Cluster Computing
https://doi.org/10.1007/s10586-024-04458-8

A novel intrusion detection system based on a hybrid quantum support vector machine and improved Grey Wolf optimizer

E. I. Elsedimy[1] · Hala Elhadidy[2] · Sara M. M. Abohashish[1]

Received: 30 December 2023 / Revised: 20 March 2024 / Accepted: 25 March 2024

Abstract

The Internet of Things (IoT) has grown significantly in recent years, allowing devices with sensors to share data via the internet. Despite the growing popularity of IoT devices, they remain vulnerable to cyber-attacks. To address this issue, researchers have proposed the Hybrid Intrusion Detection System (HIDS) as a way to enhance the security of IoT. This paper presents a novel intrusion detection model, namely QSVM-IGWO, for improving the detection capabilities and reducing false positive alarms of HIDS. This model aims to improve the performance of the Quantum Support Vector Machine (QSVM) by incorporating parameters from the Improved Grey Wolf Optimizer (IGWO) algorithm. IGWO is introduced under the hypothesis that the social hierarchy observed in grey wolves enhances the searching procedure and overcomes the limitations of GWO. In addition, the QSVM model is employed for binary classification by selecting the kernel function to obtain an optimal solution. Experimental results show promising performance of QSVM-IGWO in terms of accuracy, Recall, Precision, F1 score, and ROC curve, when compared with recent detection models.

Keywords Internet of Things (IoT) · Hybrid Intrusion Detection System (HIDS) · Quantum Support Vector Machine (QSVM) · Improved Grey Wolf Optimizer (IGWO)

Abbreviations

ABC	Artificial Bee Colony
AIDS	Anomaly based IDS
ANN	Artificial Neural Network
CNN	Convolution Neural Network
DDoS	Distributed Denial of Service
DoS	Denial of Service
DT	Decision trees
ELM	Extreme Learning Machine
GA	Genetic Algorithm
GBM	Gradient Boosting Machine
GWO	Grey Wolf Optimization
HIDS	Hybrid Intrusion Detection System
HOA	Horse Herd Optimization Algorithm
IG	Information Gain
IGWO	Improved Grey Wolf Optimizer
IoT	Internet of Things
IRF	Improved Random Forest
KNN	K-Nearest Neighbors
LIDS	Lightweight Anomaly Detection
LR	Logistic Regression
LSTM	Long Short-Term Memory
MLP	Multi-Layer Perceptron
OBL	Opposition Based Learning
OLGWO	Oppositional based Laplacian Grey Wolf Optimization
PCA	Principal Component Analysis
PSO	Particle Swarm Optimization
QSVM	Quantum Support Vector Machine
RF	Random Forest
RNN	Recurrent Neural Network
RPL	Routing Protocol for Low-Power and Lossy Networks
SDWSN	Software Defined Wireless Sensor Network
SIDS	Signature based IDS
SLR	Systematic literature review
SSO	Salp Swarm Optimization

✉ Sara M. M. Abohashish
sara_mohamed@himc.psu.edu.eg

[1] Information Technology Systems Management Department, Faculty of Management Technology and Information Systems, Port Said University, Port Said, Egypt

[2] Electrical Engineering Department, Faculty of Engineering, Port Said University, Port Said, Egypt

Published online: 02 May 2024

1 Introduction

The Internet of Things (IoT) enables intelligent communication that allows smart devices to exchange data over the Internet. It is a developing technology that involves physical objects with hardware and software components necessary for proper implementation of a network. The hardware components include sensors, processors, and actuators that gather data across the network, process on that data then take action accordingly. Moreover, IoT has a wide range of applications in various fields including industrial, healthcare, smart environments, and medical devices. The fundamental goal of IoT technology is to save time and effort in various fields. It is expected that around 38.6 billion devices will be connected to IoT by 2025 [1]. However, weak or inadequate authentication mechanisms can make it easier for attackers to gain unauthorized access to IoT devices. Similarly, insufficient authorization controls may allow unauthorized users to manipulate or control connected devices. Therefore, the growth of IoT devices has rendered them more susceptible to security threats.

In a connected IoT environment, the communication between devices is vulnerable to attacks. Securing the communication channels, implementing encryption, and protecting against man-in-the-middle attacks are vital for IoT network security. Addressing these challenges requires a holistic approach involving collaboration between manufacturers, and cyber-security experts to establish and enforce Intrusion Detection Systems (IDS) and implement effective security practices across the entire IoT ecosystem.

1.1 Hybrid IDS (HIDS)

IDS is a critical component designed to monitor and analyze network or system activities for signs of malicious behavior or security policy violations as shown in Fig. 1. Traditional IDS can be broadly categorized into two main types: Network-based Intrusion Detection Systems and Host-based Intrusion Detection Systems. Several recent studies have concentrated on constructing intrusion detection systems (IDS) to secure the IoT network from attacks and prevent the exploitation of vulnerabilities [1–4]. Different categories of IoT IDS include Signature-based (SIDS), Anomaly-based (AIDS), and Hybrid (HIDS). These are classified according to the detection technique, validation strategy, and deployment approach.

The first category SIDS aims to find the sequences and patterns of known attacks that match one of the attack signatures in the IoT network traffic [5–7]. In other words, SIDS raises an alarm when an intrusion signature matches a previous signature according to the if-else rule. SIDS needs to be updated to store the signature of new attacks. Indeed, numerous works have applied SIDS to detect attacks with a minimum rate of false rate [8–12]. The second category AIDS is more effective to detect zero-day attacks based on recognizing abnormal behaviors in the network [13]. Several works have been introduced where AIDS is used for improving accuracy and enhancing false positives [14–18]. Furthermore, various methodologies have employed individual techniques, such as Convolution Neural Network (CNN) [19], Long Short-Term Memory (LSTM) [20], AE [21], for identification and classification of attacks. Additionally, some approaches have enhanced performance by combining multiple techniques [22–24]. However, the traditional methods of AIDS have a high false positive rate as they examine input and output variables to learn behavior of normal activity. Consequently, the potential solution to the AIDS limitations is HIDS which integrates SIDS and AIDS, providing a better tradeoff between the storage and computing cost while minimizing false positive alarms and achieving effective detection capabilities.

Machine learning techniques are used to enhance the security of IoT with different techniques by either introducing and applying new metaheuristic algorithms or the fusion of two existing algorithms [25]. Furthermore, they are considered valuable for identifying attacks in IoT networks [26–30]. Deep learning involves the utilization of multiple information-processing layers within a hierarchical structure. Consequently, numerous approaches have integrated two deep learning algorithms, such as CNN and LSTM [26], or CNN and Recurrent Neural Network (RNN) [27], to address privacy and security concerns in HIDS. The potential of machine learning and deep learning algorithms in addressing anomaly detection within HIDS is investigated in [28–30]. However, it is crucial to acknowledge that the effective training of deep learning algorithms necessitates vast amounts of high-quality data, rendering them less commonly utilized in security applications. On the other hand, many researchers advocate for machine learning-based HIDS due to their capacity to handle large datasets and detect patterns in real-time [31]. In addition, there are different studies of HIDS that utilize machine learning for preventing malicious traffic when data volumes are small which take too much time to train the model [32, 33]. Furthermore, several approaches are proposed to improve the accuracy results by combining two or more machine learning algorithms, such as PSO and ensemble learners [34], PSO and RF [35], SVM and Artificial Neural Network (ANN) [36], Grey Wolf Optimization (GWO) and Extreme Learning Machine (ELM) [37], LR and DT [38], SVM and DT [39], 40, Oppositional-based Laplacian Grey Wolf Optimization (OLGWO) and SVM [41].

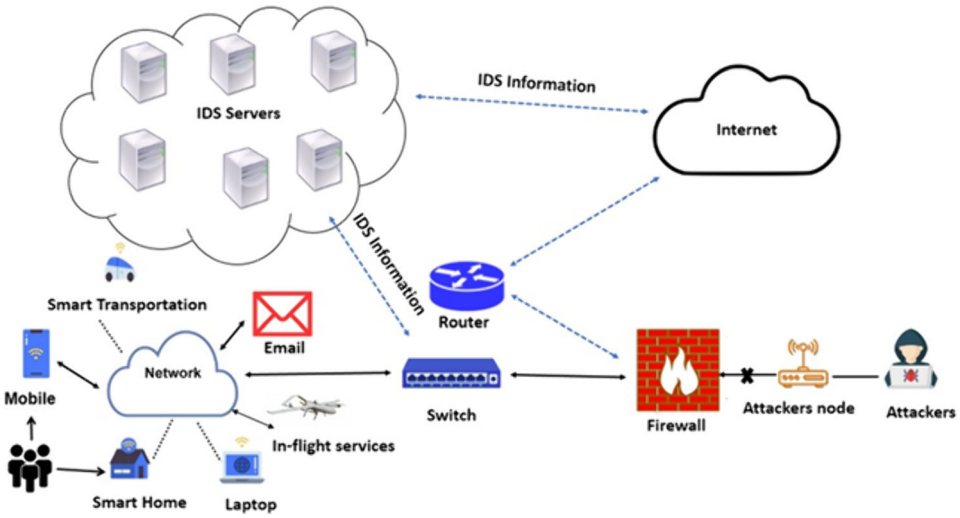


Fig. 1 Traditional IDS architecture

SVM is commonly used in machine learning for regression and classification tasks due to its powerful learning capability, which comes from the use of an optimal hyperplane to separate cases with different class labels. Furthermore, SVM is sensitive to its hyper-parameters, which directly impact its efficiency and accuracy [36]. As QSVM represents an amalgamation of quantum computing with the SVM approach, leveraging quantum systems to enhance computational speed and data processing capabilities, it demonstrates effectiveness in handling large datasets, delivering heightened accuracy when working with extensive feature maps [42, 43].

1.2 Motivation and contribution

The existing literature commonly addresses IDS concerns, where outputs are accurate but time-consuming, or accuracy is compromised for quicker training. Subsequently, QSVM is applied to assess the computational speed and data processing performance of the HIDSs. In addition, metaheuristic algorithms play an important role in HIDS which improve feature selection techniques that influence the performance of IoT security [44]. GWO is an example of a metaheuristic algorithm that directly impacts the performance of IDSs by selecting the best subset of data features. It has been proven that GWO achieves high accuracy in the detection process especially when combined with other algorithms. However, GWO drops in optima and encounters challenges in maintaining a balance between exploration and exploitation, leading to suboptimal solutions. Consequently, researchers have endeavored to overcome these limitations by integrating GWO with diverse optimization algorithms such as, GWO with PSO [44], GWO with the GA [45], and GWO with the Artificial Bee Colony (ABC) algorithm [46]. Therefore, the objective of this research is to integrate the QSVM with a modified version of GWO in order to achieve high accuracy in detecting the intrusion thus enhancing the security performance of IoT. The integration of quantum computing and SVM techniques, specifically in the cyber-attack detection systems, aims to improve efficiency and effectiveness in solving complex optimization and classification problems. This hybrid approach uses metaheuristic optimization through IGWO to fine-tune hyper parameters, transforms data to a higher-dimensional quantum feature space, and uses quantum kernels for computation of inner products in order to detect the intrusion with high efficiency.

