Computers, Materials & Continua

Tech Science Press

Doi:10.32604/cmc.2025.075212

ARTICLE

An Intelligent Multi-Stage GA–SVM Hybrid Optimization Framework for Feature Engineering and Intrusion Detection in Internet of Things Networks

Isam Bahaa Aldallal[1], Abdullahi Abdu Ibrahim[1,*] and Saadaldeen Rashid Ahmed[2,3]

[1]Department of Electrical and Computer Engineering, Altinbas University, Istanbul, 34000, Türkiye
[2]Artificial Intelligence Engineering Department, College of Engineering, Al-Ayen University, An Nasiriyah, 64006, Iraq
[3]Computer Science, Bayan University, Erbil, 44001, Iraq

*Corresponding Author: Abdullahi Abdu Ibrahim. Email: abdullahi.ibrahim@altinbas.edu.tr

Received: 27 October 2025; Accepted: 25 November 2025; Published: 10 February 2026

ABSTRACT: The rapid growth of IoT networks necessitates efficient Intrusion Detection Systems (IDS) capable of addressing dynamic security threats under constrained resource environments. This paper proposes a hybrid IDS for IoT networks, integrating Support Vector Machine (SVM) and Genetic Algorithm (GA) for feature selection and parameter optimization. The GA reduces the feature set from 41 to 7, achieving a 30% reduction in overhead while maintaining an attack detection rate of 98.79%. Evaluated on the NSL-KDD dataset, the system demonstrates an accuracy of 97.36%, a recall of 98.42%, and an F1-score of 96.67%, with a low false positive rate of 1.5%. Additionally, it effectively detects critical User-to-Root (U2R) attacks at a rate of 96.2% and Remote-to-Local (R2L) attacks at 95.8%. Performance tests validate the system's scalability for networks with up to 2000 nodes, with detection latencies of 120 ms at 65% CPU utilization in small-scale deployments and 250 ms at 85% CPU utilization in large-scale scenarios. Parameter sensitivity analysis enhances model robustness, while false positive examination aids in reducing administrative overhead for practical deployment. This IDS offers an effective, scalable, and resource-efficient solution for real-world IoT system security, outperforming traditional approaches.

KEYWORDS: Cybersecurity; intrusion detection system (IDS); IoT; support vector machines (SVM); genetic algorithms (GA); feature selection; NSL-KDD dataset; anomaly detection

1 Introduction

The Internet of Things (IoT) is transforming the way we live and work, offering enhanced connectivity and automation across various domains such as healthcare, smart homes, industrial systems, and transportation. However, this rapid growth has also been accompanied by an increase in cyber threats. IoT deployments often lack sufficient built-in security mechanisms, and as highlighted in, IoT systems typically have limited computational resources and power constraints, making them more vulnerable compared to traditional computing infrastructures. Securing these networks is crucial, as they often involve sensitive data transmission and control over critical infrastructure [1]. According to, Intrusion Detection Systems (IDS) play a pivotal role in IoT security by monitoring network traffic patterns for anomalies and generating alerts to system administrators regarding potential intrusions [2]. However, many traditional IDS models may not be well-suited for IoT networks due to their complex and dynamic nature. As noted in, such environments require security solutions that are resource-efficient and capable of adapting to diverse device types, communication protocols, and traffic patterns [3,4].

Machine learning approaches are used to develop intrusion detection systems by classifying network traffic. The challenge of applying machine learning techniques in IoT networks is that traditional models cannot cope with high computational requirements and tuned parameters [5]. Thus, there is a requirement for an IDS that provides high accuracy with low computational cost. The motivation behind this study is to develop a hybrid IDS using a support vector machine (SVM) and a genetic algorithm (GA) for enhancing the features of intrusion detection in IoT environments. The hybrid model aims to perform feature selection and tuning of several parameters so that the system can be implemented in resource-constrained IoT environments [6]. Modern cyber-attacks such as DDoS, Man-in-the-middle, and data theft on IoT devices have made traditional signature-based methods obsolete. Since most of the methods are signature-based, they are not effective against novel threats. Hence, more dynamic and adaptive intrusion detection systems are required. Another challenge is the various types of IoT networks; these environments contain many devices with different capabilities, which makes it more difficult to secure them [7]. Machine learning approaches, particularly SVM, have been proven effective in performing intrusion detection classification due to their ability to handle high-dimensional and complex datasets [8]. Due to heterogeneity, limited computation capabilities, and resource constraints of IoT devices, intrusion detection in IoT networks has specific challenges. The increasing complexity and dynamic nature of IoT traffic make it difficult for conventional intrusion detection systems (IDS) to adapt. Furthermore, the detection accuracy is affected by a high rate of false positives arising from ineffective feature selection on large datasets.

This research aims to combine the strengths of SVM and GA to make an IDS better by boosting its precision and recall, and cutting down on system costs. Standard IDSs often produce high false-positive rates in IoT networks because IoT traffic is usually varied and dynamic, which results in low trust between normal and malicious activities.

- Resource constraints in IoT devices in general, IoT devices are both computationally and energetically constrained; thus, traditional resource-intensive IDS methods cannot work efficiently in those kinds of environments and be considered practical for real-time intrusion detection.
- Unable to handle high-dimensional data for intrusion detection in IoT environments includes high-dimensional data processing. Classic machine learning models cannot handle high-dimensionality without proper feature selection, which introduces the problems of reduced accuracy and increased computational overhead.
- Suboptimal hyperparameter tuning of ML is often done in a manner that is not effective manually in traditional approaches of IDS, hence making the algorithm suboptimal and unable to adapt to the ever-changing threats in IoT networks.
- Limited scalability of current IDS solutions in current IDS models is not created to scale with the ever-increasing number of IoT devices, thus forming challenges in maintaining performance while the network grows and its traffic patterns become more complex.

This work is dedicated to the development of an optimized hybrid IDS, elaborated to meet specific IoT network needs. It combines SVM with the GA to offer improvement in detection rates while at the same time reducing the false positives and considering efficient resource utilization. This is to find the limitations of traditional IDS systems in handling the complexity of IoT environments, given that there are resource-constrained and multi-vector attacks that are highly susceptible.

- Improvement of Detection Accuracy: The main goal of this research work is therefore to enhance intrusion detection accuracy in IoT networks by proposing a hybrid model, combining Support Vector Machine, thereby efficiently classifying the normal and malicious network activities.

- Optimizing Computational Efficiency: This research thus proposes the utilization of GAs for feature selection and optimization of hyperparameters to be able to utilize resources efficiently with maximum detection performance.
- Reducing False Positives: Among the main aims of the work is the reduction of false positives in intrusion detection in IoT devices by proposing an efficient classification mechanism based on a feature selection methodology that selects only relevant features and optimizes the decision boundaries.
- Developing a Scalable Solution: Therein, the study will design an IDS that can be scaled up while the number of IoT devices keeps growing. Most importantly, its performance increases with network size and complexity in traffic.
- Real-World IoT Practical IDS: The intention is to propose a hybrid IDS model which is not only theoretically robust but practical and implementable in real-world IoT environments, balancing its detection capability with those confines inherent in IoT devices.

Our contributions can be focused on the following points:

- Hybrid SVM-GA Model: Unique integration of feature selection and hyperparameter optimization using Genetic Algorithms, reducing the feature set from 41 to 7, while maintaining high accuracy (98.79%) and low false positive rates (1.5%).
- Scalability and Efficiency: Thorough validation for scalability and efficiency properties of the model with varying sizes of IoT networks, ranging from 100 to 2000 devices, for an actual real-time application.
- Robust Performance: Comprehensive evaluation on diverse attack types, including rare ones like U2R and R2L, demonstrating adaptability and robustness in IoT-specific scenarios.
- Practical Applicability: Designed specifically for resource-constrained IoT environments, addressing key gaps in existing intrusion detection research.

The rest of this paper is structured as follows: Section 2 reviews existing research on IDS models, especially for IoT. Section 3 presents our hybrid approach using SVM and GA. Section 4 presents and examines the experimental results. Section 5 talks about comparison highlights the superiority of the hybrid SVM + GA approach, which outperforms previous models in terms of accuracy, precision, recall, and false positive rate, offering a more efficient and effective solution for intrusion detection in IoT networks. Finally, Section 6 summarizes the conclusion of the paper.

