JAZ INDIA

Journal of Advanced Zoology

ISSN: 0253-7214
*Volume **44** Issue **04 Year 2023** Page **969:975***

Clustering based Intrusion Detection System for effective Detection of known and Zero-day Attacks

Dr. Nerella Sameera[1], M.Siva Jyothi[2], K.Lakshmaji[3], Dr.V.S.R.Pavan Kumar. Neeli[*]

[1]Assoc.Prof, Dept of CSE, RV Institute of Technology, Chebrolu, A.P, INDIA
[2]Asst.Prof, Dept of IT, CMR Technical Campus, Hyderabad, Telangana, INDIA
[3]Asst.Prof, Dept of CSE, Shri Vishnu Engineering College for Women, Bhimavaram, A.P, INDIA
[4]Principal, Chirala Engineering College, Chirala, A.P, INDIA

**Corresponding author's E-mail: crrpavankumar@gmail.com*

Article History

Received: 06 June 2023
Revised: 05 Sept 2023
Accepted: 02 Dec 2023

Abstract

Developing effective security measures is the most challenging task now a days and hence calls for the development of intelligent intrusion detection systems. Most of the existing intrusion detection systems perform best at detecting known attacks but fail to detect zero-day attacks due to the lack of labeled examples. Authors in this paper, comes with a clustering-based IDS framework that can effectively detect both known and zero-day attacks by following unsupervised machine learning techniques. This research uses NSL-KDD dataset for the motive of experimentation and the experimental results exhibit best performance with an accuracy of 78%.

Keywords: *Machine Learning, Framework*

1. Introduction

In the current days everything is done online and almost all the data is digitized and computerized which makes cyber space more vulnerable and more prone to attacks [1]. This grabs the attention of modern researchers working in the area of cyber security and demands for the development of effective Intrusion Detection Systems (IDS).

IDS is a hardware or software system that observes the behavior of a computer system or a computer network to identify intrusions [2]. IDSs are of 2 types; network- based IDS and host-based IDS. Where a host-based system is for detecting the attacks at the cyber space of the host and network-based system is for detecting the attacks at the cyber space of the computer network. IDS sticks to two detection approaches; one is signature-basedand the other is anomaly-based.

In signature-based detection approach, attack detection is done by matching the incoming packet signatures with the existing attack and normal signatures. The incoming packet is labeled with appropriate class based on the result of pattern matching. The downside of this approach is it only detects known attacks but cannot detect unknown or zero-day attacks where known attacks are the attacks whose patterns are already generated and zero-day attacks are the attacks whose patterns are not yet formed. Coming to the second approach, anomaly-based detection approach; attack detection is done by observing the deviation of the packet's behavior from its analyzed normal behavior. So, any packet drift from the normal behavior can be considered as an attack. By following this way, an anomaly-based detection approach can detect unknown attacks but falls in to high rate of misclassification which generates high false positive rates (FPR).

This scenario makes the identification of zero-day attacks very tough and verychallenging to the researchers. The authors in this paper put forward a new clustering-based IDS system framework that uses unsupervised machine learning techniques to determine zero-day and known attacks. The remaining portion of the paper is structured as mentioned below. Section-II discusses the related background study, Section-III discusses the zero-day attack detection framework, Section-IV gives details of the dataset, Section-V contains the details of experimentation and discussion of results and lastly, Section-VI concludes the research work.

Literature study

Jaswal et.al in [3] implemented a hybrid IDS system which uses K-means clustering algorithm, SVM and association-based algorithm. Initially they focused much on data pre-processing step in which they used K-means algorithm for redundancy. On top of these pre-processed data they applied SVM and association based algorithms to perform binary classification. They used the KDD CUP99 data set for experimentation purposes. Goeschel et.al in [4] implemented a hybrid IDS system which uses SVM, DT and Naive Bayes classification methods for performing intrusion detection with reduced false positive rates. Initially, they used SVM for classifying the data packets as attack and normal class and further They applied DT on the attack packets by classifying the packets into known and unknown attacks. lastly, they applied Naive bayes classification method on unknown attack data to further check the likeliness with the existing attacks so that the packet which is similar to the existing attack signature can be assigned to that group and the one which is completely dissimilar can be forwarded for further enquiry. They used the KDD CUP99 data set for experimentation purposes.