The motivations and contributions of this paper can be summarized as follows:

1. A novel intrusion detection system based on a hybrid Quantum Support Vector Machine and Improved Grey Wolf Optimizer algorithm (QSVM-IGWO) is proposed to support efficient attack detection in HIDS.
2. The IGWO is introduced under the hypothesis that the social hierarchy observed in grey wolves enhances the searching procedure and overcomes the limitations of GWO. In addition, the QSVM model is employed for binary classification by selecting the kernel function to obtain an optimal solution.
3. A novel approach of quantum machine learning is implemented in HIDS to enhance computational speed and data processing.
4. The proposed QSVM-IGWO model is trained on the Bot-IoT dataset to measure accuracy, Recall, Precision, F1 score, and ROC curve.

1.3 Organization of the paper

The rest of the paper is organized as follows: The related works are explained in Sect. 2. The methodology and proposed model QSVM-IGWO are discussed in detail in

Sect. 3. Experiments and results are shown in Sect. 4 and the conclusion of this paper is presented in Sect. 5.

2 Related work

This section provides a literature review of intelligent security models to identify malicious activities in IoT networks. Recently, several studies [3–11] have concentrated on constructing IDS using machine learning. Krishna et al. [3] investigated a hybrid optimization approach to detect IoT attacks by combining the metaheuristic Lion Optimization Algorithm and Firefly Optimization algorithm in IoT devices. Two different datasets, namely NSL-KDD and NBaIoT, were employed for this purpose. Although the results showed that the hybrid optimization algorithm demonstrated a minimal attack rate, IoT security remains a challenging topic. In the same context, Verdejo et al. [5] proposed a novel configuration of SIDS in order to provide the optimal performance in the web attacks and find the recall and precision rate of three SIDS. Meng et al. [8] employed kernel Principal Component Analysis (PCA) and Long-Term Memory Recurrent Neural Network (LSTM-RNN) to achieve effective attack detection. High accuracy and low false positive rates were achieved to distinguish attacks from normal network traffic. Ingre et al. [9] proposed ANN for IDS which covered binary class and multi-class attack types based on the NSL-KDD dataset achieving accuracy rates of 81.2%. However, the accuracy of detection still needs to be improved for IDS. Qureshi et al. [10] proposed a novel IDS based on RNN with different learning rate in IoT which achieved better accuracy than other algorithms such as SVM, ANN, RNN, RF, Naive Bayes, and Multi-Layer Perceptron (MLP). Pavanang et al. [11] implemented deep learning to develop a novel (RNN-IDS) for both binary and multiclass classification and the results compared with other algorithms such as an ANN, SVM, and RF. However, they were unable to detect the signature of the new zero-day attack of IoT networks. Therefore, the development of a highly efficient IDS technique that took into account new zero-day attacks in IoT networks is still a challenge for researchers [14–19]. Table 1 provides a summary of the recent state-of-the-art methods for threat detection in IDSs.

Alsoufi et al. [14] presented AIDS techniques based on IoT and they explored seven deep learning techniques in Systematic Literature Review (SLR). The results showed that supervised learning produced better results than unsupervised and semi-supervised learning. Gothawal et al. [15] implemented Routing Protocol for Low-Power and Lossy Networks (RPL) which is utilized for detecting and confirming attacks within the game model to differentiate the malicious behavior in AIDS technique. In addition, they considered two approaches, stochastic game and evolutionary game. Likewise, Keserwani et al. [16] introduced a technique for feature selection which combines GWO and Particle Swarm Optimization (PSO). The results showed that the proposed technique improved the accuracy and enhanced the precision. Lately, Singh et al. [17] investigated AIDS techniques to detect malicious and prevent attacks in the IoT based on the DT model which achieved higher accuracy with the exponential growth of data. On the other hand, Davahli et al. [18] presented a hybrid feature selection through Genetic Algorithm (GA) and GWO based on Lightweight Anomaly Detection (LIDS) to develop SVM which has been used to distinguish between anomalous activities from normal activities in IoT. The aim of LIDS was reducing features to achieve better performance and higher accuracy.

The researchers introduced HIDS [28–30], which is an integration of SIDS and AIDS, as a solution to overcome the limitations mentioned in the above literature associated with AIDS, particularly its high false positive rate. Simon et al. [28] presented HIDS techniques based on deep learning to achieve optimal features in order to detect attacks in IoT using NSL-KDD dataset. The proposed algorithm has better performance and higher accuracy of 99.49% compared to the traditional models. Taher Azar et al. [29] proposed HIDS for satellite-terrestrial systems based on machine learning and deep learning to enhance the security of networks by effectively detecting vulnerabilities and cyber-attacks.

In the same context, Al-Yaseen et al. [30] integrated k-means and RF algorithms for the classification model using CNN and LSTM algorithms. The hybrid algorithm is implemented on Spark platform for applying classification models. Here, the purpose of deep learning algorithms is to learn hidden features of NSL-KDD and CIS-IDS2017 datasets. The proposed model generated an accuracy of 85.24% and 99.91% in NSL-KDD and CIS-IDS2017, respectively. Liu et al. [31] proposed a wrapped feature selection using a combination of Firefly algorithm and SVM for minimizing the number of features. The authors used SVM to develop a classification model and the Firefly algorithm to generate feature subsets. The proposed feature selection model is a powerful tool for reducing classification time and improving model performance. Furthermore, the results confirm that the performance produced a maximum classification accuracy of 78.89% against the NSL-KDD dataset.

Ravale et al. [32] presented a hybrid technique for intrusion detection using K Means for clustering and kernel function for classification. The proposed approach tried to minimize the number of attributes on a subset of KDD-99 dataset. The results proved that the presented approach provides better performance with low time complexity.

Table 1 Previous state-of-the-art techniques for intrusion detection systems

Refs.	SIDS	AIDS	HIDS	Dataset	Algorithm ML/DL	Metaheuristic algorithm	Evaluation criteria
[16]		√		KDDCup99, NSL–KDD, CICIDS-2017	PSO + RF	GWO	Accuracy, precision
[17]		√		NSL-KDD	DT	–	False positive rate
[18]		√		AWID real-world wireless	GA	GWO	Accuracy, F1-Score, recall, precision, and false alarm rate
[19]		√		Test-Bed	CNN	–	f- score
[20]		√		CTU-L3, Gas–water, AWID	LSTM	–	False-positive rate-false-negative rate
[21]		√		CTU-L3, Gas–water, AWID	AE	–	False-positive rate
[22]		√		NSL-KD	CCN + VAE + LSTM	–	Accuracy
[23]		√		Test-Bed	LSTM + RNN	–	Accuracy, F1-score, recall, precision
[24]		√		N-BaIO	CNN + LSTM	–	Accuracy
[25]			√	CICIDS2018, Edge_IIoT	CNN + LSTM	–	Accuracy
[26]			√	CIC-IDS 2017, UNSW-NB15, WSN-DS	CNN + LSTM	–	Accuracy, precision, detection rate, F1-score, false alarm rate
[27]			√	KDDCup 99	CNN + LSTM + RNN + GRU	–	Accuracy
[28]			√	NSL-KDD		–	Accuracy
[29]			√	UNSW-NB15 + STIN	RF + LSTM + RGU + ANN	–	Accuracy
[30]			√	NSL-KDD + CIS-IDS2017	CNN + LSTM + k-means + RF	–	Accuracy, true positive rate
[31]			√	NSL-KDD	SVM	–	Accuracy
[32]			√	KDD-99	K Means	–	Accuracy
[33]			√	KDD CUP 1999	RF	–	Delay
[34]			√	KDDTest, UNSW-NB15, CICIDS-2017	ensemble model	PSO	false positive rate
[35]			√	NSL-KDD	RF	PSO	true positive rate, false positive rate
[36]			√	Different dataset	SVM + ANN		Accuracy
[37]			√	UNSWNB-15	ELM	GWO	Accuracy
[38]			√	NSL-KDD	LR + DT		Accuracy
[39]			√	Bot-IoT	SVM + DT		Accuracy, false alarm rate
[40]			√	CICIDS2017	SVM + DT + RF		Accuracy, false alarm rate
[41]			√	KDD99	SVM	OLGWO	detection rate, false positive and false negative
[42]	√			Steam dataset	QSVM + QCNN		accuracy
[43]	√			CIC-DDoS2019	QSVM + ensemble model		accuracy, precision, recall, and F1-score
[44]		√		NSL-KDD, CSE-CIC-IDS2018	KNN	HOA	accuracy, precision
[45]	√			KDD99	GA	GWO	accuracy

Meanwhile, Indira et al. [33] utilized Salp Swarm Optimization (SSO) to find optimal features to improve the detection accuracy. Here, HIDS technique was implemented on Software Defined Wireless Sensor Network (SDWSN) to recognize abnormal behavior. In particular, the results confirmed better performance in terms of

delay, delivery ratio, and drop overhead against KDD CUP 1999 Dataset. Sequentially, Louk et al. [34] investigated a novel technique for network anomaly detection combining Gradient Boosting Machine (GBM) and bagging on different datasets. The authors used PSO to determine the most appropriate set of features. Moreover, GBM was applied as base for bagging model to enhance the performance of the network. Thus, the lower false positive rate was obtained at 1.59% and 2.1% for KDDTest + and KDDTest-21, respectively. Balyan et al. [35] introduced a new IDS model, namely HNIDS based on Enhanced Genetic Algorithm Particle Swarm Optimization (EGA-PSO) and Improved Random Forest (IRF). Here, HNIDS was implemented on two IDS datasets to find the most appropriate features and prevent malicious network. The results demonstrated that HNIDS model achieved a better solution than other methods.

