International Journal Of Engineering Research And Development
e- ISSN: 2278-067X, p-ISSN: 2278-800X, www.ijerd.com
Volume 17, Issue 4 (Jul. – Aug. 2021), PP. 21-27

Comparative Analysis of Artificial Immune Recognition System based Classifiers for Intrusion Detection

Ashalata Panigrahi
Roland Institute of Technology, Berhampur, India

ABSTRACT
Artificial immune recognition systems are inspired by the human immune systems. The human immune systems has the amazing characteristics of reacting against any foreign molecule. Such characteristics are highly desirable for the development of anomaly based network intrusion detection system. In this paper artificial immune recognition system based classifier techniques have been proposed for building a robust and accurate intrusion detection system using three classifiers namely AIRS1, AIRS2, and CLONALG. Further, three statistical based feature selection methods namely, Relief-F, One-R, Chi-Squared Attribute Evaluator and three entropy based methods namely, Symmetrical Uncertainty, Information Gain, and Gain Ratio have been employed for selection of relevant features. The performance of the model has been evaluated using ten metrics including Matthews Correlation Coefficient, Geometric Mean, and Kappa Coefficient.

KEYWORDS: *Artificial immune recognition system, CLONALG, Anomaly detection, Intrusion detection system, Feature selection,*

Date of Submission: 04-08-2021 Date of Acceptance: 17-08-2021

I. INTRODUCTION

Artificial immune systems (AIS) attempt to mimic the functions of the adaptive subsystem of biological immune systems(Watkins et al., 2004). AIS methods aimed at solving the problem of global optimization are based on some aspects of the behavior of the human immune system in the process of protecting the body. The protective cells of the immune system (antibodies) undergo many changes, the purpose of which is to create cells that provide the best protection. The AIS has the basic properties of artificial intelligence: memory, the ability to learn and make decisions in an unfamiliar situation (Yang et al., 2014, Zhukov et al., 2014). The main feature of AIS is the ability to learn new information and also recall previous information. One of the best known and efficient classification algorithms based on artificial immune systems is the Artificial Immune Recognition System (AIRS) (Watkins et al., 2004). AIRS is a novel immune inspired supervised learning algorithm (Watkins, 2001). The problems in the field of information security and artificial immune systems have the astonishing similarity of keeping the system stable in a rapidly changing environment. Artificial immune recognition system can use biological immune theoretic for references to search and design relevant models and algorithms to solve the various complex problems occurred in the field of information security (Aickelin et al., 2003). Currently, the artificial immune system (AIS) algorithms are considered as one of the most promising methods of intelligent data processing to solve the problem of intrusion detection (Dasgupta, 2006, Yang et al., 2014), pattern recognition, fault detection.

Intrusion detection system aim to identify two major categories of attacks: signature (or misuse) based and anomaly based detection. Signature-based approach analyzes network packets from particular system in order to find signatures, patterns which are characteristic for intrusive behavior. This type of technique is significantly more effective for known attacks. It cannot recognize unknown attacks and requires frequent database update (Lin et al., 2015, Buczak and Guven 2016). Anomaly-based approach analyzes data in order to recognize abnormal situations, that differ from normal network and system behaviours (Buczak and Guven 2016, Besharati et al., 2019).

In this paper anomaly based intrusion detection method based on artificial immune recognition system algorithms is proposed. Filter based feature selection methods are applied on the NSL-KDD dataset to select most relevant features for classification.

The remaining of the paper is organized as follows: Section 2 presents review of related work in the field of intrusion detection system. In Section 3 briefly describe AIRS based classifiers that are used in the experiment. The proposed model is presented in Section 4. Section 5 divided into three parts. Section 5.1 briefly describes NSL-KDD dataset. Section 5.2 briefly describe feature selection methods. Section 5.3 describes the confusion matrix used to evaluate the performance of the classifier. Section 6 describes experimental results and analysis of results. Finally the conclusion is given in Section 7.

