Journal of Education for Pure Science- University of Thi-Qar
Vol.15, No. 3 (2025)
DOI: https://doi.org/10.32792/jeps.v15i3.688

Website: jceps.utq.edu.iq Email: jceps@eps.utq.edu.iq

An efficient Network Anomaly detection based on PSO-Based Wrapper Feature Selection method and Bagging Technique

Atyaf Jarullah Yaseen[1,]

Department of Computer Science , College of Computer Science and Mathematics,University of Thi-Qar

Email: atyafjarallah82@utq.edu.iq

Received 16 / 3 /2025, Accepted 5 / 8 /2025, Published 1/ 9 /2025

Abstract:

The current high demand for internet usage has led to an increased rate of attacks in different networks, which is a major concern for cybersecurity. To complement cloud computing, fog-computing offers low-latency services to cloud and moving users. However, fog devices might face security-related challenges regarding their adjacency to end users and insufficient computational power. Moreover, most common network threats may lead to the compromise of fog computing systems. Despite extensive research on applying intrusion detection systems (IDS) in traditional networks, it may not be appropriate to immediately apply them to the fog-computing. Developing efficient intrusion detection system that can handle massive databases is important in fog computing, as fog nodes generate large volumes of data. To combat network attacks, intrusion detection systems could be deployed in fog computing, which use machine learning (ML) methods to detect network anomalies and classify threat events, proving to be effective and efficient. The present research presents a novel approach based on Particle Swarm Optimization (PSO) and Wrapper-Based feature selection and also Bagging technique for detecting intrusion in a fog-environment, using the Knowledge Discovery Dataset from Security Laboratory (NSL-KDD). This approach reduces time complexity and produces a more accurate model for outcome prediction. The outcomes demonstrate that the presented methodology outperforms related methods from related literature, achieving an overall 98.99% accuracy and 1.5% false positive (FP) rate.

Keywords: Particle Swarm Optimization, Bagging technique, Machine learning.

1-Introduction

The Internet, considered one of the most critical inventions in the history, has rapidly expanded to impact various sectors such as travel, business, research, and education. Among the newer and mostly employed applications of the Internet is the Internet of Things (IoT). The development of affordable and efficient devices such as sensors, actuators, and other similar gadgets, combined with various communication channels, has resulted in the IoT's emergence which evolved the industry sector during the recent 10 years. Nowadays, IoT devices are prevalent, and by 2020, it is predicted that over fifty billion IoT-based gadgets will be linked to the Internet, according to Cisco [1-3].

The application of the Internet of Things (IoT) has led to the creation of smart environments such as smart cities, smart grids, and smart homes, with the intention of improving human comfort and wellbeing. For instance, the city of Padua in Italy serves as a good example of a smart city [4]. The IoT has become prevalent in various sectors, including education, healthcare, energy distribution, and transportation. However, the constant collection and transmission of personal data by IoT devices make them vulnerable to intrusion by attackers, who may disrupt their normal operations, leading to fatal consequences. In 2016, the Mirai-type virus focused on Dyn, a supplier of Domain Name System (DNS), causing a far-reaching effect on IoT-based gadgets in smart situations [5]. Cyberattacks including Denial of Service (DoS) and malicious control pose significant threats to the functionality and reliability of smart environments based on IoT.

IoT devices have limitations in areas such as memory capacity, network bandwidth, computational power, and battery life. Standard intrusion detection systems (IDSs) are not applicable to IoT networks, thus specialized and reliable IDSs must be designed for this purpose. IDS is a hardware or software that monitors traffic data in order to prevent intrusions that can compromise the confidentiality, availability, and integrity of an information system. IDSs can be categorized into two major groups: Signature-based intrusion detection systems (SIDSs) and Anomaly-based intrusion detection systems (AIDSs). SIDS compares incoming traffic against a database of well-known attack signatures, and alerts the administrator if a match is found. Conversely, AIDS works by establishing a model of normal user system behavior. The basic notion is that dangerous procedures differ from normal user behavior. Because pre-defined attack signatures cannot be relied upon due to the heterogeneity and variety of IoT devices, the use of SIDS in IoT networks is limited [6].

To secure IDS models based on IoT, a centralized cloud-based security system is commonly used by most service providers. However, this approach faces challenges in handling the vast amounts of produced data by a multitude of IoT-based devices, such as limitations in data transmission capacity, power usage, memory utilization, and latency. Decentralized IoT systems based on opportunistic networks are particularly vulnerable to threats. Given the dispersed nature of IoT, a distributed security model that offers flexibility, scalability and interoperability across heterogeneous devices is necessary. One possible solution is to use fog-computing in a distributed architecture, as it provides services for the purpose of computational offloading [7].

For the purpose of analyzing the generated data by IoT sensors, ML techniques are utilized along with fog nodes. The data is preprocessed using Label-One-Hot-Encoding, that reduces number of attributes and prevents income traffic. The Correlation Coefficient technique is employed for selecting features, which eliminates highly connected data from network traffic. Various databases, including NSL-KDD, KDDCUP99, also CICIDS-2017, are available to evaluate the effectiveness of IDS [8]. Researchers in the field of IoT security frequently use the NSL-KDD IoT-based dataset to assess the model's performance as it covers various risks based on IoT in an environment based on IoT [9].

To assess the effectiveness of the suggested approach, we have made a comparison with various classification methods. Our method provides several benefits, including applying machine learning techniques and also fog computing for analyzing the produced extensive data by IoT devices. Additionally, our approach employs the real NSL-KDD database, that includes recent IoT attacks. We have also thoroughly examined the impact of feature selection on attack detection. Furthermore, we have conducted a comprehensive investigation utilizing the 10-fold cross-validation resampling method and various indicators such as F1- score and Recall.

