



A novel AI-driven intrusion detection framework for cloud-IoT sensor networks

Maryam Mahdi Alhusseini^{a,*}, Inam Abdullah Lafta^a, Fatima Faydhe Al-Azzaw^b, Fadhil Abbas Fadhil^c, Mohammad-Reza Feizi-Derakhshi^{d,*}, Azhar Naji Alyahya^e, Zaid Ameen Abduljabbar^{f,g}, Vincent Omollo Nyangaresi^{h,i}

^a Information and Communication Technology Department, Polytechnic College of Engineering – Baghdad, Middle Technical University, Baghdad, 10011, Iraq

^b Electronics Engineering and AI Technologies Department, Polytechnic College of Engineering – Baghdad, Middle Technical University, Baghdad, 10011, Iraq

^c College of Computer Science, University of Technology- Iraq, Baghdad, 10066, Iraq

^d Department of Computer Engineering, University of Tabriz, Tabriz, 5166616471, Iran

^e Department of Software Engineering, Sakarya University, Sakarya, 54050, Türkiye

^f Department of Computer Science, College of Education for Pure Sciences, University of Basrah, Basrah, 61004, Iraq

^g Shenzhen Institute, Huazhong University of Science and Technology, Shenzhen, 518000, China

^h Department of Computer Science and Software Engineering, Jaramogi Oginga Odinga University of Science & Technology, Bondo, 40601, Kenya

ⁱ Department of Applied Electronics, Saveetha Institute of Medical and Technical Sciences (SIMATS), Chennai, 602105, India

ARTICLE INFO

Publishing editor: Xin Huang

Keywords:

Cloud computing
Feature selection (FS) strategy
Internet of things (IoT)
Intelligent network intrusion detection system (NIDS)
Network detection
Novel optimization
Sampling technique
Wireless sensor network (WSN)

ABSTRACT

Securing network infrastructure against cyberattacks is essential in rapidly evolving digital landscapes. This paper proposes an AI-based real-time intrusion detection system (IDS) for wireless sensor network (WSN), cloud computing (CC), and Internet of things (IoT) environments. The framework employs classical machine learning (ML) models, including decision trees (DTs), K-nearest neighbors (KNN), and logistic regression, optimized using the energy valley optimization (EVO) algorithm on the Network Security Laboratory – Knowledge Discovery in Databases (NSL-KDD) dataset. Feature selection (FS) reduced the number of input features from 42 to 18 without compromising the detection performance. The system achieved high accuracy rates of 98.95% with a decision tree, 98.47% with KNN, and 88.84% with logistic regression, along with high precision, recall, and F1-scores. In addition, the training and testing times were significantly reduced, supporting real-time deployment. Class imbalance was addressed through downsampling to ensure balanced detection across attack types. The proposed model offers a scalable, low-latency, and accurate intrusion detection solution aligned with modern cybersecurity requirements.

* Corresponding author.

E-mail addresses: mariammahdi@mtu.edu.iq (M.M. Alhusseini), inamabdullah96@mtu.edu.iq (I.A. Lafta), fatima_faydy1981@mtu.edu.iq (F.F. Al-Azzaw), fadhil.a.fadhil@uotechnology.edu.iq (F.A. Fadhil), mfeizi@tabrizu.ac.ir (M.-R. Feizi-Derakhshi), azhar.alyahya@ogr.sakarya.edu.tr (A.N. Alyahya), zaid.ameen@uobasrah.edu.iq (Z.A. Abduljabbar), vnyangaresi@jooust.ac.ke (V.O. Nyangaresi).

<https://doi.org/10.1016/j.jnlest.2026.100375>

Received 25 December 2025; Received in revised form 24 July 2026; Accepted 23 August 2026; Available online 18 September 2026.
1674-862X/© 2026 The Authors. Publishing Services provided by Elsevier B.V. on behalf of KeAi Communications Co. Ltd. This is an open access article under the CC BY license (<http://creativecommons.org/licenses/by/4.0/>).

1 Introduction

This article addresses the pressing need to enhance network intrusion detection system (NIDS) within the domains of wireless sensor network (WSN), cloud computing (CC), and the Internet of things (IoT). Integrating cloud technology with wired and WSNs is crucial for various applications including transportation, warfare, education, healthcare, and agriculture, as shown in Fig. 1. The primary problem is the detection of intrusions with high accuracy while minimizing false positives. Conventional intrusion detection system (IDS) often suffers from high false-positive rates, leading to inefficient resource utilization and potentially overlooking genuine threats. Thus, the central aim of this study is to propose a novel hybrid IDS model that leverages cutting-edge methodologies to achieve superior detection accuracy and reduce false positives (FPs). Recent studies have emphasized the role of optimized feature selection (FS) in IDS, employing metaheuristic approaches such as the black hole algorithm combined with extreme gradient boosting (XGBoost) to significantly enhance the detection performance on the Aegean Wi-Fi Intrusion Dataset 3 (AWID3) dataset [1]. The Network Security Laboratory – Knowledge Discovery in Databases (NSL-KDD) dataset serves as a standard for evaluating IDS. These findings underscore the significance of FS in the development of successful IDS [2].

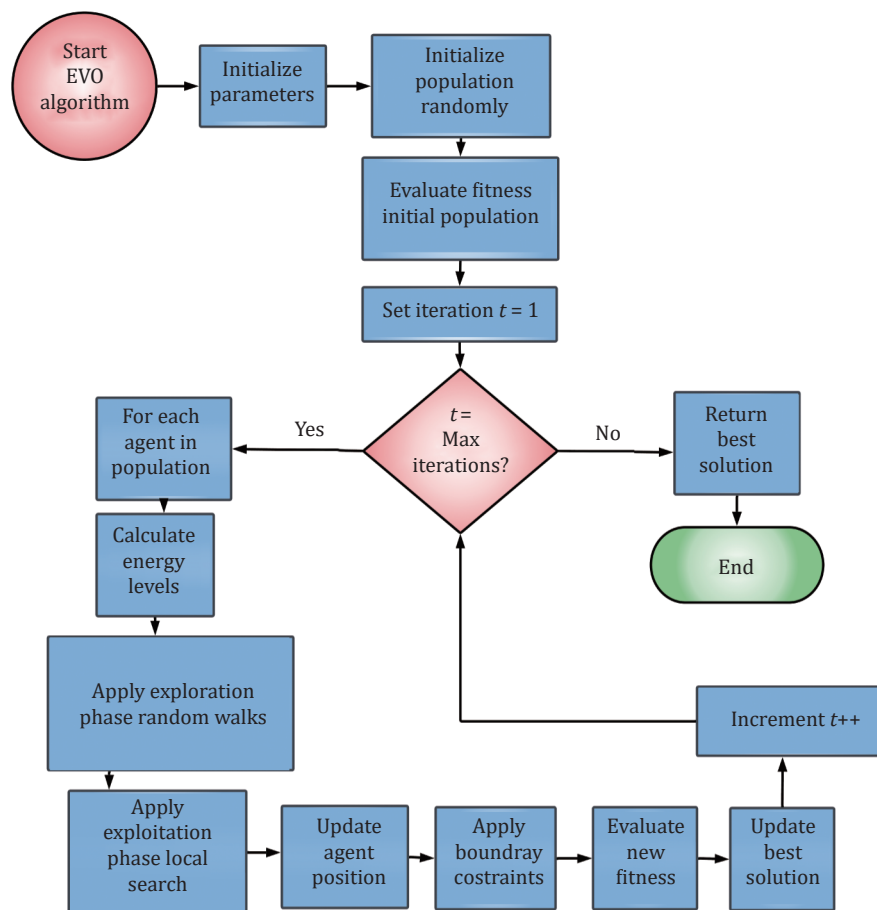


Fig. 1. Flowchart of EVO .

The FS method plays a crucial role in improving intrusion detection performance, where modern approaches employ techniques such as XGBoost-based FS to enhance accuracy and manage class imbalance in high-dimensional cybersecurity data [3]. Ref. [4] presented a hybrid intrusion detection method that utilizes correlation-based feature selection with differential evolution (CFS-DE). They employed CFS-DE to identify the optimal feature set for dimensionality reduction.

Evolutionary algorithms enhance problem-solving across various domains. The forest optimization algorithm (FOA) was initially developed for continuous search but has been adapted for discrete search in FS [3]. Recent literature emphasizes the application of chaos-based adaptive S-box-based methods, including Carlisle Adams and Stafford Tavares 128-bit (CAST-128) encryption with a logistic sine map, to enhance lightweight data protection against cryptography attacks in an IoT and WSN setup [5]. Recent secure data embedding methods, such as oriented FAST and rotated BRIEF (ORB) combined with ChaCha20, ensure protected transmission with minimal distortion, supporting IDSs in maintaining data security [6]. WSNs and CC are vulnerable to security threats and attacks. To ensure security, an effective IDS must be in place to detect these attacks [7]. Traditional IDSs are less effective as these malicious attacks become more intelligent, frequent, and complex, particularly in large detection datasets. IDSs are critical for safeguarding CC and WSNs [8].

Recent studies have focused on lightweight, privacy-preserving IoT, and WSN-cloud communication based on the QR code-based scheme, lightweight, and randomized least significant bit (LSB), and cryptographic hashing, which can be combined with AI-led IDS structures to augment confidentiality and authentication without extra equipment expenses. IDSs are essential to alleviate these risks [8]. Enhanced surveillance schemes, including optical fiber sensors (OFSS), in conjunction with machine learning (ML)- and energy valley optimizer (EVO)-based IDS, enhance the accuracy of anomaly detection by successful monitoring and FS.