II. RELATED WORK

Jabbar et.al.(2017) proposed a cluster based ensemble classifier for IDS, which is built with Alternating Decision Tree (ADTree) and k-nearest Neighbor algorithm (kNN). The experimental results shows that the proposed ensemble classifier gives better results as compared to other existing techniques in terms of accuracy and detection rate. Pham et al. (2018) proposed a hybrid model using gain ratio technique as feature selection and bagging to combine tree-based classifiers. Experimental results shows that the best performance was produced by the bagging model that used J48 as the base classifier and worked on35-feature subset of the NSL-KDD dataset. Aslahi et al. (2016) proposed a hybrid technique of SVM and GA for intrusion detection. The proposed hybrid algorithm reduces 41 features to 10 features. The features were ordered into three priorities utilizing GA algorithm as the most significant, highest significant, and least essential put in the lowest significant category. The distributed in done such that four features are set in the most significance, four features included in highest significant, and two features included in the least significant category. The results shows that the proposed hybrid algorithm achieve a genuine positive estimation of 0.973 and the false positive value of 0.017. Salo et al.(2019) proposed a hybrid IDS which combines IG and Principal Component Analysis (PCA) feature selection methods with an ensemble classifier based on Support Vector Machine(SVM), Instance-Based learning algorithms(IBK), and Multi-Layer Perceptron(MLP). A comparative analysis performed on several IDS datasets has proven that IG-PCA Ensemble method exhibits better performance than the majority of existing approaches. Khammassi and Krichen (2017) have applied wrapper approach based on a genetic algorithm as a search strategy for select of best subset features and logistic regression as a learning algorithm for network intrusion detection systems. The experimental results shows that their method provides high accuracy rate with only18 features for theKDDCup'99 dataset.

III. METHODOLOGY

Artificial Immune Recognition System based Classification Techniques:

In AIRS (Watkins, 2001) , there are two different populations: Artificial Recognition Balls (ARBs) and Memory Cells (MC). If a training antigen is presented , ARBs matching the antigen are activated and awared more resources. Through this process of stimulation, mutation and selection a candidate memory cell is selected and it is inserted to the memory cell if it gives enough information. This process is repeated for all training records and finally classification takes place by performing a nearest neighbor search on the memory cell population.

AIRS algorithm has following features (Catal et al., 2008):

Generalization: The algorithm does not require all the dataset for generalization and it has data reduction capability.

Parameter Stability: Even though user-defined parameters are not optimized for the problem, the decline of its performance is very small.

Performance: The performance is good for some dataset and totally remarkable.

Self-regulatory: There is no need to choose a topology before training.

AIRS algorithm has five steps: Initialization, Memory cell identification and ARB generation, Competition for resources and development of a candidate memory cell, Memory cell introduction, and Classification.

The performance of the AIRS algorithm depends on eight user defined parameters: Initial Memory Cell Pool Size (IMCPS), Clone Rate (CR), Affinity Threshold Scalar (ATS), Hypermutation Rate (HR), Number of Nearest Neighbours (KNN), Number of Instances to Compute the Affinity Threshold (NIAT), Stimulation Threshold (ST), and Total Resources (TR).

AIRS2 Algorithm

AIRS2 algorithm consists of Five steps (Watkins et al., 2004) :

Step 1 : Initialization

Step 2: Memory Cell (MC) Identification

Step 3: ARB Generation

Step 4: Competition for resources

Step 5: Candidate memory introduction to the set of cells.

Step 6: K-Nearest Neighbour approach for classification

The classification performance of AIRS2 algorithm (Watkins et al., 2004) : depends on the following parameters:

- Hyper Clonal Rate: Define the number of clones an ARB is allowed to produce.
- Clonal Rate: Define the number of resources an ARB can obtain and used also to determine the number of clones allowed to produce.
- Memory Cell Initial Rate: Define the number of training data to be copied in memory cells.
- Total Number of Resources: The total number of resources to share between ARBs.

- Affinity Threshold Scalar: Give a cut-off value for cell replacement.
- K: The number of memory cells to use for classification.
- Test Size: The percentage of global data to take as test data.
- Mutation Rate: The probability for a feature to mutate.

