University of Ibadan
Journal of Science and Logics in ICT Research

Enhancement of Intrusion Detection Dataset in Wireless Sensor Network using RNS - Feature Conversion with Stack Ensemble Technique

[1*]Idowu, I. R. [2]Asaju-Gbolagade, A. W. and [3]Gbolagade, K. A.

[1]Federal College of Animal Health &Production Technology, Moor Plantation, Ibadan, Nigeria.
[2]University of Ilorin, Ilorin, Nigeria. [3]Kwara State University Ilorin, Nigeria

[1*]ifedotun.idowu18@kwasu.edu.ng, [2]ayisatwuraola@gmail.com, [3]kazeem.gbolagade@kwasu.edu.ng

Abstract

This research presents a feature selection and conversion technique for Wireless sensor network (WSN) for the enhancement of classification and detection of intrusions. There are many different approaches and datasets, but the performance of the current Intrusion detection systems (IDSs) does not seem to be sufficient because there are so many data volumes that need to be processed in a less ample time that it is beyond the capacity of the most widely used hardware and software tools. However, computational challenges and inadequate quality still exist in state-of-art of feature selection approaches in IDS. In order to effectively and optimally minimize the feature size of the data dimensions, the Particle Swamp Optimization (PSO) approach was presented, thereafter Residue Number System (RNS) was used to further convert the selected features from the dataset using moduli of {2(n+1) - 1, 2(n) - 1, 2(n)} to residues in order to reduce large weighted number to several small numbers and enhance the power consumption and improve the time complexity further. The outcomes demonstrate that Case 1; a composite of Z-Score, PSO, RNS, and Ensemble Classifier performed better than the case without the procedure of features conversion in Case2;(Z-Score + PSO+ Ensemble Classifier),in terms of the well-known UNSW-NB 15 dataset's classification accuracy, error rate, sensitivity, specificity, and training time. The classification accuracy shows the highest classification rate for CASE 1 to be 97.4736% and 95.3602% for CASE 2. The result shows a clear cut difference of over 2% in variation indicating the prominence of feature conversion in WSN dataset.

Keywords: *Ensemble Classifiers, Intrusion Detection System, Particle Swarm Optimization, Residue Number System, Wireless Sensor Network.*

1. INTRODUCTION

Due to development in technology, there are a number of devices connected to the Internet, which results in an increase in data traffic on the network. The Internet is now prone to more attacks with increase in the risk for network destruction and threat persistence. A solution is needed because cyber-attacks pose a serious danger of data loss and property harm. Intrusion detection systems (IDSs) can identify network threats such as denial-of-service and unauthorized access [1].WSN security is frequently provided on two levels. The first level of protection is offered to keep WSN [2]. In the first level of security, cryptographic methods and firewalls are typically used. The IDS at the second level detects infiltration and guards the network against internal attackers. There are two basic types of intrusion detection systems, signature-based IDS, which detect attacks based on established criteria and anomaly-based IDS, which detects unanticipated attacks using statistical and data mining methods [3, 4].

Hybrid, anomaly-based, and misuse-based intrusion detection systems are the most common kinds. Anomaly and misuse detection have historically been studied from two separate perspectives.

Idowu, I.R. Asaju-Gbolagade, A.W and Gbolagade, K. A. (2023). Enhancement of Intrusion Detection Dataset in Wireless Sensor Network using RNS - Feature Conversion with Stack Ensemble Technique. *University of Ibadan Journal of Science and Logics in ICT Research (UIJSLICTR),* Vol. 10 No. 1, pp. 22 – 36.

An expected pattern of typical network activity is initially established using anomaly-based detection, and anything that deviates from it is then considered anomalous. The misuse-based or signature-based system intrusion detection technique compares the activity of a potential attacker with that of a known user, in contrast to anomaly-based IDS, which has the advantage of being able to detect both known and unknown attacks but also has a significant drawback in terms of false alarms To compare against and identify prospective threats, it builds a library of recognized malicious behaviors [5, 6].

IDS often work with a large number of data comprised of a variety of traffic patterns in wireless sensor networks. A set of features is used to characterize each pattern in a dataset, which is represented as a point in a multidimensional feature space (or attributes). The redundant and irrelevant elements of a pattern may slow down the training and testing processes, and they may also affect the effectiveness of the classification by increasing the level of mathematical complexity. In reality, it is advantageous to keep the number of characteristics as little as possible in order to reduce the computing cost and complexity of developing a classifier. Moreover, selecting optimal features improves modeling, speeds up prediction accuracy, and speeds up the classification process.

Hence, dimensionality reduction approaches like feature selection and conversion employing the PSO for feature selection and RNS for feature conversion have been successfully incorporated into the machine learning task employed in this paper. The effectiveness of RNS on the top features is to reduce large weighted number to several small numbers in order to improve the time complexity and accuracy in detecting intrusions in WSN.

The novel contributions of this paper are:

i. Reduce the dimensionality of the network intrusion dataset (UNSW-NB15) through the proposed coupling of Particle Swarm Optimization feature selection with RNS conversion.

ii. Validate the best machine learning (Hybrid Ensemble method) case model from the stacked classifiers (Base: NaïveBayes, Logistic Regression, K-Nearest Neighbor and Meta: Random Forest).

iii. Conduct a comparative performance between the ensemble classifiers with and without RNS inclusive in terms of Accuracy, Detection Rate, Precision, Specificity, F-Score, Error Rate, and Training Time. The result is used to establish the efficiency of the proposed RNS- features conversion technique.

2. REVIEW OF RELATED WORKS

A survey of current studies based on the overview of datasets often used for assessment reasons and evasion tactics employed by attackers against detection was provided. It included and discussed upcoming research problems intrusion detection algorithms [7].

Feature selection (FS) based on Random Forest (RF) algorithm for lowering imbalances was conducted, furthermore the selected features of the network intrusion dataset (NSL-KDD) were also subjected to the PSO algorithm, and a comparison study using the k Nearest Neighbor (k-NN), Support Vector Machine (SVM), Logistic Regression (LR), decision tree (DT), and Naive Bayes (NB) classifiers was conducted. The results showed a reduction in the false alarm rate and an improvement in the detection rate as well as the accuracy of the IDS [8].

An edge intelligence framework was proposed that specifically performs the intrusion detection when the WSN encounters a Denial of Service (DoS) attack, the model uses the k-Nearest Neighbor algorithm (k-NN) in machine learning and the incorporation of the arithmetic optimization algorithm (AOA) in evolutionary calculation. The benchmark function test showed that the model was effective [9].

