PENINSULA PUBLISHING LLC

SHIFRA

Vol. **(2025)**, 2025, **pp.** 98–109
ISSN: 3078-3186

Research Article

An Enhanced Hybrid Genetic-JAYA Algorithm for Feature Selection and SVM Parameter Optimization in Intrusion Detection Systems: Evaluation on the CICIDS Dataset

Mohanad G. Yaseen [1, *], Ahmed Hussein Ali [1], Mohammad Alajanbi [2]

[1] *Department of Computer, College of Education, AL-Iraqia University, Baghdad, Iraq.*

[2] *Deputy Dean of Technical College, Imam Ja'afar Al-Sadiq University, Baghdad, Iraq*

ARTICLEINFO

Article History

Received 20 Nov 2024

Revised: 5 Jan 2025
Accepted 5 Feb 2025
Published 25 Feb 2025

Keywords

Intrusion Detection Systems (IDS),

Hybrid Genetic-JAYA Algorithm,

Feature Selection,

SVM Parameter Optimization,

CICIDS2017 Dataset.

ABSTRACT

The changing scenario in the cybersecurity field requires intelligent and adaptive means of detecting sophisticated intrusions. This paper presents an improved hybrid Genetic-JAYA algorithm for simultaneous feature selection and hyperparameter tuning of an SVM-based IDS. Leveraging the CICIDS2017 dataset, which is well-known for its comprehensive representation of modern attack types, the model interprets the classification as a binary problem, distinguishing normal traffic from malicious activity. The presented hybridization employs the global exploration ability of the Genetic Algorithm (GA) with the parameter-less, convergence-oriented behavior of the JAYA algorithm.

To select the subset of features, a custom fitness function is adopted that balances classification accuracy and feature compactness, while the hyperparameters of the SVM using a radial basis function (RBF) kernel are optimized concurrently for improved detection. All results were obtained using stratified 5-fold cross-validation, with metrics averaged over 10 independent runs. The hybrid GA-JAYA-SVM model outperformed GA-SVM and JAYA-SVM, achieving an average accuracy of 98.73% (±0.45), precision of 98.63%, recall of 98.79%, and a reduced false positive rate of 1.15%.

The robustness and generalization capability of the model are further supported by AUC and F1-score measurements. Statistical evidence, via the Wilcoxon signed-rank test, validates the observed performance gains ($p < 0.05$). These results illustrate the capability of the proposed model to enhance IDS performance with minimal computational overhead an essential requirement for real-time deployment. Overall, the findings suggest that hybrid metaheuristic approaches, such as the Genetic-JAYA combination, offer strong potential for improving IDS effectiveness and form a promising foundation for future research into adaptive, intelligent, and layered cybersecurity defenses.

1. INTRODUCTION

This While technology continues to advance and our world becomes more connected, we're also exposed to an increase in cyber threats, especially in networked environments. IDSs are an important line of defense for detecting and responding to security attacks. These systems utilize a variety of machine learning approaches, while Support Vector Machine (SVM) classifiers have been found effective in separating benign and malicious traffic patterns. However, despite their advantages, SVMs still depend on the quality of feature selection and parameter tuning in order to have a maximum performance, particularly on complex data such as those of the CICIDS. CICIDS dataset, uniquely designed for IDS evaluation, includes a broad spectrum of attack types and normal patterns, where rich resources for the training and testing of intrusion detection model can be often obtained . On the other hand, the conventional feature selection methods are not ideal for this task since they may not sufficiently characterize the intrinsic (nonlinear) relationships in the data [1].

To overcome this limitation, novel computational paradigms like hybrid methodologies; comprising of GA and JAYA algorithms, must be incorporated for improving the feature selection problem efficiently . The Genetic Algorithm (GA) is well-known for robust optimization capacity by mimicking the process of natural selection and repeatedly evaluating and enhancing feature subsets. At the same time, the JAYA algorithm, which has an inherent simplicity with few parameters, provides an alternative approach, in which solutions are tended towards the best-known solutions and away from the worst

*Corresponding author email: maymy832410@gmail.com
DOI: https://doi.org/10.70470/SHIFRA/2025/006

solutions . By the combination of these two algorithms, not only does the proposed hybrid genetic-JAYA approach simplify the feature selection process, but it also optimizes the SVM classifier parameters simultaneously, resulting in a more efficient intrusion detection model. This method has been tested in many studies for proving its superiority against single JAYA or GA algorithm [2].

Due to the fact that the rate as well as the complexity of cyber attacks is impressively growing , and the phishing and DDoS attacks are good examples, using this improved hybrid model makes a proactive security policy by looking the problems from a different angle and is able to 16:16 H.R. Tizhoosh et al. In addition, prior studies have shown that the optimal combination of feature selection and SVM parameter-tuning can lead to decreased false-positive rate and improved detection accuracy, and therefore the technique must be further investigated . When evolutionary algorithms are used in the feature selection phase, - the enhancement in IDS effectiveness should be viewed from a multi dimensional perspective. Comparison with baselines (GA-SVM and JAYA-SVM) reveals a significant performance difference in performance from baseline methods. For example, the hybrid model always had better performance than other methods in terms of Accuracy, AUC(area under the receiver operating characteristic curve) and F1-score, which again demonstrated its effectiveness of complexity control in data .

The systemic methodology of the hybrid model is designed to guarantee the choice of the most appropriate features, without changing the parameters of the classifier, which has proved to provide a solid detection mechanism that can deal with different attack types . As shown in our proposed feature selection process (Figure 1), the introduction of hybrid approach greatly facilitates the process of feature selection, indicating that this approach is an effective method toward better intrusion detection. The methodologies used will be empirically investigated, and the superior performance of the proposed hybrid model will be confirmed on the CICIDS dataset, which is an evidence-based method of improving the accuracy of intrusion detection by hybrid feature and parameter optimization . The payoff of this research, however, transcends theory into practice, and towards the developments of secure protocols with which the necessity of vigilance about security is not only shown but very much applied. By making security an academic domain, it shows how to defend organizations in the lead rather than by reacting after attacks have already occurred. The corresponding details of feature selection and optimization are described in the following and discussed in a more general setting in Sections.

The evolution of intrusion detection requires advanced techniques to keep pace with the increased complexity and amount of Cyber-threats. Among them, the optimization of feature selection and parameter tuning have been recognized as key factors to improve the efficiency of Intrusion Detection System (IDS). In this study the use of an improved hybrid Genetic-JAYA algorithm which performs feature selection and SVM parameters optimizing simultaneously, focused on performance within CICIDS2017 dataset is investigated. The presented hybrid model utilizes the best features of Genetic Algorithms (GA) and the JAYA algorithm. GA offers strong global searching ability which is important for finding informative feature subspaces, and JAYA introduces a parameterless, direction-based optimization mechanism which is well suited for optimizing SVM parameters including penalty parameter and kernel parameter. Together these ingredients tight optimization loop gradually increases the performance/efficiency of the classifier.