CLONALG Algorithm:

Castro and Zuben (2002) proposed CLONALG algorithm which is based on clonal selection algorithm. The goal is to develop a set of antibodies that represents a solution for a specific problem. CLONALG generates a population of M antibodies , each specifying a random solution for the optimization process. During each iteration, the best existing antibodies are selected, cloned, and mutated to construct a new candidate solution. Next, new antibodies are evaluated and certain percentage of the best antibodies are added to the original population. Finally, some percentage of worst antibodies of previous generation are replaced with new randomly create antibodies.

CLONALG is inspired from the following elements (Catal et al., 2008)

1. Maintenance of a specific memory set.
2. Selection and cloning of most stimulated antibodies.
3. Remove of non-stimulated antibodies.
4. Affinity maturation.
5. Re-selection of clones proportional to affinity with antigen.
6. Generation and maintenance of diversity.

The classification performance of the CLONALG algorithm depends on six user defined parameters: Clonal Factor (CF), Selection Pool Size (SPS), Antibody Pool Size (APS), Number of Generations (NG), Remainder Pool Ratio (RPR), and Total Replacement (TR).

IV. PROPOSED MODEL

This study is focus on anomaly based network intrusion detection. The proposed model consists of the following steps:

- For data capturing and feature selection NSL-KDD dataset is used.
- In order to reduce the features of the high-dimensional dataset filter based feature selection methods are applied on the dataset and most relevant features are selected.
- The selected features are sent to the AIRS based intrusion model.
- During the experiment 10-fold cross-validation procedure is used to validate the model and classify intrusions and normal records.

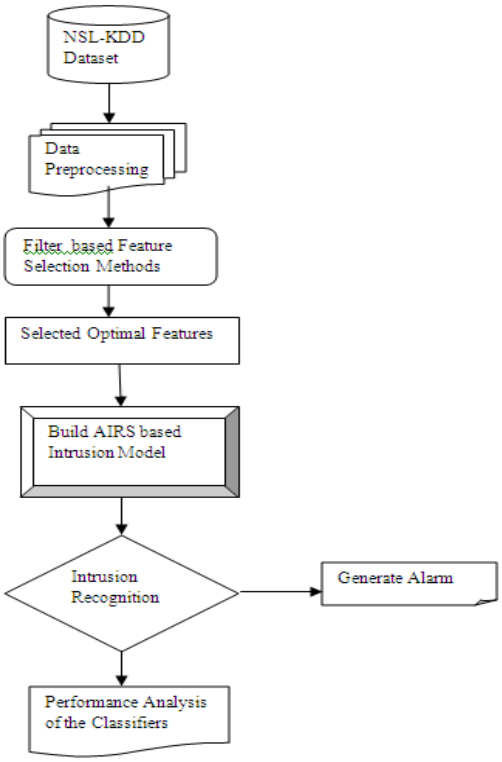

Figure 1 Proposed Model

V. EXPERIMENTAL SETUP

5.1 Dataset Description

The NSL-KDD dataset (Tavallaee et al., 2009) is a revised version of original KDDCUP 99 dataset (Lee et al., 1999) was proposed in the year 2009. The NSL-KDD dataset removed duplicate records of KDDCUP 99 dataset . So it contains moderate number of records and the experiment can be implemented on the total dataset. The total number of records in the dataset is 125973 out of which 58630 are attack records and 67343 are normal records. The dataset consists of forty one features and one class feature which identify the particular record is either normal or any one of the 24 different types of attacks. The different 24 types of attacks can be classified into four classes namely, Denial of Service (DoS), Probe, User to Root (U2R), Remote to Local (R2L). NSL-KDD dataset is highly imbalanced dataset because it has different number of normal and attack records. The number of records of U2R and R2L are very less as compared to normal class and other two attack classes namely DoS and Probe which leads to an imbalanced problem. Number of records of different class are presented in Table 1.