The subsequent section discusses related works, while sections three and four outline the suggested model and its assessment and comparison. Finally, in section five, we present our conclusions and novel directions.

2-Related Work

In recent years, a wide range of Intrusion Detection Systems (IDSs) have been developed to secure Internet of Things (IoT) networks against various types of cyberattacks. In [9], the authors simulated communication patterns of IoT devices by monitoring traffic generated by IoT services and constructed a dataset within the Distributed Smart Space Orchestration System (DS2OS) framework. They applied the BIRCH algorithm alongside K-means clustering for anomaly detection, achieving an accuracy of 96.3%, despite not incorporating any feature selection techniques to filter out irrelevant features.

In [10], a multi-method IDS approach based on several machine learning algorithms was proposed for IoT sensor networks. Among the models evaluated, Random Forest (RF) achieved the highest performance with an accuracy of 96%. The Bot-IoT dataset was used for evaluation, and the full dataset was employed in the experimental analysis. To detect anomalies within IoT backbone networks, the authors of [11] introduced a dimensionality reduction technique based on Principal Component Analysis (PCA). The reduced features were then classified using a Naïve Bayes classifier and a Certainty Factor-enhanced K-Nearest Neighbor (KNN) algorithm. This model was assessed using the NSL-KDD dataset, particularly focusing on Remote-to-Local (R2L) and User-to-Root (U2R) attacks.

In [12], a hybrid IDS architecture named PB-DID (Pattern-Based Deep Intrusion Detection) was presented to enhance network security within IoT environments. The model utilized the UNSW-NB15 dataset for training and testing, and feature selection was performed using the Information Gain method. The approach resulted in a significant improvement in both classification accuracy and attack prediction, reaching 96.3% accuracy.

For mobile IDS deployment in IoT platforms, the authors of [13] proposed a transfer learning-based approach. Their model utilized PCA for dimensionality reduction and K-means clustering in the preprocessing phase, applied to the KDDCUP99 dataset. By reducing the number of features from 41 to a range between 8 and 16, the model achieved a detection rate of 96.8% and a false alarm rate (FAR) of only 1.6%. Additionally, several studies have proposed fog-based IDS architectures that offload computational tasks to fog nodes for increased efficiency.

In [14], a cognitive fog-computing approach for IDS was introduced, which detects malicious activity at local fog nodes rather than relying on centralized cloud resources. Summaries of the local fog nodes are stored in the cloud for subsequent evaluations. The model was evaluated using the NSL-KDD dataset, and a hybrid ensemble classifier comprising Deep Neural Network (DNN), Random Forest (RF), and Extra Trees (ET) was employed for attack detection.

The authors of [15] addressed the problem of on-off attacks in wireless sensor networks (WSNs), commonly found in industrial IoT systems. They proposed an Artificial Neural Network (ANN)-based IDS capable of detecting malicious nodes that behave normally in their off state but act destructively when turned on.

A distributed IDS leveraging deep learning was introduced in [16], showing that threat detection within fog environments provides greater scalability compared to centralized cloud solutions. The model was evaluated using multiple benchmark datasets, including NSL-KDD, Bot-IoT, KDDCup99, and CICIDS-2017.

In [17], an IDS tailored for detecting Denial of Service (DoS) attacks in IoT environments was proposed using a Deep Belief Network (DBN). Similarly, the work in [18] presented a deep neural network-based IDS, evaluated on both the NSL-KDD and UNSW-NB15 datasets, achieving accuracies of 95.40% and 91.20%, respectively. Finally, in [19], the authors proposed a permissioned blockchain-based IDS designed to detect Distributed Denial of Service (DDoS) attacks. Their model demonstrated a lower false positive rate and improved detection accuracy compared to conventional IDS approaches.

3- Proposed Method

In this work, an effective method for detecting network anomalies is presented based on the PSO-based Wrapper feature selection method and the Bagging technique. The diagram of the proposed method is shown in Figure 3. The feature selection method based on wrapper, as represented in figure 1, employs PSO to explore the feature space and find a good subset of features that can improve the performance of the classifier. The Bagging classifier is used in combination with PSO to further improve the feature selection process. Bagging is a well-known ensemble learning technique that can reduce the variance of the model by training multiple instances of the classifier on different subsets of the training data. Overall, the suggested model aims to enhance the classification process by choosing a good set of features that can reduce noise and improve the discriminative power of the model. The use of PSO and Bagging can help achieve this goal by exploring the feature space more effectively and reducing the variance value. Fig. 1 illustrates the functioning of the suggested method.

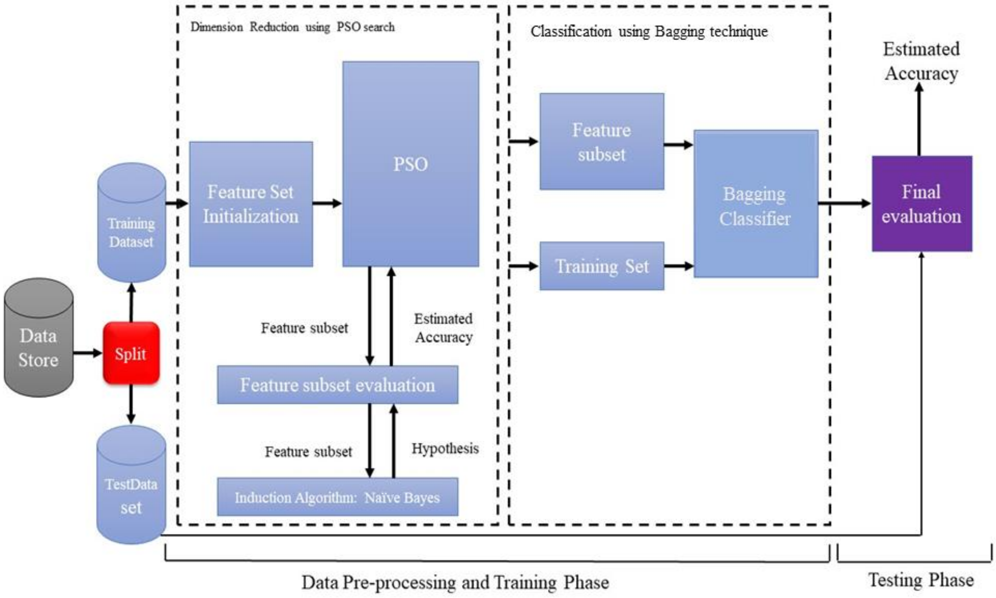
Dimension Reduction using PSO search
Classification using Bagging technique
Estimated Accuracy
Training Dataset
Feature Set Initialization
PSO
Feature subset
Bagging Classifier
Final evaluation
Training Set
Data Store
Split
Feature subset
Estimated Accuracy
Feature subset evaluation
Feature subset
Hypothesis
TestData set
Induction Algorithm: Naïve Bayes
Data Pre-processing and Training Phase
Testing Phase