Einy et al. [36] presented the metaheuristic model using fuzzy logic to avoid damage of malicious traffic based on Suricata IDS/IPS. They implemented machine learning models to detect different types of attacks such as SMB exploits, SQL injection attack, XSS, and brute force. The presented method was simulated using a web application and it was proven that it outperformed other strategies. Alzaqebah et al. [37] developed a feature selection technique that improved the performance of IDS using modified GWO (MGWO) against the UNSW-NB15 dataset. Further, a hybrid method of feature selection for wrapper-based and filter- based was implemented to achieve better accuracy. Here, the false positive rate and crossover error rate reached 27% and 28% respectively. On the Other hand, Khraisat et al. [39], presented a new technique based on C5 DT and SVM for improving the accuracy of HIDS. It was conducted in three steps; First, pattern matching was applied to find whether a test sample is normal or abnormal activity. Second, one class of SVM was used to learn from training samples. Finally, boosting techniques were utilized for improving prediction accuracy. In an effort to enhance the efficiency of intrusion detection, a new approach was explored in [41] using oppositional based Laplacian GWO along SVM to address intrusion detection. Opposition Based Learning (OBL) was an innovative concept in machine learning that has proven effective in expediting the search process. Laplacian GWO was employed for clustering, while SVM was utilized for classification. The implementation was carried out on the KDD99 dataset targeting four classes of attacks: Denial of Service (DoS), R2L, U2R, and Probing.

Khraisat et al. [42] presented the QCNN and QSVM technique to improve the feature selection process. The streaming dataset included 58 features such as average flag values, minimal and maximal packet lengths, mean values of packet length, and standard deviation. The authors employed QCNN to select the most significant features with higher probability. The proposed model was evaluated on the CIC-DDoS2019 dataset and compared with traditional techniques in terms of accuracy, precision, recall, and F1-Score. The results demonstrated that the training time was reduced by more than half compared to traditional SVM approaches. Meanwhile, the resolution of various optimization problems has witnessed the emergence of numerous metaheuristic algorithms.

Ghanbarzadeh et al. [44] introduced the Horse Herd Optimization Algorithm (HOA) to effectively select features for distinguishing between attack and normal behavior. To enhance horse movement and strike a balance between exploration and exploitation, HOA was integrated with quantum computing. The result showed that the presented model outperforms the traditional models in terms of accuracy, precision, and sensitivity against two datasets, NSL-KDD and CSE-CIC-IDS2018. Similarly, Tawhid et al. [45] introduced a hybrid IDS model to minimize a simplified energy model. The authors employed a hybrid GWO and GA to balance between exploration and exploitation in the search space.

3 The methodology and proposed model

This section provides a comprehensive explanation of the proposed hybrid QSVM-IGWO model for an advanced method of detecting cyber-attacks. The model is structured into distinct phases, each incorporating various functional components, such as preprocessing of online cyber-attack datasets and selecting important features. Then, the selected features are integrated using an appropriate technique to create an optimal feature set for cyber-attack detection. Next, a modified GWO algorithm is employed to enhance and train the fundamental QSVM model. Finally, the proposed hybrid QSVM-IGWO model can be applied to detect the intruders in the IoT network which outperforms conventional methods requiring data validation. Here, Fig. 2 illustrates the proposed model through three main phases, with each phase playing a significant role in enhancing overall performance. The intelligent QSVM-IGWO detection system is discussed in-depth below.

3.1 First phase: data preprocessing and features reduction

Data preprocessing and features reduction provide an essential part in the proposed QSVM-IGWO model. Any dataset usually contains hundreds of attributes representing hundreds of features that differ from application to application. There are some redundancies in these features and others out of the concerns. Therefore, these features need to

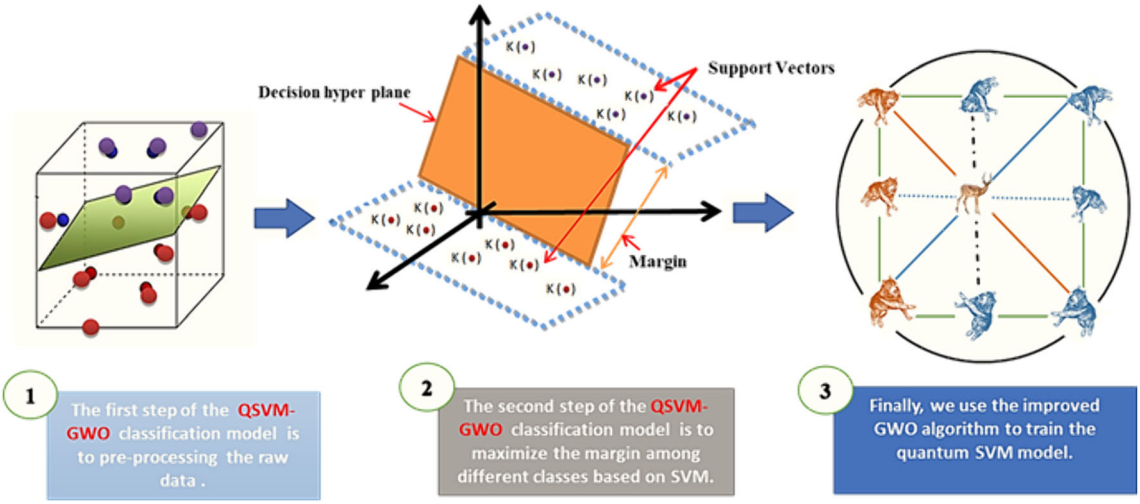


Fig. 2 The proposed QSVM-IGWO model

be reduced to remove the overhead and reduce the dimensions and calculations and therefore reduce the computational complexity [47]. Information Gain (IG) is one of the trusted models of feature subset selection concerning security in IoT which is used to obtain a small number of features [44, 45]. It is proven that the resulting probability distribution of the data classes using IG technique is close to the original distribution obtained using all given features [48]. Here, IG is calculated using Eq. (1) for extracting IoT security features based on a specific threshold which is equal to 0.2 [45].

$$IG(t) = -\sum_{i=1}^{m} P(c_i) log log P(c_i) + P(t) \sum_{i=1}^{m} P(t) log P(t) + P\prime(t) \sum_{i=1}^{m} P\prime(t) log P\prime(c_i|t) \tag{1}$$

where c_i represents i class, $P(c_i)$ is the probability that an arbitrary instance corresponds to a class c_i, $P(t)$ and $P\prime(t)$ are the chances of the feature appearing in a randomly chosen pattern, m is the class number, and $P(c_i|t)$ is the probability that a randomly picked instance corresponds to a class c_i if instance holds that feature. If the resulted value of the IG is less than that threshold, the feature is ignored.

3.2 Second phase: quantum SVM algorithm

Machine learning is concerned with the creation of algorithms that can learn from data and generate meaningful forecasts. Here, SVM is a very powerful machine learning algorithm that is used to classify new patterns. It converts inputs to feature space and turns the required nonlinear problem into a linear separation problem by constructing a hyperplane. Moreover, SVM calculates the inner product of data points in the form of kernel function. Assume that dataset $T = \{(x_1,y_1), (x_2,y_2), (x_3,y_3), \ldots\ldots,(x_m,y_m)\}$is divided into the training set $T_r = \{(x_1, y_1),..., (x_n, y_n)\}$ and testing set $T_s = \{(x_1, y_1),..., (x_{m-n}, y_{m-n})\}$ with n less than m. The hyperplane is calculated using Eq. 2)) with orientation which is controlled by weight vector w and constant b.

$$min. \|w\|_L + C \sum_{i=1}^{n} \in_i$$
$$s.t. \geq 0 \text{ and } y_i(w.\varphi(x_i) + b) \geq 1 - \in_i \ \forall i = 1, 2, ..., n \tag{2}$$

where ||w|| is the norm vector, $\varepsilon_i \geq 0$ is slack variable and $\varphi(x_i)$ is the nonlinear function that converts the inputs x_i into the feature space in the dimension of n training dataset. The inner product $w.\varphi(x_i)$ can be expressed by a kernel function as follows [49]:

$$L(A) = \sum_{i=1}^{n} A_i - \frac{1}{2} \sum_{i=1}^{n} \sum_{j=1}^{n} A_i A_j y_i y_j K(x_i, x_j)$$
$$s.t \sum_{i=1}^{n} A_i y_i = 0 \text{and} 0 \leq A_i \leq C \forall i = 1, 2, ..., n \tag{3}$$

where A is a weight with upper constraint of C, K expressed as kernel function, and class label y ∈ {± 1} given a corresponding input x ∈ X, where samples (x, y) from X × Y.

In recent years, several studies [45, 46] have presented the drawbacks of SVM especially those that involve a high degree of complexity, multi-modal functions, or discrete search spaces. Subsequently, QSVM [46] is introduced to enhance computational speed and data processing capabilities which offers advantages over classical SVM for certain types of optimization problems. QSVM is part of the emerging field of quantum machine learning, where quantum computing technologies are used to enhance the

efficiency of machine learning techniques. QSVM is shown in Fig. 3.

Quantum SVM has to follow the subsequent steps:

Firstly, the classical training data X is converted into a quantum data point $\Phi(\vec{x})$ where Φ is any classical function defined as:

$$\Phi_1(\vec{x}) = x_1 \tag{4}$$

$$\Phi_{1,2}(\vec{x}) = (\pi - x_1)(\pi - x_2) \tag{5}$$

Secondly, the classical function can be converted using quantum circuit as follows [46]:

$$V(\Phi(\vec{x})) = U(\Phi(\vec{x})) \otimes H^r \tag{6}$$

where H^r is the conventional Hadamard gate for each qubit and r is the number of qubits. The feature map can be calculated for r = 2 qubits with the classical data vector $\vec{x} = (x_1, x_2)$ as follows:

$$U(\Phi(\vec{x})) = \exp\left(i\{x_1P_1 + x_2P_2 + (\pi - x_1)(\pi - x_2)P_1P_2\}\right) \tag{7}$$

$$\text{In general, } U(\Phi(\vec{x})) = exp\, exp\left(i\sum_{j=1}^{r}\theta_j\Phi_T(x)\prod\sigma_{j\in\{X,Y,P\}}\right) \tag{8}$$

where θ is the rotation element, which affects phase rotation based on values of features. The σ depicts the X, Y, and P unitary Pauli rotation transformation.