Table 1 : Distribution and percentage of Records of NSL-KDD Dataset

Class	Number of Records	% of Occurrence
Normal	67343	53.46
DoS	45927	36.46
Probes	11656	9.25
R2L	995	0.79
U2R	52	0.04

5.2 Feature Selection

The objective of feature selection method is to remove the features which are noisy and not relevant to the class label. Feature selection methods can be classified into two approaches: individual feature evaluation and subset feature evaluation (Yu and Liu, 2004) Individual feature evaluation assesses each feature individually according to its relevance. Subset feature evaluation uses different search techniques to select best subset of features according to certain criteria and compares it with the previous best subset (Boln-Canedo et al., 2016) Basically feature selection methods are classified into three categories: filter, wrapper, and embedded methods (Guyon et al., 2008). Filter method computes the score for each feature and select the features according to the score (Mladenic et al., 1999). Wrapper method (Kohavi et al., 1997) utilizes the learning algorithm as a black box to score subsets of features. Embedded methods (Breiman et al., 1984) performs feature selection within the process of training. In this paper six filter based methods (three statistical and three entropy based) are applied on the dataset to select relevant features. Three statistical based feature selection methods are Relief-F (RF), One-R (OR) Chi-Squares (CS) and three entropy based feature selection methods are Symmetrical Uncertainty (SU), Information Gain (IG), and Gain Ratio (GR).

5.3 Confusion Matrix (CM)

The confusion matrix evaluate the performance of the classification technique. Each row of the matrix represents the number of records in an actual class and each column of the matrix represents the number of records in a predicted class. Different metrics are used to evaluate different characteristics of the classifiers. Classification of the imbalanced dataset is a challenging task requires specific considerations (Tsai, et al., 2016). In this study the properties such as failure avoidance or class discrimination metric like Youden's Index , Discriminant Power are used for evaluation of classifiers.

Confusion matrix is a tabular representation of true negatives (T_N), false positives (F_P), false negatives (F_N), and true positives (T_P) (Lippmann et al., 2000) as shown in Table 2.

Table 2: Confusion Matrix

		Predicted Class	
		Normal	Attack
Actual Class	Normal	T_N	F_P
	Attack	F_N	T_P

T_N : The number of actual legitimate records are identified as normal.
F_P : The number of actual legitimate records are identified as attacks.
F_N : The actual attack records are detected as normal.
T_P : The actual attack records are classified as attack.
Evaluate the performance of the model in terms of Error Rate, False Discovery Rate (FDR), True Negative Rate (TNR), Negative Predictive Value (NPV), False Negative Rate (FNR), Matthews Correlation Coefficient (MCC), Geometric Mean (GM), Kappa Coefficient (KC), Youden's Index (YI), and Discriminant Power (DP).

Error Rate (ER) = $(F_P + F_N) / (T_P + T_N + F_P + F_N)$ …… (1)
False Discovery Rate (FDR) = $F_P / (F_P + T_P)$ …….. (2)
Specificity or True Negative Rate (TNR) = $T_N / (T_N + F_P)$ …….. (3)
Negative Predictive Value (NPV) = $T_N / (T_N + F_N)$ …… (4)
False Negative Rate (FNR) = $F_N / (F_N + T_P)$ ……. (5)
Matthews Correlation Coefficient (MCC)

$= [(T_P \times T_N) - (F_P \times F_N)] / \sqrt{[(T_P + F_P) \times (T_P + F_N) \times (T_N + F_P) \times (T_N + F_N)]}$ ……..(6)

Geometric Mean (GM) = $\sqrt{[[T_P / (T_P + F_N)] \times [T_N / (T_N + F_P)]]}$ ……(7)
Kappa Coefficient (KC) or Kappa = (Total Accuracy − Random Accuracy) / (1 − Random Accuracy) …(8)
Where Total Accuracy = $(T_P + T_N) / (T_P + T_N + F_P + F_N)$
Random Accuracy = $[(T_N + F_P)(T_N + F_N) + (F_N + T_P)(F_P + T_P)] / (T_P + T_N + F_P + F_N)^2$
Youden's Index (YI) = $[T_P / (T_P + F_N)] + [T_N / (T_N + F_P)] - 1$ ……..(9)
Discriminant Power (DP) = $(\sqrt{3} / \pi)(\log X + \log Y)$ ……(10)
Where X = TPR / (1 – TPR)
Y = TNR / (1 – TNR)

