Proceedings of the 38th iSTEAMS Bespoke Conference – Accra Ghana 2024

Society for Multidisciplinary & Advanced Research Techniques (SMART)
West Midlands Open University – Projects, Research, Innovations, Strategies & Multimedia (PRISM) Centre
SMART Scientific Projects & Research Consortium (SMART SPaRC)
Sekinah-Hope Foundation for Female STEM Education
ICT University Foundations USA
Harmath Global Educational Services

38th International Science Technology Education Arts Management
& Social Sciences (iSTEAMS) Bespoke Conference - Accra Ghana 2024

Utilizing Metaheuristic Ensemble Feature Selection to Enhance Intrusion Detection Systems

[1]Shuaibu, Yusuf Bilal & [2]Alabi, Isiaq Oludare
[1]Department of Computer Science
[2]Department of Information Technology
Federal University of Technology, Minna, Niger State, Nigeria.
E-mails: billalyuusuf@gmail.com; isiaq.alabi@futminna.edu.ng;
Phones: +2348023130292; +2347036799142

ABSTRACT

Intrusion detection plays a crucial role in ensuring the security of computer networks by identifying and preventing unauthorized access or malicious activities. This thesis aim to develop an advanced intrusion detection model by integrating Gravitational search Algorithm (GSA) with Grey wolf Optimization (GWO) algorithm to optimize its performance. The proposed model will combine the strength of GSA-GWO in classification with the optimization capabilities of GWO to enhance the accuracy and efficiency of intrusion detection systems. The research methodology will begin with the selection of appropriate datasets, representative of real-world network traffic, for training and testing the intrusion detection model. Preprocessing techniques will be applied to prepare the datasets, including feature selection and normalization, to ensure the model's robustness and effectiveness. The GSA algorithm will then be implemented and configured, with suitable kernel functions and hyperparameter tuning, to train the intrusion detection model. To optimize the performance of the GSGW-DT model, the Grey Wolf Optimization algorithm will be employed. GWO will mimic the bio behavior of Gey wolves to search for optimal solutions in complex problem spaces. By incorporating GWO, the intrusion detection model will be able to fine-tune BGSA-BGWO parameters and select relevant features, thereby improving accuracy, reducing false positives/negatives, and enhancing overall performance. The developed model will be evaluated using various performance metrics, including accuracy, precision, recall, F1-score, and the area under the receiver operating characteristic curve (AUC-ROC). Comparative analysis will be conducted to assess the superiority of the GSA-GWO model over baseline models or existing intrusion detection approaches. Furthermore, an in-depth analysis of the results will highlight the strengths, weaknesses, and optimization benefits achieved by the proposed model. The conclusion will summarize the key findings and contributions of the study, emphasizing the effectiveness of the GSA-GWO model in optimizing intrusion detection performance. Limitations and potential areas for improvement will be discussed, paving the way for future research. Future work will include exploring additional optimization algorithms, evaluating real-time intrusion detection scenarios, and investigating hybrid approaches to further enhance the model's accuracy and robustness.

Keywords: Transformer, Fisher's Score, SMOTE, IoT, IDS

Proceedings Citation Format
Alabi, Isiaq Oludare & Shuaibu Yusuf Billal (2024): Utilizing Metaheuristic Ensemble Feature Selection to Enhance Intrusion Detection Systems. Proceedings of the 38th iSTEAMS Multidisciplinary Bespoke Conference. 17th – 19th July, 2024. University of Ghana, Accra, Ghana. Pp 243-264.. dx.doi.org/10.22624/AIMS/ACCRABESPOKE2024P27

1. INTRODUCTION

Internet has changed daily lives by providing economical, fast and reliable access to different types of services. The advancements in communication technology and universal accessibility to a wide range of service have opened many challenges Feldmann *et al. (*2020*);* Trevisan *et al.* (2020). The proliferation of IoT device and increasing interconnection of systems further worsening vulnerabilities present in network infrastructure Neupane *et al.,* (2019), etc. therefore effort have made in research and industry to prevent the critical system from intrusion. The IDS have received attention due to continuously increasing cost of fight cybercrimes, the cybercrime type includes malware infections, network intrusions, data breaches, malicious insider, Dos attacks, web-based attacks etc. consequently, the optimization of IDS performance is crucial due to evolving nature cyber threats and the potential consequences of successful intrusion as intruder constantly uses their techniques , explore new vulnerabilities and employed sophisticated attack vectors to gain access. Consequently IDS must be capable of ensuring fundamental security triad (confidentiality, integrity & availability) of an information system by identifying & preventing malicious activities in real-time before they access and harm triad of the critical system. Confidentiality refers to protecting information asset against unintentional, unauthorized disclosure, Integrity assures the correctness or accuracy/efficiency of the stored or transmitted information while Availability defines the system or service is available to use.

The network-based intelligent environment has also led to various security threats. The term cyber threats refer to any harmful activity that wants steal data or hurt resourcesZ. Chen *et al.,* (2022). It have caused economic losses and weakened Network-based infrastructures. Recent years have witnessed various cyber-attacks such as Dyn exploited IoT devices embedded within intelligent homes to operate as botnets using malware named. In 2016. Silex malware infected 1650 IoT devices in the year 2017. (Tops 5 shocking IoT security breaches of 2019) and manual reinstallation of the firmware was performed to restored the devices default settings.

In the year 2020. Thress gas pipeline companies in the USA announce another cyber attack, claiming that the electronic communication systems had been down for several days (Christine Buurma, Alyza sebenius, Ransomware Shuts Gas Compressor for Days in latest Attacks Bloomberg 2020) similarly June 2022, an HTTPS Distributed Dos cyber-attack reached its peak when a user of ' Google Cloud Armor' was attacked with 46 million requests/second which was recorded as the world largest cyber-threat(Google, How google cloud blocked largest layer 7 DDos attack yet, 46 million RPS 2022) This attack's traffic was analyzed and detected by Google early in its lifecycle. In addition, statistical reports that by 2025, the number of connected Iot gadgets will rise to 75.44 billion (Statita Research Department, Internet f things 2016). It will lead to gain 11trillion USD annually in the economy by 2025(approximately 11% of the global economy) therefore a robust, affective and more secure intelligent cyber threat detection framework is required to gadget-enabled networks from both known and unknown threats.

Regardless of technological advancement, the above-discussed attacks posed serious threat fundamental security triad V. Hajisalem *et al.,* (2018). Organization deploys different software & hardware-based security solutions like Antivirus, firewalls solutions, intrusion detection and prevention system (IDS/IPS) to defend against different security attacks Y. Zhou *e al.,* (2020).

The functionality of IDS is to observe the host or networks exposed to the attack & create alerts and warning to the Admin or Security professionals P. Kumar *et al,* (2021).

2. LITERATURE REVIEW

The literature review provides a comprehensive overview of existing research and knowledge related to intrusion detection systems, Gravitational search Algorithm(GSA) with Grey wolf Optimization (GWO) algorithm and ensemble learning methods.(Sridevi Kalaiarasi ***et al***., 2022) have proposed Intrusion Detection Technique in Wireless Sensor Network using Grid Search Random Forest with Boruta Feature Selection Algorithm to improve the classifier's performance through the feature selection method. The model is evaluated on well-known standard datasets, KDDCUP. The performance of the classifiers such as SVM, LDA, CART Random Forest is 98.5%, 98%, 97.7%, and 99%, respectively. To improve the performance of the classifier further, The BFSRF is used for efficient feature selection based on wrapper and ensemble techniques. BFS-RF performance is assessed in terms of accuracy, This work is also compared with LDA and CART machine learning algorithms.

Alghanam ***et al***., (2022) suggested an enhance feature selection model for NIDS named LS-PIO. According to the results the ensemble of classifiers iForest, LoF, and OC-SVM achieved maximum ACC(99.28) with 12 features out of 42 features for KDDCUP-99 dataset. In addition, Zhou et al.,(2020) have anticipated an efficient framework for IDS. The technique is known as CFS-BA. The model uses the BAT algorithm to get optimized features. In addition, the model is constructed using voting-based ensemble classification using C4.5, RF and forest PA, which requires less computing time. The effectiveness of the framework is assessed by the NSL-KDD, AWID, and CIC-IDS2017 database. However, key evaluation metrics: PR and F1_score are not considered in this experiment.

