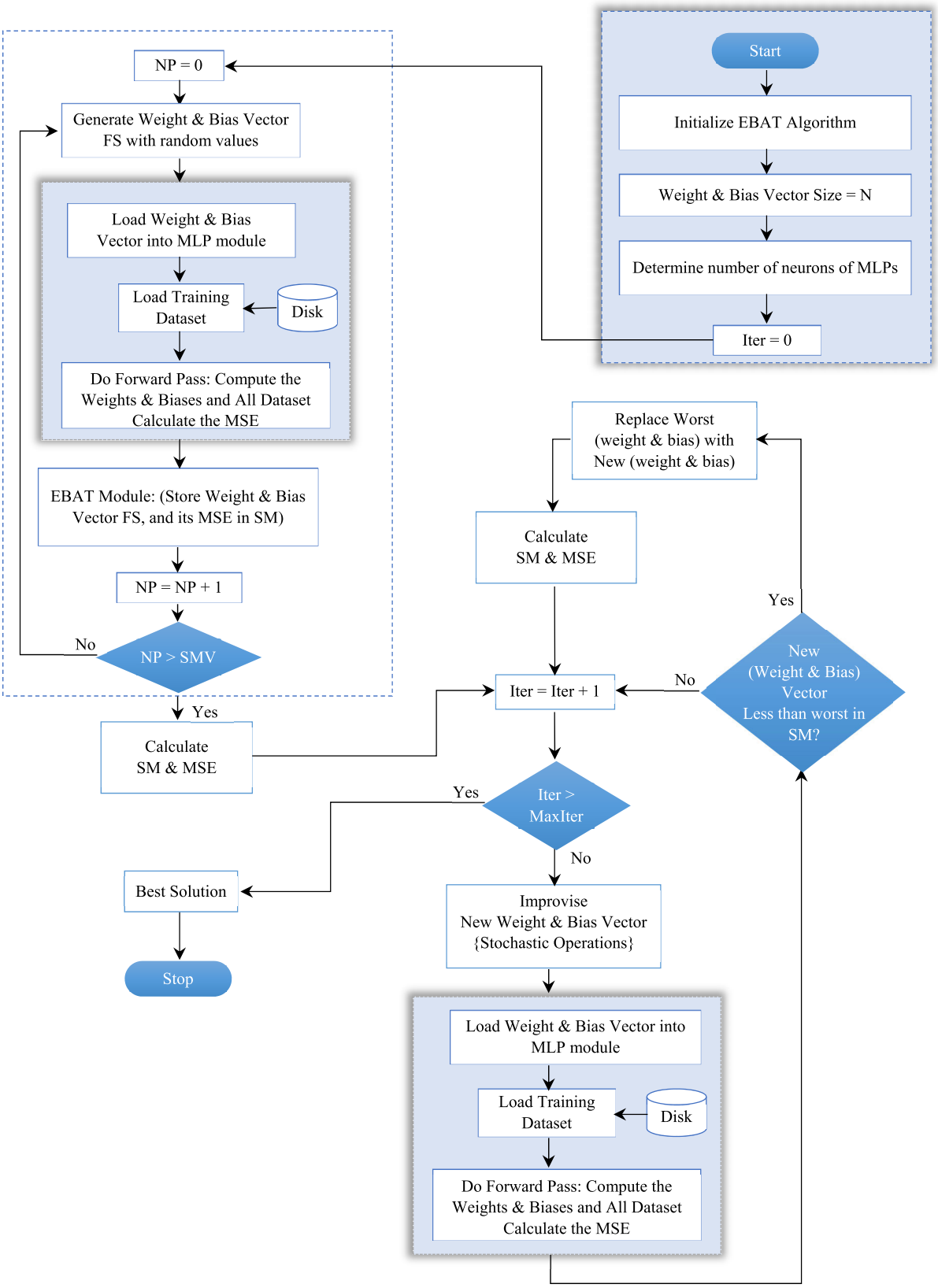

FIGURE 3. EBATMLP training algorithm flowchart.

In the third stage, the MLP model gets training features of the input data measurement from the information input components, the MLP starts to work. This component is planned as an MLP, a Feed-Forward Neural Networks organization (FFNN). The design of the MLP comprises of three layered neurons that contains an info layer, a concealed layer, and a yield layer. The outcoming information from the information input module, which are considered as preparing design information (preparing dataset) for preparing the MLP are gotten by the MLP module. It is deserving of note that the preparation interaction in this module is actualized by means of sending the loads and inclinations to the EBAT component.

In the fourth stage, the EBAT module is utilized as an independent framework (Black Box) for creating new arrangements, which depend on the refreshing of the synaptic loads and inclinations after every cycle. In every cycle of the preparation interaction, the EBAT module sends each arrangement as a bunch of loads and predispositions into the MLP component. In this manner, each arrangements dependent on a preparation dataset are assessed and afterward restored their wellness esteems. The Fitness Function (FF), Mean Square Blunder (MSE) is chosen in this work to process the wellness. The loads and inclinations are acquired by limiting the mistake rate estimation of MSE.

The preparation interaction stops once arriving at the greatest number of cycles. Thereafter, the information base of loads and predispositions is refreshed.

The EBAT algorithm is identified with other streamlining system. Consequently, the objective is deciphered as expanding or limiting a measure gotten by this FF. The objective of such FF ought to be like its usefulness in improving calculations. Other than that, its goal is like preparing techniques as shown by past examinations [20], [25], which is to decrease the general blunder. Hence, the previously mentioned FF could use any of the MLP blunder estimation equations or infer another wellness measure dependent on the recipes.

In this study, MSE is utilized as the main quality proportion of the put forward EBAT preparing calculation. On a very basic level, the preparation objective is to limit the MSE up to arriving at the greatest aggregate of emphasis.

MSE is a broadly utilized FFs. Since this work is accentuated on the categorization issues, the MSE, as the primary FF, computes the arrangement vectors that ought to be arranged from the highest to most noticeably poor with the highest being the arrangement with the lowest MSE. Accordingly, to locate an ideal arrangement, for example the MLP with the best loads and predispositions vector, the MSE esteem should be the littlest amongst the current arrangement memory vector. Furthermore, the FF is suitable for assessing the nature of the arrangement in progressive emphases. Utilizing the FF, a solution is chosen for the advancement of the nature of the arrangement.

Initially, the forward pass computations should be acted to process MSE on the given MLP; which is a monotonous interaction that includes stacking of the whole dataset preparation. It needs a cycle for the organization loads and inclinations, addressed by the arrangement vector, are stacked into the MLP design to execute the algorithm. The MLP is adaptable to permit stacking of various weight and inclination vectors during the EBATMLP calculation introduction and extemporization measures. The forward pass calculation measure is appeared in Figure 3.

The target of preparing the MLP is to accomplish the most elevated arrangement, estimate, or forecast precision for both preparing and testing tests. In this work, a comparative procedure utilized by a few examinations [20], [25] was applied to ascertain the FF. Expecting that the quantity of information hubs is equivalent to (N), the quantity of concealed hubs is equivalent to (H), and the quantity of yield hubs is (O), subsequently the yield of the i^{th} shrouded hub is determined as follows:

$$\begin{aligned} f\left(S_j\right) &= Sigmoid(s_j) \\ &= 1 \Big/ \left(1 + exp\left(-\left(\sum_{i=1}^{N} \mathcal{W}_{ij}.\mathcal{X}_i - \beta_j\right)\right)\right), \\ j &= 1, 2, \ldots, H \end{aligned} \tag{10}$$

where $S_j = \sum_{i=1}^{n} \mathcal{W}_{ij}.\mathcal{X}_i - \beta_j$, n is the number of the input nodes, $\mathcal{W}_{ij}$ is the connection weight from the i^{th} node in the input layer to the j^{th} node in the hidden layer, β_j is the bias (threshold) of the j^{th} hidden node, and $\mathcal{X}_i$ is the i^{th} input. After calculating the outputs of the hidden nodes, the final output can be defined as follows:

$$O_k = \sum_{i=1}^{N} \mathcal{W}_{kj} f\left(S_j\right) - \beta_k, k = 1, 2, \ldots, O, \tag{11}$$

where $\mathcal{W}_{kj}$ is the connection weight from the j^{th} hidden node to the k^{th} output node and θ_k is the bias (threshold) of the k^{th} output node. In conclusion, the learning error E (FF) is computed as follows:

$$E_k = \sum_{i=1}^{O} \left(O_i^k - d_i^k\right)^2 \tag{12}$$

$$\mathrm{MSE} = \sum_{\mathrm{k}=1}^{\mathrm{q}} \frac{\mathrm{E_k}}{\mathrm{q}} \tag{13}$$

where q is the number of training samples, d_i^k is the desired output of the j^{th} input unit when the k^{th} training sample is used, and O_i^k is the actual output of the i^{th} input unit when the k^{th} training sample is used. Therefore, the FF of the i^{th} training sample can be defined as follows

$$\mathrm{Fitness}(x_i) = \mathrm{MSE}(x_\mathrm{i}) \tag{14}$$

B. DESIGN OF MOBBAT

In proposing a novel method for detecting intrusion, the main issues that should be the focus are; firstly, identifying significant and eliminating insignificant features from the network. Secondly, building up a methodology with a large capacity for detecting malicious packets, reliant on the features identified in the past phase.

The initial phase in this research depends on extracting significant and disposing of the replicated features.

The overall idea is depicted in Figure 4. The methodology depends on the accompanying 5 essential stages: initialization method, discovery technique, assessment function, stopping standards and validation strategy.

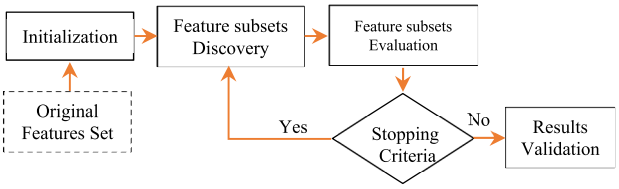

FIGURE 4. General procedure for feature selection with validation.