VI. RESULT ANALYSIS

Different combinations of three AIS based techniques namely AIRS1, AIRS2, and Clonalg with two categories of feature selection methods were applied on the NSL-KDD dataset. The performance of AIS based classifiers are evaluated on the basis of Error Rate (ER), False Discovery Rate (FDR), True Negative Rate (TNR), Negative Predictive Value (NPV), False Negative Rate (FNR), Matthews Correlation Coefficient (MCC), Geometric Mean (GM), Kappa Coefficient (KC), Youden's Index (YI), and Discriminant Power (DP). In the experiment 10-fold cross-validation has been applied because of good error estimate and low bias (Singh et al., 2015). The results are presented in Table 3, 4, 5, and 6. Table 3 and 4 presents the performance score of ER, FDR, TNR, NPV, and FNR. Table 5 and 6 presents the performance score of MCC, GM, KC, YI, and DP.

Table 3: Comparison of ER, FDR, TNR, NPV, and FNR of three AIS Classifiers using Statistical based Feature Selection Method

Statistical based Feature Selection Method	Classifier Techniques	Evaluation Metric				
		ER	FDR	TNR	NPV	FNR
Relief-F	AIRS1	**0.0616**	**0.0568**	**0.9516**	**0.9344**	**0.0768**
	AIRS2	0.0789	0.0834	0.9276	0.925	0.0864
	CLONALG	0.1613	0.1329	0.897	0.8186	0.2283
One-R	AIRS1	**0.0662**	**0.0322**	**0.9742**	0.9085	0.1127
	AIRS2	0.0924	0.0952	0.9171	**0.9107**	0.1033
	CLONALG	0.1109	0.1328	0.8801	0.9096	**0.1005**
Chi-Squared Attribute Evaluator	AIRS1	**0.0836**	**0.0744**	**0.9376**	0.9088	0.108
	AIRS2	0.0991	0.1178	0.8943	**0.9181**	**0.0916**
	CLONALG	0.1225	0.1476	0.8656	0.9013	0.1089

Table 4: Comparison of ER, FDR, TNR, NPV, and FNR of three AIS Classifiers using Entropy based Feature Selection Method

Entropy based Feature Selection Method	Classifier Techniques	Evaluation Metric				
		ER	FDR	TNR	NPV	FNR
Symmetrical Uncertainty	AIRS1	0.1115	0.1395	0.8715	0.9177	0.0898
	AIRS2	**0.0835**	**0.0934**	**0.9179**	**0.9254**	**0.085**
	CLONALG	0.1124	0.1323	0.8812	0.9059	0.1051
Information Gain	AIRS1	0.0694	**0.036**	0.9712	0.9057	0.1161
	AIRS2	**0.0676**	0.0374	**0.9699**	**0.9096**	0.1107
	CLONALG	0.111	0.1308	0.8826	0.9072	**0.1037**
Gain Ratio	AIRS1	0.3121	0.3566	0.6433	0.7391	0.2609
	AIRS2	0.1533	**0.0218**	**0.9867**	0.783	0.3141
	CLONALG	**0.1169**	0.1228	0.8938	**0.8881**	**0.1293**

Low error rate is more important in intrusion detection system. Here AIRS1 technique with Relief-F feature selection method gives lowest error rate of 0.0616. Low FDR value indicates good classification performance. AIRS2 technique with Gain Ratio feature selection method gives the lowest FDR of 0.0218. High TNR value indicates the proposed model correctly classified normal records. High TNR value also indicates very low false positive value. AIRS2 technique with Gain Ratio feature selection method gives highest TNR value of 0.9867. NPV value reflect the performance of the prediction. AIRS1 technique with Relief-F feature

selection gives highest NPV score of 0.9344. AIRS1 technique with Relief-F feature selection gives lowest FNR value of 0.0768.

