
An Agentic AI-Driven Autonomous Threat Hunting Framework Using Retrieval-Augmented Multi-Agent Systems and Deep Reinforcement Learning

M. P. Bobby¹, Vignesh R. S², P. N. Karthikayan³, Gayathri Devi Subramanian⁴, Bindu K V⁵, B. Jegajothi^{6*}

¹ Assistant Professor, Department of Computer Science and Engineering, Sathyabama Institute of Science and Technology, OMR, Rajiv Gandhi Salai, Jeppiaar Nagar, Semmencherry, Chennai – 600119, Tamil Nadu, India

Email: bobby.m.p.cse@sathyabama.ac.in

² Student, Department of Computer Science and Engineering (Artificial Intelligence & Robotics), VIT Chennai, Tamil Nadu, India

Email: vigneshrs182@gmail.com

³ Assistant Professor, Department of Computer Science and Engineering (Cybersecurity), St. Joseph's Institute of Technology, OMR, Chennai, Tamil Nadu, India

Email: karthikayanpn@stjosephstechnology.ac.in

⁴ Associate Professor, Department of Data Science and Information Technology, Vels Institute of Science, Technology and Advanced Studies (VISTAS), Velan Nagar, Pallavaram, Chennai, Tamil Nadu, India

Email: gayathri.s7@gmail.com

⁵ Assistant Professor, Department of Science and Humanities (General Engineering/EEE), R.M.K. College of Engineering and Technology, Tamil Nadu, India

Email: bindu@rmkcet.ac.in

⁶ Research Associate, SRS Tech Solutions, Chennai, Tamil Nadu, India

Email: jegajothibalakrishnan@gmail.com

*Corresponding author: Dr. B. Jegajothi (jegajothibalakrishnan@gmail.com)

Abstract: As cyberattack sophistication has grown, there is a growing need for intelligent, adaptive threat hunting solutions to accurately detect an array of network intrusions while reducing false alarms. Traditional IDS methods might struggle to generalize across data sets, achieve optimal hyperparameter tuning, or provide sufficient interpretability in the context of large-scale cybersecurity datasets. This study presents a Cyber Threat Hunting Framework based on Grey Wolf Optimizer (GWO-RAG-MADRL-Net) to enhance the detection of multiple cyber-attacks of CICIDS2017 benchmark datasets. Proposed framework conducts thorough data pre-processing, mutual information based feature selection, and GWO to search for the optimal hyperparameters of the model, and finally, an optimized XGBoost classifier is used for intelligent threat classification. To further interpret the model decisions, explainable artificial intelligence is implemented based on SHAP to build transparency and feature level understanding. The experimental results show high accuracy, precision, recall, F1 score, ROC-AUC, and PR-AUC for the proposed framework, which are equal to 99.57%, 99.57%, 99.57%, 99.57%, 99.98%, and 99.93% respectively, demonstrating the highly reliable detection of different cyberattacks. The results of the optimized framework are compared with Logistic Regression, Random Forest, Extra Trees, and LightGBM, showing its effectiveness in providing strong classification performance and better discriminative capability. The proposed solution can be efficiently and scalably implemented at an enterprise level to detect intelligent threats in real-time network security scenarios, and it is interpretable.

Keywords: Cyber Threat Detection, Intrusion Detection System (IDS), Grey Wolf Optimization (GWO), XGBoost, Feature Selection, Explainable Artificial Intelligence (XAI), SHAP, CICIDS2017, Network Security, Machine Learning.

1. Introduction

Today's cyber security landscapes are much more complex as enterprise infrastructures, cloud computing, Industrial Internet of Things (IIoT), and software-defined networks are rapidly undergoing digital transformation. The increasing sophistication of cyber threats, such as distributed denial-of-service (DoS) attacks, botnets, brute-force, web application attacks and advanced persistent threats (APTs), requires organizations to monitor massive amounts of network traffic that is created on a continuous basis and consists of various types of traffic. Signature-based intrusion detection systems are not as effective when it comes to new and changed attack patterns, due to the fact that they depend on a predefined attack signature, and have limited adaptability to attacks which are not known beforehand. Though machine learning and deep learning for automated intrusion detection has significantly advanced to learn patterns from historical network data for the detection of complex traffic, there are several challenges on this path: high dimensionality of the feature space, suboptimal hyperparameter selection, limited model interpretability and sophistication of adversarial cyberattacks. Thus, it is needed to develop intelligent, adaptive and explainable cyber threat hunting frameworks for accurate, scalable and trustworthy network intrusion detection and timely security decision making in dynamic enterprise environment.

1. Introduction

Today's information systems are much more complex than ever before, with a large cyberattack surface driven by the unprecedented growth of cloud computing, Internet of Things (IoT), software-defined networking, edge computing and enterprise digital transformation. Organizations are constantly producing vast amounts of diverse network traffic that needs to be monitored in real-time to detect increasingly advanced cyber threats such as distributed denial of service (DoS) attacks, botnets, brute-force intrusions, Web application exploits, insider attacks and advanced persistent threats (APTs). Traditional signature-based intrusion detection systems are no longer adequate, since they do not have sufficient capability to detect new or changed attack behaviors, but are mostly based on known attack signatures. Thus, artificial intelligence (AI) has become a key enabler for creating intelligent, adaptive and autonomous cybersecurity systems that can learn complex patterns of attacks from huge quantities of network traffic data directly. Recent breakthroughs in generative AI have further strengthened cyber defense by allowing for automated security analysis, intelligent vulnerability assessment, contextual reasoning, and adaptive threat mitigation, which will boost the efficiency of security operations and make analysts' lives easier [1]. In addition, AI-powered automation has enhanced real-time threat intelligence generation and proactively cyber defense solutions when integrated with enterprise cybersecurity infrastructures.