In order to propose a hybrid ensemble IDS using several IDS datasets, bootstrap aggregation, gradient boosting machine classifier, and PSO for feature selection were

used, the reduced feature subset was used as input for the hybrid ensemble [10].

Naila et al [11] proposed a stacking-based ensemble model using datasets from new generation of Internet of Things (IoT) and industrial IoT (TON-IoT (2020)), the evaluation produced best 19 features by using the chi-Square feature selection method. Comparing the suggested model to the conventional Machine Learning (ML) algorithms, considerable accuracy gains are obtained.

Principal Component Analysis (PCA) and Chinese Remainder Theorem techniques was proposed with a Naive Bayes classifier to choose features and extract features, respectively. The NSL-KDD dataset was used to train and evaluate the model [12].

Al-jarrah [13] proposed two novel feature selection methods namely Random Forest-Forward Selection Ranking (RF-FSR) and Random Forest-Backward Elimination Ranking (RF-BER). Although the 15 features selected using RF-FSR obtained higher accuracy in the cross-validation process, however the efficacy cannot be guaranteed for all cases.

Feature engineering approach was proposed in a study to improve the data distribution, the AutoEncoder(AE)- Light gradient- boosting machine (LightGBM) intrusion detection system for SDN was employed on the knowledge Discovery and Data Mining (KDDCup99) and NSL-KDD datasets. The system first employs Borderline- Synthetic Minority Oversampling Technique (SMOTE) to balance the sample distribution, then Auto Encoder (AE) to lessen the influence of redundant features, and lastly LightGBM to finish the final classification. The suggested approach performs better in real-time in terms of accuracy, precision, and F1-score [14].
Two methods of optimization for intrusion detection using NSL-KDD dataset, were suggested. First, PSO did parameter optimization using SVM to obtain the optimal values for C (cost) and g (gamma parameter), and then PSO conducted feature optimization to obtain the optimum feature. These parameters and characteristics are applied to various linear, Radial Basis Function (RBF), Gaussian, and polynomial SVM kernel functions [15].

Ariyaluran [16] analyzed how crucial it is to propose a framework that effectively handles real- time big data processing and detecting anomalies in networks. There was an attempt to address the issue of detecting anomalies in real- time and also surveyed the vital characteristics of associated machine learning algorithms.

Singh [17] presented a study based on the concept of hybridization by using two algorithms named Flower pollination Algorithm and Particle Swarm Optimization for intrusion detection systems. The author used MATLAB, which provides mathematical registration in multi-design, to simulate their work.

Several selection and classification techniques were reviewed, also testing the performance of combining two to three feature selection methods using Boolean AND was conducted. Out of the ten evaluated, Symmetric and Gain Ratio with 15 features along with instance base leaner (IBK) classifier generated the best results. However, justification on why and how random data was picked from the dataset was not made so the results cannot be reproduced [18].

A model which lowers the overall execution time was proposed with optimization algorithm as a specific factor, tasks were to be computed in a short amount of time and in turn lowers energy consumption and reduces energy usage [19].

A newly developed Ensemble Learning IDS model that uses a hybrid of Correlation and Forest Panelized Attributes (CFS-FPA) for feature selection was presented. The voting average strategy was utilized for the aggregation method, which combined the classifiers SVM, RF, NB, and K-NN. AdaBoosting, however, was used first, followed by bagging. The model's results, which were based on the intrusion detectionevaluation dataset (CIC-IDS2017), were positive [20].

These authors suggested a unique intrusion detection system by using SVM and the C4.5 decision tree technique to categorize data; NSL-KDD dataset is initially filtered using Principal Component Analysis (PCA), followed by improved PSO for feature selection. The results show high agreement when compared to the single classifier and traditional PSO approaches [21].

An ensemble model with Random Forest and Random Committee serve as the base and meta classifiers, respectively based on a Bayesian models was proposed on the unbalance data samples (KDDcup99), the proposed model was assessed using 10-fold cross-validation with accuracy and Receiver Operating Characteristics (ROC) curves as the assessment measures. For the categorization of DoS, Probe, Remote to User (R2L) and User to Root (U2R) intrusions, their model outperformed a single Bayesian model and random tree in terms of Area under Curve (AUC) [22].

Authors understudy different classification techniques for intrusion detection with KDDCup 1999 dataset. They laid emphasis on the importance of dataset for effective IDS [23]. An ensemble feature selection using deep neural network with light gradient boosting machine as its fundamental selector in particular. Series of public datasets were evaluated, and the findings demonstrate that their model's capabilities have increased its stability and resilience [24].

The proposed model with dataset UNSW-NB15 was produced by a platform known as the (IXIA) PerfectStorm software which consists of 9 contemporary types of attack and more additional normal behaviors. The properties on the dataset are divided into 5 groups known as content features, basic features, flow features, temporal features and further produced features [25].

3. RESEARCH METHODOLOGY

MATLAB 2016A was used to conduct the experimental setup based on an optimistic performance of UNSW-NB 15 WSN intrusion dataset when fed to the stack ensemble learning models necessitated multiple stages in the developed methodology, to select the best features using the computational technique as Particle Swarm Optimization method, this iteratively improves a candidate solution in relation to a given quality metric. The stages range from data acquisition, data filtering, data normalization, feature selection, feature conversion and ensemble machine learning training and classification. The frame work of the developed model is illustrated in series as given in Figure 1.