Table 5: Comparison of MCC, GM, KC, YI, and DP of three AIS Classifiers using Statistical based Feature Selection Method

Statistical based Feature Selection Method	Classifier Techniques	Evaluation Metric				
		MCC	GM	KC	YI	DP
Relief-F	**AIRS1**	**0.87**	**0.9373**	**0.8762**	**0.8748**	**3.012**
	AIRS2	0.8414	0.9206	0.8414	0.8412	2.707
	CLONALG	0.6771	0.832	0.6735	0.6687	1.864
One-R	AIRS1	**0.8688**	**0.9298**	0.8661	**0.8615**	**3.1419**
	AIRS2	0.8147	0.9069	**0.9004**	0.8138	2.516
	CLONALG	0.7782	0.8897	0.7777	0.7796	2.3063
Chi-Squared Attribute Evaluator	**AIRS1**	**0.832**	**0.9145**	**0.8315**	**0.8296**	**2.6569**
	AIRS2	0.8015	0.9013	0.7901	0.8027	2.4414
	CLONALG	0.7552	0.8783	0.7545	0.7567	2.1851

Table 6: Comparison of MCC, GM, KC, YI, and DP of three AIS Classifiers using Entropy based Feature Selection Method

Entropy based Feature Selection Method	Classifier Techniques	Evaluation Metric				
		MCC	GM	KC	YI	DP
Symmetrical Uncertainty	AIRS1	0.7799	0.8906	0.7788	0.7817	2.3315
	AIRS2	**0.8324**	**0.9164**	**0.8323**	**0.8328**	**2.6396**
	CLONALG	0.7749	0.888	0.7745	0.7761	2.2847
Information Gain	AIRS1	0.8624	0.9265	0.8597	0.8551	3.0581
	AIRS2	**0.8656**	**0.9287**	**0.8634**	**0.8591**	**3.0614**
	CLONALG	0.7776	0.8894	0.7773	0.7789	2.3002
Gain Ratio	AIRS1	0.3825	0.6896	0.3789	0.3825	0.899
	AIRS2	0.7155	**0.8226**	0.6858	0.6725	**2.8029**
	CLONALG	**0.7649**	0.8822	**0.7649**	**0.7645**	2.2252

MCC calculates the actual and predicted values. High score of MCC indicates good prediction of the classifier. AIRS1 with Relief-F feature selection gives highest MCC value of 0.87 which shows our approach is good in classifying the attacks in intrusion detection system. AIRS1 with Relief-F feature selection gives highest GM value of 0.9373. The Kappa Coefficient measures the agreement between classification and truth values. The value ranges from 0 to 1. AIRS2 with One-R feature selection gives highest value of 0.9004. A higher value of YI is an indication of a good performing of the classifier. Here AIRS1 technique with Relief-F feature selection method gives highest YI of 0.8748. DP value indicates how well the proposed model distinguish between positive and negative records. The value of DP is greater-than 2 and less-than 3 is fair and DP value greater-than 3 is good. AIRS1 With One-R feature selection method gives highest DP value of 3.1419. These results suggest that AIRS1 classifier performs better as compared to other two methods.

VII. CONCLUSION

In order to construct an effective intrusion detection system, an approach for AIRS based intrusion detection system is presented in this paper. Experiments with NSL-KDD dataset shows that the proposed approach has a good performance for detecting intrusions in network security. It was observed that AIRS1 classifier with Relief-F feature selection gives lowest error rate, lowest FNR value, highest MCC and highest GM value. AIRS1 with one-R feature selection gives highest DP value.

REFERENCES

[1]. Aslahi-Shahri, B.M., Rahmani, R., Chizari, M., Maralani, A., Eslami, M., Golkar, M.J., and Ebrahimi, A., 2016. A hybrid method consisting of GA and SVM for intrusion detection system. Neural Comput.Appl., 27, 1669-1676 .

[2]. Besharati E., Naderan M., Namjoo E., 2019. LR-HIDS: logistic regression host-based intrusion detection system for cloud environments. Journal of Ambient Intelligence and Humanized Computing, 10,3669-3692.

[3]. Bolón-Canedo**, V.,** Sánchez Maroño**, N.,** Alonso-Betanzos, A., 2016. Feature selection for high dimensional data. Progress in Artificial Intelligence, 5(2), 65-75.

[4]. Breiman, L., Friedman, J.H. , Olshen, R.A. and Stone. C. J., 1984 . Classification and regression trees. Wadsworth and Brooks.

[5]. Buczak, A.l., Guven, E., 2016. A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Communication Surveys & Tutorials. 18, 1153-1176.

