International Journal of Early Childhood Special Education (INT-JECSE)
DOI: 10.48047/INTJECSE/V14I10.30 ISSN: 1308-5581 Vol 14, Issue 10, 2022

INTRUSION DETECTION MODEL USING FEATURE SELECTION AND MACHINE LEARNING CLASSIFIER

Navjot Kaur, Jaspreet Kaur
Department of Computer Science & Engineering, CT University, Ludhiana (Punjab), India
Email: navkaurtoor@gmail.com

Abstract:
In the past decade with the advancement of networking, the network traffic size and complexity have grown. Alongside this, malicious activities are also increasing. One of the most popular methods for finding malicious activity in any network is to analyze its traffic using an intrusion detection system. There are many different approaches to designing intrusion detection systems, but the machine learning technique is the most effective. The performance of a machine learning-based intrusion detection system was negatively impacted by the redundant and unnecessary information that was discovered in network traffic. To address such issues, the detection system can use feature selection alongside effective classifiers. In this paper, we implement a hybrid Feature selection where entropy-based infinite feature selection in the first stage and Eigenvector centrality, and ranking feature selection algorithms in the second stage to optimally reduce the size of the network traffic dataset. After that three machine learning classifiers i.e., ANN, KNN, and DT are used to classify network traffic as normal or attack. Various metrics, including accuracy, recall, precision, and f1-score, are utilized to validate and evaluate the performance of the suggested feature selection and IDS model on the NSLKDD dataset.
Keywords: Feature selection (FS), Machine learning (ML), NSLKDD dataset, intrusion detection systems (IDS).

I. INTRODUCTION

Today's environment offers networking and Internet of Things technologies for daily usage since wireless sensor network (WSN) technology is always growing. It has become popular in order to solve difficult real-world problems including environmental monitoring, applications in defense, home automation, and geographical monitoring, and a vast amount of government, business, military, and personal data are kept on networking systems [1]. Despite their impressive capabilities and wide range of applications, due to limited computational power, energy, less storage memory, and low bandwidth of sensor nodes, the most significant issue facing wireless sensor network applications is network security [2]. Traditional defense mechanisms like public key infrastructure, authentication, encryption, and host-based intrusion detection techniques are available for safeguarding IoT applications [3]. These Prevention methods usually act as the first line of defense and can protect at some level. However, cryptography based on secret key management is insufficient to safeguard the WSN since, even with this first line of defense in place, multiple assaults may still be able to obtain sensitive data and utilize it for illicit reasons. These security mechanisms are effective only against external attacks but cannot adequately defend against network insider attacks such as compromised attacks as well as routing attacks which are carried out by hacked or malicious nodes already connected to the network [4]. Once the node is compromised, it has the potential to steal sensitive information and use it for malicious reasons such as controlling the whole WSN to degrade its performance. As a result, we can't rely solely on intrusion prevention systems [5]. Network users can employ intrusion detection-based network security solutions to keep their systems safe from hackers or intruders. Therefore, the goals of security are confidentiality, integrity, and availability. An intrusion detection system (IDS) is a kind of security instrument or an alarm system that keeps an eye on network activity, checks the system for questionable activity, and notifies the network administrator or system before hackers launch internal or external intrusions. It can serve as a second line of defense [6]. There are two primary types of intrusion detection systems: Network-based IDS and Host-based IDS. To monitor network traffic for intrusions, a Network-based Intrusion Detection System (NIDS) is installed at network points like routers and gateways. A host-based intrusion

detection system, or HIDS, keeps an eye on each host or device and notifies the user when it notices suspicious activity, such as altering or erasing a system file, initiating an unauthorized series of system calls, or making unauthorized configuration changes. At a high level, the detection mechanisms of IDSs are of three main kinds: Firstly, misuse-based intrusion detection systems (IDSs) monitor known attack patterns in signatures and use this signature basis to analyze network traffic for attacks that resemble them. Secondly, in order to find abnormalities, anomaly-based intrusion detection systems compare the behavior of the system to previously documented cases of normal system behavior. Third, hybrid IDS employs both techniques together [7-8].