Hajimirzaei et. al in [5], implemented a hybrid IDS system by making use of MLP (Multi-Layer Perceptron), ABC (Artificial Bee Colony) optimization methods and fuzzy based clustering method. Initially, training data is formed into groups by applying a fuzzy clustering method. On top of these homogenous groups MLP which is tuned by ABC method was applied to classify the packets as attack and normal groups.

Ariafar et.al in [6], implemented a hybrid IDS by making use of the K-means method, Genetic Algorithm and Decision Tree algorithm. initially the parameters of K-means and Decision Tree algorithms were optimized by Genetic algorithm. Later, training data is formed into clusters by using optimized K-means algorithms. On top of these clusters DT is applied to perform binary classification of traffic packets.

Clustering based IDS framework for the detection of zero-day attacks

In this work authors introduced a new clustering-based IDS model to detect known and zero-day attacks efficiently. The mechanism followed by the IDS framework is as follows.

Figure 1 presents the IDS framework. As shown in the figure, the entire data is pre-processed initially. Pre-processing step includes removal of useless fields from the data set followed by the data normalization and lastly transforming the data into the latent space by generating the principal components on top of the normalized data through the application of Principal Component Analysis-(PCA) technique. Later, for experimentation purpose the pre-processed data is divided into two modules in 80:20 ratio such that, at least one attack class data should not be present in module-1 and must be present in module-2 to represent the zero-day attack scenario.

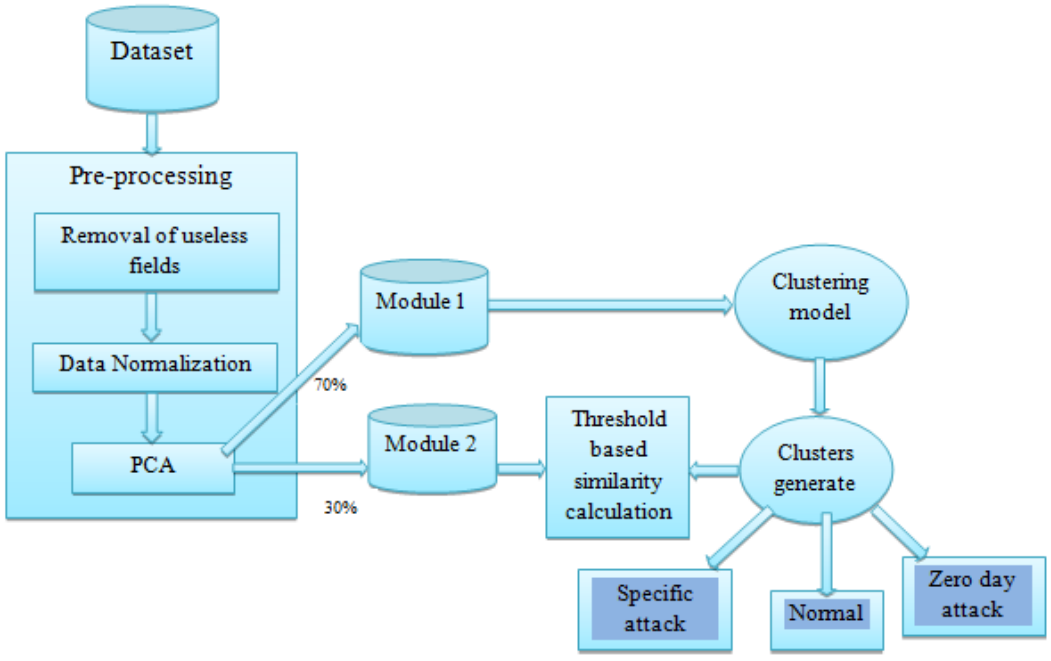

Figure1: Architecture of proposed IDS framework

At this stage, the proposed IDS framework is implemented in two phases.

