

A novel DDoS detection framework leveraging hybrid binary grey wolf optimization and explainable AI

Jyoti Mante *

Kishor Kolhe [†]

Department of Computer Engineering and Technology

Dr. Vishwanath Karad MIT World Peace University

Pune 411038

Maharashtra

India

Abstract

As the number of devices connected are more in the Internet of Things (IoT), these devices create different data sharing, which leads to security and privacy issues. Current IoT cybersecurity solutions often lack accuracy, learning difficulties, and inaccurate costs. A novel DDoS attack detection framework is proposed based on hybrid binary grey wolf optimization (BGWO) metaheuristic algorithm and SHAP to solve these problems. A hybrid model of SHAP-BGWO is proposed to optimize feature selection. Machine learning tree classifiers are used to evaluate the performance on Bot-IoT dataset. The results of the above data, including accuracy, demonstrate the effectiveness of our SHAP-BGWO based framework in predicting DDoS attacks on IoT systems, providing solutions to improve IoT security. SHAP is combined with BGWO to achieve 99+% accuracy using AdaBoost, Random Forest and decision tree respectively.

Subject Classification: 68T05, 92B20.

Keywords: SHAP, BGWO, SMOTE, DDoS, Random forest, Decision tree, Mathews correlation coefficient.

1. Introduction

IoT-enabled networks facilitate connecting diverse devices, allowing them to communicate and share data seamlessly. These networks enable everyday objects to communicate and collaborate on tasks, enhancing

* E-mail: jyoti.kharpade@mitwpu.edu.in (Corresponding Author)

[†] E-mail: kishor.kolhe@mitwpu.edu.in

efficiency and convenience in various sectors like healthcare, industry, transportation, and agriculture [1]. The goal of IoT-enabled networks is to enhance the quality of life by addressing everyday challenges and enhancing overall productivity [2]. These networks facilitate seamless connectivity and data exchange among devices, fostering innovation and enabling new applications and services. By integrating intelligent technology into common objects, IoT-enabled networks pave the way for a more interconnected and efficient world [3]. In recent years' cyber threats have increased in the IoT environment. The most common are DDoS and DoS [4]. DDoS attacks use many hijacked devices [5] from different places to attack together, while DoS attacks come from one source. These attacks can cause serious damage, so it is crucial to have strong defenses and plans to protect against them. This research looks into how DDoS and DoS attacks work, their effects, and ways to stop them, to keep networks safe and services running smoothly [6]. An IDS serves as a valuable tool for analyzing and looking after potentially suspicious activities within a network [7]. It acts as an additional layer of defense, particularly useful when encryption methods fail to secure the network. Intrusion implies any harmful action that threatens sensor nodes. The IDS using machine learning [8] examines machine and user behavior, identifies known intrusion patterns, and detects potentially harmful network activity [9].

2. Literature Survey

In [2], this research article proposed pigeon-inspired optimization (PIO) for selecting features and included one-class classifiers such as OC-SVM, iForest, and LOF. In [9], this research article on Binary Grey Wolf Optimization for Feature Selection used eighteen distinct datasets. Two binary approaches (bGWO1 and bGWO2) were contrasted with Particle Swarm Optimization and Genetic Algorithm. In [10,11], this research article used the UNSW-NB15 dataset and used a technique called GSGW-DT for best feature selection. In [12], the research article used NSGA-II-based techniques along with PCC, Chi2 and PCC to select features, aiming for better accuracy. Support Vector Machine gives accuracy of 99.48%. In [13], this research article applied Genetic-based Enhanced Grey Wolf Algorithm (GB-EGWO) on NSL-KDD to pick out the most important features. Specifically, when tested on the NSL-KDD

dataset, the GB-EGWO algorithm achieved 98.622% accuracy. In [14], this research article proposed combining a modified version of the binary Grey Wolf Optimization (GWO) with Particle Swarm Optimization (PSO) for feature selection. NSL-KDD99 and UNSW-NB15 were used for evaluation using different metrics. In [15], this research article focuses on improving intrusion detection systems (IDS) by combining the Grey Wolf Optimization (GWO) algorithm with Extreme Learning Machine (ELM). Model was tested on the UNSW-NB15 dataset. The combined method achieved an accuracy of 81%. In [16], this research article aimed to improve network intrusion detection using Grey Wolf Optimization (GWO) algorithm. Using the KDD CUP 99 dataset, researchers used GWO to choose important features, reducing the dataset's size. By using classifiers like KNN, SVM, and GRNN, they achieved a 75.80% accuracy.