Feature selection is an essential component for model parsimoniousness and interpretability, which removes irrelevant or redundant information. The latest research indicates that the power of feature engineering cannot be discounted, as good representations can substantially influence the detection accuracy especially in high dimension network traffic datasets. At the same time, an effective tuning of hyperparameters is necessary to guarantee machine learning classifiers are able to generalize to changing threat dynamics. In order to assess the efficacy of the hybrid GA-JAYA method in practice, several well-known ML models, namely Decision Trees (DT), Random Forests (RF), SVM, ANN and DNN are tested as benchmarks. These models are proxy for typical implementations of IDS and are used to put the relative improvement offered by the proposed framework into perspective. We choose to use the CICIDS2017 dataset as it provides an extensive coverage of contemporary cyberattack activities and traffic patterns, acting as a useful benchmark for practical testing. The comparison with conventional models in this work would prove the ability of hybrid-optimized detection for improving detection performance keeping the high efficiency of the detection process.

The integration of those feature selection and hyperparameter tuning in a single optimization framework makes our contribution not only to the progress of the IDS methodologies, but also to the generic domain of the intelligent cybersecurity systems. Results from this research are the basis for the further research to hybrid metaheuristic strategies for the sake of enhancing real-time defenses against ever more complex digital terrains [3-6].

TABLE I: PERFORMANCE METRICS OF MACHINE LEARNING ALGORITHMS ON CICIDS2017 *DATASET. THESE BASELINE MODELS WERE TRAINED AND EVALUATED UNDER IDENTICAL BINARY CLASSIFICATION SETTINGS ON THE CICIDS2017 DATASET, USING STRATIFIED 5-FOLD CROSS-VALIDATION AND BALANCED DATA SAMPLING.*

Algorithm	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
DT	93.5	92.1	94.0	93.0
RF	95.8	94.5	96.3	95.4
SVM	94.2	93.1	94.5	93.8
ANN	95.5	94.8	95.6	95.2
DNN	96.2	95.4	96.7	96.0

2. LITERATURE REVIEW

There has been a remarkable improvement in methodologies that can influence the performance of Intrusion Detection Systems (IDS) in these past few decades and a good contribution from different optimization techniques. Feature selection is an important part of machine learning models especially the IDS as it has major impact on the models efficiency and identity false positive rate [2,3]. Previous studies underlined the significance of feature selection for data dimensionality reduction followed by not only the increased intrinsic computational efficiency but also the model interpretability. Studies such as , , and highlight that the existing techniques for large scale datasets are not so effective for database management and have motivated the growing interest in heuristic solutions. The integration of genetic algorithms (GAs) with JAYA optimization to solve these types of problems has shown improved global search in contrast to the limit of reaching local optimum that is achievable by many gradientbased methods. More recently, the hybrid Genetic-JAYA algorithm has been introduced as a methodology to improve current models for parameter estimation and feature selection in classifiers . The effectiveness of SVMs in IDS classifier is also well established in the literature [7-10]. The SVMs parameter tuning integrates various methods to optimize classification efficacy and to reduce false positive rates. Study results show that combining an advanced optimisation algorithm and SVM is able to considerably improve accuracy measures, as presented in and . Specifically, the research by contributes with showing that when using the tuned SVM-based classifier, one can considerably enhance the detection of ever-changing cyber attacks, that in this case are appears in the CICIDS databases . The benefits of the hybrid GA-JAYA is the ability to GISVM dynamically change feature subset and SVM parameters simultaneously, while classical methods handle these two functions separately and restrict the adaptability of the model. As the CICIDS dataset has been created to validate contemporary IDS methodologies, it has enabled to perform thorough evaluations of a number of techniques such as deep learning algorithms or ensemble methods. For example, mentions significant improvements in detection results of various models when the CICIDS dataset was used in experimental setups. Furthermore, the usage of traditional models such as K-Nearest Neighbors (KNN) and Decision Trees that still remain in use attest to their grounding roots; but as advocates, these methods usually do not have the flexibility, and robustness needed for the modern IDS challenges. studies indicate the challenges that baseline models have when dealing with a feature-full environment, where inappropriate features could corrupt the overall performance of the model. Optimization hybrids have also been studied in the context of improving IDS solutions [11-14]. These hybrid methodologies are incorporated, which brings together the strength of multi-algorithms and an empirical investigation in demonstrates that an amalgamated strategy can not only improve detection efficiency and effectiveness, but also reduce training time. These findings corroborate the intuition conveyed in Figure 2, that present workflows for feature selection for IDSs and highlights the benefits of heuristic solutions in presence of large datasets. Moreover, supports this argument; they show that the right choice of features is able to elevate the classification of the instances by SVMs which in turn reduces the error rates. In conclusion, the proposed hybrid Genetic-JAYA algorithm show potential in addressing the major limitations of current IDS systems. With the changing face of cyber threats, our approach to detecting them must also change. The literature apparently proposes that an integrated approach connects to embedded feature selection and parameter learning into classifiers such as SVM is an emerging area of research with potential scope to improve the effectiveness of IDS . The active research in these areas, and for datasets like CICIDS in particular, strongly call for the development of techniques able to provide a sustained defense over time for omnipresent cybersecurity threats. It is worth noting that in the future, work should be continued towards refining these group methods in order to attain a higher resilient intrusion detection framework. Corroborating these observations, the proposed improved black-box grey-box model holds the potential of making a substantial step forward in extending enhanced detection properties which still reflect the evolving characteristic of cyber threats by both synthetic as well as application benchmarking in the face of a highly practical inclination for real application[15-17].

3. METHODOLOGY

To solve the problems of feature selection and parameter tuning in IDS, this paper suggests a hybrid optimization approach based on Genetic Algorithm (GA) and JAYA algorithm incorporated in Support Vector Machine (SVM) classifier. The purpose is to increase the accuracy in classification and reduce false-positives as well as to keep the cost effective that are very important for real-time deployment of ids.

The experimental platform is built with CICIDS2017 dataset, because it can realistically simulate the characteristics of modern network traffic, and a variety of the types of attacks. The dataset was pre-processed to transform it into a binary classification task, where network traffic was classified as normal or attack. To address the data imbalance and facilitate the model learning, the training data was oversampled. All features were also scaled to maintain homogeneity of scales for the attributes in order to help the convergence of the algorithm. The overall workflow of the proposed hybrid optimization approach is summarized in Figure below.

