International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING

ISSN:2147-6799 www.ijisae.org Original Research Paper

Machine Learning-Based Classification Techniques for Network Intrusion Detection

Ravindra S. Tambe, Dr. Hiren Dand, Dr. Mangesh D. Salunke

Submitted: 06/09/2023 **Revised**: 21/10/2023 **Accepted**: 05/11/2023

Abstract: Network intrusion detection is crucial because of how it affects several communication and security areas, to detect network intrusion is a challenging task. Additionally, network intrusion detection is arduous work because to train modern machine learning models it takes a huge number of data to recognise an intrusion into the network. Recently, in order to identify network intrusions various methods proposed. Though they face significant difficulties because novel threats are always emerging that more older systems cannot detect. The goal of this paper is to design a network intrusion detection system (NIDS) by comparing several algorithms. Considering the relationships between the features, the optimum features are chosen from the dataset. In our research, we use K-means, Decision Tree, Random Forest, KNNs, and MLP for comparison. By monitoring the network traffic is classified into attacks and normal traffic. The experimental outcomes demonstrated that our suggested technique accurately detects various network intrusion types with on the KDD Cup99 dataset. Our proposed system also helpful for research and application areas involving network security.

Keywords*: Network Intrusion, Decision Tree, K-means, MLP, Random Forest, KDD Cup99*

1. Introduction

An intrusion detection system (IDS) is a system that monitors a network or system for indications of malicious behaviour and policy breaches. IDS detects anomalies and inconsistent behaviours on a network while it is carrying out regular tasks in network or system used to identify network security threats such as denial-of-service (DoS) attacks. Additionally, it helps in determining, deciding, and controlling unauthorised system activities such unauthorized access, modification [1, 24]. There are different types of IDS like are host based and network based IDS.

These range from small networks to large ones to some extent. A host based intrusion detection system (HIDS) monitors operating system files for irregularities and suspicious behaviour on a single machine. Comparatively, the NIDS monitors the network's connections for unauthorized traffic. There are two methods are used for alerting threats i.e. signature-based and anomaly-based detection [2, 25]. The byte patterns in the network route are examined by signature-based IDS. We can consider them to be malicious instruction patterns employed by malware. As a result, the groups or patterns that are discovered in antivirus software are referred to as signatures. Attacks for which there was no prior pattern are not detectable by signature-based IDS [23, 26]. An anomaly-based IDS, it analyses network activities and checks for patterns, builds a model based on data of the expected behaviours automatically so, it finds deviations when there are anomalies[3]. The advantage of this IDS is to track most recent, undiscovered anomalies or cyberattacks like denial-of-services.

An approach for monitoring and tracking computer system events is called intrusion detection. Using security data and event-driven monitoring methods, it is utilised to detect security issue warning indicators. With the swift growth of internet-based resources, the number of computing devices and users linked to networks has raised enormously. These resources empower users and public/private sector organisations to access and utilise internet

[1]*Department Of Computer Engineering*
JJT University, Rajasthan
ravindra.tambe01@gmail.com
[2]*Department Of Computer Engineering*
JJT University, Rajasthan
dandhiren@gmail.com
[3]*Department Of Computer Engineering*
JJT University, Rajasthan
salunkemangesh019@gmail.com

services. There also been countless instances of unauthorised access to web services. Common services include protocol specific assaults (ARP, IP, TCP, UDP, and ICMP), traffic flooding, worms, and DoS [4]. Attacks that are protocol-specific take use of a particular feature of the target machine's installed protocol. SMURF, SYP, and authentication server assaults are common protocol attacks.

Technique for addressing the network security issue is the IDS. Three categories can be used to classify IDS:

1. Host intrusion detection system (HIDS)
2. Network intrusion detection system (NIDS)
3. Network node intrusion detection system (NNIDS)

Every computer on the network, as well as other areas of the enterprise network the HIDS runs. NIDS is only used and meant to control locations where the risk of vulnerability is high [22]. NNIDS is similar to NIDS, however it works only on a single host at once. For intrusion detection, there are mainly three approaches:

1.Signature based IDS

2.Anomaly based IDS

3. Hybrid of signature and anomaly based IDS

Signature-based IDS is primarily concerned with finding patterns and signatures, then comparing such patterns to the recognised fraud signature. Anomaly based IDS looks difficult-to-detect versions of unidentified signature attacks. Due to the rapid evolution of Spyware and an attack method, anomaly based IDS employs ML techniques to identify reliable pattern of activity with novel behaviours [5].

