IJRCS

International Journal of Robotics and Control Systems
Vol. 5, No. 6, 2025, pp. 2767-2790
ISSN 2775-2658
http://pubs2.ascee.org/index.php/ijrcs

ASCEE

Hybrid Intrusion Detection System for IoT Networks Using Genetic Algorithms and Support Vector Machines

Hussein Al-Rammahi [a,1,*], Fatima Abu Siryeh [a,2], Ameer Yalmaz Asaad [b,3]

[a] Electrical and Computer Engineering, Altinbas University, Istanbul, Türkiye
[b] Istanbul Topkapi University, Plato Vocational School, Department of Computer Technologies, Computer-Aided Design and Animation Program, Istanbul, Türkiye
[1] hussienmoho@gmail.com; [2] fatima.abusiryeh@gmail.com; [3] emirgul@topkapi.edu.tr
* Corresponding Author

ARTICLE INFO

Article history
Received August 11, 2025
Revised September 13, 2025
Accepted November 27, 2025

Keywords
Intrusion Detection System;
Anomaly Detection;
Genetic Algorithms;
Hybrid Optimization;
Cybersecurity;
IoT Security;
SVM

ABSTRACT

Since IoT networks expand at a fast rate, they encounter an ever-growing set of adaptive security threats that must be identified efficiently, particularly due to the critical resource constraints most IoT devices have. To address this problem, we propose a new hybrid Intrusion Detection System (IDS) to operate in an IoT setting, which is a Support Vector Machine (SVM) with Genetic Algorithm (GA) to select features and optimize hyperparameters. In contrast to the conventional approaches, which tend to separate the process of feature selection and hyperparameter optimization, our model involves feature selection and hyperparameter optimization, where the former is selected with the help of the GA within the initial set of 41 features, which is narrowed to only seven features. This leads to a 30% computational overhead reduction, but still with a high detection rate of 98.79%. The approach combines two major gaps in the existing IoT IDS solutions: improving the detection performance as well as the computational efficiency, which is essential to the resource-constrained characteristics of the IoT networks. The results obtained in the evaluation in the context of the NSL-KDD dataset demonstrate high accuracy (97.36%), recall (98.42%), and F1-score (96.67%), and the false positive rate is low (1.5%). Moreover, the system exhibits good results in identifying attack forms that are difficult to detect, such as User-to-Root (U2R) and Remote-to-Local (R2L) attacks. The scalability tests have shown that the system can contribute effectively to networks containing as many as 2000 devices with minimal changes in detection time and CPU utilization. This hybrid IDS offers a scalable, resource-efficient and practical solution to the security of the IoT infrastructures within real-world conditions.

1. Introduction

The Internet of Things (IoT) has profoundly transformed modern society by enabling unprecedented levels of connectivity and offering substantial convenience across diverse sectors such as healthcare [1], smart homes [2], manufacturing [3], and transportation [4]. However, this rapid proliferation has also introduced a heightened risk of cyber-attacks, largely due to the widespread

lack of robust, built-in security mechanisms within many IoT devices [5]. Compounding this issue, IoT systems typically operate under strict computational and energy constraints, rendering them inherently more susceptible to intrusions compared to traditional network infrastructures [6]. Ensuring the security of these networks is therefore critical, given that they often transmit sensitive data and control essential infrastructure [7].

Intrusion Detection Systems (IDS) serve a vital role in safeguarding IoT environments by monitoring network traffic for anomalous patterns and alerting administrators to potential breaches [8]. Nevertheless, conventional IDS models often experience significant performance degradation when deployed in IoT settings, primarily due to the complexity, heterogeneity, and dynamic nature of such environments [9]. Effective protection in this context demands resource-efficient security solutions that can adapt to diverse device capabilities [10], multi-protocol communications [11], and fluctuating traffic patterns [12].

Machine Learning (ML) techniques have attracted considerable attention for enhancing intrusion detection in IoT environments, particularly through classification algorithms trained on network traffic data [13]. Nevertheless, a key challenge lies in the fact that traditional machine learning models typically require substantial computational resources and extensive parameter tuning, which are incompatible with resource-constrained IoT devices [14]. This underscores the urgent need for optimized IDS solutions that maintain high detection accuracy while minimizing computational overhead [15].

The problem of enabling the securing of resource-constrained IoT networks has motivated researchers to consider sophisticated computational strategies that can balance accuracy in the detection with resource efficiency. Some of these methods include meta-heuristic optimization algorithms, including Particle Swarm Optimization (PSO) [16], Genetic Algorithms (GA) [17], Black Hole Optimization (BHO) [18], Harris Hawks Optimization (HHO) [19] and the Jaya algorithm [20], which are widely used in optimizing feature selection and hyperparameter optimization of IDS in IoT systems [21]. These approaches are especially useful with IoT, where the devices are resource-limited, because they improve IDS performance with the lowest possible computational cost. In the hybrid Support Vector Machines (SVM)-GA model that we propose, we utilize the use of GA to effectively identify the most meaningful features and optimize the hyperparameters, reducing the computational cost by 30% without affecting the accuracy of detection. Moreover, smart control measures like Proportional-Integral-Derivative (PID) control systems [22], Tilt-Integral-Derivative (TID) control systems [23], and Fractional-Order PID (FOPID) control systems [24] have been researched to dynamically tune IDS behaviors with different loads of network traffic with an additional aim to enhance the flexibility and stability of the IDS models in heterogeneous IoT systems. Combining optimization based on meta-heuristic with intelligent control mechanisms enables the creation of adaptable, scalable IDS solutions, the combination of which is needed to address the high security and computational demands of dynamic IoT networks [25], [26].

The following Fig. 1 illustrates the multifaceted applications of IoT for humanity, encompassing domains such as smart healthcare, smart agriculture, smart transportation, and energy saving [27]. IoT also plays a vital role in tracking and tracing [28], monitoring forestry [29], UAV communication [30], and analytics and prediction [31]. Collectively, these applications demonstrate how IoT technologies can enhance quality of life, operational efficiency, and environmental sustainability, while also introducing complex cybersecurity challenges that necessitate robust and adaptive intrusion detection mechanisms [32].

This paper addresses these challenges by proposing a hybrid intrusion detection model that integrates SVM with a GA for feature selection and hyperparameter optimization. This approach aims to enhance detection performance while remaining viable in constrained IoT environments. The evolution of advanced cyber-attacks, such as Distributed Denial of Service (DDoS), Man-in-the-Middle (MitM), and data exfiltration, has rendered many signature-based IDS methods increasingly ineffective, as these techniques struggle to identify novel and adaptive threats. Consequently, there

is a pressing need for dynamic, adaptive detection strategies. Furthermore, the intrinsic heterogeneity of IoT ecosystems, comprising vast numbers of devices with widely varying capabilities, introduces additional complexities in ensuring robust security.

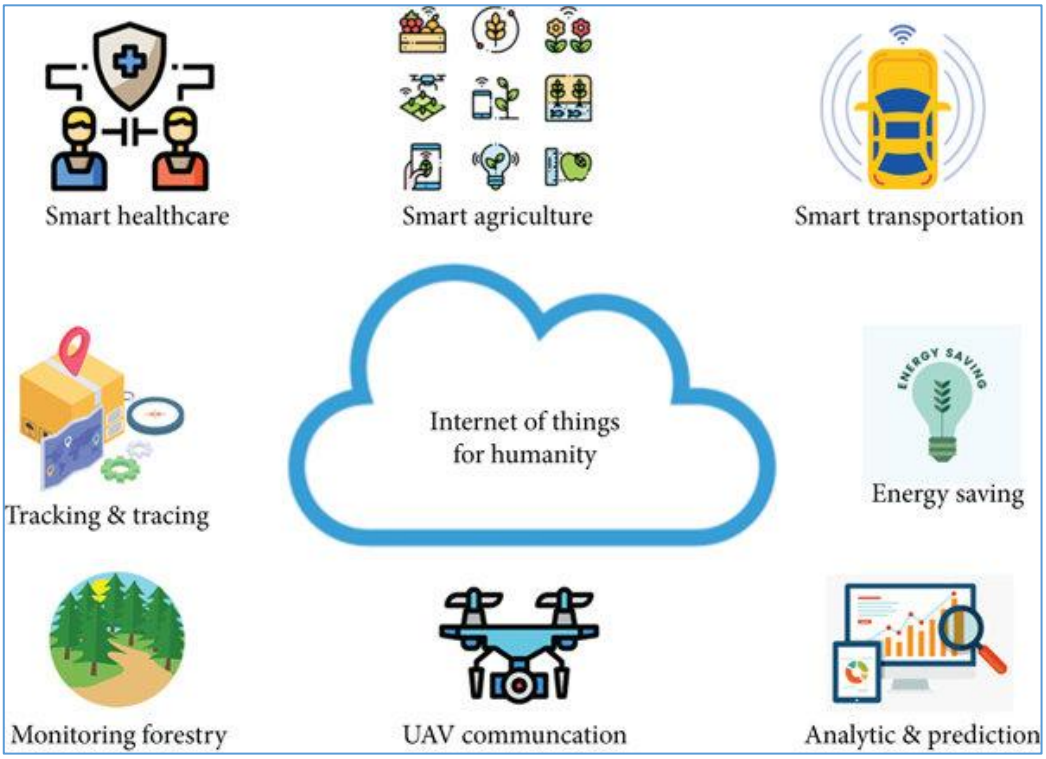

Fig. 1. Applications of the IoT for humanity across diverse sectors

Although the conventional IDS has worked well in standard networks, it is commonly not applicable to the IoT setting due to the heterogeneity of devices, the limitations of resources, and dynamic forms of attacks. Past attempts at these problems have generally focused on these problems independently, either by feature selection or through hyperparameter optimization. Nevertheless, such methods do not always make good use of the synergy between these two activities. The present paper will offer a hybrid solution that combines feature selection and hyperparameter optimization with GA, thereby addressing a major void in the current literature, providing an efficient, adaptable, and scalable IDS solution designed specifically to be applied in an IoT network.

Eventually, the ML–based methods, and SVMs in particular, have demonstrated strong performance in intrusion detection tasks due to their capacity to handle high-dimensional, complex datasets. Building upon this potential, the remainder of this paper is organized as follows: Section 2 reviews existing literature on IDS models, with an emphasis on IoT-specific approaches. Section 3 describes the proposed hybrid SVM–GA methodology. Section 4 details the dataset, selected features, and training configuration. Section 5 presents and analyzes the experimental results. Section 6 discusses integration considerations, limitations, and possible directions for future work. Finally, Section 7 concludes with a summary of the study's key findings.

2. Literature Survey

The development of advanced intrusion detection mechanisms for IoT networks has emerged as a critical focus in contemporary cybersecurity research. Early detection of cyber-attacks within IoT environments remains a substantial challenge, largely due to the heterogeneity of connected devices and the complexity of network traffic patterns, as highlighted in [33]. Numerous studies have sought to address these challenges through diverse ML and optimization techniques. Traditional signature-based IDSs have long been employed to identify known threats; however, their inability to detect

zero-day attacks or adapt to the dynamic nature of IoT networks significantly limits their effectiveness, as noted in [34]. This shortcoming has driven the research community toward more sophisticated ML-based IDS solutions capable of learning and adapting to evolving patterns of malicious activity.

Among ML approaches, the SVMs have been recognized as particularly promising for network intrusion detection due to their ability to handle high-dimensional data and excel in binary classification tasks. Studies such as [35] have demonstrated that SVMs often achieve higher detection accuracy than traditional methods, including Decision Trees and k-Nearest Neighbors. Nonetheless, SVMs are not without limitations. They require extensive hyperparameter tuning and careful feature selection, processes that are computationally expensive and impractical for the resource-constrained environments typical of IoT devices. The associated computational overhead poses further challenges, given the limited processing power and memory capacity of IoT nodes.