Phase-1:

In the first phase, out of two modules, module-1 is processed further to implement the proposed IDS framework. Module-1 is divided into 'k' clusters by applying k-means clustering algorithm and the 'k' value should be equal to the number of class types present in module-1. For example, if there are 3 attack class groups and one normal class group present at module-1 then the 'k' value should be taken as 4. After dividing the cluster into 'k' groups, label the clusters according to the majority class of that cluster. Centroid of each cluster should be calculated further to represent the respective clusters.

Phase-2:

After getting ready with cluster centroids, in phase-2, module-2 data can be categorized with appropriate labels by following the threshold-based similarity score and the details are given below.

Zero-day attack detection process:

For each packet 'X' of module-2, similarity of the packet 'X' with the module-1 clusters should be estimated by calculating the distance from 'X' to all module-1 centroids. On satisfying the threshold value 'α' the packet is assigned to the class which is having very close similarity with it and labeled accordingly. Here, the threshold value indicates the minimum (upper bound) similarity value to be satisfied for classifying the packet and the value of 'α' can be decided experimentally. In this way all packets of module-2 will be assigned with appropriate classes based on their similarity. However, if the packet is close to the particular cluster but not satisfying the threshold value will not be allocated to any existing classes but is treated as an unknown attack as it is not enough close to any existing group and hence it can be labeled as 'zero-day' attack accordingly. In this way, the proposed IDS framework can detect both known and zero-day attacks.