2 Literature Review

The increasing number of security breaches in IoT networks has made intrusion detection a significant concern in the field of cybersecurity. Detecting cyber-attacks in IoT environments quickly is challenging due to the complex nature of network traffic and the diversity of connected devices [9]. Researchers have extensively explored various machine learning and the best tech methods to address this issue. Traditional signature-based IDSs, which have been around for many years, struggle to keep up with new attacks or evolving IoT networks [10]. This limitation has led researchers to explore alternative solutions, including machine learning-based IDSs, which can learn and adapt to network behavior. Support Vector Machines are commonly used for network intrusion detection due to their ability to handle large datasets and perform well on binary classification tasks. Studies, such as [11], indicate that SVM can achieve better accuracy compared to traditional methods like Decision Trees or k-nearest neighbors in intrusion detection. However, SVM requires extensive hyperparameter tuning and feature selection, which can be challenging in resource-constrained IoT environments. Another limitation is the high computational requirements of SVM models, making them less suitable for IoT devices with limited processing power and memory. Recent research has explored optimization techniques, such as Genetic Algorithms, for improving machine learning models used in IDS [12]. GA can be employed for feature selection and hyperparameter tuning for some machine

learning algorithms, enhancing their efficiency and effectiveness. Research [13] indicates that using GA for feature selection achieves a high detection rate in IDS, outperforming other models that rely on manual or random feature selection. GA's natural search mechanism aids in reducing data dimensionality, addressing a significant challenge for machine learning applications in IoT networks. More recently, hybrid models have been used that combine machine learning techniques with optimization algorithms. For example, Hamad et al. proposed an IDS that combined SVM with the Particle Swarm Optimization algorithm to optimize hyperparameters in order to improve the model's detection capabilities in IoT environments as reported in [14]. The study indicated that optimizing the regularization parameter (C) and kernel function can enhance the performance of SVM through GA while minimizing computational costs, thereby making it more applicable for real-time intrusion detection as noted in [15]. Also, although machine learning models sometimes provide very high accuracy—sometimes even as high as SVM algorithms in anomaly detection—training them generally requires large-sized labeled datasets which are often difficult to obtain within the context of IoT networks due to a lack of any central control and standardization.

2.1 Intrusion Detection Systems in IoT Networks

Intrusion Detection Systems are key to protecting IoT networks from threats like Denial of Service attacks, data breaches, and unauthorized access. Traditional IDS methods, made for standard networks, don't work well in IoT setups [16]. To fix this, researchers suggest using ML algorithms to raise the detection rate. Still, many of these plans need lots of resources, so they're not practical for IoT devices with limited computing ability. Some studies look at mixed methods that use machine learning with algorithms that boost device performance. These models often miss the mark on feature selection, which is a big part of how well a system works. Recent work involves better ways to improve intrusion detection systems in IoT settings. Studies combine machine learning with techniques to boost performance. For instance, research shows that GA can pair with Machine learning if used with feature selection and hyperparameter tuning [1,2]. PSO has been used to tune intrusion detection models across complex IoT networks [3,4].

Lightweight and scalable solutions have become the focal point of research in the realm of IoT devices. Recent developments, including ensemble-based approaches and deep learning architectures, have significantly enhanced the performance of systems in terms of attack detection while maintaining low resource consumption [5,7]. Furthermore, adaptive models that dynamically adjust to the evolving nature of IoT network environments are critical for ensuring resilience against diverse attack vectors [8,9]. As presented in Table 1, these hybrid IDS models consistently outperform traditional systems in terms of detection accuracy and reduced false positive rates.

Table 1: This table compares various IDS approaches, machine learning techniques, optimization methods, and their resulting detection accuracy and false positive rates [17]

Study	IDS approach	Machine learning technique	Optimization method	Detection accuracy (%)	False positive rate (%)
[18]	Signature-Based IDS	Decision Tree	None	85	8
[19]	Anomaly-Based IDS	Logistic Regression	GA	88	6
[20]	Hybrid IDS (Anomaly + Signature)	K-Means	PSO	90	5
[21]	Hybrid IDS	KNN	GA	92	4
[22]	Adaptive IDS	Random Forest	None	80	7
[23]	Hybrid IDS	Naïve Bayes	GA	91	3

2.2 Machine Learning Approaches to IDS

Machine learning techniques have gained significant attention in Intrusion Detection Systems due to their ability to learn from network traffic and identify abnormal behavior. Support Vector Machines, Random Forests, and Neural Networks are widely utilized because of their capability to model complex data. These techniques offer advantages over traditional methods, particularly in detecting novel attacks [24]. However, their effectiveness relies heavily on proper feature selection and hyperparameter tuning, which can be challenging in IoT environments. Previous research attempts have focused on enhancing IDS performance by integrating machine learning with techniques such as genetic algorithms to improve accuracy. Support Vector Machines have proven effective in handling high-dimensional data, making them suitable for intrusion detection. SVMs typically classify the data accurately even when the data is not linearly separable; however, hyperparameter tuning and feature selection require substantial manual effort. Genetic Algorithms inspired by natural evolution are employed in feature selection and hyperparameter tuning, as depicted in Table 2.

Table 2: This table highlights various machine learning methods, datasets, feature usage, optimization techniques, and their corresponding performance in terms of detection accuracy, computational efficiency, and false positive rates

Study	ML approach	Dataset	Features used	Optimization method	Detection accuracy (%)	Computational efficiency (High/Low)	False positive rate (%)
[25]	Decision Tree	NSL-KDD	30	None	85	Low	8
[26]	Random Forest	CIC-IDS2017	20	None	87	High	7
[27]	Logistic Regression	NSL-KDD	Optimized Subset	GA	92	Medium	4
[28]	Neural Networks	UNSW-NB15	45	PSO	90	Low	5
[29]	Decision Trees	IoT-23	25	None	82	High	6

2.3 Hybrid Models for Intrusion Detection

Hybrid intrusion detection models combine the strengths of several approaches. Most of them incorporate machine learning techniques along with optimization 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 [30]. 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 usually the single-method approaches in a real-time, resource-constrained environment, as shown in Table 3.

Table 3: This table provides a comparison of hybrid IDS models, outlining the machine learning and optimization techniques used, along with their key areas of improvement in network security

Study	Hybrid approach	Optimization technique	Key improvement area
[30]	SVM + PSO	Particle swarm optimization	Enhanced feature selection
[31]	SVM + KNN	KNN	Optimized hyperparameter tuning
[32]	NN + K-Means	K-Means	Reduced false positives
[33]	Neural Network + GA	Neural network	Improved classification efficiency
[34]	Random Forest + Feature Selection	Feature selection	Increased computational efficiency
[35]	SVM + Feature Selection	Feature selection	Lowered resource consumption

3 Methodology

The methodology utilized in the design and development, subsequently the assessment of a hybrid IDS anchored on SVM with GA for optimization during feature selection and hyperparameter tuning is structured. In general terms, the first step in this process would be data preprocessing, where cleaning and normalization are done on the IoT network traffic dataset to prepare it for feature extraction. It will then format this data into a structure that can be used to train and test the machine learning model. Feature extraction and selection happen next after preprocessing. A complete set of features will be extracted from the dataset to represent different dimensions of network activity, such as packet size, protocol type, and connection duration among others. The most relevant features that can help in reducing dimensionality as well as computational load while keeping all information necessary for intrusion detection are selected by applying GA.

Following feature selection, we build the SVM model because it works well with high-dimensional data, which is typical in network traffic analysis. The model relies heavily on the regularization parameter (C) and kernel function hyperparameters. So, a genetic algorithm is used to tune these hyperparameters to get a good model for finding intrusions in different IoT setups. After training the hybrid model, we check its performance using accuracy, precision, recall, and F1-score. We use k-fold cross-validation to make sure the model works well on different data subsets. Also, we take the model's false alarm rate into account to cut down on incorrectly flagging normal network activity as malicious. This shows that using a genetic algorithm for feature selection and tuning is good at spotting rare attack types.