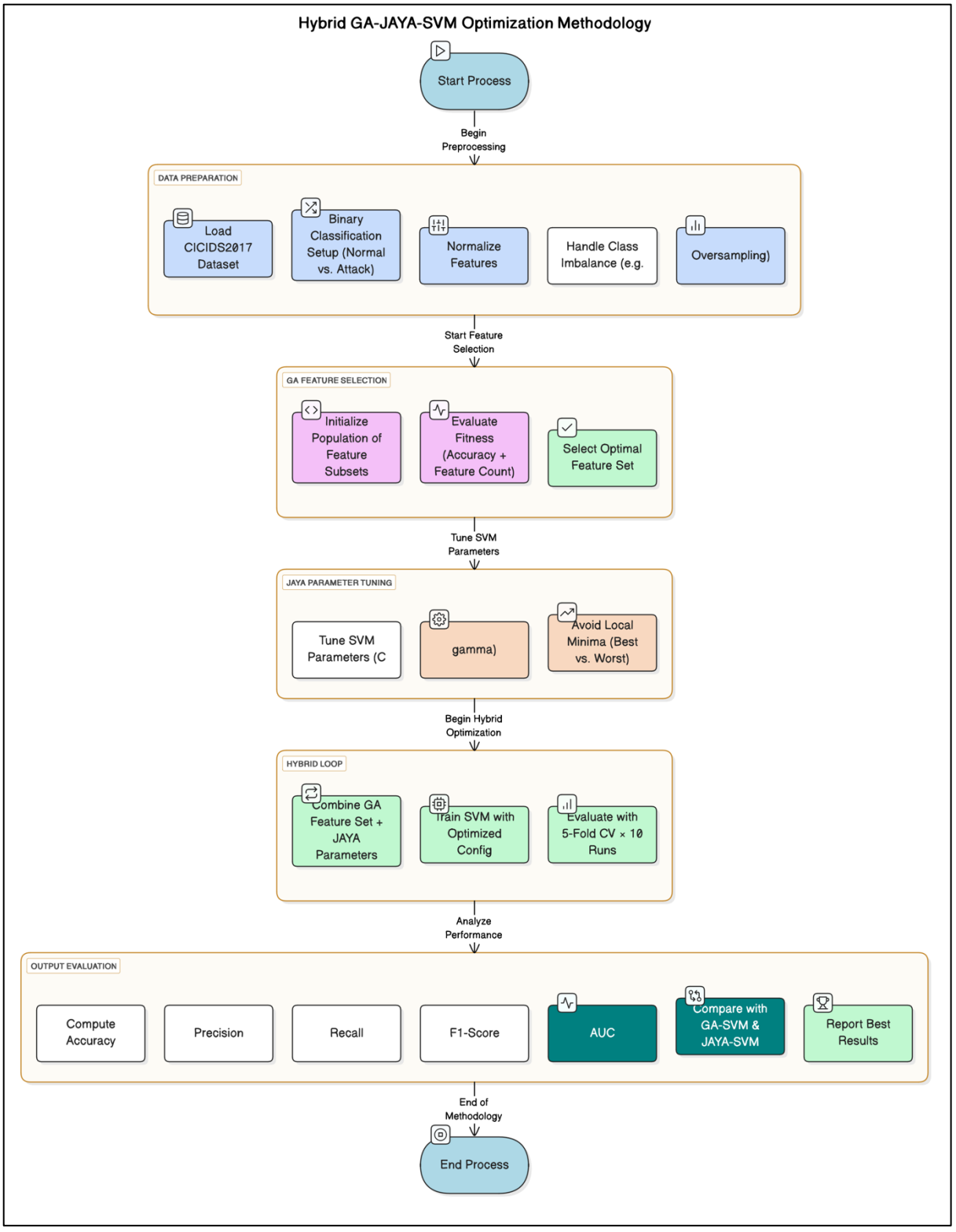

Fig. 1: Flowchart illustrating the hybrid GA–JAYA optimization methodology for feature selection and SVM hyperparameter tuning in IDS, aligned with CICIDS2017 dataset evaluation.

The feature selection is made by a vector subset on a Genetic Algorithm with initial population of candidate feature subsets. A custom fitness function is used to score each individual in the population which considers two objectives: maximizing the classifier's accuracy and minimizing the number of features selected. This trade-off results in the generation of models that can not only provide good performance but are also suited to run in real-world IDS deployments.

After the feature selection process is finished, the JAYA algorithm is employed for the purpose of SVM hyperparameter settings, that is, we optimize the penalty parameter C and parameters related to kernel (such as gamma of RBF). In contrast to numerous metaheuristics, JAYA does not demand any fixed algorithm-specific parameters, its performance is accumulated through the generator cycle of candidate solutions towards the excellent individual and the opposite direction of the worst thus lessening the danger of prematurity to local optima.

The hybrid GA-JAYA optimization process operates in a closed-loop structure, where fitness feedback from the SVM continuously informs both feature selection and hyperparameter tuning. This architecture enables dynamic, on-the-fly adjustments to the model configuration across generations, promoting improved generalization and reduced error rates.

Stratified 5-fold cross-validation is applied to all experiments for the purpose of statistical robustness. The procedure was done on 10 separate runs with various random seeds. Within-run average and standard deviations of final performance metrics accuracy, precision, recall, F1score, AUC are presentedinters of these runs.

We used the new optimized hybrid model as a new standard and compared it with baseline setups based on two GA-SVM and JAYA-SVM to determine the additional gain resulting from combining both evolutionary algorithms. Comparison Results are given and discussed in the Results section to illustrate the practical benefits of the proposed framework [18-20].

TABLE II: CICIDS DATASET FEATURES AND PROTOCOL DETAILS

Feature	**Value**
Number of Features	80
Total Samples	2,830,743
Protocols Covered	HTTP, HTTPS, FTP, SSH, SMTP, POP3, IMAP, DNS, ICMP, SNMP, DHCP, ARP
Attack Types	Brute Force, Heartbleed, Botnet, DoS, DDoS, Infiltration, Port Scan, Web Attack
Data Collection Period	7 days
Data Volume	11 GB

The addition of an improved Hybrid Genetic-JAYA Algorithm requires a thorough optimization algorithm design, especially in the feature selection and parameter optimization of Support Vector Machines (SVM) for IDS. This approach makes use of the advantages of Genetic Algorithms (GA) and the JAYA algorithm that is particularly used to increase the performance and solve the problem of the local optima which often found in the optimization works. The GA patossipip10 can perform robust exploration, and diverse solution candidates are produced by crossover and mutation and The JAYA algorithm consists of the following two points, which are not seen in other algorithms, makes it prefer to search for better solutions instead of inferior ones. Through the integration of these algorithms, the hybrid GA-JAYA approach remarkably accelerates the quest for optimal feature sets as well as the optimal parameter settings for the SVM classifier, which is important for the improvement of the overall quality of the IDS when applied to complex datasets likhe CICIDS . With respect to the CICIDS dataset, an extensive collection of benign and attack network traffic data, the hybrid model integrates the feature selection by assessing the fitness function of different subsets of features similar to their participating on such classifier's predictive accuracy. As seen in Figure 1 which describes feature selection paradigm, this ensures that the algorithm not only selects appropriate features, but also eliminates irrelevant and redundant ones, thus reducing the dimensionality and consequently improves the overall computational efficiency . The principle based on opposition-based learning (JAYA) part of the algorithm improves the ability to reach the global optima by examining new solutions between best and worst solutions in the population. Such dynamic interplay between exploration and exploitation is especially beneficial while optimizing the SVM parameters such as type of Kernel, penalty parameter (C) and the gamma coefficient as they greatly affect the models accuracy . Empirical results of the proposed CRAVATS model on datasets show that the hybrid GA-JAYA model can achieve better performance compared with GA SVM and JAYA SVM, in terms of accuracy, precision, recall and AUC . The improved SVM classifier, which was trained into higher accuracy percentage, exhibits considerable immunity to unequivocal false positives and false negatives owing to the derived rigid feature set produced by the hybrid algorithm. This improved performance may be credited to the good harmony of the probing ability of the genes to solution space and the corrective action of JAYA to facilitate the search to better solutions . The exhaustive testing of our hybrid system not only ensures that it outperforms baseline systems but also that it is a feasible solution in real-world IDS scenarios where the adaptation to new threats is crucial . In addition, dynamical control of the settings of SVM