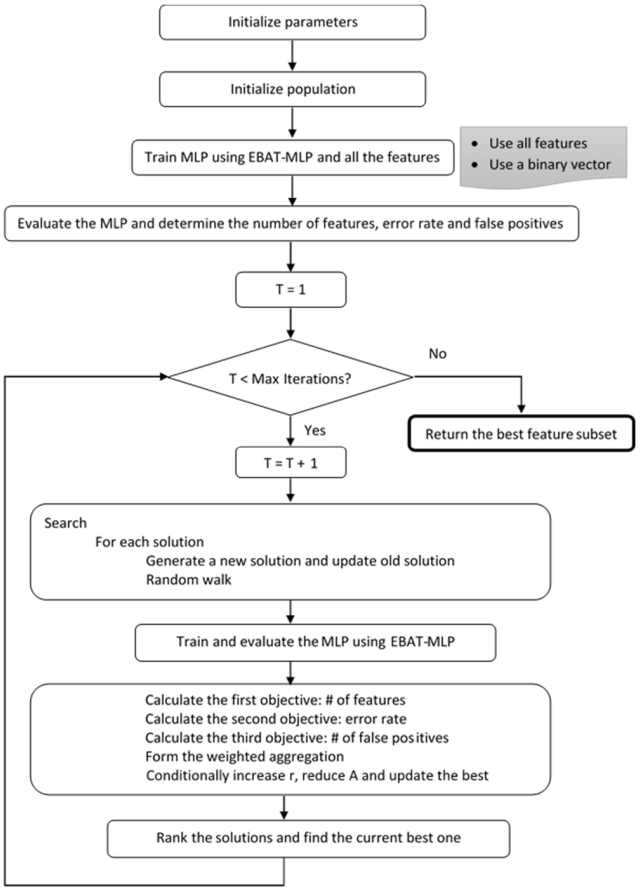

FIGURE 5. MOBBAT algorithm flowchart.

The initial step begins with an introduction strategy for all the first dataset features. In the presented MOO model, the dimension of the search space is regularly adjusted as the aggregate of all accessible features in the system. The initialization method is relative to the first period of the MOBBAT.

Subsequent phase creates candidate feature subsets. It begins with an arbitrary sub-features produced by the MOBBAT as potential solutions. Third phase assesses the feature subset created by the subsequent phase utilizing the EBAT-MLP system for training MLP NN. This phase assumes a significant part in the entire process of FS and classifies the FS model as wrapper based. It enables control and finding the ideal feature subset.

The fourth phase tests the stopping rule to choose to stop the search or not for additional feature subsets. The standard depends on a predetermined amount of chosen features or on the scope to the greatest amount of predetermined iterations.

The fifth phase validates parts of the approach that does not belong to the FS procedure; notwithstanding, most FS algorithm needs to validate the result of the search procedure. The significant phases in Figure 4 are depicted with synopsis in Figure 5, while the accompanying subgroups expound more on the principle modules of the algorithm.

1) WRAPPER APPROACH USING EBATMLP

MOBBAT being a wrapper-based FS method requires a classifier that is wrapper-based to assess all produced subdivisions by the methodology. Thus, MOBBAT is the feature selector. The evaluator classifier is the EBATMLP presented in Section IV. The part of EBATMLP appears in the lower circle of the chart in Figure 5. Whenever a new solution is produced, another feature subset is chosen. This is passed to an MLP trained by EBATMLP utilizing the new features, and the outcome act as input to the algorithm, from where the 3 objectives are determined and the new result is positioned.

2) MOBBAT PARAMETERS

The MOBBAT utilizes similar parameters to the first BAT model. The control parameters are r, A, and the most extreme amount of iterations to find solutions for. This study utilizes the highest aggregate of iteration to 50. The solution space's dimension depends on the feature's number for each dataset utilized to assess the completed methodology. The populace size NP equals 50. The MOBBAT system is run 10 times for each analysis and after arriving at the greatest number, the iteration is halted.

3) BINARY ENCODING

A significant step prior to processing data via any ML strategy is the representation and formatting of data. A quality representing model is of an essential significance in the greater part of the classification approaches of ML.

This work explored the feature-value as the representation system. Along these lines, each instance in this framework is depicted as a vector for characterizing the problem domain. The network traffic is reserved as a dataset, normally addressed as a table where individual row addresses an occurrence and individual column addresses an alternate element in the network.

In the MOBBAT, the depiction of a solution is an n-bit string; n stands for the aggregate amount of features in the dataset. The value in the d^{th} position of the solution (x_d) is in [0, 1], which depicts the probability of the d^{th} feature being chosen. Another method is utilizing the threshold θ. A threshold θ is utilized for finding if a feature is chosen or

not. If ($x_d > \theta$) the d^{th} feature is chosen, otherwise, the d^{th} feature is not chosen. Thus, the new sub-features are obtained from the regular features. MOBBAT is using the threshold approach. Figure 6 shows a new subset feature that can be regarded as a potential answer, which is uniquely identified by a binary string.

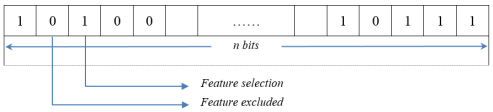

FIGURE 6. Representation of a possible solution as binary string.

4) MULTI-OBJECTIVE CRITERIA

The overall idea of MOO is clarified in Section II. A critical characteristic for MOBBAT, is its dependence on different objectives to assess the quality of generated solutions, rather than depending on a solitary criterion. In MBO, the goodness of every arrangement against a specific objective or rule is controlled by the FF which assumes the role of the cost function or objective. On the off chance that the required optimization is a minimization issue, at that point, the least the value of the FF, the better the solution and vice versa for maximization issues. Having more than one objective requires corresponding FFs with potential dissension in their deduction of the quality of a similar solution.

The goal of high precision on account of MOBBAT is self-evident, just as the target of low false positives. These are well-grounded measures for assessing the performance of NNs. There is additionally another objective that ML literature consistently emphasizes and fits the motivation behind an FS algorithm, which relates with the issue of high dimensionality; i.e., to decrease the feature's number and thus lessen the computational intricacy. The 3 aims are itemized as follows:

- Number of features ➜ as least as could be expected.
- Accuracy ➜ as greatest as could be expected.
- False positives ➜ as least as could be expected.

On the off chance that objective had its own FF, three (3) unique assessments would be created for a similar solution, with conflicting characteristics, and afterwards, these assessments must be solidified somehow or another to deliver a final judgment on the quality of the solution. In any case, there is no requirement for different objectives to have their own FFs.

A typical technique to manage multiple objectives is to total the objectives into a single value, to allow a single FF that runs just a single time, giving a single assessment output. Since various goals might be distinctive in their significance, their collection may handle them distinctly. A regular option involves increasing the different objective values by distinct weights, as indicated by their significance in the assessment, and afterwards adding them together. For instance, on account of choosing features for a NN, it is fundamental that the chosen feature help in improving the accuracy of the framework. Besides, it is essential to maintain low false positive rate. Lastly, it is vital having lesser feature's number.

To total 3 objectives of MOBBAT, the contention in their characteristics ought to be resolved, with the goal that while computing all objective values in the assessment of the solution in a single FF, all qualities limit or augment each estimation of the FF as per the quality of their relating objectives. However, they do not drop the impact of one another. To accomplish that, the three (3) objectives and their relating characteristics are adjusted as follows, taking note of the fact that a high precision rate is equivalent to a lesser error rate:

- Number of features ➜ as least as could be expected.
- Error rate ➜ as least as could really be expected.
- False positives ➜ as least as could be expected.

To assess feature subsets for performing great with MLP classifications, in view of the above argument, the weighted accumulation utilized by MOBBAT is:

$$\begin{aligned} \textit{Aggregated Objective} = {} & w_1 \times \textit{no.of features} + w_2 \\ & \times \textit{error rate} + w_3 \\ & \times \textit{false positive rate} \end{aligned} \tag{15}$$

In Equation (15), w_1 represents the weight for the number of features, w_2 is the weight for the classification error rate while w_3 is the weight of the false positive rate. Both w_2 and w_3 are set to be greater than w_1 because the false positive rate and the classification error rate are presumed to be more significant selected features number. The chosen values for w_1, w_2 and w_3 in the evaluation are 0.1, 0.5 and 0.4, correspondingly.

5) COMPUTATIONAL COMPLEXITY

The computational complexity of the enhanced bat algorithm is mainly based on the number of solutions which is referred to as the dimension (D), and the number of the populations which is the population size (NP) of the MOBBAT algorithm.

In the worst-case scenario the overall computational complexity is O (DNP) $\approx$ O (O (calculate the bat position of all solutions and evaluate its fitness) + O (sort solutions of population and bat population)).

The time complexity of the generation in the generative process of the MOBBAT algorithm is analysed as follows:

In phase 1, the basic process is the creation of the initial population, and the time complexity is O (NPD).

In phase 2, Decision making based on stop/termination criteria, the time complexity is O (1).

In phase 3, Calculate the value of an aggregated objective parameter based on three objectives which are a number of features, error rate, and false positives, the time complexity is O (1).

In phase 4, Updating the solution, the time complexity is O (N).

In phase 5, Generation continues and returns to Step 2. Therefore, the time complexity of the MOBBAT algorithm is O (NPD).

C. INTEGRATING MOBBAT WITH EBAT-MLP FOR IDS

The fundamental contribution of this study is to present a total IDS approach, in light of the trained MLP by EBATMLP which is augmented by an enhanced set of selected features. This objective involves two fundamental parts: FS and classification. The FS segment is processed by MOBBAT. The classification segment is arranged by the MLP trained to utilize the EBATMLP system.