To address these challenges, this study proposes employing a unique FS method, specifically the energy valley FS algorithm, to analyze substantial volumes of potential intrusion data. To assess our novel approach, it was evaluated on an IDS platform, a sophisticated system employing ML techniques, and applied to actual large-scale intrusion data, NSL-KDD.

We proposed an optimized approach for detecting malicious packets by integrating metaheuristic algorithms into an IDS. The proposed algorithm aims to improve the accuracy and precision while reducing the space and time complexity by integrating metaheuristic algorithms with existing ML classifier techniques. The experimental results demonstrate that this hybrid approach outperforms the existing classifiers, making it a promising solution for IDS optimization.

In the preliminary stage of our methodology, a novel EVO algorithm [9] was employed to generate an optimal FS. This FS method significantly enhances the capacity of the system to accurately represent data and improves the precision of intrusion detection.

During the second phase, three unique ML models, namely, logistic regression (LogReg), decision tree (DT), and *K*-nearest neighbors (KNN), were employed to attain comprehensive and efficient intrusion detection using data enhanced by our proposed methodology.

The IDS was evaluated by rigorous tests on real-world NSL-KDD datasets across various scenarios, with six experiments executed. The system performance is evaluated based on the detection accuracy, precision, sensitivity, false positive rates (FPRs), and computational efficiency.

This study pioneers the use of EVO for FS within the area of intrusion detection, achieving a significant reduction in the number of features, improved detection performance, and real-time operational requirements relevant to networked and embedded systems.

The key contributions are as follows: i) The introduction of the first approach of EVO for efficient FS, reducing the features of the NSL-KDD dataset from 42 to 18 while improving the detection performance; ii) The optimization of ML models LogReg, DT, and KNN for real-time intrusion detection in networked environments; iii) A comparative evaluation of the proposed method against existing methods based on accuracy, precision, recall, and F1-score; iv) The demonstration of real-time feasibility with low training and testing times suitable for embedded and communication systems; v) The dataset was balanced using downsampling techniques, ensuring fair and reliable detection across both majority and minority attack classes; vi) Improving cybersecurity in WSN, IoT, and CC environments.

This investigation pioneered the use of EVO as an FS strategy in intrusion detection, achieving significant feature reduction, improved detection performance, and real-time operational efficiency, specifically tailored for networked wired and wireless environments.

2 Methodology

ML methods combined with EVO for FS aim to create a balanced dataset, leading to enhanced intrusion detection for WSNs and CC.

2.1 Experimental environment and system configuration

This section presents the computing performance and resource consumption of the proposed models on the NSL-KDD penetration-testing dataset. Tests were conducted with the same system settings to ensure fair evaluation and reproducible results. The tests were performed on the Google Colab Pro platform using an 11th-generation Intel Core i5-1135G7 processor (2.40 GHz, 8 cores) and 12 GB of RAM, running Windows 11 Home 64-bit (version 10.0, build 26100). The model was trained on the Google Colab platform (Python Pro 3 environment) with 1.3/12.7 GB of RAM, using the scikit-learn 1.6.1, NumPy 2.0.2, and SHAP 0.48.0 libraries. Connected to the host runtime: v2-8 TPU. All tests were run with GPU acceleration, whenever possible.

2.2 Recent study of EVO

EVO is an innovative metaheuristic algorithm derived from sophisticated physical concepts. The objective is to enhance the alignment between conceptual and mathematical models, focusing on the particle stability of the neutron and proton ratios [9]. Advanced monitoring methods such as OFSS, recognized for their exceptional sensitivity and accuracy, underscore the significance of precision in anomaly detection. Similarly, IDS employing ML and EVO leverages efficient monitoring and FS to improve cybersecurity. EVO incorporates a dynamic configuration for exploration and exploitation by employing three novel position vectors throughout its search process. The intricacy, along with its mathematical underpinnings, establishes EVO as a potential instrument for optimization tasks, especially in high-dimensional datasets [9].

2.2.1 Mathematical formulation of EVO

This algorithm simulates the process through which unstable particles attempt to reach a stable state by adjusting their neutron-to-proton ratio (N/Z). In nature, unstable particles emit energy and decay into more stable forms, often through alpha, beta, or gamma decay, depending on their instability level. The EVO models this behavior, where solution candidates (particles) in a search space strive to move toward an optimal solution (stability) by adjusting their parameters [9]. The fundamental concept of EVO is that each particle inside the search space signifies a potential solution with the objective of identifying the most stable (optimal) solution through the iterative evolution of the particles. Each particle modifies its stability through multiple phases, including enrichment and decay processes, analogous to natural physical processes, as shown in Fig. 1 [9]. The subsequent equations dictate the location updates of the particles in the EVO algorithm.

$$X_{i\text{NEW}1} = X_i (X_{\text{BS}} (X'_{ti})) \quad (1)$$

where $X_{i\text{NEW}1}$ represents the new position of the i -th particle after the first update or decay process, and X_{BS} represents the best stability (position/stability information of the best particle found to date). X'_{ti} represents a randomly generated value that controls the degree of positional adjustment of particle i during the alpha-decay process.

Equation (1) describes the alpha-decay process, where a new position for the i -th particle is generated based on the best particle X_{BS} and the current position of the particle X_i . The random value X'_{ti} controls the degree of adjustment, allowing the particle to move toward the best solution through minor positional changes

$$X_{i\text{NEW}2} = X_i (X_{\text{NG}} (X'_{ti})) \quad (2)$$

where X_{NG} describes the neighbor (the position of a neighboring particle used to guide the update).

Equation (2) describes the gamma-decay process, in which the particle's position is updated based on X_{NG} , which represents information obtained from another particle in the population. This process encourages information sharing among particles and facilitates convergence toward the optimal solution

$$X_{i\text{NEW}1} = X_i + (\tau_1 X_{\text{BS}} - \tau_2 X_{\text{CP}}) / \text{SL}_i \quad (3)$$

where X_{CP} denotes the center point of the population, and describes the current particle (current particle/solution position), X_i represents the current position of the i -th particle, and n is the total number of particles, while τ_1 and τ_2 are the weight factors that control the impact of the best particle and the current particles (X_{CP}), respectively.

Equation (3) models the beta-decay process, in which a new position is generated based on both the best particle X_{BS} , and the current particles X_{CP} . The stability level SL_i determines the magnitude of the particle's adjustment, such that a more unstable particle undergoes a larger positional change, reflecting the tendency of particles to move toward greater stability.

$$X_{i\text{NEW2}} = X_i + (\tau_3 X_{BS} - \tau_4 X_{NG}) \quad (4)$$

Equation (4) describes another beta-decay process, in which the position of a particle is updated based on the best particle X_{BS} and the new gravitational point X_{NG} . X_{BS} denotes the position of the best particle found so far, while X_{NG} represents the new gravitational point. The weighting factors τ_3 and τ_4 control the contributions of the best particle and the new gravitational point, respectively, promoting information sharing and exploration within the population.

2.2.2 Cost function in EVO

The objective function (cost function) utilized in EVO is contingent on the optimization problem. In the context of IDS, the cost function is generally developed based on the classification accuracy, F1-score, or weighted amalgamation of many performance measures.

$$\text{Cost function} = w_1(1 - \text{Accuracy}) + w_2\text{FPR} + w_3\text{FNR} \quad (5)$$

where w_1 , w_2 , and w_3 are weighting factors that determine the contribution of accuracy, false positive rate (FPR), and false negative rate (FNR), respectively.

2.3 EVO for FS in IDSs

This study employed an IDS as a platform to evaluate the efficacy of our proposed FS method, EVO. IDSs are essential for detecting hostile actions in a network; however, their precision and efficacy are frequently impeded by high-dimensional datasets that include irrelevant and duplicate characteristics. EVO is used as an FS technique to diminish dimensionality and improve the IDS performance. Utilizing the NSL-KDD dataset, the influence of EVO for FS on the IDSs capacity to accurately differentiate between benign and malicious traffic while reducing the computational overhead was assessed. The proposed methodology on the IDS platform is shown in Fig. 2, which primarily encompasses the following procedures. The initial phase preprocesses the NSL-KDD dataset by handling empty values, scaling data uniformly, and converting nominal features into numeric features [4]. EVO-based FS is then applied to reduce irrelevant features to improve model efficiency and accuracy [4,10]. The NSL-KDD dataset has 37 attack types classified as denial of service (DoS), probe, user to root (U2R), and remote to local (R2L), exhibiting substantial imbalances. For instance, U2R attacks are markedly underrepresented relative to DoS. This disparity was rectified by downsampling to ensure a balanced distribution of training data [4]. This disparity may result in biased models that overfit the majority class and underperform the minority class. To resolve this issue, we implemented a downsampling strategy that decreased the number of majority class instances (DoS assaults) to align with the minority class (U2R traffic).