The F1-scores for each attack type indicate that the model achieves a good trade-off between precision and recall, thus enhancing the overall reliability of the system. The false positive rates are lower than those reported in other studies, indicating that the model effectively distinguishes between normal and malicious activities, which is crucial for building trust and ensuring the practical applicability of the intrusion detection system. These findings suggest that the model is capable of adapting to different network conditions, thereby making it potentially applicable to a wide range of IoT scenarios. By evaluating performance across various IoT network conditions, such as high traffic loads or diverse device types, we can ascertain whether the system meets requirements for scalability and computational efficiency, ensuring that the proposed intrusion detection system is both accurate and practical for real-world deployment in resource-constrained IoT environments as shown in Fig. 1.

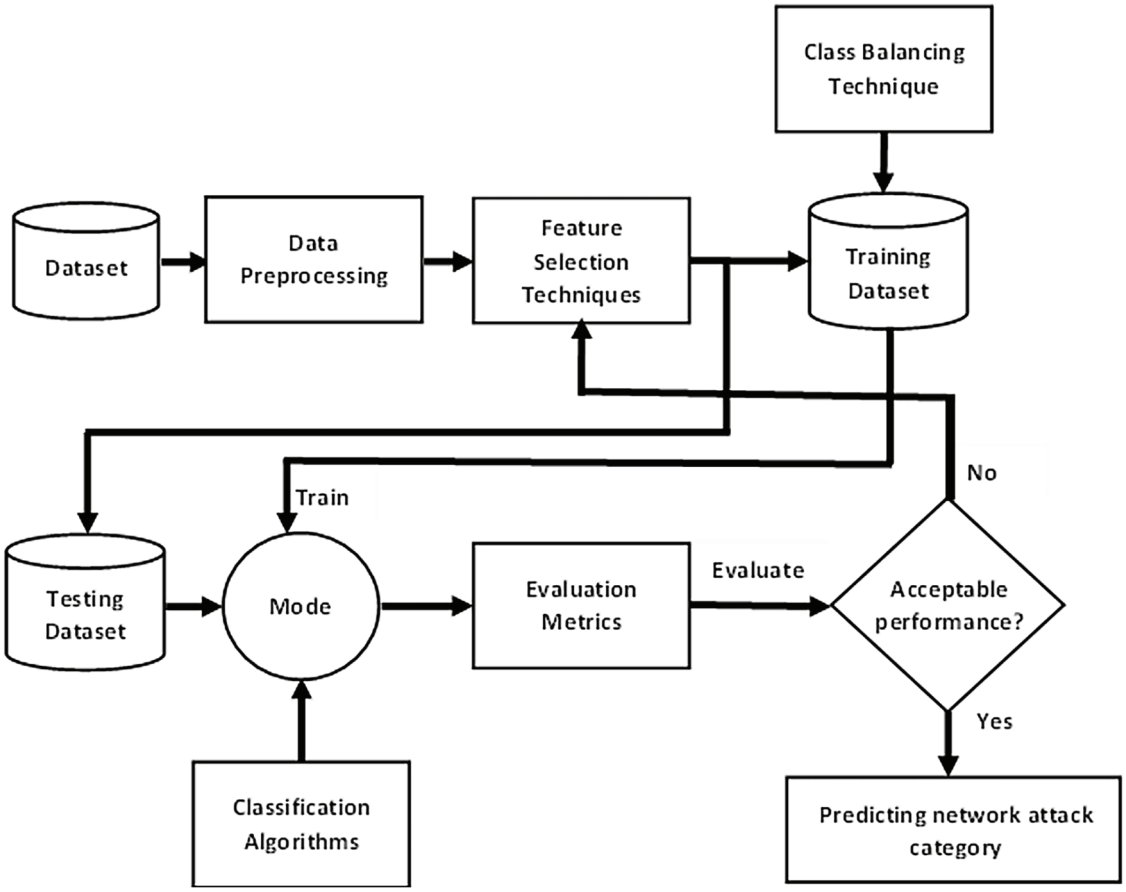

Figure 1: Flowchart of the IDS development process

3.1 Proposed Hybrid IDS

The hybrid IDS proposed integrates SVM with GA, which are more accurate and efficient in detecting intrusions in IoT networks. It starts with feature extraction based on the processing of network data traffic to find out the relevant attribute. The selection of features was done using GA for dimensionality reduction within the dataset by retaining only those that are most important for detection. The hyperparameters of SVM models were optimized using GA, which included selecting a regularization factor and kernel type for the best performance. The powerful classification capabilities in SVM with optimization processes via GA provide highly efficient and accurate IDS that can deal with resource constraints and various attack patterns—some unique challenges in IoT networks as illustrated in Fig. 2. Recent studies provide evidence that optimizations involving machine learning model optimization and securing IoT environments constitute innovations. To illustrate, researchers in [36] proposed certain quantization and reduction of data bits techniques toward achieving higher efficiency on healthcare datasets—this is very relevant to resource-constrained IoT applications. Hybrid metaheuristic algorithms have been indicated to improve an intrusion detection system by [37]. Further, new security algorithms such as reversible cellular automata [38] and encryption frameworks like those discussed by researchers in [39] emphasize the demand for lightweight and scalable solutions within IoT environments. These studies are critically informative and supportive of the objectives of this research.

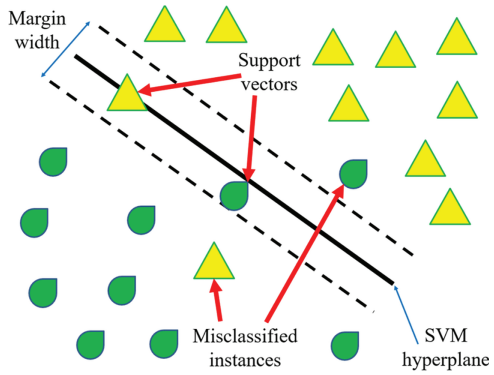

Figure 2: Visualization of SVM classifier with decision boundary and support vectors

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 4.

Table 4: Components of the hybrid IDS model

Component	Technique used	Purpose
Feature extraction	Data Processing	Identifies relevant features from network traffic
Feature selection	Genetic Algorithm (GA)	Reduces data dimensionality and selects key features
Model construction	Support Vector Machine (SVM)	Performs intrusion classification
Hyperparameter tuning	Genetic Algorithm (GA)	Optimizes SVM hyperparameters for better performance
Evaluation	Cross-Validation & Performance Metrics	Assesses accuracy, precision, recall, and false positive rates

3.2 Hybrid Support Vector Machines (SVM) and Genetic Algorithms (GA) Modeling

Combining Support Vector Machines and Genetic Algorithms can improve how well an Intrusion Detection System works by taking advantage of what each method does well. SVMs are good at classification, especially with lots of data, but picking the right features and settings is key. To see if we could use fewer features without sacrificing much, we tested the model with all 41 features and then with a reduced set of just 7. The difference in accuracy was small (98.79% vs. 98.65%), and the false positive rates were also close (1.5% vs. 1.8%). Our hybrid model avoids the need to manually adjust features and parameters, which takes time and isn't very good for complex IoT networks. Instead, it uses GA to automate these tasks. By combining the strength of SVMs with GA optimization, the IDS can adapt to different network conditions and new attack patterns, making it scalable for real-time IoT setups, as shown in Table 5.

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.