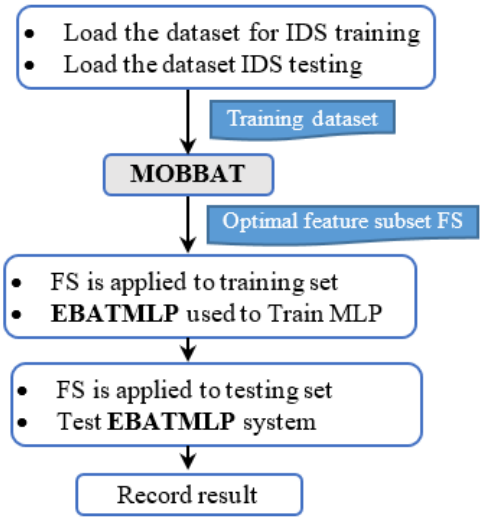

FIGURE 7. Integrating MOBBAT with EBATMLP to form MOB-EBATMLP.

The Figure 7 portrays how every one of the mentioned segments fits into the master plan of the full IDS. It is important that EBATMLP is additionally utilized inside the MOBBAT as the wrapper classifier for the FS. Subsequent to choosing the ideal feature set, EBATMLP is utilized for training the MLP and characterizing the patterns of the traffic dependent on the chosen features. The unified model is utilized in the ensuing assessments for testing the performance of MOBBAT and the complete IDS referred to as MOB-EBATMLP.

D. IDS DATASETS

Dissimilar to the datasets used for classification, the assessment of the proposed NN system for the particular reason for IDS defines the utilization of remarkable benchmark datasets for this particular framework. Five available datasets for testing IDSs are briefly explained in this section.

1) KDD CUP 99 DATASET

KDD Cup 1999 is a universally recognized and very popular dataset for detecting anomalies and attacks. Lee and Stolfo [55] created and developed it in 1999. It is based on data acquired from MIT Laboratory, for Defense Advanced Research Projects Agency (DARPA ITO) and Air Force Research Laboratory (AFRL/SNHS) sponsorship. It has around 5 million records addressing TCP/IP packet connections. A packet consists of 41 features; with 3 being symbolic and 38 numeric.

It has 23 attacks classified into 4 sorts of attack information: Denial of service (DOS), Remote to Local (R2L), User to Root (U2R) and probing (PROBE). It is divided to 3 sections: basic, traffic and content attributes. Basic attributes consist of complete attributes procured from the packet headers. Traffic attributes comprise: the ''same host'' and ''same service''. Content attributes are extracted from the payload of the packets for finding malicious behaviour in the payload section. Each one helps in deciding whether the connection is with the normal host or service accordingly [56]. Four sets of the KDD Cup '99 were utilized in this study. They were made and randomized by [57], and are utilized by numerous researchers [20], [25]. Each and every information set holds roughly 4000 records. 50% of the information (50-55%) is categorized as normal and the extras are attacks. Dataset 1 is utilized for training, while datasets 2, 3, and 4 are used for testing. Thorough details are organized in Table 1.

TABLE 1. Distribution statistics of the KDD CUP 99 training and testing datasets.

Type	Dataset 1		Dataset 2		Dataset 3		Dataset 4	
	Actual	%	Actual	%	Actual	%	Actual	%
Dos	1000	25%	1203	30%	1050	26%	903	23%
Probe	563	14%	400	10%	491	12%	475	12%
R2L	122	3%	55	1%	30	1%	62	2%
U2R	15	0%	45	1%	30	1%	10	0%
Normal	2300	58%	2300	57%	2400	60%	2550	64%
Total	4000	100%	4003	100%	4001	100%	4000	100%

2) NSL-KDD DATASET

The NSL-KDD dataset was presented to cater for a large number of the intrinsic issues of the KDD'99 dataset. Its size is practicable, making it appropriate for applying a complete set in one pass; subsequently, the evaluation outcome of various studies becomes practically comparable and reliable [58]. It has additionally the accompanying advantages as against the regular KDD dataset:

- The training set has no repetitive records, so that there would be less inclination of classifiers as regards more regular data.
- The testing set has no duplication of records; in this manner, learner's performance is not impacted by the strategies having detection rates that are better on normal records.
- Each degree of difficulty group would have different data that is contrarily relative to the records percentage in the regular dataset of KDD. Accordingly, providing precise assessment of various learning procedures, owing to the variety in scope of characterization rates of different ML.

The dataset is outlined from the different divisions of the original KDD Cup 99 without replication or redundancies. Also, the concern of having an unequal dispersion in an individual class during the training or testing set was addressed to enhance the precision of the system. The dataset

of NSL-KDD integrates 41 features marked by attack types or regular connections. It is divided into training and testing sets with 4 attack divisions, in particular: DoS, R2L, U2R, and test. The dataset can be reached on (http://nsl.cs.unb.ca/NSL-KDD/). The dispersion of the records in NSL-KDD is given in Table 2.

TABLE 2. Distribution statistics of the NSL-KDD training and testing datasets.

	Train NSL-KDD		Test NSL-KDD	
	Actual	%	Actual	%
Attack	11743	46.61%	12829	56.90%
Normal	13449	53.38%	9714	43.09%
Total	25192	100%	22543	100%

3) ISCX 2012 DATASET

To address the shortcomings of the dataset of KDD cup 1999, the Information Security Center of excellence (ISCX) put forward ISCX which is additionally utilized for testing and assessing the performance of the presented method for IDS. ISCX contains 20 features and almost 1512000 packets which encompasses network activities for 7 days. It is accessible in packet capture structure. The extraction of features is performed using tcptrace utility (http://www.tcptrace.org).

TABLE 3. Distribution statistics of the ISCX 2012 training and testing datasets.

Date	Train ISCX 2012		Test ISCX 2012	
	Normal	Attack	Normal	Attack
11^{th}	0	0	0	0
12^{th}	2775	1388	1388	690
13^{th}	27144	13572	3393	6786
14^{th}	5028	2514	2514	1257
15^{th}	12459	6229	6229	3115
16^{th}	0	0	0	0
17^{th}	6938	3468	3468	1735
Total	54344	27171	16992	13583
	81515		30575	

The approaching packets are chosen by the author of the dataset for a specific days and host as introduced in Table 3. Normal traces in the training data is 54344; attack traces 27171. Normal traces in the testing data is 16992; attack traces 13583 [59].

4) UNSW-NB15 DATASET

UNSW-NB15 is a fusion of contemporary coordinated attack events and regular traffic (can be accessed at http://www.cyber-security.unsw.adfa.edu.au/ADFA%20NB15%20Data sets). It was developed by scientists; Nour and Jill utilizing IXIA PerfectStorm device in the Cyber Range Lab o the Australian Centre for Cyber Security. It has in excess of forty (40) features. In any case, note that the initial two datasets share regular features with the UNSW-NB15, and the remainder of the features are different, making the comparison challenging [60].

The UNSW-NB15 dataset incorporates nine diverse present-day attack (in contrast to twenty-three attack types in NSL-KDD and KDD'99) and an extensive variety of genuine typical events alongside 44 features notwithstanding the class label, comprising of 2,540,044 records totality. The six categories of the are features are: Additional Generated Features (AGF), Time Features (TF), Content Features (CF), Basic Features (BF), class features and Flow Features (FF). The AGF is additionally characterized to two sub-divisions; Connection and General Purpose Features.

TABLE 4. Distribution statistics of the UNSW-NB15 training and testing datasets.

	Train UNSW NB15		Test UNSW NB15	
	Actual	%	Actual	%
Attack	119341	68.06%	45332	55.06%
Normal	56000	31.94%	37000	44.94%
Total	175341	100%	82332	100%

It is split to two sets, the first set addresses the training and consists of 175,341 records. The second addresses the testing dataset and consists of 82,332 records. Table 4 depicts the distribution of the datasets in the wake of totaling the attack types into one class. It should be noted that the id feature is not referenced in the complete UNSW-NB15 dataset along with the features scrip, sport, dstip, time, and ltime are absent in the dataset [61].

5) CICIDS2017 DATASET

The CICIDS2017 dataset is a fusion of contemporary coordinated attack events and regular traffic (can be accessed at https://www.unb.ca/cic/datasets/ids-2017.html). It was developed by scientists; Iman S., Arash H. L., and Ali A. G. [62] utilizing CICFlowMeter software system that is publicly obtainable via the Canadian Institute for Cybersecurity website. The dataset is fully labeled and contains over eighty network traffic features extracted and calculated for all benign and intrusive flows alike.

It is also distributed over eight different files containing five days' (Monday, Thursday, Friday, Wednesday, and Tuesday) normal attacks traffic data of the Canadian Institute of Cybersecurity [63]. Thursday operating hour afternoon and Friday records are properly proper for binary classification. Whereas, Tuesday, Wednesday, and Thursday morning records are particularly used for designing multi-class detection versions. From perspective, the eight files or some of them can be combined to form an appropriate data set to be used in the evaluation phase when building intrusion detection models. All files combined will contain a dataset of 3119345 instances and 83 features with 15 class classifications (1 normal 14 attack classes).

The CICIDS2017 dataset collectively carry 2,830,743 which is a set of eight files of each benign attacks and every file carries seventy-nine features with the label. In this research only two files have been nominated: File 1(Friday WorkingHours Afternoon DDos.pcap_ISCX) and file 8 (Wednesday workingHours.pcap ISCX). File 1 includes elegance labels along with benign and DDos attacks, and file 8 includes multi-elegance labels along with benign DOS GOLDEN EYE, DOS HULK, DOS SLOW HTTP TEST, DOS SLOW LORIS, HEART BLEED. For performance comparison purposes of CICIDS2017, it has been split into two sets, the first set addresses the training and consists of 44,98039 records. The second addresses the testing dataset and consists of 25,2671 records.

E. EVALUATION METRICS

The performance of the presented strategy is assessed utilizing the accompanying measurements: accuracy ACC, false alarm rate FAR, detection rate DR, specificity, sensitivity, and precision. The FAR, DR, and ACC are determined dependent on particular types of instances: true positives TP, true negatives TN, false positives FP, and false negatives FN.

TABLE 5. Confusion matrix for binary classification.

		Actual		Total
		Normal	Attacks	
Predicted	Normal	TN	FN	TN + FN
	Attacks	FP	TP	FP + TP
Total		TN + FN	FN + TP	

TABLE 6. Definitions of measurement types used to calculate performance indicators.