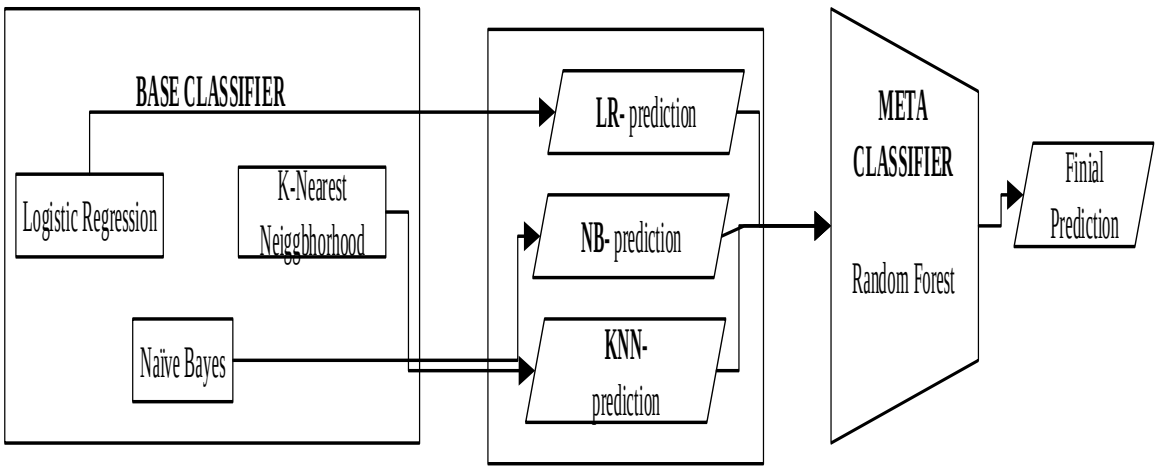

Figure 1: Schematic of a Stacking Classifier Framework

3.1 WSN Dataset Acquisition

The raw network packets of the UNSW-NB 15 dataset acquired in the Cyber Range Lab of the Australian Centre for Cyber Security (ACCS) is for generating a hybrid of real modern normal activities and synthetic contemporary attack behaviors with nine types of attacks formulated into binary class in order to become a single attack class label and the normal class is set to the non-attack class label. A total record of 82,332 observations was used from the different types, attack and normal.

3.1 Data Filtering and Pre-Processing

Pre-processing task was carried out which included eliminating any errors or outliers and irregularities present in the data. Factors like the source IP address, source port number, destination IP address, destination port number were discarded while categorical features were converted to numeric labeling.

3.2 Data Standardization / Normalization

Data Scaling is important in order to standardize datasets. At this phase, Z-score is use by measuring how far the data point is from the mean in terms of standard deviation, with this technique, it can also be determined how common or uncommon a particular data point is in a given distribution.

$$x' = (x - \mu/\sigma) \quad (1)$$

where: x: Original value, μ: Mean of data,
σ: Standard deviation of data

3.3 Feature Selection

The computational method employed is PSO based meta-heuristic algorithm which uses fitness function to select optimal features from the pre-processed dataset of 42 attributes. It solved the problem by using the collected intrusion dataset into dubbed particles, and moving these particles around in the search-space according to simple mathematical formula over the particle's position and velocity.

Each particle's movement is influenced by its local best known position, but was also guided toward the best known positions in the search-space, which was updated as better positions and found by other particles. This has moved the swarm toward the best solutions

Let x_n , v_n represent each particle's position and velocity respectively
then the population particles' position and velocity is $x_i = x_1, x_2, x_3 \ldots x_i$ and
$v_i = v_1, v_2, v_3 \ldots v_i$ respectively.

Local memory of the best initial position for each particle p_{best} is stored. Also, the global best position for each particle is $g_{best..}$ Then p_{best} and g_{best} of each particle are used to determine the subsequent best position of the particle.

Furthermore, The new position is
$x_{i+1}=x_i+v_{i+1}$ (2)

The new velocity is
$v_{i+1} = w*v_i - c_1*r_1*(p_{best} - x_i) + c_2*r_2*(g_{best} - x_i)$ (3)

Where: w is the inertia weight
c_1 and c_2 are the corresponding learning factors
r_1 and r_2 are the random numbers

Pseudo Code for the Experimental Frame work:

1. Acquire dataset P
2. Filter and Clean Dataset P
3. Project dataset P into P_Pred_factors (predicting factors) x, P_response (y).
4. Normalize Dataset P to Z using Z-score
5. Optimize Z features to get new features using PSO to return Z_New
6. Perform Feature Conversion on Z_New Data using RNS with the moduli set {2(n+1) - 1, 2(n) - 1, 2(n)} at n =2
7. Obtain Residues M1, M2, M3

8. Concatenate Residues to become N
9. Partition N in training (N_train) and testing set (N_test)
10. Project N_train into the Ensemble Classifiers
11. Train Residues against P_response(y)
12. Evaluate Classifier Performance using N_test.

Figure 2 illustrates the feature selection stage for an instance of a response variable with respect to the predicting factors.