ML (Machine Learning) is a subset of Artificial Intelligence (AI), where ML improves the system's automatic ability to experiment and increases learning and prediction without requiring extensive programming in accordance with a set of algorithms. Additionally, ML algorithms are more effective at quickly detecting attacks from a large amount of data [6]. A machine learning algorithm can be of three different types-

1. Supervised
2. Unsupervised
3. Semi-supervised

2. Background and Related Work

Intrusion detection is utilised to detect evidence of infiltration on a network and unauthorised access to the system. Many researchers have used data mining approaches to find intrusions in this domain. In this study, techniques for supervised machine learning are proposed based on distance measurements [21]. Compared to other techniques, supervised machine learning techniques outperform them in terms of detection rate, accuracy, false alarm rate. The performance of the supervised ML algorithms in terms of serial execution time is superior to that of the other Actions [13].

In this paper, author uses several types of well-known ML-based techniques for classification, such as Bayesian Network, Naive Bayes classifier, Decision Tree, Random Decision Forest, Random Tree, Decision Table, and Artificial Neural Network, to detect intrusions and to give services in the area of cyber-security [14].

An IDS is used to look into malicious activity that takes place within a network or a system. Now a days connectivity between computers is increasing so, intrusion detection essential for network security. To protect the networks, many Intrusion Detection Systems have been developed with statistical and machine learning techniques [20]. Accuracy is the primary factor that determines how well an IDS performs. To decrease false alarms and improve detection rates, accuracy it is necessary to enhance intrusion detection. Different methods have been used in recent works to enhance performance. Main objective of an ID is to analyse significant amount of network traffic data. To solve this issue systematic classification method is required. This methodology considers this problem and applies ML methods like the Support Vector Machine (SVM) and Naive Bayes. SVM performs better than Nave Bayes, according to the results [15].

Data normalisation or transformation is crucial for ML-based IDS to achieve a high detection rate. Before training a classification model, it is possible to normalise the attributes of the data using a number of techniques. Selecting the best normalisation approach, however, remains a difficult task. In this study, a statistical approach is suggested that can help determine which normalization technique is best for a given dataset [19]. The recommended approach identified the normalization method that provides the optimum

accuracy for an intrusion detection system. Five different datasets with two different feature selection approaches were utilised to demonstrate the effectiveness of the suggested approach [4].

In this research, novel attack detection methods utilising deep learning techniques is given for precisely detecting the attacks by examining the smart meter traffic. In order to correctly detect attacks, the suggested approach uses various multilayer deep learning algorithms that are organised in a hierarchical sequence. Using the CICIDS 2017 dataset, proposed system's effectiveness is compared with hierarchical SVM algorithms with feature selection methods and simple multilayer deep learning algorithms [16].

This research aims to examine if deep learning algorithms are appropriate for an anomaly based IDS. In this study, the author designed anomaly detection models based on several deep neural network structures, such as convolutional neural networks, auto encoders and recurrent neural networks. The NSLKDD training data set was used for training these deep models and NSLKDDTest+ and NSLKDDTest21 test data sets were used to evaluate their performance [17].

This research provides novel approach using service-aware dataset partitioning, which offers capability to handle large and quickly expanding flexible use of network data enables the classifier to enhance classification performance in terms of speed and accuracy. To accomplish the best results, the widely used Kyoto2016 dataset was employed, which is a well-known dataset for highly unbalanced data [18].

3. Methodology

This study proposes an effective NIDS based on the machine learning techniques. In addition, this study provides methods for classifying network traffic as threats or normal traffic. Also K-means, Decision tree, Random forest, KNN, Multilayer perceptron techniques are used in our proposed system. The techniques are described below.

- K-Means

In order to preserve and guarantee the confidentiality of data and information flows throughout the process they access, efficient NIDSs are required. Identifying the patterns and behaviours of network activity is crucial for improving the detection of anomalies and illegal behaviour and securing the network. When performing outlier detection as part of clustering, there is a possibility that outliers will end up in the normal clusters. Outliers are the points of observation that greatly differ from other observations, and these are frequently viewed as noise that needs to be eliminated. Outliers could also be a sign of the intrusion. The process of clustering may get disturbed by outliers that are not a part of a larger cluster as they might be excluded from the process of clustering, mixed in with the usual data, and could make the grouping less precise. A significant percentage of false alarms is also likely to be produced by anomaly-based detection utilising K-Means clustering. There may be a large percentage of false positive and false negative warnings, where false positive means unusual behaviour that is not intrusive but is reported as and false negative refers to a situation in which intrusive anomalous activities are flagged as non-intrusive. IDS design may become unreliable and inefficient due to a high false alarm rate.

This is the main issue with anomaly-based intrusion detection, which is regularly monitored and attempted to be reduced utilising a number of techniques and approaches. Thus, it appears that the current anomaly detection based method using the K-Means clustering technique suffers from number of major unresolved issues, including the locally optimal issue the outlier detection problem, the high false alarm rate, the cluster K determination problem, the data overload problem.