Thirdly, a quantum circuit of depth 2 can be presented by repeating the approximation of Eq. (6) two times and becomes as follows:

$$V(\Phi(\vec{x})) = U(\Phi(\vec{x})) \otimes H^{\mathrm{r}} \otimes \mathrm{U}(\Phi(\vec{x})) \otimes H^{\mathrm{r}} \tag{9}$$

Finally, the quantum kernel $K(x_i, x_j)$ is extracted from the quantum circuit to be fed into the classical SVM algorithm $x_i, x_j \in T$. Here, Eq. (3) can be transformed to estimate the fitness function of QSVM as follows:

$$L(\theta) = \sum_{i=1}^{n}\theta_i - \frac{1}{2}\sum_{i=1}^{n}\sum_{j=1}^{n}\theta_i\theta_j y_i y_j K(x_i, x_j)$$
$$s.t. \quad \sum_{i=1}^{n}\theta_i y_i = 0 \text{and } 0 \le \theta_i \le C \ \forall i = 1, 2, \ldots, n \tag{10}$$

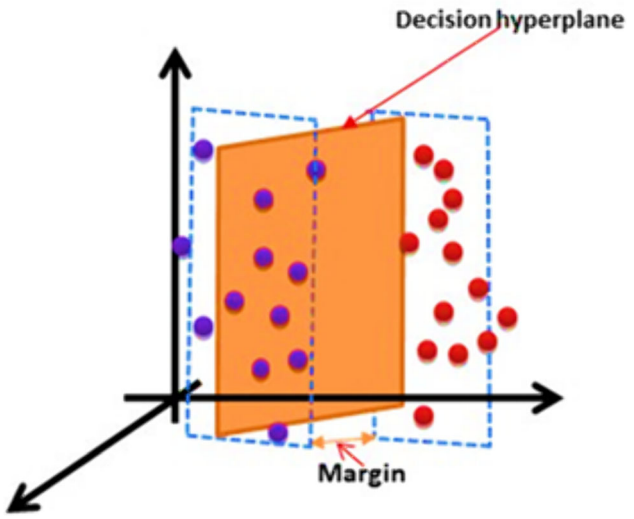


Fig. 3 The Quantum SVM

3.3 Third phase: IGWO algorithm

GWO algorithm has several characteristics that make it the greatest competitor for optimization problems, including its simplicity, ease of implementation, scalability, flexibility, uncomplicated computations, and, most importantly, delivery of a high rate of convergence and degree of exploitation. Nevertheless, it suffers from some limitations leading to premature convergence [50]. Firstly, it is based on mathematical equations, which requires a long processing time. Secondly, it sticks easily to local optima. Finally, it suffers from a lack of exchanged information across search agents. Consequently, it provides poor variety. For these reasons, several studies have been conducted on hybrid techniques based on GWO or improved it to overcome its poor characteristics. The first appearance of it was by Davahli et al. in 2020 [51]. The GWO algorithm assigns three leader wolves (α, β, and δ) based on their fitness values as the best solutions. They lead the rest of the wolves (ω) to find the global solution [52].

In the search space, each α wolf can be a solution for the problem. To hunt a prey (find the optimum solution), three procedures are carried out; searching prey, encircling prey and attacking prey as shown in Fig. 4. As long as the dismissal requirement is met, the encircling and attacking prey processes are repeated [53].

The encircling prey stage begins by assuming two wolves in the search space, then update the position of one of the two wolves according to the other one as follows: [51]

$$R(i+1) = R(i) - \Lambda \,.\, H \tag{11}$$

$$H = \left| G \,.\, R_{pp}(i) - R(i) \right| \tag{12}$$

where R is the wolf location, R_{pp} represents the location of the prey, i is the iteration number and Λ, G are the coefficient vectors calculated as follows:

$$\Lambda = 2\Delta \,.\, d1 - \Delta \tag{13}$$

$$G = 2 \,.\, d_2 \tag{14}$$

where Δ drops from 2 to 0, $d_1$and d_2 are random values between [0,1]. The factor Δ is updated in every iteration as follows:

$$\Delta = 2 - i\left(\frac{2}{MaxCycle}\right) \tag{15}$$

where *MaxCycle* is the total allowed iterations numbers.

At the beginning, it is assumed that α, β, and δ know the prey position. So the other wolves ω are obliged to follow them. The equations from Eq. (16) to Eq. (22) outline the hunting technique as follows:

$$R_1 = R_\alpha(i) - \Lambda_1.H_\alpha \tag{16}$$

$$R_2 = R_\beta(i) - \Lambda_2.H_\beta \tag{17}$$

$$R_3 = R_\delta(i) - \Lambda_3.H_\delta \tag{18}$$

where H_α, H_β, and H_δ are obtained as follows:

$$H_\alpha = |G_1.3_\alpha - 3| \tag{19}$$

$$H_\beta = |G_2.3_\beta - 3| \tag{20}$$

$$H_\delta = |G_3.3_\delta - 3| \tag{21}$$

The next iteration solution can be determined as follows:

$$R(i+1) = \frac{(R_1 + R_2 + R_3)}{3} \tag{22}$$

When the maximum iteration is achieved, wolves' specifying positions are stopped. When the prey stops moving, the attacking process begins. This may be accomplished analytically by decreasing the value of Δ throughout the duration of iterations, which controls the exploration and exploitation based on the algorithm. As mentioned in the GWO algorithm, Δ reduces linearly from 2 to 0 as in Eq. (15). However, the algorithm's convergence mechanism is not linearly convergent. Subsequently, a tangent trigonometric function-based nonlinear convergence factor is used as follows [54]:

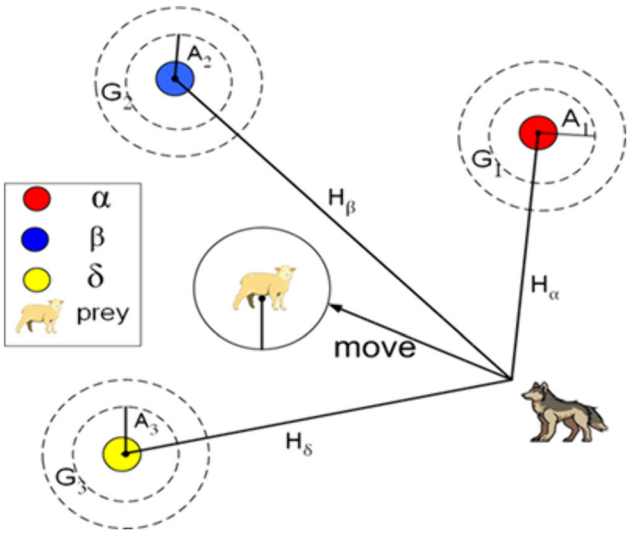


Fig. 4 The improved GWO Algorithm

$$\Delta = \Delta_{initial} - \left(\Delta_{initial} - \Delta_{final}\right) \times \tan\left(\frac{1}{\varepsilon} - \frac{1}{MaxCycle}\pi\right) \tag{23}$$

where $\Delta_{initial}$, Δ_{final} are the starting and ending values of Δ respectively, and ε is the modification factor, practically, take ε = 4. By using this modification, the convergence becomes better and the overall performance is improved [54]. The details of IGWO are explained in Algorithm 1.

Algorithm 1: IGWO Algorithm

1. Initialize the wolf population size N and MaxCycle.
2. Initialize the parameters Λ, G and Δ.
3. **For** *j =1* to MaxCycle
4. Evaluate the fitness function for each wolf.
5. Select the first best solution as R_α, the second-best solution as R_β and the third best solution as R_δ.
6. **For** *i =1 to N* // for all population
7. R_1, R_2 and R_3 are calculated from Eq. (16) to Eq. (21)
8. Calculate $R(i+1) = \frac{(R_1 + R_2 + R_3)}{3}$ and assign to the best solution.
9. **End For**
10. The parameters are updated according to Eq. (23)
11. **End For**
12. Display R as the best solution
13. **End**

3.4 The hybrid QSVM-IGWO

The integration between QSVM and IGWO aims to increase the efficiency of solving complex optimization and classification problems, particularly in the cyber-attack detection sector. The core idea behind this hybrid approach

is to harness the power of quantum computing within the SVM technique providing QSVM. Furthermore, it incorporates metaheuristic optimization through IGWO to fine-tune the hyper parameters of QSVM, ultimately enhancing its performance. Subsequently, the data undergoes a transformation, being mapped to a higher-dimensional quantum feature space through quantum operations. This step is pivotal as it leverages quantum computing principles. Here, the flowchart for QSVM-IGWO is presented in Figure 5**.** Quantum kernels come into play here, facilitating the computation of inner products between data points within the quantum feature space. These quantum kernels have the capability of capturing intricate relationships between data points that might be challenging to compute efficiently in classical SVMs. The next stage involves training the quantum SVM using the transformed data and quantum kernels.

The objective of the hybridization is to identify the optimal hyperplane within the quantum feature space, effectively separating data points belonging to distinct classes. The QSVM model is trained on a designated training dataset which is known as intrusion or normal data, striving to pinpoint the hyperplane that offers the most effective class separation. This process occurs in parallel with the IGWO optimization process, which is designed to refine the hyper parameters or configurations of the QSVM model through the IGWO population. The IGWO population explores various combinations of QSVM parameters with the aim of enhancing the performance of the QSVM. Upon successful training of the QSVM, it becomes capable of classifying new, unseen data based on the hyperplane and support vectors that were determined during the training phase. These steps are described in Algorithm 2.

The essential part of QSVM involves the classical preprocessing steps, such as feature mapping and kernel computation. The time complexity of these steps depends on the algorithm that is used for kernel computation. The overall time complexity of QSVM is the summation of the time complexities of both the classical and quantum parts. If we denote the classical preprocessing time complexity as $T_{classical}$ and the quantum part time complexity as $T_{quantum}$, then the overall time complexity (T_{total}) can be expressed as: $T_{total} = T_{classical} + T_{quantum}$. The complexity of both $T_{classical}$ and $T_{quantum}$ is $\boldsymbol{O(M.N)}$. On the other hand, the overall time complexity of the IGWO algorithm is determined by the number of iterations multiplied by the time