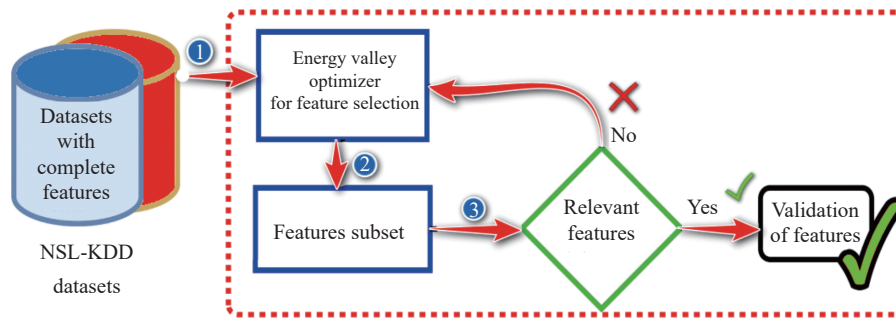


Fig. 2. Overall architecture of proposed FS framework using EVO.

This method guarantees a more equitable dataset, mitigates bias, and enhances the model's generalization capability. Downsampling diminishes the total size of the training dataset, although it improves the model's ability to identify both benign and malicious traffic more efficiently. Furthermore, to guarantee a thorough assessment, we employed the F1-score, precision, and recall, instead of depending exclusively on accuracy, to evaluate the model performance across both classes. The findings indicated that downsampling enhanced the performance equilibrium and improved the identification of the minority class while preserving strong predictions for the majority class. The NSL-KDD dataset comprises 42 numerical features and different attack types, with the prevalence of benign instances and DoS attacks balanced to improve IDS training [4,11]. Following the preprocessing steps, the datasets were divided into two portions for ML algorithms. The initial 80% of the data were allocated for training the model, while the remaining 20% were set aside for testing [4]. Algorithm 1 and Fig. 3 illustrate a detailed step-by-step workflow of the EVO algorithm for FS as an evolutionary optimization approach.

2.4 Computational complexity analysis

The computational complexity of the proposed EVO-based FS approach can be expressed as $O(N \times d \times T)$, where N denotes the population size, d represents the number of features, and T is the number of optimization iterations.

Although the EVO algorithm involves iterative optimization, the resulting feature reduction significantly decreases the dimensionality of the dataset, thereby reducing the overall training and testing times of the ML models. This renders the proposed framework suitable for real-time IDS applications.

2.5 Novelty and distinction of EVO in IDS using the FS method

Unlike conventional metaheuristic algorithms, such as the genetic algorithm (GA) and particle swarm optimization (PSO), which typically depend on fixed update strategies, EVO introduces a dynamic valley-based search mechanism that adaptively adjusts the exploration–exploitation balance. This flexibility enables EVO to explore complex feature spaces more effectively, and increases its capability to discover high-quality feature subsets without relying on rigid search patterns. Contrary to old techniques that use predefined update rules, EVO modulates the search pressure in response to the fitness of solutions and communication between solution neighborhoods.

In the context of IDS, this allows overcoming the high-dimensional feature space, minimizing premature convergence, and optimizing the sampling of small, informative feature sets, which, in turn, leads to better classification performance and computational efficiency.

2.5.1 Recent studies of intrusion datasets

Most datasets used for the evaluation of IDSs contain a large amount of feature information. Irrelevant and redundant features may degrade the performance of IDSs. FS is a common method used for selecting important features. Table 1 provides an overview of the IDS literature.

Algorithm 1 Pseudocode of EVO for FS.

Input: Training data: train = (X, Y) // Training data
 MaxIter = Maximum number of iterations
 PopSize = Population size

Output: Best_features/optimal selected features

Initialize population and evaluate initial fitness
 1: Population = initialize_population(PopSize)
 2: Fitness = evaluate_fitness (population, Train_data)
 # Main optimization loop
 3: **for** iter = 1 to MaxIter **do**
 4: **for** each candidate in a population, perform
 5: Energy_valley = calculated energy (candidate)
 6: Neighbors = find_neighbors (candidate, energy_valley)
 7: Update_position (candidate, neighbors)
 8: Candidate_fitness = Evaluate_fitness (candidate, train_data)
 9: **end for**
 10: Best_candidate = Select_best (population fitness)
 11: **if** Stopping_criteria_met, **then**
 12: **break**
 13: **end if**
 14: **end for**
 # Return optimal feature subset
 15: Return Best_features = Best_candidate.features

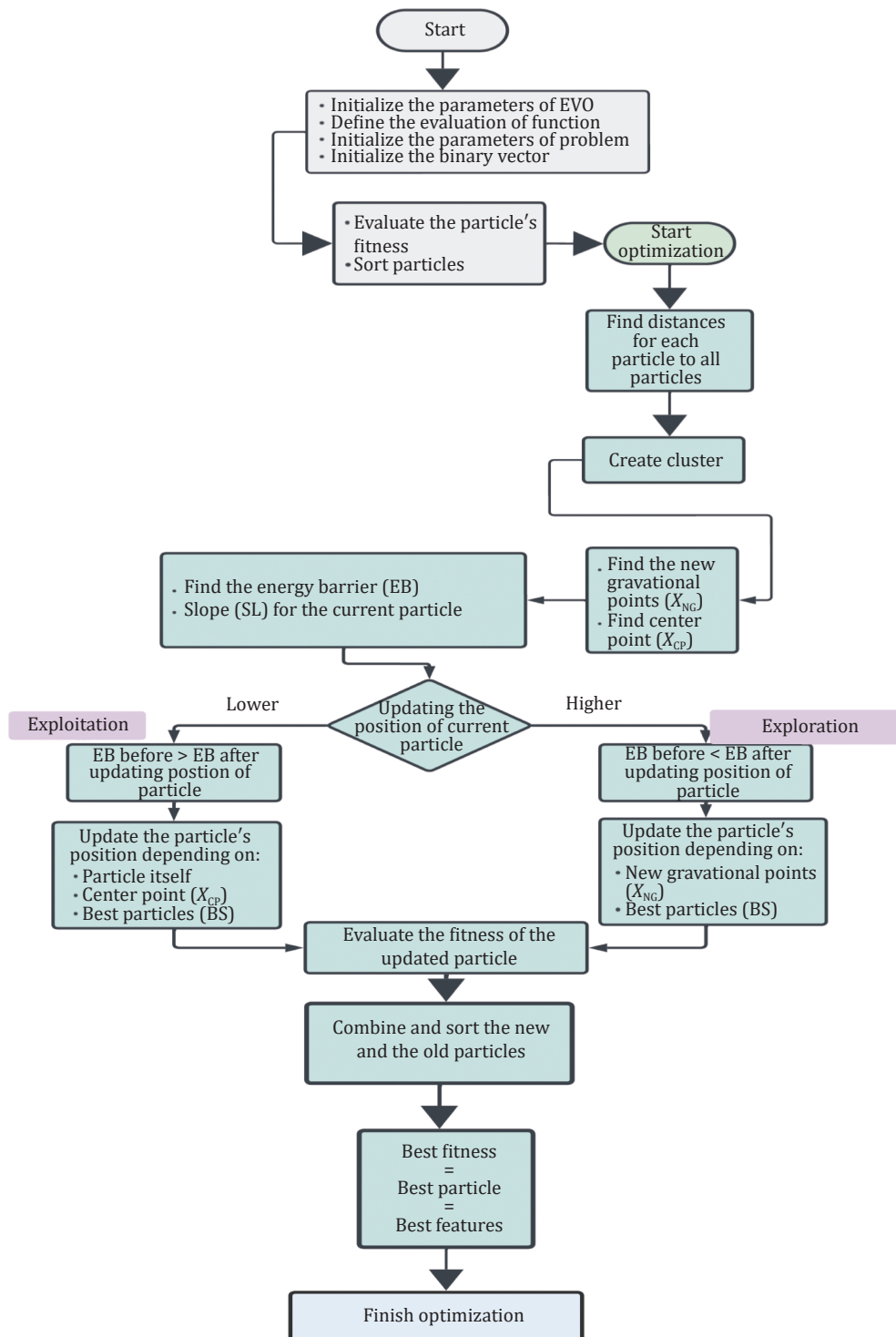


Fig. 3. Step-by-step operational workflow of the EVO algorithm includes the initialization stage, exploration of the neighborhood, fitness scoring, updating strategy of the particles, stopping criteria applied to the selection of features, and data processing for intrusion detection.

In high-dimensional datasets, efficient FS is essential to pinpoint the most valuable properties and minimize computing burden [4]. Meta-heuristic optimization techniques have demonstrated potential for overcoming these restrictions by offering a versatile, global search capacity adept at managing diverse FS

Table 1

Summary of recent studies on the NSL-KDD detection dataset.

Ref.	Datasets	Type of attacks	Years
[12]	NSL-KDD	Normal, DoS, R2L, U2R, probing	2023
[13]	NSL-KDD	Normal, DoS, probe, R2L, U2R	2024

issues [14]. Ref. [15] proposed an enhanced krill swarm (KH) optimization algorithm for feat FS on the NSL-KDD and CICIDS-2017 datasets, retaining an average of 7.0 and 10.2 features, respectively. This approach effectively eliminates redundant features while ensuring a high detection accuracy. To identify cyber threats accurately, IDS models must analyze large amounts of dynamic data, making FS a crucial step.

Research shows that intrusion detection data are large, complex, and imbalanced between attack and normal data. Many intrusion detection methods require FS and data balancing to reduce the model training time and improve classification accuracy. This study's FS and data balance strategy ensured a high detection accuracy.