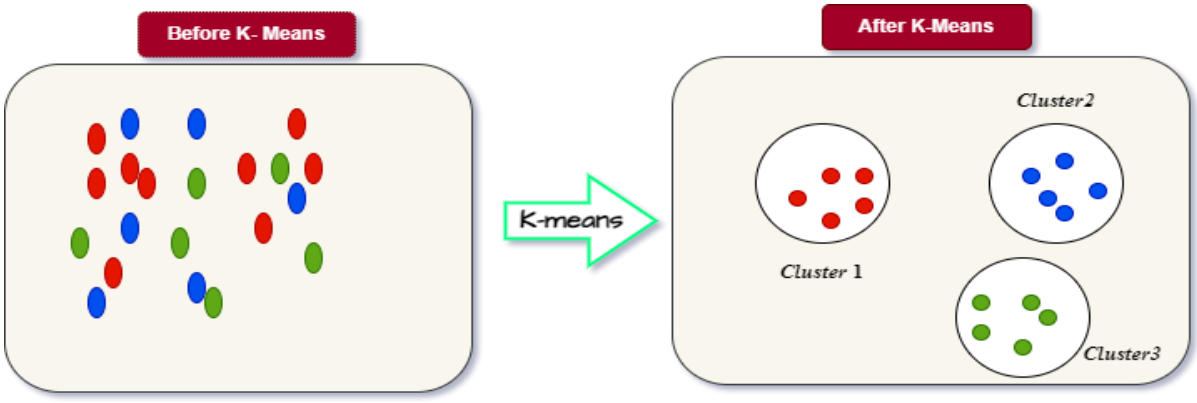

Fig 1: General working principal of K-means clustering algorithms

In order to optimise the detection rate and lower the false alarm rate needs both enhancement and minimization, which is a challenging feature. The K-Means Clustering integrated machine learning algorithm is being used in this study to enhance the current K-Means clustering methodology employed in the Anomaly Based Detection (ABD) method.

- Decision Tree

Using a decision tree, you can classify objects, that employs the divide and conquer method. Decision nodes and leaf nodes forms a decision tree, in which class value is represented by a leaf node, and the decision node describes a test over one of the features. Every route follows rule from root node to leaf node. Error in classification is the main performance metric for decision trees. The percentage of incorrectly classified cases is used to measure classification error.

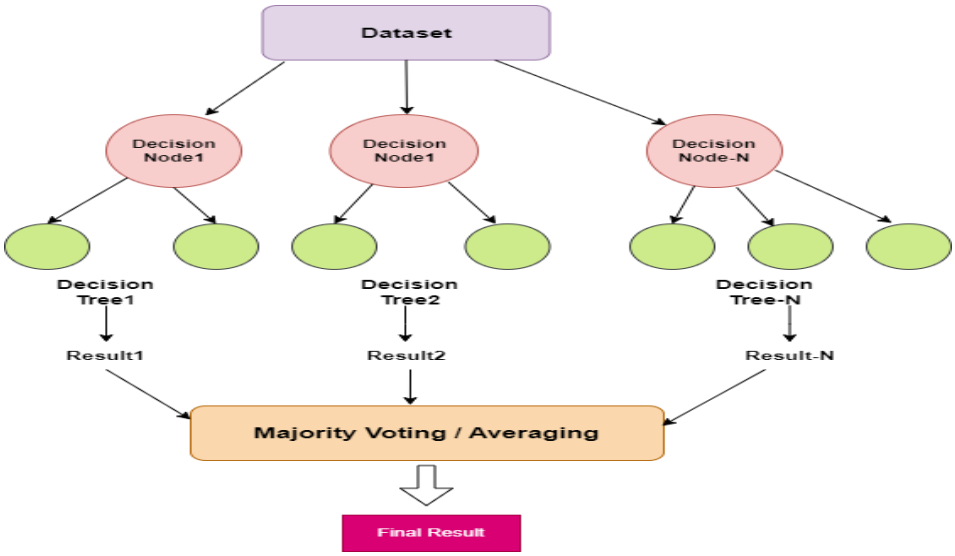

Fig 2: General working principal of decision tree

Large training data sets are frequently used in practise, which increases the number of branches and levels in the decision tree that is produced. The classification accuracy of a decision tree is significantly decreased as the number of class categories increases. Different algorithms, including ID3, J48, FT, BFTree, LMT, and many others, can be used to create decision trees. We used the J48 algorithm for our study since it has a higher accuracy rate Quinalan first introduced the J48 algorithm in 1993.

Pseudo code for C4.5 (J48) algorithm

```
1: Create a root node N;
2: If (T belongs to same category C)
{leaf node=N;
mark N as class C;
return N;}
3: For i=1 to n
{Calculate Information_gain (Ai);}
4: ta= testing attribute;
5: N. ta= attribute having highest information_gain;
6: if (N. ta==continuous)
{find threshold; }
7: For (Each T' in the splitting of T)
8: if (T' is empty)
{ child of N is a leaf node;}
9: else
{child of N= dtree (T')}
10: calculate classification error rate of node N;
11:   return N;
```

- Random forest

Random forest refers to a group of unpruned classification or regression trees. Among the existing data mining techniques, it has the highest accuracy, particularly for large data sets with numerous features.