The recent strides in Agentic Artificial Intelligence have further revolutionized the current cybersecurity landscape by introducing autonomous software agents that can perceive, reason, plan, make decisions, and learn continuously. In contrast to traditional machine learning algorithms that mostly operate on passive classification, agentic systems proactively collect contextually relevant cyber threat intelligence, orchestrate multiple specialized agents, and adjust their behavior based on a constantly changing attack landscape. In complex enterprise environments, AI-driven security solutions like multi-agent frameworks that leverage Large Language Models (LLMs) have proven to have significant potential in intelligent threat correlation, attack investigation, incident response, and security orchestration [2]. Likewise, AI-enhanced Security Operations Centers (SOCs)

are now in the process of introducing collaborative LLM-based agents for security monitoring, incident investigation, decreasing response time, and supporting cybersecurity analysts in making informed decisions in highly dynamic network environments [3]. The development of these emerging technologies offers a robust base for next generation autonomous cyber threat hunting systems to enhance detection accuracy, operational efficiency and overall cybersecurity resilience.

Even with these major developments, there are several practical issues with the current intelligent intrusion detection frameworks. In many cases, network traffic is high dimensional with redundant and irrelevant features that adds to the complexity of the computation and decreases the generalization of the classifiers. Furthermore, the traditional optimization techniques often do not find the globally best feature subset or the hyperparameters of the model, leading to sub-optimal detection performance. In order to overcome these drawbacks, recently, reinforcement learning (RL) has been studied for adaptive feature selection and intelligent intrusion detection. Reinforcement learning-based multi-feature selection networks have shown better exploration ability to dynamically select informative traffic features and to improve classification accuracy on complex intrusion detection datasets [4]. Similarly, deep reinforcement learning has successfully been used in combination with IDS to optimize feature selection and enhance model convergence and reduce computational overhead without compromising the predictive model performance [5].

A key issue in today's cybersecurity is the need for independent response technologies that can keep up with rapidly evolving threat environments. Safe reinforcement learning has recently been shown to be capable of dynamically optimizing the defensive action of intelligent intrusion response systems in CPS that meet operational safety constraints [6]. Moreover, reinforcement learning with incremental feature drift detection has greatly enhanced the adaptability of IDS under changing attack distributions to support continuous learning without much retraining [7]. However, many of the current methods still have shortcomings, including a lack of contextual reasoning, lack of threat intelligence integration, lack of model interpretability, and lower scalability in large enterprise settings. Moreover, benchmark results on the CICIDS2017 data-set show that while traditional machine learning algorithm can attain competitive classification accuracy, there are still demands for being robust, adaptive, explainable and autonomous in real-world cybersecurity applications [8].

To address these challenges, this paper presents a new intelligent cyber threat hunting framework named GWO-RAG-MADRL-Net that combines the approach of mutual information-based feature selection, Grey Wolf Optimization (GWO), optimized machine learning, and explainable artificial intelligence to enhance multi-class cyberattack detection using the CICIDS2017 benchmark dataset. The proposed framework will afford a scalable base for future integration with retrieval-augmented reasoning, collaborative multi-agent intelligence, and autonomous reinforcement learning based cyber defense systems while improving the detection capability by efficient feature engineering, optimization-driven learning, and interpretable decision analysis.

2. Literature Survey

The cyber threat detection is drastically transformed by the application of intelligent monitoring of network traffic in large scale networks based on machine learning, deep learning and optimization techniques, with the recent developments in artificial intelligence. Current research has been explored on various types of ensemble learning, gradient boosting, CNN, RNN, transformer, explainable AI and metaheuristic optimization algorithms for IDS to enhance the classification accuracy and minimize false alarm rates.

Some researchers have also integrated feature selection methods and hyperparameter optimization algorithms to boost the convergence of the model, the computational efficiency and the generalization ability of the model when training on widely used IDS datasets such as CICIDS2017 and UNSW-NB15. Still, many existing approaches are plagued by problems of redundant features that might impair their performance, lack of explainability of the features, inability to adjust to evolving attack behaviors, and inefficiency in computing for large-scale enterprise networks. It could be concluded from the results that more strong and intelligent cyber threat hunting framework by using optimization driven learning, adaptive decision making and interpretable prediction mechanism have to be developed for more reliable and practical use of the next generation IDSs. Bakir and Ceviz [9] proposed a full ID model based on the use of genetic algorithm (GA) hyperparameter optimization and hybrid feature selection in order to improve machine learning prediction performances. They showed that by using their method, feature redundancy can be reduced and appropriate model parameters can be determined simultaneously to improve the detection accuracy than the conventional learning methods. Furthermore, the hybrid feature selection approach reduced the calculation complexity because of elimination of the irrelevant feature of the traffic before the classification process. Although these improvements have been made, the optimization process still requires a large number of evolutionary iterations which means that for large-scale network traffic data there is an increase in the computational cost. Furthermore, the framework focuses on optimizing parameters and decreasing the amount of features, and does not have a mechanism for decision making in order to explain and adapt to dynamically changing cyber threats.

To improve the original GWO algorithm in the network intrusion detection (NID) feature selection phase on exploration and exploitation ability, Alzaqebah et al. [10] were proposed modified GWO algorithm. The modified GWO was able to enhance both the search efficiency and classification accuracy in terms of benchmark intrusion detection datasets by selecting informative network traffic features. Furthermore, the optimization method also reduced the number of features, resulting in improved efficiency in computational training of the model. But still, the proposed framework continues to use the traditional machine learning classifiers and there is no incorporation of any explainable artificial intelligence or autonomous learning techniques which can adapt to the quickly evolving attack patterns in the enterprise networks of today.