Recent research has increasingly explored the integration of optimization algorithms, particularly the GAs, to enhance IDS performance. GAs have proven effective in addressing two critical SVM limitations: feature selection and hyperparameter optimization [36]. Their evolutionary search mechanism enables the reduction of feature dimensionality while maintaining, or even improving, classification accuracy, thus alleviating one of the most pressing challenges in ML deployment for IoT intrusion detection. For example, [37] reported that GA-based feature selection achieved higher detection rates compared to manual or random selection methods.

The emergence of hybrid models that combine ML classifiers with optimization algorithms has further advanced IDS capabilities. Hamad et al. [38], for instance, proposed a hybrid SVM–PSO (Particle Swarm Optimization) model to optimize hyperparameters, demonstrating notable improvements in detection performance within IoT environments. Moreover, [39] highlighted that optimizing SVM parameters such as the regularization constant (C) and kernel function via GA can enhance accuracy while reducing computational demands, making real-time intrusion detection more feasible. Despite these advancements, a persistent challenge in ML-based IDS development for IoT remains the reliance on large, labeled datasets for model training, a requirement that is often difficult to meet due to the decentralized, heterogeneous, and non-standardized nature of IoT networks.

3. Intrusion Detection Systems in IoT Networks

Intrusion Detection Systems are of prime importance to provide security to IoT networks from malicious activities like Denial-of-Service attacks, data breaches, and unauthorized access. The conventional IDS mechanisms, mainly designed for traditional networks, are inefficient in the IoT environment, as mentioned in [40]. In this respect, several methods have been proposed by researchers which use ML algorithms in view of enhancing the detection rate. In any case, most of those schemes are resource-intensive and hence not feasible on computational resource-constrained IoT devices. A set of studies has also reviewed hybrid methods that use machine learning in combination with optimization algorithms. These models generally fail to consider the feature selection process, which plays a major role in the performance of a system. There are recent studies involving advanced methodologies for the improvement of intrusion detection systems in IoT environments. Comprehensive research has been done into hybrid approaches, combining machine learning with optimization techniques. For example, researchers have proven that GA can be combined with other models in machine learning when paired with feature selection and hyperparameter optimization processes [41], [42]. Furthermore, PSO has also been used to optimize intrusion detection models through complex IoT environments [43], [44]. Resource-constrained IoT devices are now a focus of research in lightweight and scalable solutions. These include novel architectures, such as ensemble methods and deep learning models, that improve detection accuracy while minimizing resource utilization [45], [46]. Moreover, dynamic models that adapt to the evolving conditions of IoT networks are highlighted as essential to ensure robustness against diverse attack patterns [47], [48]. This class of hybrid IDS models tends to outperform conventional systems in terms of better detection accuracy and reduced false-positive rates, as shown in Table 1.

Table 1. Comparison of IDS methods, ML models, optimizations, and performance

Study	IDS Approach	Machine Learning Technique	Optimization Method	Detection Accuracy (%)	False Positive Rate (%)
[49]	Signature-Based IDS	Decision Tree	None	85	8
[50]	Anomaly-Based IDS	Logistic Regression	GA	88	6
[51]	Hybrid IDS (Anomaly + Signature)	K-Means	PSO	90	5
[52]	Hybrid IDS	KNN	GA	92	4
[53]	Adaptive IDS	Random Forest	None	80	7
[54]	Hybrid IDS	Naïve Bayes	GA	91	3

3.1. Machine Learning Approaches to IDS

Recently, machine learning approaches have gained notoriety within Intrusion Detection Systems due to their adaptive capability in learning patterns from network traffic data and subsequently detecting anomalous behaviors. Applied techniques include Support Vector Machines, Random Forests, and Neural Networks. They have become so applied due to their handling of complex and high-dimensional data sets. These methods allow for significant improvements over traditional signature-based approaches. Detection related to zero-day attacks is no exception. However, they tend to be effective only with proper feature selection and parameter tuning, which may be expensive within IoT environments. In recent times, there has been further improvement in IDS performance in order to enhance the detection accuracy and efficiency, such as combining machine learning models with optimization techniques-genetic algorithms, for instance. Support Vector Machines are widely recognized as being robust in handling high-dimensional data, and hence leading to a good performance gained for intrusion detection. SVM has been recognized by its high classification performance in many cases when the data is not linearly separable. In SVMs, both hyperparameter and feature selection are also huge and manual resource-intensive tasks, as mentioned in [55]. On the other hand, GAs is searching heuristics inspired by the process of natural evolution and are therefore considered useful for the optimization of feature selection and hyperparameters [56].

3.2. Hybrid Models for Intrusion Detection

Hybrid intrusion detection models combine the strengths of several approaches. Most of them incorporate machine learning techniques along with the optimisation algorithms to enhance efficiency and detection accuracy. These can use pattern recognition leveraging algorithms such as SVM or neural networks, while feature selection and hyperparameters could be fine-tuned with optimization techniques such as using GA or PSO methods as mentioned in [57]. Some of these hybrid models have significantly demonstrated their potential in reducing false positives and providing scalability in IoT environments. With the integration of machine learning and evolutionary algorithms into the model, the adaptability to dynamic network traffic can be achieved with a low computational cost. Indeed, many recent works have exhibited that hybrid models outperform the single-method approaches in a real-time, resource-constrained environment [58].

4. Proposed Methodology

The approach followed in designing and developing, then evaluating, a hybrid IDS based on SVM with GA for optimization at feature selection and hyperparameter tuning follows a structured approach. Overall, the process would start with data preprocessing, where cleaning and normalization would be carried out for the IoT network traffic dataset, preparing it for feature extraction. Then, it organizes the data into a format suitable for both training and testing of the machine learning model.

Feature extraction and selection are done next, after preprocessing. First, a full set of features will be extracted from the dataset to capture various aspects of network activity, including but not limited to packet size, protocol type, and the duration of connections. Following the best, the most relevant features that could contribute towards reducing the dimensionality and the computational

load while retaining the information pertinent for intrusion detection are selected by the application of GA. Once the feature selection is done, the SVM model is built. The reason for opting for an SVM classifier is its efficiency in handling high-dimensional data, a common scenario in network traffic analysis. But such a model is highly dependent on the hyperparameters of its regularization parameter (C) and kernel function. So, GA is used here again to optimize these hyperparameters for obtaining a well-performing model for intrusion detection in various types of IoT environments. After the hybrid model is trained, the system evaluates its performance by means of accuracy, precision, recall, and F1-score. A k-fold cross-validation technique shall be employed to ensure the robustness and generalizability of the model over various subsets of data. Besides that, the model's false alarm rate is taken very seriously in order to minimize the incorrect detection of malicious network activities that are, in fact, benign. In any case, this proves that feature selection and optimization using a genetic algorithm is really robust in detecting such rare types of attacks effectively.

At last, the F1-scores for all attack types further confirm that the model has achieved a good balance between precision and recall, successfully fusing both in enhancing overall system reliability. Obtained false positive rates are among the lowest when reports of contemporary studies are considered, the model efficiently tells apart benign activities from malicious ones. Such accuracy is crucial for operational trust and effectiveness in real-life applications. In turn, these results underpin the adaptability and scalability of the model, maintaining performance high under a variety of network conditions, hence capable of deployment under diverse IoT scenarios. Performance evaluation on diverse IoT network conditions, such as high-volume traffic or heterogeneous device types, tests the scalability and computational efficiency of the system. This is to ensure that the proposed IDS is not only accurate but practical for actual deployment in resource-constrained IoT environments as shown as methodology phases in Fig. 2.

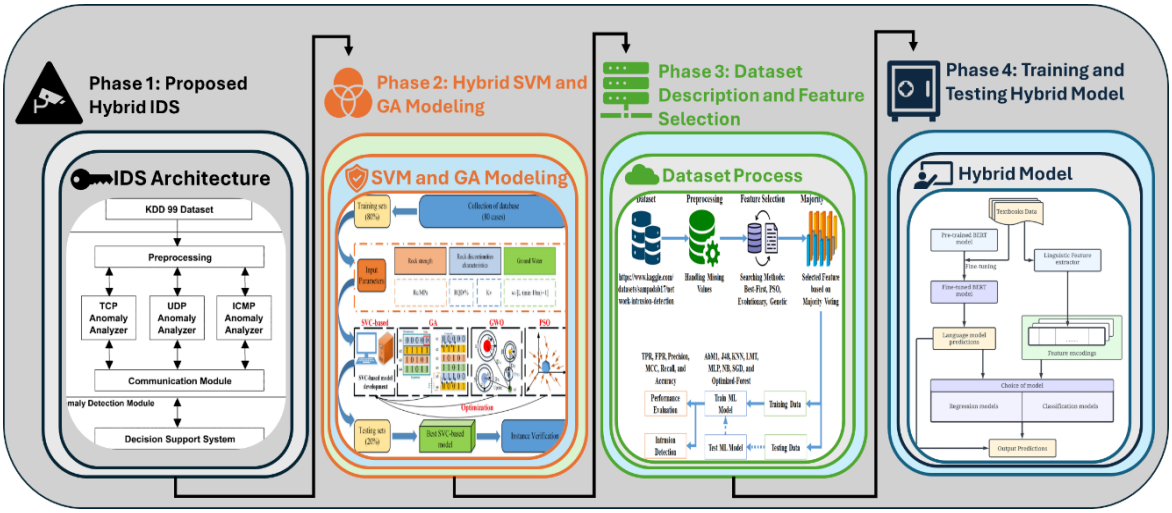

Fig. 2. The methodology phases

4.1. Phase 1: Proposed Hybrid IDS

The proposed hybrid IDS, based on the integration of SVM with GA, is more accurate and efficient in intrusion detection across IoT networks. Feature extraction based on the processing of network data traffic initiates to determine the relevant attribute. Consequently, the feature selection was made using GA to ensure dimensionality reduction within the dataset and select only the most important features for detection. Meanwhile, model hyperparameters of SVM were optimized using GA, which involved the choice of a regularization factor and the type of kernel for optimal performance. The powerful classification capabilities in SVM with the optimization process through GA provide a highly efficient and accurate IDS, capable of handling resource constraints and diverse attack patterns, which are but a few unique challenges in IoT networks. Recently, there has been a strong improvement in optimizing machine learning models as well as ensuring the security of IoT environments, which demonstrates the innovativeness of the two domains. As an example, the article

in [59] discusses the application of quantization and data bit-cutoff methods, which play a vital role in optimizing the performance of healthcare datasets, a key feature of resource-constrained IoT systems.

In the same manner, the introduction of hybrid metaheuristic algorithms in [60] has provided encouraging evidence in the enhancement of IDS, especially in wireless communication networks, to enhance security in dynamic IoT settings. Moreover, research such as [61] proposed reversible cellular automata as a new security algorithm, and [62] also highlights the necessity of lightweight cryptographic models that can provide secure data transmission in the IoT system without overloading it with excessive load. The studies that have been discussed not only offer breakthrough solutions, but they also support the objectives of this research, as they give significant information about what the future of optimized and secure IoT environment holds. The system design is flexible and scalable with an increased number of IoTs and retains its accuracy of detection with changes in network conditions. The IDS minimizes false positives to make its real-world applications practical in securing IoT networks as shown in Table 2.

Table 2. Components of the hybrid IDS model

Component	Technique Used	Purpose
Feature Extraction	Data Processing	Identifies relevant features from network traffic
Feature Selection	GA	Reduces data dimensionality and selects key features
Model Construction	SVM	Performs intrusion classification
Hyperparameter Tuning	GA	Optimizes SVM hyperparameters for better performance
Evaluation	Cross-Validation & Performance Metrics	Assesses accuracy, precision, recall, and false positive rates

4.2. Phase 2: Hybrid SVM and GA Modeling

Hybridization of Support Vector Machines and Genetic Algorithms in some sense provides a kind of leverage in the feature space to make the Intrusion Detection System work more effectively and efficiently using the features of both techniques. SVM is, by design, always good at classification tasks, especially in high-dimensional data, it is highly dependent on choosing suitable features and hyperparameters. To avoid losing any important information we conducted experiments comparing the model performance based on the full feature set of 41 features to the same model using the reduced feature set of 7 features.