Figure 1. Proposed method frame work.

3.1 PSO/wrappers based selecting features

In this study, the Particle Swarm Optimization (PSO) algorithm is employed as a wrapper-based method to identify the optimal subset of features for anomaly detection. PSO is indeed a popular optimization algorithm that can be used for feature selection. It works by iteratively updating the positions and velocities of particles swarm in order to search for the best solution in a given search space. In the context of feature selection, the particles represent different feature subsets, and the fitness function evaluates the quality of each subset based on a specified evaluation metric, such as accuracy, AUC, or F1 score. The algorithm begins by initializing a swarm of candidate solutions, where each particle represents a potential feature subset. The representation format of each particle (e.g., binary, character, or integer) is determined based on the characteristics of the NSL-KDD dataset and the structure of its features. Each particle's quality is assessed using a fitness function designed to evaluate classification performance. If a particle's current fitness exceeds its previously recorded best fitness, the new value is retained as its personal best. Simultaneously, the global best particle across the entire swarm is updated accordingly. The positions and velocities of the particles are iteratively updated based on both individual and global bests, as detailed in Algorithm 1. This process continues until the maximum number of iterations is reached or convergence is achieved. After applying PSO-based dimensionality reduction, the feature set was effectively reduced to optimum informative features from the original NSL-KDD dataset. Figure 2 shows a detailed diagram of the PSO-based wrapper feature selection method.

Algorithm 1 Pseudocode of PSO algorithm

```
Input: Dataset; Initialize parameter; Maximum number of iterations: $T_{max}$
Output: Relevant subset features
Initialize each particle and its velocity $V$ and location $X$;
repeat
    for each particle $i$ do
        calculate the fitness value $f_i$ of particle $i$;
        if $f_i < f_{pbest_i}$ Then
            $pbest_i = X_i$;
        end
        if $f_i < f_{gbest}$ Then
            $gbest = X_i$;
        end
        update $X_i$ and $V_i$;
    end
until $T_{max} = max$ or $f_{gbest} = 0$;
Return $gbest$
```

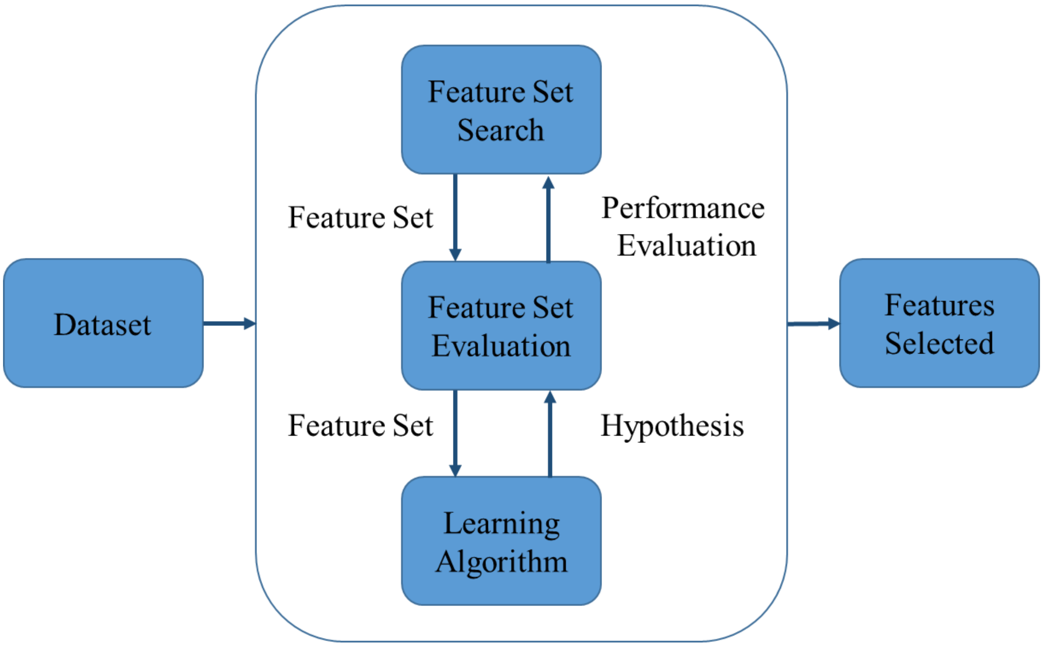

Figure 2. Choosing features using a wrapper strategy.

3.2 Bagging technique

In the bagging method, which is used in this work to anomaly detection, a subset of the original data is sent to each classifier. This means that each classifier observes a part of the data set and builds its model according to the subset it has. Selection of this subset is associated with substitution. Based on this, each sample can be selected several times. The conducted research has shown that the classification method can increase the ability to learn and recognize with higher accuracy on all types of data [20]. Figure 3 shows the overall performance of this method for classifying and detecting network anomalies using the bagging technique.