Data set

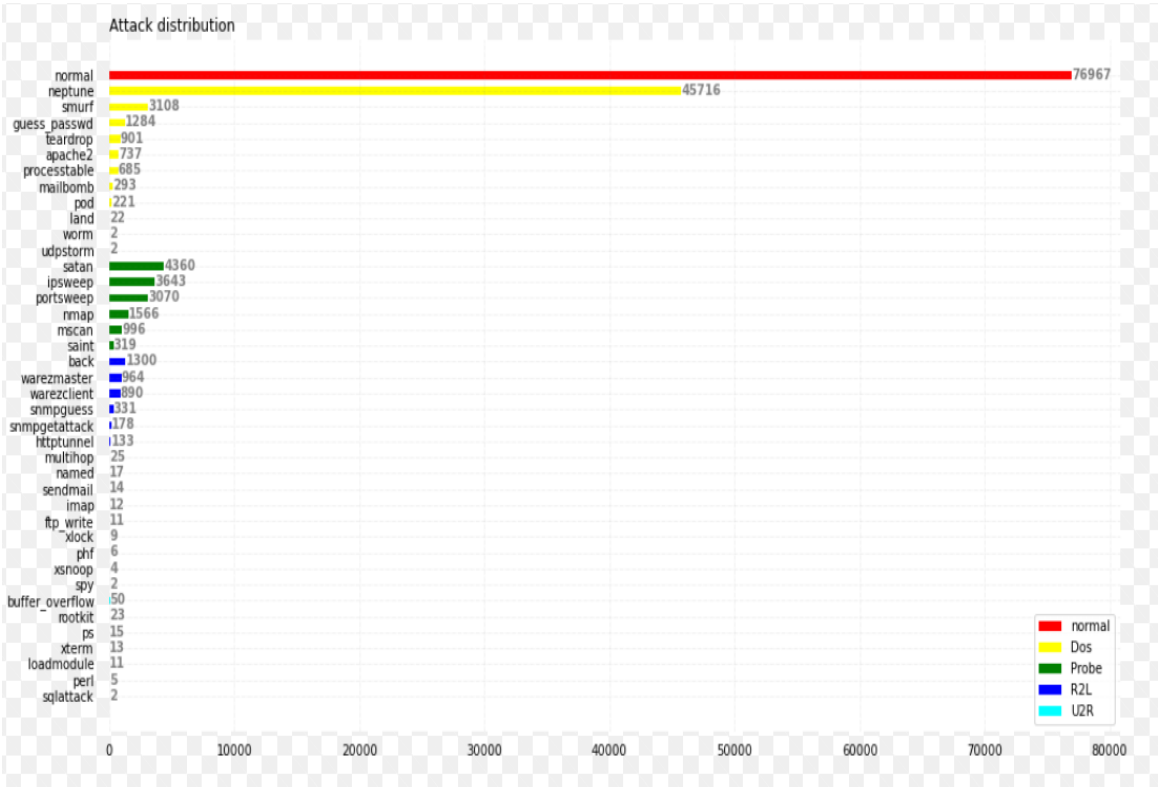

Figure 2: Specific attack distribution of the NSL-KDD dataset.

To implement the proposed framework, authors make use of the NSL-KDD [7] data set which is an improved category of the KDD99 dataset [8]. This NSL-KDD dataset is known to be the benchmark dataset used by many researchers for the purpose of experimenting on the cyber security domain. As given in figure 2, the data set consists of many specific attack instances along with many normal instances where every attack belongs to one of the four attack groups and the details of the dataset are given below in detail.

No. of instances:147907

No. of attributes:43

No. of specific attacks: 40

No. of generic attack groups: 4 (DoS, R2L, Probe and U2R)

The overall distribution of attack and normal instances in the dataset is mentioned in Figure 3. As shown in the figure, almost attack and normal instances share equal amounts in the dataset. Coming to the attacks part, DoS attack group occupy most of the attack space of the dataset and next to the DoS is the Probe attack group followed by the R2L attack group and the least is the U2R attack group.

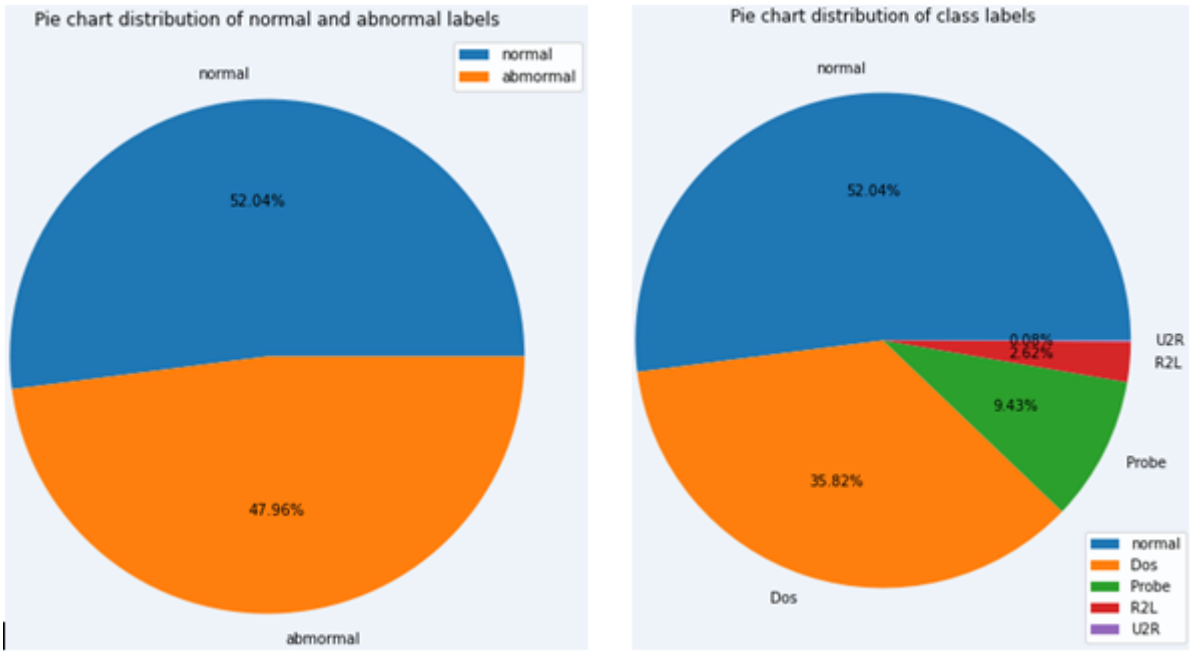

Figure 3 (a,b): Attack and normal distribution of the NSL-KDD dataset.