XuKui Wei Zhang ***et al***.,(2020) Building Auto-Encoder Intrusion Detection System based on Random forest feature selection Auto-Encoder technique can efficiently solve the sample imbalance problem, which is very common in network environment. AE-IDS works online and performs better than some popular batch/offline methods. It reduces the computation cost by feature selection and feature grouping operation. AP clustering is helpful to find significant feature subset and merge similar features. The Experimental results show it can detect most attacks accurately and speedup training and testing procession.

Oseni ***et al***.,(2022) have developed a explainable framework using Deep Learning for cyber threat detection in IoT-enabled networks. Correlation coefficient method to select the features in the framework . convolution Neutral Network is applied to detect the threats. The effectiveness of the framework is evaluated by ToN-IoT dataset. This techniques achieved ACC of 99.15% and 90.55% for the binary-label and multi label detection problem respectively, overall FPR was not discussed in this experiment. Kumar et al., (2021) have developed a cyber threat detection model named DLTIF, In this model deep feature extractor is used to find hidden pattern. Next, cyber threat intelligence is applied to detect cyber threats. Based on the experiment result, the model achieved the highest ACC of 99.98 for ToN-IoT dataset. However, feature selection, overall DR, and FPR were not discussed in this experiment. Dey *et al.,* (2023)have proposed a hybrid framework for cyber threat detection. In this framework, features are selected by hybrid NSGA-II techniques. Next, Support Vector Machine is to detect cyber threats. Experimental results indicate the model achieved an ACC of 99.48% and selected 13 features from 45 in the ToN-IoT dataset. However, the authors have not discussed DR and FPR.

Tama *et al*., (2019) suggested another hybrid model named TES-IDS. Metaheuristic techniques such as ACO, GA, and PSO are adapted for feature selection. Then an innovative two-stage classifier is designed to detect cyber threats. The effectiveness of the model is assessed by the UNSW-NB 15 and NSL-KDD dataset. Experimental results indicate that model achieved maximum ACC of 91.2% and minimum 19 features out of 42 in the UNSW-NB 15 dataset. However, result shows low DR for R2L and U2R threats and the model still suffer from high FPR. In addition, Dwivedi *et l.,* (2021) have presented novel hybrid techniques named EFSGOA to detect intrusions in the network traffic data. Optimal features are selected by filter methods such as CMIM, mRMR, and JMI. After that, to get final subset of features, grasshopper optimization technique is applied. Then benign and malicious activities are detected by SVM.

Based on the experiment result model achieved ACC of 99.89% and 99.89% for the NSL-KDD and KDDCUP-99 datasets respectively. This approach, however, relies on an outdated dataset that does not incorporate advanced cyber threats. *Kumar et al., (2022)* have proposed a Deep Learning-based technique named PBDL. In this technique, data is secured by blockchain technology then a novel hybrid deep learning technique named SA-BiLSTM is used to detect cyber threats. The IoT-Botnet and ToN-IoT datasets are used to evaluate the performance of the technique. However, overall DR, and FPR were not discussed in this experiment. *Kumar et al., (2022)* have proposed a blockchain and deep learning-based IDS model named P2TIF. The model uses blockchain techniques for secure communication and a deep variational encoder for data encoding. in addition, GRU is used to extract useful features. To detect cyber threats, an attention-based deep-gated recurrent neural network is used. Based on the experiment result, the model achieved ACC of 99.88% and 00.29 for the IoT-Botnet and ToN-IoT datasets respectively. However, the number of selected features, overall DR, and FPR is not discussed by the authors.

Outlier Detection suggested by Alif Nur Iman *et Al.,* (2020*)* Outliers are dynamically formed through the results of k-means clustering of all features. There are two techniques proposed in Spatial division negative selection algorithm (SD-RNSA) *Ruiru Zhang et Al., (2019)* Inspired by a negative selection algorithm in the biological immune system, paper proposes a wireless sensor network intrusion detection model based on the spatial division negative selection algorithm (SD-RNSA). The main contributions of this model are as follows. (1) The algorithm analyzes the distribution of self-set in the real valued space and divides the real-valued space. (2) The negative selection algorithm is implemented in the subspace, which reduces the tolerance range of the candidate detector and saves resources of sensor nodes. (3) In the detection process of detectors, the antigen to be detected only needs to match with mature detectors in the subspace where the antigen is located, thus accelerating the detection process. In this paper, the performance of the model is analyzed in theory; experimental results show that the model has better time efficiency and detector quality.

3. RESEARCH METHODOLOGY

The research methodology section describes the approach and procedures used to achieve the objectives of the study, including the development of the intrusion detection model based on metaheuristics-based wrapper feature selection techniques such as: Gravitational Search Algorithm (GSA), Grey Wolf Optimization (GWO), and ensemble learning methods are discussed.

3.1 Binary Gravitational Search Algorithm (BGSA)

BGSA is the process of converting the continuous solution obtained by the GSA to a binary solution Rashedi et al., (2010). GSA can solve continuous optimization problem and feature selection is a discrete optimization problem Alazzam et al., (2020). Hence, it is necessary to convert the solution of GSA in to the binary form to represent the FS problem.

3.2 Binary Grey Wolf Optimization (BGWO)

BGWO is the process of converting the continuous solution obtained by GWO to a binary solution Emary et al, (2015) GWO can tackle continuous optimization problems but the selection of features is a discrete optimization problem Alazzam et al., (2020). Hence, it is necessary the solution of GWO should be converted into binary values {0,1} in nature.

3.3 Dataset selection

UNSW-NB15 - Identify and select appropriate datasets for training and testing the intrusion detection model. The datasets should be representative of real-world network traffic, and include both normal and malicious instances. Commonly used datasets for intrusion detection research is UNSW-NB15 (https://www.unsw.adfa.edu.au/unsw-canberra-cyber/cybersecurity/ADFA-NB15-Datasets/) Moustafa *et al., (2015).*