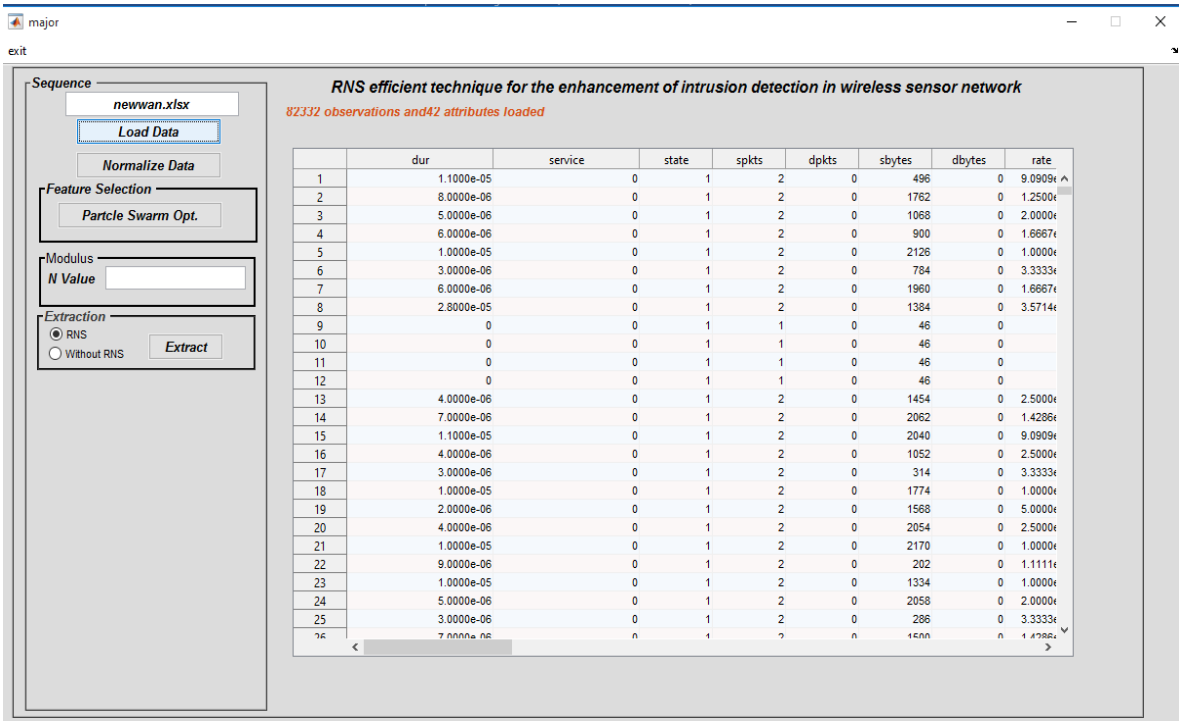

Figure 2: Feature selection of Dataset

Algorithm: Particle Swarm Optimization Method

Begin
for each particle i = 1, ..., S do
  Initialize the particle's position with a uniformly distributed random vector: **xi ~ U(blo, bup)**
  Initialize the particle's best known position to its initial position: **pi ← xi**
  if *f(pi) < f(g) then*
    update the swarm's best known position: **g ← pi**
  Initialize the particle's velocity: **vi ~ U(-|bup-blo|, |bup-blo|)**
while a termination criterion is not met do:
  for each particle i = 1, ..., S do
    for each dimension d = 1, ..., n do
      Pick random numbers: **rp, rg ~ U(0,1)**
      Update the particle's velocity: **vi,d ← ω vi,d + φp rp (pi,d-xi,d) + φg rg (gd-xi,d)**
    Update the particle's position: **xi ← xi + vi**
    if *f(xi) < f(pi) then*
      Update the particle's best known position: **pi ← xi**
      if *f(pi) < f(g) then*
      Update the swarm's best known position: **g ← pi**
End

3.4 Feature Conversion

Effectiveness of the RNS is to reduce dataset by converting large weighted number to several small numbers to enhance the power consumption and improve the time complexity further.

The RNS is of interest to researchers dealing with computationally intensive applications as it provides efficient highly parallelizable arithmetic operations. After the optimal selection of best data subset, the residue number system was used to further extract features from the dataset using moduli set of {2(n+1) - 1, 2(n) - 1, 2(n)},this is done in order to reduce over fitness and enhance the classification accuracy while reducing the training time.

The RNS uses a dynamic power range method, it operates in a way to represent integers using the values they have when divided by several, pairwise coprime integers referred to as the moduli. Chinese Remainder Theorem gives allowance to represent this, stating that if N is the product of the moduli, then there is precisely one integer inside an interval of length N that has a specified set of modular values.

If (X) is a decimal integer and $X_n = (b_{n-1}... b_1, b_0)2$ is the binary representation of X, then X modulo-m_i can be calculated using:

$$|X|m_i = |\sum_{i=0}^{n-1} bi|2|m_i| \; m_i \qquad (4)$$

Where b_i is a bit value of either 0 or 1 in the binary number system after performing modular operations. Residues are obtained as the remainders when the given number is divided by the moduli.

3.6. Ensemble Classification

The Ensemble approach resulted in multiple models combined to yield better results than a single model in a number of machine learning competitions. The predictions of multiple Base classifiers, Logistic Regression, K-Nearest Neighbors (KNN) and Naïve Bayes were stacked and used as further features to train the meta-classifier, Random Forest for the final prediction in which two cases of classification which are direct composite of the feature selection algorithm and residual number system. The first case implements the classification with the inclusion of the Residual Number System (RNS) while the other case excludes it. The PSO reduced dataset was passed into both cases for the experimental framework.

Case 1: Z-Score + PSO + RNS + Ensemble Classifier: The first case

emphasizes the inclusion of the Residual Number System, the wireless sensor network dataset was first pre-processed, then standardized using z-score, the particle swarm optimization was used for feature selection, the selected features were further processed with RNS which helps to convert the features to residues for faster data processing and enhancement, format and the stack model illustrated in figure 2 was used for classification.

Case 2: Z-Score + PSO+ Ensemble Classifier: The second case combined the Z- score, feature selection with Particle Swarm Optimization, the selected results were then introduced to the stack ensemble model. The results were evaluated for both cases and compared so as to extensively highlight the importance of residual number system on intrusion detection dataset in wireless sensor network.

4. RESULTS AND DISCUSSION

A data split of 75% to 25% was employed for the training and testing dataset respectively and series of evaluation metrics such as F-Score, Recall, Precision, Specificity, Sensitivity, Accuracy, Error rate were employed to carry out efficient rating of performance on the implemented stack ensemble model.

i. Particle Swamp Optimization Reduced Features

The PSO reduced the dataset to a total of 22 features as shown in figure 4, from an initial attribute of 42, the selected features are highlighted in table 1 with corresponding data index.

Table 1: Selected Attributes with index

No	Feature Index	Selected Features
1	41	'is_sm_ips_ports'
2	16	'dinpkt'
3	22	'dwin'
4	2	'service'
5	19	'swin'
6	20	'stcpb'
7	1	'dur'
8	14	'dloss'
9	33	'ct_src_dport_ltm'
10	18	'djit'
11	36	'is_ftp_login'
12	21	'dtcpb'
13	32	'ct_dst_ltm'
14	4	'spkts'
15	5	'dpkts'
16	38	'ct_flw_http_mthd'
17	17	'sjit'
18	10	'dttl'
19	8	'rate'
20	28	'trans_depth'
21	12	'dload'
22	13	'sloss'

ii. Converted features with RNS

Figure 5 shows the residues obtained after performing forward conversion process of the RNS module at n = 2 thereby producing the dynamic range (5, 3, and 4).