Type	Definition
TP	Specifies the number of attack data detected is actually attack data.
TN	Specifies the number of normal data detected is actually normal data.
FP	Indicates the normal data that is detected as attack data.
FN	Indicates the attack data that is detected as normal data.

These four fundamental models were gathered from the confusion matrix (CM). CM summarizes the classification results. Table 5 provides the CM for binary classification. Definitions of the types are provided in Table 6 and the definitions of all performance pointers are provided in Equations (16-21).

$$ACC = \frac{TP + TN}{TP + TN + FP + FN} \tag{16}$$

$$DR = \frac{TP}{TP + FN} \tag{17}$$

$$FAR = \frac{FP}{FP + TN} \tag{18}$$

$$Specificity = \frac{TN}{TN + FP} \tag{19}$$

$$Sensitivity = \frac{Tp}{TP + FN} \tag{20}$$

$$Precision = \frac{TP}{TP + FP} \tag{21}$$

V. EVALUATION OF MOB-EBATMLP

Like the works in past sections, the proposed MOBBAT system is altogether assessed with regards to MOB-EBATMLP, so the performance of the ensuing IDS procedure is verified. The methodology is tried against the five benchmark datasets detailed in Section IV, and the outcomes are contrasted and chosen well-known works from the literature.

A. KDD CUP 1999 RESULTS

The MOB-EBATMLP was initially used on the KDD Cup 99 dataset using the subsets itemized in Table 1. The union is presented in Table 7. Furthermore, the table presents the particular features selected by the MOBBAT when utilizing other subsets. The relating classification outcome is presented in Table 8.

TABLE 7. Selected features when testing against the KDD CUP 1999 dataset.

Training	Testing	Selected features	Size
Dataset 1	Dataset 2	{1,3,6,7,10,11,17,20,25,28,31,32,34,36,37,38,39 }	17
	Dataset 3	{1,7,8,10,13,15,17,18,20,24,26,30,32,33,35,36,37 }	17
	Dataset 4	{1,2,9,12,13,16,18,22,23,24,28,29,31,33,36,38,39}	17
Dataset 2	Dataset 1	{2,3,5,6,8,9,10,11,12,14,15,17,24,25,31,32,40}	17
	Dataset 3	{3,4,6,8,13,14,15,17,18,19,20,21,24,25,26,30,38,39}	18
	Dataset 4	{1,4,7,13,21,26,28,29,30,32,35,37,38,39,40}	15
Dataset 3	Dataset 1	{1,3,5,7,8,11,12,13,15,17,19,25,27,29,30,31,33,36,38,39}	20
	Dataset 2	{1,2,3,4,7,8,10,11,13,15,17,20,22,24,26,27,29,30,31,32,33,34,35,37,38,39}	26
	Dataset 4	{1,2,3,7,8,9,10,11,12,16,19,22,25,30,31,32,34,36,37,38,39}	21
Dataset 4	Dataset 1	{3,6,7,8,9,10,11,12,13,14,16,21,23,24,25,28,29,30,34,35,36,38,39}	23
	Dataset 2	{1,3,4,5,6,8,9,10,11,13,14,16,18,21,22,23,24,28,29,30,34,36,37}	23
	Dataset 3	{1,2,3,4,5,6,9,12,14,16,17,18,19,20,21,22,24,25,27,30,31,33,35,38,39}	25

Table 8 records results for: number of true and false positives, true and false negatives, the precision, false alarm and detection rate. The estimations of the last three measures are gotten from the initial four values, based on the equations given in Section IV. Each row correlates to a pair of training/testing datasets. The last row generates an average accuracy of 94.24%, rate of average detection:96.09%, and rate of false alarm: 0.0786.

Figure 8 shows the specificity, sensitivity and Precision results illustrated after testing the MOB-EBATMLP approach against the 1999 KDD CUP data set.

TABLE 8. Classification results when testing against the KDD CUP 1999 dataset.

No.	Training	Testing	ACC	DR	FAR
1		Dataset 2	98.05%	99.59%	0.0285
2	Dataset 1	Dataset 3	95.55%	97.90%	0.0843
3		Dataset 4	91.85%	99.72%	0.1461
4		Dataset 1	89.03%	89.89%	0.1239
5	Dataset 2	Dataset 3	97.60%	96.48%	0.0059
6		Dataset 4	95.63%	96.97%	0.0549
7		Dataset 1	83.33%	89.41%	0.2771
8	Dataset 3	Dataset 2	98.38%	98.14%	0.0132
9		Dataset 4	95.20%	99.34%	0.0824
10		Dataset 1	90.88%	90.57%	0.0855
11	Dataset 4	Dataset 2	98.15%	97.90%	0.0150
12		Dataset 3	97.25%	97.22%	0.0270
	Average		94.24%	96.09%	0.0786

TABLE 9. Selected features when testing against the NSL-KDD dataset.

Dataset	Selected features	Size
NSL-KDD	{1,3,4,8,13,16,18,21,23,31,32,37}	12

TABLE 10. Classification results when testing against the NSL-KDD dataset.

Dataset	ACC	DR	FAR
NSL-KDD	99.16%	99.38%	0.0148

B. NSL-KDD RESULTS

Table 9 lists the 12 most effective features of attack detection information being proposed here using NSL-KDD, and these features are the most valuable feature for intrusion detection. Table 10 provides performance measures for the proposed method with 12 features, and clearly shows a highly achieved a detection rate and accuracy of 99.16% and 99.38% respectively. In addition, the false detection rate was close to zero with a score of 0.01. Figure 9 depicts the performance results in terms of sensitivity, specificity, and precision obtained from applying the NSL-KDD Dataset against the MOB-EBATMLP approach.

TABLE 11. Selected features when testing against the ISCX 2012 dataset.

Dataset	Date	Selected features	Size
ISCX12	12^{th}	{1,2,4,6,8,10,13,14,17,19}	10
ISCX12	13^{th}	{1,2,4,5,6,11,12,14,15,16}	10
ISCX12	14^{th}	{5,8,9,11,12,14,16,17,19}	9
ISCX12	15^{th}	{2,3,10,12,13,14,15,16,18,19}	10
ISCX12	17^{th}	{1,4,9,13,14,17,18,19}	8

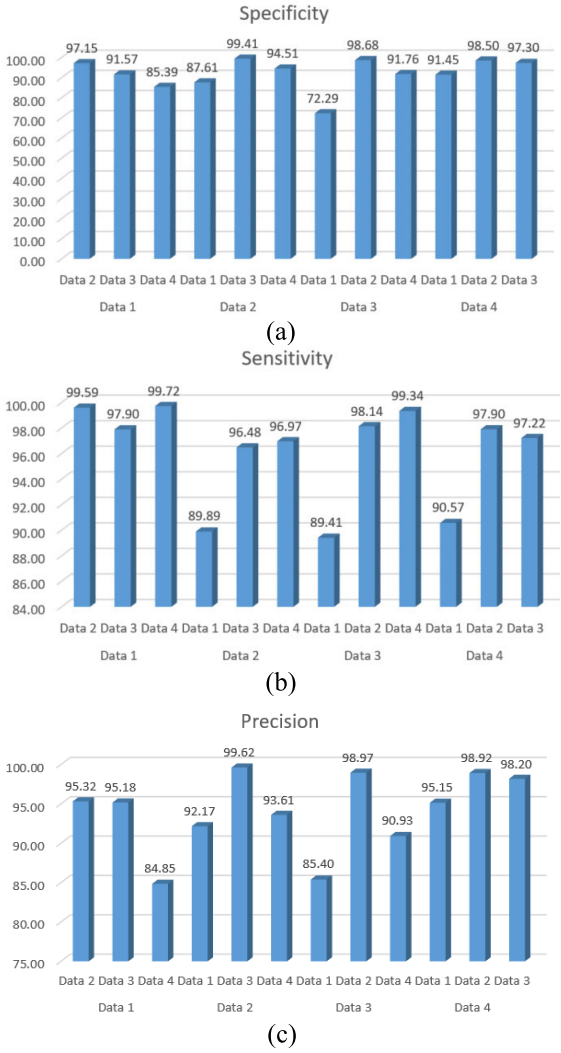

FIGURE 8. Performance in terms of a) sensitivity, b) specificity, and c) precision for running MOB-EBATMLP against the KDD Cup 1999 dataset.

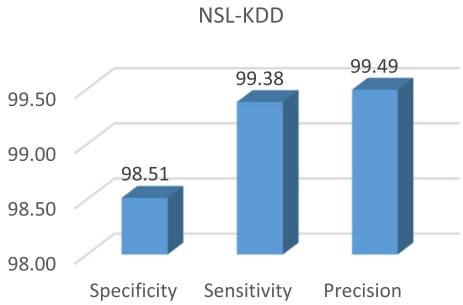

FIGURE 9. Performance in terms of sensitivity, specificity, and precision for running MOB-EBATMLP against the NSL-KDD dataset.

C. ISCX 2012 RESULTS

As previously described, the ISCX 2012 dataset is partitioned into 5. Each relates to a different network traffic day. The features selected for every set are presented in Table 11.

TABLE 12. Classification results when testing against the ISCX 2012 dataset.

Dataset	Date	ACC	DR	FAR
ISCX12	12th	99.76%	99.86%	0.0029
ISCX12	13th	96.09%	95.22%	0.0172
ISCX12	14th	99.92%	99.87%	0.0004
ISCX12	15th	99.99%	100.00%	0.0002
ISCX12	17th	99.96%	99.95%	0.0003
Average		99.14%	98.98%	0.0042

Table 12 itemizes the outcome of the performance averaged against the five sets in the last row. The five results of relative performance in terms of sensitivity, specificity, and precision obtained from the application of the ISCX 201 Dataset against the MOB-EBATMLP approach are shown in Figure 10.