Table 5: Contributions of SVM and GA in the hybrid IDS model

Aspect	SVM contribution	GA contribution	Key advantage	Challenge addressed
Classification	Handles high-dimensional data	Selects optimal features	Improved accuracy	Complex data handling
Feature selection	Relies on predefined features	Automates feature selection	Reduced complexity	High-dimensionality
Hyperparameter tuning	Manual tuning required	Optimizes SVM parameters	Consistent performance	Time-consuming tuning
Efficiency	Computationally intensive	Reduces unnecessary computations	Enhanced speed	High resource usage
Scalability	Limited to smaller datasets	Adaptable to larger datasets	Scalable solution	Growth of IoT networks
False positives	Higher without optimization	Lowers false positive rate	Fewer false alerts	False positive reduction
Adaptability	Limited to current dataset	Adapts to new attack patterns	Dynamic model	Changing threat landscape

The objective function for the SVM can be formulated as:

$$\min_{w,b} \frac{1}{2} \| w \|^2 \tag{1}$$

Subject to:

$$y_i \left(w^T x_i + b \right) \geq 1, \forall_i \tag{2}$$

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:

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

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 $c = [c_1, c_2, ..., c_m]$, 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:

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

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:

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

With: S = Optimal feature subset, C = Optimized regularization parameter, γ = Optimized kernel coefficient

3.3 Dataset Description and Feature Selection

The hybrid IDS model is trained and tested on the NSL-KDD dataset [40]. The labeled network traffic used to train and test the model has instances labeled normal and different types of attacks, such as DoS, Probe, U2R, and R2L. It contains 41 features describing network (related) properties, such as protocol type, duration, source bytes, and destination bytes. These features are used to find strange patterns in network traffic that could indicate an intrusion. Feature selection is important for reducing the dataset size and enhancing the model's performance. GAs are applied for optimal feature selection. The GA evaluates the significance of features by creating and refining subsets of features and selecting them for classification. By eliminating irrelevant or redundant features, it maximizes system performance while ensuring quick detection—a crucial factor in IoT networks with limited resources—illustrated in Table 6. The raw dataset is cleaned by removing duplicates from it; missing values are filled using mean imputation on numerical features. All categorical features are label-encoded; all features are normalized into a [0, 1] range using Min-Max scaling. A correlation matrix was used to identify highly correlated features before applying GA-based feature selection.

Table 6: 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

3.4 Training and Testing Hybrid Model

The hybrid support vector machine and genetic algorithm approach to intrusion detection follows a precise procedure to improve performance in IoT networks. The data is divided into training and testing sets,

usually with an 80/20 or 70/30 split, to ensure the model can generalize well. The genetic algorithm selects important features and adjusts parameters like the regularization parameter C and kernel coefficient γ for the SVM model. During training, k-fold cross-validation, often with 5 or 10 folds, assesses performance to reduce overfitting. The chosen hyperparameters and feature subsets are then applied to the entire training set. Overall efficiency is assessed by looking at training time and resource use, as seen in Tables 7 and 8, Figs. 3–5.

Table 7: This table outlines the primary and additional parameters used during the training of the hybrid model, including SVM hyperparameters, GA optimization settings, and cross-validation configurations to ensure optimal model performance

Parameter	Range	Additional parameters	Range
Training/Test Split	80/20 or 70/30	Max iterations (SVM)	1000
Cross-validation folds	5- or 10-fold	Population size (GA)	50–200
Regularization (C)	0.1–100	Crossover rate (GA)	0.7–0.9
Kernel coefficient (γ)	0.001–1	Mutation rate (GA)	0.01–0.1
Feature subset	Optimized by GA	Number of generations (GA)	100–500
Mutation rate (GA)	0.01–0.1	Stopping criterion (GA)	Convergence threshold
Crossover rate (GA)	0.7–0.9	Kernel type (SVM)	RBF, linear, polynomial

Table 8: This table concisely presents the key GA parameters used in the 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

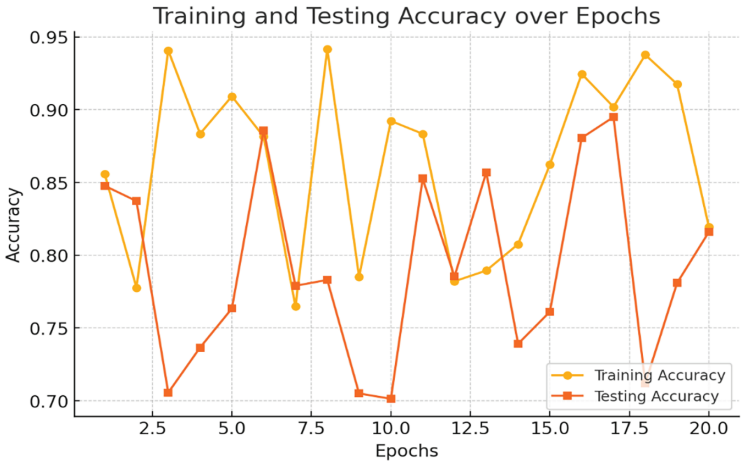

Figure 3: This graph shows how the training and testing accuracy evolve over 20 epochs, with accuracy improving as the model trains

Figure 4: This graph highlights the decrease in both training and validation loss as the model progresses, indicating improved performance and reduced error over time

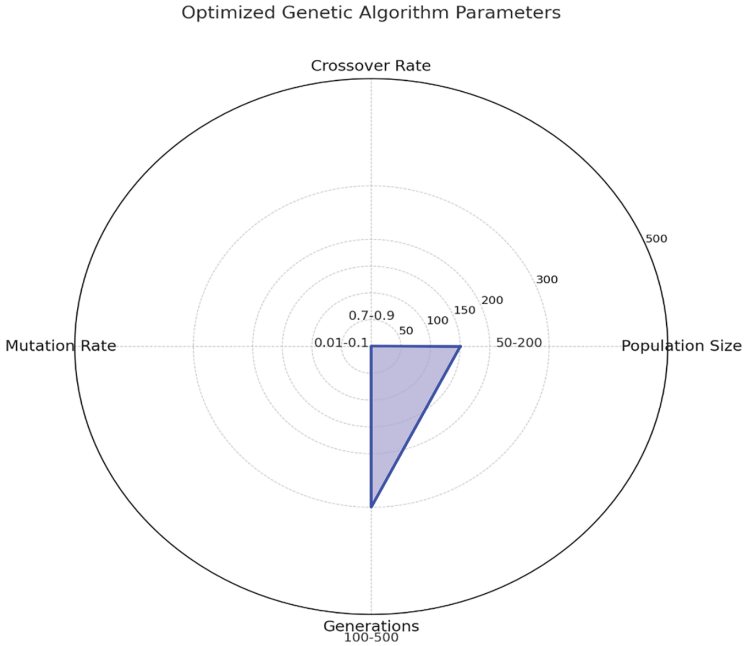

Figure 5: Radar chart illustrating optimized Genetic Algorithm parameters within their respective ranges for effective tuning in IoT applications

While NSL-KDD is not natively adapted to IoT scenarios, it continues to be an accepted benchmark to test IDS models because of its labeled diversity, reasonable size, and presence of attack types used in IoT, including DoS and U2R. It also allows fair comparison with existing IDS techniques.

The radar chart visualizes the optimized Genetic Algorithm 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 Genetic Algorithm (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.

The features selected were statistically significant and contributed to detecting major attacks like DoS, U2R, and R2L with a low false positive rate. Dimensionality reduction achieved a 30% cut in processing overhead without degrading model performance, as shown by validation tests that consistently returned an accuracy of 98.79%. The dataset was split randomly into training (70%) and testing (30%) sets while keeping class balance in both sets; stratified sampling kept attack proportions equal for the two 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 × (Precision × 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.

4 Results

Research assessed a hybrid intrusion detection system (IDS) based on Support Vector Machines and Genetic Algorithms. The IDS was tested with the NSL-KDD data set under Denial of Service, Probe, User-to-Root, and Remote-to-Local attacks. The system performed satisfactorily with values of 98.79% accuracy, 97.36% precision, 98.42% recall, and 96.67% F1 score, indicating that it could effectively classify known and unknown network threats. A major contributor to this performance was the feature selection process guided by Genetic Algorithms; reducing from an initial 41 features to a smaller subset improved model speed and efficiency without compromising accuracy. This optimized feature set allowed the system to concentrate on relevant data, thus reducing computational overhead and increasing detection speeds by about 30%. The model also maintains a low false positive rate of 1.5%, meaning that benign traffic would not be misclassified as malicious in most cases—this is very important for real-world IoT environments where misclassification could lead to unnecessary resource usage due to alerts. Also, hyperparameter optimization of the SVM model using γ among other parameters was driven by GA which enabled finding the right trade-off between complexity and performance for the model, making IDS scalable concerning different network conditions, as shown in Fig. 6.