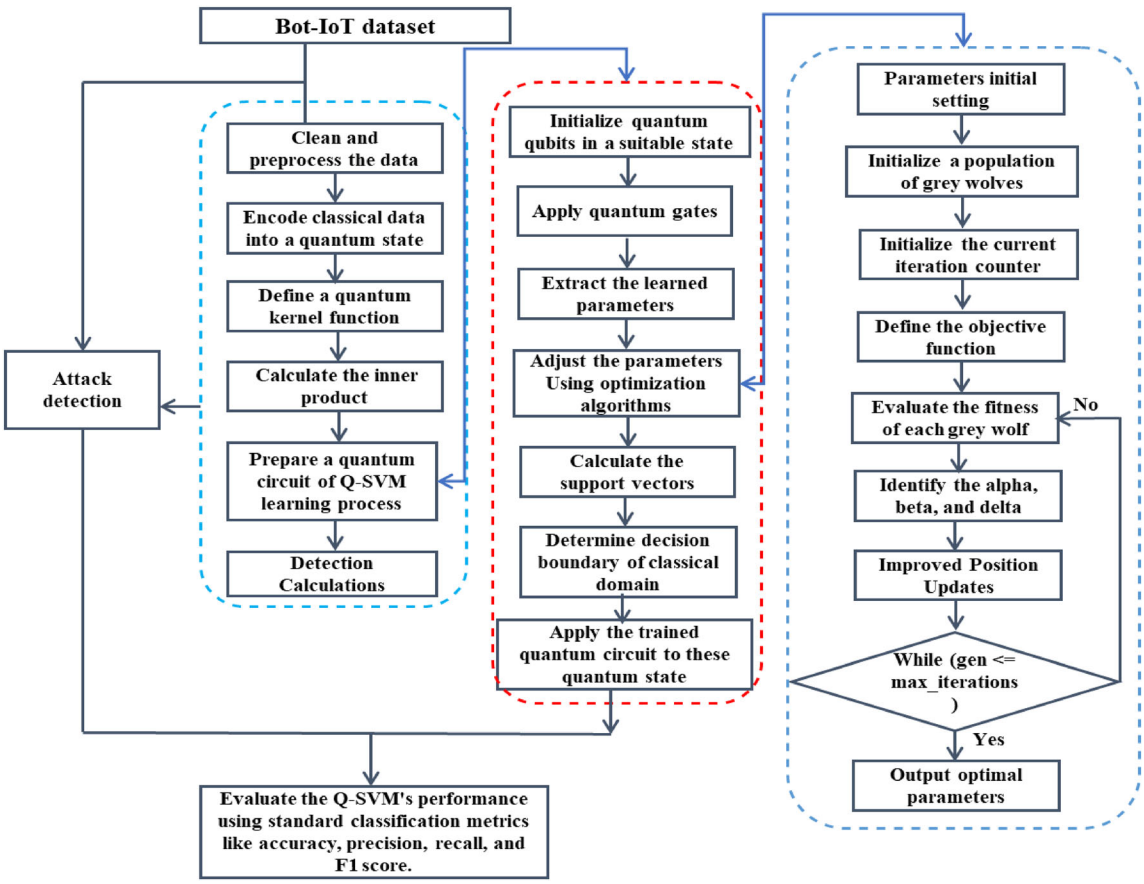


Fig. 5 The flowchart of the proposed QSVM—IGWO model

complexity of each iteration. If the number of iterations is denoted as MaxCycle, and the time complexity of an iteration is denoted as *T*iter, then the overall time complexity (*T*total) can be expressed as: *T*total = MaxCycle × *T*iter.

techniques. Table 2 shows the initial parameters for the competitive classification models KKN, LR, DT, and RF.

Algorithm 2: The proposed Hybrid QSVM and IGWO

1. **Step 1:** Data Preparation.
2. **Remove** redundant data from the dataset.
3. **Select** the required features from the feature list according Eq. (1).
4. **Divide** the data into training and test dataset with a ratio 4:1.
5. **Step 2:** Data Encoding into Quantum space using QSVM.
6. **Search** for the pattern in the Signature intrusion list saved in memory.
7. **If** it is found in the list
8. **Then** Announce it intrusion and process the next pattern from the dataset.
9. **End if**
10. **Step 3:** QSVM Algorithm.
11. **Use** QSVM to have Kernel Function to specify the margin of the classification from Eq. (3) to Eq. (8)
12. **Step 4:** IGWO Algorithm.
13. **Apply** IGWO algorithm 1 to assign all the dataset into four groups according to fitness values in order to train QSVM model
14. **Step 5:** Apply the updated Kernel function to classify the packet.
15. **If** the packet is intrusion // Anomaly based IDS (AIDS)
16. Announce it is intrusion and save it to use later in other detections (in the signature list).
17. **Else If**
18. Announce the packet is normal and safe.
19. **End If**
20. **Step 6:** Return list of intrusion and normal packets.

4 Experimental results and discussion

This section provides a detailed description of the experiments that were conducted to evaluate the effectiveness of the proposed QSVM-IGWO model in comparison to the existing intrusion detection systems (IDSs). The studies were carried out using a 64-bit Desktop Windows operating system. The system includes an Intel i7-3540 processor running at 3.0 GHz and 16 GB of RAM.

There are a number of parameters in the proposed QSVM-IGWO model that need to be initialized before optimization. QSVM-IGWO was trained using grid search

4.1 Bot-IoT dataset and evaluation metrics

The suggested model uses the well-known Bot-IoT dataset [53]. This dataset is partitioned into a 80% training set and a 20% testing set. In this dataset, the features attack has two values: attack traffic is 1 and normal traffic is 0. As illustrated in Table 3, attack aspects are divided into four categories: DoS, DDoS, reconnaissance, and information theft. Furthermore, with over 53,000,000 records, each entry is classified as either normal or attack. Here, the suggested detection model performance is evaluated using confusion matrix, accuracy, precision, recall, and F1 score. The following defines these metrics:

Table 2 The Initial parameters of the classification models

Models	Parameters
KNN	num _neighbors = 1–50, leaf size = 1–60, power parameter = Manhattan distance
LR	random state = 30, max_iteration = 1000
DT	maximum depth = 30, criterion = 'gini', plitter = 'best', max, min_samples_split = 2, min_samples_leaf = 1
RF	num _trees = 100–1000, maximum depth = 3–11, random state = 30
QSVM-IGWO	num _wolves = 100, min range = 30, max range = -30, initial population = 100, Crossover Rate = values between 0.7 and 0.9, num_qubits = 2, depth = 3, max fun = 100, shots = 1024

Table 3 Features of Bot-IoT dataset

Feature	Data type	Values	Feature Description
pkSeqID	Discreet	distinct values from 1,650,261 to 3,577,361	Identifier for a specific row
Sbytes	Discreet	distinct values from 42 o 754,981	Byte count from the source to the destination
Sport	Discreet	distinct values from − 1 to 65.5 k	Number assigned to the source port
Dbytes	Discreet	distinct values from 0 to 34.2 m	Packet count from the destination to the source
TnBPSrcIP	Discreet	distinct values from 70 to 220 m	Aggregate byte count per source IP
TnP_PDstIP	Discreet	distinct values from 1 to 226 k	Cumulative packet count per destination IP
Proto	nominal	Tcp, udp, etc	A textual representation of transaction protocols
N_IN_Conn_P_SrcIP	Discreet	distinct values from 0 to 100	The count of incoming connections per source IP
N_IN_Conn_P_DstIP	Discreet	distinct values from 0 to 100	The count of incoming connections per destination IP
Bytes	Discreet	distinct values from 60 to 71.8 m	Aggregate byte count within the transaction
Pkts_P_State_P_Protocol_P_SrcIP	Discreet	distinct values from 1 to 118 k	The count of packets organized by flow states and protocols for each source IP
AR_P_Proto_P_DstIP	Discreet	distinct values from 0 to 182 k	The mean rate for each protocol per destination IP
Stddev	Discreet	distinct values from 0 to 2.5	The variability measure of combined records
Dpkts	Discreet	distinct values from 0 to 35 k	Packet count from the destination to the source
Rate	Discreet	distinct values from 0 to 90.9 k	The overall packet rate per second within a transaction
Saddr	nominal	192.168.100.147, 192.168.100.148, etc	Source IP address
Drate	Discreet	distinct values from 0 to 2.18 k	Packets per second from the destination to the source
Pkts	Discreet	distinct values from 1 to 70.1 k	Cumulative packet count within the transaction
Srate	Discreet	distinct values from 0 to 1000 k	Packets per second from the source to the destination
TnBPDstIP	Discreet	distinct values from 70 to 220 m	Cumulative byte count per destination IP
Pkts_P_StateP_Protocol_P_DestIP	Discreet	distinct values from 1 to 113 k	The count of packets organized by flow states. and protocols for each destination
Spkts	Discreet	distinct values from 1 to 35 k	Packet count from the source to the destination
Attack	nominal	0 or 1	Class label assignment: 0 indicates Normal traffic, while 1 denotes Attack Traffic
Category	nominal	DoS, DDoS, reconnaissance, and information theft	Traffic category

- Accuracy indicates the ratio of correctly predicted attack over the total requests. Here, the symbols TP, TN, FP, FN, and FP denote true positive, true negative, false positive, and false negative, respectively.

$$Accuracy = \frac{TP + TN}{TP + FP + FN + TN} \tag{24}$$

- Precision gives the information about the ratio of correctly predicted malicious requests over the total predicted malicious requests as follows:

$$Precision = \frac{TP}{TP + FP} \tag{25}$$

- Recall denotes the ratio of correctly predicted malicious requests over the total malicious requests and is defined as follows:

$$Recall = \frac{TP}{TP + FN} \tag{26}$$

- F1-Score can be measured from the mean of precision and recall as follows:

$$F1 = \frac{2 \times (Recall \times Precision)}{Recall + Precision} \tag{27}$$

4.2 Experimental analysis

The proposed QSVM-IGWO detection model is evaluated using the BoT-IoT dataset. Additionally, it is compared to four conventional machine learning models, namely KNN, DT, LR, and RF, through the utilization of a tenfold cross-validation. The accuracy, sensitivity, and specificity performance of the KNN, DT, LR, and RF models, as well as