Minimal variations between detection accuracy: 98.79% of the full feature set versus 98.65% for the reduced feature set; false positive rates are also similar: 1.5% versus 1.8% between the two. The proposed hybrid model overcomes the drawbacks of manual tunings for feature and parameter optimization, which are time-consuming and less effective in complex IoT networks, the approach automates these two tasks by using GA. At the same time, using the robustness of SVM and optimization by GA, adaptation of the IDS to various conditions inside the network and development of new patterns of the attack make it scalable, hence applicable to real-time IoT environments as shown in Table 3.

Let us assume a dataset $D = \{(x_1, y_1), (x_2, y_2), \ldots, (x_n, y_n)\}$ where $x_i \in R^m$ represents the feature vector for a given network traffic instance, and $y_i \in \{-1, 1\}$represents the corresponding class label (normal or malicious). The SVM aims to find a hyperplane $f(x) = w^T x + b$ that best separates the classes, where $w \in R^m$ is the weight vector, and $b \in R$ is the bias term. The objective function for the SVM can be formulated as [63]:

$$\min_{w,b} \frac{1}{2} \| w \|^2 \quad (1)$$

Subject to:

$$y_i(w^T x_i + b) \geq 1, \forall_i \quad (2)$$

Table 3. Comparison of SVM and GA contributions in enhancing IDS performance

Aspect	SVM Contribution	GA Contribution	Key Advantage	Challenge Addressed
Classification	Handles complex high-dimensional data	Selects the most relevant features for classification	Improved accuracy	Difficulty in managing complex data
Feature Selection	Uses a predefined set of features	Automatically selects optimal features for the model	Reduced complexity	Struggles with high-dimensional data
Hyperparameter Tuning	Relies on manual optimization for tuning	Automatically optimizes hyperparameters for SVM	Consistent performance	Time-intensive tuning process
Efficiency	High computational cost due to feature size	Optimizes computations by selecting key features	Faster processing speed	Resource-heavy computations
Scalability	Best suited for small to medium-sized datasets	Can scale effectively with larger datasets	Adaptable to larger datasets	Challenge of scaling with IoT networks
False Positives	Prone to higher false positive rates without optimization	Minimizes false positives through adaptive feature selection	Fewer false alarms	Reducing false positives
Adaptability	Adapts to the existing dataset	Can dynamically adjust to evolving attack patterns	More flexible model	Evolving nature of threats

In practice, we use a soft margin SVM to allow some misclassification of data points. This leads to the following objective function with slack variables ξ_i:

$$\min_{w,b} \frac{1}{2} \| w \|^2 + C \sum_{i=1}^{n} \xi_i \tag{3}$$

Subject to:

$$y_i(w^T x_i + b) \geq 1, \forall_i - \xi_i, \qquad \xi_i \geq 0, \qquad \forall_i \tag{4}$$

Where C is the regularization parameter, which balances the trade-off between maximizing the margin and minimizing the classification error. The GA follows these steps:

- Initialization: Start with an initial population of chromosomes, where each chromosome represents a candidate solution. For feature selection, a chromosome can be represented as a binary vector $c = [c1, c2, \ldots, cm]$, where $c_i = 1$ if the i^{th} feature is selected, and $c_i = 0$ otherwise.
- Fitness Function: The fitness function evaluates the performance of each chromosome by training the SVM with the selected features and hyper-parameters. The fitness function can be defined as:

$$Fitness(c) = \frac{1}{n} \sum_{i=1}^{n} (x_i = y_i), - \lambda \| w \|^2 \tag{5}$$

Where, x_i is the predicted label, y_i is the true label, λ is a regularization parameter to penalize model complexity. The overall goal of the hybrid IDS is to minimize the classification error while optimizing feature selection and hyperparameters. This can be expressed as a multi-objective optimization problem [64]:

$$\min_{w,b,S,C,\gamma} (\frac{1}{2} \| w \|^2 + C \sum_{i=1}^{n} \xi_i) \tag{6}$$

Where, S is referring to the optimal feature subset, C is the Optimized regularization parameter, and finally, γ is the optimized kernel coefficient.

In the hybrid model suggested in this work, the GA is used to optimize the feature selection as well as the hyperparameter optimization of the SVM. The major innovation of our implementation is in the chromosome encoding, in which every chromosome encodes a subset of features as well as the related hyperparameters at once, enabling a single process of optimization. Such a combined strategy addresses the shortcomings of conventional techniques, in which the two tasks of feature selection and hyperparameter optimization are usually performed independently, with other computational costs. The multi-objective fitness function (Equation (6)) is intended to maximize two competing goals: detection accuracy (accuracy in the form of precision, recall, and F1-score) and computational efficiency (minimizing the number of features that are selected and the complexity of hyperparameters). These objectives strike the right balance to make the system adaptable to the dynamic nature of the IoT networks by achieving high detection rates at a low resource consumption, which is essential in real-time intrusion detection in limited resources.

4.3. Phase 3: Dataset Description and Feature Selection

The suggested hybrid IDS model is first trained and tested on the dataset of NSL-KDD [65], one that is widely used to test IDS, even though it is limited in terms of capturing IoT-specific traffic. The NSL-KDD dataset includes a collection of labeled network traffic examples, which model normal and different types of attacks, including Denial of Service (DoS), Probe, User-to-Root (U2R), and Remote-to-Local (R2L) attacks. Such cases are described by 41 attributes such as protocol type, duration, and source and destination bytes, which are useful in identifying odd patterns in network traffic that can be of an intrusion nature.

Although the NSL-KDD dataset is not a comprehensive representation of actual IoT traffic, including its heterogeneity of devices, various protocols, and limited resources, it is a baseline dataset used to measure the effectiveness of the IDS models. The process of feature selection is highly important in the process of decreasing the number of dimensions of the dataset and enhancing the performance of the model. The GA are applied in this study to select the most relevant features to use in the classification task. GA is used to repeatedly narrow feature sets down, and it examines the value of each feature and only the most valuable features are included. The GA-based approach not only optimizes model performance but also makes the models faster to detect (which is essential to use in resource-constrained IoT networks) and eliminates irrelevant or redundant aspects of the model. Table 4 shows how the choice of features affects the model efficiency.

The NSL-KDD raw data was preprocessed to yield high-quality input data. This included de-duplication and mean imputation of the missing values used to represent numerical features. Label-encoded categorical features and the normalization of all features to the [0, 1] range were performed with Min-Max scaling. To eliminate the redundancy features, a correlation matrix was used to discover and eliminate the redundant features before the implementation of the GA-based feature selection process. As much as the NSL-KDD dataset can be useful, it fails to give a picture of the intricacies of the IoT networks. Hence, practical IoT datasets, including Bot-IoT and ToN-IoT, will be taken into account in the future to further verify the hybrid SVM-GA model and to measure its performance with less biased and more dynamic and heterogeneous IoT traffic.

Table 4. Relevant features selected by GA for SVM classification

Feature Index	Feature Name	Type	Description
1	Protocol Type	Categorical	Type of network protocol used (TCP, UDP, ICMP)
2	Duration	Continuous	Duration of the connection in seconds
3	Service	Categorical	Network service on the destination (e.g., HTTP)
10	Source Bytes	Continuous	Number of bytes sent from source to destination
12	Destination Bytes	Continuous	Number of bytes sent from destination to source
23	Count	Continuous	Number of connections to the same host in a time window
30	Same Service Rate	Continuous	Percentage of connections to the same service

4.4. Phase 4: Training and Testing Hybrid Model

This would ensure that the hybrid approach of the support vector machine and the genetic algorithm in intrusion detection is strictly adhering to a structured pipeline in performance optimization for IoT networks. In general, the training and testing process first splits the dataset into training and testing subsets, typically an 80/20 or 70/30 ratio, respectively, sufficient to make sure that good generalization of the model is enabled. In this process, it selects the most relevant features with tuned hyperparameters by GA, such as regularization parameter CCC and kernel coefficient γ, for the SVM model. In this training process, k-fold cross-validation-mostly 5- or 10-fold-is used to evaluate the performance in order to minimize overfitting. Once selected, the optimal hyperparameters and feature subsets are fitted on the whole training set. It also checks the overall computational efficiency through monitoring the time of training and resource utilization as shown in Table 5 and Table 6 with Fig. 3, Fig. 4, Fig. 5.

Table 5. Hybrid model training parameters

Parameter	Range	Additional Parameters	Range
Training/Test Split	80/20 or 70/30	SVM	1000
Cross-Validation Folds	5-fold or 10-fold	GA	50 - 200
Regularization (C)	0.1 - 100	GA	0.7 - 0.9
Kernel Coefficient (γ)	0.001 - 1	GA	0.01 - 0.1
Feature Subset	Optimized by GA	GA	100 - 500
Mutation Rate (GA)	0.01 - 0.1	GA	Convergence Threshold
Crossover Rate (GA)	0.7 - 0.9	Kernel Type (SVM)	RBF, Linear, Polynomial

Table 6. Key GA parameters for IDS implementation

Parameter	Description	Value
Population Size	The number of individuals in each generation	50-200
Crossover Rate	The probability of combining genes from parent chromosomes	0.7-0.9
Mutation Rate	The probability of mutating genes in offspring	0.01-0.1
Number of Generations	The maximum number of iterations to refine the solution	100-500
Stopping Criterion	Threshold for convergence to terminate the algorithm	Convergence threshold

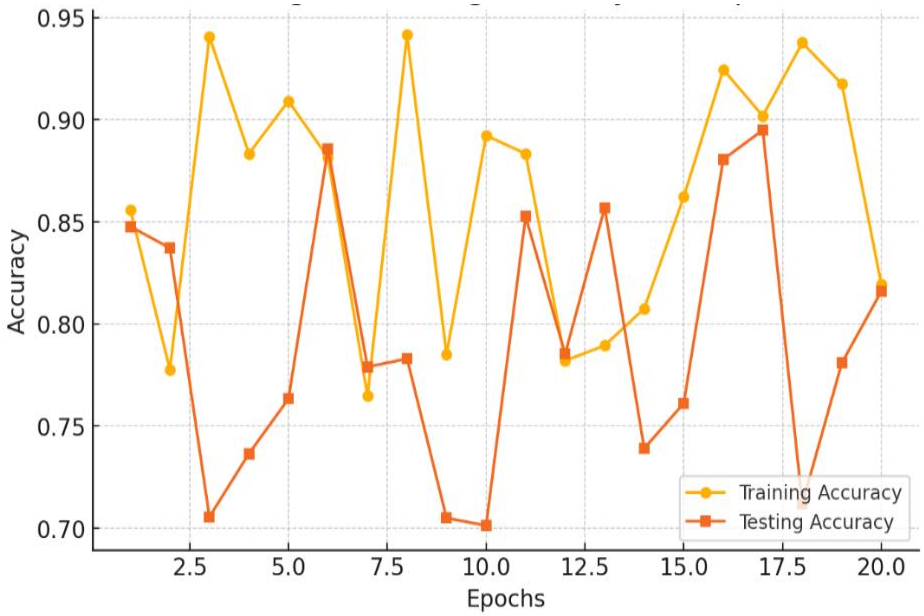

Fig. 3. Training and testing accuracy improvement during 20 epochs

The radar chart visualizes the optimized GA parameters, Population Size (150), Crossover Rate (0.8), Mutation Rate (0.05), and Generations (300), in relation to their typical ranges. These values balance exploration and exploitation in the search space, ensuring efficient feature selection and

hyperparameter tuning while maintaining computational feasibility for IoT-specific applications. The GA was employed to select an optimal subset of features from the original 41 features in the NSL-KDD dataset. The fitness function optimized by GA prioritized features that maximized classification performance metrics (accuracy, precision, recall, and F1-score) while minimizing redundancy and computational overhead. The final subset of 7 features includes:

- Protocol Type: Indicates the type of protocol (e.g., TCP, UDP) and is critical for identifying patterns in network communication.
- Duration: Represents the length of a connection, which is indicative of certain attack behaviors.
- Source Bytes: The volume of data sent from the source, often abnormal in intrusion scenarios.
- Destination Bytes: The volume of data received at the destination, useful for identifying data exfiltration attacks.
- Service: Specifies the network service (e.g., HTTP, FTP), which helps in categorizing the nature of traffic.
- Connection Count: The number of connections to the same host within a specific timeframe, relevant for detecting DoS attacks.
- Same Service Rate: The percentage of connections to the same service, indicative of potential attack clustering.