Many classification trees are created using a random forest. Applying a tree classification technique, every tree is constructed using a unique bootstrap sample taken from the original data. After the forest formed each tree in the forest is given a new object that needs to be classified and placed there for classification. Each tree casts a vote indicating its choice for the object's class. The class that receives the most votes for the object is selected by the forest. To obtain an unbiased estimation of the test error in the random forests algorithm, cross-validation or a test set are not required.

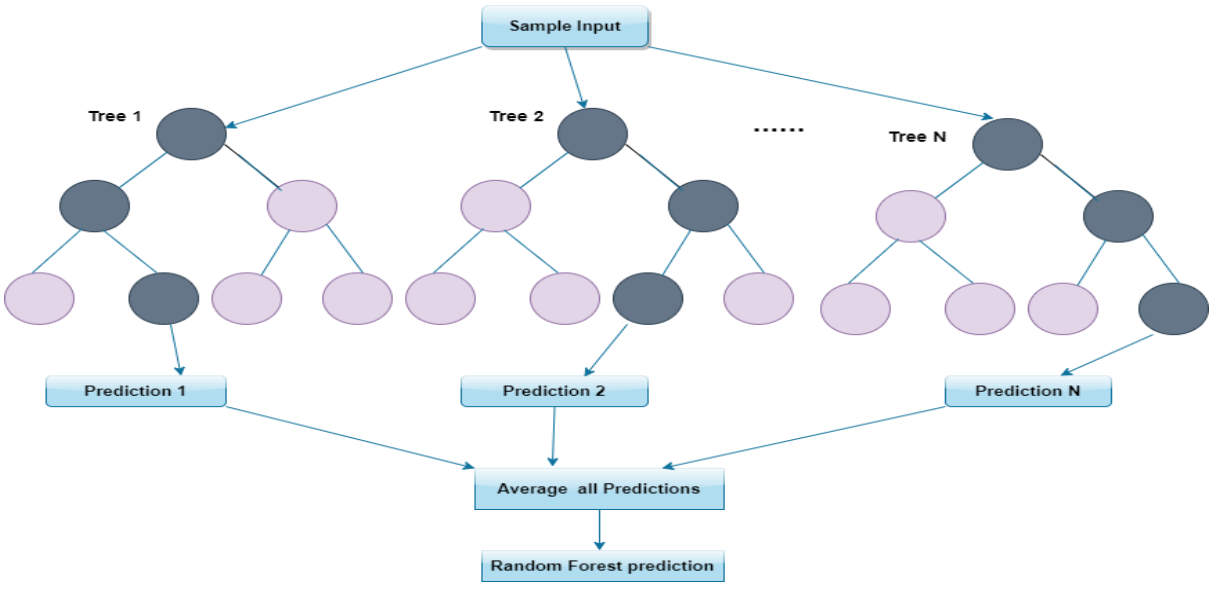

Fig 3: General working principal of Random Forest Prediction

It employs proximity to identify outliers in the data that are generally small. Most helpful tool of the random forests algorithm is the proximities. All of the dataset's instances are placed under each tree in the forest after it has been created. The proximity between k and n is raised by one if they are on the same leaf of a tree. The proximities are finally normalised by dividing by the total number of trees.

- K-Nearest Neighbours

KNN is an algorithm for supervised ML which is used to solve both classification and regression issues. All labelled samples require any pre-processing of all labelled samples before their use. The algorithm makes use of "feature similarity" to forecast the values of new data points. An unclassified input sample vector y is matched with its closest neighbours x. as part of the method. This idea can be extended to the nearest neighbours. The closest distance becomes the decisive criterion when the number of nearest neighbours between classes is equal. Of course, this could still result in equality, therefore it's about creating a task for the last gathering with individuals who will be impacted by equality. We opted the Euclidean distance, which is defined as follows, out of the several distance metrics.

$$D = \sqrt{\sum_{k=1}^{n}(X_i - Y_i)^2} \quad (1)$$

Better accuracy depends on selecting the right k. It depends on the learning data set. After executing a number of tests, we decided on the value of k=1, which provides the best outcomes.