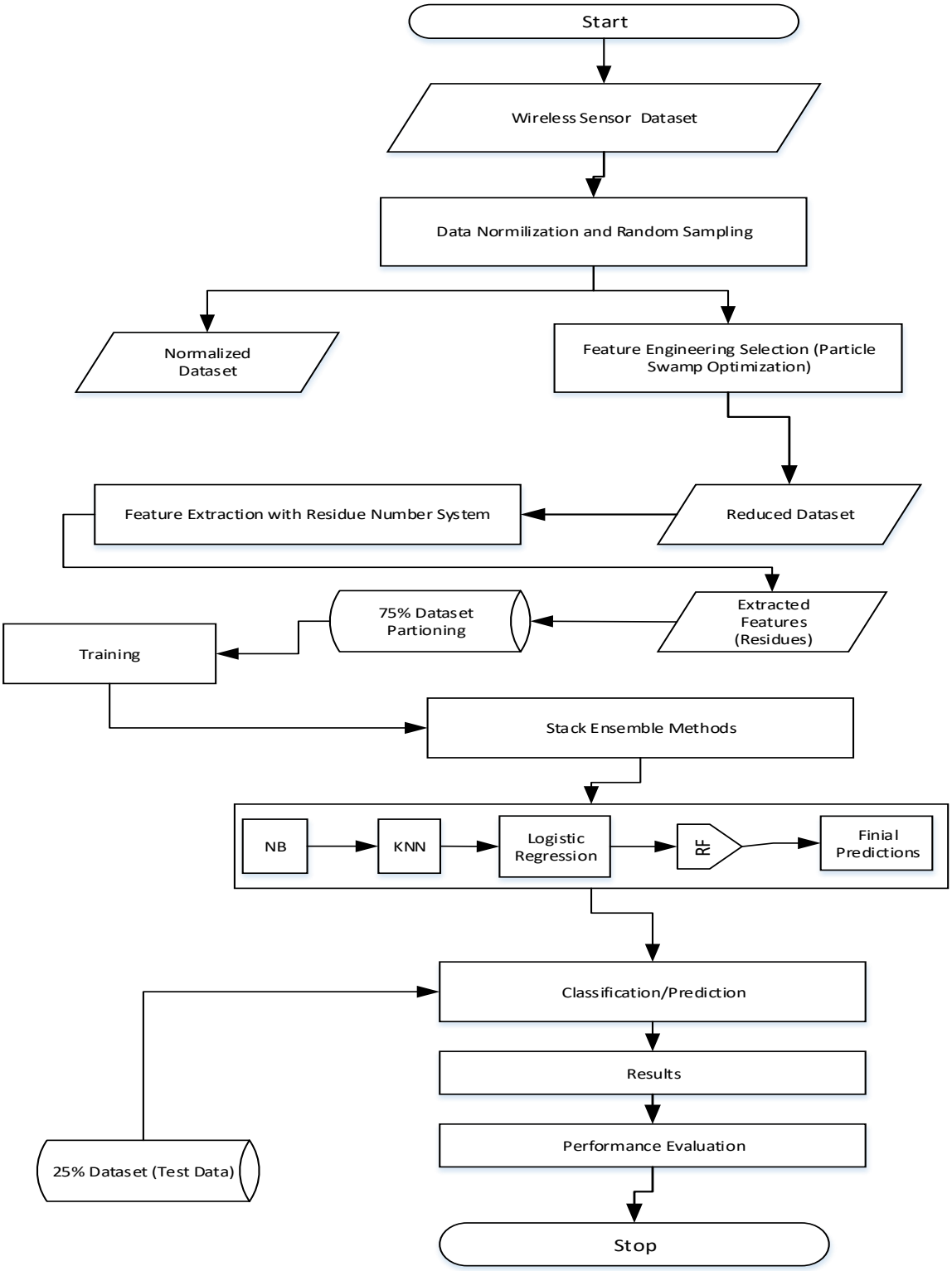

Figure 3: Flow chart of full training and testing on intrusion dataset using 75% 25% split rate