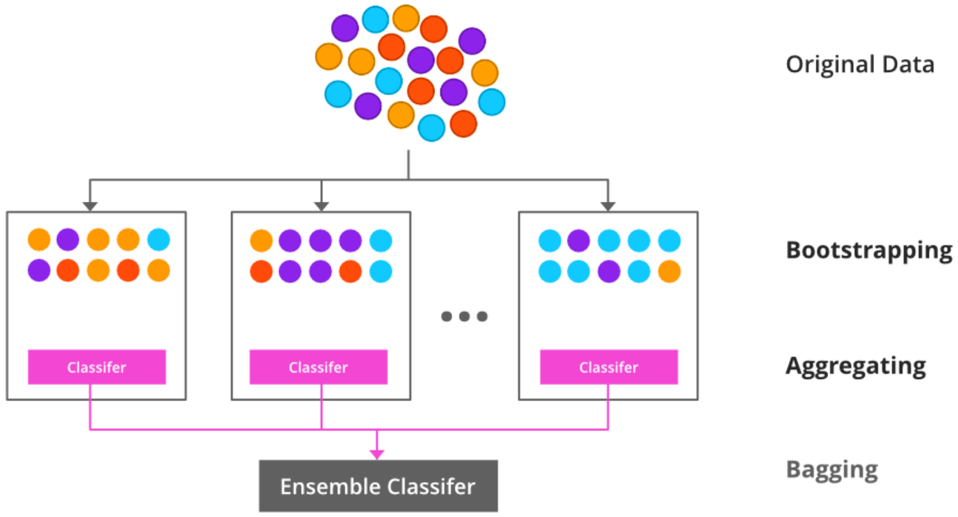

Figure 3. Classification diagram using Bagging algorithm

4- Experimental Results

In this study, the NSL-KDD database was utilized for evaluating the proposed model. the dataset comprised 25,192 instances with 41 attributes and also four different types of attack (Probing, DoS, R2L, and U2R), along with a normal class label. The whole number of attack and normal instances for every fold of training and test data is provided in Tables one and two. Also to prevent overfitting of the classification model, 10-fold cross-validation, a commonly used strategy, was employed for all tests.

In order to prevent the model from being complicated and minimize errors, three pre-processing stages were conducted. The first stage involved converting string features into numerical values. The second stage involved data normalization to decrease the range of attribute values. This was done to ensure that features with lower values were not overshadowed by those with higher values. One-standard deviation normalization technique and zero mean has been employed in the proposed model. In the third stage of our pre-processing, we aimed to tackle the class imbalance issue present in the NSL-KDD database, which is evident in Table 1. As a result of this imbalance, the model may incorrectly categorize U2R and R2L groups. To overcome the raised challenge, we utilized Synthetic Minority Oversampling (SMOTE) to level the dataset, as shown in Tables two and three.

Our model was able to detect uncommon types of threats in the training data, while identifying known threats in the testing data. DOS, Probe, U2R, and R2L attacks were among the important types of attacks identified in two datasets of training and test. the instances of attacks in the dataset with all their details is described in table 3.

Table 1. type of attacks in the KDD-train dataset

Types of Attack	Samples number
Normal	67343
DoS	45927
Probe	11656
R2L	995
U2R	52
Total	125973

Table 2. type of attacks in the KDD-test dataset

Types of Attack	Samples number
Normal	9711
DoS	7452
Probe	2421
R2L	2756
U2R	200
Total	22544

Table 3. instances of attacks in the dataset with all their details

Types of Attack	Dtails
DoS	Back, Smurf, Neptune, Land, Teardrop, Pod, Mailbomb, Udpstorm, Aache2, Processtable, Worm.
Probe	Satan, Saint, Portsweep, IPsweep, Mscan, Namp.
R2L	Ftp_write, Multihop, Guess_Password, Xlock, lamp, Xsnoop,Snmpguess, Phf Httptunnel, Snmpgeattack, Sendmail,Warezmaster, Named.
U2R	Buffer_overflow, Xterm, Rootkit, Perl, Loadmodule Sqlattack Ps

4.1 Assessment Criteria

The efficiency of the presented method is assessed using several metrics, including execution time, F1 score, accuracy, and precision. These measures are specified in the following:

(1) F1- score: The dataset is divided into two groups, normal and abnormal, and there are 4 possible classes: True Positive, False Positive, False Negative, and True Negative. The F1 score represents a measure of the accuracy of the classification, with positive samples representing the normal class and negative instances representing the abnormal class. Table four displays the corresponding values for these categories.

(2) True Positive: It is determined which normal occurrence is in question.

(3) False Positive: An unusual event is mistakenly classified as normal.

(4) False Negative: Mistaking an instance of regular behavior for an aberrant one.

(5) True Negative: It is known which anomalous situation applies.

Precision is a measure of how many relevant examples there are among the detected instances (P). The formula below may be used to compute P:

$$P=TP/(TP + FP) \tag{9}$$

The definition of recall is the proportion of related instances that are selected, as compared to whole related samples. (R). The formula below may be used to compute R:

$$R=TP/(TP + FN) \tag{10}$$

While P and R indications may sometimes be inconsistent, the F1 score is the most often used assessment indicator. The formula below is utilized for calculating the weighted-average of recall and precision, also known as F1 -score:

$$F1\ score =2PR/((P+R)) \tag{11}$$

(2) The duration of the computation required for the IDS detection method is referred to as the "calculation time". The amount of time needed for the initial computation of the suggested technique can be seen in Figure 1, which depicts the detection time.