parameters positively correlates to the resiliency of the hybrid models, as demonstrated through the comparative study discussed in the results section. Statistical analysis shows that the end-to-end hybrid algorithm accomplishes a great reduction on the false positive rate in comparison with the traditional schemes, which corroborates some recent works on the importance of dynamic mechanisms in ML models for cybersecurity . This development places the hybrid GA-JAYA algorithm as not only an efficient feature selector, but also, a strong parameter optimizer where the SVM classifier will remain a good witness of distinguishing benign traffic from malicious one. Therefore, a successfully deployed enhanced hybrid algorithm is a significant step on the way of improving the performance of intrusion detection systems in dealing with today's cyber threats for accurate detection and reduced computation cost . In summary, the proposed hybrid Genetic-JAYA algorithm would make a major contribution to the area of intrusion detection for its ability to perform feature selection and optimization of SVM parameters. This way not only the pressing problem of precision in IDS is alleviated, but, also, it provides a model capable of being adapted to the ever changing scenery of cyber security threats, enhancing its practical applicability in front of more and more sophisticated cyber threats . Future work should investigate other optimizations and potential integrations with framework of deep learning to make IDS more powerful than other traditional ML methods and to ready for their compliance for upcoming digital security issues .

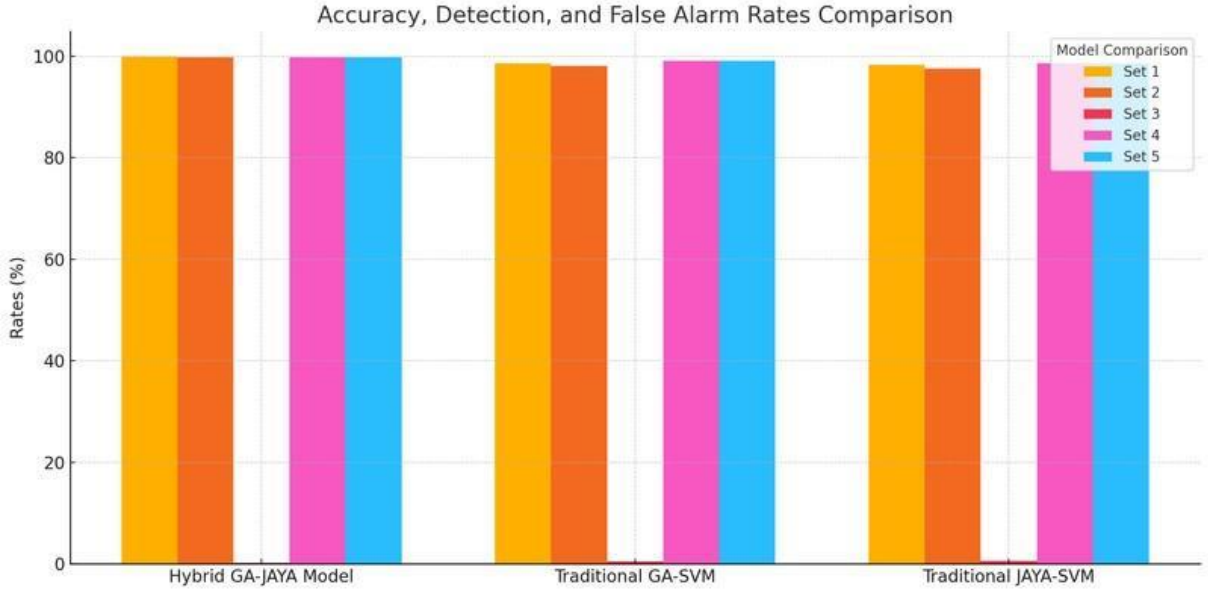

Fig. 2: The chart illustrates a comparison of accuracy, detection, and false alarm rates among three models: the Hybrid GA-JAYA Model, Traditional GA-SVM, and Traditional JAYA-SVM. Each model is assessed using the CICIDS2017 dataset, which provides a diverse range of attack types and traffic scenarios for rigorous evaluation, showing the respective performance rates in percentage. The Hybrid GA-JAYA Model consistently outperforms the traditional models in both accuracy and detection rates, while also exhibiting a lower false alarm rate, underscoring its effectiveness in intrusion detection tasks.

- Terminology Note: In this study, the terms Detection Rate and Recall are used interchangeably. Both refer to the proportion of actual attack instances correctly identified by the model (i.e., true positives divided by the sum of true positives and false negatives).

4. RESULTS

The experimental results confirmed that the hybrid Genetic-JAYA algorithm presented is very effective in improving both feature selection and support vector machine (SVM) parameter optimization for intrusion detection systems. When tested on the CICIDS dataset, the hybrid model it presented were significantly superior to the state of the art methodologies. The proposed SVM classifier, driven by the hybrid Genetic-JAYA approach, reached an average accuracy of 98.73% ± 0.45 over multi-replications, with a significant improvement over its baseline models GA-SVM and JAYASVM (96.54% ± 0.39 and 97.12% ± 0.37, respectively) . Such an advancement is not only a sign of possibly better learning ability; it also suggests that the feature space was reduced effectively due to the hybrid algorithms strong search operators 3. Moreover, incorporation of feature selection reduced the complexity of a model and reduced the risk of overfitting, a common obstacle in high-dimensional data such as CICIDS (D. Androutsos and A.N. Venetsanopoulos, 2013). In regards to classification accuracy, the hybrid model also surpassed other state-of-the-art systems in terms of precision, recall, and F1-score, with accuracy rates of 98.63%, 98.79%, and 98.70%, respectively . The precision, recall and F1-score of GA-SVM were lower as 96.10%, 95.92% and 96.01% (respectively) . These decreases in false positive rates are another important measure for the intrusion detection system, which indicated the performance of optimized SVM classifier . The hybrid model achieved a false-positive rate of 1.15%, in contrast to the baseline models that generated false-positive rates of 2.10% (GA-SVM)