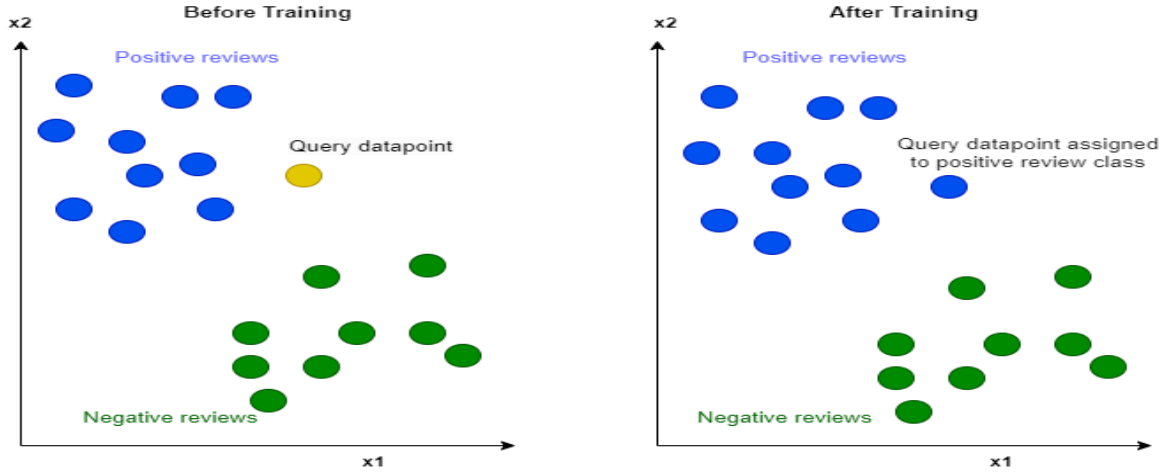

Fig 4: General working principal of K-Nearest Neighbours Algorithms

- Multilayer Perceptron

Three main components make up a neuron: nucleus, dendrites, and axons. An ANN is used to solve complex issues, and each of these parts is taken into consideration. The nervous system's network, (i.e. neural network) is a complex structure for solving problems that is made up of billions of neurons. It is possible to use algorithms to solve complex and challenging issues that emulate the behaviour of this natural system. A group of neurons can be utilised to recognise patterns and categorise information while a single neuron performs weakly in making decisions. An ANN typically consists of the several components shown in Figure 5. The output of an ANN is produced in each section by the interaction of multiple artificial neurons.

As depicted in Figure5, it consists of three different types of layers- input, output, and hidden. In input layer input signals are received for processing. The output layer performs the necessary tasks, like prediction and classification. Arbitrary number of hidden layers that are positioned in between the input and output layers make up the MLP's computational engine. In MLP, the data flows forward from the input to the output layer, similar to a feed-forward network. The MLP neurons are trained using the back propagation learning algorithm.

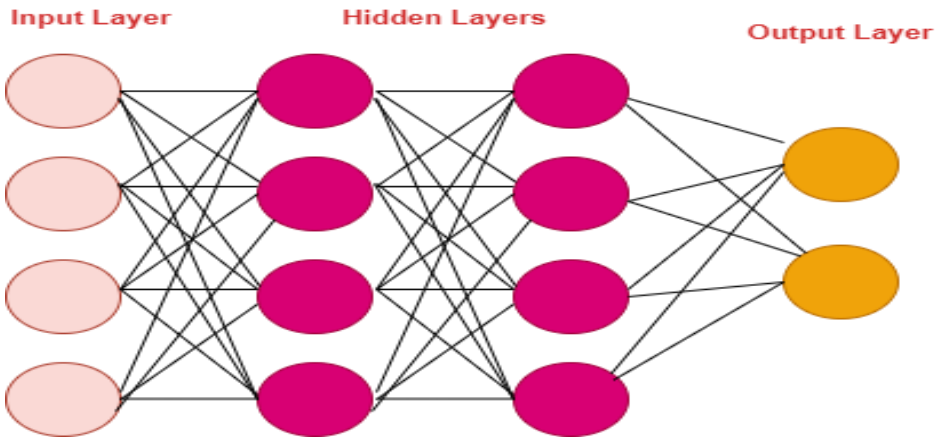

Fig 5: General working principal of Multilayer perceptron (MLP)

3.1 Dataset

The KDDCUP'99 dataset is the largest and most complete dataset that is commonly utilised in research and development of machine learning-based IDS.

The KDDCUP'99 dataset's classification of the attack types is initially grouped into two categories of connections: normal traffic and attack connections. In addition, the attack linkages are divided into 4 different categories, namely:

- DoS (Denial of Service): This attack which aims to overflows networks with specific data packets in an effort to shut down network services.
- Probe: This attack designed to monitor activity and search for information about possible vulnerabilities from a specific network address.
- R2L (Remote to Local): This attack used to get unauthorised remote access to a specific network address.
- U2R (User to Root): This attack used to extend user access rights to superuser or other levels of privilege.

Each of these four attack types is divided into a number of sub types. Table1 provides a summary of the entire attack classification.