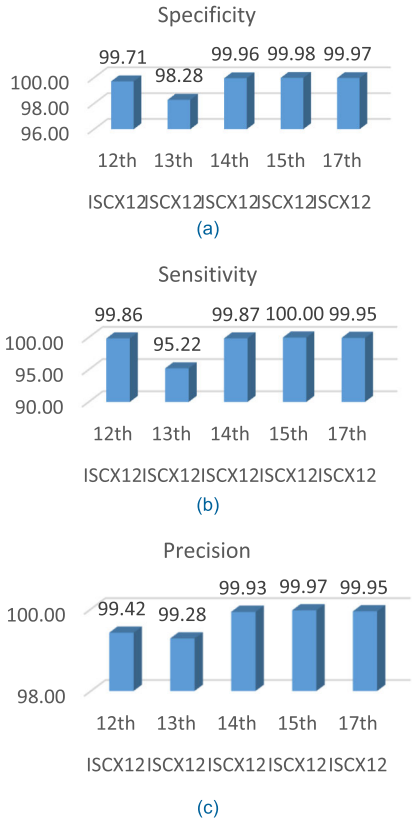

FIGURE 10. Performance in terms of a) sensitivity, b) specificity, and c) precision for running MOB-EBATMLP against the ISCX 2012 dataset.

The above result proves beyond doubts that the proposed method has a very high detection rate of standard attacks across all the datasets, and a good accuracy in detecting all attacks using ISCX2012 datasets. The proposed method has also a very low FAR on all ISCX2012 datasets. Additionally, it has good Precision, Sensitivity, and Specificity as shown in Figure 10.

TABLE 13. Selected features when testing against the UNSW-NB15 dataset.

Dataset	Selected features	Size
UNSW-NB15	{3,6,7,10,16,17,21,27,33,34,35,38,42}	13

TABLE 14. Classification results when testing against the UNSW-NB15 dataset.

Dataset	ACC	DR	FAR
UNSW-NB15	97.63%	98.18%	0.0326

D. UNSW-NB15 RESULTS

The primary purpose of feature selection methods is to identify informative features that improve the intrusion detection rate and accuracy and also decrease the false alarm rate. The MOBBAT algorithm of the proposed wrapper-based method selects the most informative features for EBATMLP-based IDS. The features found as informative for the classification of normal and intrusion data from the UNSW-NB15 dataset are given in Table 13. Table 13 and Table 14 listed the results for UNSW-NB15 dataset. The set of selected features and performance metrics values are shown correspondingly. The performance of the classifier using 13 features defined by the MOBBAT algorithm is listed in Table 14. The proposed method against the recent UNSW-NB15 dataset had the highest accuracy of 97.63%, and it was able to detect the attack with a detection rate of 98.18%. Surprisingly, it had the lowest FAR of 0.033. Figure 11 shows the results of 3 performance measures for each attack in the UNSW-NB15 dataset. The outcome shows that the proposed method with feature selection achieved great results when detecting attacks with 98.18% of sensitivity, 97.99% of precision, and 96.74% of specificity, confirming the efficiency of the method. Through false detection analysis in Table 14, it is possible to notice that most errors are false negatives with nearly zero false positives.

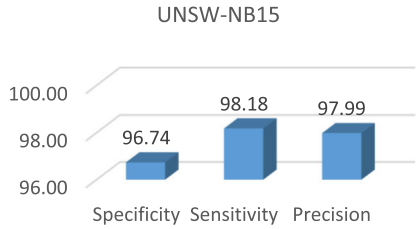

FIGURE 11. Performance in terms of sensitivity, specificity, and precision for running MOB-EBATMLP against the UNSW-NB15 dataset.

E. CICISD 2017 RESULTS

In this section, the proposed model is evaluated using a recent dataset called CICIDS2017 for the purpose of intrusion detection. Tables 15 and 16, as well as Figure 12 summarize

TABLE 15. Selected features when testing against the CICIDS2017 dataset.

Dataset	Selected features	Size
CICIDS2017	{1,2,7,8,9,11,12,13,14,18,19,20,21,22,23 ,24,25,28,36,38,39,40,41,42,53,54,55,63, 65,66,67,73,75,76,77}	35

TABLE 16. Classification results when testing against the CICIDS2017 dataset.

Dataset	ACC	DR	FAR
CICIDS2017	99.23%	99.26%	0.013

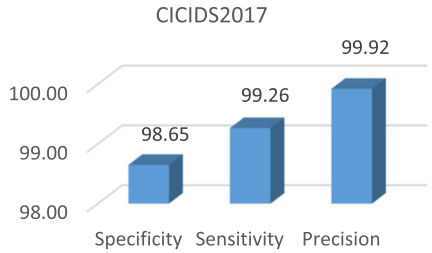

FIGURE 12. Performance in terms of sensitivity, specificity, and precision for running MOB-EBATMLP against the CICIDS2017 dataset.

TABLE 17. Comparison between the EBATMLP and MOB-EBATMLP.

Dataset	EBATMLP			MOB-EBATMLP		
	ACC%	FAR	DR%	ACC%	FAR	DR%
KDD Cup 99	97.08	0.0031	95.34	98.05	0.0285	99.59
NSL-KDD	97.48	0.0215	97.20	99.16	0.015	99.38
ISCX2012	98.62	0.0199	98.89	99.96	0.0003	99.95
UNSW-NB15	96.86	0.0403	97.54	97.63	0.0326	98.18
CICIDS2017	99.07	0.042	98.89	99.23	0.013	99.26
Average	97.82	0.025	97.57	98.80	0.017	99.27

the results of our approach. Table 15 shows the effectiveness of MOBBAT in discovering compact sets of features with a significantly high performance. The methodology presented in Section IV has been applied to obtain a better quality estimate for each solution. Table 15 shows the attributes selected by the MOBBAT algorithm feature selection technique. Only 35 features are selected out of the complete 78 features based on the wrapper method.

Table 16 shows the performance metrics such as accuracy, detection rate, and false alarm rate based on equations (16-18). The results reported by the MOB-EBATMLP approach were similar in quality to the previous dataset, with the MOB-EBATMLP scoring an accuracy of 99.23%, a detection rate of 99.26%, and a false alarm rate of 0.013.

The MOB-EBATMLP develop using a wrapper feature selection method implemented with MOBBAT to maximize the specificity, sensitivity, and sensitivity of the IDS model. Figure 12 shows the performance in terms of testing sensitivity, specificity, and precision metrics. As shown in the figure, the MOB-EBATMLP approach yielded impressive results with the CICIDS2017 dataset.

The results shown in Table 16 and Figure 12 prove the efficiency of the proposed MOBBAT-based feature selection method using a neural network whose performance is optimized by the EBat algorithm to detect network attacks in computer networks. This method detects normal data and data related to network attacks with low FPRs and FNR rates, which is positively reflected in the results shown in Figure 12.

It is deduced from the results in Section V that on account of most datasets, FS leveraging MOBBAT upgrades the EBAT-MLP's performance. With the exception of some ISCX 2012 subsets, the rate of detection rate, rate of false alarm, and values of accuracy are better in the put forward IDS technique with FS.

F. THE ADVANTAGE OF THE MOBBAT FEATURE SELECTOR

The results of assessing the EBATMLP and MOB-EBATMLP approach against the five dataset is given in Table 17. Evaluation relies on the performance that is best obtained by the EBAT-MLP which used all features and MOB-EBATMLP which utilized the features selected.

The detection rate, classification accuracy and false alarm rate are utilized as metrics for measuring the performance. It is noticeable from the outcome that the final approach of MOB-EBATMLP shows a higher classification accuracy and detection rate on all datasets. Also, the MOB-EBATMLP documented the most outstanding results as regards to false alarm rate on; NSL-KDD, ISCX2012, CICIDS2017 and UNSW-NB15, with the exception of KDD Cup 99, in which the EBAT-MLP system is superior.

G. COMPARISON OF THE RESULTS WITH WORKS IN THE LITERATURE

The principal goal of the invention in this study is to construct an IDS technique. The culminating IDS system integrates the EBATMLP classifier along with the MOBBAT feature selector. To estimate the performance of the designed approach, other IDS works from the literature will be compared with the proposed system. Table 18 itemize an outline of the IDS along with the algorithms explored in the framework, the dataset used for benchmarking, the accuracy, detection rate, false alarm rate, the number of the selected feature and the type of FS if applicable. FS was not explored in the majority of works in the literature, also, single dataset was utilized for their benchmarking. The last row elucidates the outcome of the approach put forward. The proposed approach performs best as regards DR, ACC and FAR. Moreover, MOB-EBATMLP showed a noteworthy lower FAR, and a remarkable higher ACC and DR, than studies of the recent works.

Few deductions can be made from the comparative results in Table 18. First, the proposed MOB-EBATMLP system is superior and has an overall performance in the case of almost all datasets. Aside KPCA-DEGSA-HKEL, MOB-EBATMLP had the most remarkable rate of accuracy and detection rates.

TABLE 18. Summary of IDS works with selected features and classification performance.