[6]. Catal, C., Diri, B., 2008. Investigating the Effect of Dataset Size , Metric Sets, and Feature Selection Techniques on Software Fault Prediction Problem. Information Sciences. 179(8), 1040-1058.

[7]. Castro, L. de and Zuben, F., 2002. Learning and Optimization Using the Clonal Selection Principle. IEEE Transactions on Evolutionary Computation, 6(3), 239-251.
[8]. Guyon I., Gunn S, Nikravesh M, Zadeh LA., 2008. Feature extraction foundation and applications, vol. 207, Berlin, Springer
[9]. Jabbar,M.,Aluvalu,R.,Reddy,S.S.S.,2017.Cluster based ensemble classification for intrusion detection system ,in: Proceedings of the 9th International Conference on Machine Learning and Computing, pp.253–257.doi:10.1145/3055635.3056595
[10]. Khammassi, C., Krichen, S., 2017. A GA-LR wrapper approach for feature selection in network intrusion detection. Computers & Security 70, 255–277 .doi:10.1016/j.cose.2017.06.005.
[11]. Kohavi, R., John, G.H., 1997. Wrappers for feature subset selection. Artificial Intelligence, 97(1-2), 273-324.
[12]. Lee,W.,Stolfo,S.J.,Mok,K.W.,1999. A data mining framework for building intrusion detection models, in: Proceedings of the1999 IEEE Symposium on Security and Privacy (Cat.No.99CB36344), IEEE.pp.120–132.doi:10.1109/SECPRI.1999.766909.
[13]. Lin W-C, Ke S-W, ,Tsai C-F , 2015. CANN: An intrusion detection system based on combining cluster centers and nearest neighbours. Knowledge-Based Systems, 78(1), 13-21.
[14]. Lippmann,,R., Haines,,J.W., Fried, D.J., Korba,J., Das,K,. 1999. DARPA off-line intrusion detection evaluation. . Computer Networks. 34(4), 579–595. https://doi.org/10.1016/S1389-1286(00)00139-0
[15]. Mladenic, D. and. Grobelnik, M. Feature selection for unbalanced class distribution and Naïve Bayes, ICML 1999.
[16]. Pham,N.T., Foo,E., Suriadi,S., Jeffrey,H., Lahza,H.F.M., 2018. Improving performance of intrusion detection system using ensemble methods and feature selection, in: Proceedings of the Australasian Computer Science Week Multiconference, ACM. p.2. doi:10.1145/ 3167918.3167951
[17]. Salo, F., Nassif, A.B., Essex, A., 2019. Dimensionality reduction with IG-PCA and ensemble classifierf or network intrusion detection. Computer Networks. 148, 164–175. doi:10.1016/j.comnet.2018.11. 010.
[18]. Singh R., Kumar H., Singla R., 2015. An intrusion detection system using network traffic profiling and online sequential extreme learning machine. Expert Systems with Applications. 42(22), 8609-8624.
[19]. Tsai, M.F., Yu, S.S., 2016. Distance metric based oversampling method for bioinformatics and performance evaluation. Journal of Medical Systems.
[20]. Tavallaee, M., Bagheri, E., Lu, W., Ghorbani, A.A., 2009. A detailed analysis of the kddcup99 dataset, in:2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications, IEEE.pp.1–6.doi:10.1109/CISDA.2009.5356528.
[21]. Watkins, B.A., 2001. A Resource Limited Artificial Immune Classifier. Mississippi state University, Master Thesis.
[22]. Watkins, A., Timmis, J., and Boggess, L. C. , 2004. Artificial Immune Recognition System (AIRS) : An Immune Inspired Supervised Machine Learning Algorithm. Genetic Programming and Evolvable Machines. 5(3), 291–317.
[23]. Yu, L. and Liu, H., 2004. Efficient feature selection via analysis of relevance and redundancy. Journal of Machine Learning Research. 5 , 1205–1224.

Ashalata Panigrahi. “Comparative Analysis of Artificial Immune Recognition System based Classifiers for Intrusion Detection." *International Journal of Engineering Research and Development*, vol. 17(04), 2021, pp 21-27.