Table 1. Attacks classification in KDD'99 cup dataset

Two-Class				
normal	abnormal/attack			
Multiclass (5 Labels)				
normal	DoS	Probe	R2L	U2
Multiclass (23 Labels)				
normal	smurf	satan	warezclient	buffer_overflow
	neptune	ipsweep	guess_passwd	rootkit
	back	portsweep	warezmaster	loadmodule
	teardrop	nmap	imap	perl
	pod	ftp_write		
	land	multihop		
		phf		
		spy		

4. Experimental Results and Discussion

This section includes, using KDD CUP99 dataset, we analyse our method's performance for two classification tasks (normal traffic vs. threats). Finally, a comparison of the K Means, Decision Trees, Multi-Level Perceptrons, Random Forest, and KNN classification algorithms is given. To determine the effectiveness of the proposed system, we conducted a number of experiments. For the

implementation of our model, we employed Python and TensorFlow. On a 64-bit Windows machine with 12th Gen Intel(R) Core(TM) i3-12100 3.30 GHz all of our experiments were carried out. For the purpose of our assessments, we made use of the KDD CUP99 dataset (which is mentioned in Section 3). This dataset is used as a benchmark in NIDS. Additionally, using this dataset makes it easier to compare results with recent methods and research.

We examined the effectiveness of our strategy using various performance metrics. Out of the total samples, accuracy determines how many classifications were accurate. Precision, recall, f1-score, and accuracy are calculated as described below to compare the potential of different classifiers.

$$Accuracy = \frac{TP+TN}{Total\ Samples} \tag{2}$$

$$Precision = \frac{TP}{TP+FP} \tag{3}$$

$$Recall = \frac{TP}{TP+FN} \tag{4}$$

$$Fscore = 2 * \frac{Precision*Recall}{Precision+Recall} \tag{5}$$

Table 2. System Performance using the KDD CUP99 dataset

	K Means	Decision Trees	Multi-Level Perceptron	Random Forrest Classifier	KNN
Precision	0.93	0.95	0.94	0.95	0.94
Recall	0.93	0.93	0.92	0.93	0.92
F1-score	0.93	0.93	0.93	0.93	0.93

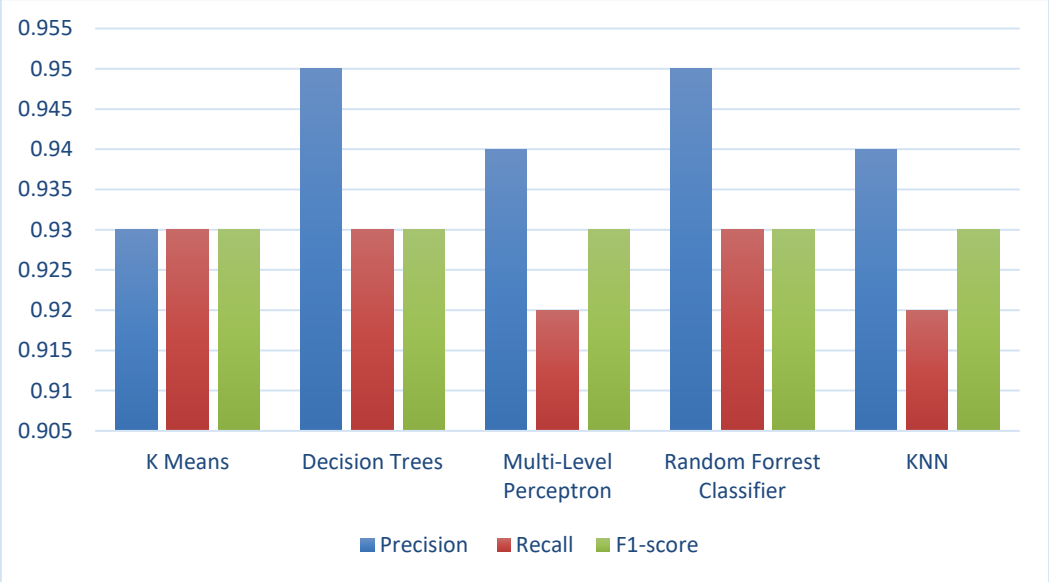

Fig 6. Performance matrix based on different classifiers

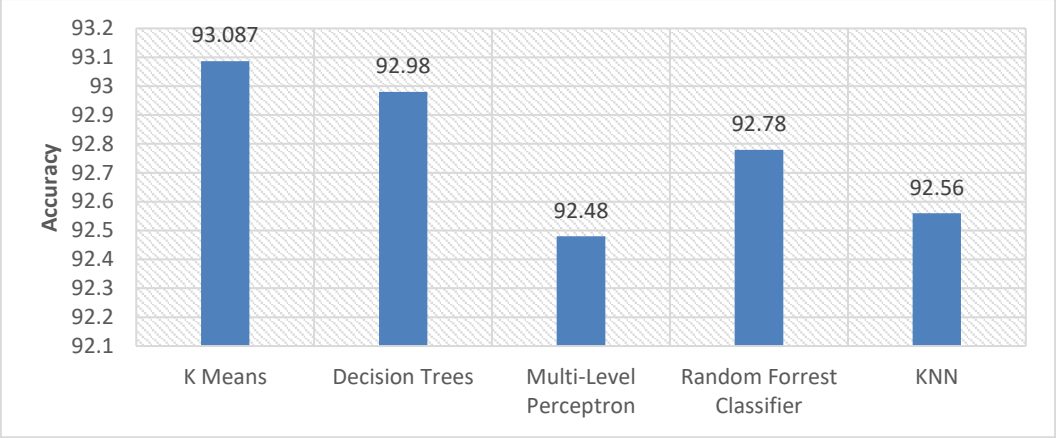

Fig 7. Results of accuracy performance comparisons between several machine learning-based methods

To evaluate the performances of each classifier based IDS model, Figure 6 and Figure 7 show the comparison of accuracy, precision, recall, and f1-score, respectively.