4.2 Evaluation of the proposed method

Figure 4 illustrates the True Positive Rate (TPR) and False Positive Rate (FPR) of the proposed method in detecting each class. As shown in the figure, the "Normal" class achieves the highest TPR of 99.89% and the lowest FPR of 0.11%. The numerical results corresponding to this chart are presented in Table 4. In this table, the average TPR and FPR across all classes are reported as 98.5% and 1.5%, respectively, indicating the effectiveness of the proposed method in network anomaly detection.

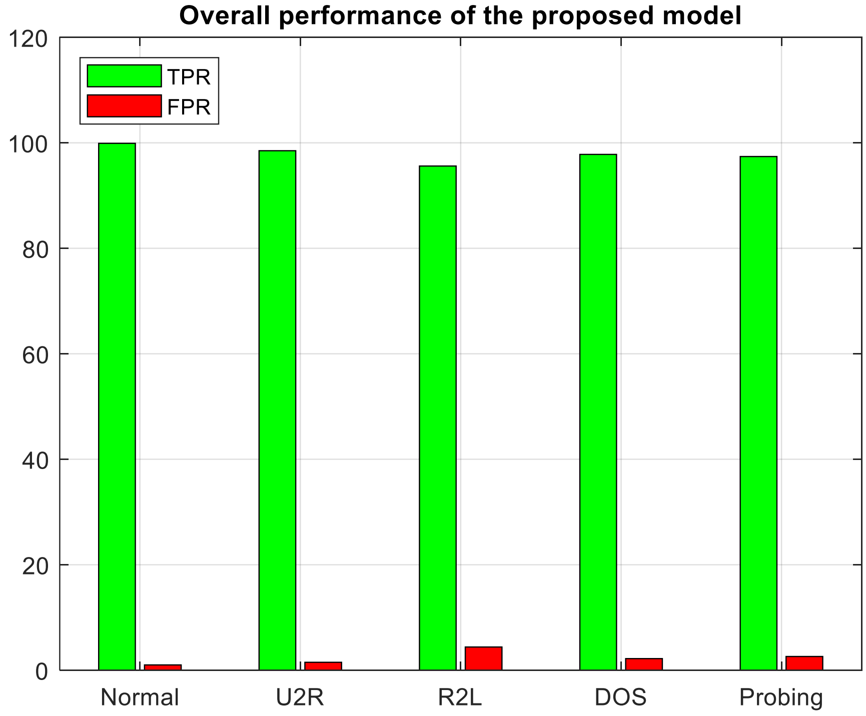

Figure 4. The overall performance of the suggested method

Table 4. the proposed model evaluation metrics

Class	True Positive Rate (TPR)%	False Positive Rate (FPR)%
Normal	99.89	0.11
DoS	98.6	1.4
Probe	95.7	4.3
R2L	97.9	2.1
U2R	97.5	2.5
Average Weight	98.5	1.5

The performance of the proposed method in terms of Accuracy and Precision is compared with other methods in Table 5. As can be observed, the proposed method achieves the best performance, with an Accuracy of 98.9% and a Precision of 99%. In contrast, the Bayesian Network method demonstrates the weakest performance, with an Accuracy of 86% and a Precision of 92%. To facilitate visual comparison, the results of this table are also presented as a bar chart in Figure 5.

Table 5. results comparison of different methods

Algorithms	**Bayesian network**	**J48**	**SMO**	**Proposed model**
Accuracy	0.86	0.97	0.96	0.989
Precision	0.92	0.97	0.98	0.99

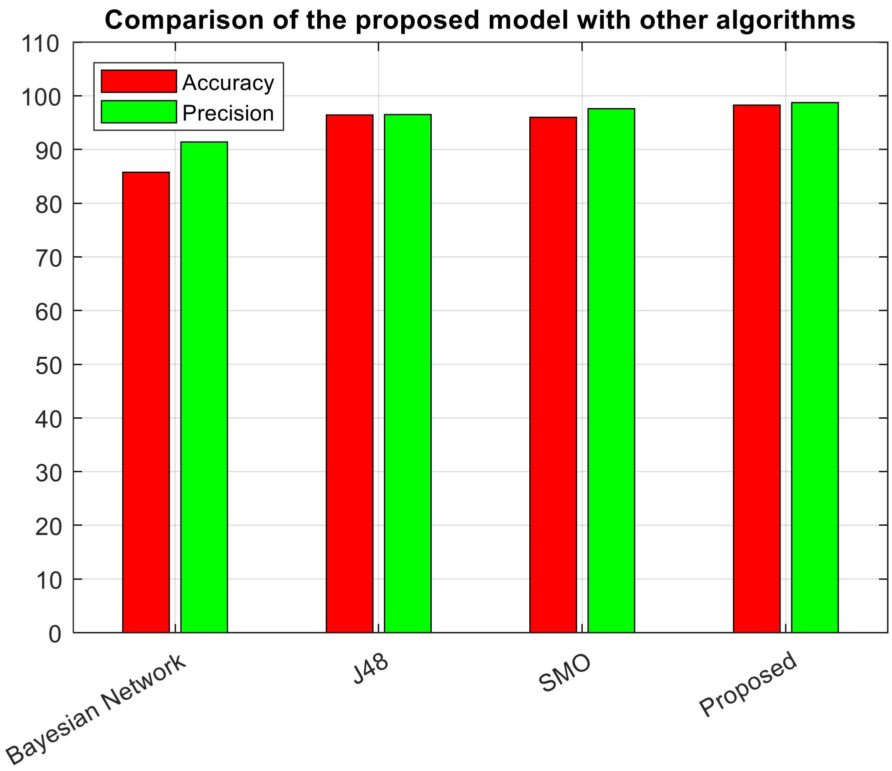

Figure 5. Comparing the results of the suggested model with various techniques

4.3 Performance evaluation of the proposed feature selection method

Table 6 presents a comparison of the performance of the proposed method with and without using the optimal features selected by the feature selection algorithm introduced in this study, in terms of Accuracy and Precision. As observed, using all features yields an Accuracy of 92.68% and a Precision of 92.05%. In contrast, when using the selected features obtained through the proposed feature selection method, these metrics increase to 98.99% and 98.10%, respectively. This clearly indicates an improvement in the performance of the proposed method through the use of optimized features. The visual representation of these results is provided in the form of a bar chart in Figure 6.