3. Results and Discussion

The authors have used the NSL-KDD data set for experimenting with the proposed IDS framework. Specifically, this research uses the numeric version of NSL-KDD [9] which is a slightly simplified class of the original dataset consisting of all 33 numeric fields formed by applying an encoding approach that converts categorical fields into numeric fields [9]. To begin with, the dataset is pre-processed initially to prepare the data for experimentation. As a first step of pre-processing, the useless fields were identified and removed in such a way that the fields with too many zeros were considered as useless fields. After that the reduced data is normalized by applying z-score. Later, PCA is applied as discussed in Section-III, to transform the data into the latent space. where the number of principal components were decided experimentally as shown in Figure 4. From the figure, it is clear that the best number of principal components to further produce good quality clusters is 4.

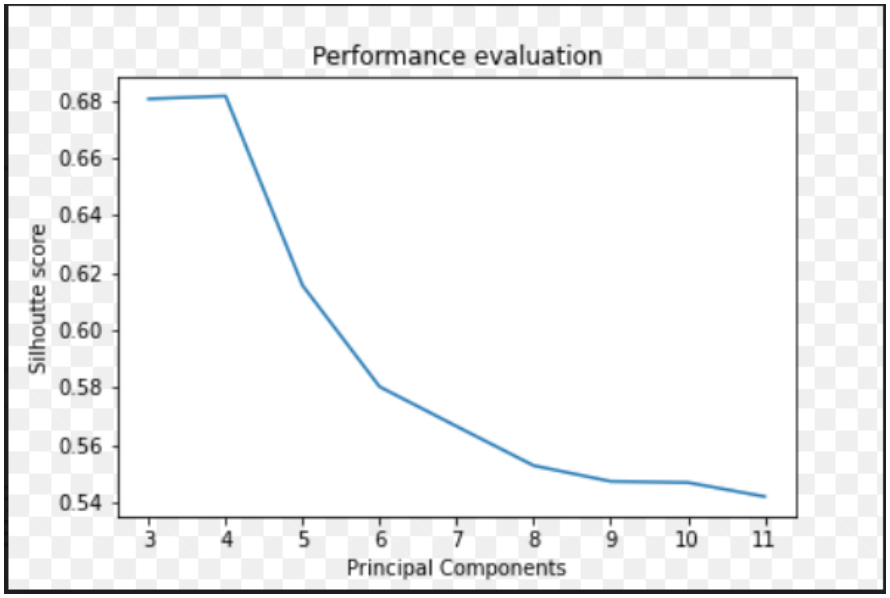

Figure 4: cluster purity against principal components

As discussed earlier, the transformed dataset is divided into two modules in 80:20 ratio. To reflect the zero-day attack scenario, DoS and Probe examples together with some normal examples were chosen for module-1 and the remaining U2R and R2L examples together with some normal examples were chosen for module-2. Class distribution of module-1 and module-2 were given in Figure 5 in detail.

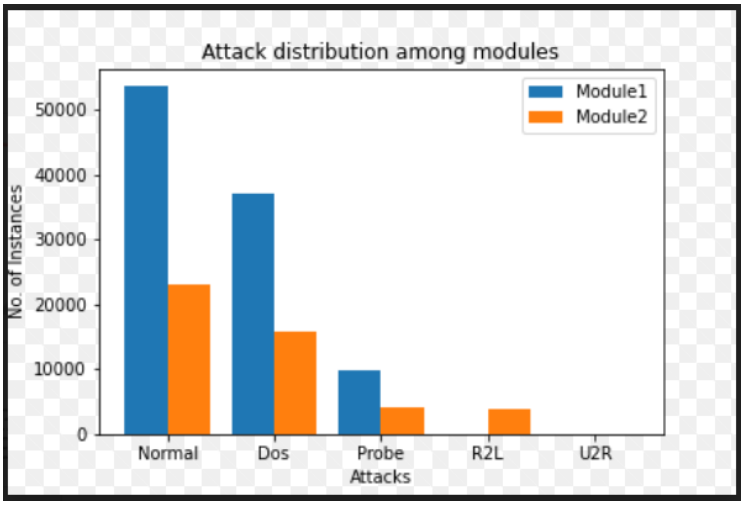

Figure 5: module wise attack and normal distribution.