5. Conclusion

With the use of machine learning, we successfully developed a network intrusion detection model which applies to a real network. The developed model that is used with IDS performs effectively in identifying attacks on a real network. Results from the experiment on a number of categorization models show that K-means provides the best results. With the KDD CUP99 dataset, the proposed method for network intrusion detection has high accuracy. To show how the proposed NIDS system outperforms the existing systems, we have compared it to state-of-the-art methodologies and analysed it using several performance metrics. This work can be extended to find dynamic intrusions on live network traffic.

References

[1] Alabdulatif, A. and Rizvi, S.S.H., 2023. Network intrusion detection system using an optimized machine learning algorithm. *Mehran University Research Journal of Engineering & Technology*, *42*(1), pp.153-164.

[2] Sable, N.P., Rathod, V.U. (2023). Rethinking Blockchain and Machine Learning for Resource-Constrained WSN. In: Neustein, A., Mahalle, P.N., Joshi, P., Shinde, G.R. (eds) AI, IoT, Big Data and Cloud Computing for Industry 4.0. Signals and Communication Technology. Springer, Cham. https://doi.org/10.1007/978-3-031-29713-7_17.

[3] Solanke, O.O., Adegboyega, T.A., Taiwo, A.I., Abdullah, K.A., Ayo, F.E., Odule, T.J., Hassan, S.O. and Efuwape, B.T., 2022. A HYBRID MACHINE LEARNING MODEL FOR NETWORK INTRUSION DETECTION. *LAUTECH Journal of Engineering and Technology*, *16*(2), pp.152-157.

[4] N. P. Sable, V. U. Rathod, M. D. Salunke, H. B. Jadhav, R. S. . Tambe, and S. R. . Kothavle, "Enhancing Routing Performance in Software-Defined Wireless Sensor Networks through Reinforcement Learning", International Journal of Intelligent Systems and Applications in Engineering (IJISAE), vol. 11, no. 10s, pp. 73–83, Aug. 2023.

[5] Ahmad, I., Ul Haq, Q.E., Imran, M., Alassafi, M.O. and AlGhamdi, R.A., 2022. An efficient network intrusion detection and classification system. *Mathematics*, *10*(3), p.530.

[6] Y. Mali, "A Comparative Analysis of Machine Learning Models for Soil Health Prediction and Crop Selection", International Journal of Intelligent Systems and Applications in Engineering (IJISAE), vol. 11, no. 10s, pp. 811–828, Aug. 2023.

[7] Al-magsoosi, A.A.D., Mohammed, G.N. and Ramadhan, Z.A., 2021. Comparison and analysis of supervised machine learning algorithms. *Periodicals of Engineering and Natural Sciences*, *9*(4), pp.1102-1109.

[8] Rathod, V.U. and Gumaste, S.V., 2022. Role of Neural Network in Mobile Ad Hoc Networks for Mobility Prediction. International Journal of Communication Networks and Information Security, 14(1s), pp.153-166.

[9] Alhajjar, E., Maxwell, P. and Bastian, N., 2021. Adversarial machine learning in network intrusion detection systems. *Expert Systems with Applications*, *186*, p.115782.

[10] Vijay U. Rathod* & Shyamrao V. Gumaste, “Effect Of Deep Channel To Improve Performance On Mobile Ad-Hoc Networks”, J. Optoelectron. Laser, vol. 41, no. 7, pp. 754–756, Jul. 2022.

[11] N. P. Sable, V. U. Rathod, P. N. Mahalle, and P. N. Railkar, “An Efficient and Reliable Data Transmission Service using Network Coding Algorithms in Peer-to-Peer Network”, IJRITCC, vol. 10, no. 1s, pp. 144–154, Dec. 2022.

[12] Alqahtani, H., Sarker, I.H., Kalim, A., Minhaz Hossain, S.M., Ikhlaq, S. and Hossain, S., 2020. Cyber intrusion detection using machine learning classification techniques. In *Computing Science, Communication and Security: First International Conference, COMS2 2020, Gujarat, India, March 26–27, 2020, Revised Selected Papers 1* (pp. 121-131). Springer Singapore.

[13] N. P. Sable, R. Sonkamble, V. U. Rathod, S. Shirke, J. Y. Deshmukh, and G. T. Chavan, “Web3 Chain Authentication and Authorization Security Standard (CAA)”, IJRITCC, vol. 11, no. 5, pp. 70–76, May 2023.