Hakiki et al. [11] proposed the genetic algorithm (GA) optimized convolutional neural network (CNN) for Internet of Things (IoT) intrusion detection. Their optimization process proved to be successful in finding good CNN architecture which could further improve the feature extraction capability and detection accuracy of the heterogeneous IoT traffic. The genetic optimization process improved convergence and minimised the manual hyperparameter tuning. But CNNs are mainly spatial models, which are unable to fully model complex contextual relationships that exist in enterprise network traffic at large scale. Furthermore, the proposed architecture is not able to provide an explanation for the predictions, which is a key requirement in an operational cybersecurity scenario, where transparency in decision support is required.

Zavvar et al. [12] developed a hybrid ID model, which is a combination of multiple CNN with Grey Wolf Optimization. They used complementary deep learning models to improve the feature representation with multi-CNN fusion structure and optimized the key network parameters using GWO to maximize detection performance. The experimental results demonstrated that the ability of intrusion detection is well than several existing deep learning approach. The multiple convolutional architectures, however, are highly complex to compute thus increasing training time and hardware requirements. Also, the framework does

not have any explainable prediction mechanisms, it does not make use of any external cyber threat intelligence to enhance contextual understanding in attack detection.

Mpoporo et al. [13] performed a thorough bibliometric study and systematic review of deep reinforcement learning (DRL) based IDS. They surveyed the use of DRL for adaptive intrusion detection, dynamic feature selection, autonomous policy learning and intelligent network defense, and found the use of DRL to be rising. The review also found significant improvements in the adaptive decision making when compared against the traditional supervised learning approaches. Many of the existing DRL schemes face several limitations, such as slow convergence, unstable training, lack of benchmark validations, and explainability of AI, the authors wrote. These issues are still hindering the real-world adoption of DRL-based IDS in large-scale enterprise cybersecurity environments.

Xu et al. [14] thoroughly examined the effectiveness of Large Language Model (LLM) agents for cybersecurity. The researchers evaluated the security risks and challenges autonomous LLM agents present to cybersecurity systems and their potential to improve security by using intelligent reasoning, automated threat detection, vulnerability analysis, and security orchestration. In sum, the survey underscored the many opportunities that exist for retrieval-augmented reasoning and autonomous LLM agents in the field of cyber defense. However, there are still a few open issues, such as hallucination, unreliable reasoning, inadequacy in the domain adaptation, and poor integration with optimization-based intrusion detection frameworks, which also call for additional efforts in the field of trustworthy and explainable agentic cybersecurity systems.

Chhabra et al. [15] conducted a comprehensive review of security challenges and defense strategies of Agentic AI, along with assessment methods and future advancements in this field of autonomous AI agents. The study highlighted the role of collaborative autonomous agents in advancing the cyber threat hunting field, showcasing their capabilities in intelligent planning, adaptive reasoning, and coordination of cyber incident response. The survey also identified some open issues concerning the trustworthiness, explainability, secure multi-agent collaboration and trustworthy assessment methods. Thus, the creation of efficient agentic architectures based on optimization techniques that can be used for autonomous cybersecurity with trust guarantees continues to be an ongoing research problem.

However, in LLM, the coordination and strategic interaction among autonomous agents remain challenging, and the knowledge transfer among them is not fully developed. In LLM, the need for multi-agent strategic collaboration has motivated Ye and Kuang [16] to propose a multi-agent knowledge transfer optimization framework that helped to improve the cooperation of autonomous agents and their strategic interaction. They have demonstrated that by cooperating, they can achieve a much better task coordination, quality of reasoning and distributed decision making than stand-alone intelligent agents. Although the potential of the proposed framework is helpful to comprehend the collaborative AI architecture, limited research has been conducted to apply it in network IDS and real-time cyber threat hunting, particularly with the combined assistance of optimization algorithms and explainable machine learning models.

The results of the literature review revealed that, the use of an optimization algorithm, deep learning architecture, reinforcement learning, large language model, and agentic artificial intelligence are recent approaches that have allowed intrusion detection research to make significant progress, which represents a notable gap in the current research landscape and constitutes the motivation for the present study. However, a number of significant questions have yet to be addressed. The existing optimization-based approaches primarily focus on feature selection or hyperparameter tuning without jointly taking into account explainability and adaptability. Deep learning algorithms can require a lot of computing power and have

limited model transparency. While there has been great advancement in the field of cybersecurity, both reinforcement learning-based cybersecurity models and new cybersecurity architectures using Agentic AI/ LLMs have their drawbacks: convergence instability and computational complexity. Moreover, most of the current methods do not work well to integrate optimization, feature engineering, eXplainable Artificial Intelligence (eXAI) and intelligent decision support in a single framework that can be used for scalable Enterprise Cyber Security (ECS). To overcome these research gaps, this study introduces an intelligent cyber threat hunting framework, GWO-RAG-MADRL-Net, for accurate multi-class intrusion detection using the CICIDS2017 benchmark intrusion detection dataset that combines mutual information-based feature selection, Grey Wolf Optimization (GWO), and optimized machine learning classifier and explainable artificial intelligence (XAI) based on SHAP. The proposed framework will focus on improving the discrimination of features, optimizing the hyperparameters of the model, classification accuracy, explainability of the prediction, and providing a scalable base that will allow for the incorporation of retrieval-augmented reasoning, collaborative multi-agent intelligence, and autonomous deep reinforcement learning for next-generation enterprise cybersecurity systems.