A typical Intrusion Detection System (IDS) must overcome a number of obstacles, including the massive volume of network data, uneven distribution of the data, and difficulties in classifying the data as normal or anomalous. However, using normal procedures does not distinguish between authorized and unauthorized communications, hence automatic and effective solutions are required. The use of AI-based methods for machine learning (ML) and deep learning (DL) can increase the efficacy of IDSs. Nowadays, Artificial intelligence (AI)-based methods are used to construct IDS, and they are more beneficial than earlier methods. While more effective, data mining techniques don't offer an ideal solution. Even for small networks, however, the IDS must analyze a large volume of data with high dimensions, which results in higher calculations and lower detection rates (DR). Due to the exponential growth in network traffic, the level of complexity of network behavior is increasing resulting in the possibility of overfitting the IDS Model. IDS's performance was negatively impacted by the redundant and unnecessary information that was discovered in its traffic. As a result, it is critical that only essential functionalities be chosen for an IDS. With the restricted availability of computing resources, a real-time intrusion detection system (IDS) is another challenge. Many ways have been presented throughout the years to draw attention to the aforementioned problems related to the IDS. Feature Selection (FS) methods is one of these techniques. Building an effective machine learning (ML) based network attack detection model requires appropriate feature selection techniques. More efficient collection and storage may be achieved with fewer features, which is essential for a high-speed Internet of Things network environment.

Our aim is to present an effective machine learning-based attack detection model that can effectively address the aforementioned constraints. This study's principal contribution is to design a hybrid feature selection to optimally reduce the size of the network traffic dataset and to validate and evaluate the performance of the proposed feature selection and IDS using various parameters such as accuracy (AC), recall, precision, and f1-score.

II. RELATED WORK

The literature studies based on machine learning techniques for network intrusion detection systems are covered in this part. Very few publicly accessible benchmark datasets are available for use in network intrusion detection system-based research projects. KDD CUP'99, NSL-KDD dataset, CAIDA 2007, and UNSW-NB15 are a few of them. To test out our suggested work, we used the NSL-KDD benchmark dataset. To start with R. Tahri et al. [9] employed three distinct machine learning algorithms: NB, SVM, and KNN. The USNWNB 15 dataset was used to evaluate the performance of three machine learning algorithms in order to identify the best accuracy outcomes. Based on the outcomes of the previous phase, the database was analyzed in the second step using the most efficient method. The NSLKDD and UNSWNB15 are two different datasets that the authors utilized to evaluate the model's performance. According to Sumaiya et al. [10], an IDS approach using multiclass support vector machine classification and chi-square feature selection yields low false alarm rates and high degree detection. The multi-class SVM shortens the time spent on exams and instruction. The NSL-KDD data set was used to evaluate the high accuracy of 98% and 0.13 as false positives. Manzoor and Kumar [11] proposed an Intelligent Intrusion Detection System. Pre-processing of the KDD-99 dataset was done to remove duplicate and redundant data from the dataset. Information Gain (IG) and Correlation Algorithm were combined for feature selection and the reduced features were fed to the ANN algorithm for training and testing purposes. The system was tested using five different subsets of the KDD-99 dataset. Achieved results were outperforming. Ravale et al., [12] a hybrid technique combination of K-means clustering algorithm and SVM classifier was proposed and evaluated using the KDD CUP 99 dataset. To decrease the number of attributes K-means clustering was used so that complexity was reduced and performance of the classifier increased in terms of

detection rate and accuracy. Simulation results proved that accuracy and detection rate increased for reduced attribute set but the overall detection rate still needs to be improved. Dong et al. [13] in order to solve the problem of high-dimension network traffic dataset to reduce the computation complexity, an intrusion detection model for WSN based on the Information Gain (IG) Ratio and Bagging Algorithm was proposed. In the data pre-processing stage, IG was used for feature selection and then the Bagging Algorithm was used to construct an ensemble classifier to train several C4.5 decision trees. The parameters of the ensemble classifier were optimized by 10 iterations and then a dynamic pruning process was used to reduce prediction error. The detection accuracy of Blackhole, Grey hole, Flooding, Scheduling, and Normal was 99.04%, 97.96%, 99.02%, 96.21%, and 98.85% respectively. Research can be extended for another type of attack in the WSN data set, using other feature selection techniques combined with deep learning models for WSN intrusion detection. In order to identify network intrusion, Miranal et al. [14] developed an intrusion detection system (IDS) based on a deep learning method utilizing the NSL-KDD dataset. The model is capable of learning and adapting to identify novel patterns that were previously uninterpreted. The suggested model combines auto-encoder and logistic regression with the NSL-KDD dataset for training. The model has an accuracy score greater than 84%. S Manimurugan [15] proposed an IDS in which the Crow Search Optimisation method combined with the Adaptive Neuro-Fuzzy Inference System (CSO-ANFIS). The ANFIS was a hybrid of a fuzzy interference system and an artificial neural network, and the crow search optimization technique was used to improve the ANFIS's performance. The NSL-KDD data set was utilized to test the proposed model's performance of intrusion detection, and the experiment results were compared to other current methodologies for overall performance validation. The results of intrusion detection based on the NSL-KDD dataset were better and more efficient, with a detection rate of 95.80% and a FAR of 3.45%. Faezah et al. [16] used a wrapper approach based on the Differential Evolution methodology for IDS to decrease the characteristics of the data. Because characteristics that aren't important affect the accuracy of IDS, fewer features have been included. The objective is to use differential evolution to choose some features from the NSL-KDD dataset, and to use ETM to assess the model's performance. 0.15% for five classes and 87.3% for two classes was the classification rate that the suggested model managed to achieve. Tang et al. [17] implemented a deep learning algorithm for detecting network intrusion and trained the model with the NIDS dataset by taking only 6 basic features from 41 features. In this study, only those features are considered that contain more valuable information on one specific type of attack, like DDoS, to increase the accuracy of the NIDS. Ieracitano et al. [18] suggested an IDS that extracts optimized and more connected characteristics by combining statistical methods, data analytics, and the latest developments in machine learning theory. Then IDS is validated against the benchmark NSL-KDD database in terms of AUC: 95.65% and 96.1% for binary classification and multi-class classification, respectively.