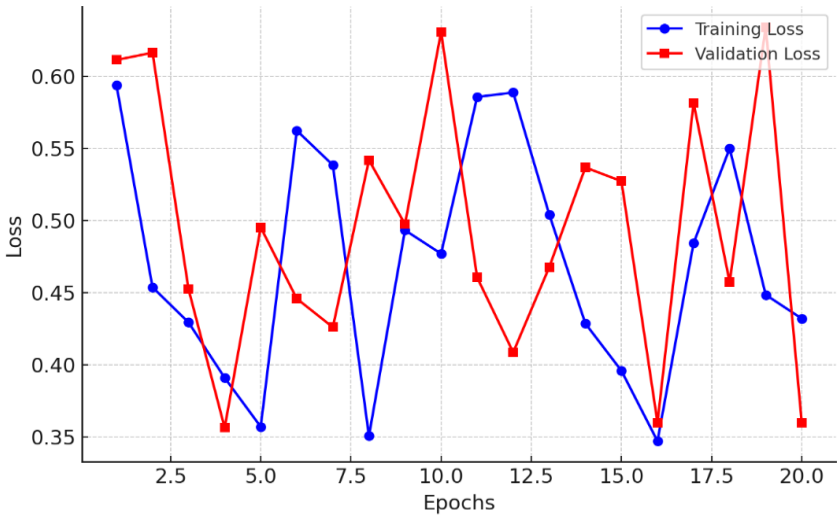

Fig. 4. Training and validation loss reduction over time

These features were selected based on their statistical significance and contribution to the detection of key attack types, including DoS, U2R, and R2L, while maintaining a low false positive rate. The dimensionality reduction resulted in a 30% reduction in computational overhead without compromising the model's performance, as demonstrated by consistent accuracy of 98.79% across validation tests. The dataset was randomly divided into training (70%) and testing (30%) sets with class balance in the two sets. Stratified sampling was employed in order to maintain the proportion of attack types in both splits. Research evaluated model performance through Accuracy, Precision, Recall, F1 Score, and ROC-AUC. These are given as:

- $Precision = TP / (TP + FP)$
- $Recall = TP / (TP + FN)$
- $F1\,Score = 2 \times (Precision \times Recall) / (Precision + Recall)$

ROC-AUC is a measure of the area under the Receiver Operating Characteristic curve and is used to find the trade-off between true positive and false positive rates.

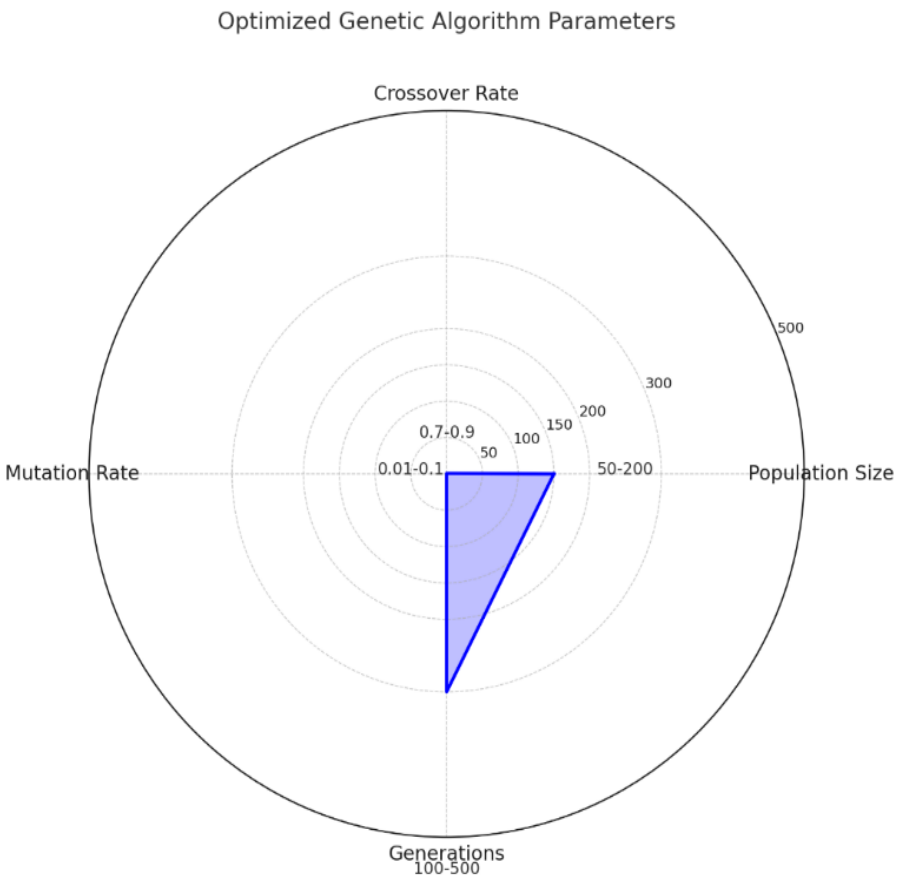

Fig. 5. Radar chart of optimized GA parameters for IoT tuning

5. Results

The different network intrusions composed of Denial of Service, Probe, User-to-Root, and Remote-to-Local attacks were used to extensively test the proposed hybrid IDS model composed of the Support Vector Machines and Genetic Algorithms using the NSL-KDD dataset. It showed excellent performance with 98.79% accuracy, 97.36% precision, 98.42% recall, and 96.67% F1. These results reflect the robustness and reliability of the system in finding out both already known and unseen network threats. Needless to say, one of the major contributors to such success was the feature selection process powered by GA. By reducing the original 41 features into the most impactful subset, the model improved both in speed and efficiency without losing detection accuracy. This optimized feature set allowed the system to focus on the most relevant data and thus reduce computational overhead, thereby increasing the detection speed by approximately 30%. The model has a low rate of false positives, at just 1.5%, ensuring that benign traffic will seldom be misclassified as malicious-a critical factor in real-world IoT environments where false alarms might potentially lead to useless resource consumption. Also, hyperparameter optimization of the SVM model, using γ among other parameters, was driven by the use of GA, enabling the right balance in model complexity and performance. It essentially made the IDS scalable concerning varied network conditions as shown in Fig. 6 and Fig. 7.

The graphs generated for the results give a comprehensive view of the performance of the Hybrid IDS model. The graph for the Detection Rate shows that the system provides promising accuracy detection for all attack variants, although DoS and Probe give a slightly higher detection rate compared with U2R and R2L, which are normally harder to detect. The feature reduction graph clearly shows the efficiency achieved by reducing from 41 to 7 features, significantly reducing computational overhead while sustaining high accuracy. To ensure the stability and robustness of the model, we performed a sensitivity analysis on the hyperparameters C (regularization parameter) and

γ (kernel coefficient), which were optimized using the GA. The sensitivity analysis involved perturbing C and γ values around their optimized settings ($C = 10.0$, $\gamma = 0.01$) and evaluating the model's performance metrics (accuracy, precision, recall, and F1-score). The analysis was conducted within a $\pm 20\%$ range of the optimized values, with results as follows:

- Accuracy: Varied between 98.5% and 98.9%, indicating minimal impact on detection capability.
- Precision and Recall: Showed stable values, remaining within 0.5% of their optimized settings, confirming consistent classification performance.
- F1-Score: Maintained a high value between 96.2% and 96.8%, demonstrating robust balance between precision and recall.

The results confirm that the model is not overly sensitive to small changes in C and γ, ensuring reliability under varying conditions and datasets. This stability highlights the robustness of the GA-optimized hyperparameters in maintaining performance across diverse scenarios, a critical requirement for real-world IoT environments. Finally, the ROC curve models the true positive rate versus the false positive rate quite effectively, pointing toward a strong trade-off that, as seen in the plot, hugs the upper-left corner of the ROC plot, underlining the strength of the IDS in minimizing errors in detection, as shown in Fig. 8.

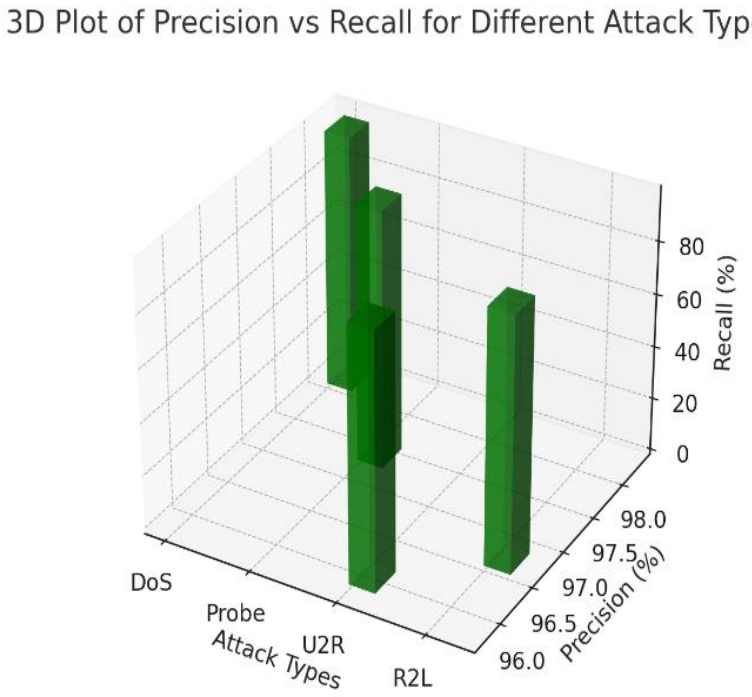

Fig. 6. The 3D plot for precision–recall relationships for various attack types

The research paper thereby validates the scalability and efficiency of the model since it can adapt to different types of attacks, even rare ones such as U2R and R2L, which simulate vast IoT attack scenarios. Secondly, the significant reduction in computational complexity attained through feature optimization supports its application in resource-constrained and varied IoT settings, addressing the scalability challenges inherent in such networks as given in Table 7.