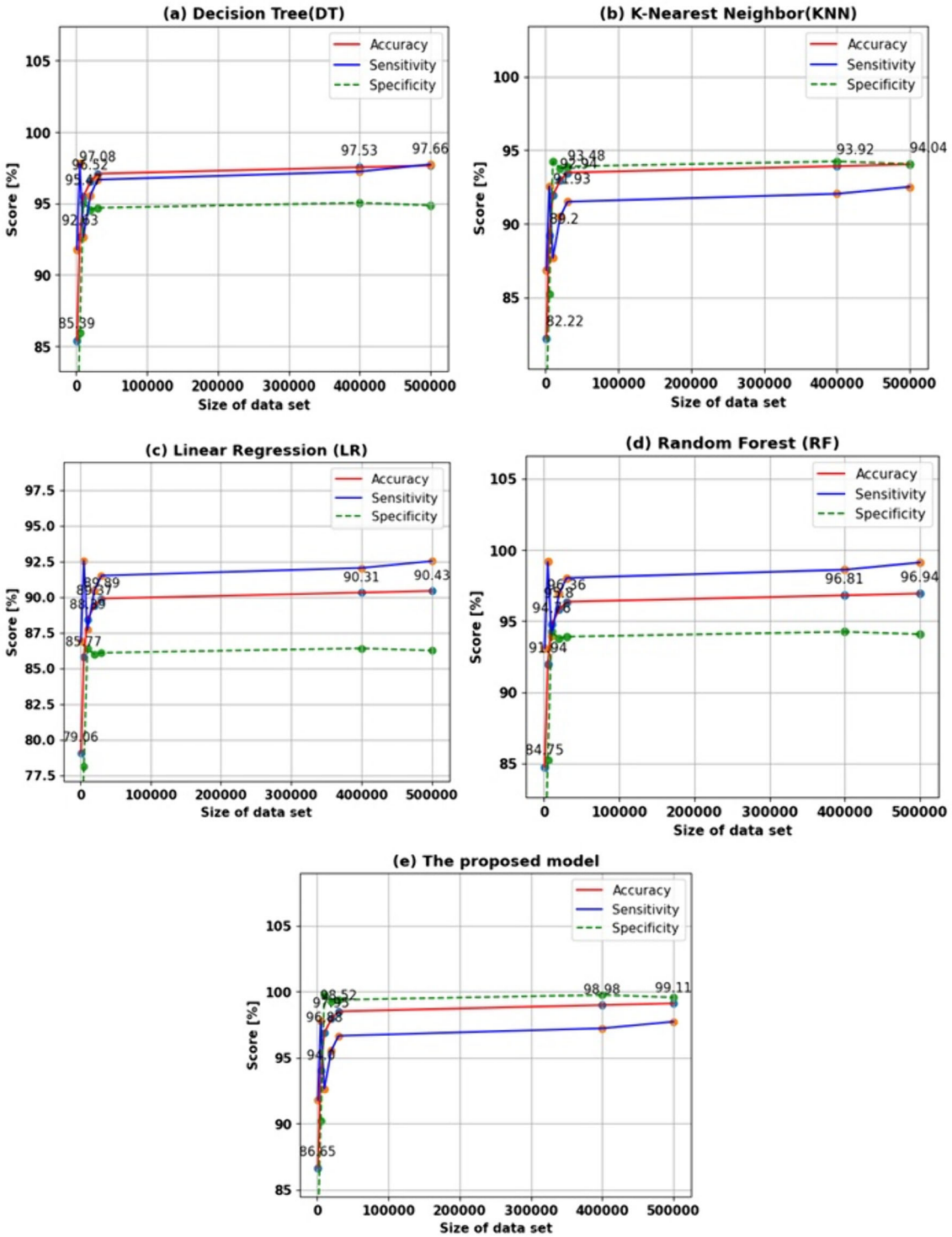


Fig. 6 The accuracy, Sensitivity and Specificity of **a** DT, **b** KNN, **c** LR **d** RF, and **e** the proposed QSVM-IGWO using BoT-IoT dataset

the suggested model, are displayed graphically in Fig. 6a–e. It is important to note that the LR classifier demonstrates a low level of reliability, offering a minimum accuracy of only 90.43%. Both RF and KNN have achieved a minor improvement in their accuracy, with the former reaching 96.64% and the latter reaching 94.04%. Besides, the DT was able to identify the attacks with a precision of 97.66%, but the proposed model outperformed it with a precision of 99.11%.

Table 4 Average performance including all attacks of BoT-IoT dataset

BoT-IoT dataset						
Size of data	Classifiers	KNN (%)	LR (%)	DT (%)	RF (%)	QSVM-IGWO (%)
10,000	Measures					
	Train accuracy	91.23	88.23	95.24	93.67	95.56
	Test accuracy	88.33	88.56	96.45	94.09	96.09
	F1-Score	90.71	89.79	94.79	94.12	96.78
	Precision	91.22	88.13	95.12	93.56	96.34
	Recall	91.13	88.45	95.09	94.89	97.89
20,000	Train accuracy	91.34	88.89	95.78	94.89	97.65
	Test accuracy	91.67	88.98	95.34	93.33	95.22
	F1-Score	88.89	88.45	96.67	94.56	96.88
	Precision	90.80	89.89	94.89	94.12	96.87
	Recall	91.34	88.23	95.35	93.56	96.19
30,000	Train accuracy	91.99	89.43	96.12	95.78	98.89
	Test accuracy	91.87	88.67	95.67	94.23	96.45
	F1-Score	89.45	89.50	96.78	95.68	97.78
	Precision	91.54	89.89	95.34	94.89	97.36
	Recall	91.89	89.23	96.11	94.21	97.17
40,000	Train accuracy	93.33	90.32	97.55	96.48	98.78
	Test accuracy	92.67	89.45	96.12	95.12	97.34
	F1-Score	91.25	90.46	97.33	96.33	98.45
	Precision	93.45	90.58	96.89	95.38	97.99
	Recall	93.44	90.01	97.16	95.56	98.67
50,000	Train accuracy	94.04	90.43	97.66	96.94	99.11
	Test accuracy	94.66	91.66	98.12	97.67	98.79
	F1-Score	95.56	89.67	95.67	96.67	97.78
	Precision	95.33	90.27	96.33	96.87	99.45
	Recall	95.78	91.54	96.67	97.83	99.34

Table 4 provides a summary of the performance of LR, DT, RF, KNN and the proposed QSVM-IGWO model based on the BoT-IoT dataset. It is clear that the proposed QSVM-IGWO model consistently demonstrates the highest degree of accuracy across a wide variety of dataset sizes. For a small dataset size (10,000 instances), LR and KNN achieve low test accuracy, reaching minimum values of 88.23% and 91.23%, respectively. In contrast, DT shows some improvement with a test accuracy of 95.24%, while the proposed model outperforms the others with the maximum test accuracy of 95.56%. For a larger dataset size (50,000 instances), LR and KNN achieve the least test accuracy of 90.43% and 94.04%, respectively, while DT achieves moderate results with an average training accuracy of 97.66%. However, the proposed classifier produces the highest average training accuracy of 99.11%. On the other hand, when examining F1-Scores, LR and KNN give the minimum values of 89.67% and 95.56%, respectively, while DT and RF achieve slightly higher F1-Scores with averages of 95.67% and 96.67%, respectively. The proposed model demonstrates superior performance with the most effective result, achieving the best F1-Score of 97.78%.

In the same context, as shown in Table 4, a detailed average Recall analysis was performed across several models to compare the proposed QSVM-IGWO to existing approaches. For a small dataset size (10,000 instances), both LR and KNN models achieve the minimal values of average Recall at 88.45% and 91.13%, respectively. Meanwhile, RF and DT models improve average Recall with slight increases reaching 94.89% and 95.09%, respectively. However, the proposed model shows superior performance by attaining the maximum average Recall of 99.34% under a larger dataset size (50,000 instances). Consequently, it can be deduced that the proposed model exhibits high effectiveness in terms of train accuracy, test accuracy, F1-score, Precision, and Recall under a larger dataset size (50,000 instances), while it keeps the performance at a constant level with a decrease in data size.

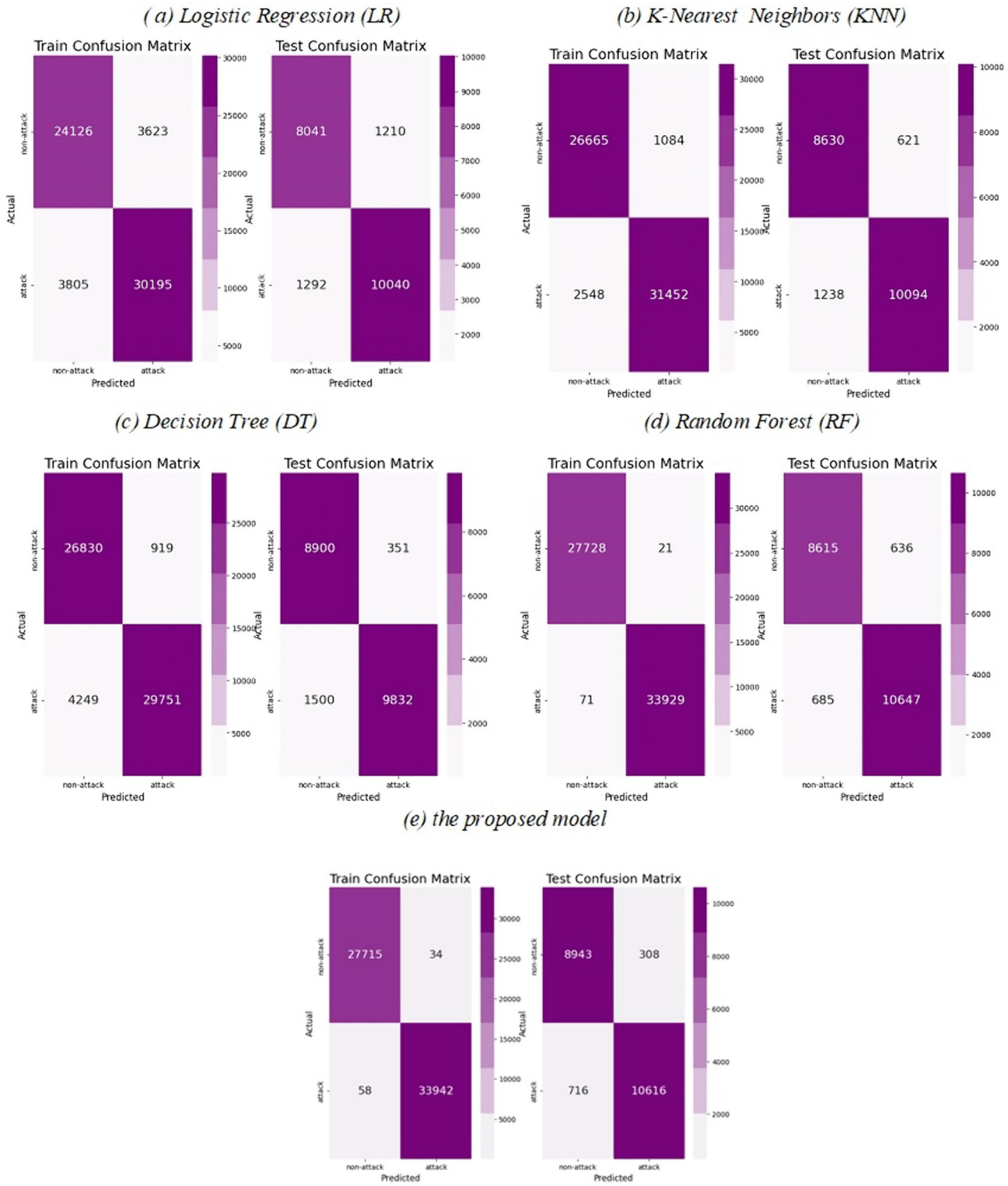


Fig. 7 Quantitative results comparisons **a** LR, **b** KNN, **c** DT, **d** RF, and **e** QSVM-IGWO

Figure 7 illustrates the distribution of each class in the training and testing data by the proposed model and the competitive algorithms LR, DT, RF, and KNN against the BoT-IoT dataset. It emphasizes the superior performance of the proposed model's confusion matrix compared to all competitive models. Specifically, the proposed model correctly classifies 33,942 attack requests while misclassifying only 58 non-attack requests as attacks. Furthermore,

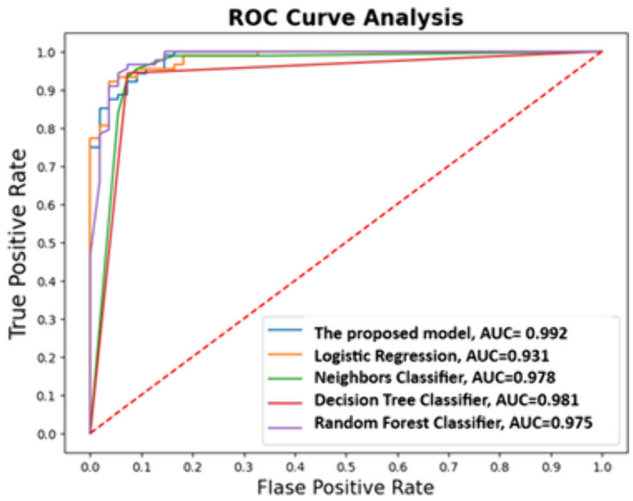


Fig. 8 The ROC curves analysis based on using BoT-IoT dataset

it accurately identifies 27,715 non-attack requests and misclassifies only 34 non-attack requests as attacks. Concerning the ROC curve, Fig. 8 demonstrates that the proposed model is the top classifier in this regard as well, achieving a result close to 99%. On the other hand, the second-best classifier is DT with a score of 98%, while LR has the lowest ROC at 93%.