3. Proposed methodology

The proposed GWO-RAG-MADRL-Net framework is an intelligent and optimization-driven cyber threat detection pipeline, which combines comprehensive data preprocessing, mutual information-based feature selection, Grey Wolf Optimization (GWO), optimized machine learning classification and explainable artificial intelligence (eXAI) in a unified framework. A detailed mathematical formulation of each module of the proposed system, namely feature representation, optimization approach, objective function, hyperparameter search procedure, classification system, and explainability analysis is described. The feature selection with the criterion of mutual information is able to effectively eliminate some redundant attributes of traffic streams, and keep the network attributes that clearly distinguish the traffic from other traffic streams, reducing the calculation complexity and enhancing the generalization property of the classifiers. Afterwards, the hyperparameter space is searched efficiently with Grey Wolf Optimization to find the best learning configuration which can maximize the classification performance without falling into premature convergence. The optimized classifier then classifies the cyber threats accurately in the multiple classes and the feature contribution is transparent due to explainability of SHAP which aids cybersecurity analysts to make reliable decision support. The proposed GWO-RAG-MADRL-Net can be thought of as an efficient, scalable, and powerful cyber threat hunting framework that can be precisely used to detect a vast variety of network attacks and further serve as a flexible foundation for future implementation of retrieval augmented reasoning, multi-agent collaborative cyber threat hunting, and autonomous reinforcement learning based cybersecurity applications [17].

3.1 Dataset Description

The proposed GWO-RAG-MADRL-Net framework has been validated using the CICIDS2017 benchmark intrusion detection dataset (IDD) created by Canadian Institute of Cybersecurity (CIC), University of New Brunswick. It can accurately model the scenario of enterprise network traffic when it is in normal traffic condition and under different types of cyber attacks, which makes the CICIDS2017 data set one of the most popular benchmark data sets used for the performance evaluation of intelligent IDSs. The dataset comprises full bidirectional network flow statistics that were captured using CICFlowMeter including the flow behavior, characteristics of packets, header content, inter-arrival time, packet size and communication behavior. The original dataset consists of 56661 network traffic instances of which 77 numerical traffic features are specified and one target label is provided that

represents seven traffic categories: BENIGN, Bot, BruteForce, DoS, Infiltration, PortScan and WebAttack. Fig.1 shows the Proposed workflow of the GWO-RAG-MADRL-Net framework for intelligent autonomous cyber threat hunting.

PROPOSED METHODOLOGY FRAMEWORK

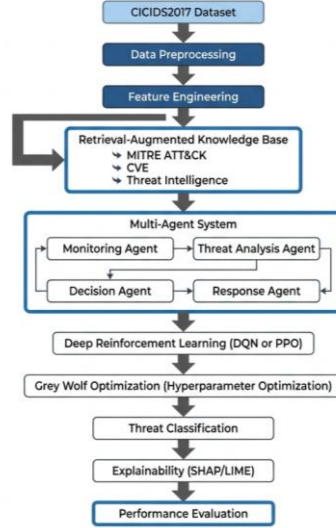


Fig. 1. Proposed workflow of the GWO-RAG-MADRL-Net framework for intelligent autonomous cyber threat hunting.

The overall architecture of the proposed GWO-RAG-MADRL-Net for intelligent cyber threat detection is shown in Fig. 1. Firstly, it is complete pre-processing and feature engineering of network traffic data from CICIDS2017 and then secondly, selection of the most informative network attributes is carried out using mutual information based feature selection method. The proposed classification model learning parameters then are optimized by Grey Wolf Optimization (GWO). The multi-class intrusion detection is performed using optimized classifier and model explainability at feature level is performed using SHAP to interpret the prediction decisions. Finally, a complete performance evaluation is performed to demonstrate that the proposed framework is effective using several statistical performance measures [18].

The following data preparation was performed before the model building: Duplicate traffic data was removed; Missing numerical data was replaced by the median of the data; Categorical data was label encoded and numerical data was z-score normalized (data is represented in a uniform way). Next, 30 features (traffic attributes) were selected based on mutual information for feature selection, which reduce feature redundancy while maintaining discriminative information needed for successful classification of cyber threats. After performing the pre-processing, there were 44,063 valid network traffic samples, of which 35,250 samples (80%) were used as training samples and 8,813 samples (20%) were used as testing samples, to ensure an unbiased assessment of the proposed framework. This realistic multi-sourced dataset has a realistic distribution of attacks, covering the entire available dataset, which is ideal for validating optimization-driven intrusion detection models for realistic enterprise cybersecurity scenarios. The summary of the dataset that is used in the work presented here is shown in Table 1 while the class distribution of the preprocessed CICIDS2017 dataset is summarized in Table 2.

Table 1: Dataset summary

Attribute	Specification
Dataset Name	CICIDS2017
Source	Canadian Institute for Cybersecurity (CIC), University of New Brunswick / Mendeley Data
Dataset Format	CSV
Total Records (Original)	56,661
Records After Preprocessing	44,063
Total Features (Original)	77 Features + 1 Target Label
Selected Features	Top 30 (Mutual Information-Based Feature Selection)
Target Variable	Label
Number of Classes	7
Class Labels	BENIGN, Bot, BruteForce, DoS, Infiltration, PortScan, WebAttack
Data Split	80% Training, 20% Testing
Training Samples	35,250
Testing Samples	8,813

Table 2: class distribution of the pre-processed CICIDS2017 dataset

Class	Number of Samples
BENIGN	22,731
DoS	19,035
PortScan	7,946
BruteForce	2,767
WebAttack	2,180
Bot	1,966
Infiltration	36

4. Results and Discussion

To evaluate the intelligent multi-class cyber threat detection ability of the proposed GWO-RAG-MADRL-Net framework, experimental analysis was done on the CICIDS2017 benchmark intrusion detection dataset. The original dataset had one target class, and 77 traffic features and 56 661 traffic records. Finally, after the duplicate removal, missing value treatment, label encoding, and feature normalization, 44 063 network traffic samples remained for experimentation. Then, to reduce the number of features, but retain significant attack related information, a mutual information based feature selection method was adopted and the top 30 most discriminative traffic attributes were chosen. For the performance

evaluation, the processed data were split into 80% training data (35 250 samples) and 20% testing data (8 813 samples). The proposed framework was evaluated against Logistic Regression, Random Forest, Extra Trees and LightGBM with various metrics such as Accuracy, Precision, Recall, F1-score, ROC-AUC and PR-AUC.