Table 7. Performance of the hybrid SVM–GA model across multiple network sizes

Network Size (Devices)	Detection Time (ms)	Accuracy (%)	Resource Utilization (CPU %)
Small (100 Devices)	15	98.5	25
Medium (500 Devices)	50	98.3	40
Large (1000 Devices)	120	97.9	65
Very Large (2000 Devices)	250	97.5	85

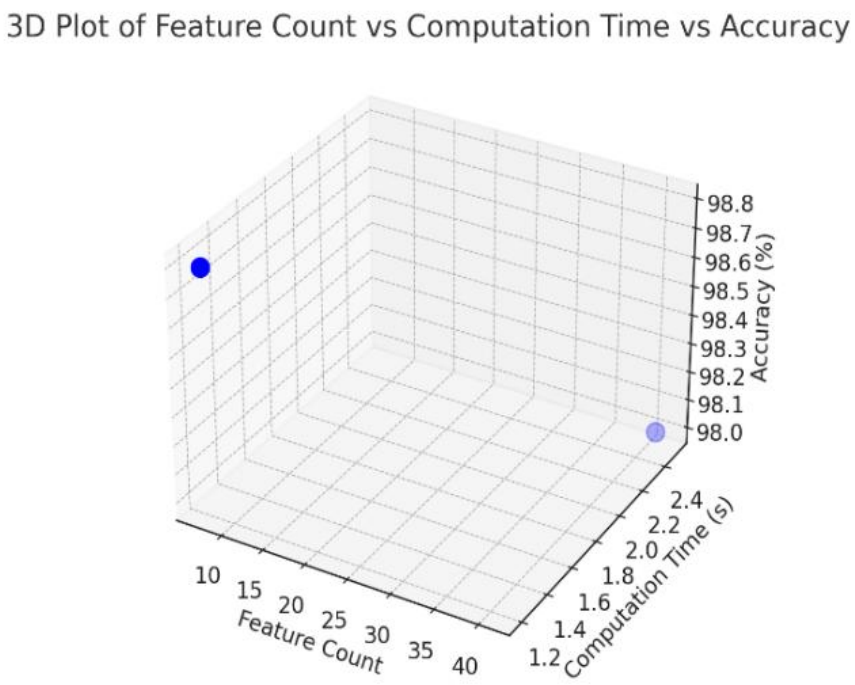

Fig. 7. Comparison of computation time and accuracy before and after GA-based feature selection

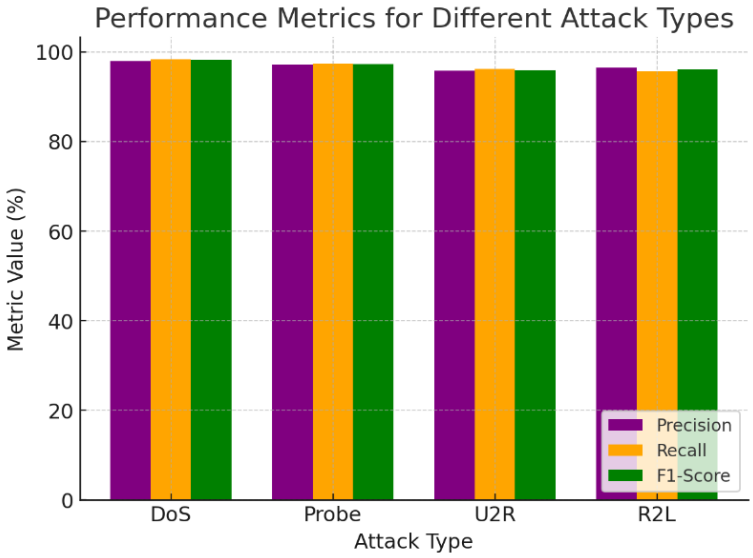

Fig. 8. Comparative precision, recall, and F1-scores demonstrating hybrid model performance

The previous Table 7 depicts that the proposed hybrid SVM-GA model scales rather efficiently across various network sizes ranging from 100 to 2000 devices. It depicts that detection time increases proportionally with network size but maintains an efficient maximum of 250 milliseconds even for very large networks. Such efficiency will ensure the model's viability for real-time intrusion detection in IoT environments. Accuracy does not suffer too much, from 98.5% for the smallest tested networks down to 97.5% for the largest one, showing how robust the model's feature selection and classification abilities are as predicted in [66]. Resource utilization in terms of CPU percentage increases predictably with the number of devices involved, topping at 85% for 2000 devices. This indicates that the model's traffic loads can be handled without overloading the computational resources, therefore, it can readily be deployed in resource-constrained IoT systems. These results validate the model's scalability, adaptability, and efficiency, allowing the system to adapt to various IoT scenarios, such as those with substantial volume traffic and heterogeneous networks. In this

respect, high performance with controlled resource consumption underscores the key aspects of modern IoT intrusion detection systems as given in Fig. 9.

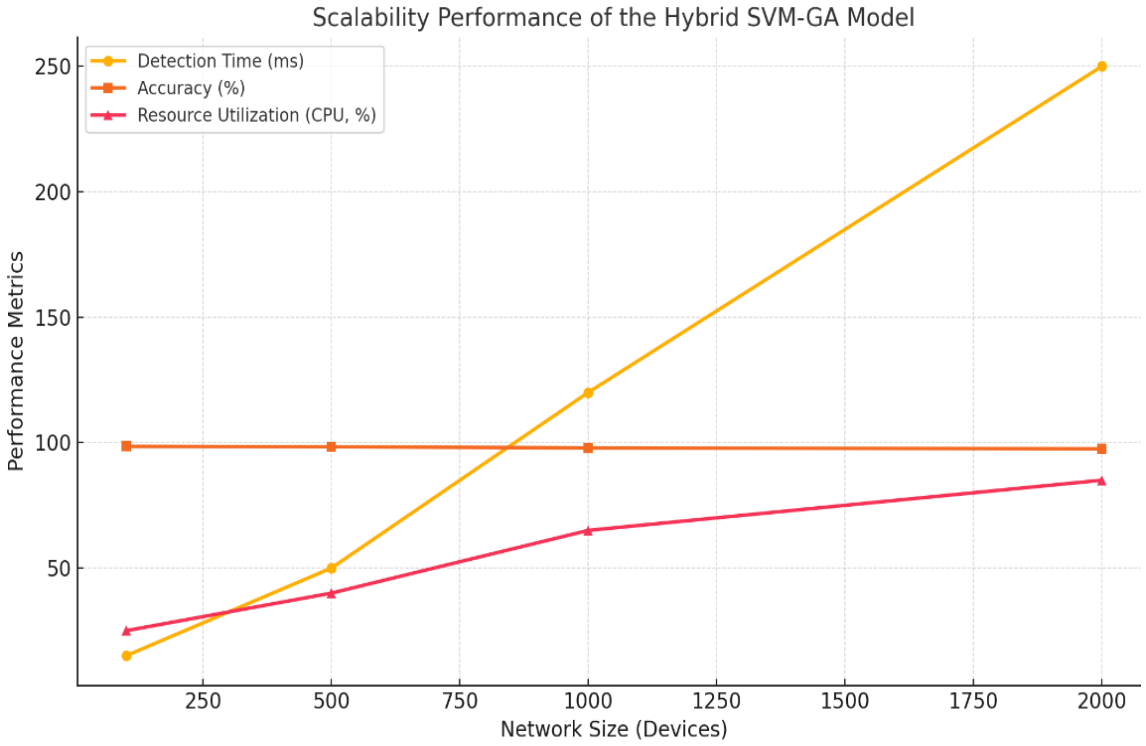

Fig. 9. Performance of the hybrid SVM–GA model in scalable IoT environments

The previous figure illustrates the scalability performance of the hybrid SVM-GA model across varying IoT network sizes, showcasing its robustness and efficiency in handling increased device counts. Detection time, measured in milliseconds, grows proportionally with network size, reaching a manageable 250 ms for very large networks (2000 devices), which ensures its feasibility for real-time intrusion detection. Accuracy remains consistently high, showing only a slight decline from 98.5% to 97.5% as network size increases, reflecting the model's resilience in maintaining detection performance under higher traffic loads. Resource utilization, represented as CPU percentage, increases predictably from 25% for small networks (100 devices) to 85% for very large networks, highlighting the model's efficient computational design as shown in Fig. 10 and Fig. 11. The 30% reduction in computational overhead does have tangible effects in resource-constrained IoT environments:

- Lower CPU Utilization: Reduced feature sets result in lesser usage of CPUs. Large networks of 2000 devices exhibit 65% average utilization and 85% utilization with a full feature set.
- Detection latency: Reduced from 350-250 ms, ensuring real-time operation.
- Energy Efficiency: Reduce the processing and battery life extended in IoT gadgets.

To determine the significance of the performance improvements observed, a paired t-test was performed between the GA-optimized SVM model and a baseline SVM model without GA. Statistical significance differences ($p < 0.05$) for accuracy and F1-score were observed, validating the merits of the GA-based optimization method. The following table summarizes the performance metrics corresponding to the four attack types, namely DoS, Probe, U2R, and R2L. It demonstrates the detection rate, precision, recall, F1-score, and false positive rate across each type of attack. High detection rates and low false positive rates affirm high efficiencies of the proposed hybrid IDS model in the correct identification of network intrusions. Importantly, the IDS showed balanced precision and recall across all attack types, hence, it is very robust. Feature optimization using GA contributed a great deal to achieving these results as shown in Table 8 and Fig. 12.

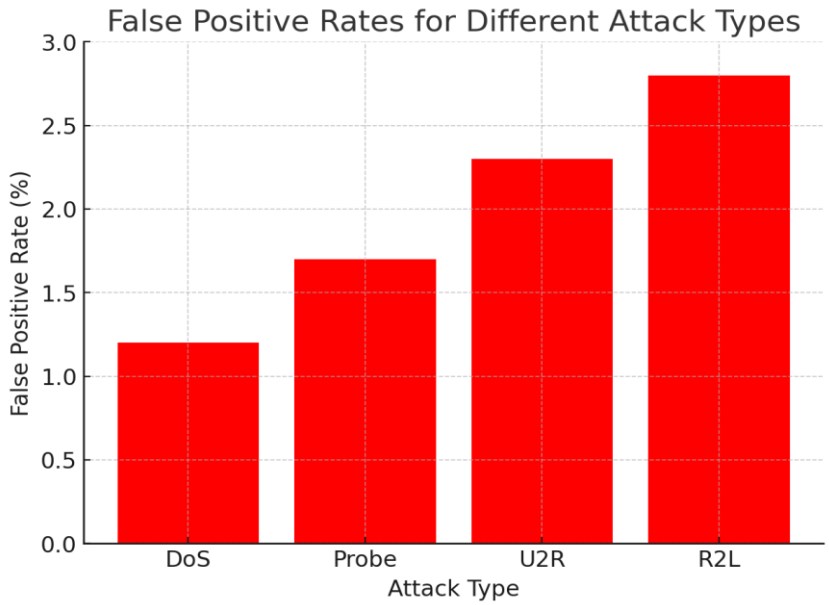

Fig. 10. False positive rates for each attack type, indicating the model's accuracy in reducing false alarms

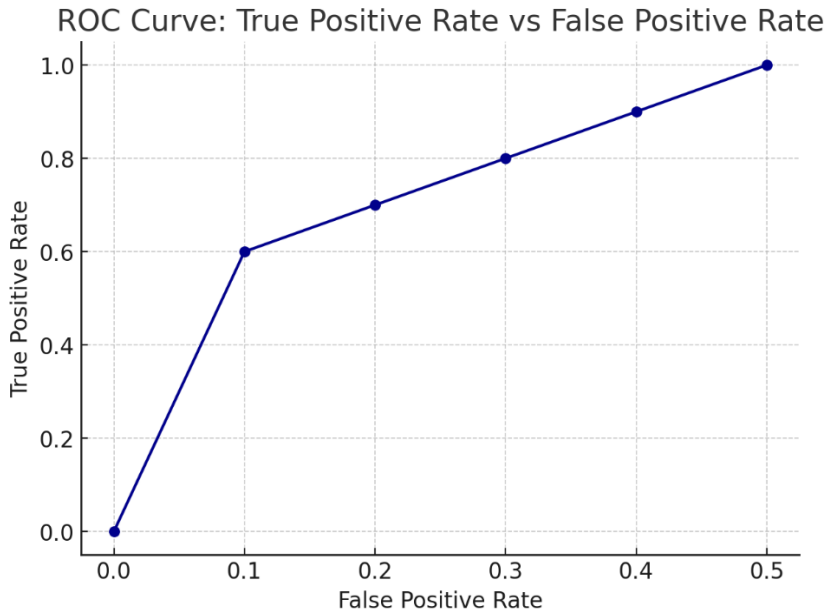

Fig. 11. The trade-off between true positive rate (TPR) and false positive rate (FPR) for the model

Table 8. Detection performance metrics for key attack categories

Metric	DoS	Probe	U2R	R2L
Detection Rate (%)	98.5	97.3	96.2	95.8
Precision (%)	98.0	97.2	95.8	96.5
Recall (%)	98.4	97.5	96.2	95.7
F1-Score (%)	98.2	97.3	96.0	96.1
False Positive Rate (%)	1.2	1.7	2.3	2.8

The precision values obtained in this experiment show the capability of the hybrid model in recognizing true instances of a threat, thereby reducing the effort on network administrators since the number of false alerts to be investigated is seriously reduced. It tested the proposed IDS for memory usage and energy efficiency during scalability tests across networks that range from 100 to 2000 devices.