2.5.2 Proposed detection of real datasets NSL-KDD

The NSL-KDD dataset is widely used as a benchmark for evaluating IDSs, owing to its structured format and balanced distribution of normal and attack samples. It was introduced to address several limitations of the KDD'99 dataset, particularly the presence of redundant records that could bias learning algorithms toward frequent patterns. By removing duplicate instances, NSL-KDD provides a reliable and unbiased evaluation environment [16].

It is important to note that the primary objective of this study is to evaluate the effectiveness of FS rather than to model specific IoT environments. Therefore, NSL-KDD serves as an appropriate and controlled testbed for benchmarking the proposed EVO-based FS method.

However, compared with modern IoT environments, NSL-KDD has certain limitations. Specifically, it does not include encrypted traffic, and contains a limited range of attack scenarios. In contrast, real IoT networks are characterized by dynamic traffic patterns, diverse protocols, and evolving threats. Consequently, the performance obtained in this study reflects a controlled evaluation setting, and further validation on IoT-specific datasets is recommended for future work.

The NSL-KDD dataset comprises two main subsets: KDDTrain+ and KDDTest+. The training set contains 125973 network connection records, whereas the test set includes 22543 records, resulting in a total of 148517 samples [16]. The dataset includes 23 different attack types, categorized into four main classes: DoS, probe, U2R, and R2L. Table 2 presents the characteristics of the NSL-KDD dataset.

Table 2

Characteristics of the NSL-KDD datasets.

Classes	37 types of attacks
DoS	Back, Mailbomb, Neptune, Pod, Smurf, UDPstore, Teardrop, Processtable, Apache2, Worm
Probe	Satan, IPsweep, Portsweep, Mscan, Nmap, Saint
R2L	Guess_password, Ftp_write, Imap, Warezmater, Xlock, Phf, Xsnoop, Snmpgue, Snmpgetattack, Multi hop, Named Httpunnel, Sendmail
U2R	Buffer_overflow, Rootkit, Perl, Loadmodule, Sqlattack, Xterm, Ps
Normal	Normal

A significant class imbalance was observed in the dataset, where DoS attacks dominated, whereas U2R and R2L were underrepresented. This imbalance can lead to biased model learning toward majority classes. To address this issue, a downsampling strategy was applied to the dominant DoS class while preserving the minority classes to maintain their statistical characteristics. Model performance was evaluated using F1-score, precision, and recall to ensure balanced performance across all categories. Table 3 illustrates the classification types of the features in NSL-KDD.

Furthermore, although NSL-KDD was originally developed to detect traditional network intrusions, its core attack classes (DoS, probe, R2L, and U2R) remain relevant to the communication layers of the IoT and WSN. Because many IoT systems operate over IP-based network infrastructures, data-traffic-level attack

patterns persist. Therefore, NSL-KDD provides a structured standard for validating optimization-based intrusion-detection frameworks in environments that share similar network-layer characteristics.

Table 3

Classification types of features in NSL-KDD.

Features	Type	Features	Type	Features	Type
duration	int64	num_file_creations	int64	diff_srv_rate	float64
protocol_type	int64	num_shells	int64	srv_diff_host_rate	float64
service	object	num_access_files	int64	dst_host_count	int64
flag	object	num_outbound_cmds	int64	dst_host_srv_count	int64
src_bytes	object	is_host_login	int64	dst_host_same_srv_rate	float64
dst_bytes	int64	is_guest_login	int64	dst_host_diff_srv_rate	float64
land	int64	srv_count	int64	dst_host_same_src_port_rate	float64
wrong_fragment	int64	serror_rate	float64	dst_host_srv_diff_host_rate	float64
urgent	int64	srv_serror_rate	float64	dst_host_serror_rate	float64
hot	int64	rerror_rate	float64	dst_host_srv_serror_rate	float64
num_failed_logins	int64	srv_rerror_rate	float64	dst_host_rerror_rate	float64
logged_in	int64	same_srv_rate	float64	dst_host_srv_rerror_rate	float64
num_compromised	int64	su_attempted	float64	class	object
'root_shell'	int64	num_root	int64	/	/

This work focuses on evaluating the effectiveness of the EVO-based FS mechanism, while generalizing the dataset is considered as a future extension. [Table 4](#) presents the distribution of the FS method for the proposed datasets.

2.5.3 Downsampling

This study tackles the problem of class imbalance in the NSL-KDD dataset using a systematic downsampling method. The dataset included five primary traffic categories: DoS, probe, R2L, U2R, and normal. Notably, the DoS category contains a significantly higher number of instances (45927) compared to the U2R and R2L categories, which are drastically underrepresented with only 52 and 995 instances, respectively. Such discrepancies can result in skewed intrusion detection models that are ineffective at identifying rare but critical attack types.

To address this issue, a class-based downsampling technique is applied to the training subset (KDDTrain+). First, the dataset was divided into class labels. The dominant DoS class was downsampled [10] to equal the size of each minority class individually, thereby creating a balanced training dataset customized for each underrepresented category. Specifically, instances from the DoS class were resampled to match the counts of the U2R, R2L, probe, and normal-traffic classes. Samples from the minority classes were kept intact to maintain their statistical properties.

Downsampling was used to balance the data to overcome the class imbalance. This method was favored over synthetic methods (e.g., SMOTE) to prevent the presence of artificial samples that could affect the original distribution of data. Moreover, downsampling can result in a lower computational cost, which is significant when considering the number of repeated evaluations in the EVO optimization process.

This balancing method guarantees equal representation of all classes during training, enhancing the overall generalization and detection performance, especially for uncommon attack types. Model effectiveness was then assessed using metrics such as precision, recall, and F1-score to gauge the success of the balancing

Table 4

Distribution of selected features for NSL-KDD datasets using the proposed method.

Datasets	Statistics by category of NSL-KDD datasets	
	Class label	Number of flow/count
KDDTrain+	Benign	67343
	DoS	45927
	Probe	11656
	R2L	995
	U2R	52
	Total	125973
KDDtest+	Benign	9711
	DoS	7460
	Probe	2421
	R2L	2754
	U2R	197
	Total	22543

technique across both the majority and minority classes. Refer to [Algorithm 2](#).

2.6 ML models

ML classification was performed on the NSL-KDD datasets utilizing LogReg, DT, and KNN methods to classify data as benign or malicious. DT is a type of supervised ML algorithm employed for classification and regression problems, notably in classification tasks.

It is noteworthy that its ability to handle both numeric (continuous) and nominal (categorical/attributes) data is considered a significant advantage. A DT comprises two types of nodes: Decision nodes, which facilitate choices with numerous branches, and leaf nodes, which represent the outcomes of decisions without additional branches [10]. KNN is one of the simplest ML algorithms [10], and is primarily utilized for classification tasks, although it is also capable of regression. KNN classifies new data by assuming similarity with existing data points, and determines categories based on the highest degree of resemblance [16]. Logistic regression predicts the probability of events such as stealth attacks by classifying logs into normal or attack categories. It uses independent variables to predict a categorical outcome and can handle multiclass scenarios to estimate the likelihood of different outcomes [17]. [Fig. 4](#) shows the proposed ML model.

Algorithm 2 Procedure balance for the NSL-KDD training dataset.

Input: Imbalanced training dataset from NSL-KDD (KDDTrain+)

Output: Balanced training dataset

```

1: Initialize an empty dataset: balanced_training_dataset
2: Define the majority class as "DoS" with 45927 samples
3: Identify minority classes
4:   Normal (13449 instances)
5:   Probe (11656 instances)
6:   R2L (995 instances)
7:   U2R (52 instances)
8: Apply downsampling to the majority class "DoS" to match the
9:   largest minority class "Normal" (13449 instances)
10: for each class 'C' in {Normal, Probe, R2L, U2R}, do
11:   if instance count of class 'C' < 1000, then
12:     Downsample the majority class "DoS" to match instance
       count of 'C'
13:     Add downsampled "DoS" data and class 'C' to
       Balanced_training_dataset
14:   else
15:     Add all samples of class 'C' to Balanced_training_dataset
16:   end if
17: end for
18: Return Balanced_training_dataset
19: end procedure

```

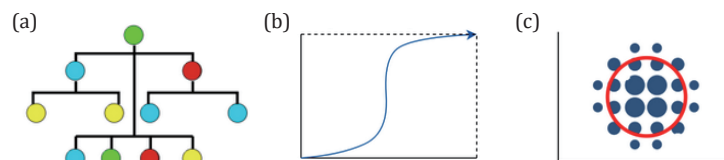


Fig. 4. ML classifiers used in the experimental assessment: (a) DT, (b) LogReg, and (c) KNN, which reveal their structural differences in the context of IDS.

Hybridizing these ML models with an evolutionary algorithm for FS. This methodology finds essential elements and improves the precision of cybersecurity, attaining maximal accuracy in the shortest amount of time. Upon completion of the loop, the global best position obtained from the optimization loop was utilized to train the final ML model. [Fig. 5](#) illustrates the proposed IDS.

3 Results

In this section, the experimental findings that resulted from testing the proposed EVO in selecting features using the NSL-KDD dataset are shown. Three ML classifiers, DT, KNN, and LogReg, were evaluated with and without an FS framework built using EVO.