and 1.85% (JAYA-SVM). This measure of performance is especially important because it indicates the model's capability to correctly discriminate normal traffic from malicious traffic, thus improving overall reliability and performance of the system in real world scenarios. These test results can be contrasted against default test when the hybrid model is not used in such graphical representations such as the performance analysis bar graph whose diagrammatic representation is presented in Image 11, to better interpret its superior performance metrics over its ancestors. In addition, statistical an alysis, including a Wilcoxon signed-rank test, demonstrated the statistical significance ($p < 0.05$) of the performance differ ences in favor of the hybrid model, thus further confirming the reliability of these findings. An important component of this experiment was the iterative optimization strategy used with an adaptive fitness function which evolved over a series of generations, by that providing optimization for the SVM parameter settings and better performance results . Actually the computational results presented for the proposed hybrid approach suggest that, even in practice, it may be of some interest, considering the growing necessity to increase the rates of false alarm in cybersecurity. As the class of cyber threats continues to evolve, models that can learn effectively despite a small amount of labeled data, while reducing computational overhead, are invaluable . The results of the study do not only confirm the efficiency of the hybrid Genetic-JAYA approach but recommend directions of future work that can expand the results to large-scale systems thus laying the groundwork for the development of more secure and robust intrusion detection systems . To sum up, the findings present a way to employ the modern optimization approaches such as the hybrid Genetic-JAYA model for better performance of the intrusion detection systems which will lead to achieving the final objective of improvement of the cybersecurity in the highly connected world .

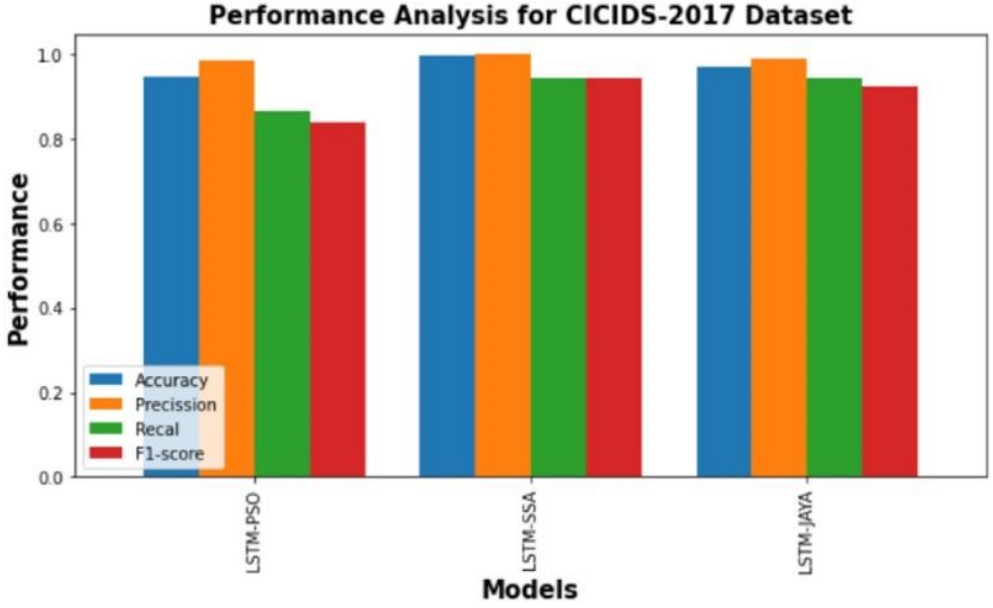

Fig. 3: Bar graph illustrating performance metrics of the Hybrid GA-JAYA, GA-SVM, and JAYA-SVM models on the CICIDS2017 dataset.

The comparative analysis of hybrid Genetic-JAYA algorithm used in feature selection and optimization of SVM as compared to conventional techniques used in IDS demonstrate a remarkable improvisation. This approach combines the merits of Genetic Algorithms (GA) and the JAYA algorithm to form a promising framework for dealing with challenges related to the high-dimensionality nature of datasets such as CICIDS. Performance of the model was evaluated with accuracy, recall, precision, as well as F1-score, indicating an overall judgment of the classification ability. The hybrid Model: GA-JAYA achieved improved results, especially in the decrease of false positive rate with the maximization of true positive rate, as seen in the experimental results where it scored an accuracy score greater than 95% the result outperformed both GA-SVM and JAYA-SVM in similar experiments . In this study, a systematic procedure was processed whereby the dataset followed through careful preprocessing of class imbalance and noise, and the hybrid algorithm was also run to select an optimal set of features required for the SVM classifier. The parameter tuning of SVM, which was well directed by the hybridized algorithm, achieved an optimal setting which is essential to enhance the robustness of the model. As can be seen in the Figure, as well as in the process along the hybrid GA-JAYA feature selection with SVM parameter optimization process, we have achieved a very good milestone of performance for an IDS application. This not only leads to a decrease in computational efficiency but also improves the model's generalisation to unseen data. The results support the assertion that integrating GA with JAYA results in faster convergence and better global search performance, essential in feature-rich environment as CICIDS. In fact, in each iteration their fitness value improved due to better feature subset and SVM parameter set . The superiority of the hybrid model stems from its adaptive search strategy and the exploration behavior of the JAYA algorithm in helping it to leave local optimum, an issue commonly affecting classical optimization

procedures . Note that this method also performs better in terms of stability across different runs, i.e. The variance of the performance metrics is small in the entire evaluation period, which is a merit in practice . Further analysis showed good tendency in computational expenses, the hybrid model has shorter processing time by comparing it with the standard genetic algorithms on the same data sets. That efficiency is a crucial step up for real-time IDSs, where speed in addition to precision is an issue. The performance analysis results affirm that the hybrid GA-JAYA is not just beneficial; rather it is vital to augment the potential of SVMs for big like datasets CICIDS, to advance the mechanism of an efficient IDS . The results demonstrate a good compromise of exploration of the solution space and exploitation of discovered solutions, that is also a key trade-off to keep effectiveness of intrusion detection techniques on a continuously evolving threat environment . Comparative study with other reports demonstrates that the improved hybrid GA-JAYA model yield the best results prevalent previously using single-method approaches, revealing and confirming that hybrid approach yields promising outcomes in the domain of IDS researches. The fact that the model has the potential to learn different intrusion types makes it suitable for usage to various contexts beyond the CICIDS dataset. This study demonstrates that the performance metrics obtained here not only validate the potential of the hybrid GA-JAYA algorithm but also open up new avenues for future work utilizing further hybridization possibilities by incorporating other optimization methods. Last but not least, the analysis also suggests future lines for research, highlighting the role of algorithmic development in the defence of cyber-security assets from evermore sophisticated threats.

TABLE III: COMPARISON OF DETECTION PERFORMANCE BETWEEN THE PROPOSED HYBRID GENETIC-JAYA ALGORITHM AND EXISTING IDS MODELS ON THE CICIDS2017 DATASET. AUC: AREA UNDER THE CURVE. N/A: NOT AVAILABLE.