Table 5 shows the superiority of the proposed QSVM-IGWO algorithm comparing with others. Ayubkhan et al. used auto-encoder and LightGBM algorithm to classify IoT traffics achieving 97.43% accuracy. Emil Selvan et al. [56] proposed a novel model, namely FACVO-DNFN, to predict the attacks in IoT networks using Bot-IoT data set achieving 92% accuracy and 86.48% Precision. It is obvious that the accuracy (96.13%), Precision (93.56%), Recall (94.23%), and F1 score (0.95%) achieved by QSVM-IGWO are better than those obtained by other competing algorithms.

Table 6 provides a detailed result of the F1-score for each category achieved by the proposed models and traditional algorithms LR, DT, RF, and KNN based on BoT-IoT dataset. Notably, the F1-Score for each category obtained by the proposed QSVM-IGWO outperforms the competitive algorithms. For the Information theft category, the F1-Scores of KNN, LR, DT, RF, and the proposed model are 89.58%, 81.48%, 85.46%, 93.89%, and 94.09% respectively. In comparison to LR, DT, RF, and KNN, the proposed model exhibits improvements in the F1-Score for Information theft by approximately 4.51%, 12.42%, 3.44%, and 0.2%, respectively. Additionally, the mean F1-Scores of KNN, LR, DT, RF, and the proposed model are 94.97%, 88.86%, 95.23%, 96.49%, and 97.48% respectively. The proposed model achieves percentage increases of approximately 2.51%, 8.62%, 2.25%, and 0.99% for the mean F1-Score, compared to LR, DT, RF, and KNN, respectively.

Table 5 Comparison of proposed model with other existing works

References	Datasets	Model	Accuracy	Precision	Recall	F1-Score
Louk et al. [34]	UNSW-NB15	PSO	–	92.93%	93.84%	93.38%
	KDDTest			65.87%	94.00%	73.325
Balyan et al. [35]	NSL-KDD	EGA-PSO	88.14%	82.86%	90.44%	70.10%
Alzaqebah et al. [37]	UNSWNB-15	MGWO	80.93%	–	–	78.08%
Ayubkhan et al. [54]	Bot-IoT	autoencoder and LightGBM	97.43%	–	–	–
Adeel et al. [40]	CICIDS2017	Linear SVM	85.56	–	–	–
Khraisat et al.[42]	Steam dataset	QSVM + QCNN	98	–	–	–
Sharma et al. [55]	Bot-IoT	DPNN	94%	–	–	–
Emil Selvan et al. [56]	Bot-IoT	FACVO-DNFN	92%	86.48%	–	–
The proposed model	Bot-IoT	QSVM-IGWO	99.11	99.45	99.34	97.48

Table 6 the detailed F1-Score of each category obtained by the proposed model competitive algorithms LR, DT, RF and KNN against the BoT-IoT dataset

Class	KNN (%)	LR (%)	DT (%)	RF (%)	QSVM-IGWO (%)
DoS	94.78	91.77	96.31	97.56	98.17
DDoS	98.64	95.67	98.74	98.45	99.78
Reconnaissance	96.79	86.32	95.22	96.08	97.89
Information theft	89.58	81.67	90.65	93.89	94.09
Mean	94.97	88.86	95.23	96.49	97.48

5 Conclusion and future works

This paper presents a hybrid QSVM-IGWO model for IoT cyber-attack detection. The suggested model compares harmful data packets to signature intrusion lists to protect the IoT network. It uses QSVM and IGWO to increase detection and reduce false positives. First, the proposed QSVM-IGWO model splits the dataset into 80% training and 20% testing. It then uses the QSVM algorithm to select the kernel function and find the best binary classification result. Finally, the IGWO tests different QSVM parameters to improve model performance. The proposed QSVM-IGWO is compared to recent detection models against the Bot-IoT dataset. The proposed attack detection model is also tested using cutting-edge approaches including LR, DT, RF, and KNN. Experimental results demonstrate that the proposed QSVM-IGWO model achieved training accuracy of 99.11%. Furthermore, the proposed model outperforms the detection of attack and non-attack requests considered in this research in terms of testing accuracy, Recall, Precision, F1 score, and ROC curve. Accordingly, the mean F1-Scores of KNN, LR, DT, RF, and the proposed model are 94.97%, 88.86%, 95.23%, 96.49%, and 97.48% respectively.

Further integration of machine learning and artificial intelligence techniques is recommended for future works to enhance the accuracy and efficiency of cyber-attack detection. This includes the development of advanced anomaly detection algorithms and predictive models to identify new and evolving threats. Improved behavioral analysis to understand the normal patterns of IoT devices and detect anomalies that may indicate a cyber-attack. This involves creating more sophisticated models that can adapt to changing behaviors and recognize subtle deviations.

Author contributions All Authors contributed equally to this work and approved the final manuscript.

Funding Open access funding provided by The Science, Technology & Innovation Funding Authority (STDF) in cooperation with The Egyptian Knowledge Bank (EKB). Funding Open access funding provided by The Science, Technology & Innovation Funding Authority (STDF) in cooperation with The Egyptian Knowledge Bank (EKB).

Data availability Not applicable.

Declarations

Competing interests The authors declare that they have no competing interests.

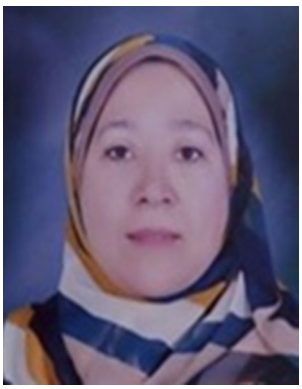
References

1. Elrawy, M.F., Awad, A.I., Hamed, H.F.A.: Intrusion detection systems for IoT-based smart environments: a survey. J. Cloud Comput. Adv. Syst. Appl. **7**, 21 (2018)
2. Aghili, S.F., Mala, H., Shojafar, M., Peris-Lopez, P.: LACO: lightweight three-factor authentication, access control and ownership transfer scheme for E-health systems in IoT. Future Gener Comput Syst. **96**, 410–424 (2019)
3. Krishna, E.S.P., Thangavelu, A.: Attack detection in IoT devices using hybrid metaheuristic lion optimization algorithm and firefly optimization algorithm. Int. J. Syst. Assur. Eng. Manag. (2021). https://doi.org/10.1007/s13198-021-01150-7
4. Shah, S.A.R., Issac, B.: Performance comparison of intrusion detection systems and application of machine learning to snort system. Futur. Gener. Comput. Syst. **80**, 157–170 (2018)
5. Verdejo, J.D., Calle, J.M., Alonso, A.E., Alonso, R.E., Madinabeitia, G.: On the Detection capabilities of signature-based intrusion detection systems in the context of web attacks. Appl. Sci. **12**(2), 1–16 (2022)
6. Neminath, H., Suryanarayanan, V.: False alarm minimization techniques in signature-based intrusion detection systems: a survey. Comput Commun. **49**, 1–17 (2014)
7. Kumar, V., Sangwan, O.P.: Signature based intrusion detection system using SNORT. Int. J. Comput. Appl. Inf. Technol. **1**(3), 35–41 (2012)
8. Meng F., Fu Y., Lou F., Chen Z.: An effective network attack detection method based on kernel PCA and LSTMRNN, International Conference on Computer Systems, Electronics and Control (ICCSEC), 2017
9. Ingre, B., Yadav A.: Performance Analysis of NSL-KDD dataset using ANN, 2015 International Conference on Signal Processing and Communication Engineering Systems, 92–96 (2015)
10. Qureshi, A., Larijani, H., Ahmad, J., Mtetwa, N.: A heuristic intrusion detection system for internet-of-things (IoT), vol. 997, pp. 89–98. Springer, New York (2019)
11. Pavananag, N., Divakar, R.: A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks, International Journal of Advanced Research in Computer and Communication Engineering, 2022
12. Muhammad, F., Alberto, S.: Anomaly detection, analysis and prediction techniques in IoT environment: a systematic literature review. IEEE Access **7**, 81664–81681 (2019)
13. Alzahrani, A., Baabdullah, T., Danda, B.: Rawat attacks and anomaly detection in IoT network using machine learning, pp. 465–472. Springer Nature, Cham (2021)
14. Muaadh A., Shukor R., Maheyzah Md S., Ibtehal N., Fuad A. G., Faisal S., and Maged N.: Anomaly-Based Intrusion Detection Systems in IoT Using Deep Learning: A Systematic Literature Review, MDPI, Applied Science, 2021
15. Gothawal, D.B., Nagaraj, S.V.: Anomaly-based intrusion detection system in rpl by applying stochastic and evolutionary game