3.1 Performance before FS

The classification accuracy, training duration, and test duration for each model when all 42 features of the NSL-KDD dataset were used without optimization are summarized in [Table 5](#). DT was selected as the most accurate method, with an accuracy of 98.95%. The training time was 0.03367 s, and the test time was 0.00581 s, which was shown to be the best predictive model and the fastest to compute. KNN achieved

98.47% accuracy, which was slightly lower than that of DT. Nevertheless, it had the longest test time (0.0168 s), which may limit its applicability in real-time intrusion-detection environments. The accuracy of LogReg was far lower (88.84%) than that of the other models. It had a relatively short test time (0.002103 s), but its predictive performance was low, limiting its use in high-security situations. The detailed confusion matrices and supplementary performance graphs are provided in Figs. S1-S3 in Appendix A to support the quantitative findings presented in the main text.

3.2 Performance after EVO-based FS strategy

Table 6 presents the results of the classification using the proposed EVO FS mechanism. This outcome suggests a gain in model efficiency without decreasing or worsening classification accuracy. The chosen feature set helped reduce dimensionality, which in turn reduced the computational costs and improved the stability of the model. DT continued to outperform KNN, and KNN showed an improvement in testing efficiency with feature reduction. Another advantage of LogReg was that it had FS, which exhibited better generalization than when it was pre-optimized. Appendix A provides a detailed confusion matrix and other performance measures.

The superior performance of the DT model can be attributed to several factors related to both the dataset characteristics and FS process. i) The NSL-KDD dataset is structured and tabular in nature, making it particularly suitable for tree-based models that rely on hierarchical decision rules. DT can effectively capture the nonlinear relationships between features without requiring complex transformations. ii) EVO-based FS plays a significant role in enhancing the performance of DTs. By removing redundant and irrelevant features, EVO produces a compact and highly discriminative feature subset. This allows DT to construct clearer and more precise decision boundaries.

Additionally, DTs are less sensitive to feature scaling and can efficiently exploit reduced feature spaces compared with other models, such as SVM or KNN, which may require careful parameter tuning. These factors collectively explain the strong performance of the DT model in this study. This indicates that the effectiveness of EVO is reflected not only in improved accuracy but also in enhanced congruence between the selected features and the classifier.

The EVO algorithm was used to identify 18 of the 41 features originally, and the dimensionality of the features was reduced by 56.1%. The optimization process was stopped when the highest number of function evaluations was achieved (MaxFEs = 20). Table 7 and Fig. 6 show the parameters of the EVO optimizer.

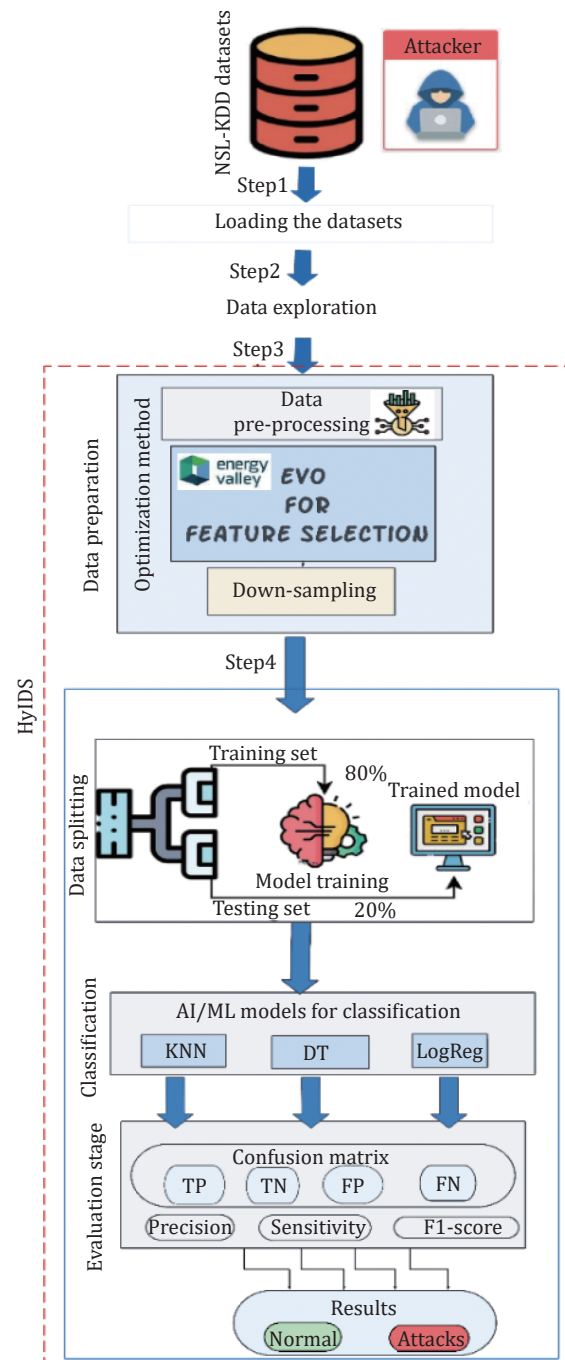


Fig. 5. Complete flowchart of the proposed IDS methodology illustrating the interaction among the EVO-based FS phases, class imbalance handling, model training, and performance evaluation.

Table 5

Classification results based on all features before optimization (42 features).

Model	No. of features	Accuracy (%)	Precision (%)	Recall (%)	F1-score (%)	Training time (s)	Testing time (s)
LogReg	42	87.94	88.67	88.48	88.41	16.08020	0.004958
DT	42	87.79	99.34	99.35	99.34	0.10229	0.005765
KNN	42	97.38	97.38	97.37	97.37	0.01731	70.213000

Table 6

Performance improvement with EVO FS (18 features).

Model	Number of features	Accuracy (%)	Precision (%)	Recall (%)	F1-score (%)	Training time (s)	Testing time (s)
LogReg-EVO	18	88.84	89.00	89.00	88.50	78.79060	0.002103
DT-EVO	18	98.96	98.96	98.97	98.97	0.33679	0.005815
KNN-EVO	18	98.47	98.47	98.47	98.47	0.016897	22.32870

Table 7

EVO parameter settings and configurations.

Datasets	Number of features before EVO	Selected features	Unselected features	Search space bounds	No. of iterations (MaxFes) /EVO	Populations size (n particles)	Binarization threshold	Selection ratio (%)	Reduction ratio (%)
NSL-KDD	42	18	23	[1, 0]	20	50	0.5	43.9	56.1

3.3 Statistical validation using *k*-fold cross-validation

To ensure the robustness and generalization capability of the proposed model, 5-fold cross-validation was performed on the NSL-KDD dataset. The dataset was divided into five equal subsets, where each subset was used once as a test set, whereas the remaining subsets were used for training. The average performance metrics and their standard deviations are presented in Table 8.

The results demonstrate that the proposed EVO-based FS framework achieves consistently high performance with a low standard deviation, indicating strong stability and reliability across different data splits.

To verify the effectiveness of the proposed EVO-based FS method further, a comparison with modern metaheuristic-based intrusion detection methods on the NSL-KDD dataset is presented in Table 9.

As shown in Table 9, several metaheuristic-based FS methods, such as the GA and PSO, have been successfully applied to the NSL-KDD dataset, achieving high detection accuracy. However, these methods often suffer from limitations, such as slow convergence, premature convergence, and instability in high-dimensional feature spaces.

Table 8*k*-fold cross-validation results (*k* = 5).

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-score (%)
DT + EVO	98.95 ± 0.12	98.96 ± 0.11	98.96 ± 0.10	98.98 ± 0.10
KNN + EVO	98.47 ± 0.15	98.47 ± 0.14	98.47 ± 0.13	98.47 ± 0.14
LogReg + EVO	88.84 ± 0.30	89.00 ± 0.28	89.00 ± 0.27	88.50 ± 0.29

Feature space reduction analysis (NSL-KDD)

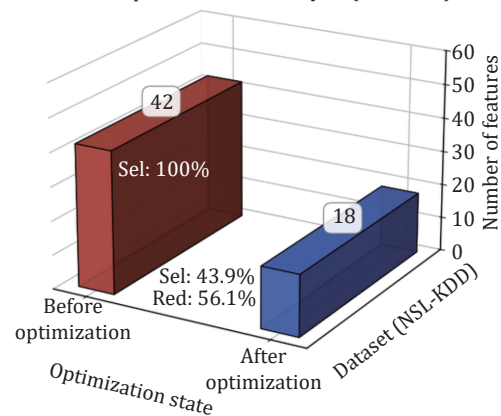
**Fig. 6.** Parameter settings and configuration of EVO.

Table 9

Comparison with metaheuristic-based method.

Reference	Optimization method	Datasets	Accuracy (%)	Method
[18]	GA	NSL-KDD	99.73	Binary classification
[19]	PSO	NSL-KDD	98.97	Hybris PSO + SVM
Proposed method	EVO	NSL-KDD	99.78	EVO for FS

In comparison, the proposed EVO-based approach achieves competitive or superior performance while maintaining a better balance between exploration and exploitation. This results in more stable FS and improved classification performance across different models.

4 Discussion

The experimental results demonstrate that the proposed EVO algorithm is effective in identifying the most informative features in the NSL-KDD dataset, thereby reducing redundancy without compromising classification quality. The high accuracy of the baseline DT indicates that tree-based models can effectively handle high-dimensional intrusion detection data. Nonetheless, the implementation of EVO also increases the computational efficiency, making the model more suitable for real-time implementation in cloud and IoT settings. With a highly competitive accuracy, KNN was disadvantaged by its greater testing latency before optimization, owing to the distance nature of its computation mechanism. This limitation was significantly reduced by the dimensionality reduction of the features, making it more useful in time-sensitive detection systems. The reduced execution time observed in the experiments aligns with the theoretical computational complexity of the proposed EVO-based framework.