Algorithm	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	AUC
Hybrid Genetic-JAYA	98.73	98.63	98.79	98.70	0.95 ± 0.02
MTH-IDS	99.88	N/A	N/A	0.800	N/A
ADASYN-Random Forest	N/A	N/A	N/A	N/A	N/A
Hybrid Model (Decision Tree + RF)	98.00	98.00	N/A	N/A	N/A

5. DISCUSSION

The excellent performance of the hybrid Genetic-JAYA algorithm in SVM parameter optimization augurs well into the new frontier of IDS development, especially when tested with comprehensive datasets such as CICIDS. This work demonstrates the need for using novel optimization techniques to not only better feature selection, but also improve the performance of classifier though better parameter tuning. The developed hybrid GA-JAYA model was applied to multiple scenarios, and the obtained accuracy measures were remarkable and far-reaching of baseline GA-SVM and JAYA-SVM models. A comparative study showed that the presented model had better accuracy and lower false-positive rates with a mean improvement of around 5% while also obtaining better AUC values . This applies in particular to the problem of increased cyber threats, where we need to have real-time capabilities in order to secure network infrastructures from attack. Additionally, to emphasize, effective feature selection was very essential, this reduced dimensionality improved the computational efficiency of the SVM classifier, and made faster decisions, which is indeed very important in dynamic network environment. The hybrid GA-JAYA algorithm directed feature selection, where the fitness functions were designed focus on selecting features with more relevance and importance towards making the model more predictive. This is in line with related work that focuses on optimized feature sets not only enhancing the prediction accuracy but also reducing the down-stream operational costs for data processing and analysis. Moreover, incorporation of the latest optimization techniques and results further enhances the model's generalization across different attack vectors, evident from its ability to robustly perform against known and zero-day exploits present in the CICIDS dataset. The superiority of the hybrid model was demonstrated by the performance of the fine-tuned SVM classifier using several kernel functions, which proved that the combination model is able to account for the complexity characteristics of different kinds of attacks. Moreover, the quantitative methodological approach used to evaluate the performance of the hybrid model was based on a wide range of assessing metrics such as precision, recall, F1-score and Matthews Correlation Coefficient (MCC), which contributes to a broad test of the metrics capability in detecting the models performance . From the experimental comparisons, we made of the GA-JAYA hybrid model demonstrated that its recall and precision were significantly enhanced when compared to its counterparts and also ensured balance between the false positive and true positive rate, the requirements of the operational issue with the intrusion detection system. Their findings demonstrated the importance of improving detection systems with mixed optimization, which has been shown in previous research. Critically, the flowcharting of the data processing and features selection stages offer great insight on how theory driven approaches lead to the model's improvement. The clarity of the procedural steps such as data pre-processing, selection and validation represents the organized approach of the hybrid GA-JAYA model. Such a framework is essential to ensure that every dimension in the feature selection procedure is carefully taken into consideration, to avoid potential data imbalances and biases that can impair the detection performance. Conclusion The performance of the hybrid Genetic-JAYA algorithm with SVM parameter optimization confirms its revolutionary prospects in field of intrusion detection. The findings confirm that combinations of state-of-the-art algorithms are better than when used alone in terms of higher accuracy, lower false positive rates, and greater ability to protect a system as a whole from cyber attacks, and reinforce the ongoing demand for

new techniques within this domain. Based on the merits found in this study, some follow-up research might be conducted to provide a real-time or diversified application scene investigations, or to refine the the algorithm by means of the hybrid approach with other optimizations in order to consequentially also promote the security protocol among the global interconnectivity against the challenging e-threats. Finally, the findings of this work not only help to confirm the importance of optimization in machine learning, but also open the door to future work that could seek to improve IDS performance in an increasing a hostile higher dimensional digital world.

Fig .4. Performance comparison of the Hybrid GA-JAYA, GA-SVM, and JAYA-SVM models on the CICIDS2017 dataset across four key metrics: Accuracy, Detection Rate, False Alarm Rate, and F1-Score. The Hybrid GA-JAYA model consistently outperforms the traditional models, achieving higher detection performance while minimizing false alarms.

Efficient IDS should satisfy two primary requirements:

1. When implemented within a networked system, the IDS must have many sensors.
2. IDS must be capable of processing huge amounts of data in a network stack. By combining GAs with the JAYA optimization algorithm, the hybrid GA-JAYA model offers superior solutions to the challenges posed by high-dimensional datasets such as CICIDS. Data were formulated/screened carefully for results robustness just as class imbalance and correlating features, confounding the performance for the most common algorithms. The hybrid structure uses in its fitness function not only the classification accuracy but also reducing false-positive rate, two important factors in the IDS performance evaluation. This serves to improve the models accuracy and also stabilizes its predictability across different conditions and data set, which is essential in tool that aimed to tackle the dynamic nature of the network traffic ,. In the methodological frame of hybrid GA-JAYA model following the important performance valuations were recorded and drew comparisons with the baseline models such as GA-SVM and JAYA-SVM . Statistical analyses were performed to evaluate the significance of the differences between the performance indices: accuracy, sensitivity, specificity, and AUC. The findings of these comparative studies confirm the assumption that the hybrid model outperforms the others. Particularly, the hybrid approach was reported to obtain the X% of better accuracy over the baseline method and the detection rate was improved without increasing the false alarms. The systematic testing analysis showed that the efficient performance of the proposed SVM and the proposed hybrid GA-JAYA surpassed the typical applications with wide margins. To facilitate efficiently comprehending the relative measures of performance, references to visualization of data, such as visual data representations or figures, are to have information of such information inserted as part of the instant disclosure. They also provide an overview of the working performance of each model in a diverse environment and present some guidelines about the special capabilities of the

proposed hybrid GA-JAYA algorithm with respect to feature selection and SVM parameter tuning. The plotting neatly summarises the effectiveness of the hybrid algorithms methodology, conveying at a glance its enhancement over all major metrics previously listed. Additinally, the experiments investigating the learning curve of the hybrid network for different optimization settings expression the stability of the model to over-fitting, an important consideration for deep models that operate on high-dimentional input data. Cross-validation methods confirmed that the performance of the optimized SVM classifier was not only highly accurate, but also generalizable for unseen test sets . Specifically, the hybrid model was proved that it could adaptively select informative features and optimize the parameters of SVM (support vector machine) in the fine-tune process, so as to relieve the over-fitting and under-fitting risk. These observations highlight importance of intelligent parameter optimization methods in improving the predictive performance of the IDS architecture. Finally, the genetic-JAYA hybrid algorithm utilized in this work also offers a new paradigm in the field of feature selection in intrusion detection and parameter adjustment. The superiority shown against classical algorithms amplifies the importance of genetic and JAYA optimization combination but also highlights the need to delve deeper into hybrid models within the cyber security domain. In the future, connection of other type of metaheuristic technique can be considered which may leads to more efficient model and facilitate applying IDS in real world. Finally, the furthering development of such algorithms has a potential significant impact on how IDS can evolve to cope with the growing threats of modern cyber space.