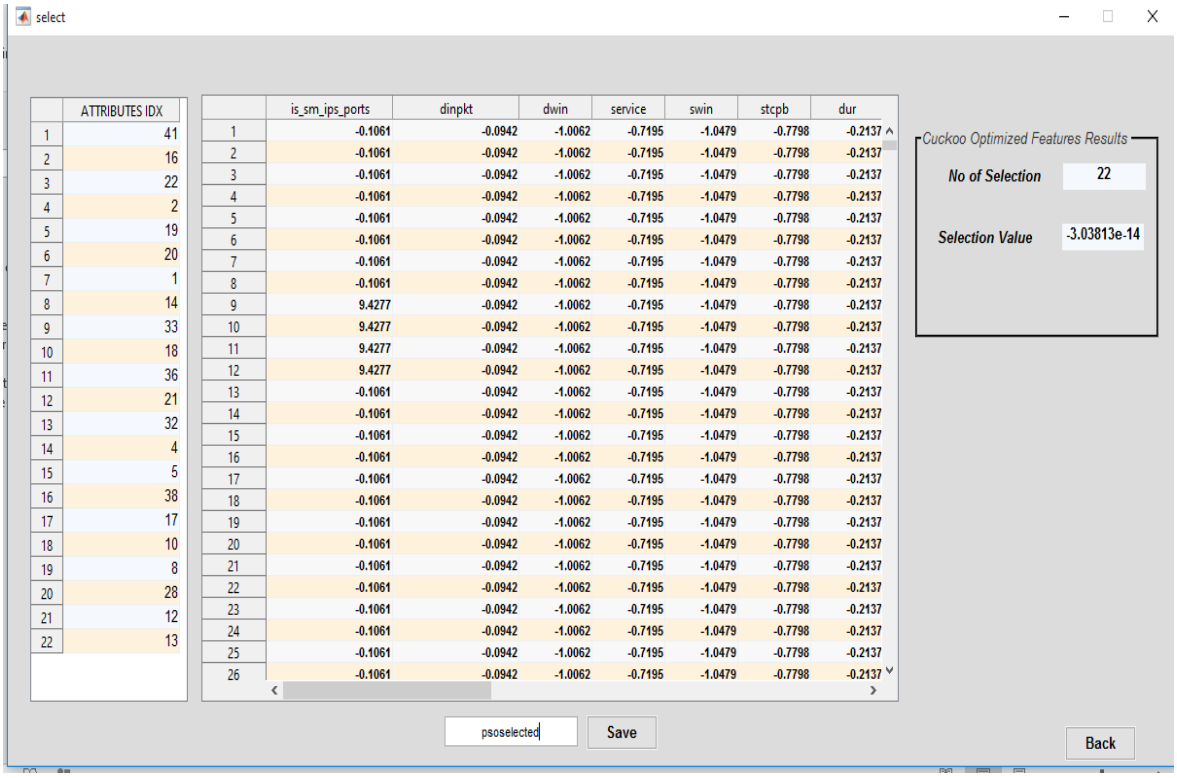

Figure 4: PSO Selected Features

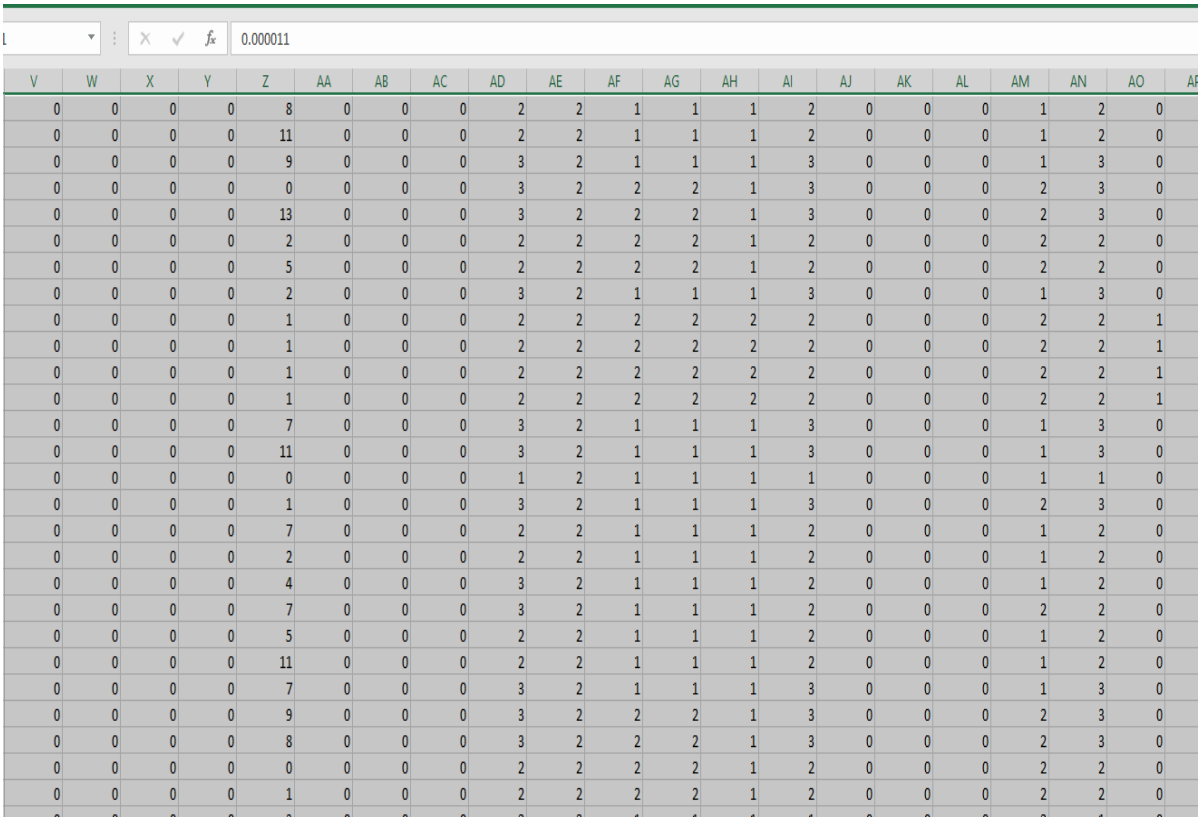

Figure 5: Features Converted into Residues

iii. Performance Evaluation

The specific performance of machine learning methods for IDS is based on the following observations to generate the performance metrics from table 2

True Positive (TP): The instance where model correctly predict as Normal
False Negative (FN): The instance where model wrongly predict an Attack as Normal.
False Positive (FP): The instance where model wrongly predict Normal as an Attack.
True Negative (TN): The instance where model correctly predicts as Normal.

Table 2: The Matrix of Prediction

Actual	Classify Normal	Classify Attack
Normal	**TP**	**FP**
Attack	**FN**	**TN**

(iv) Comparison Evaluation

The comparative result is accessed with the following performance metrics of the training time, classification accuracy, error rate, precision, f-score, specificity and detection rate for the two considered cases. Table 3 shows the comparative analysis of the two case models:
Case 1: Z-Score + PSO + RNS + Ensemble Classifier
Case 2: Z-Score + PSO+ Ensemble Classifier.

Table3: Comparative Machine Learning Evaluation for cases 1 and 2.

Technique	Detection Rate	Specificity	F-score	Precision	Error Rate	Classification Accuracy%	Training Time (sec.)
CASE 1	0.976324	0.97344	0.972016	0.967745	0.0253	97.4736	48.1264
CASE 2	0.96573	0.943704	0.949259	0.9334	0.0464	95.3602	63.2529

(a) Result Analysis for Classification Accuracy

$$\text{Accuracy} = \frac{TP+TN}{TP+TN+FP+FN} \quad (5)$$

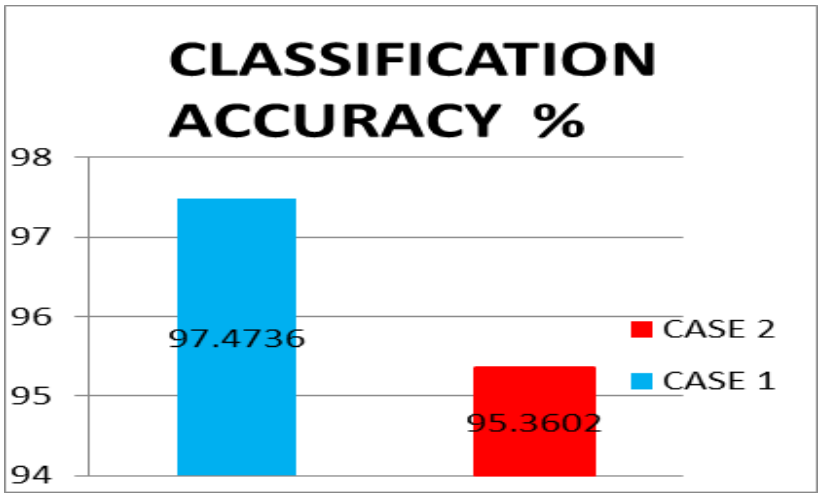

Figure 6: Comparative Classification Accuracy

The classification accuracy shows that higher classification rate was attained for the CASE 1 (Z-Score + PSO + RNS + Ensemble Classifier) with 97.4736% while 95.3602% for Case 2 (Z-Score + PSO + Ensemble Classifier) respectively. The results as shown in figure 6. There is a clear cut difference of over 2% in variation indicating the prominence of coupling PSO feature selection with RNS conversion in UNSW-NB15 dataset.

a. Result Analysis for Error Rate

$$\text{Error Rate} = \frac{FN+FP}{TP+TN+FP+FN} \quad (6)$$

Figure 7: Comparative Error Rate

The error rate shows the lowest possible error rate for any classifier in a random outcome during the classification. The Case 1 shows the lower error rate compared to Case 2, this is indicative that reduced features help to attain a very high positive rate detection and lower negative detection rate.

b. Result Analysis for Precision

$$\text{Precision} = \frac{TP}{TP+FP} \quad (7)$$

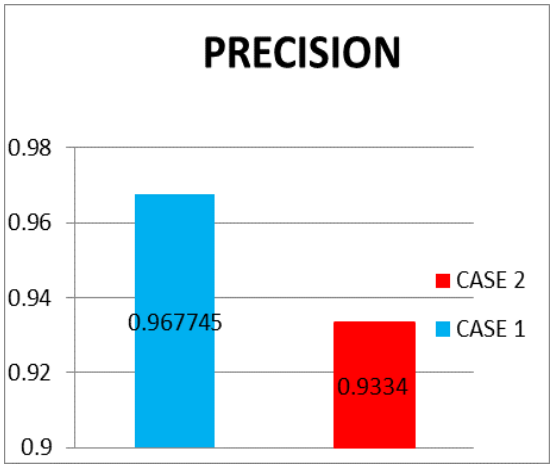

Figure 8: Comparative Precision

The higher precision value as shown in figure 8 for case 1 with RNS compared to case 2 without RNS indicates that more observations are correctly predicted over the amount of correct and incorrect predictions.