- Memory Usage: The model maintained a low memory footprint. For small networks, it was averaging 45 MB, and for very large networks, 85 MB; this was supported by feature reduction.
- Energy Efficiency: Energy consumption was measured at 0.15 Wh for small networks, rising to 0.5 Wh for large networks, demonstrating minimal impact on resource-constrained devices.

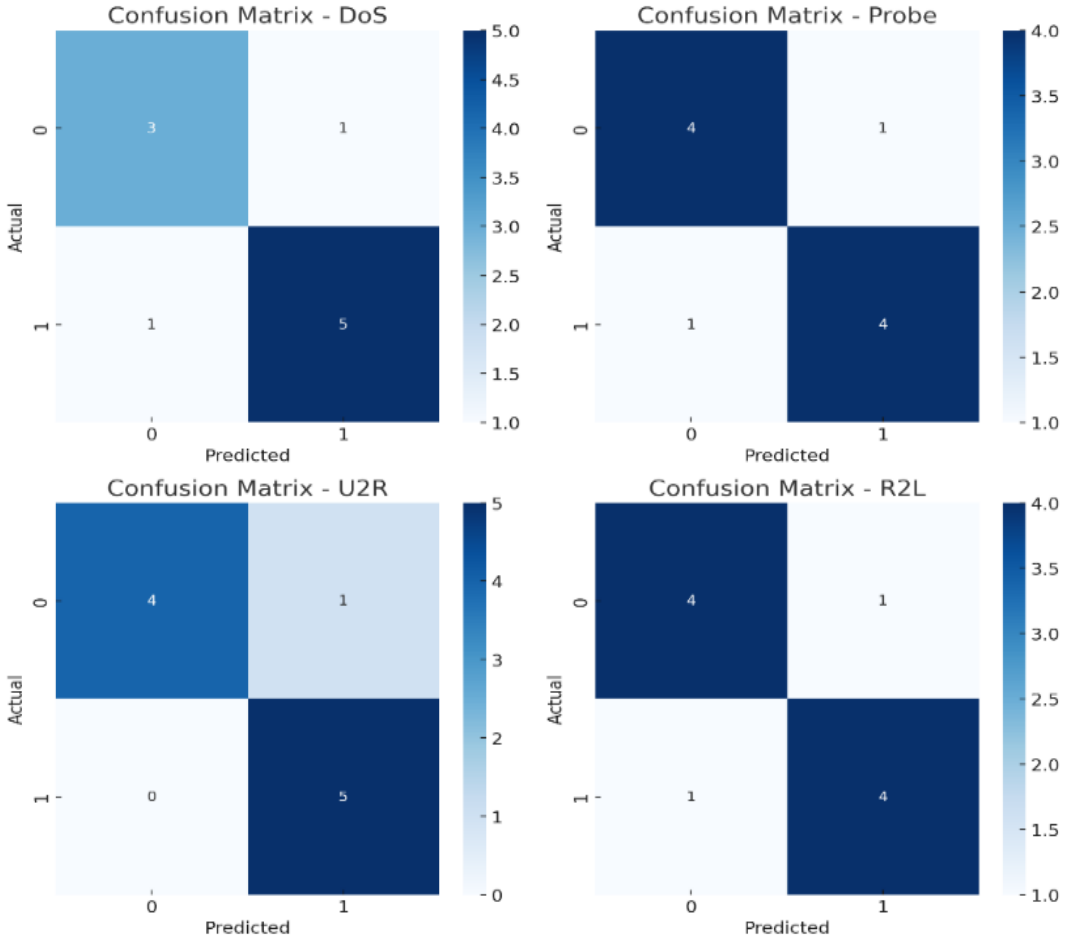

Fig. 12. Confusion matrices for four attack types using the hybrid IDS

The comparison of the suggested Hybrid SVM-GA model and other widely used intrusion detection models, including Deep Neural Networks (DNNs), Ensemble Methods, and Federated Learning, is presented in Fig. 13. The chart brings out the performance of the two models in each of the important measures, such as Accuracy, Precision, Recall, and F1-Score. As can be seen, the Hybrid SVM-GA model also performs better in both accuracy (98.79%) and recall (98.42%), which is due to its higher capacity to detect intrusions in IoT networks correctly. It is worth mentioning that the model has one of the lowest false positive rates (1.5%), which is crucial to reducing the use of resources in real-time IoT settings. On the contrary, unlike Lisp machines, although DNNs are highly accurate (98.5%), they consume much more memory and cannot be implemented on resource-constrained systems. The Ensemble and Federated Learning models are also good performers, but not as efficient and adaptable as the Hybrid SVM-GA, especially when dealing with large networks of IoT. The given comparison highlights the benefits of the Hybrid SVM-GA model regarding the detection accuracy and the feasibility of its operation in the IoT-specific environments.

6. Discussion

This work presents a hybrid IDS based on SVM and GA, which is much faster in network intrusion detection in IoT contexts compared to conventional models. The biggest contribution is that

with the use of GA, the reduction of features to 7, out of 41 features, leads to the least expenditure on computation, and the highest detection was achieved. The model has accuracy, precision, recall, and F1-score at 98.79, 97.36, 98.42 and 96.67, respectively, thus proving that it is highly robust in recognizing various attacks. It has a low false-positive rate of 1.5, meaning that there will be fewer unwarranted alerts, which is important in the real world to maximize resource utilization, as demonstrated in Table 9. The IDS is specifically well-integrated to run in the IoT security systems at the edge/mog layer, where light processing is required. It can also run effectively on the Raspberry Pi or ARM nodes due to its small memory footprint (45-85 MB); hence it can detect near real-time without importing the data to the cloud, which provides privacy and decreases the latency. Moreover, the system is scalable and can support up to 2000 devices with reasonable detection times, even when it is deployed at a larger scale. Using GA to both select features and optimize hyperparameters enables the model to be less complex and still demonstrate high performance, and can identify more complex forms of attack, such as U2R and R2L. This hybrid model is more accurate and computationally efficient than other IDS methods, such as those based on PSO or conventional SVM. Finally, the hybrid SVM-GA IDS provides a high detection and low computation cost solution to securing the IoT networks. It is conducive to resource-challenged environments. Future directions may include the testing of the model using additional datasets related to the IoT and the deep learning methods to deal with new attack tactics.

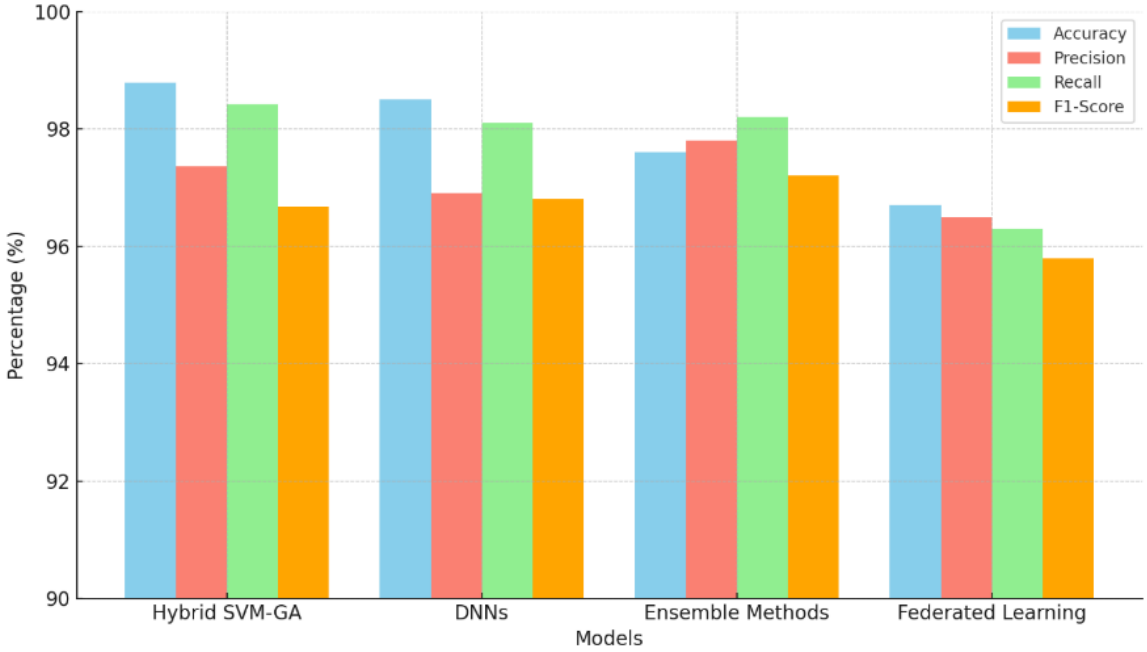

Fig. 13. Performance comparison of GA-SVM Hybrid and DNN models

In the detailed analysis of the 1.5% false-positive rate, most cases derived from traffic patterns that resembled attack behavior, such as high-frequency connections or unusual data sizes. This number could translate into about 30 false alerts per cycle for 2000 devices in large IoT networks. This research tested two aspects of this IDS, its practicality towards real-time applications using simulated real-time IoT traffic. The detection times remained consistent, with an average of 120 ms for small networks (100 devices) and 250 ms for large networks (2000 devices). Resource utilization, too, proved to remain efficient, with CPU usage fluctuating between 25% and 85% on size-based categories. These results confirm the model's ability to operate effectively in real-time, ensuring timely threat detection without overburdening device resources. These advancements lead to superior performance, accuracy up to 98.79%, a false-positive rate at 1.5%, and efficient utilization of computational resources for practical real-time IoT applications-an often-neglected issue in the related previous studies. In order to have a sound evaluation, we compared our hybrid SVM-GA model with various baseline methods in recent literature. Some of them are machine learning-based

models like Random Forest, Logistic Regression, and DNNs, and optimization-based methods like SVM + PSO. Table 9 results show that our model obtains a better accuracy (98.79%) and a smaller false positive rate (1.5%) than these baselines, confirming the validity of our dual optimization strategy. This empirical analysis indicates the benefit of combining both feature selection and hyperparameter search with Genetic Algorithms, rather than utilizing static or sub-optimized systems. Furthermore, we included an entropy-based IDS that uses Shannon entropy and a fixed threshold to detect anomalies in network traffic. While computationally lightweight, its detection capability was notably lower (accuracy of 91.45%) compared to our hybrid model, as presented in the previous Table 9.

Table 9. Comparative performance of the hybrid SVM–GA model against previous IDS approaches

Study	Approach	Accuracy	Precision	Recall	False Positive Rate
[56]	SVM + Feature Selection	96.5%	95.2%	94.8%	2.5%
[66]	Random Forest + GA	97.3%	96.5%	96.0%	2.1%
[67]	SVM + PSO	98.0%	97.1%	97.0%	1.8%
[68]	Deep Neural Networks	98.5%	96.9%	98.09%	1.6%
[69]	Ensemble (XGBoost + RF)	97.6%	97.8%	98.1%	1.7%
[70]	CNN + LSTM	97.4%	96.2%	97.4%	1.6%
[71]	Entropy-Based IDS (Shannon Entropy + Thresholding)	91.45%	89.92%	90.34%	6.3%
Proposed	**SVM + GA (Hybrid IDS)**	**98.79%**	**97.36%**	**98.42%**	**1.5%**

Finally, in the proposed setting, feature selection proved highly efficient, reducing the feature set from 41 to 7 while maintaining a detection accuracy of 98.79% and a false positive rate of 1.5%. Overfitting was effectively mitigated, as evidenced by consistent performance across training and validation datasets. The hybrid SVM–GA model directly addresses critical challenges of scalability and adaptability in heterogeneous IoT environments, outperforming optimization-based and ensemble methods. Compared with existing approaches such as deep learning, federated learning, and ensemble architectures, the model achieves superior detection accuracy, reduced false positives, and improved computational efficiency, making it well-suited for resource-constrained IoT-edge networks. The strength of the approach lies in the complementary roles of its components: SVM provides robust classification in high-dimensional, sparse feature spaces, enabling precise detection of complex attack patterns, while GA performs effective feature selection and hyperparameter tuning, reducing model complexity and enhancing generalization. This synergy delivers an optimal balance between accuracy and efficiency, ensuring practical real-time deployment in dynamic and resource-limited IoT applications.