The most considerable improvement in terms of post-selection features was shown in LogReg, which means that the linear models are more susceptible to irrelevant or redundant features. This highlights the significance of feature subset optimization in the application of simpler classification algorithms. Overall, the findings indicate that EVO not only increases computational efficiency but also model robustness and generalization ability. Dimensionality reduction also helps reduce the processing overhead, which is important in real-time IDSs installed in cloud-based and IoT environments.

The results confirm that EVO is a competitive evolutionary optimization algorithm for FS in cybersecurity applications.

4.1 Comparative performance analysis with state-of-the-art methods based on NSL-KDD datasets

A comparative analysis of the proposed EVO-based FS (EVOFS) framework and several state-of-the-art methods using the NSL-KDD dataset is presented in Table 10. The results demonstrate that the proposed method achieves high competitiveness and, in several cases, superior performance compared with existing approaches.

Table 10

Comparison results with other methods based on the NSL-KDD datasets.

Reference	Year	Proposed FS method	Accuracy (%)
[20]	2024	DR-MOFS	86.86
[21]	2025	ICSA	97.91
[22]	2025	CNN-BiLSTM (DL-based)	89.00
[23]	2026	Hybrid CNN-BLTM	95.40
		KNN + EVOFS	98.47
Our proposed method	/	DT + EVOFS	98.95
		LogReg + EVOFS	88.84

Specifically, DT combined with EVOFS achieved the highest accuracy of 98.95%, outperforming recent methods such as the improved chameleon swarm algorithm (ICSA) with an accuracy of 97.91% and hybrid deep learning models such as convolutional neural network (CNN)-BLSTM with an accuracy of 95.40%. Similarly, the KNN + EVOFS model achieved an accuracy of 98.47%, confirming the effectiveness of EVO for selecting highly discriminative feature subsets.

In contrast, earlier approaches, such as detection rate-emphasized multi-objective evolutionary FS (DR-MOFS), reported significantly lower performance, with an accuracy of 86.86%. Additionally, deep learning-based models such as CNN-BiLSTM (DL-based) achieved only 89% accuracy, indicating that advanced deep architectures do not necessarily guarantee superior performance when FS is not optimally handled. These findings highlight that carefully optimized FS combined with efficient classical classifiers can outperform more complex models.

Moreover, the results reveal that the EVO-based FS approach provides a strong balance between the feature reduction and classification accuracy. This balance is particularly important for real-time IDSs in cloud and IoT environments where both efficiency and accuracy are critical.

Another key observation is the consistent performance improvement across multiple classifiers, including KNN, DT, and LogReg. This demonstrates that the effectiveness of EVO is largely classifier-independent, which enhances its robustness and applicability across various cybersecurity scenarios.

Overall, the comparative results confirm that the proposed EVO-based FS method is a competitive, scalable, and efficient optimization approach for intrusion detection using the NSL-KDD dataset.

4.2 Comparative analysis of feature reduction performance based on different FS methods

The comparative performance of the proposed EVO-based FS method on the NSL-KDD dataset in terms of dimensionality reduction is illustrated in Fig. 7. The suggested EVO technique decreased the number of features in the feature space from 42 to 18, achieving a competitive reduction ratio compared with recent FS methods [24]. The ratio of feature reduction is competitive with other top optimization algorithms, namely, filter + NSGA-II for FS (13 features), where NSGA is a non-dominated sorting GA II. The proposed EVO method reduced the feature space from 42 to 18 features. This reduction is competitive with other feature selection approaches, including Filter+NSGA-II (13 features), DR-MOFS (17 features), CFS+XGBoost (25 features), and DL+FS (12 features), demonstrating that EVO achieves a substantial dimensionality reduction while retaining a relatively compact feature subset.

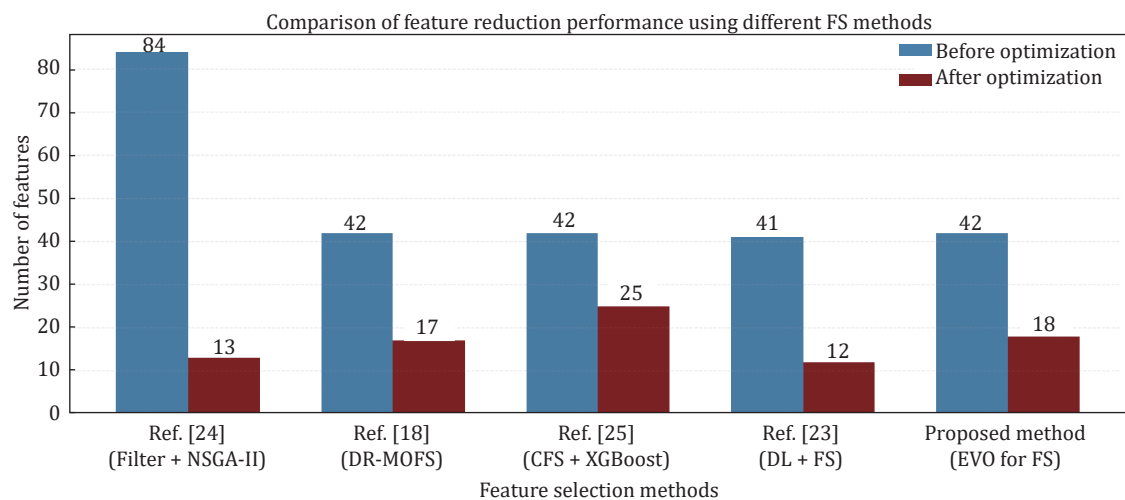


Fig. 7. Comparison results with other methods based on FS.

In general, the findings support the thesis that EVO provides an effective and competitive FS process in which the dimensionality reduction is quite high without affecting the robustness of the model, which is

consistent with recent studies on optimization-based penetration testing [25].

In addition to the quantitative comparisons that can be made based on Table 10, we also discuss the methodological variations between EVO and similar optimization-based FS approaches such as NSGA-II, DR-MOFS, and GA-based FS. In contrast, EVO uses a less expensive, more balanced exploration-exploitation mechanism, whereas NSGA-II relies on multi-objective Pareto ranking and requires more control parameters. EVO has a competitive dimensionality reduction (18 out of 42 features) compared to wrapper-based methods, such as DR-MOFS and ICSEA, and it has better classification stability across a variety of classifiers. This implies that EVO offers good trade-offs between the complexity of the models and detection accuracy.

5 Conclusions

The research highlights enhancements to EVO for FS on large-scale real-world datasets. Our novel approach demonstrated a strong performance and confirmed its effectiveness in enhancing the attributes of the NSL-KDD dataset, with the feature set reduced while improving performance, that is, 18 out of 42 features increased. The enhanced dataset was assessed using the IDS platform. EVO effectively reduces data dimensionality while improving classification performance, achieving an accuracy of DT of 88.84%, precision of 89.00%, recall of 89.00%, F1-score of 88.50%, and LogReg of 98.95%, 98.96%, and 98.98% for accuracy, precision, recall, and F1-score, respectively. On the other hand, the KNN model showed an accuracy of 98.47% for each metric, utilizing only 18 features out of 42, while also optimizing the training duration in real time. This development confirms the role of EVO in optimizing FS and significantly enhancing the performance of ML classifiers such as DT, LogReg, and KNN. The results demonstrate the effectiveness of EVO in enhancing real-world datasets, boosting intrusion detection capabilities, and protecting cybersecurity systems of WSNs and CC.

Future research efforts will focus on improving EVO, specifically for real-time IDS environments. Real-time IDS require adaptive FS methods that are computationally efficient for handling high-velocity network traffic. The application of EVO in streaming environments enhances IDS responsiveness by reducing the detection latency while maintaining high accuracy levels. The combination of EVO with another type of optimizer and ensemble deep learning models, including CNNs, recurrent neural networks (RNNs), and long short-term memory (LSTM) networks, improves IDS by effectively recognizing both spatial and temporal attack patterns.

In future work, the proposed framework will be evaluated on recent IoT-focused datasets, including Edge-IIoTset and TON_IoT, to verify its effectiveness in diverse and large-scale environments. These datasets cover modern attack patterns and complex data traffic characteristics, thereby providing a more realistic assessment of intrusion detection performance in CC and IoT systems.

Appendix A. Supplementary data

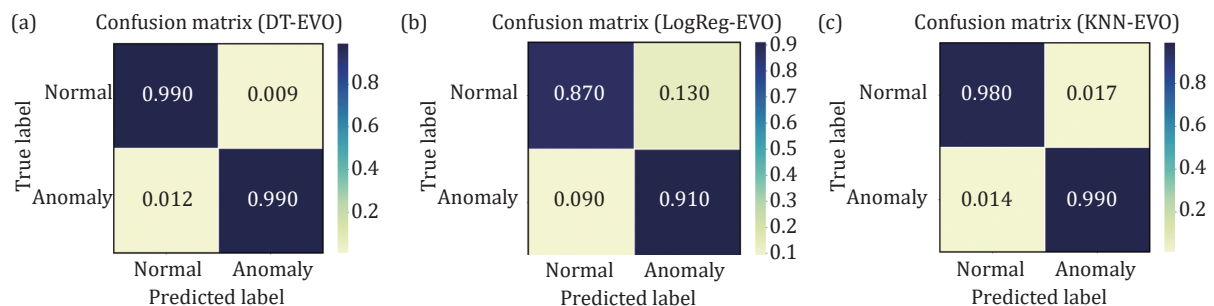


Fig. S1. Confusion matrices for (a) DT-EVO, (b) LogReg-EVO, and (c) KNN-EVO.