Table 6. Comparing the features in the whole dataset and features selected according to Accuracy and Precision

NSL-KDD Database	**Acc**	**Precision**
Total Features	92.68	92.05
8 Selected Features	98.99	98.10

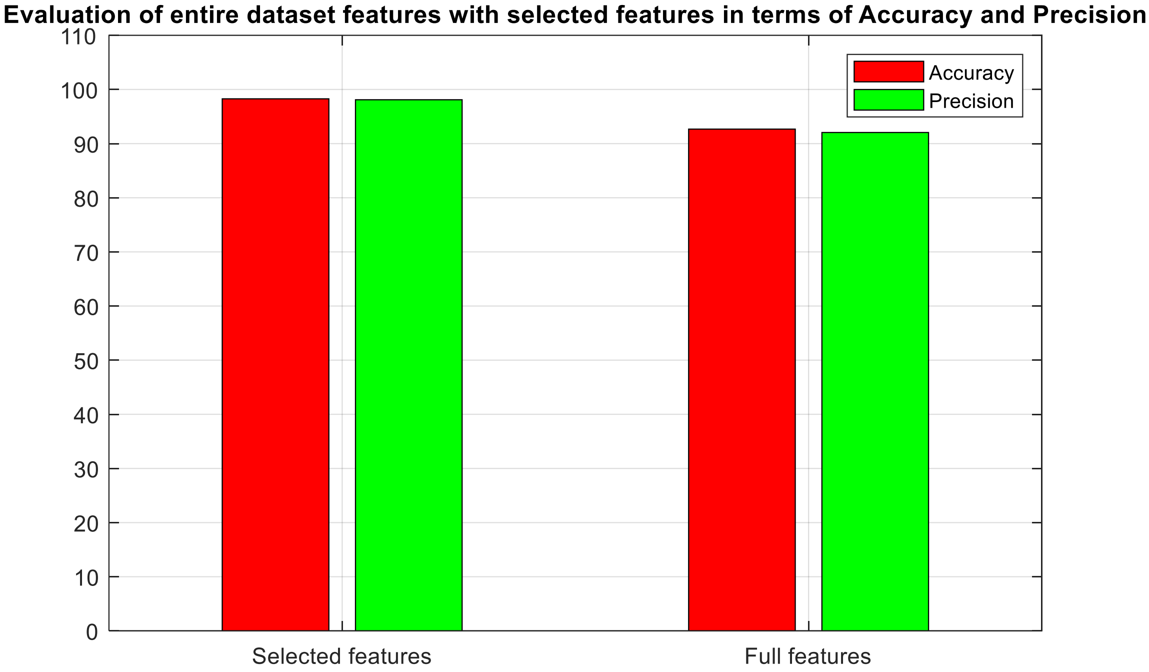

Figure 6. Comparing total dataset features and the Accuracy/Precision-based features

Also, table 7 compares the performance of the proposed method in terms of Accuracy with other feature selection techniques. The table reports the feature selection methods, the number of selected features, and the Accuracy achieved by each method. As shown in this table, the proposed method demonstrates a significant advantage with an Accuracy of 98.99%. In addition, Accuracy and Precision of the proposed method with and without feature selection are presented in Table 8. As observed, applying optimal feature selection has led to improvements in both metrics. The visual representation of these results is provided in the form of a bar chart in Figure 7.

Table 7. suggested wrapper method is contrasted with earlier techniques for feature selection.

Feature Selection techniques	Number of Selected Feature	Accuracy
BestFirst+ConsistencySubsetEval	9	97.00
GeneticSearch+CfsSubsetEval	23	91.20
GreedyStepwise+CfsSubsetEval	11	92.80
RankSearch+CfsSubsetEval	14	94.90
RankSearch+ConsistencySubsetEval	26	93.15
Nil	41	92.70
Presented Method	8	98.99