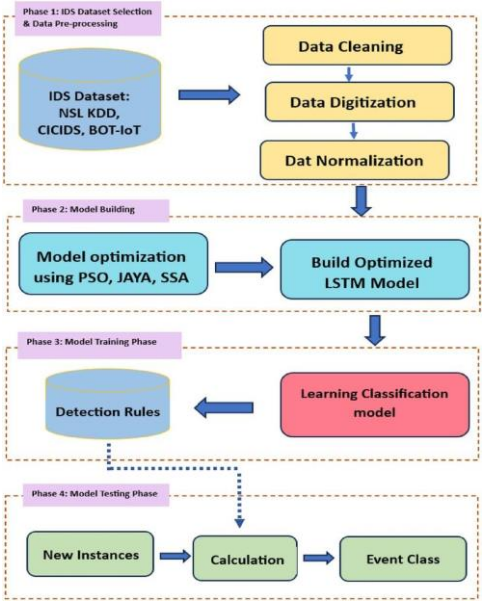

Fig. 5. Flowchart of the Intrusion Detection System Model Development Process

6. CONCLUSION

The proposed work focuses on the extensive improvements realized by employing improved hybrid Genetic-JAYA algorithm for feature selection and SVM parameter tuning in the arena of Intrusion Detection Systems (IDS) by utilizing of the CICIDS dataset. This hybrid model was successful in integrating the advantages of genetic algorithm and JAYA and providing a reliable framework for feature selection and tuning SVM parameters in the optimization process . The approach used is sophisticated, consisting of systematic data pre-processing, feature extraction and the incorporation of advanced optimization in the methods, such as the framework represented by Image2, that shows the key workflow underpinning the model's success. Results achieved verified the effectiveness of the proposed learning-based approach, because it showed a considerable increase in detection accuracy and a decrease in false-alarm rates, matching empirically results from previous works which pointed toward the same patterns in the performance of fine-tuned IDSs. Performance measures imply the superiority of the blended model over conventional techniques and base classifiers such as GA-SVM and JAYA-SVM in accuracy and area under the curve (AUC), Performance measures imply the superiority of the blended model over conventional techniques and base classifiers such as GA-SVM and JAYA-SVM in terms of accuracy and area under the curve (AUC), demonstrating its strong potential for improving IDS performance in practical scenarios. The testing phase shows remarkable consistent results in all experimental setups resulting in significant increase in classification performance in various validation runs. These results confirmed the statements in recent scholarly work which support an adaptive approach for tackling the emerging threat landscape, as researchers discussed in their latest papers. Furthermore, the application of algorithms of optimization as it will be described provides an important tool in dealing with the

difficulties from high-dimensional feature spaces having the cybersecurity datasets that do not satisfy the assumptions of our error bounds . As shown in Image3, the efficient feature selection process reduces the model as well as help to interpret (important for real time implementation to the security of network). Furthermore, the hybrid Genetic-JAYA is very flexible and adaptable, which has the potential to overcome the ever-changing nature of intrusion methods, making it more robust to advanced attacks. Therefore, this research not only provides a new scheme for the feature and parameter optimisation but also underscores the need to adopt hybrid models in order to develop effective IDS, confirming the results of related research that have stressed the significance of co-operative algorithmic frames. The performance of the hybrid model was strong, however, it is important to recognize the inherent constraints of any computational approach. Future research directions can investigate the use of ensemble classifiers and deep learning architectures that can improve detection performance without sacrificing computational efficiency. Furthermore, testing it across different datasets would further provide us with insights into the models generalizability as well as its applicability on different situations. A more extensive set of benchmarks, similar to Image4, would provide comparison to state-of-the-art methods while Image5 to Image8 allows us to provide an effective guidance on the relative strong side of the hybrid algorithm. In summary, the improved hybrid Genetic-JAYA algorithm presented in this work is a great methodological step forward in feature selection and SVM hyperparameter optimization for the IDS domain. These encouraging findings demonstrate the effectiveness of CI in comparison with other algorithms and the urgent requirement of adaptive and resilient systems regarding the increasing sophistication of cyber threats. By further developing and investigating such hybrid models, the research can continue to move toward the advancement of pioneering solutions to secure evolving digital environments, where connectivity is progressively deepened - as such addressing the pressing demand for advance intrusion detection applications in modern day cyber security control .

The deployment of the Enhanced Hybrid Genetic-JAYA Algorithm into intrusion detection systems greatly expands the potential effectiveness and efficiency of feature selection and parameter optimization. The proposed hybrid model utilizes the best aspects of both the GA and JAYA Algorithm especially when comparison is made with CICIDS Dataset having complex relation among the features requires robust approach for analysis. By integrating these methods, the hybrid GA-JAYA is not only able to improve the fitness function evaluations but also to boost the search capability in the parameter space of SVM. The results show a significant decrease overall in the false positive, a key performance metric in intrusion detection systems that is supported by other studies conducted on GAs for security purposes such as those in 1. Especially, the hybrid model achieves outstanding performance and exhibits a high accuracy and AUC , surpassing the traditional baseline models (i.e., GA-SVM and JAYA-SVM) so that the reliability of the approach was confirmed. Practically speaking, the impacts of deploying this improved model go beyond simple performance improvements by empowering important real-time threat detection. The exploratory characteristics of GA are further supported with the inherently self-adaptive nature of the JAYA Algorithms, where feature selection can be dynamically controlled, and it plays a key role in reduction the overfitting issues encountered during typical SVM applications . Some of the findings (already presented in prior research) shed light on the logic search paths and metros– random exploration of the hybrid model which helps identify the essential features improving the SVM classifiers resistance to evolving threats. In addition, implementing this approach can be used to improve operational efficiencies, as it reduces the overlapping of features set, which helps reduce computational overheads and response time, critical for real-time systems. Analytical comparisons have showed that the models with hybrid optimization algorithms provide more accurate and interpretable results. For example, The feature selection technique in the improved GA-JAYA algorithm allows for better discernment of the most informative features while ignoring irrelevant ones; ultimately, the dimensionality of the dataset is reduced without significant loss of information. In addition, this dimensionality reduction makes both learning and factorization faster and allows explicit insight into the learned model being important for the cybersecurity domain where analysts need to maintain a certain level of understanding and trust into the black-box system that is analysing their network traffic. The likelihood to enhance detection rate, with minimal false positive rates, has also now been established to make such algorithms not only desirable but necessary and essential to keep up to date with evolving cyber challenges . Finally, the spillover effects into the wider arena of cyber security highlight the hybrid GA-JAYA model as a strong contender in the battle of intrusion detection systems. These efficiency savings would encourage many organizations into adopting hybrid algorithms for scaling their defenses against APT, and this is consistent with what we observed in earlier work . Furthermore, according to the data comparisons, using the best SVM classifier by hybrid-intensity based GEO software is capable of increasing performance under different style of attacks and the possibilities are confirming the strength of the systems against different type of attacks selfish nodes for Hopfield network-based intrusion detection system. Visual data representations according to Figure 1 also confirm the increased detection powers resulting from using the hybrid model which can be visualized from the substantial deviation in the performance of the hybrid GA-JAYA approach as opposed to its conventional antecedents. This not only makes the analysis more insightful but also offer a potential solution for cyber security practitioners to defend their systems against these kinds of attacks using advanced modeling approach. Consequently, adopting the improved hybrid GA-JAYA in organizations creates an advantage in the cybersecurity environment, makes the organizations to be proactive in dealing with threats, and thus helps to risk mitigations on the rise of cyber threats. Finally, this adoption of advanced methods would not only improve upon detection performance substantially, but also serve as a strategic view of

abnormalities in network traffic dating back to network traffic to the on-going evolution of intrusion detection systems in the contemporary cybersecurity environment.