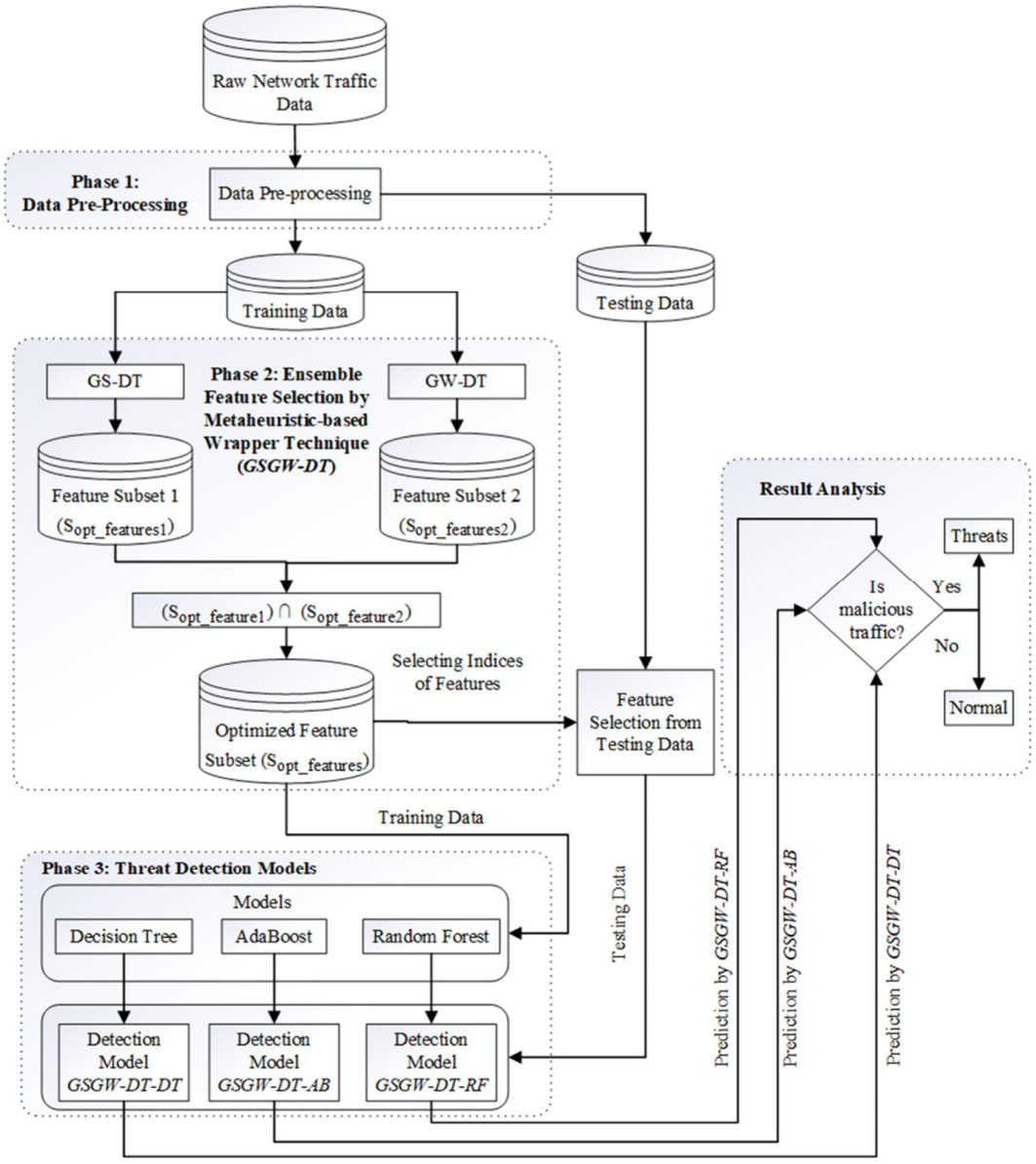

Fig 1: The overall flowchart of the model for intrusion detection system

Algorithm: Ensemble Feature Selection Technique: GSGW-DT

Input: Set of actual features $f \epsilon \{f_1, f_2, f_3, \ldots\ldots\ldots, f_n\}$
Output: Optimized subset of features ($S_{opt-}f$)

1. Initialise random population of k objects in n-dimension features space $f \epsilon \{f_1, f_2, f_3, \ldots\ldots\ldots, f_n\}$
2. Calculation to get first optimized features **subset** $S_{opt-}f_t$ using GS-DT
3. **For** index = 1, 2, 3. ……..,n) do // n is total number of features
4. Calculate GS-DT by using BGSA
5. $S_{opt-}f_{t1}$ = space $f \epsilon \{f_1, f_2, f_3, \ldots\ldots\ldots, f_p\}$// where p represents the optimized features in subset $S_{opt-}f_{t1}$
6. **End for**
7. Calculation to get second optimized features in subset $S_{opt-}f_{t2}$ using GW-DT
8. **For** index = (1, 2, 3, ……..n) do
9. **Compute GW-DT by using BGWO**
10. $S_{opt-}f_{t2}$ = space $f \epsilon \{f_1, f_2, f_3, \ldots\ldots\ldots, f_k\}$// where $_k$ represents the optimized features in subset $S_{opt-}f_{t2}$
11. **End for**
12. $S_{opt-}f_{t2}$ = $\{ ff \epsilon (S_{opt-}f_{t1} \cap S_{opt-}f_{t2})\}$
13. **Return** $S_{opt-}f_t$

3.3 Intrusion Detection Background For Internet-Enabled Gadget Networks

The detailed description of the working idea of the flowchart of the model for intrusion detection system is presented in fig. 2 and model is designed based on the concept of anomaly-based NIDDS for detection of intrusions, it consist of four stages: data pre-processing, feature selection, intrusion detection and evaluation of performance. Explanation of each stage is discussed as follows:

Stage 1: Data Pre-processing. This portion describes the steps involved in data pre-processing. As Internet-enabled network gadgets generate traffic from several devices and sensors, it is observed that these traffics contain various types of features including categorical and symbolic data. For this reason, data pre-processing is crucial to the creation of a robust and effective detection model, as described in the following.

i. **Label and Data Transformation**: Symbolic and categorical data from IoT network traffic are transformed into numerical numbers through data and label transformations. In addition, the target class is converted into binary classes 1 or 0, where 1 refers to normal traffic whereas 0 refers to malicious traffic.
ii. **Normalization**: It has been observed that features in IoT network traffic have distinct magnitude values, which can slow the learning process. In this model, min–max data normalization is applied in the dataset to rescaling the data value of each feature into the range [0,1]. This is because data normalization is a crucial step to avoid bias of higher values features from the dataset G.P. Gupta et al. (2020). Also, to enhance convergence, and reduce training time, data normalization is an important step.

The normalization formula P. Kumar et al.,(2021) is applied by using .

$$Fnormalized = F - Fminimum Fmaximum - Fminimum \ldots\ldots \text{eqn (1)}$$

Where F is the attribute that should be rescaled, $Fminimum$ represents minimum value, and $Fmaximum$ represents maximum value for each attribute in the dataset

Stage 2: Ensemble Feature Selection by Metaheuristic-based Wrapper methods: At this stage, two metaheuristic-based wrapper feature selection methods are designed in which Binary Gravitational Search Algorithm (BGSA) and Binary Grey Wolf Optimization (BGWO) are used as feature optimizers and Decision Tree (*DT*) is used as its evaluator for intrusion detection in Internet-enabled networks gadget. The designed method is based on BGSA and BGWO metaheuristic as Feature Selection optimization and Decision Tree is used as evaluator. Thus, the designed methods are apply to as *GS-DT* and *GW-DT,* respectively.

Firstly, the reason to apply metaheuristic-based wrapper Feature Selection methods is because these methods are more efficient to handling the search space complexity. Search space complexity means suppose network traffic data contains 'n' number of features then possible count of proper subset of features will be 2^n-1. This implies that the search space complexity of various subsets of features will have 2^n-1 B. Selvakumar et al.,(2019), which belongs to the NP-hard problem A. Nazir, R.A. Khan et al., (2021) that can be tackled in an efficient manner by the metaheuristic-based wrapper methods. Furthermore, wrapper methods are more accurate than filter methods A. Nazir, R.A. Khan et al., (2021). Secondly, a significant advantage of metaheuristic-based wrapper methods is that they use classifiers to guide the feature selection process E. Emary, H.M. Zawbaa et al.,(2016), since a classifier evaluates features based on their predictive accuracy. In this model DT classifier is used to train and evaluate the features subset. The reason to use DT as a class evaluator in BGSA and BGWO is because DT is able to handle complex features interrelation more easily than other types of base classifier H. Alazzam, A. Sharieh., (2020), S. Peddabachigari, A. Abraham., (2004). After that, we define a novel fitness function as defined in Eq. (1) is used to get the most suitable subset of features, and the workflow of this process is shown in Fig. 3.

The next step is to design an ensemble of *GS-DT* and *GW-DT* techniques to obtain more optimal features, which is apply to as a *GSGW-DT* model. This ensemble model integrates and takes advantage of *GS-DT* and *GW-DT* methods. As a result of these methods, two feature subsets are obtained. The first subset of features is selected by the *GS-DT apply to* $\boldsymbol{S}_{\text{opt\_f t1}}$. The second subset of features is selected by the *GW-DT* apply to $\boldsymbol{S}_{\text{opt\_f t2}}$. In the next step, the set intersection (∩) operation is applied on the above two subsets to get a single and more optimized subset of features (*i.e.*, all the features are selected from the above two subsets if and only if features are common), as defined in line # 12 of Algorithm 1. Then the final resulting subset of features obtained by *GSGW- DT* which is referred to $\boldsymbol{S}_{\text{opt\_f t}}$ is fed into the DT classifier as well as ensemble learning based classifiers such as AdaBoost and Random Forest separately to detect intrusion in Internet-enabled networks gadget.. Algorithm 1 shows the proposed ensemble feature selection methods.

Stage3: Intrusion Detection Using Machine Learning Algorithms

As this stage, three renowned machine learning approaches, such as DT, AdaBoost, and RF, are applied separately to the optimized feature subset ($\boldsymbol{S}_{\text{opt\_f t}}$) which is obtained by the *GSGW-DT* model. The designed detection model based on DT, AdaBoost, and Random Forest, which are denoted by *GSGW-DT-DT*, *GSGW-DT-AB*, and *GSGWDT-RF* respectively. Here, AdaBoost and Random Forest are ensemble learning-based classification methods. This is because many researchers stated that the performance of ensemble learning-based classifiers are much better than the use of a single classification method Y. Zhou, G. Cheng., (2020). A short-term explanation of the machine learning algorithms used in this research work is presented below:

Decision Tree (DT): The approach used in the DT classifier is a top-down, recursive, and divide-and-conquer approach. A greedy approach is used to solve a classification problem. The main procedure is to select a best feature (i.e., root node) and split it into from a larger training set into smaller training sets according to a certain splitting criteria M. Taradeh, et al., (2019). In the DT model, classification problem can be solved by asking the series of questions (i.e., the values) about the independent features from the training dataset. In which the independent features and their dependent features (i.e., target features) are organized in the form of decision tree. The hierarchical structure of the DT consisting of root node, internal nodes, leaf nodes, and edges where root node and internal nodes represents independent features, edges are the values of the independent features, and leaf node represents the class-label i.e., outcome of the classification. Once a DT model is built, it is applied to the test dataset for classification.