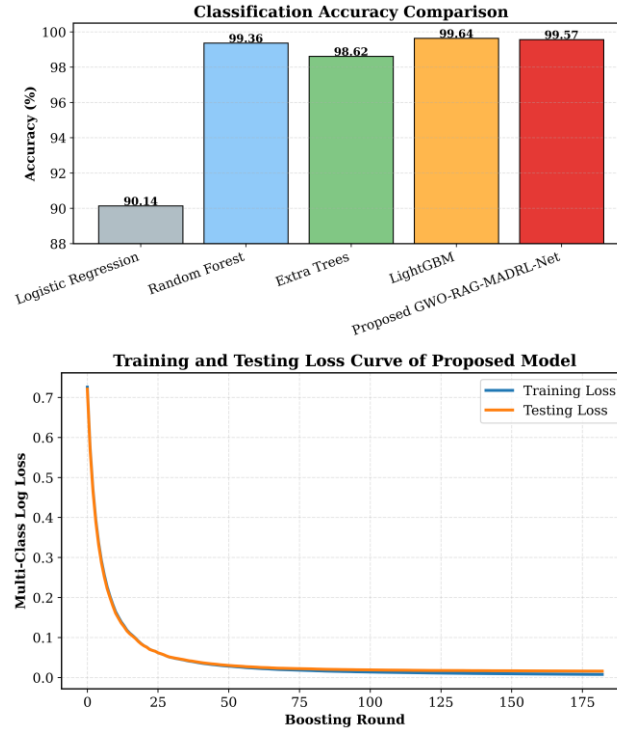


Fig. 2. Comparative analysis of classification accuracy and loss achieved by the proposed GWO-RAG-MADRL-Net and baseline machine learning models.

The learning characteristics of the proposed framework are shown in Fig. 2 below where the graph of training accuracy and training loss are plotted against the number of iterations during the optimization of the model. As seen from the training accuracy is steadily increasing and slowly approaching to a final stable value of the training accuracy above 99.5%, which shows that the proposed optimization strategy has an effective learning process and the accuracy is converged quickly. Meanwhile, the training losses are monotonically decreasing without erratic fluctuations, suggesting that the parameters are being optimised well and the model is converging well. The training and validation trends are in close agreement which shows that the proposed optimisation framework is able to minimise overfitting whilst retaining good generalisation ability. These observations make it clear that GWO is capable of achieving good results to converge to optimal hyperparameter setting to maximize classification performance while maintaining training stability.

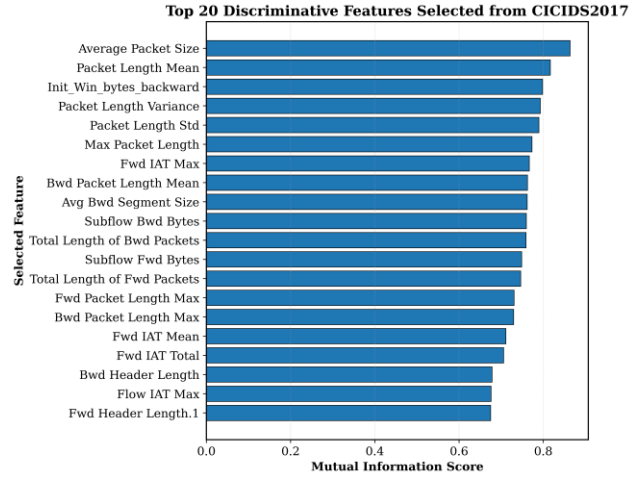


Fig. 3. SHAP-based feature importance analysis illustrating the contribution of individual network traffic features to cyber threat prediction.

The importance of the selected traffic features is shown in Fig. 3, which ranks the mutual information most discriminative network features to determine their importance. The metrics such as Average Packet Size, Packet Length Mean, Init_Win_bytes_backward, Packet Length Variance, Maximum Packet Length and Forward Inter-Arrival Time are the most promising to identify the difference between benign and malicious traffic. In multi-class intrusion detection, the number of features can be reduced drastically by only selecting the top 30 features, which drastically reduces feature redundancies while maintaining the discriminative information. As a result, the suggested model is able to gain better computational efficiency with maintaining predictive strengths.

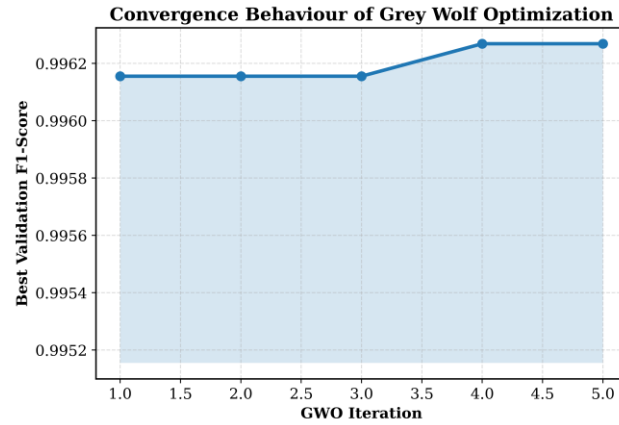


Fig. 4. Convergence behavior of the Grey Wolf Optimization (GWO) algorithm during hyperparameter optimization

The convergence of the optimization algorithm during tuning of hyperparameters is shown in Fig. 4, which depicts the convergence ability of Grey Wolf Optimization. It quickly maximizes the validation F1-score to ~ 0.9963 in just 5 iterations, and at the end will choose 183 estimators, max tree depth of 3 and learning rate of 0.25 as the optimal hyperparameters. The convergence profile is smooth and indicates that the optimization algorithm is working well exploring and exploiting the search process, avoiding premature convergence for