In [17], this research article combined CGWO and One-Class Support Vector Machine (OC-SVM) classifiers without using any Feature Selection (FS) technique on the Scada dataset. The results showed high accuracy, with 95.76% and 95.82%. In [18], this research article focused on detecting intrusions using key features selected through GWO, Information Gain, and Principal Component Analysis (PCA). They achieved an accuracy of 99.5%. In [19], this research article used correlation, principal component analysis (PCA), and mutual information-based feature selection, along with support vector machines (SVM). An accuracy of 99.85% was achieved, better than other feature selection techniques. In [20], this research article compared different methods like Genetic Algorithm, BGWO1 and BGWO2, Binary Particle Swarm Optimization and Competitive Binary Grey Wolf Optimizer. CBGWO gives the best solution as compared to the other algorithms proposed.

In [7, 21], this research article used the NSL-KDD dataset and Grey Wolf Optimization (GWO) for choosing important features. The study demonstrated that their GWO-based method surpassed other feature selection techniques such as Particle Swarm Optimization (PSO), Genetic Algorithm (GA), and Ant Colony Optimization (ACO) in both classification and feature selection. In [3, 6, 22], this research article addresses the growing challenges in healthcare as IoMT advances. Using PCA and correlation coefficient, the research proposes a hybrid PCA-GWO technique and a deep neural network (DNN) classifier, achieving 99.37% accuracy. In [23], this research article uses Binary Grey Wolf Optimizer

(BGWO) to select important features and Naive Bayes (NB) to classify them. This hybrid BGWO-NB model achieved an impressive accuracy of 99.15%. In [24], this research article utilizes ensemble methods including Random Forests, XGBoost, CNNs, enhancing anomaly detection in IoT networks. Leveraging PSO and hybrid algorithms, it achieves 93.75% accuracy. In [25], this research article utilizes the UNSW-NB15 dataset, intrusion detection in IoT was explored using Particle Swarm Optimization (PSO) and Exclusive Feature Bundling (EFB). Incorporating Binary PSO and Genetic Algorithm, alongside Support Vector Machine (LSSVM) and One-class SVM (OCSVM) classifiers, achieved 70.51% accuracy. In [26], this research article proposes metaheuristic based feature selection using genetics algorithm on Bot-IoT dataset with the highest accuracy of 99.98% using DT classifier.

In this paper, a DDoS attack detection framework in IoT network traffic with optimal number of features, high accuracy, and low false positives is proposed. The key contributions include:

- Proposed a two-layer framework for efficient distributed denial of service attack detection in Internet of things networks.
- A feature selection framework based on metaheuristic methods, incorporating SHAP and BGWO techniques, is proposed.
- The proposed DDoS attack detection framework performance is assessed using machine learning classifiers on Bot-IoT dataset and is evaluated using metrics accuracy (ACC), precision (PR), Recall, f1 score.

3. Preliminaries

This section gives a detailed explanation of *SHapley Additive exPlanations*(SHAP) and Binary Grey Wolf Optimisation (BGWO) metaheuristic algorithm based feature selection technique.

A. *SHapley Additive exPlanations* (SHAP):

Explainable AI (XAI): Explainable AI infers to processes and techniques in artificial intelligence (AI) that make the outcomes of AI models more human understandable.