AdaBoost

The AdaBoost algorithm, also called Adaptive Boosting, is a repetitive method of boosting to classify the binary class Y. Zhou, T.A. Mazzuchi., (2020). It works by selecting and combining base learners in order to create a strong classifier. The implementation of AdaBoost in which with just one node and two leaf nodes, or it may be having many num initial base learners such as $model_1$ is selected on the basis of minimum bers of leaf nodes. Later than training set (f_1, f_2, f_3, ……f_{n-1}, f_n) entropy of stumps. Stump is nothing but a base learner which is a tree where $f_n \in$ {0, 1} is labeled class with weight of each record of size can classify the sample in a better way. This process is iterative to generate each DT in the forest. Finally, every DT in the forest produces a prediction for a single vote then by counting the majority vote from all the DTs prediction, results of the ensemble model is determined.

A significant benefit of RF model is that it is more accurate than DT and AdaBoost on unseen data and less likely to become overfit A. Nazir, R.A. Khan et al., (2021), I. Ahmad, M. Basheri,. (2018). Moreover, it requires minimal computational resources and does not require tree pruning, which is a time-consuming task I. Ahmad, M. Basheri,. (2018). k is calculated by k_{-1} are passed to the $model_1$ for training. If some records are misclassified by the $model_1$ then new model such as $model_2$ is created sequentially and only misclassified records with updated weights are passed to the $model_2$ to train the model, by doing this there is less chance of overfitting W. Hu, S. Member, W. Hu, S., (2008). Simultaneously, if $model_2$ produces some more misclassifications, then errors and updated weights are passed to the next base learner such as $model_3$ for training. This is repetitive unless and until with specific number of base learners to minimize the errors in each cycle during training process. Finally, the test data will be fed into every model in the sequence after that weight of each model is combined using weighted vote to make an ultimate prediction.

Random Forest (RF): RF is a kind of ensemble learning classifier based on the bagging technique, which can be defined as an ensemble of decision trees in a randomized way A. Nazir, R.A. Khan., (2021) to make a forest. The implementation of RF in which it works parallelly into two stages of randomization at each iteration; first phase of randomization is to create bootstrap dataset from the training set f_i^1, f_i^2, ……f_i^{n-1}, f_i^n; $\forall i = 1, 2,$ ……$k$where f^1, f^2, ……, f^{n-1} are independent features, $f^n \in$ {0, 1} is a dependent feature and k is total number of records). Bootstrap dataset is randomly picked any of the records such as $sample_1$ (f_j^1, f[ ],f_j^n); $\forall j = 2, 3, 5$…… from the training set. Records which are not present in the $sample_1$ is called out of bag records for $sample_1$ and further it is used to validate RF model.

In the second phase of randomization, to train every decision tree in the forest, a random decision tree is generated using a bootstrap dataset. In addition, the root node of the decision tree is decided randomly by the subset of features of $sample_1$ at each step. Now, these subsets are candidates to becoming a root node by doing this it can classify the sample in a better way.

This process is iterative to generate each DT in the forest. Finally, every DT in the forest produces a prediction for a single vote then by counting the majority vote from all the DTs prediction, results of the ensemble model is determined. A significant benefit of RF model is that it is more accurate than DT and AdaBoost on unseen data and less likely to become overfit A. Nazir, R.A. Khan., (2021) I. Ahmad, M. Basheri,. (2018) . Moreover, it requires minimal computational resources and does not require tree pruning, which is a time-consuming task I. Ahmad, M. Basheri,. (2018).

4. RESULTS AND DISCUSSION

4.1 Experiment Results

This chapter features the presentation of the results of the study, This portion comprises of four parts: 4.2 description of dataset is described. portion 4.3 describes the experimental setup. In Section 4.4, results of the models are Reconnaissance, Analysis, Backdoor, Shellcode, Worms, as shown in Table 3. Original dataset having 49 features belonging to the target feature with approximately 25,40,044 samples.

Apart from this, openly accessible training and testing dataset are separated into 1,75,341 and 82,332 data instances respectively N. Moustafa, J. Slay., (2015). It is observed that, the training and testing dataset having 43 features with a labeled class as shown in Table 2 and majority of investigators have used this separated dataset for the experimental purpose. Therefore, for this experiment discussed. portion 4.5 compares six state-of-the-art models with the models in the same experimental situation.

4.2. Data Collection

UNSW-NB15 is a network traffic-based dataset with modern low foot print cyber threats, as suggested by Moustafa et al.(2015) for cyber threats detection. IXIA Perfect Strom tool is used by the Australian Center for Cyber Security to develop. Experimental setup

4.2 Experimental Environment, Implementation Details, And Evaluation Metrics For Experimental Evaluation:

Experimental Environment: Python 3.9 – SVC package is used for implementation of the model. Experiments are carried out on Windows 10 PC. The experiments are performed on Spyder IDE using 2.20 GHz 8-Core Intel i7 CPU with 16 GB RAM.

Implementation Details: To find an optimized subset of features using BGSA and BGWO, different parameters are considered for the implementation, as described in Table 4. Further, to detect intrusions, DT, AdaBoost, and RF are used to learn the model. the UNSW-NB15 dataset. It consists of real-world examples of threats and synthetic threats simulated using Pump, which can generate up to 100 GB of cap files each to simulate 9 different types of intrusion: DoS, Exploits, Fizzers, Generic, In this work, hyperparameters are tuned for AdaBoost and RF from scikit-learn library in Python, as described in Tables 5 and 6.

Evaluation Metrics: To measure the detection performance of the models, four basic classification metrics i.e., number of True Positive, False Positive, True Negative, and False Negative (FN) are calculated, as described in the Table 7. Based on the above metrics, five evaluation metrics: Accuracy (ACC), F1-Score, False Positive Rate (FPR), Detection Rate (DR), Precision (PR) are calculated in this experiment to check the performance of the presented model. Where ACC measures the proportion of correctly classified network traffic H. Alazzam, A. Sharieh., (2020). In DR, actual attacks are compared to the percentage of correct predictions, which reflects an analysis model's ability to predict

PERFORMANCE EVALUATION

- ACCURACY: This shows the overall number of accurate predictions and is calculated through using Equation
  Accuracy=TP+TN/TN +FP+FN +TP. .....Eqn 2.
- SPECIFICITY: In what percentage of cases the normal traffic is accurately labeled as normal and Eqn 2 is used to calculate it.
  Specificity=TN/TN +FP.....Eqn 3.
- DETECTION RATE: In what percentage of cases the proposed algorithm detects the intrusion traffic accurately and uses Eqn4
  DETECTION RATE=TP/ TP+FN.....Eqn 4.
- PRECISION= TP/ TP+FN Eqn5

Table 1: Parameters & Descriptions

Parameter	Description
Total count of independent features	42
Total count of dependent features	1 (Binary class)
Number of objects/epochs	10
Train-test split	68.05% for training and 39.95% for testing, as shown in Table 2.
Fitness function	Formulated and expressed in Eq. (1)
Number of iterations	BGSA: 180, BGWO:140
Population initialization scheme	rand ()
Activation function	Sigmoid
Classifier for evaluation	Decision Tree for both BGSA and BGWO
base_estimator	Decision Tree
n_estimator	500
learning_rate	0.1
algorithm	SAMME.R
random_state	None

Table 2
Hyperparameter tuning for RF.

max_depth	4
max_features	4
min_samples_leaf	1
min_samples_split	2

n_estimators	10

Table 3: Class Types

S.N.	Class types	Total samples in training set	Total samples in testing set	Total samples
1	DoS	12,264	4,089	16,353
2	Exploits	33,393	11,132	44,525
3	Fuzzers	18,184	6,062	24,246
4	Generic	40,000	18,871	58,871
5	Reconnaissance	10,491	3,496	13,987
6	Analysis	2,000	677	2,677
7	Backdoor	1,746	583	2,329
8	Shellcode	1,133	378	1,511
9	Worms	130	44	174
10	Normal	56,000	37,000	93,000
	Total	**1,75,341**	**82,332**	**2,57,673**

Table 4:Distribution of samples of UNSW_NB15 training and testing dataset.

Technique	FS Techniques	Number of selected features	Index of selected subset of features
BGSA	GS-DT	8	{F_0, F4,F5,F10,F27,F30,F31,F38,}
BGWO	GW-DT	12	{F_0, F2,F3,F4,F6,F10,F14,F19,,F22,F30,F34,F3
	GSGW-DT 4		{F_0, F4,F10,F30}

Table 5
Intrusions detection performance o
the model.