Now to implement phase-1, clustering is performed on top of module-1 data by applying K-means clustering method where the 'K' value is taken as 3. Later, these clusters are labeled with 'DoS', 'Probe' and 'Normal' types based on the majority label of the group. Cluster centroids are calculated for each cluster which are further used to represent the respective clusters.

To implement phase-2, similarity value between every packet of module-2 packets and every centroid of module-1 is calculated by applying Euclidean distance measure. Threshold 'α'is fixed in a trial-and-error procedure as shown in Figure 6. As per the results exhibited in the figure, best detection performance is exhibited at threshold value 4.26. Hence, a module-2 packet is assigned with a 'DoS' label if it is close to the module-1's DoS cluster with the similarity value less than or equal to 4.26. Similarly, a module-2 packet is assigned with a 'Probe' label if it is close to the module-1's Probe cluster with the similarity value less than or equal to 4.26. Last but not least, a module-2 packet is assigned with a 'Normal' label if it is close to the module-1's Normal cluster with the similarity value less than or equal to 4.26. Lastly, the packet which is not satisfied by the given threshold is labeled as 'zero-day' attack.

The authors used accuracy, precision and other performance scores for evaluating the proposed model. The experimental outcomes and comparative study were mentioned in Tables 1 and 2 respectively in detail. From the experimental outcomes it is clear that the proposed method performs better to the state-of-the-art with an accuracy of 78%.The state-of-the-art mentioned were performing binary-class classification aimed at the identification of zero-day attacks by applying Transfer Learning-(TL) [10] technique which is an advancement of machine learning that contains complex domain unification procedures. whereas the proposed approach performs multiclass classification and is not using any kind of transfer learning like complex procedures but, it attains best detection performance in detecting zero-day attacks.

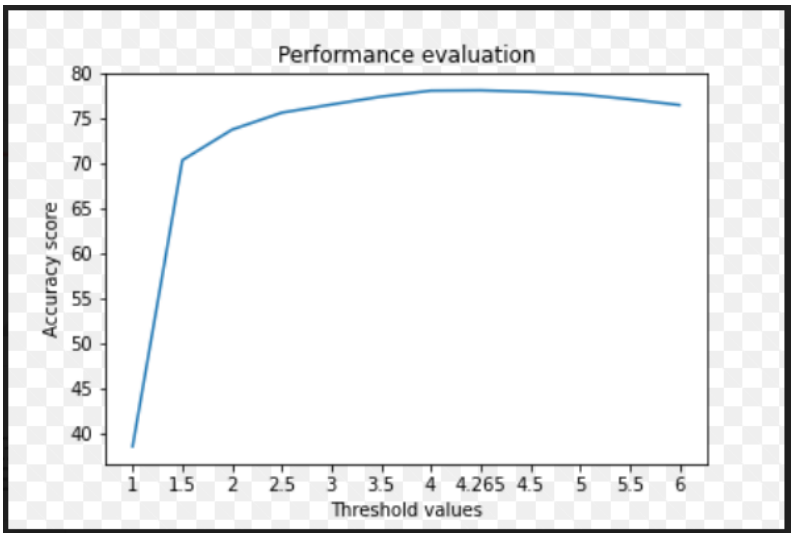

Figure 6: Analysis on different threshold values based on accuracy scores

Classification report :

	precision	recall	f1-score	support
Dos	0.98	0.68	0.80	15845
Probe	0.33	0.52	0.40	4143
Unknown	0.56	0.42	0.48	3999
normal	0.83	0.96	0.89	23184
accuracy			0.78	47171
macro avg	0.67	0.64	0.64	47171
weighted avg	0.81	0.78	0.78	47171