No.	Reference	Year	Algorithms	NFS	Datasets	ACC	DR	FAR
1	[41]	2020	NNIA	24	NSL-KDD	99.47	N/A	N/A
		2020	NNIA	16	UNSW-NB15	79.81	N/A	N/A
2	[42]	2020	CFS-BA	10	NSL-KDD	99.81	99.8	0.08
3	[43]	2019	FGLCC-CFA	10	KDD CUP 99	95.03	95.23	1.65
4	[44]	2019	DFR	N/A	ISCX 2012	99.41	N/A	N/A
5	[45]	2019	DNN	N/A	KDD CUP 99	93.0	91.4	N/A
				N/A	NSL-KDD	79.4	96.7	N/A
				N/A	UNSW-NB15	78.4	72.5	N/A
6	[46]	2019	DNN	N/A	NSL-KDD	75.9	N/A	N/A
			PCA-DNN	N/A	NSL-KDD	79.3	N/A	N/A
7	[47]	2020	1D-CNN 3L	N/A	UNSW-NB15	91.2	96.17	N/A
			1D-CNN+LSTM	N/A	UNSW-NB15	89.93	95.15	N/A
8	[48]	2020	Sigmoid_PIO	10	KDD CUP 99	94.7	97.4	0.097
			Cosine_PIO	7	KDD CUP 99	96	98.2	0.076
			Sigmoid_PIO	18	NSL-KDD	86.9	81.7	0.064
			Cosine_PIO	5	NSL-KDD	88.3	86.6	0.088
			Sigmoid_PIO	14	UNSW-NB15	91.3	89.7	0.052
			Cosine_PIO	5	UNSW-NB15	91.7	89.4	0.034
9	[49]	2020	MSCNN-LSTM	N/A	UNSW-NB15	89.8	N/A	0.049
10	[50]	2019	ELM50	N/A	ISCX 2012	58.76	N/A	0.513
			MLP50	N/A	ISCX 2012	87.22	N/A	0.145
11	[51]	2020	KPCA-DEGSA-HKEL	N/A	KDD CUP 99	99.00	N/A	0.94
			KPCA-DEGSA-HKEL	N/A	UNSW-NB15	89.01	N/A	2.41
12	[52]	2019	AdaBoost	25	NSL-KDD	99.61	98.90	N/A
			AdaBoost	N/A	ISCX 2012	83	73	N/A
13	[53]	2020	Fast-MCD	N/A	KDD CUP 99	98.61	N/A	0.0169
				N/A	NSL-KDD	91.71	N/A	0.0624
				N/A	UNSW-NB15	91.02	N/A	0.2748
14	[6]	2021	MVO-BAT	24	UNSW-NB15	92.80	N/A	N/A
15	[15]	2021	MFFSEM	N/A	NSL-KDD	84.33	N/A	24.82
			MFFSEM	N/A	UNSW-NB15	88.85	N/A	2.27
			MFFSEM	N/A	KDD CUP 99	92.48	N/A	2.03
			MFFSEM	N/A	CICIDS2017	99.95	N/A	0.013
16	[16]	2021	SVM-GA	N/A	NSL-KDD	99.3	N/A	N/A
17	[17]	2021	FL-NIDS	N/A	NSL-KDD	84.89	N/A	N/A
			FL-NIDS	N/A	UNSW-NB15	87.89	N/A	N/A
18	[18]	2021	DNN	N/A	UNSW-NB15	98.80	97.92	N/A
				N/A	CICIDS2017	97.02	92.80	N/A
19	[38]	2021	DNN	N/A	UNSW-NB15	95.6	97.9	N/A
20	[9]	2021	PSO+DT	N/A	KDD CUP 99	98.6	89.6	1.1
			PSO+KNN	N/A	KDD CUP 99	99.6	96.2	0.4
21	[32]	2021	PCA-DL	N/A	NSL-KDD	92	N/A	N/A
22	[8]	2021	PSO-RF	N/A	UNSW-NB15	75.94	N/A	N/A
			PSO-RF	N/A	KDD CUP 99	97	N/A	N/A
23	[39]	2021	APSO-SVM	N/A	KDD CUP 99	97.69	N/A	N/A
24	[40]	2021	D-ONN	N/A	KDD CUP 99	98	N/A	N/A
25	[33]	2022	B-STACKING	N/A	NSL-KDD	98.5	N/A	N/A
				N/A	CICIDS2017	99.11	N/A	N/A
26	[34]	2022	DS-KELM+MCMIFS	N/A	UNSW-NB15	N/A	94.00	0.041
			DS-KELM+MCMIFS	18	NSL-KDD	N/A	99.53	0.14
			DS-KELM+MCMIFS	18	KDD CUP 99	N/A	99.82	0.15
			DS-KELM+MCMIFS	N/A	CICIDS2017	99	N/A	N/A
27	[35]	2022	RL-NIDS	N/A	NSL-KDD	81.38	N/A	N/A

TABLE 18. *(Continued.)* **Summary of IDS works with selected features and classification performance.**

28	[36]	2022	RANet	N/A	UNSW-NB15	85.36	N/A	N/A
			RANet	N/A	NSL-KDD	87	N/A	N/A
			RANet	N/A	CICIDS2017	96.37	N/A	N/A
29	[37]	2022	LD-EJP	N/A	KDD CUP 99	N/A	96.80	11.40
30	[7]	2022	GA-RF	9	UNSW-NB15	92.06	N/A	1.60
				12	NSL-KDD	96.12	N/A	2.91
31	[54]	2022	QBSA-IELM	30	CICIDS2017	94.55	N/A	N/A
32	Our Proposal		MOB-EBATMLP	17	KDD CUP 99	98.05	99.59	0.0285
				12	NSL-KDD	99.16	99.38	0.0148
				8	ISCX 2012	99.96	99.95	0.0003
				35	CICIDS2017	99.23	99.26	0.013
				13	UNSW-NB15	97.63	98.18	0.0326

Number of Features Selected (NFS), Not Available (N/A), Accuracy (ACC), Detection Rate (DR), False Alarm Rate (FAR)

The designed model also had the best rate of false alarm and detection against the KDD CUP 99 dataset, with the exception of the DS-KELM and MCMIFS model which was superior to all in terms of detection rate of 99.82%. In terms of accuracy, models PSO and KNN and KPCA-DEGSA-HKEL scored the best results are 99.6% and 99%, respectively; the comparison includes 14 models along with the proposed technique. Surpassing over 18 models that utilized the NSL-KDD dataset for assessment, no model accomplished a superior (detection rate and false alarm) than MOB-EBATMLP. Only those models (NNIA, CFS-BA, and AdaBoost) had better accuracy compared to the proposed approach. Similarly, with regards to the ISCX 2012 dataset, MOB-EBATMLP showed the best performance ever. The proposed framework has likewise top execution on account of the new UNSW-NB15 dataset, but the DNN model in ref [18] outperformed the proposed framework only in terms of accuracy with a score of 98.8%. Finally, the proposed framework also has the highest level of implementation at the expense of the new CICIDS2017 dataset, with the exception of the MFFSEM model which beats our framework only in terms of accuracy with a score of 99.95%.

A significant observation from the outcomes is that the designed MOB-EBATMLP is homogeneous with its extraordinary execution on all IDS datasets, dissimilar to different frameworks that may perform better against one dataset however fail to meet expectations on other datasets. In comparison with similar models, this remarkable performance across varied datasets is a powerful attribute for MOB-EBATMLP. It is additionally noticed that there is a moderately small amount of selected features in the presented MOB-EBATMLP compared to other models. Thus, suggesting greater performance as to computational efficiency.

VI. CONCLUSION

This study presents a few points. First, the introduction of MOBBAT, a novel metaheuristic algorithm, constructed on the binary version of the BAT algorithm, for multi-objective FS purpose. Second, the wrapper approach of FS and use of the EBATMLP algorithm employed this algorithm as the wrapper classifier. Third, three goals are utilized as criteria to assess the potential solutions for enhancing the quality of selected features: the number of features, false-positive rate, rate of error. The purpose of selecting an excellent characteristic subset is to feed the NN version that performs the intrusion detection, which is the core purpose of this study. Before explaining how MOB-EBATMLP fits into the bigger picture of the proposed IDS approach, it is worth noting that five benchmark IDS-based datasets were utilized to assess the performance of the final approach, and the outcome was compared with those acquired from works in literature. The outstanding results show the productive results of this study towards delivering a better IDS.

REFERENCES

[1] A. Tchernykh, U. Schwiegelsohn, E.-G. Talbi, and M. Babenko, "Towards understanding uncertainty in cloud computing with risks of confidentiality, integrity, and availability," *J. Comput. Sci.*, vol. 36, Sep. 2019, Art. no. 100581.

[2] T. Alharbi, "Deployment of blockchain technology in software defined networks: A survey," *IEEE Access*, vol. 8, pp. 9146–9156, 2020.

[3] V. S. F. Enigo, K. T. Ganesh, N. N. V. Raj, and D. Sandeep, "Hybrid intrusion detection system for detecting new attacks using machine learning," in *Proc. 5th Int. Conf. Commun. Electron. Syst. (ICCES)*, Jun. 2020, pp. 567–572.

[4] S. A. A. Ghaleb, M. Mohamad, S. A. Fadzli, and W. A. H. M. Ghanem, "Training neural networks by enhance grasshopper optimization algorithm for spam detection system," *IEEE Access*, vol. 9, pp. 116768–116813, 2021.

[5] M. S. Haghighi, F. Farivar, and A. Jolfaei, "A machine learning-based approach to build zero false-positive IPSs for industrial IoT and CPS with a case study on power grids security," *IEEE Trans. Ind. Appl.*, early access, Jul. 23, 2020, doi: 10.1109/TIA.2020.3011397.

[6] O. Almomani, "A hybrid model using bio-inspired metaheuristic algorithms for network intrusion detection system," *Comput., Mater. Continua*, vol. 68, no. 1, pp. 409–429, 2021.

[7] Z. Liu and Y. Shi, "A hybrid IDS using GA-based feature selection method and random forest," *Int. J. Mach. Learn. Comput.*, vol. 12, no. 2, pp. 43–50, 2022.

[8] M. Ajdani and H. Ghaffary, "Introduced a new method for enhancement of intrusion detection with random forest and PSO algorithm," *Secur. Privacy*, vol. 4, no. 2, Mar. 2021, Art. no. e147.

[9] R. O. Ogundokun, J. B. Awotunde, P. Sadiku, E. A. Adeniyi, M. Abiodun, and O. I. Dauda, "An enhanced intrusion detection system using particle swarm optimization feature extraction technique," *Proc. Comput. Sci.*, vol. 193, pp. 504–512, Jan. 2021.

[10] F. H. Almasoudy, W. L. Al-Yaseen, and A. K. Idrees, "Differential evolution wrapper feature selection for intrusion detection system," *Proc. Comput. Sci.*, vol. 167, pp. 1230–1239, Jan. 2020.

[11] W. A. H. M. Ghanem and A. Jantan, "Training a neural network for cyberattack classification applications using hybridization of an artificial bee colony and monarch butterfly optimization," *Neural Process. Lett.*, vol. 51, no. 1, pp. 905–946, Feb. 2020.