Threat Detection models	Detection technique	ACC (%)	DR (%)	PR (%)	F1-Score (%)	FPR (%)
GSGW-DT-DT	Decision Tree	99.02	98.32	99.50	99.04	0.24
GSGW-DT-AB	AdaBoost	99.36	98.47	**99.94**	99.27	0.04
GSGW-DT-RF	Random Forest	**99.41**	**99.09**	99.92	**99.33**	**0.03**

4.3. Performance of the project work

In this section, the performance of the proposed FS techniques such as *GS-DT*, *GW-DT*, and *GSGW-DT* are evaluated using the UNSWNB15 dataset. UNSW-NB15 includes all 9 types of threats, but attacks are not equally distributed, as shown in Table 3. Therefore, during the evaluation, repeated stratified-10-fold cross-validation approach is used to ensure that the classifier could generalize to unseen data. Table 8 shows the number of selected features obtained by the proposed FS techniques. Moreover, many researchers stated that a general improvement in accuracy is also associated with a higher FPR A. Nazir, R.A. Khan., (2021) A. Oseni, et al.,(2022). Therefore, the proposed model is designed to maintain the highest accuracy, detection rate, precision, and f1_score with lowest FPR.

It can be observed form Table 9 data that the proposed model *GSGW-DTRF* reaches the highest level of accuracy with 99.41% and the lowest FPR with 0.03%. However, the model *GSGW-DT-AB* achieved a better result in terms of precision with 99.94% as compared to the proposed model such as *GSGW-DT_RF* and *GSGW-DT-DT*. In summary, based on the result described in Tables 8 and 9, it can be concluded that *GSGW-DT-RF* is a better model than other models.

4.4 Validation of feature selection framework

In order to validate the number of selected features, Pearson Correlation Coefficient technique is applied to calculate the correlation coefficient scores among individual feature exist in the dataset. Figs. 3 shows the correlation coefficient matrix for all feature versus selected features by the method named *GSGW-DT*. Fig. 3

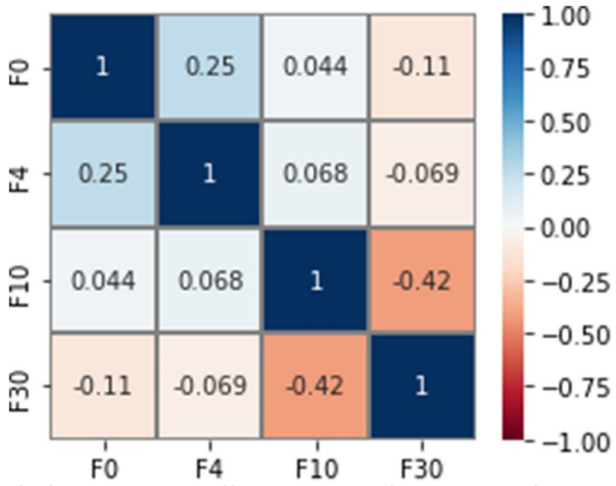

Fig. 3. Correlation coefficient matrix for selected features.

shows that all the selected independent features such as F_0, F_4, F_{10}, and F_{30} have correlation coefficient values less than 0.50, which implies that there is low correlation among independent features. Due to this, the model has achieved the best classification results.

Table 6: references Model Name and Parameters

References	Model name	Selected features	Detection technique	ACC (%)	DR (%)	PR (%)	F1-Score (%)	FPR (%)
Vajiheh et al.	ABC-AFS	5	CART	98.60	99.0	98.70	98.88	0.13
Nazir et al.	TS-RF	16	RF	83.12	86.22	86.32	86.21	3.7
Alazzam et al.	Cosine-PIO	5	DT	91.70	89.40	90.93	90.90	0.34
Gauthama et al.	HC-IBGSA SVM	30	SVM	94.11	98.47	98.74	98.62	2.18
Kumar et al.	Rule-based IDS	13	DT	84.83	90.32	57.01	68.13	2.01
Tama et al.	TES-IDS	19	TES	91.27	91.30	91.60	91.50	8.90
model	GSGW-DT-DT	4	DT	99.02	98.32	99.50	99.04	0.24
model	GSGW-DT-AB	4	AB	99.36	98.47	99.94	99.27	0.04
model	GSGW-DT-RF	4	RF	99.41	99.09	99.92	99.33	0.03

5. COMPARISON OF THE FRAMEWORK WITH EXISTING TECHNIQUES

This section compares intelligent intrusion detection models with six state-of-the-art models using the same experimental scenario. Table 10 shows the comparison results in terms of the number of selected features, accuracy, detection rate, precision, F1-score, and FPR. The model *GSGW-DT-RF* records the highest accuracy with 99.41%, detection rate with 99.09%, F1-Score with 99.33%, and model such as *GSGW-DT_RF* and *GSGW-DT-DT*. In summary, based on the result described in Tables 8 and 9, it can be concluded that *GSGW-DT-RF* is a better model than other models. The lowest FPR with 0.03% with minimum number of features (4 features).

Fig. 4 illustrates the result analysis of the models such as *GSGW-DT-DT*, *GSGW-DT-AB*, *GSGW-DT-RF* in terms of accuracy and, also compare its performance with the six state-of-the-art models. It is observed from Fig. 7 that *GSGW-DT-RF* model perform better than the remaining models with 99.41% accuracy. Moreover, two other models, such as *GSGW- DT-AB* and *GSGW-DT-DT*, achieved the second and third highest accuracy with 99.36% and 99.02%, respectively among other existing models. This is due to more robust optimized features provided by the models as compared with the existing models. Moreover, an ensemble learning approach produces more accurate results than a single classifier.

Fig. 5 illustrates the result analysis of the models such as *GSGW-DT-DT*, *GSGW-DT-AB*, *GSGW-DT-RF* in terms of detection rate and, also compare its performance with the six state-of-the-art models. It is observed from Fig. 6 that *GSGW-DT-RF* model perform better than the remaining models with 99.09% detection rate. This is because of the fact that the model obtains more robust, optimized features that minimize the problem of model overfitting and high detection errors. However, the model based on V. Hajisalem, S. Babaie.(2018) have achieved the second-highest detection rate of 99% from other two model such as *GSGW-DT-AB* and *GSGW-DT-DT*, but it is also significant to note that the number of selected features in *GSGW-DTAB* and *GSGW-DT-DT* are 4, which is less than the selected features obtained by model V. Hajisalem, S. Babaie.(2018).

Fig. 6 illustrates the result analysis of the models such as *GSGW-DT-DT*, *GSGW-DT-AB*, *GSGW-DT-RF* in terms of precision rate and, also compare its performance with the six state-

of-the-art models. It is observed from Fig. 6 that now *GSGW-DT-AB* model perform better than the remaining models with 99.94% precision rate. However, in the evaluation of precision rate, two other proposed models such as *GSGW-DT-RF* and *GSGW-DT-DT*, achieved the second and third highest precision with 99.92% and 99.5%, respectively among other existing models. The reason behind this is that malicious network traffic should not be missed during the detection process. Therefore, the False Negative as defined in Table 7 should be as low as possible. In these circumstances, precision rate can be low, but detection rate should be high. Fig. 7 illustrates the result analysis of the models such as *GSGW-DT-DT*, *GSGW-DT-AB*, *GSGW-DT-RF* in terms of F1-Score and, also compare its achieving results with the six state-of-the-art models. As seen in Fig. 7, the *GSGW-DT-RF* model performs better than the rest of the models, with 99.33% F1-score. Moreover, two other models, such as *GSGW-DT-AB* and *GSGW-DT-DT*, achieved the second and third highest precision rates with 99.27% and 99.04%, respectively among other existing models. This is because F1-Score calculates the harmonic mean of precision and detection rate, and models achieved the highest detection rate and precision as compared to existing models.

6. CONCLUSIONS

In conclusion, the result analysis of the models such as *GSGW-DT-DT*, *GSGW-DT-AB*, GSGW-*DT-RF* in terms of FPR and, also compare its performance with the six state-of-the-art models are observed as the *GSGW-DT-RF* model performs better than the remaining models with the lowest FPR of 0.03%. This is due to ensemble learning techniques such as RF that combines multiple base classifiers to reduce false positive rate and produce more accurate solutions. Moreover, the proposed model *GSGW-DT-AB* has achieved the second lowest FPR with 0.04% among other models. This is due to ensemble learning techniques such as RF that combines multiple base classifiers to reduce false positive rate and produce more accurate solutions. However, model based on V. Hajisalem, S. Babaie.(2018) have achieved the third lowest FPR with 0.13% from the model *GSGW-DT-DT*, but it is also important to note that the number of selected features in *GSGWDT-DT* is 4, which is less than the selected features observed by the model V. Hajisalem, S. Babaie.(2018).