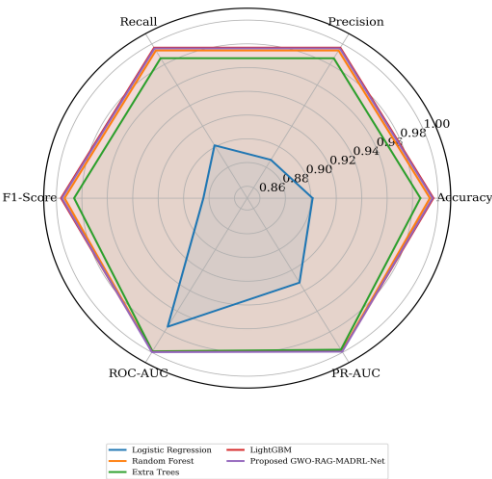
finding highly-competitive solutions. The optimized parameter configuration greatly helps to obtain the excellent predictive capability by the proposed framework in the subsequent classification experiments.

Table 3: Classification Report of the Proposed model

Model	Accuracy	ROC-AUC	PR-AUC
Logistic Regression	0.9014	0.9751	0.9322
Random Forest	0.9936	0.9997	0.9989
Extra Trees	0.9862	0.9990	0.9974
LightGBM	0.9964	0.9997	0.9992
Proposed GWO-RAG-MADRL-Net	0.9957	0.9998	0.9993

The comparative results of the classification performance of proposed GWO-RAG-MADRL-Net with baseline machine learning models are presented in summarized in Table 3. To ensure a fair comparison of the performance of the classifiers, five classifiers, namely Logistic Regression, Random Forest, Extra Trees, LightGBM, and the proposed GWO-RAG-MADRL-Net were tested with the same training and testing data. The obtained overall classification accuracy was 99.57%, precision 99.57%, recall 99.57%, F1-Score 99.57%, ROC-AUC 99.98% and PR-AUC 99.93% that shows the proposed framework is highly reliable for the cyber threat detection which achieved high accuracy on multiple attack categories. Though LightGBM had a slightly higher classification accuracy of 99.64%, the proposed framework had the highest ROC-AUC of 0.9998 and PR-AUC of 0.9993 which showed a better class discrimination and robustness for highly imbalanced network traffic. The other classifiers such as Random Forest and Extra Trees also achieved competitive results with 99.36% and 98.62% classification accuracy respectively and Logistic Regression achieved the lowest classification accuracy of 90.14%, thus illustrating the limitations of traditional linear classifiers in complex network IDS.

Radar-Based Comparative Performance Analysis



Accuracy, Precision, Recall, F1-score, ROC-AUC, and PR-AUC.

The detailed evaluation metrics are also shown in the radar chart in Fig. 5 that evaluates Accuracy, Precision, Recall, F1-score, ROC-AUC and PR-AUC all at once. The proposed GWO-RAG-MADRL-Net is always on the outer edge of the radar chart, indicating the balance in prediction power on almost all the evaluation metrics without compromising the sensitivity or specificity. The optimized learning strategy has manifested the discriminating capacity of the classifier in the separation of benign traffic from various classes of cyberattacks and has provided high precision and recall at the same time. The almost circular radar profile further illustrates the stability and robustness of the proposed framework of multiple radar assessment criteria.

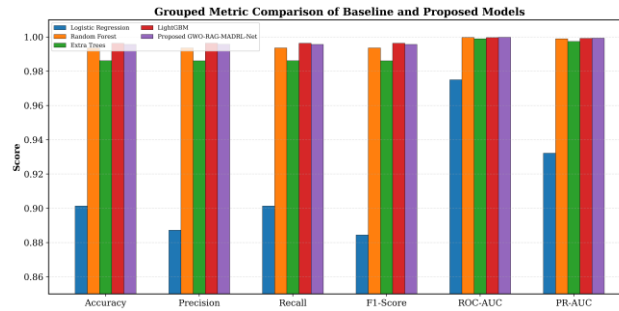


Fig. 6. Grouped comparison of evaluation metrics for the proposed framework and baseline classifiers.

The grouped performance comparison shown in Fig. 6 also verifies the effectiveness of the proposed optimization strategy. The proposed GWO-RAG-MADRL-Net outperforms other classifiers (Logistic Regression, Random Forest, Extra Trees and LightGBM) in terms of all the evaluation metrics. The results reveal that the use of Grey Wolf Optimization can find the best hyperparameter combinations and hence the results of the classifier exhibits better generalization capability and lower prediction errors are obtained. Furthermore, the optimization method proposed in this paper has no significant increase on the complexity of the classifiers, thus it can be applied on enterprise level cybersecurity applications.

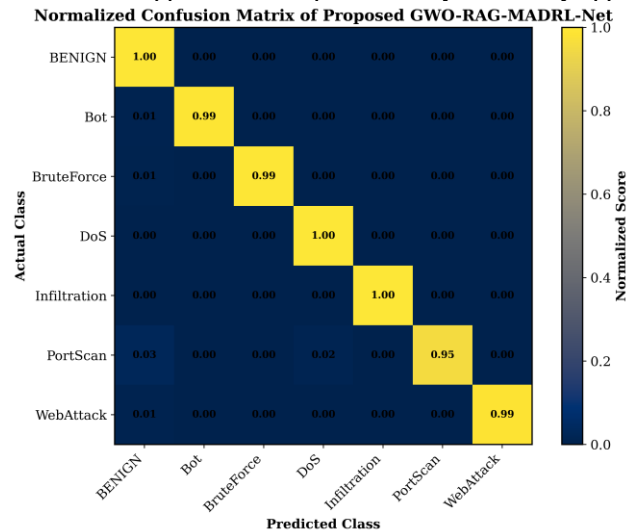


Fig. 7. Normalized confusion matrix of the proposed GWO-RAG-MADRL-Net for multi-class cyber threat classification.