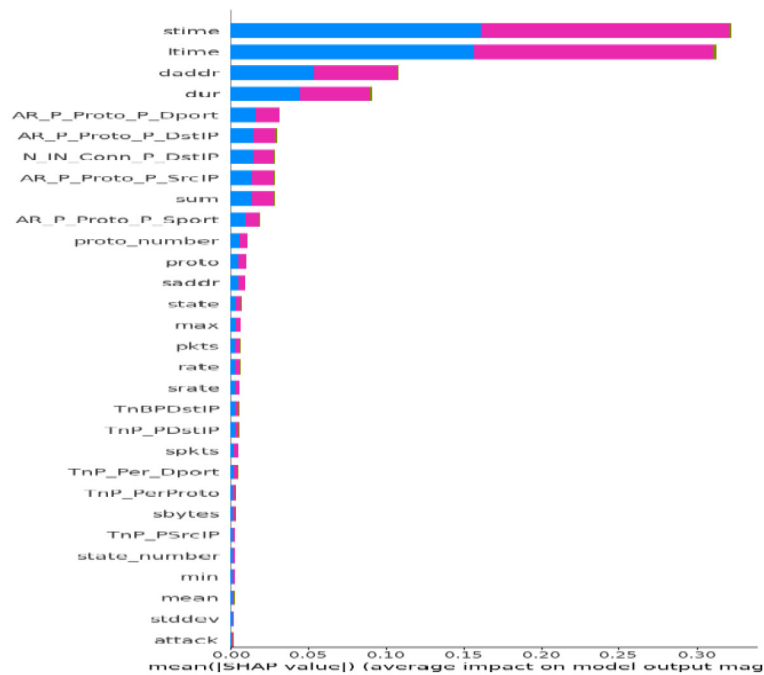


Figure 1

Feature importance by SHAP value on BoT-IoT dataset

SHAPLEY values [27, 28] provide a way to measure the contribution of every feature to the outcome of a particular instance, offering detailed insights into how every feature contributes, positively or negatively, to finding the final prediction. The summary plot in Fig. 1 presents the average impact of each feature on the prediction of the BoT-IoT dataset using Random Forest model. This summary plot gives a global explanation of this model. The Y-axis displays the names of the features in descending order of contribution. The SHAP values mean absolute values from the X-axis.

B. Binary Grey Wolf Optimization (GWO) Algorithm

Binary Grey Wolf Optimization (BGWO) is a metaheuristic algorithm inspired by the hunting and social behavior of grey wolves. It incorporates swarm intelligence principles and classifies wolves into [29] four distinct ranks: alpha (α), beta (β), delta (δ), and omega (ω). The alpha wolf leads the pack, beta wolf, who acts as the second-in-command, assists in decision-

making, delta wolf obeys both the alpha and beta wolves and plays supporting role, omega wolves, who, despite their lower status, play a vital role in maintaining the pack's social harmony.

A. Encircling the Prey

Encircling the prey is represented by equations (1) and (2) which represent the swarming behavior around the target.

$$B = |C' \cdot Y_{prey}(t) - Y_{wolf}(t)| \quad (1)$$

$$Y_{wolf}(t+1) = Y_{prey}(t) - A' \cdot B \quad (2)$$

The coefficients A' and C' are calculated using equations (3) and (4)

$$A' = 2 \cdot \alpha \cdot rand_1 - \alpha \quad (3)$$

$$C' = 2 \cdot rand_2 \quad (4)$$

where $rand_1, rand_2 \in [0 \text{ to } 1]$

B. Hunting Stage

The location of prey is mathematically represented as follows:

$$Y_{wolf}(t+1) = \frac{Y_\alpha + Y_\beta + Y_\delta}{3} \quad (5)$$

Here, are the positions of alpha, beta & delta wolves represented by:

$$Y_i = X_i - A' \cdot D_i \quad i \in \{\alpha, \beta, \delta\} \quad (6)$$

D is calculated as :

$$D_i = |C' \cdot X_i - Y_{wolf}| \quad (7)$$

C. Attacking Prey Stage

The parameter α gradually decreases from 2 to 0 across the iterations as shown

$$\alpha = 2 - t \left(\frac{2}{TotalLoops} \right) \quad (8)$$

where t is within $[-1,1]$, the wolves focus on exploitation (when $A' < 1$ and $C' < 1$).

D. Search Stage

In the Binary Grey Wolf Optimizer (BGWO) algorithm, the exploration and exploitation process are governed by the strategic movements of the wolves towards their prey, guided by the wolves α , β , and δ . Exploration is enhanced when the random coefficient A' deviates from the range $[-1,1]$. While the coefficient C' , which varies between 0 and 2, thus encouraging randomness in their search behavior to avoid local optima. The binary version equations [11] of grey wolf as follow (Emary, E. et al., 2016):

$$x_1^{ds} = \{1 \text{ if } (x_\alpha^{ds} + y \text{ step}_\alpha^{ds}) \geq 1 \quad 0 \text{ otherwise} \quad (9)$$

where x_i^{ds} is the position of $\{\alpha, \beta, \delta\}$ ds is the dimension of search space, and $y \text{ step}_\alpha^{ds}$ represents the binary step that can be expressed :

$$y \text{ step}_\alpha^{ds} = \{1 \text{ if } z \text{ step}_\alpha^{ds} \geq rand \quad 0 \text{ otherwise} \quad (10)$$

where $rand$ in between, and $z \text{ step}_\alpha^{ds}$ denotes the continuous valued step size that can be calculated as in equation (11).