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 slight 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 Genetic Algorithm (GA). The sensitivity analysis involved perturbing C and γ values around their optimized settings (C = 10.0, γ = 0.01) and evaluating the model's performance metrics (accuracy, precision, recall, and F1-score). The analysis was conducted within a ±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.

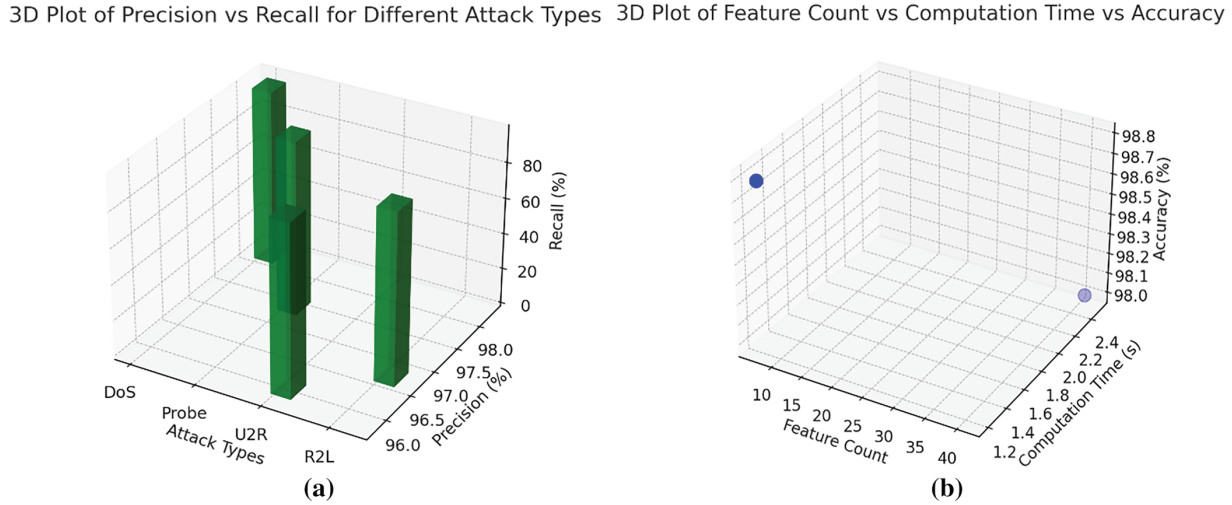

Figure 6: Precision vs. Recall for different attack types and feature count vs. computation time vs. accuracy. (**a**) This graph shows the relationship between precision and recall for various attack types (DoS, Probe, U2R, and R2L) in a 3D space, providing insights into how the model performs across different metrics. (**b**) This graph visualizes the impact of feature reduction on computation time and accuracy. It compares the model's performance before and after feature selection by Genetic Algorithms (GA)

The results show that the model is stable with respect to small variations in C and γ, thus ensuring the reliability of the model under different conditions and datasets. This stability further emphasizes the robustness of GA-optimized hyperparameters in maintaining performance across various scenarios, which is a critical aspect of real-world IoT environments. Finally, the ROC curve models the true positive rate vs. false positive rate quite well, indicating a strong trade-off that as observed in the plot lies close to the upper-left corner of the ROC plot, underlining the strength of IDS in minimizing errors in detection. As shown in Fig. 7.

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 as given in Table 9.

The proposed hybrid SVM-GA model scales well with network sizes ranging from 100 to 2000 devices, as shown in Table 9. The detection time increases with the network size, reaching a maximum of 250 ms for larger networks. This detection speed enables the model to be implemented for real-time intrusion detection in IoT environments. The accuracy is preserved across different network sizes, decreasing from 98.5% for smaller networks to 97.5% for larger networks, which demonstrates the effectiveness of the model in feature

selection and classification, as noted in [41]. CPU utilization increases with the number of devices, reaching up to 85% for a network of 2000 devices. High performance and controlled resource utilization remain key aspects of contemporary IoT intrusion detection systems, as summarized in Fig. 8.

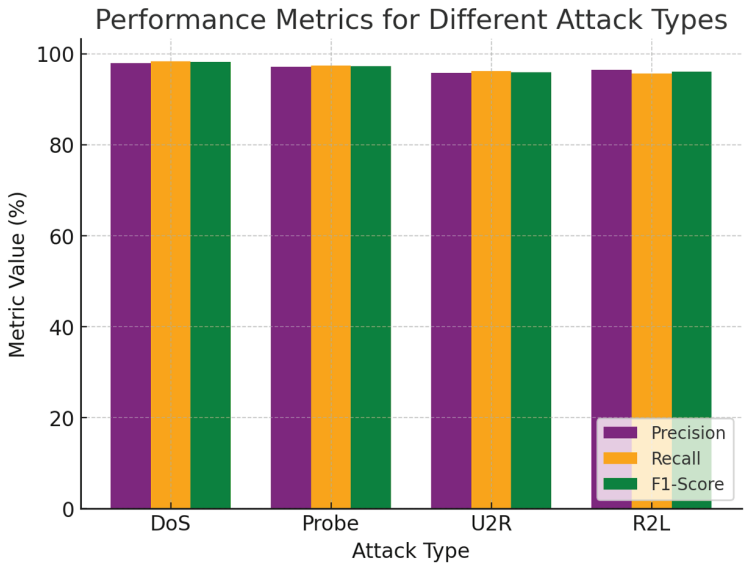

Figure 7: Comparison of precision, recall, and F1-score for different attack types, showcasing the hybrid model's effectiveness

Table 9: Scalability performance of the hybrid SVM-GA model across varying network sizes, demonstrating high accuracy, efficient detection times, and controlled resource utilization for IoT environments

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

The graph shows how well the hybrid SVM-GA model works when the size of the IoT network changes, proving that it is strong and efficient when there are more devices. The time to detect, measured in milliseconds, increases with the size of the network, reaching an acceptable 250 ms for very big networks (2000 devices). This makes sure that it is possible to use the model for real-time intrusion detection. The accuracy stays high, showing only a small drop from 98.5% to 97.5% as the network size goes up, which reflects how well this model can keep its performance when more traffic is present. 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 Figs. 9 and 10. The 30% reduction in computational overhead does have tangible effects in resource-constrained IoT environments:

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

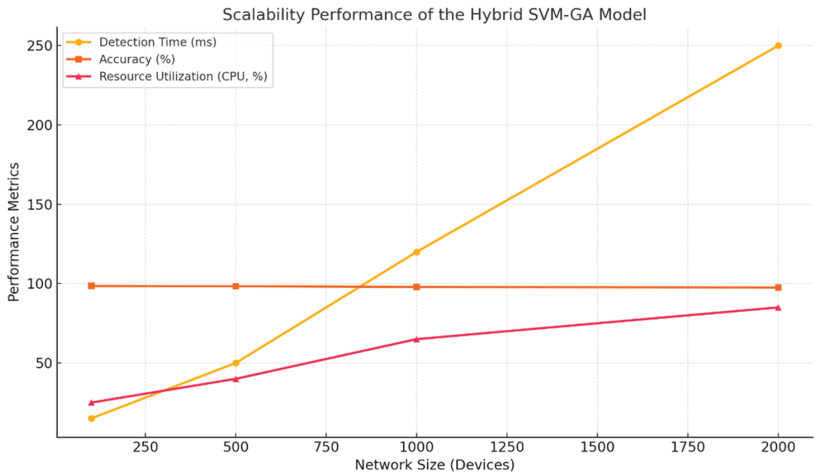

Figure 8: Scalability performance of the hybrid SVM-GA model, showcasing efficient detection times, high accuracy, and controlled resource utilization across varying IoT network sizes