Table 1: Experimentation results

Method	Dataset Used	ML algorithm used	Accuracy %
Proposed approach	Numeric NSL-KDD	K-Means	78
HeTL [11]	NSL-KDD	KNN	78.00
Transductive TL [12]	Numeric NSL-KDD	KNN	75.76
TL based prototype approach [13]	NSL-KDD	KNN	89.79

Table2: comparative study of proposed method with state-of-art

4. Conclusion

To combat the rapid growth of cyber-attacks, the authors proposed a clustering-based IDS framework which can digoutknown and zero-day attacks effectively. Coming to the details of the IDS framework, initially the entire data is pre-processed and made into two modules. further the framework was implemented in two phases. in the first phase, module-1 data is clustered using k-means clustering by representing every cluster with their respective centroids. In the second phase, module-2 instances were assigned with an appropriate label by relaying on their threshold-based similarity value where, the packet which does not satisfying the threshold value is labeled as zero-day attack. the authors perform experimentation using NSL-KDD dataset from the experimentation outcomes it is noticed that the proposed approach results into the best performance with the accuracy of 78%.

References:

[1] Nerella Sameera and M. Shashi, A survey on cyber security analytics, International Journal of computer sciences and engineering (IJCSE) ISSN:2347-2693; volume 6 Issue 11 (2018).

[2] Nerella Sameera and M. Shashi, Intrusion detection analytics: A comprehensive survey. International Journal of Advanced Scientific Research and Management (IJASRM), Volume 4, Issue 6, ISSN:2455-6378, June (2019).

[3] Jaswal K, Kumar P and Rawat S, Design , Development of a prototype application for intrusion detection using data mining. 4th international conference on reliability, infocom technologies and optimization (ICRITO) (trends and future directions) pp. 1-6. IEEE, (2015)

[4] Goeschel and Kathleen, Reducing False positives in intrusion detection systems using data-mining techniques utilizing support vector machines, decision trees, and naive Bayes for off-line analysis. In Southeast Con 30 (pp. 1-6). IEEE, (2016).
[5] Hajimirzaei B and Navimipour NJ, Intrusion detection for cloud computing using neural networks and artificial bee colony optimization algorithm. ICT Express, (2018).
[6] Ariafar E and Kiani R, Intrusion detection system using an optimized framework based on datamining techniques. IEEE4th International Conference on Knowledge-Based Engineering and Innovation (KBEI),pp. 0785-0791, (2017).
[7] Botes FH, Leenen L and De La Harpe R, Ant colony induced decision trees for intrusion detection. In ECCWS 16th European Conference on Cyber Warfare and Security (p. 53). Academic Conferences and publishing limited, (2017).
[8] Tavallaee, Mahbod, Ebrahim Bagheri, Wei Lu, and Ali A. Ghorbani. "A detailed analysis of the KDD CUP 99 data set." In 2009 IEEE symposium on computational intelligence for security and defense applications, pp. 1-6. Ieee, 2009.
[9] Nerella Sameera and M. Shashi, Encoding approach for Intrusion Detection using PCA and KNN classifier. Proceedings of the third international conference on computational intelligence and informatics, Springer, AISC, Volume 1090, (2020).
[10] Weiss, Karl, Taghi M. Khoshgoftaar, and DingDing Wang, “A survey of transfer learning”, Journal of Big Data 3.1 (2016): 9.
[11] Zhao, Juan, Sachin Shetty and Jan Wei Pan,“Feature-based transfer learning for network security”, In MILCOM IEEE Military, (2017).
[12] Nerella Sameera and M. Shashi, Deep Transductive Transfer learning framework for zero-day attack detection, ICT Express, **Elsevier,** ISSN: 2405-9595,Vol. 6, Issue 4, pages 361-367, (2020).
[13] Nerella Sameera and M. Shashi, Transfer-learning based prototype for zero-day attack detection. International Journal of Engineering and Advanced Technology (IJEAT), Volume 8, Issue 4, ISSN: 2249-8958, (2019).