$$z \text{ step}_\alpha^{ds} = \frac{1}{1 + e^{-10(A_1^{ds} D_\alpha^{ds} - 0.5)}} \quad (11)$$

The updated binary position in the BGWO iteration is as shown in the equation below:

$$X_{ds}^{t+1} = \{1 \text{ if } S\left(\frac{X_1 + X_2 + X_3}{3}\right) \geq rand \quad 0 \text{ otherwise} \quad (12)$$

where sigmoid function is:

$$S(x) = \frac{1}{1 + e^{-10(x-0.5)}} \quad (13)$$

$$\text{Fitness} = \alpha * P + \beta * \frac{N-L}{N} \quad (14)$$

Where the classification accuracy is P , the length of selected attribute subset is L , the total number of attributes in the data is N . The weight of classification accuracy is α and attribute selection quality is β where $\alpha \in [0,1]$ and $\beta = 1 - \alpha$.

BGWO serves as the methodology for scoring the attribute landscape, seeking to optimize the criteria for evaluating attributes as specified in equation (14), with the Naive Bayes (NB) algorithm functioning as the classifier.

4. Proposed Methodology

This research focuses on feature selection for DDoS attack detection using BoT-IoT dataset to enhance model accuracy and computational efficiency by eliminating redundant or irrelevant features using 2 Layer Feature Selection Framework, in which the first layer employs SHapley Additive exPlanations (SHAP) for initial ranking and the second layer having optimization algorithms: Binary Grey Wolf Optimization Algorithm (BGWO) to generate final selected feature subsets.

A. Data Preprocessing

This paper removes specific features such as ‘subcategory’ and ‘pkseqid’ after label encoding, with the ‘pkseqid’ being an index type, as they do not contribute towards the prediction of type of attack[10].The dataset originally contains more than 72,000,000 records, and in this paper, it is strategically sampled to extract 2.3Lakhs samples using k-means++ clustering [30].K-means clustering algorithms partition data points into k clusters, utilizing various distance metrics such as Euclidean, Manhattan, or Mahalanobis distances[31][32][33].The categorical features undergo label encoding, transforming them into a format required for machine learning algorithms. Standard Scalar is used to standardize the dataset. The synthetic instances of the minority class (Class: “Normal”) are generated by SMOTE technique by balancing the distribution of data points. The minority class, i.e, “Normal”, originally contained 381 samples which were then increased to 77183.

B. Proposed Feature Selection Framework

The Proposed Framework is divided into two layers. The input feature subset contains 43 features which are passed to Layer 1. The Entire Proposed Feature Selection Framework is demonstrated in Fig 2. Layer 1 comprises SHapley Additive exPlanations (SHAP) which is an Explainable-AI algorithm which determines the importance of each feature. Within this process, SHAP selects 30 features (Feature Subset 1) from the initial set of 43 features, based on their importance. These selected features i.e. Feature Subset 1 is then passed to the Second Layer of the proposed framework. Layer 2 comprises the prominent feature selection algorithm Binary Grey Wolf Optimization Algorithm [BGWO]. BGWO take Feature Subset 1 as the input Feature subset and return Selected

Feature Subset 2. The Feature Subset 2 SHAP-BGWO obtained from BGWO contains a total of 7 Features.

This Final Feature Subset is then evaluated using various Machine Learning Classifiers with a training split of 80% and testing split of 20% and cross validation.

C. DDoS Attack Detection in IoT networks using Machine Learning (ML) Algorithms

After feature selection machine learning classifiers are used for DDoS attack detection. Machine Learning classifiers used are *Decision Tree (DT)*, *Random Forest (RF)*, *Logistic Regression (LR)*, *AdaBoost (ADA)*, *XG-Boost (XGB)*, *K-Nearest Neighbours (KNN)*, *Support Vector Machine (SVM)*