[12] S. A. A. Ghaleb, M. Mohamad, S. A. Fadzli, and W. A. H. M. Ghanem, "E-mail spam classification using grasshopper optimization algorithm and neural networks," *Comput., Mater. Continua*, vol. 71, no. 3, pp. 4749–4766, 2022.

[13] S. A. A. Ghaleb, M. Mohamad, E. F. H. S. Abdullah, and W. A. H. M. Ghanem, "An integrated model to email spam classification using an enhanced grasshopper optimization algorithm to train a multilayer perceptron neural network," in *Proc. Int. Conf. Adv. Cyber Secur.* Singapore: Springer, 2020, pp. 402–419.

[14] W. A. H. M. Ghanem and A. Jantan, "A cognitively inspired hybridization of artificial bee colony and dragonfly algorithms for training multi-layer perceptrons," *Cogn. Comput.*, vol. 10, no. 6, pp. 1096–1134, Dec. 2018.

[15] H. Zhang, J.-L. Li, X.-M. Liu, and C. Dong, "Multi-dimensional feature fusion and stacking ensemble mechanism for network intrusion detection," *Future Gener. Comput. Syst.*, vol. 122, pp. 130–143, Sep. 2021.

[16] A. Aldallal and F. Alisa, "Effective intrusion detection system to secure data in cloud using machine learning," *Symmetry*, vol. 13, no. 12, p. 2306, Dec. 2021.

[17] M. Mulyanto, M. Faisal, S. W. Prakosa, and J.-S. Leu, "Effectiveness of focal loss for minority classification in network intrusion detection systems," *Symmetry*, vol. 13, no. 1, p. 4, Dec. 2020.

[18] I. Jamal and F. Jamil, "An ensemble of prediction and learning mechanism for improving accuracy of anomaly detection in network intrusion environments," *Sustainability*, vol. 13, no. 18, p. 10057, 2021.

[19] S. A. A. Ghaleb, M. Mohamad, E. F. H. S. Abdullah, and W. A. H. M. Ghanem, "Spam classification based on supervised learning using grasshopper optimization algorithm and artificial neural network," in *Proc. Int. Conf. Adv. Cyber Secur.* Singapore: Springer, 2020, pp. 420–434.

[20] W. A. H. M. Ghanem and A. Jantan, "A new approach for intrusion detection system based on training multilayer perceptron by using enhanced bat algorithm," *Neural Comput. Appl.*, vol. 32, no. 15, pp. 11665–11698, Aug. 2020.

[21] W. A. H. M. Ghanem, Y. A. B. El-Ebiary, M. Abdulnab, M. Tubishat, N. A. M. Alduais, A. B. Nasser, N. Abdullah, and O. A. Al-Wesabi, "Metaheuristic based IDS using multi-objective wrapper feature selection and neural network classification," in *Proc. Int. Conf. Adv. Cyber Secur.* Singapore: Springer, 2020, pp. 384–401.

[22] W. A. H. M. Ghanem and A. Jantan, "An enhanced bat algorithm with mutation operator for numerical optimization problems," *Neural Comput. Appl.*, vol. 31, no. S1, pp. 617–651, Jan. 2019.

[23] S. A. A. Ghaleb, M. Mohamad, E. F. H. S. Abdullah, and W. A. H. M. Ghanem, "Integrating mutation operator into grasshopper optimization algorithm for global optimization," *Soft Comput.*, vol. 25, no. 13, pp. 8281–8324, Jul. 2021.

[24] V. K. Ojha, A. Abraham, and V. Snášel, "Metaheuristic design of feedforward neural networks: A review of two decades of research," *Eng. Appl. Artif. Intell.*, vol. 60, pp. 97–116, Apr. 2017.

[25] W. A. H. M. Ghanem, A. Jantan, S. A. A. Ghaleb, and A. B. Nasser, "An efficient intrusion detection model based on hybridization of artificial bee colony and dragonfly algorithms for training multilayer perceptrons," *IEEE Access*, vol. 8, pp. 130452–130475, 2020.

[26] W. A. H. M. Ghanem and A. Jantan, "Novel multi-objective artificial bee colony optimization for wrapper based feature selection in intrusion detection," *Int. J. Adv. Soft Comput. Appl.*, vol. 8, no. 1, pp. 70–81, 2016.

[27] V. S. Kumar, P. V. N. Rajeswari, and M. Susmitha, "A multi-objective hyper-heuristic improved particle swarm optimization based configuration of SVM for big data cyber security," *Eur. J. Mol. Clin. Med.*, vol. 7, no. 11, pp. 7552–7560, 2021.

[28] X.-S. Yang, "A new metaheuristic bat-inspired algorithm," in *Nature Inspired Cooperative Strategies for Optimization (NICSO 2010)*. Berlin, Germany: Springer, 2010, pp. 65–74.

[29] A. Saad, S. A. Khan, and A. Mahmood, "A multi-objective evolutionary artificial bee colony algorithm for optimizing network topology design," *Swarm Evol. Comput.*, vol. 38, pp. 187–201, Feb. 2018.

[30] X.-S. Yang, "Bat algorithm for multi-objective optimisation," *Int. J. Bio-Inspired Comput.*, vol. 3, no. 5, pp. 267–274, 2011.

[31] E.-G. Talbi, "A unified taxonomy of hybrid metaheuristics with mathematical programming, constraint programming and machine learning," in *Hybrid Metaheuristics*. Berlin, Germany: Springer, 2013, pp. 3–76.

[32] H. Rajadurai and U. D. Gandhi, "An empirical model in intrusion detection systems using principal component analysis and deep learning models," *Comput. Intell.*, vol. 37, no. 3, pp. 1111–1124, Aug. 2021.

[33] S. Roy, J. Li, B.-J. Choi, and Y. Bai, "A lightweight supervised intrusion detection mechanism for IoT networks," *Future Gener. Comput. Syst.*, vol. 127, pp. 276–285, Feb. 2022.

[34] S. Gavel, A. S. Raghuvanshi, and S. Tiwari, "Maximum correlation based mutual information scheme for intrusion detection in the data networks," *Expert Syst. Appl.*, vol. 189, Mar. 2022, Art. no. 116089.

[35] W. Wang, S. Jian, Y. Tan, Q. Wu, and C. Huang, "Representation learning-based network intrusion detection system by capturing explicit and implicit feature interactions," *Comput. Secur.*, vol. 112, Jan. 2022, Art. no. 102537.

[36] X. Zhang, F. Yang, Y. Hu, Z. Tian, W. Liu, Y. Li, and W. She, "RANet: Network intrusion detection with group-gating convolutional neural network," *J. Netw. Comput. Appl.*, vol. 198, Feb. 2022, Art. no. 103266.

[37] W. Wang, X. Hu, and Y. Du, "Algorithm optimization and anomaly detection simulation based on extended jarvis-patrick clustering and outlier detection," *Alexandria Eng. J.*, vol. 61, no. 3, pp. 2106–2115, Mar. 2022.

[38] L. Ashiku and C. Dagli, "Network intrusion detection system using deep learning," *Proc. Comput. Sci.*, vol. 185, pp. 239–247, 2021.

[39] Y. Luo, "Research on network security intrusion detection system based on machine learning," *Int. J. Netw. Secur.*, vol. 23, no. 3, pp. 490–495, 2021.

[40] M. Ramaiah, V. Chandrasekaran, V. Ravi, and N. Kumar, "An intrusion detection system using optimized deep neural network architecture," *Trans. Emerg. Telecommun. Technol.*, vol. 32, no. 4, Apr. 2021, Art. no. e4221.

[41] W. Wei, S. Chen, Q. Lin, J. Ji, and J. Chen, "A multi-objective immune algorithm for intrusion feature selection," *Appl. Soft Comput.*, vol. 95, Oct. 2020, Art. no. 106522.

[42] Y. Zhou, G. Cheng, S. Jiang, and M. Dai, "Building an efficient intrusion detection system based on feature selection and ensemble classifier," *Comput. Netw.*, vol. 174, Jun. 2020, Art. no. 107247.

[43] S. Mohammadi, H. Mirvaziri, M. Ghazizadeh-Ahsaee, and H. Karimipour, "Cyber intrusion detection by combined feature selection algorithm," *J. Inf. Secur. Appl.*, vol. 44, pp. 80–88, Feb. 2019.

[44] Y. Zeng, H. Gu, W. Wei, and Y. Guo, "Deep-full-range: A deep learning based network encrypted traffic classification and intrusion detection framework," *IEEE Access*, vol. 7, pp. 45182–45190, 2019.

[45] R. Vinayakumar, M. Alazab, K. Soman, P. Poornachandran, A. Al-Nemrat, and S. Venkatraman, "Deep learning approach for intelligent intrusion detection system," *IEEE Access*, vol. 7, pp. 41525–41550, 2019.

[46] S. Rawat, A. Srinivasan, and R. Vinayakumar, "Intrusion detection systems using classical machine learning techniques versus integrated unsupervised feature learning and deep neural network," 2019, *arXiv:1910.01114*.

[47] M. Azizjon, A. Jumabek, and W. Kim, "1D CNN based network intrusion detection with normalization on imbalanced data," in *Proc. Int. Conf. Artif. Intell. Inf. Commun. (ICAIIC)*, Feb. 2020, pp. 218–224.

[48] H. Alazzam, A. Sharieh, and K. E. Sabri, "A feature selection algorithm for intrusion detection system based on pigeon inspired optimizer," *Expert Syst. Appl.*, vol. 148, Jun. 2020, Art. no. 113249.

[49] J. Zhang, Y. Ling, X. Fu, X. Yang, G. Xiong, and R. Zhang, "Model of the intrusion detection system based on the integration of spatial-temporal features," *Comput. Secur.*, vol. 89, Feb. 2020, Art. no. 101681.