III. PROPOSED MODEL

Our suggested technique, which is depicted in Fig. 1, breaks this research down into five steps. The first phase is data collecting. Phase 2 follows data gathering and is known as data pre-processing. Duplicate values inside the dataset are eliminated during data pre-processing. Furthermore, inconsistent values are eliminated. The dataset was examined to determine whether or not missing values existed. Normalization of data was also carried out in order to reduce the entire dataset to a single standard scale. A non-numerical value was transformed by encoding it into a numeric value. Feature selection was the third step after data pre-processing, and it was carried out using hybrid feature selection. Following feature selection, the fourth phase involves the application of a machine learning classifier. The evaluation step, which is the fifth stage, compares this research to other recent studies that employed the same methodology.

A. Data Collection:

As previously indicated, the proposed approach makes use of datasets i.e. NSLKDD to identify various attacks in the WSN ecosystem. The NSL-KDD dataset, an improved version of the widely used KDD-Cup99 dataset that has garnered popularity in the cybersecurity community, is incorporated into the suggested ID model. Like its predecessor, this dataset consists of 41 characteristics divided into groups depending on traffic, content, and fundamental attributes. NSL-KDD is distinguished by its accurate labelling system, which correctly determines the kind of attack in addition to classifying incoming traffic as either regular or assault. There are four different classes

in the dataset: DOS, probe, U2R, and R2L. These classes each correspond to a particular type of attack.

Table I Different attacks present in NSLKDD database

Class	Training dataset	Testing dataset
Dos	back, land, Neptune, pod, smurf, teardrop	back, land, neptune, pod, smurf, teardrop, (mailbomb), process table, udpstorm, apache2, worm
Probe	ipsweep, nmap, portsweep, satan	IPS-weep, Nmap, ports-weep, satan, mscan, saint
U2R	Buffer overflow, load module, Perl, Rootkit	Buffer overflow, load module, perl, rootkit, sql attack, xterm, pst
R2L	ftp-write, guess-passwd, imap, multihop, phf, spy, warezmaster	ftp-write, guess-passwd, imap, multihop, phf, spy, warezmaster, xlock, xsnoop, snmpguess, snmpget attack, HTTP tunnel, send-mail, named, warez client

B. Preprocessing

Pre-processing of original data from KDD and NSL databases is used in the proposed research to prepare data for subsequent phases because the data in the training and testing sets are unequal and imbalanced. However, this data cannot be directly used in the suggested ID technique. It needs to eliminate any null or empty cells from the data in order to reduce their complexity, so it might not lead to biased or unsatisfactory findings. It further improves detection accuracy and reduces False Alarm Rates (FAR).

C. Feature Selection

It is clear from reviewing the literature related to IDSs that intrusion detection systems (IDS) are the first line of defense, constantly monitoring network activity to spot and stop possible security breaches. All ID systems, however, find it challenging to evaluate the massive volume of data created on the internet every minute, which results in processing times, complexity, and accuracy results that are lower. The necessity of applying the FS approach stems from the reality that not every element in the massive landscape of network data is equally significant or instructive for identifying intrusions. Choosing the appropriate characteristics is like shining a light on the most important facets of network behaviour. IDS may drastically lower the computing burden, increase the speed of analysis, and improve detection accuracy by carefully selecting characteristics that capture key patterns and abnormalities.