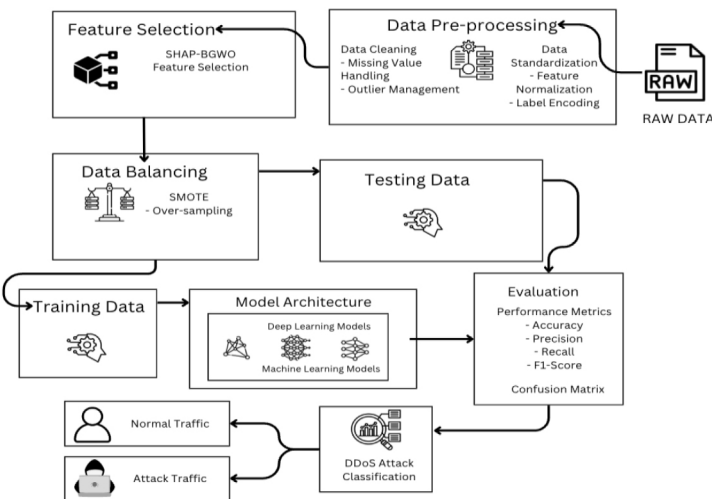


Figure 2

Proposed Work Flow of the DDoS attack Detection

5. Results and Discussion

The experiments are conducted for the Proposed Feature Selection using the hybrid SHAP-BGWO method on BOT-IoT dataset.

Dataset Description

The dataset that was utilized is BOT-IoT [34] which is used for research purposes and has a big collection of data. It includes samples of DoS , DDoS attack samples and normal samples of network traffic. We have

used 5% of the BOT-IoT dataset consisting of 36,00000 records with 7 types of attacks. The dataset is filtered for DDoS, DOS and Normal attack type instances. Originally there are 47 features in the dataset.

Evaluation Metrics

The evaluation metrics used are Accuracy (ACC), Precision (PR), Recall (RE), F1-Score and the Matthews Correlation Coefficient (MCC).

Results

This paper assesses the performance of features selected using SHAP-BGWO. Fig. 3 shows the accuracies obtained by Feature Subset 2. RF followed by DT and XGBoost achieves accuracy 99.9, 99.89, 99.86 respectively.

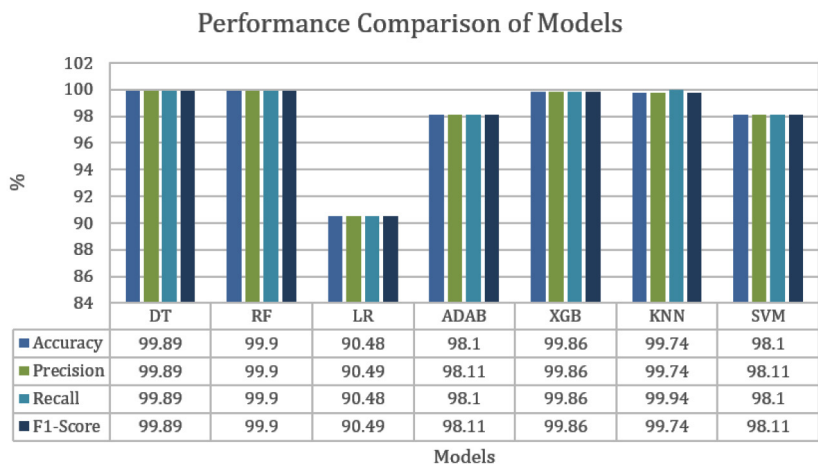


Figure 3
Comparison of Various Metrics obtained by ML Models on Feature Subset 2

The Matthews correlation coefficient (MCC) is a performance measurement for classification models that accounts for the model's accuracy by considering true positives, true negatives, false positives, and false negatives. Fig 4. shows the MCC values for machine learning models. RF, DT and XGB shows good values for MCC. All models assessing features selected by SHAPE-BGWO consistently achieve an MCC greater than 0.8, demonstrating their ability to accurately predict outcomes.

The persistent high recall scores observed across models for SHAP-BGWO selected features signify the models’ strong capacity to effectively capture a substantial proportion of positive instances within the dataset. This research also has attained F1 scores surpassing 0.8 for features selected by SHAP-BGWO. Such outcomes underscore the models’ adeptness in mitigating both false positives and false negatives, affirming their reliability across diverse datasets and enhancing their applicability with real-world scenarios.