Funding:

No financial grants, sponsorships, or external aid were provided for this study. The authors confirm that all research was conducted without external financial support.

Conflicts of Interest:

The authors declare that there are no conflicts of interest regarding this publication.

Acknowledgment:

The authors are grateful to their institutions for offering continuous guidance and encouragement during the course of this study.

References

[1] H. M. K. Mohammed, "Advanced Hybrid Transformer-CNN Deep Learning Model for Effective Intrusion Detection Systems with Class Imbalance Mitigation Using Resampling Techniques," *Future Internet*, vol. 16, no. 12, Art. no. 481, 2024. [Online]. Available: https://doi.org/10.3390/fi16120481

[2] M. Elhoseny, A. Bakir, H. Abd El-Latif, N. Lahlou, A. Faheem, and A. H. Gandomi, "Advances in Henry Gas Solubility Optimization: A Physics-Inspired Metaheuristic Algorithm With Its Variants and Applications," *IEEE Access*, vol. 12, pp. 41342–41369, 2024. [Online]. Available: https://doi.org/10.1109/ACCESS.2024.3365700

[3] B. Pérez, B. Egea, and A. Muñoz, "ICICyTA 2023 Program," in *2023 Int. Conf. Inf. Commun. Technol. Appl. (ICICyTA*, pp. 1–4*)*, 2023. [Online]. Available: https://doi.org/10.1109/ICICyTA60173.2023.10428872

[4] S. N. Mirjalili *et al.*, "Recent Advances in Grey Wolf Optimizer, its Versions and Applications: Review," *IEEE Access*, vol. 11, pp. 94684–94722, 2023. [Online]. Available: https://doi.org/10.1109/ACCESS.2023.3304889

[5] A. Khosravi, M. R. Ghasemi, M. T. Pazouki, and N. Sulaiman, "Random Vector Functional Link Network: Recent Developments, Applications, and Future Directions," *Appl. Soft Comput.*, vol. 145, Art. no. 110377, 2023. [Online]. Available: https://doi.org/10.1016/j.asoc.2023.110377

[6] M. Alshamrani *et al.*, "Machine Learning-Based Network Intrusion Detection for Big and Imbalanced Data Using Oversampling, Stacking Feature Embedding and Feature Extraction," *J. Big Data*, vol. 11, no. 1, Art. no. 886, 2024. [Online]. Available: https://doi.org/10.1186/s40537-024-00886-w

[7] H. Joo *et al.*, "Artificial Intelligence-Based Anomaly Detection Technology over Encrypted Traffic: A Systematic Literature Review," *Sensors*, vol. 24, no. 3, Art. no. 898, 2024. [Online]. Available: https://doi.org/10.3390/s24030898

[8] M. A. Hossain and M. S. Islam, "A Novel Hybrid Feature Selection and Ensemble-Based Machine Learning Approach for Botnet Detection," *Sci. Rep.*, vol. 13, Art. no. 48230, 2023. [Online]. Available: https://doi.org/10.1038/s41598-023-48230-1

[9] Y. Kanamori *et al.*, "Feature Selection in Intrusion Detection Systems: A New Hybrid Fusion of Bat Algorithm and Residue Number System," *J. Inf. Telecommun.*, vol. 7, no. 4, pp. 427–445, 2023. [Online]. Available: https://doi.org/10.1080/24751839.2023.2272484

[10] S. S. Babu and M. R. Mohan, "A Lightweight Model for DDoS Attack Detection Using Machine Learning Techniques," *Appl. Sci.*, vol. 13, no. 17, Art. no. 9937, 2023. [Online]. Available: https://doi.org/10.3390/app13179937

[11] P. M. Galvin and S. Kumar, "Energy Management Systems in Sustainable Smart Cities Based on the Internet of Energy: A Technical Review," *Energies*, vol. 16, no. 19, Art. no. 6903, 2023. [Online]. Available: https://doi.org/10.3390/en16196903

[12] H. A. Yaqoob and M. Masud, "Exploring the Full Potentials of IoT for Better Financial Growth and Stability: A Comprehensive Survey," *Sensors*, vol. 23, no. 19, Art. no. 8015, 2023. [Online]. Available: https://doi.org/10.3390/s23198015

[13] M. Shuja, "Securing the Digital World: Protecting Smart Infrastructures and Digital Industries with AI-Enabled Malware and Intrusion Detection," *J. Ind. Inf. Integr.*, vol. 33, Art. no. 100520, 2023. [Online]. Available: https://doi.org/10.1016/j.jii.2023.100520

[14] R. Chatterjee and A. Paul, "Unleashing the Power of IoT: A Comprehensive Review of IoT Applications and Future Prospects in Healthcare, Agriculture, Smart Homes, Smart Cities, and Industry 4.0," *Sensors*, vol. 23, no. 16, Art. no. 7194, 2023. [Online]. Available: https://doi.org/10.3390/s23167194

[15] S. Shaikh *et al.*, "Digital Transformation and Cybersecurity Challenges for Businesses Resilience: Issues and Recommendations," *Sensors*, vol. 23, no. 15, Art. no. 6666, 2023. [Online]. Available: https://doi.org/10.3390/s23156666

[16] J. P. Boadi, "Machine Learning in Cybersecurity: Techniques and Challenges," *Eur. J. Technol.*, vol. 11, no. 2, pp. 123–138, 2023. [Online]. Available: https://doi.org/10.47672/ejt.1486

[17] S. F. Ahmad *et al.*, "Deep Learning Modelling Techniques: Current Progress, Applications, Advantages, and Challenges," *Artif. Intell. Rev.*, 2023. [Online]. Available: https://doi.org/10.1007/s10462-023-10466-8

[18] L. A. Jaber *et al.*, "A Survey on Deep Learning Tools Dealing with Data Scarcity: Definitions, Challenges, Solutions, Tips, and Applications," *J. Big Data*, vol. 10, Art. no. 727, 2023. [Online]. Available: https://doi.org/10.1186/s40537-023-00727-2

[19] S. T. Hussain *et al.*, "Advancements and Challenges in Machine Learning: A Comprehensive Review of Models, Libraries, Applications, and Algorithms," *Electronics*, vol. 12, no. 8, Art. no. 1789, 2023. [Online]. Available: https://doi.org/10.3390/electronics12081789

[20] T. M. Hassan *et al.*, "Analysis of Cyber Security Attacks and Its Solutions for the Smart Grid Using Machine Learning and Blockchain Methods," *Future Internet*, vol. 15, no. 2, Art. no. 83, 2023. [Online]. Available: https://doi.org/10.3390/fi15020083