c. Result Analysis for Specificity

$$\text{Specificity} = \frac{TN}{TN+FP} \quad (8)$$

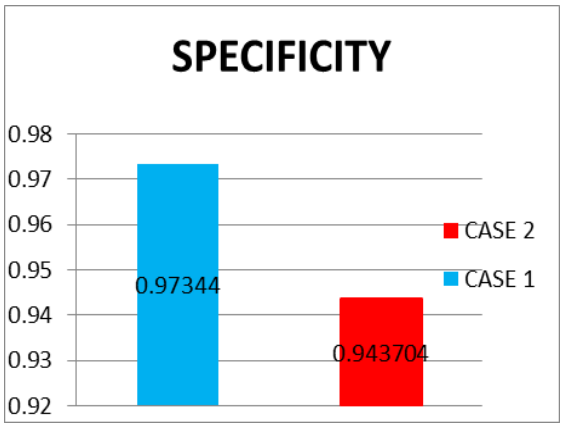

Figure 9: Comparative Specificity Analysis.

It can be deduced that the best specificity and recall fall at 1. From the obtained results, case 1 has value closer to 1 than the case 2 which is indicative that the case 1 has the better positive and negative predictive rate respectively.

e. Result Analysis for Detection Rate

$$\text{Detection Rate} = \frac{TP}{TP+FN} \quad (9)$$

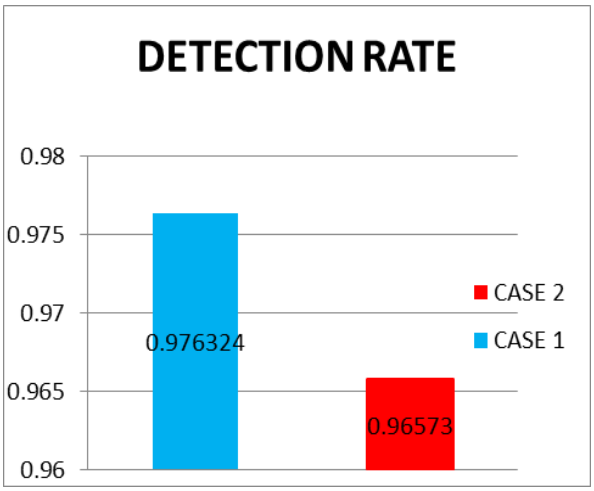

Figure 10: Comparative Detection Rate Analysis

f. Result Analysis for Training Time

The higher detection value for case 1 with RNS compared to case 2 without RNS indicates that more observations are correctly predicted over the amount of correct and incorrect predictions

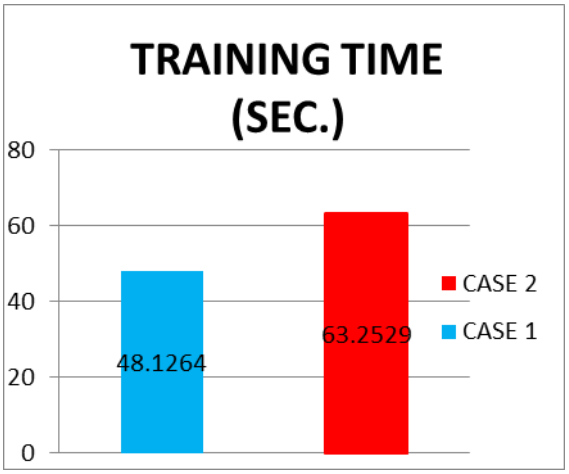

Figure 11: Training Time for models

The training time indicate the computational time taken by each case model to create knowledge retention and processing of the data supplied. RNS based for Case 1 outperformed the Case 2 with optimal time of 48.1264secs as compared to 63.2529secs for Case 2 respectively.

g. Result Analysis for F-Score

$$F - Score = \frac{2(Precision \times Recall)}{Precision + Recall} \quad (10)$$

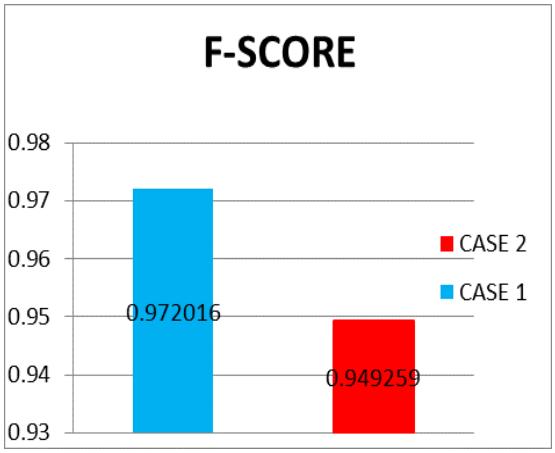

Figure 12: F- score for the models

Higher F-score value in case 1 indicates a better performance than case 2 based on the Recall and Precision as illustrated.

5. CONCLUSION

Apparently, from the experimental results, the need for feature selection and feature extraction has been justified for detection and prediction of anomalous based attack in wireless sensor network intrusion dataset, from the obtained results, it shows that the Case 1 outperformed the Case 2 with the absence of features selection in terms of the classification accuracy, error rate, sensitivity, specificity and training time with a number of 22 features optimized by the particle swarm algorithm making the data more redundant, for an efficient and suitable ensemble classification task. Therefore, the importance of feature selection and feature extraction which was achieved with particle swarm optimization and residue number system respectively cannot be withdrawn with a clear cut difference of over 7% in variation.

References

[1]. M. F. Kabir and S. Hartmann,"Cyber security challenges: An efficient intrusion detection system design," *2018 International Young Engineers Forum (YEF-ECE)*, Costa da Caparica Portugal, 2018, pp. 19-24, doi: 10.1109/YEF-ECE.2018.8368933.