[14] Khraisat, A., Gondal, I., Vamplew, P. and Kamruzzaman, J., 2019. Survey of intrusion detection systems: techniques, datasets and challenges. *Cybersecurity*, *2*(1), pp.1-22.

[15] V. U. Rathod and S. V. Gumaste, “Role of Deep Learning in Mobile Ad-hoc Networks”, IJRITCC, vol. 10, no. 2s, pp. 237–246, Dec. 2022.

[16] V. U. Rathod, Y. Mali, R. Sable, M. D. Salunke, S. Kolpe and D. S. Khemnar, "The Application of CNN Algorithm in COVID-19 Disease Prediction Utilising X-Ray Images," 2023 3rd Asian Conference on Innovation in Technology (ASIANCON), Ravet IN, India, 2023, pp. 1-6, doi: 10.1109/ASIANCON58793.2023.10270221.

[17] Ghurab, M., Gaphari, G., Alshami, F., Alshamy, R. and Othman, S., 2021. A detailed analysis of benchmark datasets for network intrusion detection system. *Asian Journal of Research in Computer Science*, *7*(4), pp.14-33.

[18] V. U. Rathod, N. P. Sable, N. N. Thorat and S. N. Ajani, "Deep Learning Techniques Using Lightweight Cryptography for IoT Based E-Healthcare System," 2023 3rd International Conference on Intelligent Technologies (CONIT), Hubli, India, 2023, pp. 1-5, doi: 10.1109/CONIT59222.2023.10205808.

[19] Sarker, I.H., Abushark, Y.B., Alsolami, F. and Khan, A.I., 2020. Intrudtree: a machine learning based cyber security intrusion detection model. *Symmetry*, *12*(5), p.754.

[20] N. P. Sable, M. D. Salunke, V. U. Rathod and P. Dhotre, "Network for Cross-Disease Attention to the Severity of Diabetic Macular Edema and Joint Retinopathy," 2022 International Conference on Smart Generation Computing, Communication and Networking (SMART GENCON), Bangalore, India, 2022, pp. 1-7, doi: 10.1109/SMARTGENCON56628.2022.10083936.

[21] Moustafa, N., Creech, G. and Slay, J., 2018. Anomaly detection system using beta mixture models and outlier detection. In *Progress in Computing, Analytics and Networking: Proceedings of ICCAN 2017* (pp. 125-135). Springer Singapore.

[22] N. P. Sable, V. U. Rathod, P. N. Mahalle and D. R. Birari, "A Multiple Stage Deep Learning Model for NID in MANETs," 2022 International Conference on Emerging Smart Computing and Informatics (ESCI), Pune, India, 2022, pp. 1-6, doi: 10.1109/ESCI53509.2022.9758191.

[23] Moustafa, N., Turnbull, B. and Choo, K.K.R., 2018. An ensemble intrusion detection technique based on proposed statistical flow features for protecting network traffic of internet of things. *IEEE Internet of Things Journal*, *6*(3), pp.4815-4830.

[24] V. U. Rathod and S. V. Gumaste, "Role of Routing Protocol in Mobile Ad-Hoc Network for Performance of Mobility Models," 2023 IEEE 8th International Conference for Convergence in Technology (I2CT), Lonavla, India, 2023, pp. 1-6, doi: 10.1109/I2CT57861.2023.10126390.

[25] Sarker, I.H., Kayes, A.S.M., Badsha, S., Alqahtani, H., Watters, P. and Ng, A., 2020. Cybersecurity data science: an overview from machine learning perspective. Journal of Big data, 7, pp.1-29.

[26] N. P. Sable, V. U. Rathod, R. Sable and G. R. Shinde, "The Secure E-Wallet Powered by Blockchain and Distributed Ledger Technology," 2022 IEEE Pune Section International Conference (PuneCon), Pune, India, 2022, pp. 1-5, doi: 10.1109/PuneCon55413.2022.10014893.

[27] G, A. ., K, S. ., S, B. ., M, B. ., & M, P. . (2023). Power Consumption and Carbon Emission Equivalent for Virtualized Resources – An Analysis: Virtual Machine and Container Analysis for Greener Data Center. International Journal on Recent and Innovation Trends in Computing and Communication, 11(1), 110–116. https://doi.org/10.17762/ijritcc.v11i1.6057

[28] Andrew Hernandez, Stephen Wright, Yosef Ben-David, Rodrigo Costa, David Botha. Optimizing Resource Allocation using Machine Learning in Decision Science. Kuwait Journal of Machine Learning, 2(3). Retrieved from http://kuwaitjournals.com/index.php/kjml/article/view/195

[29] Sharma, R., Dhabliya, D. A review of automatic irrigation system through IoT (2019) International Journal of Control and Automation, 12 (6 Special Issue), pp. 24-29.