[50] M. Monshizadeh, V. Khatri, B. G. Atli, R. Kantola, and Z. Yan, "Performance evaluation of a combined anomaly detection platform," *IEEE Access*, vol. 7, pp. 100964–100978, 2019.

[51] L. Lv, W. Wang, Z. Zhang, and X. Liu, "A novel intrusion detection system based on an optimal hybrid kernel extreme learning machine," *Knowl.-Based Syst.*, vol. 195, May 2020, Art. no. 105648.

[52] M. Mazini, B. Shirazi, and I. Mahdavi, "Anomaly network-based intrusion detection system using a reliable hybrid artificial bee colony and AdaBoost algorithms," *J. King Saud Univ., Comput. Inf. Sci.*, vol. 31, no. 4, pp. 541–553, Oct. 2019.

[53] M. Ahsan, M. Mashuri, M. H. Lee, H. Kuswanto, and D. D. Prastyo, "Robust adaptive multivariate Hotelling's T2 control chart based on kernel density estimation for intrusion detection system," *Expert Syst. Appl.*, vol. 145, May 2020, Art. no. 113105.

[54] Y. Dong, W. Hu, J. Zhang, M. Chen, W. Liao, and Z. Chen, "Quantum beetle swarm algorithm optimized extreme learning machine for intrusion detection," *Quantum Inf. Process.*, vol. 21, no. 1, pp. 1–26, Jan. 2022.

[55] W. Lee and S. J. Stolfo, "A framework for constructing features and models for intrusion detection systems," *ACM Trans. Inf. Syst. Secur.*, vol. 3, no. 4, pp. 227–261, Nov. 2000.
[56] D. S. Terzi, R. Terzi, and S. Sagiroglu, "Big data analytics for network anomaly detection from netflow data," in *Proc. Int. Conf. Comput. Sci. Eng. (UBMK)*, Oct. 2017, pp. 592–597.
[57] A. Zainal, M. A. Maarof, and S. M. Shamsuddin, "Feature selection using rough-DPSO in anomaly intrusion detection," in *Proc. Int. Conf. Comput. Sci. Appl.* Berlin, Germany: Springer, 2007, pp. 512–524.
[58] L. M. Ibrahim, D. T. Basheer, and M. S. Mahmod, "A comparison study for intrusion database (KDD99, NSL-KDD) based on self-organization map (SOM) artificial neural network," *J. Eng. Sci. Technol.*, vol. 8, no. 1, pp. 107–119, 2013.
[59] A. Shiravi, H. Shiravi, M. Tavallaee, and A. A. Ghorbani, "Toward developing a systematic approach to generate benchmark datasets for intrusion detection," *Comput. Secur.*, vol. 31, no. 3, pp. 357–374, May 2012.
[60] N. Moustafa and J. Slay, "UNSW-NB15: A comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set)," in *Proc. Mil. Commun. Inf. Syst. Conf. (MilCIS)*, Nov. 2015, pp. 1–6.
[61] N. Moustafa and J. Slay, "The significant features of the UNSW-NB15 and the KDD99 data sets for network intrusion detection systems," in *Proc. 4th Int. Workshop Building Anal. Datasets Gathering Exper. Returns Secur. (BADGERS)*, Nov. 2015, pp. 25–31.
[62] I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, "Toward generating a new intrusion detection dataset and intrusion traffic characterization," in *Proc. ICISSP* vol. 1, 2018, pp. 108–116.
[63] A. H. Lashkari, G. D. Gil, M. S. I. Mamun, and A. A. Ghorbani, "Characterization of tor traffic using time based features," in *Proc. ICISSP*, 2017, pp. 253–262.

WAHEED ALI H. M. GHANEM received the B.Sc. degree in computer sciences and engineering from Aden University, Yemen, in 2003, and the M.Sc. degree in computer science and the Ph.D. degree in network and communication protocols from the Universiti Sains Malaysia, in 2013 and 2019, respectively. His research interests include computer and network security, cybersecurity, machine learning, artificial intelligence, swarm intelligence, optimization algorithm, and information technology.

SANAA ABDULJABBAR AHMED GHALEB received the bachelor's degree from Aden University, Yemen, in 2011, the master's degree from Universiti Sains Malaysia, Malaysia, in 2017, and the Ph.D. degree in computer science from Universiti Sultan Zainal Abidin, Malaysia, in 2022. Her general research interests include technology-enhanced learning and instructional design and technology. Her research interests include computer and network security, cybersecurity, machine learning, artificial intelligence, swarm intelligence, and optimization algorithm.

AMAN JANTAN is currently an Associate Professor with the School of Computer Sciences, Universiti Sains Malaysia, Malaysia. He has published more than 100 articles in reputed journals. His research interests include digital forensics, artificial intelligence, malware, intrusion detection systems, computer security, cryptography, and computer and network security. He received national and international recognition for some of his work.

ABDULLAH B. NASSER (Member, IEEE) received the B.Sc. degree from Hodeidah University, Yemen, in 2006, the M.Sc. degree from the Universiti Sains Malaysia, Malaysia, in 2014, and the Ph.D. degree from Universiti Malaysia Pahang, Malaysia, in 2018, all in computer science. He is currently an Assistant Professor with the Faculty of Computing, Universiti Malaysia Pahang. He is the author of many scientific papers published in renowned journals and conferences. His research interests include software testing and soft computing, specifically, the use of artificial intelligence methods (metaheuristic algorithms) for solving different software engineering problems.

SAMI ABDULLA MOHSEN SALEH received the B.Eng. degree in computer engineering from Hodeidah University, Yemen, in 2005, and the M.Sc. degree in electronic systems design engineering and the Ph.D. degree in computer vision and machine learning from the Universiti Sains Malaysia, in 2013 and 2022, respectively. He worked as a Researcher with the Intelligent Biometric Group, School of Electrical and Electronic Engineering, Universiti Sains Malaysia. He is currently working as a Researcher with the Aerial Vehicle and Surveillance System Research Group, Aerospace Engineering School. His research interests include computer vision, deep learning, swarm intelligence, and soft biometrics. He has served as a Reviewer for several well-known conferences and international journals, such as *Pattern Recognition Letter Journal*.

AMIR NGAH received the Ph.D. degree from Durham University, U.K., in 2012. He is currently an Associate Professor with the Faculty of Ocean Engineering Technology and Informatics, Universiti Malaysia Terengganu. He has published more than 20 research papers at various refereed journals, conferences, seminars, and symposiums. His research interest includes on software engineering field, specifically in software testing, regression testing, software changes, software maintenance, software metrics, program analysis, and program slicing. He is also interested in AI and machine learning to assist in research in software engineering.

ARIFAH CHE ALHADI received the M.Sc. degree in information science from Universiti Kebangsaan Malaysia, in 2005, and the Ph.D. degree in computer science from Universiti Malaysia Terengganu. She is currently a Senior Lecturer with the Faculty of Ocean Engineering and Informatics, Universiti Malaysia Terengganu. Her research interests include information systems and information retrieval. She has published articles in journals and proceedings in these areas. She received national and international recognition for some of her work.

HUMAIRA ARSHAD received the master's degree in information technology from the National University of Science and Technology (NUST), Pakistan, and the Ph.D. degree from the School of Computer Science, Universiti Sains Malaysia. She joined the Faculty of Computer Sciences and IT, in 2004. She is currently an Associate Professor with the Department of Computer Sciences and IT, Islamia University of Bahawalpur, Pakistan. Her research interests include digital and social media forensics, information security, online social networks, cybersecurity, intrusion detection, reverse engineering, and semantic web.

ABDUL-MALIK H. Y. SAAD (Senior Member, IEEE) was born in Jeddah, Saudi Arabia, in 1983. He received the B.Sc. degree in computer engineering from Hodeidah University, Hodeidah, Yemen, in 2006, and the M.Sc. degree in electronic systems design engineering and the Ph.D. degree in digital systems from Universiti Sains Malaysia (USM), in 2014 and 2018, respectively. He is currently a Senior Lecturer with the Faculty of Engineering, School of Electrical Engineering, Universiti Teknologi Malaysia. His research interests include digital and embedded systems design, image processing, and AI.

ABIODUN ESTHER OMOLARA received the Ph.D. degree from the School of Computer Sciences, Universiti Sains Malaysia. Her research interests include computer and network security, cyber-security, cryptography, artificial intelligence, natural language processing, network and communication protocol, forensics, and IoT security.

YOUSEF A. BAKER EL-EBIARY (Member, IEEE) received the bachelor's degree in software engineering, the two master's degrees in IT and business administration, and the Ph.D. degree in MIS. He is currently working at the Faculty of Informatics and Computing (FIK), Universiti Sultan Zainal Abidin (UNISZA), Malaysia, as a Senior Lecturer and a member of several committees. He is also working as a part-time Senior Lecturer at MEDIU University and SSM College, Switzerland. He is also a Senior Fellow Researcher at AIU University, Malaysia. Moreover, he is an Academic Consultant for the Ph.D. degree in MIS Program, Geomatika University College, Malaysia. He is assigned as a Technical Advisor at the Academic Exchange Information Centre (AEIC), China, and a Board Member of the Gyancity Research Laboratory for research and development, India. He has over 11 years of experience in teaching, supervision, and administrative work in the education sector. He held many positions such as the Dean of student affairs, a Faculty's Deputy for postgraduate and scientific research, and a Deputy for scientific research deanship. He has experience in scientific publication and international conferences participating in more than 70 international conferences with a good enough number of indexed research papers (WoS "ISI" and Scopus) and around 150 published. He received a good number of awards from international exhibitions and competitions, and has acquired ntellectual property. He is a member of many related associations such as IAENG, ACSE, and IACSIT.

OLUDARE ISAAC ABIODUN received the Ph.D. degree in nuclear and radiation physics from the Nigerian Defence Academy, Kaduna. He also received the second Ph.D. degree in computer science, with a specialization in security and digital forensics from Universiti Sains Malaysia, Penang, Malaysia. His research interests include artificial intelligence, robotics, cybersecurity, digital forensics, nuclear security, terrorism, national security, and IoT security.