[2].Abderazek Seba,N.Nouali, N.Badache, Hamida Seba..A review on security challenges of wireless communications in disaster emergency response and crisis management situations. Journal of Network and computer Applications

(JNCA), 2019, 126,pp150-161, ⟨10.1016/j.jnca.2018.11.010⟩

[3]. Smys S, Basar A, Wang H. Hybrid intrusion detection system for internet of things Journal of ISMAC (2020) Vol.02/ No.04 Pages: 190-199 http://irojournals.com/iroismac/

[4]. Maldonado, J.; Riff, M.C.; Neveu, B. A review of recent approaches on wrapper feature selection for intrusion detection. Expert System with Application, 2022,198, DOI:10.1016/j.eswa.2022.116822.

[5]. Gilberto Fernandes & Joel J. P. C. Rodrigues & Luiz Fernando Carvalho & Jalal F. Al- Muhtadi & Mario Lemes Proença "A comprehensive survey on network anomaly detection," Telecommunication Systems: Modelling, Analysis, Design and Management, Springer, 2019vol. 70(3), pages 447-489, March.

[6]. Ankit,Thakka and Ritika, Lohiya,. A survey on intrusion detection system: Feature selection, model, performance measures, application perspective, challenges, and future research directions. Artif. Intell. Rev. 55,1 (Jan 2022), 453–563. https://doi.org/10.1007//s10462-021-10037-9

[17].Khraisat, A.; Gondal, I.; Vamplew, P.; Kamruzzaman, J. Survey of intrusion detection systems: Techniques, datasets and challenges. *Cybersecurity* **2019**, *2*, 20.

[8].Kunhare, Nilesh & Tiwari, Ritu & Dhar, Joydip. (2020). Particle swarm optimization and feature selection for intrusion detection system. Sādhanā. 45. 10.1007/s12046-020-1308-5.

[9].Liu G, Zhao H, Fan F, Liu G, Xu Q, Nazir S. An Enhanced Intrusion Detection Model Based on Improved kNN in WSNs. *Sensors*. 2022; 22(4):1407. https://doi.org/10.3390/s22041407

[10] Louk MHL, Tama BA. PSO-Driven Feature Selection and Hybrid Ensemble for Network Anomaly Detection. *Big Data and Cognitive Computing*. 2022; 6(4):137. https://doi.org/10.3390/bdcc6040137

[11].Naila Naz, Muazzam A Khan, Suliman A. Alsuhibany, Muhammad Diyan, Zhiyuan Tan, Muhammad Almas Khan, Jawad Ahmad. Ensemble learning-based IDS for sensors telemetry data in IoT networks[J]. Mathematical Biosciences and Engineering, 2022, 19(10): 10550-10580. doi: 10.3934/mbe.2022493

[12] Bukola Fatimah Balogun,Kazeem Alagbe Gbolagade and Ayisat Wuraola Asju-Gbolagade Feature Selection based on BAT Algorithm and Residue Number System for Intrusion Detection Sytem. International Journal of Applied Information Systems 12(39) :32-37,June 2022

[13]. O. Y. Al-Jarrah, A. Siddiqui , M. Elsalamouny , P. D. Yoo, S. Muhaidat, , K. Kim. “Machine-learning-based feature selection techniques for large-scale network intrusion detection,” in Proceedings of The 34th International Conference on Distributed Computing Systems Workshops (ICDCSW’14), 2014pp. 177–181, Madrid, Spain. routing in wireless networks. J Artif Intell 3(01):62–71.

[14].Ruizhe Yao, Ning Wang, Zhihui Liu, Peng Chen, Di Ma, Xianjun Sheng, Intrusion detection system in the Smart Distribution Network: A feature engineering based AE-LightGBM approach,Energy Reports,Volume 7, Supplement 7,2021,Pages 353-361,ISSN 2352-4847,https://doi.org/10.1016/j.egyr.2021.10.024

[15] Manekar V. and Waghmare K. “Intrusion Detection System using Support Vector Machine (SVM) and Particle Swarm Optimization (PSO),” no. 3, pp.2-6, 2014

[16]. Ariyaluran Habeeb, Riyaz Ahamed & Nasaruddin, Fariza & Gani, Abdullah & Targio Hashem, Ibrahim Abaker & Ahmed, Ejaz & Imran, Muhammad."Real-time big data processing for anomaly detection: A Survey,"International Journal of Information Management,2019 Elsevier, vol. 45(C), pages 289-307.

[17] Singh, Amanpreet & Goyal, Akhil.. Intrusion Detection System Based on Hybrid Optimization and using Neural Network: A Review. 10.13140/RG.2.2.23285.83681.August 2018

[18]. Garg, Tanya & Kumar, Yogesh. Combinational feature selection approach for network intrusion detection system. Proceedings of 2014 3rd International Conference on Parallel, Distributed and Grid Computing, PDGC 2014. 8287.10.1109/PDGC.2014.7030720.https://doi.org/10.9734/bpi/rhmcs/v4/4079B.

[19] Idowu, I. R. ., Okewale , K. ., Bamidele, S. A. ., & Ayobioloja, S. P. An Optimized Energy Aware Code Offloading Using Task Scheduling Algorithm for Wireless Sensor Networks. Research Highlights in Mathematics and Computer Science2023 Vol. 4, 21–41.

[20].Mhawi DN, Aldallal A, Hassan S. Advanced Feature-Selection-Based Hybrid Ensemble

Learning Algorithms for Network Intrusion Detection Systems. *Symmetry*. 2022; 14(7):1461. https://doi.org/10.3390/sym14071461

[21].Sandeep, V., Kondappan, S., Jone, A. A., & Raj Barath S "Anomaly Intrusion Detection Using SVM and C4.5 Classification With an Improved Particle Swarm Optimization (I-PSO)." IJISP vol.15, no.2 2021: pp.113-130. http://doi.org/10.4018/IJISP.2021040106

[22]. Y. Wang, Y. Shen, G. Zhang, Research on intrusion detection model using ensemble learning methods, in 2016 7th IEEE International Conference on Software Engineering and Service Science (ICSESS), (2016), 422–425. https://ieeexplore.ieee.org/document/7883100

[23].P Amudha, S Karthik and S Sivakumari. Article: Classification Techniques for Intrusion Detection .An Overview. *International Journal of Computer Applications* 76(16):33-40, August 2013.

[24].Wang, Z.; Liu, J.; Sun, L. EFS-DNN: An Ensemble Feature Selection-Based Deep Learning Approach to Network Intrusion Detection System. *Secur. Commun. Netw.* **2022**, *2022*, 2693948

[25] Moustafa, N.; Slay, J. UNSW-NB15: A comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set). In Proceedings of the 2015 Military Communications and Information Systems Conference (MilCIS), Canberra, Australia, 10–12 November 2015; pp. 1–6