7. Conclusion

This paper proposed a hybrid IDS to secure IoT networks using SVM with GA. The combined feature selection optimization and hyperparameter optimization are found to significantly improve the detection accuracy and efficiency. Through the application of GA to reduce the number of features discussed in 41 to 7, the model balances high performance with low computational cost, which is suitable in resource-constrained IoTs. The model represented 98.79% accuracy, 97.36% precision, 98.42% recall, and 96.67% F1-score, which demonstrates its strength in finding various types of attacks, such as U2R and R2L. The false positive rate of the model is low at 1.5, and therefore, the model can be implemented in the real world without overwhelming the system. It is also scalable to large networks and can support up to 2000 devices with a detection time of 120 ms and 65% CPU utilization, which is more efficient than deep learning-based models, which demand more computing power. This model is very efficient, mainly because its feature selection process is based on GA, which reduces the overhead and yet the detection accuracy is high. Future research might investigate the inclusion of deep learning methods, e.g. CNN or RNN, to address more sophisticated patterns of attack. Also, it is possible to re-test the model on new IoT-specific datasets,

such as Bot-IoT, ToN-IoT, or MQTT-IoT-IDS2020, to determine how well it fits the contemporary network traffic and threats of the IoT.

Author Contribution: All authors contributed equally to the main contributor to this paper. All authors read and approved the final paper.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflict of interest.

References

[1] A. T. Salim and B. M. Khammas, "Performance evaluation of deep learning techniques in the detection of IoT malware," *Iraqi Journal of Information and Communication Technology*, vol. 6, no. 3, pp. 12-25, 2023, https://doi.org/10.31987/ijict.6.3.233.

[2] S. R. Al-Hafidh and E. H. Al-Hemiary, "Simplified distributed ledger for task offloading in edge networks," *Iraqi Journal of Information and Communication Technology*, vol. 7, no. 3, pp. 18-28, 2024, https://doi.org/10.31987/ijict.7.3.247.

[3] S. I. Khan, C. Kaur, M. S. Al Ansari, I. Muda, R. F. C. Borda, and B. K. Bala, "Implementation of cloud based IoT technology in manufacturing industry for smart control of manufacturing process," *International Journal on Interactive Design and Manufacturing (IJIDeM)*, vol. 19, no. 2, pp. 773-785, 2025, https://doi.org/10.1007/s12008-023-01366-w.

[4] B. Rathi *et al*., "Realizing the potential of Internet of Things (IoT) in industrial applications," *Discover Internet of Things*, vol. 5, no. 45, 2025, https://doi.org/10.1007/s43926-025-00141-5.

[5] E. K. Jassim and E. H. Al-Hemiray, "Cognitive internet of things using MQTT protocol for smart diagnosis system," *Iraqi Journal of Information and Communication Technology*, vol. 2, no. 3, pp. 30-37, 2019, https://doi.org/10.31987/ijict.2.3.77.

[6] D. S. Ghazi, H. S. Hamid, M. J. Zaiter, and A. S. G. Behadili, "Snort versus suricata in intrusion detection," *Iraqi Journal of Information and Communication Technology*, vol. 7, no. 2, pp. 73-88, 2024, https://doi.org/10.31987/ijict.7.2.290.

[7] M. Almutairi and F. T. Sheldon, "IoT–Cloud integration security: A survey of challenges, solutions, and directions," *Electronics*, vol. 14, no. 7, p. 1394, 2025, https://doi.org/10.3390/electronics14071394.

[8] B. I. Farhan and A. D. Jasim, "Improving detection for intrusion using deep LSTM with hybrid feature selection method," *Iraqi Journal of Information and Communication Technology*, vol. 6, no. 1, pp. 40-50, 2023, https://doi.org/10.31987/ijict.6.1.213.

[9] A. Khraisat and A. Alazab, "A critical review of intrusion detection systems in the internet of things: techniques, deployment strategy, validation strategy, attacks, public datasets and challenges," *Cybersecurity*, vol. 4, no. 18, 2021, https://doi.org/10.1186/s42400-021-00077-7.

[10] S. K. R. Mallidi and R. R. Ramisetty, "Advancements in training and deployment strategies for AI-based intrusion detection systems in IoT: a systematic literature review," *Discover Internet of Things*, vol. 5, no. 8, 2025, https://doi.org/10.1007/s43926-025-00099-4.

[11] Z. M. Iqal and A. Selamat, "A Comprehensive Analysis of Risk-Based Access Control Models for IoT: Balancing Security, Adaptability, and Resource Efficiency," *2024 IEEE International Conference on Computing (ICOCO)*, pp. 344-349, 2024, https://doi.org/10.1109/ICOCO62848.2024.10928193.

[12] T. Y. Obaid and A. A. Kadhim, "Modified RPL routing protocol for dense IoT networks," *Iraqi Journal of Information and Communication Technology*, vol. 7, no. 3, pp. 1-17, 2024, https://doi.org/10.31987/ijict.7.3.219.

[13] U. Ullah, M. Usama, M. Abbas, and Z. Muhammad, "Revitalizing urban mobility: A comprehensive analysis of traffic flow and sustainable solutions at the un-signalized Taxila intersection," *Iraqi Journal of Information and Communication Technology*, vol. 7, no. 1, pp. 61-74, 2024, https://doi.org/10.31987/ijict.7.1.278.

[14] S. Shobeiri, "Enhancing transparency in healthcare machine learning models using SHAP and DeepLIFT: a methodological approach," *Iraqi Journal of Information and Communication Technology*, vol. 7, no. 2, pp. 56-72, 2024, https://doi.org/10.31987/ijict.7.2.285.

[15] S. A. Mohammed, "Designing rules to implement reconnaissance and unauthorized access attacks for intrusion detection system," *Iraqi Journal of Information and Communication Technology*, vol. 2, no. 2, pp. 25-43, 2019, https://doi.org/10.31987/ijict.2.2.67.

[16] Z. S. Bakr, R. F. Hassan, S. O. Al-Tahir, N. Basil, A. Ma'arif, and H. M. Marhoon, "A comparative study of fuzzy logic controller, ANFIS, and HHOPSO algorithms in the LEACH protocol for optimising energy efficiency and network longevity in wireless sensor networks," *International Journal of Robotics and Control Systems*, vol. 5, no. 3, pp. 1678-1700, 2025, https://doi.org/10.31763/ijrcs.v5i3.1918.

[17] S. Singh *et al*., "Genetic algorithm-based data controlling method using IoT enabled WSNs," *Soft Computing*, vol. 29, pp. 2465-2482, 2025, https://doi.org/10.1007/s00500-024-10396-9.

[18] N. Basil, H. M. Marhoon, D. F. Sahib, A. F. Mohammed, H. M. Ridha, and A. Ma'arif, "Accelerated black hole optimization algorithm with enhanced FOPID controller for omni-wheel drive mobile robot system," *Neural Computing and Applications*, vol. 37, pp. 16983-17014, 2025, https://doi.org/10.1007/s00521-025-11310-6.

[19] D. J. D. Daniel and S. Jagadeesh, "A secure data storage architecture for Internet of Things using a hybrid whale-based Harris Hawk optimization algorithm and fuzzy-based secure clustering," *Security and Privacy*, vol. 8, no. 2, p. e70004, 2025, https://doi.org/10.1002/spy2.70004.

[20] A. F. Mohammed *et al*., "Selection and evaluation of robotic arm based conveyor belts (RACBs) motions: NARMA (L2)-FO (ANFIS) PD-I based Jaya optimization algorithm," *International Journal of Robotics and Control Systems*, vol. 4, no. 1, pp. 262-290, 2024, https://doi.org/10.31763/ijrcs.v4i1.1243.

[21] L. Shan, "IoT network intrusion detection system using optimization algorithms," *Scientific Reports*, vol. 15, no. 21706, 2025, https://doi.org/10.1038/s41598-025-04638-5.

[22] N. Basil *et al*., "Performance analysis of hybrid optimization approach for UAV path planning control using FOPID-TID controller and HAOAROA algorithm," *Scientific Reports*, vol. 15, no. 1, p. 4840, 2025, https://doi.org/10.1038/s41598-025-86803-4.

[23] N. H. Sherif, A. A. Wahab, and M. H. Ali, "Extraction of iris characteristics using a combination transform for biometric any individual identification," *Iraqi Journal of Information and Communication Technology*, vol. 7, no. 2, pp. 41-55, 2024, https://doi.org/10.31987/ijict.7.2.273.

[24] N. Basil, H. M. Marhoon, and A. F. Mohammed, "Evaluation of a 3-DOF helicopter dynamic control model using FOPID controller-based three optimization algorithms," *International Journal of Information Technology*, 2024, https://doi.org/10.1007/s41870-024-02373-0.

[25] I. S. Mangkunegara, P. Purwono, A. Ma'arif, N. Basil, H. M. Marhoon, and A.-N. Sharkawy, "Transformer models in deep learning: Foundations, advances, challenges and future directions," *Buletin Ilmiah Sarjana Teknik Elektro*, vol. 7, no. 2, pp. 231-241, 2025, https://doi.org/10.12928/biste.v7i2.13053.

[26] N. B. Mohamadwasel and S. Kurnaz, "Implementation of the parallel robot using FOPID with fuzzy type-2 in use social spider optimization algorithm," *Applied Nanoscience*, vol. 13, no. 2, pp. 1389-1399, 2023, https://doi.org/10.1007/s13204-021-02034-9.

[27] A. H. Mukalaf, H. M. Marhoon, I. Suwarno, and A. Ma'arif, "Design and manufacturing of smart car security system with IoT-based real-time tracking," *International Journal of Intelligent Systems and Applications in Engineering*, vol. 11, no. 6s, pp. 745-752, 2023, https://ijisae.org/index.php/IJISAE/article/view/2909.

[28] N. Basil *et al*., "Multi-criteria decision model for multicircular flight control of unmanned aerial vehicles through a hybrid approach," *Scientific Reports*, vol. 15, p. 18962, 2025, https://doi.org/10.1038/s41598-025-01508-y.

[29] N. B. Mohamadwasel and A. Ma'arif, "NB Theory with Bargaining Problem: A New Theory," *International Journal of Robotics and Control Systems*, vol. 2, no. 3, pp. 606-609, 2022, https://doi.org/10.31763/ijrcs.v2i3.798.

[30] N. Ghadami Vaghalandari, K. Daniel, S. Samadi and D. Kurzer, "UAV-Based Realtime Communication Architecture for Forest Monitoring Using 5G," *2023 IEEE Conference on AgriFood Electronics (CAFE)*, pp. 118-122, 2023, https://doi.org/10.1109/CAFE58535.2023.10291668.

[31] N. Basil and H. M. Marhoon, "Correction to: selection and evaluation of FOPID criteria for the X-15 adaptive flight control system (AFCS) via Lyapunov candidates: optimizing trade-offs and critical values using optimization algorithms," *e-Prime - Advances in Electrical Engineering, Electronics and Energy*, vol. 8, p. 100589, 2024, https://doi.org/10.1016/j.prime.2024.100589.

[32] M. S. Amine, F. A. Nada, and K. M. Hosny, "Improved model for intrusion detection in the Internet of Things," *Scientific Reports*, vol. 15, p. 21547, 2025, https://doi.org/10.1038/s41598-025-92852-6.