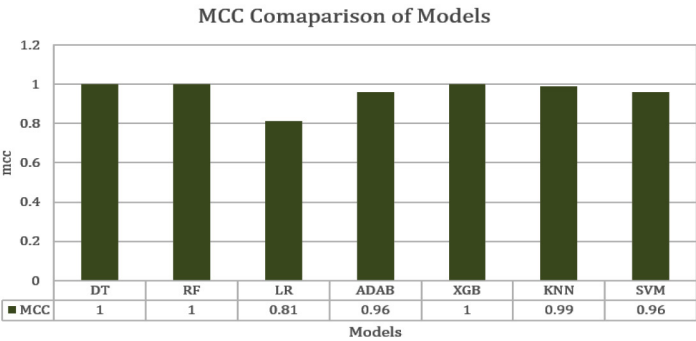


Figure 4

MCC for ML models on Feature Subset 2

This research work also achieves higher precision values for SHAP-BGWO selected features; these results signify the models’ capability to make fewer false positive predictions, enhancing their accuracy in identifying positive instances. This is particularly advantageous as it reduces the chances of misclassifying negative instances as positive, thus

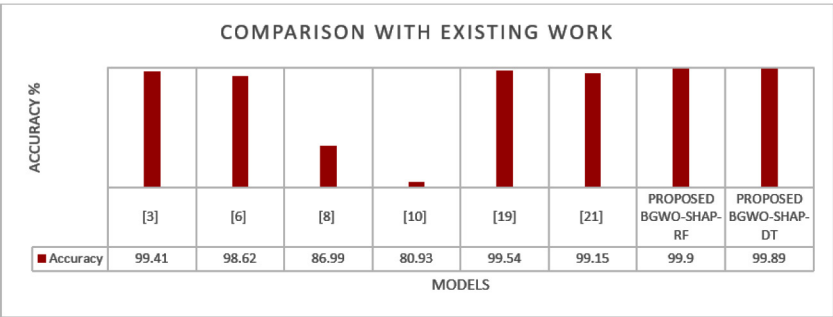


Figure 5

Comparison of Results obtained by Feature Subset 2 with the other State of Art Frameworks

increasing the reliability of the models' positive predictions. It can be observed from the Fig. 5 that the proposed model surpasses the existing models with RF giving accuracy of 99.9% and DT giving accuracy of 99.89% with high detection rate.

The proposed framework performs better than the other frameworks, as shown in Fig. 5 which is evaluated using the Features Selected by SHAP-BGWO. Comparing the Proposed Framework with the existing state of art work, it achieves better accuracies with various ML Models.

6. Conclusion

This study suggests a feature selection framework that combines SHAP with metaheuristic feature selection method BGWO to reduce the amount of features in the dataset and increase the accuracy of the classification against DOS and DDOS assaults. The reduced feature subset is found in the first step by applying the SHAP Feature Importance. In the second phase of creating a hybrid framework, the BGWO algorithm get the reduced feature subset as input. The classification of DOS and DDOS attacks is done using Machine Learning Classifiers like Decision Tree, Random Forest, Linear Regression, AdaBoost, XGBoost, Support Vector Machine, & K-Nearest Neighbors The performance of the machine learning classifiers is assessed using the BOT-IOT Dataset. Results are compared with the State of Art DOS & DDOS Attack Detection Techniques. Overall the proposed Random Forest Machine Learning Model when evaluated for Feature Subset selected by SHAP-BGWO outperforms all the other models exhibiting an accuracy of 99.9% respectively whereas DT, RF, AdaBoost, XG-Boost & KNN Machine Learning Models having accuracies 100% each.

In future we plan to extend the work by changing transfer functions of BGWO and also implementing and evaluating SHAP-PSO algorithms on different IOT Datasets by generating test samples using generative adversarial networks.

References

- [1] S. Fraihat, S. Makhadmeh, M. Awad, M. A. Al-Betar, and A. Al-Redhaei, "Intrusion detection system for large-scale IoT NetFlow networks using machine learning with modified Arithmetic Optimization Algorithm," *Internet Things*, vol. 22, p. 100819 (2023).