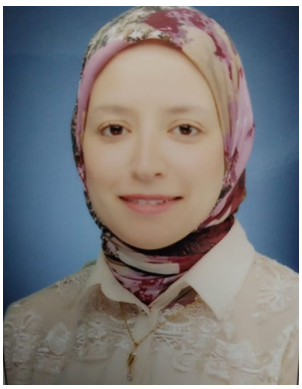
models over IoT environment. Wireless Pers. Commun. **110**, 1323–1344 (2020)
16. Keserwani, P.K., Govil, M.C., Pilli, E.S., Govil, P.: A smart anomaly-based intrusion detection system for the Internet of Things (IoT) network using GWO–PSO–RF model. J Reliable Intell Environ. **7**, 3–21 (2021)
17. Singh, K.P., Kesswani, N.: An anomaly-based intrusion detection system for IoT networks using trust factor. SN Comput Sci **3**, 1–9 (2022)
18. Davahli, A., Shamsi, M., Abaei, G.: A lightweight Anomaly detection model using SVM for WSNs in IoTthrough a hybrid feature selection algorithm based on GA and GWO". J Comput Secur **7**, 63–79 (2020)
19. Munir, M., Siddiqui, S.A., Dengel, A., Ahmed, Sh.: DeepAnT: a deep learning approach for unsupervised anomaly detection in time series. IEEE Access **2018**(7), 1991–2005 (2018)
20. Li, X., Xu, M., Vijayakumar, P., Kumar, N., Liu, X.: Detection of low-frequency and multi-stage attacks in industrial internet of things. IEEE Trans Vehicle Technol **69**, 8820–8831 (2020)
21. Kim, S., Hwang, C., Lee, T.: Anomaly based unknown intrusion detection in endpoint environments. Electronics. **9**, 1022–1041 (2020)
22. Malaiya, R.K., Kwon, D., Suh, S.C., Kim, H., Kim, I., Kim, J.: An empirical evaluation of deep learning for network anomaly detection. IEEE Access **7**, 140806–140817 (2019)
23. Shi, W.-C., Sun, H.M.: DeepBot: a time-based botnet detection with deep learning. Soft. Comput. **24**, 16605–16616 (2020)
24. Parra, G., Rad, P., Choo, K., Beebe, N.: Detecting internet of things attacks using distributed deep learning. J. Netw. Comput. Appl. **163**, 102662 (2020)
25. Hnamte, V., Hussain, J.: DCNNBiLSTM: an efficient hybrid deep learning-based intrusion detection system. Telematics Inf Rep. **10**(1), 1–13 (2023)
26. Bai, L., Yao, L., Kanhere, S. S., Wang, X., Yang, Z.: Automatic device classification from network traffic streams of Internet of Things, in Proceeding IEEE 43rd Conference Local Computer Network (LCN), pp. 1–9 (2018)
27. Vinayakumar, R., Soman, K. P., Poornachandran, P.: Applying convolutional neural network for network intrusion detection, in Proceeding. International Conference Advance Computer Communication Information (ICACCI), Udupi, India, Sep. 2017, pp. 1222–1228.
28. Simon, J., Kapileswar, N., Polasi, P., Mathiyalakendran, A.E.: Hybrid intrusion detection system for wireless IoT networks using deep learning algorithm. Comput. Electr. Eng. **102**(4) (2022)
29. TaherAzar, A., Shehab, E., Mattar, A.M., Hameed, I.A., Ahmed Elsaid, Sh.: Deep learning based hybrid intrusion detection systems to protect satellite networks. J. Netw. Syst. Manag. **31**, 82 (2023). https://doi.org/10.1007/s10922-023-09767-8
30. Al-Yaseen, W.L.: Improving intrusion detection system by developing feature selection model based on firefly algorithm and support vector machine. IAENG Int. J. Comput. Sci. **46**, 1–7 (2019)
31. Liu, C., Gu, Z., Wang, J.: A hybrid intrusion detection system based on scalable K-MeansC random forest and deep learning. IEEE Access **9**, 75729–75740 (2021)
32. Ravale, U., Marathe, N., Padiya, P.: Feature selection based hybrid anomaly intrusion detection system using K means and RBF kernel function. Proc Comput Sci **45**, 428–435 (2015)
33. Indira, K., Sakthi, U.: A hybrid intrusion detection system for SDWSN using Random Forest (RF) machine learning approach. Int J Adv Comput Sci Appl. **11**, 275–284 (2020)
34. Louk, M., Tama, B.A.: PSO-driven feature selection and hybrid ensemble for network anomaly detection. Big Data Cogn Comput **6**, 1–3 (2022)
35. Balyan, A.K., Ahuja, S., KumarLilhore, U., KumarSharma, S., Manoharan, P., Algarni, D.A., Elmannai, H., Raahemifar, K.: A hybrid intrusion detection model using EGA-PSO and improved random forest method. Sensors. **22**, 1–20 (2022)
36. Einy S., Oz C., and Dorostkar Navaei Y.: The Anomaly-and Signature-Based IDS for Network Security Using Hybrid Inference Systems, Mathematical Problems in Engineering, 2021, 1–10 (2021)
37. Alzaqebah, A., Aljarah, I., Al-Kadi, O., Damaševicius, R.: A Modified Grey Wolf Optimization algorithm for an intrusion detection system. Mathematics **10**, 1–16 (2022)
38. Kunhare, N., Tiwari, R., Dhar, J.: Intrusion detection system using hybrid classifiers with meta-heuristic algorithms for the optimization and feature selection genetic algorithm. Comput. Electr. Eng. **103**(8) (2022)
39. Khraisat, A., Gondal, I., Vamplew, P., Kamruzzaman, J., Alazab, A.: A novel ensemble of hybrid intrusion detection system for detecting internet of things attacks. Electronics **8**, 1–18 (2019)
40. Abbas, A., Khan, M.A., Latif, S., Ajaz, M., Shah, A.A., Ahmad, J.: A new ensemble-based intrusion detection system for internet of things. Arab J Sci Eng **47**, 1805–1819 (2022)
41. Anitha, P., Kaarthick, B.: Oppositional based Laplacian Grey Wolf Optimization algorithm with SVM for data mining in intrusion detection system. J Ambient Intell Hum Comput **12**, 3589–3600 (2021)
42. Kalinin, M., Krundyshev, V.: Security intrusion detection using quantum machine learning techniques. J Comput Virol Hacking Tech **19**, 125–136 (2023)
43. Park, J. E., Quanz, B., Wood, S., Higgins, H., Harishankar, R.: Practical Application Improvement to Quantum SVM: Theory to Practice, 34th Conference on Neural Information Processing Systems, 1–9 (2020).
44. Ghanbarzadeh, R., Hosseinalipour, A., Ghaffari, A.: A novel network intrusion detection method based on metaheuristic optimisation algorithms. J. Ambient. Intell. Humaniz. Comput. **14**, 7575–7592 (2023)
45. Tawhid, M.A., Ali, A.F.: A hybrid Grey Wolf Optimizer and genetic algorithm for minimizing potential energy function. Memetic Comp. **9**, 347–359 (2017)
46. Prashant, J., Madhav, J.: A hybrid Grey Wolf optimizer and artificial bee colony algorithm for enhancing the performance of complex systems. J Comput Sci **27**, 284–302 (2018)
47. Khraisat, A., Gondal, I., Vamplew, P., Kamruzzaman, J., Alazab, A.: A novel ensemble of hybrid intrusion detection system for detecting internet of things attacks. Electronics. **8**, 1–18 (2019)
48. Azhagusundari, B., Thanaman, A.S.I.: Feature selection based on information gain. Int J Innov Technol Explor Eng (IJITEE). **2**, 18–21 (2013)
49. Mirjalili, S., Mirjalili, S.M., Lewis, A.: Grey Wolf Optimizer. Adv. Eng. Softw. **69**, 46–61 (2014)
50. Gao, Z., Zhao, J.: An improved Grey Wolf Optimization algorithm with variable weights. Hindawi Comput Intell Neurosci **2019**, 1–13 (2019)
51. Davahli, A., Shamsi, M., Abaei, G.: Hybridizing genetic algorithm and Grey Wolf optimizer to advance an intelligent and lightweight intrusion detection system for IoT wireless networks. J. Ambient. Intell. Humaniz. Comput. **11**, 5581–5609 (2020)
52. Guo, K., Cui, L., Mao, M., Zhou, L., Zhang, Q.: An improved Gray Wolf Optimizer MPPT algorithm for PV system with BFBIC converter under partial shading. IEEE access **8**, 103476–103490 (2020)
53. Nickolaos, K., Moustafa, N., Sitnikova, E., Turnbull, B.: "Towards the development of realistic botnet dataset in the internet of things for network forensic analytics: Bot-IoT dataset. Futur. Gener. Comput. Syst. **100**, 779–796 (2019)

54. Ayubkhan, Sh., Ab, H., Yap, W.S., Morris, E., Begam Kasim Rawthar, M.: A practical intrusion detection system based on denoising autoencoder and LightGBM classifier with improved detection performance. J Ambient Intell Hum Comput. **14**, 7427–7452 (2023)
55. Sharma, M., Pant, S., Yadav, P., Kumar, S.D., Gupta, N., Srivastava, G.: Advancing security in the industrial internet of things using deep progressive neural networks. Mobile Netw Appl **28**, 782–794 (2023)
56. Selvan, E., Ganeshan, R., DianaJebaJingle, I., Ananth, J.P.: FACVO-DNFN: deep learning-based feature fusion and distributed denial of service attack detection in cloud computing. Knowl Based Syst **261**, 4001–4008 (2023)

E. I. Elsedimy has joined the Port Said University, Egypt, in December 2012 as Assistant lecturer after 8 years being tSenior Lecturer (Associate Professor) at Ministry of Higher Education. Currently, he is Assistant professor of information technology at Faculty of Technology and Information System, Port Said University, Egypt. He obtained his Ph.D. degree in Computer Science (mainly in Cloud Computing and Artificial Modeling) in 2018 from the University of Mansoura, Egypt, and the M.Sc. and B.Sc. degrees in Rough set theory and Decision support systems applications, from the University of Mansoura, Egypt. In the past 20 years, he was involved in numerous collaborative research and development projects, and also he has been a reviewer of many reputed international journals and conferences, such as China Communications, Computing, and IEEE Transactions on Systems, Man, and Cybernetics. His current research interests are in the areas of Cyber Security, Cloud Computing, Machine Learning, Artificial Intelligent and the internet of things.



Hala Elhadidyis is Assistant Professor in the Electrical Engineering Department, Faculty of Engineering, Port Said University. She has had the opportunity to teach in the computer Engineering and Networks Department, Computer and Information Science College, Jouf University in Kingdom of Saudi Arabia for three years. She has received her B.Sc. Degree with Distinction (First Class Honour) in Electrical Engineering from Suez Canal University (Port Said, Egypt) in 1998 and the Master and Doctoral Degree in Electrical Engineering from the Port Said University (Port Said, Egypt) in 2011 and 2015 respectively. She was the manager of portal of Port Said University from 2015 until 2019. Her main interests are system engineering, automatic control, intelligent systems, Artificial Intelligent and computer networks especially the wireless sensor networks (WSNs).



Sara M. M. AboHashish is a professor in Faculty of Management Technology and Information Systems, Port Said University, Egypt. She received a B.Sc., M.Sc. and Ph.D. in degrees in Communication and Electronics engineering from the Port Said University, in 2007, 2013, 2018; respectively. Her research interests are in the area of wireless networks, cloud computing, machine learning, and deep learning.