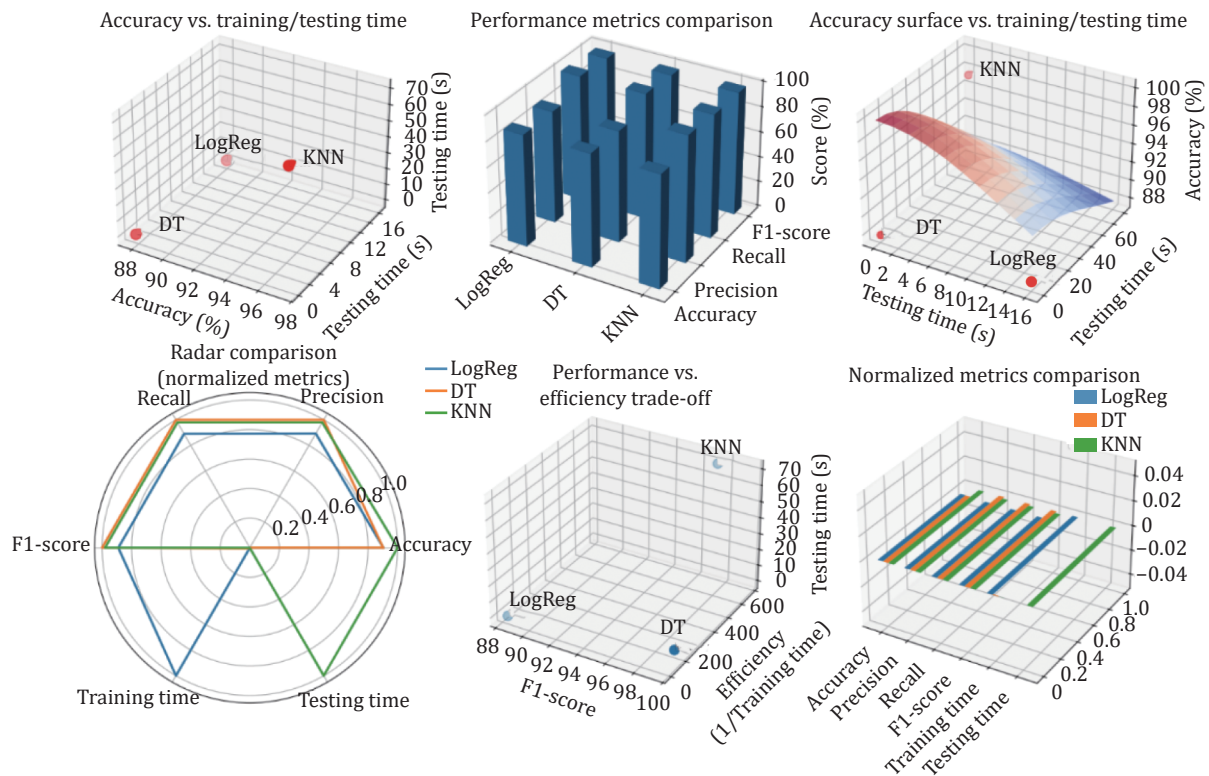


Fig. S2. Baseline classification results using all 42 original features before applying EVO-based FS showing the comparative performance of the evaluated ML models.

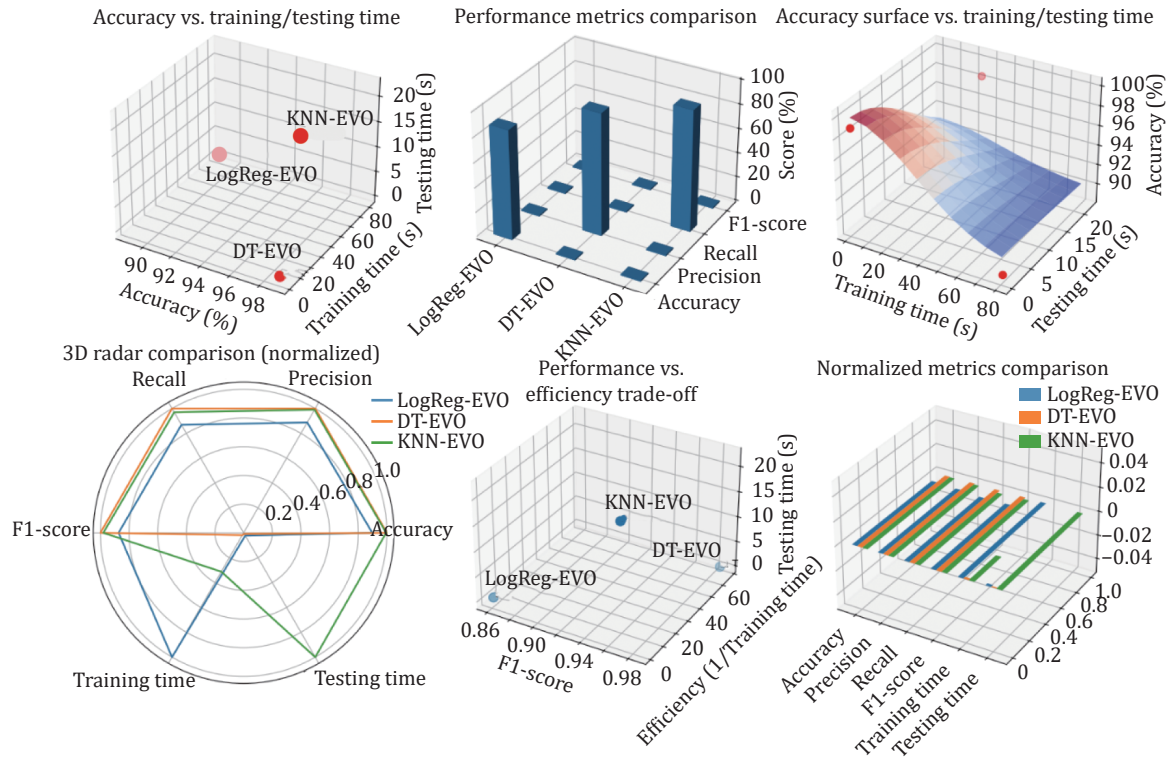


Fig. S3. Classification results using 18 enhanced features after applying EVO-based FS illustrating the comparative performance of the evaluated ML models.

Acknowledgments

The authors would like to express their heartfelt thanks to the Polytechnic College of Engineering, Baghdad, Middle Technical University (MTU), Iraq, for supporting this research by providing the necessary academic resources and facilities.

The data utilized in this work "NSL-KDD" is publicly accessible and was acquired from the Canadian Cybersecurity Institute at the University of New Brunswick via the following Links: <https://www.unb.ca/cic/datasets/nsl.html> and DOI: 10.1109/CISDA.2009.5356528 for the datasets.

CRedit authorship contribution statement

Maryam Mahdi Alhusseini: Writing—original draft, Conceptualization, Methodology, Formal analysis, Investigation, Data curation, Visualization, Supervision. **Inam Abdullah Lafta:** Writing—review & editing, Investigation, Data curation. **Fatima Faydhe Al-Azzawi:** Writing—review & editing, Validation, Data curation. **Fadhil Abbas Fadhil:** Data curation and resources. **Mohammad-Reza Feizi-Derakhshi:** Writing—review & editing, Supervision, Validation, Project administration. **Azhar Naji Alyahya:** Investigation, Data curation. **Zaid Ameen Abduljabbar:** Resources, Investigation, Data curation. **Vincent Omollo Nyangaresi:** Writing—review & editing, Validation.

Declaration of competing interests

The authors declare no conflicts of interest.