- [2] A. Almomani, M. Alweshah, S. Al Khalayleh, M. Al-Refai, and R. Qashi, "Metaheuristic algorithms-based feature selection approach for intrusion detection," *ResearchGate* (2019). [Online]. Available: <https://www.researchgate.net/publication/331182093>. [Accessed: Mar. 11, 2025].
- [3] S. Nandy, M. Adhikari, M. A. Khan, V. G. Menon, and S. Verma, "An intrusion detection mechanism for secured IoMT framework based on swarm-neural network," *IEEE J. Biomed. Health Informatics*, vol. 26, no. 5, pp. 1969–1976, May (2022). doi: 10.1109/JBHI.2021.3101686.
- [4] H. Liu and B. Lang, "Machine learning and deep learning methods for intrusion detection systems: A survey," *Appl. Sci.*, vol. 9, no. 20, p. 4396 (2019). doi: 10.3390/app9204396.
- [5] S. Kumar, S. V. N. Selvi, and A. Kannan, "A comprehensive survey on machine learning-based intrusion detection systems for secure communication in the internet of things," *Comput. Intell. Neurosci.*, vol. 2023, p. 8981988 (2023).
- [6] M. Usman, M. A. Jan, X. He, and J. Chen, "P2DCA: A privacy-preserving-based data collection and analysis framework for IoMT applications," *IEEE J. Sel. Areas Commun.*, vol. 37, no. 6, pp. 1222–1230, Jun. (2019). doi: 10.1109/JSAC.2019.290434.
- [7] J. J. Kponyo, J. O. Agyemang, G. S. Klogo, and J. O. Boateng, "Light-weight and host-based denial of service (DoS) detection and defense mechanism for resource-constrained IoT devices," *Internet Things*, vol. 12, p. 100319 (2020).
- [8] A. Awajan, "A novel deep learning-based intrusion detection system for IoT networks," *Computers*, vol. 12, p. 34 (2023).
- [9] E. Emary, H. M. Zawbaa, and A. E. Hassanien, "Binary gray wolf optimization approaches for feature selection," *Neurocomputing* (2015). doi: 10.1016/j.neucom.2015.06.083.
- [10] A. K. Dey, G. P. Gupta, and S. P. Sahu, "A metaheuristic-based ensemble feature selection framework for cyber threat detection in IoT-enabled networks," *Decision Analytics Journal*, vol. 7, p. 100206 (2023). doi: 10.1016/j.dajour.2023.100206.

- [11] S. Ahmadi, "AI in the detection and prevention of distributed denial of service (DDoS) attacks," *Int. J. Adv. Comput. Sci. Appl.*, vol. 15, no. 10 (2024). doi: 10.14569/IJACSA.2024.0151004.
- [12] A. K. Dey, G. P. Gupta, and S. P. Sahu, "Hybrid meta-heuristic based feature selection mechanism for cyber-attack detection in IoT-enabled networks," *Procedia Comput. Sci.*, vol. 218, pp. 318–327 (2023). doi: 10.1016/j.procs.2023.01.014.
- [13] Y. T. Ta and G. Murtugudde, "An efficient algorithm for anomaly intrusion detection in a network," *Global Transitions Proceedings*, vol. 2, pp. 255–260 (2021). doi: 10.1016/j.gltp.2021.08.066.
- [14] Q. M. Alzubi, M. Anbar, Y. Sanjalawe, M. A. Al-Betar, and R. Abdullah, "Intrusion detection system based on hybridizing a modified binary grey wolf optimization and particle swarm optimization," *Expert Syst. Appl.*, vol. 204, p. 117597 (2022). doi: 10.1016/j.eswa.2022.117597.
- [15] A. Alzaqebah, I. Aljarah, O. Al-Kadi, and R. Damaševičius, "A modified grey wolf optimization algorithm for an intrusion detection system," *Mathematics* (2023). doi: 10.3390/math10060999.
- [16] D. Srivastava, S. Hooda, R. Gill, and C. Singla, "Detection of cyber-attacks by using grey wolf optimizer," in *Proc. 2023 Int. Conf. Intelligent Systems for Communication, IoT and Security (ICISCoIS)*, Coimbatore, India, pp. 596–600 (2023). doi: 10.1109/ICISCoIS56541.2023.10100556.
- [17] H. Yang and Z. Zhou, "A novel intrusion detection scheme using cloud grey wolf optimizer," in *Proc. 37th Chinese Control Conf. (CCC)*, Wuhan, China, pp. 8297–8302 (2018). doi: 10.23919/ChiCC.2018.8483324.
- [18] J. K. Seth and S. Chandra, "Intrusion detection based on key feature selection using binary GWO," in *Proc. 3rd Int. Conf. Computing for Sustainable Global Development (INDIACom)*, New Delhi, India, pp. 3735–3740 (2016).
- [19] H. Almazini and K. Ku-Mahamud, "Heuristic initialization using grey wolf optimizer algorithm for feature selection in intrusion detection," *Int. J. Intell. Eng. Syst.*, vol. 16 (2023). doi: 10.22266/ijies2023.0228.36.
- [20] J. W. Too, A. R. Abdullah, N. M. Saad, N. M. Ali, and W. Tee, "A new competitive binary grey wolf optimizer to solve the feature selection