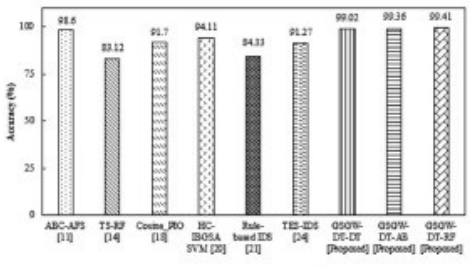

Fig 4: Result Evaluation of the Models in terms of Accuracy

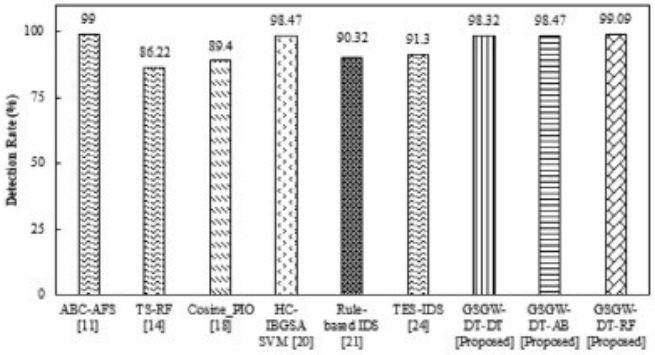

Fig 5: Result Evaluation of the Models in terms of Detection Rate

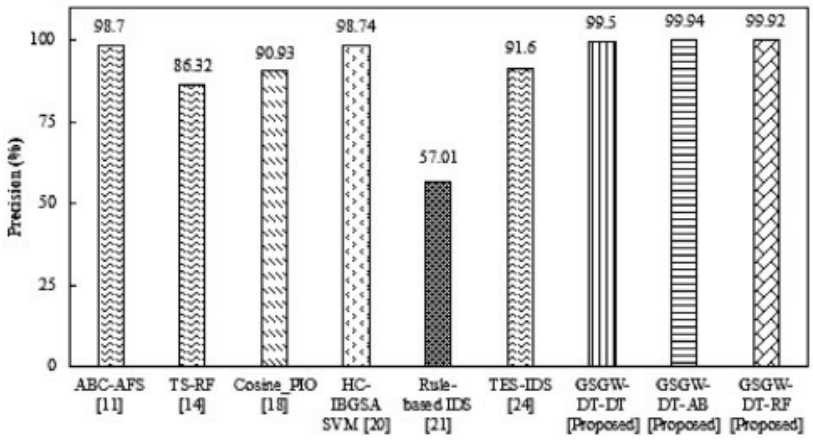

Fig 6: Result Evaluation of the Models in terms of Precision

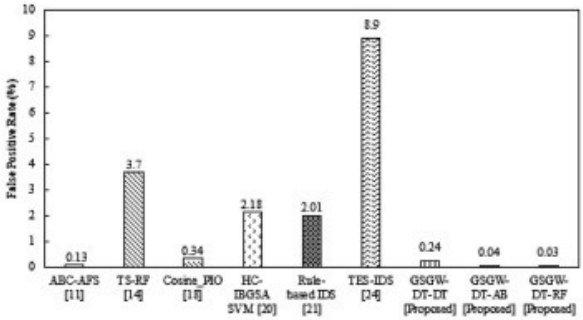

Fig 7: Result Evaluation of the models in term of F alse Positive Rate

REFERENCE

1. Nazir et al. A novel combinatorial optimization based feature selection method forNetworkintrusion detection Comput. Secur. (2021)
2. Alzubi QM, Anbar M, Alqattan ZN, Al-Betar MA, Abdullah R. Intrusion detection system Basedon a modified binary grey wolf optimisation. Neural ComputApplic. 2019;1-13.
3. A.Zhu, C.Xu, Z. Li,J.Wu, and Z.Liu,''Hybridizing grey wolf optimization with differentialevolution for global optimization and test scheduling for 3D stacked SoC,'' J. Syst. Eng.Electron., vol. 26, no. 2, pp. 317–328, Apr. 2015.
4. Axelsson S. Intrusion Detection Systems: A Survey and Taxonomy. Technical Report99-15.Department of Computer Engineering, Chalmers University; 2000.
5. Ahmim A, DerdourM, Ferrag MA. An intrusion detection system based on combining probability predictions of a tree of classifiers. Int J Commun Syst. 2018; (9): e3547. https://doi.org/10.1002/dac.3547.
6. B. Abhale and S. S. Manivannan, "Supervised machine learning classification algorithmicapproach for finding anomaly type of intrusion detection in wireless sensor network," Opt.Memory Neural Netw., vol. 29, no. 3, pp. 244–256, 2020.
7. Nazir, R. A. Khan, A novel combinatorial optimization based feature selection method
8. f or network intrusion detection, Comput. Secur.102(2021)102164, http://dx.doi.org/10.1016/j.cose.2020.102164.
9. A.K. Dey, G. P. Gupta and S. P. Sahu Decision Analytics Journal 7(2023)100206 J. Ambient Intell.Humaniz.Comput. 12(10)(2021)9555–9572, http://dx.doi. org/10.1007/s12652 020-02696-3
10. Oseni, etal., An explainable deep learning frame work for resilient intrusion detection in IoT enabled transportation networks, IEEE Trans. Intell. Transp. Syst. (2022)1–15,http://dx.doi.org/10.1109/TITS.2022.3188671.
11. K. Dey, G. P. Gupta, S. P. Sahu, Hybrid meta-heuristic based feature selection mechanism for cyber-attack detection in IoT-enabled networks, ProcediaComput. Sci. 218(2023)318–327,http://dx.doi.org/10.1016/j.procs.2023.01.014.
12. Selvakumar, K. Muneeswaran, Fire fly algorithm based feature selection for network intrusion detection, Comput. Secur.81(2019)148–155, http://dx.doi. org/10.1016/j.cose.2018.11.005.
13. Niu and L. Li, ''A novel PSO-DE-based hybrid algorithm for global optimization,'' in Proc. Int. Conf. Intell. Comput., 2008, pp. 156–163.
14. A. Tama, M. Comuzzi, K. H. Rhee, TSE-IDS: A two-stage classifier ensemble for intelligent anomaly-based intrusion detection system, IEEE Access 7(2019) 94497–94507, http://dx.doi.org/10.1109/ACCESS.2019.2928048.
15. Christine Buurma, AlyzaSebenius, Ransom ware Shuts Gas Compressor for Days in Latest Attack, Bloomberg, 2020, https://www.bloomberg.com/news/ articles/2020-02-18/ransomware-shuts-u-s-gas-compressor-for-2-days-in-latestattack#xj4y7vzkg.
16. D.Jitkongchuen,''Ahybriddifferentialevolutionwithgreywolfoptimizer
17. Denning DE.An intrusion-detection model.IEEE Trans Soft wEng.1987; 2:222-232. https://doi.org/10.1109/TSE.1987.232894.
18. Rashedi, H. Nezamabadi-pour, S. Saryazdi, GSA: A gravitational search algorithm, Inf. Sci. (Ny). 179(13)(2009)2232–2248,http://dx.doi.org/10.1016/ j.ins.2009.03.004