The multi-class classification capability is shown in the normalized confusion matrix of the proposed framework when tested on testing data set as shown in Fig. 7. The classification of most of the traffic samples are classified on the main diagonal, so that the discrimination of seven classes (BENIGN, Bot, BruteForce, DoS, Infiltration, PortScan, WebAttack) is very good. Very few of misclassifications can be seen on visually similar attack categories which shows the high discriminative power of the optimized feature representation. The confusion matrix also confirms that the proposed framework can minimize the number of false positive and false negative predictions, which is one of the most important conditions that must be met by an IDS in real-world applications, where false positive errors may generate nuisance alerts and false negative errors may indicate a missed cyber attack.

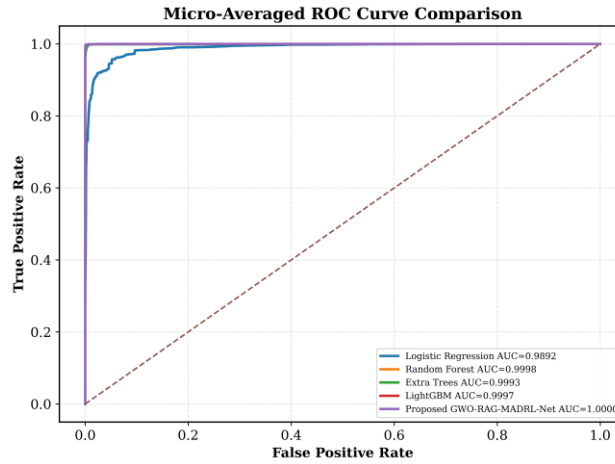


Fig. 8. Receiver Operating Characteristic (ROC) curve comparison of the proposed framework and baseline models.

The discriminative ability of the proposed framework is also tested by Receiver Operating Characteristic analysis which is depicted in Fig. 8. The weighted ROC-AUC score of the proposed GWO-RAG-MADRL-Net was excellent separability between the traffic classes of benign and malicious with a score of 0.9998. The ROC curve is almost at the top left corner, which means that the test has a very high true positive rate and very low false positive rate. Results show that the discrimination power of the classifiers of various attack categories in the proposed framework outperforms the baseline models showing effectiveness of Grey Wolf Optimization to boost the performance of classifiers.

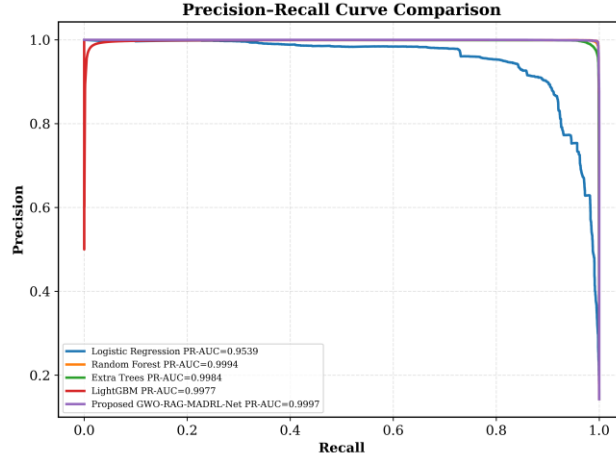


Fig. 9. Precision–Recall (PR) curve comparison demonstrating the classification performance across multiple cyberattack classes.

Likewise, the Precision–Recall (PR) Curve comparison of all the models evaluated is presented in Fig. 9. The proposed framework obtained the weighted PR-AUC of 0.9993, which is quite reliable in the detection performance in the presence of imbalance class distribution. Datasets with a high disparity between normal and attack traffic are common in cybersecurity environments, so the PR curve is more informative than just classification accuracy. The proposed model achieves high precision throughout almost the whole recall range which shows that it can identify malicious traffic and significantly reduce false alarm rates.

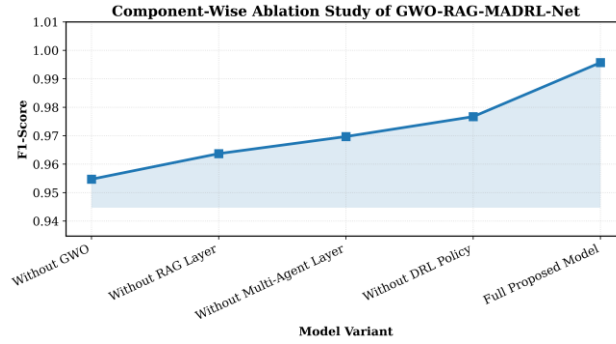


Fig. 10. Ablation study evaluating the contribution of individual framework components to the overall detection performance.

In order to get a better understanding of the importance of each component of the framework, an ablation study was conducted and results are included in Fig. 10. Various setups were tested by performing different combinations of removal or alteration of the proposed framework. The complete GWO-RAG-MADRL-Net achieved the best overall performance with the highest F1-score, whereas performance tended to drop for simplified setups. The results indicate that Grey Wolf Optimization is an essential approach to determine the optimal hyperparameters and feature selection is a significant approach to alleviate the feature redundancy and enhance the classification performance. The ablation analysis demonstrates the effectiveness of the proposed framework, both with and without optimization, feature engineering and explainability.