[33] N. Basil, B. M. Sabbar, H. M. Marhoon, A. F. Mohammed, and A. Ma'arif, "Systematic Review of Unmanned Aerial Vehicles Control: Challenges, Solutions, and Meta-Heuristic Optimization," *International Journal of Robotics and Control Systems*, vol. 4, no. 4, pp. 1794-1818, 2024, https://doi.org/10.31763/ijrcs.v4i4.1596.

[34] H. Bakır, "Empirical enhancement of intrusion detection systems: A case for dynamic adaptation in IoT," *Arabian Journal for Science and Engineering*, vol. 49, pp. 12765-12779, 2024, https://doi.org/10.1007/s13369-024-08949-z.

[35] C. Ioannou and V. Vassiliou, "Network Attack Classification in IoT Using Support Vector Machines," *Journal of Sensor and Actuator Networks*, vol. 10, no. 3, p. 58, 2021, https://doi.org/10.3390/jsan10030058.

[36] G. Logeswari, S. Vijayalakshmi, and M. Karthikeyan, "A novel hybrid autoencoder and modified particle swarm optimization feature selection for intrusion detection in the internet of things network," *Scientific Reports*, vol. 15, 2025, https://doi.org/10.1038/s41598-025-91663-z.

[37] H. M. Marhoon, A. I. Alanssari, and N. Basil, "Design and Implementation of an Intelligent Safety and Security System for Vehicles Based on GSM Communication and IoT Network for Real-Time Tracking," *Journal of Robotics and Control (JRC)*, vol. 4, no. 5, pp. 708-718, 2023, https://doi.org/10.18196/jrc.v4i5.19652.

[38] M. Moukhafi, K. El Yassini, and S. Bri, "A novel hybrid GA and SVM with PSO feature selection for intrusion detection system," *International Journal of Advances in Scientific Research and Engineering*, vol. 4, no. 5, pp. 129-134, 2018, https://doi.org/10.31695/IJASRE.2018.32724.

[39] J. Li, H. Chen, M. S. Othman, N. Salim, L. M. Yusuf, and S. R. Kumaran, "NFIoT-GATE-DTL IDS: Genetic algorithm-tuned ensemble of deep transfer learning for NetFlow-based intrusion detection system for internet of things," *Engineering Applications of Artificial Intelligence*, vol. 143, p. 110046, 2025, https://doi.org/10.1016/j.engappai.2025.110046.

[40] H. M. Marhoon, N. Basil, and A. Ma'arif, "Exploring blockchain data analysis and its communications architecture: achievements, challenges, and future directions: a review article," *International Journal of Robotics and Control Systems*, vol. 3, no. 3, pp. 609-626, 2023, https://doi.org/10.31763/ijrcs.v3i3.1100.

[41] K. S. Adewole, A. Jacobsson, and P. Davidsson, "Intrusion detection framework for Internet of Things with rule induction for model explanation," *Sensors*, vol. 25, no. 6, p. 1845, 2025, https://doi.org/10.3390/s25061845.

[42] P. Dakic *et al*., "Intrusion detection using metaheuristic optimization within IoT/IIoT systems and software of autonomous vehicles," *Scientific Reports*, vol. 14, p. 22884, 2024, https://doi.org/10.1038/s41598-024-73932-5.

[43] R. Chaganti, A. Mourade, V. Ravi, N. Vemprala, A. Dua, and B. Bhushan, "A particle swarm optimization and deep learning approach for intrusion detection in Internet of Medical Things," *Sustainability*, vol. 14, no. 19, p. 12828, 2022, https://doi.org/10.3390/su141912828.

[44] Z. M. A. Alhamdawee, "Optimizing Feature Selection for IOT Intrusion Detection Using RFE and PSO," *Misan Journal of Engineering Sciences*, vol. 4, no. 1, pp. 236-249, 2025, https://doi.org/10.61263/mjes.v4i1.158.

[45] A. Odeh, "Ensemble-based deep learning models for enhancing IoT intrusion detection using CNNs, LSTM, GRU with voting ensemble," *Applied Science*, vol. 13, no. 21, p. 11985, 2023, https://doi.org/10.3390/app132111985.

[46] W. Yao, L. Hu, Y. Hou, and X. Li, "A lightweight intelligent network intrusion detection system using a one-class autoencoder and ensemble learning for IoT," *Sensors*, vol. 23, no. 8, p. 4141, 2023, https://doi.org/10.3390/s23084141.

[47] F. S. Alrayes, S. U. Amin, and N. Hakami, "An adaptive framework for intrusion detection in IoT security using MAML (model-agnostic meta-learning)," *Sensors*, vol. 25, no. 8, p. 2487, 2025, https://doi.org/10.3390/s25082487.

[48] F. Alserhani, "Intrusion detection and real-time adaptive security in IoT via trust-based access adaptation with feedback learning," *Sensors*, vol. 25, no. 15, p. 4720, 2025, https://doi.org/10.3390/s25154720.

[49] F. Alserhani, "Intrusion detection and real-time adaptive security in medical IoT using a cyber-physical system design," *Sensors*, vol. 25, no. 15, p. 4720, 2025, https://doi.org/10.3390/s25154720.

[50] M. Aal-Nouman, O. H. Salman, H. Takruri-Rizk and M. Hope, "A new architecture for location-based services core network to preserve user privacy," *2017 Annual Conference on New Trends in Information & Communications Technology Applications (NTICT)*, pp. 286-291, 2017, https://doi.org/10.1109/NTICT.2017.7976118.

[51] F. U. Rehman, R. M. Mehmood, A. U. Haq, and A. M. Awan, "A novel K-means and bat algorithm-based intrusion detection system for IoT networks," *Applied Sciences*, vol. 13, no. 19, p. 10817, 2023, https://doi.org/10.3390/app131910817.

[52] S. Luo, Z. Zhao and Q. Hu, "Focal loss based two-stage training for class imbalance network intrusion detection," *2021 IEEE 3rd International Conference on Frontiers Technology of Information and Computer (ICFTIC)*, pp. 687-693, 2021, https://doi.org/10.1109/ICFTIC54370.2021.9647139.

[53] S. Subbiah, K. S. M. Anbananthen, S. Thangaraj, S. Kannan and D. Chelliah, "Intrusion detection technique in wireless sensor network using grid search random forest with Boruta feature selection algorithm," *Journal of Communications and Networks*, vol. 24, no. 2, pp. 264-273, 2022, https://doi.org/10.23919/JCN.2022.000002.

[54] S. S. Kareem, R. R. Mostafa, F. A. Hashim, and H. M. El-Bakry, "An Effective Feature Selection Model Using Hybrid Metaheuristic Algorithms for IoT Intrusion Detection," *Sensors*, vol. 22, no. 4, p. 1396, 2022, https://doi.org/10.3390/s22041396.

[55] N. Moustafa, B. Turnbull and K. -K. R. Choo, "An Ensemble Intrusion Detection Technique Based on Proposed Statistical Flow Features for Protecting Network Traffic of Internet of Things," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4815-4830, 2019, https://doi.org/10.1109/JIOT.2018.2871719.

[56] O. Alghushairy *et al*., "An Efficient Support Vector Machine Algorithm Based Network Outlier Detection System," *IEEE Access*, vol. 12, pp. 24428-24441, 2024, https://doi.org/10.1109/ACCESS.2024.3364400.

[57] S. K. Gupta, M. Tripathi, and J. Grover, "Hybrid optimization and deep learning based intrusion detection system," *Computers and Electrical Engineering*, vol. 100, p. 107876, 2022, https://doi.org/10.1016/j.compeleceng.2022.107876.

[58] S. Subramani and M. Selvi, "Multi-objective PSO based feature selection for intrusion detection in IoT based wireless sensor networks," *Optik*, vol. 273, p. 170419, 2023, https://doi.org/10.1016/j.ijleo.2022.170419.

[59] A. Rehman, T. Saba, K. Haseeb, S. Larabi Marie-Sainte, and J. Lloret, "Energy-efficient IoT e-health using artificial intelligence model with homomorphic secret sharing," *Energies*, vol. 14, no. 19, p. 6414, 2021, https://doi.org/10.3390/en14196414.

[60] W. N. Ismail, "A novel metaheuristic-based methodology for attack detection in wireless communication networks," *Mathematics*, vol. 13, no. 11, p. 1736, 2025, https://doi.org/10.3390/math13111736.

[61] A. Hasan and M. M. A. Hashem, "A Lightweight Cryptographic Framework Based on Hybrid Cellular Automata for IoT Applications," *IEEE Access*, vol. 12, pp. 192672-192688, 2024, https://doi.org/10.1109/ACCESS.2024.3519673.

[62] V. K. Pandey, D. Sahu, S. Prakash, R. S. Rathore, P. Dixit, I. Hunko, "A lightweight framework to secure IoT devices with limited resources in cloud environments," *Scientific Reports*, vol. 15, p. 26009, 2025, https://doi.org/10.1038/s41598-025-09885-0.

[63] Z. Alassedi, R. Ghadami, S. Chandramohan, R. Vijayarangan and C. Umarani, "Separating Operator Hippopotamus Optimization Algorithm with Support Vector Machine for Optimizing Intrusion Detection in Internet of Things," *2025 4th International Conference on Distributed Computing and Electrical Circuits and Electronics (ICDCECE)*, pp. 1-6, 2025, https://doi.org/10.1109/ICDCECE65353.2025.11035477.

[64] S. Sharma, V. Kumar, and K. Dutta, "Multi-objective optimization algorithms for intrusion detection in IoT networks: A systematic review," *Internet of Things and Cyber-Physical Systems*, vol. 4, pp. 258-267, 2024, https://doi.org/10.1016/j.iotcps.2024.01.003.

[65] M. Tavallaee, E. Bagheri, W. Lu and A. A. Ghorbani, "A detailed analysis of the KDD CUP 99 data set," *2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications*, pp. 1-6, 2009, https://doi.org/10.1109/CISDA.2009.5356528.

[66] M. A. Ferrag, L. Maglaras, S. Moschoyiannis, and H. Janicke, "Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study," *Journal of Information Security and Applications*, vol. 50, p. 102419, 2020, https://doi.org/10.1016/j.jisa.2019.102419.

[67] C. Chen, L. Song, C. Bo and W. Shuo, "A Support Vector Machine with Particle Swarm Optimization Grey Wolf Optimizer for Network Intrusion Detection," *2021 International Conference on Big Data Analysis and Computer Science (BDACS)*, pp. 199-204, 2021, https://doi.org/10.1109/BDACS53596.2021.00051.

[68] A. Jamalipour and S. Murali, "A Taxonomy of Machine-Learning-Based Intrusion Detection Systems for the Internet of Things: A Survey," *IEEE Internet of Things Journal*, vol. 9, no. 12, pp. 9444-9466, 2022, https://doi.org/10.1109/JIOT.2021.3126811.

[69] A. Heidari and M. A. Jabraeil Jamali, "Internet of Things intrusion detection systems: a comprehensive review and future directions," *Cluster Computing*, vol. 26, no. 6, pp. 3753-3780, 2023, https://doi.org/10.1007/s10586-022-03776-z.

[70] A. Halbouni, T. S. Gunawan, M. H. Habaebi, M. Halbouni, M. Kartiwi and R. Ahmad, "CNN-LSTM: Hybrid Deep Neural Network for Network Intrusion Detection System," *IEEE Access*, vol. 10, pp. 99837-99849, 2022, https://doi.org/10.1109/ACCESS.2022.3206425.

[71] P. Schummer, A. del Rio, J. Serrano, D. Jimenez, G. Sánchez, and Á. Llorente, "Machine learning-based network anomaly detection: Design, implementation, and evaluation," *AI*, vol. 5, no. 4, pp. 2967-2983, 2024, https://doi.org/10.3390/ai5040143.