- problem in EMG signals classification,” *Computers*, vol. 7, no. 4, p. 58 (2018). doi: 10.3390/computers7040058.
- [21] H. Almazini and K. Ku-Mahamud, “Grey wolf optimization parameter control for feature selection in anomaly detection,” *Int. J. Intell. Eng. Syst.*, vol. 14 (2021). doi: 10.22266/ijies2021.0430.43.
- [22] R. Hireche, H. Mansouri, and A.-S. K. Pathan, “Security and privacy management in Internet of Medical Things (IoMT): A synthesis,” *J. Cybersecur. Priv.*, vol. 2, pp. 640–661 (2022). doi: 10.3390/jcp2030033.
- [23] I. Nur and E. Ülker, “A novel hybrid IoT-based IDS using binary grey wolf optimizer (BGWO) and naive Bayes (NB),” (2020). [Online]. Available: <https://doi.org/10.31590/ejosat.804113>.
- [24] A. Chohra, P. Shirani, E. B. Karbab, and M. Debbabi, “Chameleon: Optimized feature selection using particle swarm optimization and ensemble methods for network anomaly detection,” *Comput. Secur.*, vol. 117, p. 102684, Jun. (2022). doi: 10.1016/j.cose.2022.102684.
- [25] J. Liu, D. Yang, M. Lian, and M. Li, “Research on intrusion detection based on particle swarm optimization in IoT,” *IEEE Access*, vol. 9, pp. 38254–38268 (2021). doi: 10.1109/ACCESS.2021.306367.
- [26] X. Liu and Y. Du, “Towards effective feature selection for IoT botnet attack detection using a genetic algorithm,” *Electronics*, vol. 12, no. 5, p. 1260 (2023). doi: 10.3390/electronics12051260.
- [27] S. M. Lundberg and S. I. Lee, “A unified approach to interpreting model predictions,” *Advances in Neural Information Processing Systems*, vol. 30 (2017).
- [28] L. S. Shapley, “17. A value for n-person games,” in *Contributions to the Theory of Games (AM-28), Volume II*, Princeton University Press, pp. 307–318 (2016).
- [29] S. Mirjalili, S. M. Mirjalili, and A. Lewis, “Grey wolf optimizer,” *Advances in Engineering Software*, vol. 69, pp. 46–61 (2014). doi: 10.1016/j.advengsoft.2013.12.007.
- [30] K. M. Faraoun and A. Boukelif, “Neural networks learning improvement using the K-means clustering algorithm to detect network in-

- trusions," *INFOCOMP J. Comput. Sci.*, vol. 5, no. 3, pp. 28–36 (2006). doi: 10.5281/zenodo.1059752.
- [31] N. Shi, X. Liu, and Y. Guan, "Research on k-means clustering algorithm: An improved k-means clustering algorithm," in *3rd Int. Symp. Intell. Inf. Technol. Secur. Informatics (IITSI)*, pp. 63–67 (2010). doi: 10.1109/IITSI.2010.74.
- [32] A. Moubayed, M. Injadat, A. Shami, and H. Lutfiyya, "Student engagement level in e-learning environment: Clustering using K-means," *Am. J. Distance Educ.*, vol. 34, no. 02, pp. 1–20 (2020). doi: 10.31235/osf.io/ecg4x.
- [33] A. Moubayed, M. Injadat, A. Shami, and H. Lutfiyya, "DNS Typo-Squatting domain detection: A data analytics & machine learning-based approach," in *2018 IEEE Glob. Commun. Conf. (GLOBECOM)* (2018). doi: 10.1080/08923647.2020.1696140.
- [34] N. Koroniotis, N. Moustafa, E. Sitnikova, and B. Turnbull, "Towards the development of realistic botnet dataset in the Internet of Things for network forensic analytics: Bot-IoT dataset," *Future Gener. Comput. Syst.*, vol. 100, pp. 779–796 (2019).

Received November, 2024