19. Rashedi, H. Nezamabadi-Pour, S. Saryazdi, BGSA: Binary gravitational search algorithm, Nat. Comput. 9(3)(2010)727–745, http://dx.doi.org/10.1007/ s11047-009-9175-3.
20. Emary, H. M. Zawbaa, A. E. Hassanien, Binary grey wolf optimization approaches for feature selection, Neurocomputing172(2016)371–381,http://dx. doi.org/10.1016/j.neucom.2015.06.083.
21. E. Kabir, J. Hu, H. Wang, and G. Zhuo, "A novel statistical technique for intrusion detection systems," Future Gener. Comput.Syst., vol. 79, pp. 303–318, 2018.
22. Xie, C. Lei, F. Li, D. Huang, and J. Yang, ''Unsupervised hyperspectral feature selection based on fuzzy c-means and grey wolf optimizer,'' Int. J. Remote Sens., vol. 40, no. 9, pp. 3344–3367, May 2019.
23. Garcia-Teodoro P, Diaz-VerdejoJ, Maciá-Fernández G, Vázquez E. Anomaly-based network intrusion detection: techniques systems and challenges. ComputSecur. 2009; 28(1-2):18-28. https://doi.org/10.1016/j.cose.2008.08.003.
24. Guo C, PingY, Liu N, Luo SS. A two-level hybrid approach for intrusion detection.Neuro computing.2016; 214:391-400. https://doi.org/ 10.1016/j.neucom.2016.06.021.
25. Google, How Google Cloud Blocked Largest Layer 7 DDoS Attack Yet, 46 Million Rps |
26. Google Cloud Blog, Google Cloud Blog, 2022, https://cloud.google.com/blog/products/identity-security/how-google-cloudblocked-largest-layer-7-ddos-attack-at-46-million-rps.
27. Wang, J. Gu, and S. Wang, "An effective intrusion detection framework based on SVM with feature augmentation," Knowledge-based Syst., vol. 136, pp. 130–139, 2017.
28. Alazzam, A. ,K.E.Sabri, A feature selection algorithm for intrusion detection system based on Pigeon InspiredOptimizer,ExpertSyst.Appl.148 (2020)http://dx.doi.org/10.1016/j.eswa.2020.113249.
29. H. M. Zawbaa, E.Emary, C.Grosan, and V.Snasel, ''Large-dimensionality small-instance set feature selection: A hybrid bio-inspired heuristic approach,'' Swarm Evol. Comput., vol. 42, pp. 29–42, Oct. 2018.
30. Ahmad, M. Basheri, M. J. Iqbal, A. Rahim, Performance comparison of support vector machine, random forest, and extreme learning machine for intrusion detection, IEEE Access 6(2018)33789–33795, http://dx.doi.org/10.1109/ACCESS. 2018.2841987.
31. Rojas-Delgado, R. Trujillo-Rasúa, R. Bello, A continuation approach for training Artificial Neural Networks with meta-heuristics, Pattern Recognit. Lett.125 (2019)373–380, http://dx.doi.org/10.1016/j.patrec.2019.05.017.
32. Khorram T, Baykan NA. Feature selection in network intrusion detection using metaheuristic algorithms. Int J Adv Res, Ideas Innovat Technol. 2018;4(4):704-710.
33. C. Darrell Etherington, Large DDoS attacks cause outages at Twitter, Spotify, and other sites, Techcrunch (2016) https://techcrunch.com/ 2016/10/21/many-sites-including-twitter-and-spotify-suffering-outage/#:~: text=Twitter%2CSoundCloud%2CSpotify%2CShopify, first reported on Hacker News.
34. Lopez-Martin, B. Carro, J. I. Arribas, and A. Sanchez-Esguevillas, "Network intrusion detection with a novel hierarchy of distances between embeddings of hash IP addresses," Knowledge-based Syst., vol. 219, 2021.
35. Abdel-Basset, D. El-Shahat, I. El-henawy, V. H. C. de Albuquerque, and S. Mirjalili, ''A new fusion of grey wolf optimizer algorithm with a two-phase mutation for feature selection,'' Expert Syst. Appl., vol. 139, Jan. 2020, Art. no. 112824.

36. L. M. Abualigah, A. T. Khader, and E. S. Hanandeh, ''A new feature selection method to improve the document clustering using particle swarm optimizationalgorithm,''J.Comput.Sci.,vol.25,pp. 456–466,Mar.2018.
37. L. M. Abualigah and A. T. Khader, ''Unsupervised text feature selection technique based on hybrid particle swarm optimization algorithm with genetic operators for the text clustering,'' J. Supercomput., vol. 73, no. 11, pp. 4773–4795, Nov. 2017
38. M.Mafarja, A.Qasem, A.A.Heidari,I.Aljarah,H.Faris, and S. Mirjalili, ''Efficient hybrid nature-inspired binary optimizers for feature selection,'' Cognit. Comput., vol. 12, no. 1, pp. 150–175, Jan. 2020.
39. Mukkamala S, JanoskiG, SungA. Intrusion detection using neural networks and support vector machines. Paper presented at: Proceedings of the 2002 International Joint Conference on Neural Networks. IJCNN'02 (Cat.No.02CH37290). Honolulu, HI ,USA: IEEE; vol. 2, 2002: 1702-1707.
40. Ma W. Analysis of anomaly detection method for Internet of things based on deep learning.Trans EmergTelecommun Technol. 2020;e3893.https://doi.org/10.1002/ett.3893.
41. Z. Chen, F. Han, L. Wu, J. Yu, S. Cheng, P. Lin, and H. Chen, "Random forest based intelligent fault diagnosis for PV arrays using array voltage and string currents," Energy Convers. Manage., vol. 178, pp. 250–264, 2018.
42. M. Taradeh, et al., An evolutionary gravitational search-based feature selection, Inf. Sci. (Ny). 497 (2019)219–239, http://dx.doi.org/10.1016/j.ins.2019.05.038.
43. Moustafa, J. Slay, UNSW-NB15: A comprehensive dataset for network intrusion detection systems (UNSW-NB15networkdataset), in: Mil. Commun. Inf. Syst. Conf.MilCIS2015-
44. Neri F. Comparing local search with respect to genetic evolution to detect intrusions in computer networks.Paper presented at: Proceedings of the Proceedings of the 2000 Congresson Evolutionary Computation. CEC00 (Cat.No.00TH8512).LaJolla, CA, USA: IEEE; vol. 1,2000:238-243.
45. P.Kumar,G.P.Gupta,R.Tripathi,Towarddesignofanintelligentcyberattack detection system using hybrid feature educed approach for IoT networks, Arab. J.Sci.Eng.46(4)(2021)3749–3778,http://dx.doi.org/10.1007/s13369-02005181-3.
46. Kumar, R. Kumar, S. Garg, A Secure Data Dissemination Scheme for IoT-Based E-Health Systems using AI and Blockchain, GLOBE COM 2022-2022 IEEE Global Communications Conference, Riode Janeiro, Brazil, 2022, pp. 1397–1403.
47. Kumar, G. P. Gupta, R. Tripathi, A distributed ensemble design based intrusion detection system using fog computing to protect the internet of things network
48. P. Kumar, R. Kumar, G. P. Gupta, R. Tripathi, G. Srivastava,P2TIF: A blockchain and deep learning frame work for privacy-preserved threat intelligence in industrial IoT, IEEE Trans. Ind.Inform.18(9)(2022)6358–6367, http://dx.doi.org/ 10.1109/TII.2022.3142030.
49. P. Kumar, G. P. Gupta, R. Tripathi, S. Garg, M. M. Hassan, DLTIF: Deep learning driven cyber threat intelligence modeling and identification framework in IoT-enabled maritime transportation systems, IEEE Trans. Intell. Transp. Syst. 24(2)(2021)1–10, http://dx.doi.org/10.1109/tits.2021.3122368.
50. P. Sinha, V. K. Jha, A. K. Rai, and B. Bhushan, "Security vulnerabilities, attacks and countermeasures in wireless sensor networks at various layers of osi reference model: A survey," in Proc. IEEE ICSPC, 2017