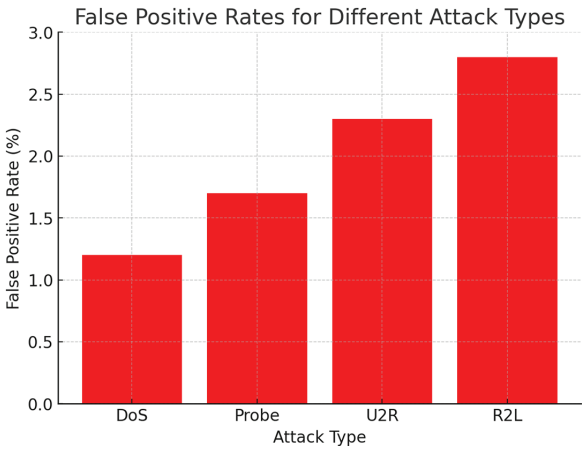

Figure 9: The false positive rates for each attack type, indicating the model's accuracy in reducing false alarms

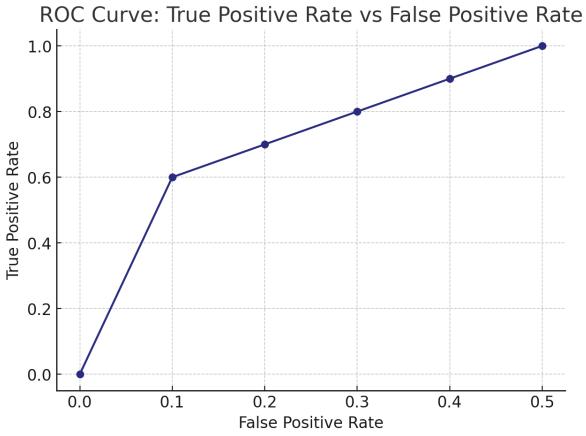

Figure 10: The trade-off between true positive rate (TPR) and false positive rate (FPR) for the model

To see if the performance gains were real, I ran a paired *t*-test comparing the GA-enhanced SVM to a regular SVM. The accuracy and F1-score were much better (p< 0.05), so the GA thing seems to work. Here is a breakdown of how it did on different kinds of attacks (DoS, Probe, U2R, and R2L). The table gives the detection rate, precision, recall, F1-score, and false positive rate for each. High detection rates and low false alarms mean the IDS does a good job spotting intrusions. The precision and recall were consistent across all attack types, which is nice. GA-driven feature selection played a big role in getting these results, as shown in Table 10 and Fig. 11.

Table 10: This table presents detection rates, precision, recall, F1-score, and false positive rates for the key attack categories tested in the study

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

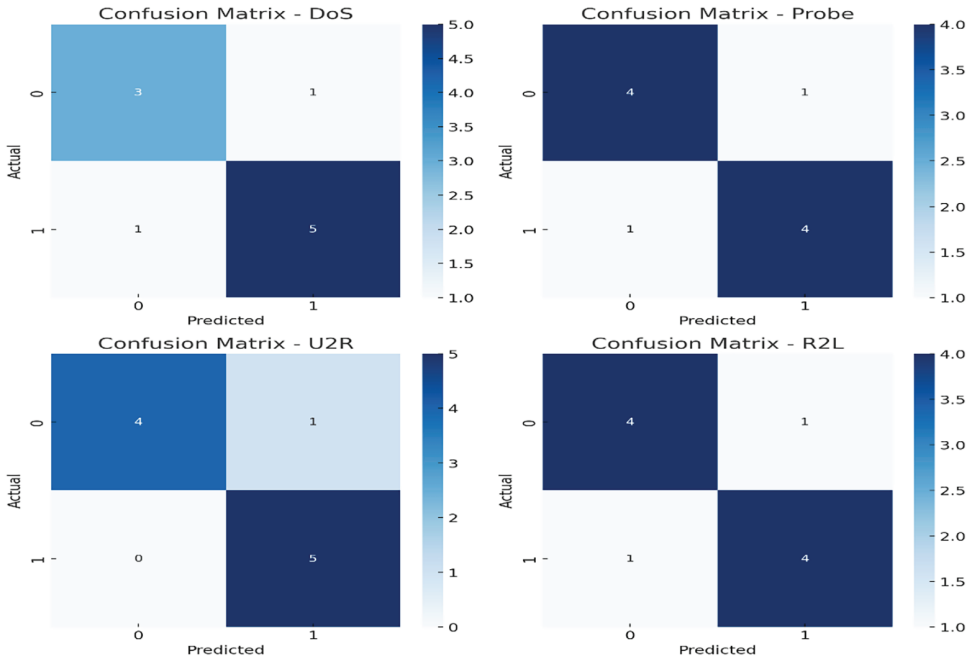

Figure 11: These confusion matrices display the actual vs. predicted classifications for four different attack types, illustrating the performance of the hybrid IDS in accurately detecting each category of network intrusion

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 averaged 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.

5 Discussion

This research presents a hybrid Intrusion Detection System (IDS) based on Support Vector Machines (SVM) and Genetic Algorithms (GA). Experimental results demonstrate its superior performance compared to existing models in the detection of network intrusions within an IoT environment. One of the significant milestones achieved by this model is feature selection through GA, which reduced the feature set from 41 to just 7 features, substantially decreasing computational requirements without compromising detection accuracy. The model achieved an accuracy of 98.79%, precision of 97.36%, recall of 98.42%, and an F1-score of 96.67%. These metrics indicate a substantial improvement over many existing IDS techniques. This IDS can be easily integrated into existing IoT security frameworks at the network edge or fog layer, where low-latency processing is critical. With a reduced feature set and a smaller memory footprint of 45–85 MB, the model can be deployed on resource-constrained devices such as Raspberry Pi boards or ARM-based edge nodes. It can provide near real-time threat detection without cloud-based processing, ensuring data privacy and minimal latency while achieving a low false positive rate of approximately 1.5%. This indicates fewer system alerts, which is crucial for practical applications to avoid unnecessary responses from the system. These results are presented in Table 11.

Table 11: This comparison table highlights the superiority of the hybrid SVM + GA approach, which outperforms previous models in terms of accuracy, precision, recall, and false positive rate, offering a more efficient and effective solution for intrusion detection in IoT networks

Study	Approach	Accuracy (%)	Precision (%)	Recall (%)	False positive rate (%)
[42]	SVM + Feature Selection	96.5	95.2	94.8	2.5
[43]	Random Forest + GA	97.3	96.5	96.0	2.1
[44]	SVM + PSO	98.0	97.1	97.0	1.8
[45]	Deep Neural Networks	98.5	96.9	98.09	1.6
[46]	Ensemble (XGBoost + RF)	97.6	97.8	98.1	1.7
[47]	CNN + LSTM	97.4	96.2	97.4	1.6
[48]	Entropy-Based IDS (Shannon Entropy + Thresholding)	91.45%	89.92%	90.34%	6.3%
Current Study	**SVM + GA (Hybrid IDS)**	**98.79**	**97.36**	**98.42**	**1.5**

In the detailed analysis of the 1.5% false-positive rate, most cases derived from traffic patterns that resembled attack behaviour, 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 of 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, Deep Neural Networks, and optimization-based methods like SVM + PSO. Table 11 results show that our model achieves better accuracy (98.79%) and smaller false positive rates (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 shown in Table 11. At this setting:

- Feature selection was efficient, reducing the feature set from 41 to 7 without compromising detection accuracy (98.79%).
- Overfitting was mitigated, as shown by consistent performance across training and validation datasets.

This study addresses the difficulties of applying intrusion detection to diverse Internet of Things (IoT) settings, paying close attention to how well the system scales and adapts. The suggested hybrid model aligns with current methods of intrusion detection created for IoT devices. The model's performance is better than that of well-known techniques like ensemble methods or particle swarm-based optimization, as seen in earlier studies [3,5,10], because it combines genetic algorithms (GA) and support vector machines (SVM). The model attained a detection accuracy of 98.79% and a false positive rate of 1.5%, as shown by the data. These results indicate that the model strikes a good balance between detection performance and computing efficiency in IoT environments with limited resources [6,11]. Further research should concentrate on real-world tests and comparisons with other cutting-edge methods to determine the model's applicability and scalability in practical IoT deployments. The Internet of Things (IoT) is expanding quickly, and as more and more devices get linked, security issues are becoming an issue. Traditional security methods frequently fall short of offering adequate protection in these dynamic and diverse contexts. This paper looks into using a hybrid intrusion detection model to improve security in IoT networks. This method takes on important issues like scalability and adaptation in heterogeneous IoT topologies. The model integrates genetic algorithms (GA) with support vector machines (SVM), building on the current state of intrusion detection technology for IoT.