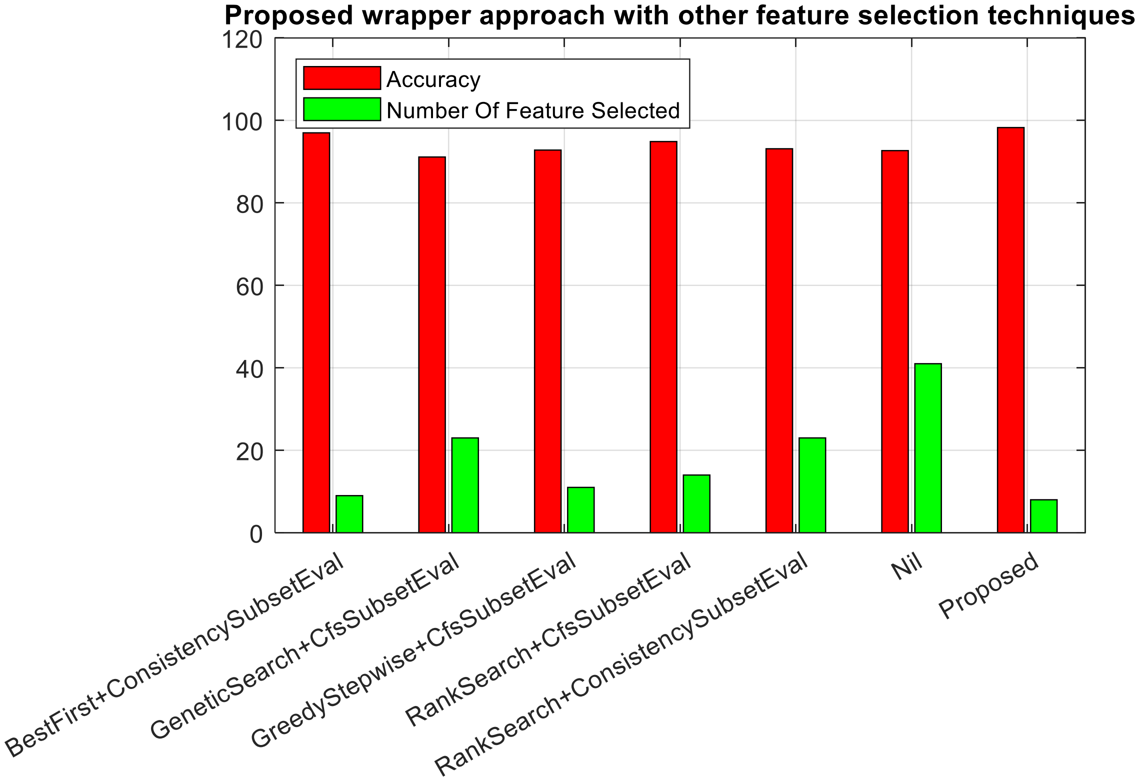

Figure 7. Results comparison between the presented model and various feature-selection techniques

As demonstrated by the results, the proposed method outperforms other algorithms in terms of accuracy due to the optimal feature selection performed by a wrapper-based method utilizing the Particle Swarm Optimization (PSO) algorithm. The selection of optimal features using the proposed approach contributes to dimensionality reduction by eliminating irrelevant and redundant features, thereby reducing the size of the search space. With lower dimensionality, the proposed model can learn more efficiently and effectively, as it becomes more focused on the actual data patterns and less affected by noise. This, in turn, enhances the model's generalization capability and helps prevent overfitting. Moreover, optimal feature selection leads to reduced model complexity, which not only improves performance but also enhances interpretability.

4.4 Comparing of the results

According to Table 8, this research project outperforms other relevant investigations in terms of accuracy. Moreover, Table 9 shows that the suggested technique performs better compared to various techniques in this field based on F-score metric.

The superiority of the proposed method over existing approaches is attributed to its hybrid architecture, which combines Particle Swarm Optimization (PSO)-based wrapper feature selection with the Bagging ensemble learning technique. The PSO-based wrapper method performs a guided search through the feature space by directly optimizing the classification performance, enabling the selection of an optimal subset of relevant and non-redundant features. Unlike traditional filter methods that evaluate features independently of the learning algorithm, the wrapper approach takes into account interactions among features and their collective impact on the classification process. This leads to more effective dimensionality reduction, which in turn lowers the computational complexity, enhances learning efficiency, and improves the model's ability to focus on informative patterns while mitigating the influence of noisy or irrelevant data.

In addition to feature optimization, the proposed method benefits from the Bagging ensemble strategy, which builds multiple base classifiers on different bootstrap samples of the training data and aggregates their outputs. This reduces the variance of individual models, improves generalization, and enhances robustness against overfitting—especially in the presence of imbalanced or complex data distributions. The integration of these two complementary techniques significantly improves anomaly detection performance, achieving higher detection accuracy and lower false positive rates compared to several state-of-the-art methods evaluated on the same benchmark datasets.

Table 8.
Assessment of the proposed approach utilizing data from pertinent research

Author	Method	Acc
Rahman et al. [21]	GAN-KNN	84.00
Xu et al. [22]	Bi-directional-GAN	91.00
Silivery et al. [23]	RNN	98.68
Silivery et al. [23]	DNN	98.95
Sun et al.[24]	KNN	92.00
Sun et al.[24]	Adaboost	98.50
Presented Method	Wrapper Based PSO + Bagging Classifier	98.99

Table 9. Comparison of the stated and alternative techniques using the F-score standards

Attacks	SVM	Random forest	Decision tree	Proposed model
Normal	0.93	0.99	0.99	0.99
DoS	0.96	0.99	0.99	0.99
Probe	0.40	0.94	0.94	0.98
R2L	0.88	0.99	0.99	0.96
U2R	0.61	0.85	0.79	0.79

5- Conclusion and future works

The utilization of PSO and Bagging techniques in fog-computing environments presents a novel approach for detecting network intrusions. Presented method is on the basis of bagging method and a wrapper feature selection method. In this way, in order to prepare the database, among the original 41 characteristics, 8 features were changed to new features, and the data has been sorted using the Bagging technique. The suggested method demonstrated 98.99% accuracy and 1.6% false positive rate (FPR), surpassing the performance of existing classifiers. Moreover, the F-scores for Decision Tree and Random Forest algorithms were observed to be significantly higher than those of SVM. The wrapper approach shows a high potential for detecting anomalous intrusions when applied to suitable features.

References

[1] Krishnamoorthy, S., Dua, A., & Gupta, S. (2023). Role of emerging technologies in future IoT-driven Healthcare 4.0 technologies: A survey, current challenges and future directions. *Journal of Ambient Intelligence and Humanized Computing*, *14*(1), 361-407.

[2] Ashok, K., & Gopikrishnan, S. (2023). Statistical analysis of remote health monitoring based IoT security models & deployments from a pragmatic perspective. *IEEE Access*, *11*, 2621-2651.

[3] Douiba, M., Benkirane, S., Guezzaz, A., & Azrour, M. (2023). An improved anomaly detection model for IoT security using decision tree and gradient boosting. *The Journal of Supercomputing*, *79*(3), 3392-3411.