51. Li, H. Chen, H. Huang, X. Zhao, Z. Cai, C. Tong, W. Liu, and X. Tian, ''An enhanced grey wolf optimization based feature selection wrapped kernel extreme learning machine for medical diagnosis,'' Comput. Math.Methods Med., vol. 2017, pp. 1–15, 2017.
52. Q. Al-Tashi, H. M. Rais, S. J. Abdulkadir, S. Mirjalili, and H. Alhussian, ''A Review of Grey Wolf Optimizer-Based Feature Selection Methods for Classification,'' in Evolutionary Machine Learning Techniques. Springer, 2020, pp. 273–286.
53. Q.Tu,X.Chen, and X.Liu, ''Multi-strategy ensemble grey wolf optimizer and its application to feature selection,'' Appl. Soft Comput., vol. 76, pp. 16–30, Mar. 2019.
54. Q. Tu, X. Chen, and X. Liu, ''Hierarchy strengthened grey wolf optimizer for numerical optimization and feature selection,'' IEEE Access, vol. 7, pp. 78012–78028, 2019.
55. Q. Al-Tashi, S. J. Abdul Kadir, H. M. Rais, S. Mirjalili, and H. Alhussian, ''Binary optimization using hybrid grey wolf optimization for feature selection,'' IEEE Access, vol. 7, pp. 39496–39508, 2019.
56. SaiSindhuTheja, G. K. Shyam, An efficient metaheuristic algorithm based feature selection and recurrent neural network for DoS attack detection in cloud computing environment ,Appl. SoftComput.100(2021)106997, http: //dx.doi.org/10.1016/j.asoc.2020.106997.
57. R. Kumar, P. Kumar, R.Tripathi, G. P. Gupta, S. Garg, M.M. Hassan, BDT win: An integrated framework for enhancing security and privacy in cyber twin-driven automotive industrial internet of things, IEEEInt.ThingsJ.9(18)(2022) 17110–17119, http://dx.doi.org/10.1109/JIOT.2021.3122021.
58. R. Kumar, P. Kumar, R. Tripathi, G. P. Gupta, S. Garg, M. M. Hassan, A distributed intrusion detection system to detect DDoS attacks in block chain-enabled IoT network, J. Parallel Distrib. Comput.164(2022)55–68, http://dx.doi.org/10. 1016/j.jpdc.2022.01.030.
59. R.Kumar,P. Kumar, R. Tripathi, G. P. Gupta, A. K. M. N. Islam, M. Shorfuzzaman, Permissioned block chain and deep learning for secure and efficient data sharing in industrial health care systems, IEEE Trans. Ind. Inform.18(11)(2022) 8065–8073, http://dx.doi.org/10.1109/TII.2022.3161631.
60. R. Kumar, A.Aljuhani, P. Kumar, A. Kumar, A. Franklin, A. Jolfaei, Blockchain enabled secure communication forum manned aerial vehicle(UAV)networks, in: Drone Com 2022-Proc. 5thInt. ACM Mobicom Work. Drone Assist. Wirel. Commun.5Gbeyond,2022,pp.37–42,http://dx.doi.org/10.1145/3555661. 3560861.
61. Dwivedi, M. Vardhan, S. Tripathi, Building an efficient intrusion detection system using grasshopper optimization algorithm for anomaly detection, Clust.Comput.24(3)(2021)1881–1900, http://dx.doi.org/10.1007/s10586020-03229-5.
62. S. Mirjalili, S. M. Mirjalili, A. Lewis, Grey wolf optimizer, Adv. Eng. Soft w.69 (2014)46–61, http://dx.doi.org/10.1016/j.advengsoft.2013.12.007.
63. S. Peddabachigari, A. Abraham, J. Thomas, Intrusion detection systems using decision trees and support vector machines, Int. J. Appl. Sci. Comput. 11(3) (2004)118–134.
64. S. Garg, et al., 2020 En-ABC:An ensemble artificial bee colony based anomaly detection scheme for cloud environment, J. Parallel Distrib. Comput.135(2020) 219–233, http://dx.doi.org/10.1016/j.jpdc.2019.09.013.
65. S.Mirjalili,G.-G.Wang, and L.D.S.Coelho, ''Binary optimization using hybrid particle swarm optimization and gravitational search algorithm,'' Neural Comput. Appl., vol. 25, no. 6, pp. 1423–1435, Nov. 2014.

66. S. Fong, R. Wong, and A. Vasilakos, ''Accelerated PSO swarm search feature selection for data stream mining big data,'' IEEE Trans. Services Comput., vol. 9, no. 1, pp. 33–45, Jan./Feb. 2016.
67. Statita Research Depratment, Internet of things-number of connected devices world wide 2015–2025, Statista (2016) https://www.statista.com/statistics/ 471264/iot-number-of-connected-devices-worldwide/.
68. S.Mirjalili,G.-G.Wang,andL.D.S.Coelho,'' Binary optimization using hybrid particle swarm optimization and gravitational search algorithm,'' Neural Comput. Appl., vol. 25, no. 6, pp. 1423–1435, Nov. 2014
69. S. Mirjalili and S. Z. M. Hashim, ''A new hybrid PSOGSA algorithm for function optimization,'' in Proc. Int. Conf. Comput. Inf. Appl., Dec. 2010, pp. 374–377.
70. SrideviSubbiah, KalaiarasiSonaiMuthuAnbananthen, SaranyaThangaraj, Subarmaniam
71. Kannan, and DeisyChelliah and Journal of Communications And Networks, Vol. 24, No. 2, April 2022
72. Top 5 shocking IoT security breaches of 2019, Penta Security (2019) https: //www.pentasecurity.com/blog/top-5-shocking-iot-security-breaches-2019
73. Saranya, S. Sridevi, C. Deisy, T. D. Chung, and M. K. A. A. Khan,"Performance analysis of machine learning algorithms in intrusion detection system: A review," in ProcediaComput. Sci., vol. 171, pp. 1251–1260, 2020.
74. Uddin M, Rahman AA, Uddin N, Memon J, Alsaqour RA, Kazi S. Signature-based multi-layer distributed intrusion detection system usingmobileagents.IntJNetwSecur
75. Ucar Mk, Sakarya University, Faculty of Engineering, Electrical –Electronics Engineering,Sakarya, Turkey. 2020.
76. Verwoerd T, Hunt R. Intrusion detection techniques and approaches. ComputCommun. 2002; 25(15): 1356-1365. https://doi.org/10.1016/ S0140-3664(02)00037-3. 2013;15(2):97-105.https://doi.org/10.6633/IJNS.201303.15(2).03.
77. Vasilomanolakis E, Karuppayah S, Mühlhäuser M, Fischer M. Taxonomy and survey of collaborative intrusion detection. ACM Comput Surv.2015;47(4):1-33.https://doi.org/10.1145/2716260.
78. Hajisalem, S. Babaie, A hybrid intrusion detection system based on ABC-AFS algorithm form is use and anomaly detection, Comput. Netw .136(2018)37–50, http://dx.doi.org/10.1016/j.comnet.2018.02.028.
79. Kumar, D. Sinha, A. K.Das,S.C.Pandey,R.T.Goswami,Anintegratedrule based intrusiondetection system: analysis on UNSW-NB15 dataset and thereal time online dataset, Clust. Comput. 23(2)(2020)1397–1418, http://dx.doi.org/10.1007/s10586-019-03008-x.
80. Hu, S. Member, W. Hu, S. May bank, AdaBoost-based algorithm for network, IEEE Trans.Syst. Man. Cybern. 38(2)(2008)577–583.
81. Lai and M. Zhang, ''An efficient ensemble of GA and PSO for real function optimization,'' in Proc. 2nd IEEE Int. Conf. Comput. Sci. Inf. Technol., 2009, pp. 651–655.
82. X. Lai and M. Zhang, ''An efficient ensemble of GA and PSO for real function optimization,''
83. in Proc. 2nd IEEE Int. Conf. Comput. Sci. Inf. Technol., 2009, pp. 651–655.
84. XuKuiLia,Wei Chen a,Qianru Zhang b, LifaWua Zhang b, Lifa Wu a a Nanjing University of Posts and Telecommunications, No.9,Wenyuan Road, Nanjing, Jiangsu, China b University of Hong Kong, Pokfulam Road, Central and Western District, Hong Kong, China

85. Y.Zhou, G.Cheng, S.Jiang, M.Dai, Building an efficient intrusion detection system based on feature selection and ensemble classifier, Comput. Netw.174 (March) (2020) http://dx.doi.org/10.1016/j.comnet.2020.107247.
86. Wang, D. Wang, N. Geng, Y. Wang, Y. Yin, Y. Jin, Stacking-based ensemble learning of decision trees for interpretable prostate cancer detection, Appl. Soft Comput.77(2019)188–204, http://dx.doi.org/10.1016/j.asoc.2019.01.015.
87. Y. Zhou, T. A. Mazzuchi, S. Sarkani, M-AdaBoost-Abased ensemble system for networkintrusion detection, Expert Syst. Appl. 162(August)(2020)113864,http://dx.doi.org/10.1016/j.eswa.2020.113864.
88. Y. Zhang, D.-W. Gong, and J. Cheng, ''Multi-objective particle swarm optimization approach for cost-based feature selection in classification,'' IEEE/ACM Trans. Comput. Biol. Bioinf., vol.14, no. 1, pp. 64–75, Jan. 2017.
89. Zhang Z,Shen H, Sang Y. An observation-centric analysis on the modeling of anomaly-based intrusion detection.Int J NetwSecur. 2007; 4(3):292-305.https://doi.org/10.6633/IJNS.200705.4(3).08.
90. Chen, et al., Machine learning-enabled IoT security: Open issues and challenges under advanced persistent threats, ACM Comput. Surv.(2022)1–35, http://dx.doi.org/10.1145/3530812./.