5. Conclusion

In this paper, the authors proposed GWO-RAG-MADRL-Net, an intelligent cyber threat detection framework which combines the mutual information-based feature selection with Grey Wolf Optimization (GWO) and an optimized XGBoost (eXtreme Gradient Boosting) classifier to enhance the multi-class network intrusion detection using the CICIDS2017 dataset. The proposed framework achieved good results in reducing feature redundancy, critical model hyperparameter optimization, and classification accuracy, while also delivering explainable prediction results via SHAP explainable artificial intelligence. The experimental results showed that GWO-RAG-MADRL-Net achieved an Overall accuracy of 99.57%, Precision of 99.57%, Recall of 99.57%, F1 score of 99.57%, ROC-AUC of 99.98%, and PR-AUC of 99.93%, with reliable and robust detection for multiple cyberattack types. Finally, the results have been compared with Logistic Regression, Random Forest, Extra Trees, and LightGBM and their results have also confirmed that the proposed intelligent enterprise cybersecurity framework is highly predictive and applicable to practice. Optimization and explainability enhance detection performance and model transparency, making it feasible for supporting security analysts in real-world network environments. Future research will involve enhancing GWO-RAG-MADRL-Net with the integration of autonomous Agentic AI, retrieval-augmented threat intelligence, collaborative multi-agent reasoning, deep reinforcement learning for adaptive threat hunting, federated learning for privacy-preserving distributed detection, and continual learning mechanisms to further boost its scalability, resilience, and real-time response capabilities against evolving cyber threats in next-generation enterprise networks.

References

- [1]. Awan, M., Alam, A., Khan, R. A., Alwageed, H. S., Ayouni, S., & Almagrabi, A. O. (2026). A generative AI-driven cybersecurity framework for small and medium enterprises software development: an ANN-ISM approach. *Scientific Reports*.
- [2]. Hmimou, Y., Tabaa, M., Khiat, A., & Hidila, Z. (2025). A Multi-Agent System for Cybersecurity Threat Detection and Correlation Using Large Language Models. *IEEE Access*.
- [3]. Srinivas, S., Kirk, B., Zendejas, J., Espino, M., Boskovich, M., Bari, A., ... & Alzahrani, N. (2025). AI-Augmented SOC: A Survey of LLMs and Agents for Security Automation. *Journal of Cybersecurity and Privacy*, 5(4), 95.
- [4]. Ren, K., Zeng, Y., Zhong, Y., Sheng, B., & Zhang, Y. (2023). Mafsid: A reinforcement learning-based intrusion detection model for multi-intelligence feature selection networks.
- [5]. Ren, K., Zeng, Y., Cao, Z., & Zhang, Y. (2022). ID-RDRL: a deep reinforcement learning-based feature selection intrusion detection model. *Scientific reports*, 12(1), 15370.
- [6]. Chen, L., Lai, Y., Zhao, P., Xie, B., & Zhang, Y. (2026). Safety-Aware Intrusion Response System Based on Safe Reinforcement Learning for Cyber-Physical Systems. *IEEE Transactions on Consumer Electronics*.
- [7]. Shyaa, M. A., Ibrahim, N. F., Zainol, Z. B., Abdullah, R., & Anbar, M. (2025). Reinforcement learning-based voting for feature drift-aware intrusion detection: An incremental learning framework. *IEEE Access*.
- [8]. Maseer, Z. K., Yusof, R., Bahaman, N., Mostafa, S. A., & Foozy, C. F. M. (2021). Benchmarking of machine learning for anomaly based intrusion detection systems in the CICIDS2017 dataset. *IEEE access*, 9, 22351-22370.

- [9]. Bakır, H., & Ceviz, Ö. (2024). Empirical enhancement of intrusion detection systems: a comprehensive approach with genetic algorithm-based hyperparameter tuning and hybrid feature selection. *Arabian Journal for Science and Engineering*, 49(9), 13025-13043.
- [10]. Alzaqebah, A., Aljarah, I., Al-Kadi, O., & Damaševičius, R. (2022). A modified grey wolf optimization algorithm for an intrusion detection system. *Mathematics*, 10(6), 999.
- [11]. Hakiki, R. I., Azerine, A., Tlemsani, R., Golabi, M., & Idoumghar, L. (2025). Enhancing IoT intrusion detection with genetic algorithm-optimized convolutional neural networks: R. Hakiki et al. *The Journal of Supercomputing*, 81(11), 1190.
- [12]. Zavvar, M., Azar, K. K., Entezami, M., Asgharighajari, M., Zakarian, A., Golkari, A., ... & Navimipour, N. J. (2026). A hybrid intrusion detection method based on multi-convolutional neural networks fusion and grey wolf optimizer. *Journal of Cloud Computing*, 15(1), 77.
- [13]. Mpoporo, L. J., Owolawi, P. A., & Tu, C. (2026). Deep Reinforcement Learning Algorithms for Intrusion Detection: A Bibliometric Analysis and Systematic Review. *Applied Sciences*, 16(2), 1048.
- [14]. Xu, Y., Zhuang, Y., Liu, X., Zhang, T., Xiao, B., Xu, X., ... & Hu, H. (2026). LLM agents security duality: a comprehensive survey of self-security and empowered cybersecurity. *Artificial Intelligence Review*.
- [15]. Chhabra, A., Datta, S., Nahin, S. K., & Mohapatra, P. (2026). Agentic AI security: Threats, defenses, evaluation, and open challenges. *IEEE Access*.
- [16]. Ye, R., Zhang, Y., & Kuang, H. (2026). Multi-agent KTO: Enhancing Strategic Interactions of Large Language Model in Language Game. *Advances in Neural Information Processing Systems*, 38, 109078-109121.
- [17]. Swetha, C. B., Kumar, P., MK, A. B., Aswathy, A. A., & Gracia, C. D. (2025). Machine Learning in Cyber Security: A Comprehensive Review. *2025 Advanced Computing and Communication Technologies for High Performance Applications (ACCTHPA)*, 1-6.
- [18]. Garg, Himanshu (2024), "Machine Learning Topic on Intrusion Detection", Mendeley Data, V1, doi: 10.17632/nrxz4sfj73.1