[4] Casillo, M., Colace, F., Lorusso, A., Marongiu, F., & Santaniello, D. (2022). An IoT-based system for expert user supporting to monitor, manage and protect cultural heritage buildings. In *Robotics and AI for Cybersecurity and Critical Infrastructure in Smart Cities* (pp. 143-154). Cham: Springer International Publishing.

[5] Kumar, S., & Chandavarkar, B. R. (2023, January). Analysis of mirai malware and its components. In *Machine Learning, Image Processing, Network Security and Data Sciences: Select Proceedings of 3rd International Conference on MIND 2021* (pp. 851-861). Singapore: Springer Nature Singapore.

[6] Mohy-Eddine, M., Guezzaz, A., Benkirane, S., & Azrour, M. (2023). An efficient network intrusion detection model for IoT security using K-NN classifier and feature selection. *Multimedia Tools and Applications*, *82*(15), 23615-23633.

[7] Ngo, D. M., Lightbody, D., Temko, A., Pham-Quoc, C., Tran, N. T., Murphy, C. C., & Popovici, E. (2022). HH-NIDS: Heterogeneous hardware-based network intrusion detection framework for IoT security. *Future Internet*, *15*(1), 9.

[8] Mahamat, M., Jaber, G., & Bouabdallah, A. (2023). Achieving efficient energy-aware security in IoT networks: a survey of recent solutions and research challenges. *Wireless Networks*, *29*(2), 787-808.

[9] Reddy, D. K., Behera, H. S., Nayak, J., Vijayakumar, P., Naik, B., & Singh, P. K. (2021). Deep neural network based anomaly detection in Internet of Things network traffic tracking for the applications of future smart cities. *Transactions on Emerging Telecommunications Technologies*, *32*(7), e4121.

[10] Pavaiyarkarasi, R., Manimegalai, T., Satheeshkumar, S., Dhivya, K., & Ramkumar, G. (2022, April). A Productive Feature Selection Criterion for Bot-IoT Recognition based on Random Forest Algorithm. In *2022 IEEE 11th International Conference on Communication Systems and Network Technologies (CSNT)* (pp. 539-545). IEEE.

[11] Jafer, S. H. (2022, August). Optimize network intrusion detection system based on PCA feature extraction and three naïve bayes classifiers. In *Journal of Physics: Conference Series* (Vol. 2322, No. 1, p. 012092). IOP Publishing.

[12] Zeeshan, M., Riaz, Q., Bilal, M. A., Shahzad, M. K., Jabeen, H., Haider, S. A., & Rahim, A. (2021). Protocol-based deep intrusion detection for dos and ddos attacks using unsw-nb15 and bot-iot data-sets. *IEEE Access*, *10*, 2269-2283.

[13] Deng, L., Li, D., Yao, X., & Wang, H. (2019). Retracted article: mobile network intrusion detection for IoT system based on transfer learning algorithm. *Cluster Computing*, *22*(Suppl 4), 9889-9904.

[14] De Souza, C. A., Westphall, C. B., & Machado, R. B. (2022). Two-step ensemble approach for intrusion detection and identification in IoT and fog computing environments. *Computers & Electrical Engineering*, *98*, 107694.

[15] Farea, A. H., & Küçük, K. (2021). Enhancement trust management in iot to detect on-off attacks with cooja. *International Journal of Multidisciplinary Studies and Innovative Technologies*, *5*(2), 123-128.

[16] Fatani, A., Abd Elaziz, M., Dahou, A., Al-Qaness, M. A., & Lu, S. (2021). IoT intrusion detection system using deep learning and enhanced transient search optimization. *IEEe Access*, *9*, 123448-123464.

[17] Malik, R., Singh, Y., Sheikh, Z. A., Anand, P., Singh, P. K., & Workneh, T. C. (2022). [Retracted] An Improved Deep Belief Network IDS on IoT-Based Network for Traffic Systems. *Journal of Advanced Transportation*, *2022*(1), 7892130.

[18] Sahar, N., Mishra, R., & Kalam, S. (2020, December). Deep learning approach-based network intrusion detection system for fog-assisted iot. In *Proceedings of international conference on big data, machine learning and their applications: ICBMA 2019* (pp. 39-50). Singapore: Springer Singapore.

[19] Babu, E. S., SrinivasaRao, B. K. N., Nayak, S. R., Verma, A., Alqahtani, F., Tolba, A., & Mukherjee, A. (2022). Blockchain-based Intrusion Detection System of IoT urban data with device authentication against DDoS attacks. *Computers and Electrical Engineering*, *103*, 108287.

[20] Hazim Obaid, Z., Mirzaei, B., & Darroudi, A. (2024). An efficient automatic modulation recognition using time–frequency information based on hybrid deep learning and bagging approach. *Knowledge and Information Systems*, *66*(4), 2607-2624.

[21] Rahman, S., Pal, S., Mittal, S., Chawla, T., & Karmakar, C. (2024). SYN-GAN: A robust intrusion detection system using GAN-based synthetic data for IoT security. *Internet of Things*, *26*, 101212.

[22] Xu, W., Jang-Jaccard, J., Liu, T., Sabrina, F., & Kwak, J. (2022). Improved bidirectional GAN-based approach for network intrusion detection using one-class classifier. *Computers*, *11*(6), 85.

[23] Silivery, A. K., Kovvur, R. M. R., Solleti, R., Kumar, L. S., & Madhu, B. (2023). A model for multi-attack classification to improve intrusion detection performance using deep learning approaches. *Measurement: Sensors*, *30*, 100924.

[24] Sun, Z., An, G., Yang, Y., & Liu, Y. (2024). Optimized machine learning enabled intrusion detection 2 system for internet of medical things. *Franklin Open*, *6*, 100056.