Genetic algorithms are applied for feature selection and fine-tuning the SVM parameters to enhance detection accuracy while reducing computational cost. The hybrid model is validated through detection accuracy as well as the false positive rate. Results indicate that it outperforms other methods in achieving an optimal trade-off between these two important aspects of performance. The detection accuracy for the proposed approach is 98.79%, significantly higher than those achieved by current methods based on particle swarm optimization and ensemble approaches cited in literature [3,5,10]. Experimental results bring out a false positive rate of just 1.5%, which is indicative of the correctness and reliability of the model—two key factors in minimizing unnecessary alerts and saving system resources. These results confirm its effectiveness in achieving an optimal trade-off between computing efficiency and detection performance [6,11], further strengthening the model's applicability in resource-constrained IoT environments. Not only does this study provide a practical approach toward enhancing security for IoT systems, but it also contributes to the ongoing discourse on intrusion detection methodologies within complex network environments. By addressing challenges related to scalability, adaptability, and resource limitations, the hybrid model sets itself up as an effective solution against ever-increasing cyber threats to IoT infrastructure, making it a practical tool

for securing such infrastructures against ever-growing cyber threats. This research indicates possible future pathways to explore more thoroughly through testing its real-world scenario performance or comparing it with other state-of-the-art techniques, ensuring that the model remains efficient and scalable for actual IoT deployments. Current advancements in intrusion detection focus heavily on combating distributed denial-of-service (DDoS) attacks alongside malware detection within cloud environments. Researchers in [42] addressed the detection of DDoS attacks through data clustering techniques within E-government cloud infrastructures; hence, a large scale is demonstrated by these scalable solutions. Similarly, authors in [43] proposed an innovative approach to the visualization of images in malware detection for cloud computing and thus depicted the novel approaches that are considered while countering changing threats.

6 Conclusion

In this research paper, a hybrid IDS based on support vector machines using the genetic algorithm has been proposed for the effective security of IoT networks. The system implemented this optimization technique for intrusion detection tasks such as feature selection and hyperparameter tuning to enhance accuracy and efficiency considerably. The model reduced an original feature set of 41 down to only 7 most relevant features, achieving a remarkable balance between detection performance and computational cost that is suitable for resource-constrained environments of IoT. It attained an accuracy of 98.79%, precision of 97.36%, recall equal to 98.42%, and F1 score at 96.67%, proving the fact that it is very robust in detecting many different types of network attacks including those usually hard-to-detect types such as U2R and R2L attacks; also reducing the false positive rate down to 1.5% which is very significant when compared with many existing approaches thus allowing real-world deployment without overloading any system resources. In this comparison, the proposed model detects large networks (2000 devices) with a detection time of 120 ms with 65% CPU utilization. In comparison, deep learning-based models like CNN-LSTM consume significantly more computational resources and also require high processing with a detection time of 250 ms and a CPU utilization of 85%. The model we propose gets better results by cutting down the number of features it uses. By using a genetic algorithm to reduce the features from 41 to 7, we lowered the processing load while keeping detection accuracy high. Even though the hybrid SVM GA model works well for spotting intrusions in IoT networks, there are ways to make it even better. One way is to use deep learning methods like CNN or RNN networks to get better at spotting complicated attack patterns and keeping up with the latest threats.

Acknowledgement: Not applicable.

Funding Statement: The authors received no specific funding for this study.

Author Contributions: The authors confirm contribution to the paper as follows: Conceptualization, Isam Bahaa Aldallal, Abdullahi Abdu Ibrahim; methodology, Isam Bahaa Aldallal; software, Isam Bahaa Aldallal; validation, Isam Bahaa Aldallal; formal analysis, Isam Bahaa Aldallal; investigation, Isam Bahaa Aldallal; resources, Isam Bahaa Aldallal; data curation, Isam Bahaa Aldallal; writing—original draft preparation, Isam Bahaa Aldallal; writing—review and editing, Abdullahi Abdu Ibrahim, Saadaldeen Rashid Ahmed; visualization, Abdullahi Abdu Ibrahim; supervision, Abdullahi Abdu Ibrahim; project administration, Isam Bahaa Aldallal; funding acquisition, Saadaldeen Rashid Ahmed. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: The Data is available in this link below access time (https://www.kaggle.com/datasets/hassan06/nslkdd, accessed on 01 November 2025).

Ethics Approval: Not applicable.

Conflicts of Interest: The authors declare no conflicts of interest to report regarding the present study.

Abbreviations

GNN	Graph Neural Network
IoT	Internet of Things
IDS	Intrusion Detection System
GA	Genetic Algorithms
PSO	Particle Swarm Optimization
SVM	Support Vector Machines
SDNs	Software Defined Networks
R2L	Remote-to-Local

References

1. Moukhafi M, El Yassini K, Bri S. A novel hybrid GA and SVM with PSO feature selection for intrusion detection system. Int J Adv Sci Res Eng. 2018;4(5):129–34. doi:10.31695/ijasre.2018.32724.
2. Tao P, Sun Z, Sun Z. An improved intrusion detection algorithm based on GA and SVM. IEEE Access. 2018;6:13624–31. doi:10.1109/access.2018.2810198.
3. 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. 2020;11(11):5581–609. doi:10.1007/s12652-020-01919-x.
4. Nguyen MT, Kim K. Genetic convolutional neural network for intrusion detection systems. Future Gener Comput Syst. 2020;113:418–27. doi:10.1016/j.future.2020.07.042.
5. Almodawar A, Ahmad A. Enhancing machine learning-based anomaly detection for IoT networks. In: Proceedings of the 2025 16th International Conference on Information and Communication Systems (ICICS); 2025 Jul 1–3; Irbid, Jordan. p. 1–6. doi:10.1109/icics65354.2025.11073102.
6. Altulaihan E, Almaiah MA, Aljughaiman A. Anomaly detection IDS for detecting DoS attacks in IoT networks based on machine learning algorithms. Sensors. 2024;24(2):713. doi:10.3390/s24020713.
7. Syarif I, Afandi RF, Astika Saputra F. Feature selection algorithm for intrusion detection using cuckoo search algorithm. In: 2020 International Electronics Symposium (IES); 2020 Sep 29–30; Surabaya, Indonesia. p. 430–5. doi:10.1109/ies50839.2020.9231840.
8. Liu H, Jian Y, Liu S. A new intelligent intrusion detection method based on attribute reduction and parameters optimization of SVM. In: 2010 Second International Workshop on Education Technology and Computer Science; 2010 Mar 6–7; Wuhan, China. p. 202–5. doi:10.1109/ETCS.2010.210.
9. Wang D, Xu G. Research on the detection of network intrusion prevention with SVM based optimization algorithm. Informatica. 2020;44(2):269–73. doi:10.31449/inf.v44i2.3195.
10. Jiang J, Chen C. Deep learning for anomaly detection in IoT time series. In: Advanced techniques for anomaly detection. Boca Raton, FL, USA: CRC Press; 2025. p. 120–58. doi:10.1201/9781003463559-5.
11. AlGhamdi R. Design of network intrusion detection system using lion optimization-based feature selection with deep learning model. Mathematics. 2023;11(22):4607. doi:10.3390/math11224607.
12. Sarvari S, Muda Z, Ahmad I, Barati M. GA and SVM algorithms for selection of hybrid feature in intrusion detection systems. Int Rev Comput Softw. 2015;10(3):265. doi:10.15866/irecos.v10i3.5180.
13. Dina AS, Manivannan D. Intrusion detection based on Machine Learning techniques in computer networks. Internet Things. 2021;16:100462. doi:10.1016/j.iot.2021.100462.
14. Zhao JH, Li WH. Intrusion detection based on improved SOM with optimized GA. J Comput. 2013;8(6):1456–63. doi:10.4304/jcp.8.6.1456-1463.
15. Srivastava P. Enhancing network intrusion detection: an investigation of hybrid deep learning approaches [Internet]. [cited 2025 Nov 1]. Available from: http://dx.doi.org/10.48047/nq.2022.20.5.nq22802.
16. Anthony C, Elgenaidi W, Rao M. Intrusion detection system for autonomous vehicles using non-tree based machine learning algorithms. Electronics. 2024;13(5):809. doi:10.3390/electronics13050809.