References

- [1] N. Kumar, J.P. Singh, P. Kumar, Machine learning-enhanced IoT network security: a black hole algorithm-based feature selection approach for intrusion detection, *Journal of Cyber Security Technology* 10 (1) (2026) 1–9.
- [2] G. Zhu, Y.-T. Yu, Z.-Y. Li, et al., GMDDPM-CT: advancing network intrusion detection through diffusion-based sample synthesis and deep learning, *ICT Express* (2026), doi.org/10.1016/j.icte.2026.01.014.
- [3] A.H. Khan, M. Sajid, K.R. Malik, et al., Meta-learning meets transformers: a novel approach to enterprise network intrusion detection, *Expert Syst. Appl.* 318 (2026) 131859.
- [4] R.-Z. Zhao, Y.-X. Mu, L. Zou, et al., A hybrid intrusion detection system based on feature selection and weighted stacking classifier, *IEEE Access* 10 (2022) 71414–71426.
- [5] F.A. Fadhil, M.M. Alhusseini, M.R. Feizi-Derakhshi, Enhanced cast-128 with adaptive s-box optimization via neural networks for image protection, in: F.P.G. Márquez, A. Jamil, A.A. Hameed, et al. (Eds.), *Advanced Engineering, Technology and Applications on Power Systems*, Springer, Cham, Germany, 2026, pp. 568–583.
- [6] F.A. Fadhil, M.M. Alhusseini, M.R. Feizi-Derakhshi, et al., Video streams integration of secure text with ORB feature mapping and ChaCha20 algorithm, in: *Proc. of the 5th Intl. Conf. on Electrical, Computer & Telecommunication Engineering*, Rajshahi, Bangladesh, 2026, pp. 1–6.
- [7] B.M. Kumar, J. Ragaventhiran, V. Neela, Hybrid optimization integrated intrusion detection system in WSN using Elman network, *International Journal of Data Science and Artificial Intelligence* 2 (2) (2024) 55–62.
- [8] K. Sundaramoorthy, K.E. Purushothaman, J. Jeba Sonia, et al., Enhancing cybersecurity in cloud computing and WSNs: a hybrid IDS approach, *Comput. Secur.* 147 (2024) 104081.
- [9] M. Azizi, U. Aickelin, H.A. Khorshidi, et al., Energy valley optimizer: a novel metaheuristic algorithm for global and engineering optimization, *Sci. Rep.-UK* 13 (1) (2023) 226.
- [10] J.H. Joloudari, H. Saadatfar, A. Dehzangi, et al., Computer-aided decision-making for predicting liver disease using PSO-based optimized SVM with feature selection, *Informatics in Medicine Unlocked* 17 (2019) 100255.
- [11] J.L. Leevy, J. Hancock, R. Zuech, et al., Detecting cybersecurity attacks across different network features and learners, *Journal of Big Data* 8 (1) (2021) 38.
- [12] G. Logeswari, S. Bose, T. Anitha, An intrusion detection system for SDN using machine learning, *Intell. Autom. Soft Co.* 35 (1) (2023) 867–880.
- [13] S. Altamimi, Q. Abu Al-Haija, Maximizing intrusion detection efficiency for IoT networks using extreme learning machine, *Discover Internet of Things* 4 (1) (2024) 5.
- [14] I. Sharafaldin, A.H. Lashkari, S. Hakak, et al., Developing realistic distributed denial of service (DDoS) attack dataset and taxonomy, in: *Proc. of Intl. Carnahan Conf. on Security Technology (ICCST)*, Chennai, India, 2019, pp. 1–8.
- [15] E.S. Alomari, O.A. Hassen, W.M. Salim, et al., A new descriptor based on machine learning for intrusion detection in wireless sensor networks WNSs, *Journal of Intelligent Systems and Internet of Things* 16 (1) (2025) 176–188.
- [16] M. Tavallae, E. Bagheri, W. Lu, et al., A detailed analysis of the KDD CUP 99 data set, in: *Proc. IEEE Symposium on Computational Intelligence for Security and Defense Applications (CISDA)*, Ottawa, Canada, 2009, pp. 1–6.

- [17] L. Abualigah, M.H. Almomani, S.A. Alomari, et al., Optimizing intrusion detection in wireless sensor networks via the improved chameleon swarm algorithm for feature selection, *IET Commun.* 19 (1) (2025) e70029.
- [18] Z.-H. Cheng, H.P. Shang, C. Qian, Detection-rate-emphasized multi-objective evolutionary feature selection for network intrusion detection [Online]. Available, <https://arxiv.org/abs/2406.09180>, June 2024.
- [19] X. Li, P. Yi, W. Wei, et al., LNNLS-KH: a feature selection method for network intrusion detection, *Security and Communication Networks* 2021 (2021) 8830431.
- [20] J.O. Onah, S.M. Abdulhamid, M. Abdullahi, et al., Genetic algorithm based feature selection and Naïve Bayes for anomaly detection in fog computing environment, *Machine Learning with Applications* 6 (2021) 100156.
- [21] S. Subramani, M. Selvi, Multi-objective PSO based feature selection for intrusion detection in IoT based wireless sensor networks, *Optik* 273 (2023) 170419.
- [22] V.R. Joshi, K. Assa-Agyei, T. Al-Hadhrami, et al., Hybrid AI intrusion detection: balancing accuracy and efficiency, *Sensors* 25 (24) (2025) 7564.
- [23] L.K.S. Kumar, S.R. Nethi, R. Uyyala, et al., Anomaly-based intrusion detection on benchmark datasets for network security: a comprehensive evaluation, *Sci. Rep.-UK* 16 (1) (2026) 8507.
- [24] A.K. Dey, G.P. Gupta, S.P. Sahu, Hybrid meta-heuristic based feature selection mechanism for cyber-attack detection in IoT-enabled networks, *Procedia Computer Science* 218 (2023) 318–327.
- [25] G. Nassreddine, M. Nassereddine, O. Al-Khatib, Ensemble learning for network intrusion detection based on correlation and embedded feature selection techniques, *Computers* 14 (3) (2025) 82.

Maryam Mahdi Alhusseini received the B.S. degree in computer engineering from Middle Technical University (MTU), Baghdad, Iraq in 2007, and the M.S. degree in computer engineering (software engineering–cybersecurity using AI) from the Azerbaijan Shahid Madani University (ASMU), Tabriz, Iran in 2023. She is a Lecturer with the Information and Communication Technology Department, Polytechnic College of Engineering–Baghdad, MTU. She is a member of the IEEE and serves as a reviewer for several peer-reviewed journals indexed in Scopus and Clarivate, as well as international conferences. She is also an Elsevier-recognized reviewer and has received official certification for her peer-review contributions. Her research interests include applied artificial intelligence (AI), cybersecurity, optimization algorithms, cloud computing (CC), Internet of things (IoT), natural language processing (NLP), and sentiment analysis.



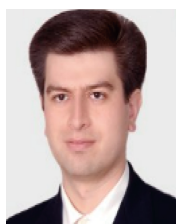
Inam Abdullah Lafta received the M.S. degree in information technology from Universiti Utara Malaysia (UUM), Kedah, Malaysia in 2016. She is currently a Lecturer with the Information and Communication Technology (ICT) Department, Polytechnic College of Engineering–Baghdad, MTU. She has published several research papers and has held various administrative positions, including the Head of the ICT Department at the Polytechnic College of Engineering, Baghdad, MTU. Her research interests include AI, software requirements engineering, computer system safety, cryptography, medical imaging, and digital steganography.



Fatima Faydhe Al-Azzawi received the M.S. degree in communications engineering from the University of Technology–Iraq, Baghdad, Iraq in 2005. She is currently an Assistant Professor with the Electronics Engineering and AI Technologies Department, Polytechnic College of Engineering–Baghdad, MTU. Her research interests include communication engineering, wireless communication, networking, and modulation.



Fadhil Abbas Fadhil received the M.S. degree in computer science (cybersecurity) from Ural Federal University (UrFU), Yekaterinburg, Russia in 2022. He is currently a Lecturer with the College of Computer Science, University of Technology–Iraq, Baghdad, Iraq, where he also served as the Head of the IT Division. His research focuses on data and multimedia security, neural network-based encryption optimization, secure information embedding in video streams, and AI applications in cybersecurity.



Mohammad-Reza Feizi-Derakhshi received the B.S. degree in software engineering from the University of Isfahan, Isfahan, Iran in 1997, and the M.S. and Ph.D. degrees in artificial intelligence from the Iran University of Science and Technology, Tehran, Iran in 2000 and 2007, respectively. He is currently a full-time Professor with the University of Tabriz, Tabriz, Iran. His research interests include NLP, optimization algorithms, social network analysis, and intelligent databases.



Azhar Naji Alyahya received the M.S. degree from Sakarya University, Sakarya, Türkiye in 2024. She is currently a Lecturer with the Department of Software Engineering, Sakarya University. Her research interests include applied AI, optimization algorithms, and machine learning.



Zaid Ameen Abduljabbar received the B.S. and M.S. degrees in computer science from the University of Basrah, Basrah, Iraq in 2002 and 2006, respectively, and the Ph.D. degree in computer engineering from Shenzhen Institute, Huazhong University of Science and Technology, Shenzhen, China in 2017. He is currently a Lecturer and Researcher with the Department of Computer Science, College of Education for Pure Sciences, University of Basrah, Basrah, Iraq. He has published regular articles in more than 100 IEEE and Springer international conferences and articles in SCI journals, and holds eight international patents and two international computer software copyrights. His research interests include cloud security, searchable encryption systems, similarity measures, IoT, secure computation, biometrics, and soft computing.



Vincent Omollo Nyangaresi received the B.S. degree in telecommunications & information technology and the M.S. and Ph.D. degrees in information technology security & audit from Jaramogi Oginga Odinga University of Science & Technology, Bondo, Kenya in 2010, 2018, and 2022, respectively. He is currently serving as the Chair of the Department of Computer Science and Software Engineering, Jaramogi Oginga Odinga University of Science & Technology. He is an adjunct faculty member at the Department of Applied Electronics, Saveetha Institute of Medical and Technical Sciences (SIMATS), Chennai, India. He is an experienced researcher in the areas of computer science and information technology and has published over 200 research articles in peer-reviewed journals and conferences. He is ranked among the top 2% scientists in the world in information and communication technology by Stanford/Elsevier. He is currently serving as an Editor in top journals. He has served as a Guest Editor in top journals. Moreover, he is a renowned reviewer for more than 120 journals in IEEE, IGI, Taylor & Francis, MDPI, PLOS ONE, Elsevier, and Springer. He has served as a Technical Committee Member (TPC) for numerous international conferences and symposia. His research interests include AI, machine learning, wireless network security, quantum computing, IoT, wireless sensor networks (WSNs), cellular networks, information systems acceptance modeling, TCP architecture and design, radio wave propagation, virtualization, and CC.

Maryam Mahdi Alhusseini's photograph is not available at the time of publication.