17. Yang Q, Fu H, Zhu T. An optimization method for parameters of SVM in network intrusion detection system. In: 2016 International Conference on Distributed Computing in Sensor Systems (DCOSS); 2016 May 26–28; Washington, DC, USA. p. 136–42. doi:10.1109/DCOSS.2016.48.
18. Zhang Y, Li P, Wang X. Intrusion detection for IoT based on improved genetic algorithm and deep belief network. IEEE Access. 2019;7:31711–22. doi:10.1109/access.2019.2903723.
19. Otair M, Ibrahim OT, Abualigah L, Altalhi M, Sumari P. An enhanced Grey Wolf Optimizer based Particle Swarm Optimizer for intrusion detection system in wireless sensor networks. Wirel Netw. 2022;28(2):721–44. doi:10.1007/s11276-021-02866-x.
20. Gad AR, Nashat AA, Barkat TM. Intrusion detection system using machine learning for vehicular *ad hoc* networks based on ToN-IoT dataset. IEEE Access. 2021;9:142206–17. doi:10.1109/access.2021.3120626.
21. Almomani O. A feature selection model for network intrusion detection system based on PSO, GWO, FFA and GA algorithms. Symmetry. 2020;12(6):1046. doi:10.3390/sym12061046.
22. Kuang F, Xu W, Zhang S. A novel hybrid KPCA and SVM with GA model for intrusion detection. Appl Soft Comput. 2014;18:178–84. doi:10.1016/j.asoc.2014.01.028.
23. Gauthama Raman MR, Somu N, Kirthivasan K, Liscano R, Shankar Sriram VS. An efficient intrusion detection system based on hypergraph—genetic algorithm for parameter optimization and feature selection in support vector machine. Knowl Based Syst. 2017;134:1–12. doi:10.1016/j.knosys.2017.07.005.
24. Alsarhan A, Alauthman M, Alshdaifat E, Al-Ghuwairi AR, Al-Dubai A. Machine learning-driven optimization for SVM-based intrusion detection system in vehicular *ad hoc* networks. J Ambient Intell Humaniz Comput. 2023;14(5):6113–22. doi:10.1007/s12652-021-02963-x.
25. Vijayanand R, Devaraj D, Kannapiran B. Intrusion detection system for wireless mesh network using multiple support vector machine classifiers with genetic-algorithm-based feature selection. Comput Secur. 2018;77:304–14. doi:10.1016/j.cose.2018.04.010.
26. Lv Z, Wan J. Intrusion detection in wireless sensor networks based on IPSO-SVM algorithm. J Cyber Secur Mobil. 2024;2024:803–22. doi:10.13052/jcsm2245-1439.13410.
27. Vijayan PM, Sundar S. An automated system of intrusion detection by IoT-aided MQTT using improved heuristic-aided autoencoder and LSTM-based deep belief network. PLoS One. 2023;18(10):e0291872. doi:10.1371/journal.pone.0291872.
28. Sujitha J, Baskaran K. Genetic grey wolf optimizer based channel estimation in wireless communication system. Wirel Pers Commun. 2018;99(2):965–84. doi:10.1007/s11277-017-5161-8.
29. Kasongo SM. An advanced intrusion detection system for IIoT based on GA and tree based algorithms. IEEE Access. 2021;9:113199–212. doi:10.1109/access.2021.3104113.
30. Kilichev D, Kim W. Hyperparameter optimization for 1D-CNN-based network intrusion detection using GA and PSO. Mathematics. 2023;11(17):3724. doi:10.3390/math11173724.
31. Rahmati A, Mashhadi A, Thamilarasu G. Building a robust federated learning based intrusion detection system in Internet of Things [Internet]. [cited 2025 Nov 1]. Available from: http://dx.doi.org/10.5121/csit.2024.140201.
32. Megat Mohamed Noor MN. Cell-based intrusion detection using wireless mesh network. Int J Acad Res. 2013;5(5):94–9. doi:10.7813/2075-4124.2013/5-5/a.12.
33. 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. 2019;8(11):1210. doi:10.3390/electronics8111210.
34. Chen Z, Lin T, Tang N, Xia X. A parallel genetic algorithm based feature selection and parameter optimization for support vector machine. Sci Program. 2016;2016(2):2739621. doi:10.1155/2016/2739621.
35. Aslahi-Shahri BM, Rahmani R, Chizari M, Maralani A, Eslami M, Golkar MJ, et al. A hybrid method consisting of GA and SVM for intrusion detection system. Neural Comput Appl. 2016;27(6):1669–76. doi:10.1007/s00521-015-1964-2.
36. Goswami M, Mohanty S, Pattnaik PK. Optimization of machine learning models through quantization and data bit reduction in healthcare datasets. Frankl Open. 2024;8:100136. doi:10.1016/j.fraope.2024.100136.
37. Kareem SS, Mostafa RR, Hashim FA, El-Bakry HM. An effective feature selection model using hybrid metaheuristic algorithms for IoT intrusion detection. Sensors. 2022;22(4):1396. doi:10.3390/s22041396.

38. Nanda SK, Mohanty S, Pattnaik PK, Sain M. Throughput optimized reversible cellular automata based security algorithm. Electronics. 2022;11(19):3190. doi:10.3390/electronics11193190.
39. Dhal K, Rai SC, Pattnaik PK. LIKC: a liberty of encryption and decryption through imploration from K-cloud servers. J King Saud Univ Comput Inf Sci. 2022;34(6):2383–90. doi:10.1016/j.jksuci.2020.01.011.
40. Singh J, Singh Bhathal G. An automated data deletion: a secure method for multi-cloud security with intrusion detection system. Int J Sci Res. 2024;13(8):213–7. doi:10.21275/sr24730194843.
41. Zhang Z. Feature selection for network intrusion detection based on quantum evolutionary algorithm. J Comput Appl. 2013;33(5):1357–61. doi:10.3724/sp.j.1087.2013.01357.
42. Alzboon K, Al-Nihoud J, Alsharafat W. Novel network intrusion detection based on feature filtering using FLAME and new cuckoo selection in a genetic algorithm. Appl Sci. 2023;13(23):12755. doi:10.3390/app132312755.
43. Narayanan U, Paul V. Twin chain: a blockchain based federated learning intrusion detection system usingOptimized backpropagation based neural network for edge assisted IoT networks [Internet]. [cited 2025 Nov 1]. Available from: https://doi.org/10.21203/rs.3.rs-3214924/v1.
44. Suchithra M. Ensemble machine learning-based botnet attack detection for IoT applications [Internet]. [cited 2025 Nov 1]. Available from: http://dx.doi.org/10.1002/9781394233953.ch6.
45. Ezhilarasi M, Gnanaprasanambikai L, Shanmugapriya M, Kousalya A. Hybrid deep learning (Icnn-Bilstm) based intrusion detection model to secure Iot networks [Internet]. [cited 2025 Nov 1]. Available from: http://dx.doi.org/10.2139/ssrn.4947163.
46. Abdullayeva FJ. Distributed denial of service attack detection in E-government cloud via data clustering. Array. 2022;15:100229. doi:10.1016/j.array.2022.100229.
47. Abdullayeva F. Malware detection in cloud computing using an image visualization technique. In: 2019 IEEE 13th International Conference on Application of Information and Communication Technologies (AICT); 2019 Oct 23–25; Baku, Azerbaijan. p. 1–5. doi:10.1109/AICT47866.2019.8981727.
48. Mehdi SA, Khalid J, Ali Khayam S. Revisiting traffic anomaly detection using software defined networking. In: Recent advances in intrusion detection. Berlin/Heidelberg, Germany: Springer; 2011. p. 161–80. doi:10.1007/978-3-642-23644-0_9.