In this research, we use the hybrid feature selection algorithms not only to reduce dimensionality, but also to select optimal features that produce high results in terms of accuracy, precision, recall, and F1-Scores. It also decreases the computational cost of the Algorithm. In this phase, features are selected in two steps in which two algorithms i.e., i.e., Modified Infinite Feature Selection (MIFS) and Eigenvector Centrality and Ranking Feature Selection (ECRFS) are used due to their benefits and shown effectiveness in raising the dependability of ID systems. In the first step, the infinite feature selection technique is used in its modified form to extract the most informative features from a dataset in which entropy is one of the important factors that must be taken into consideration along with other two factors i.e., Standard Deviation (STD) and Correlation while calculating the feature weights. It considers an infinite pool of features and uses a ranking criterion to determine their relevance. IFS's basic principle is to repeatedly assess every feature that might be present while progressively raising the feature selection threshold until the required number of features or a certain performance condition is satisfied. The Eigenvector Centrality and Ranking FS algorithm (ECRFS) is utilised in the second step of the suggested hybrid feature selection approach to determine the significance of the features. The ECRFS calculates a feature's relevance based on the significance of its neighbours by using features produced by the MIFS algorithm in the preceding phase as input.

DOI: 10.48047/INTJECSE/V14I10.30 ISSN: 1308-5581 Vol 14, Issue 10, 2022

D. Classification

Following the collection and selection of all pertinent features from the databases that are accessible, the presented data has to be categorised as either normal or intrusive data. In the current work, ANN, KNN, and DT were used as intrusion classifiers to categorise the data as either normal or intrusive and whose effectiveness is evaluated and examined using the NSLKDD dataset. The process used for each classifier divides the dataset into training and testing datasets in a 70:30 ratio once the best feature set with lots of patterned information is chosen. The testing data is sent to the classifier during training, and it attempts to match the final feature set. The classifiers identify an attack if the supplied data fits the properties in the feature set.

ANNs are a class of machine learning algorithms that draw inspiration from the behaviour of real neurons in the central nervous system and brain. Artificial neurons in one or more hidden layers receive ANN inputs, which are then weighted and processed to choose the output for the following layer. ANNs use a "learning rule" to adjust the hidden layer and output layer neurons' weights and biases in an adaptive manner. ANNs are ideally suited for tasks where the underlying patterns are not clearly described because of their tremendous adaptability and capacity to learn from fresh data. Given that network infiltration patterns are frequently intricate and non-linear. The multilayer nature of artificial neural networks (ANNs) allows them to capture these complex, non-linear interactions between various network activities [19].

In machine learning, KNN is a simple yet effective method, especially for applications involving regression and classification. KNN is a supervised learning classifier that divides the data into several classes based on the value of K and the Euclidean distance. It is simple to use and comprehend since it memorizes the full dataset, negating the need for training. It can, however, be computationally demanding, particularly when dealing with big datasets. Furthermore, the suitable distance metric and the selection of 'k' have a significant impact on its performance [20].

A decision tree solves the categorization issue by forming a structure like a tree. The features are represented by the tree's nodes, and their possible values are shown by the pathways. They work by recursively splitting the dataset into subsets based on the most significant features. The recursive method used by DT ends after all the data has been categorized because the tree's depth was set to zero.

Regarding the ANN, a feed-forward neural network with twenty neurons is used; the neighbour count for the KNN is set to the number of classes in the dataset; also, the count of bags for the DT classifier is set to three because that is how the number of bags is defined in the suggested scheme. After doing several runs to get the best results, these parameters are chosen.

IV. RESULT & ANALYSIS

Using MATLAB software, the effectiveness of the suggested intrusion detection model is monitored and examined. The proposed system aims to evaluate the effectiveness of the recommended method using a dataset, namely NSL-KDD. In addition, the suggested model makes use of three classifiers (ANN, KNN, and DT) to recognize and classify different kinds of attacks. Accuracy (AC), precision, recall, and F1-measure are used for evaluating NIDS performance.

- Accuracy (AC): The accuracy of an Intrusion detection model depicts the proportion of accurately predicted values in the network. Mathematically, it can be computed by using the formula given below

$$Accuracy\ or\ AC = \frac{TP + FP}{FP + TP + FN + TN}$$

- Precision: It can be defined as the percentage of those malicious activities which are actually malicious in a network. The precision of an ID system is inversely proportional to FAR, which means greater the precision, lesser will be FAR. Mathematically, it can be written as;

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

- Recall: It can be described as the ratio of True positive to the summation of True positive and false negative values. Mathematically, it can be represented as;

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

- F1-Score: It can be described as the harmonic mean of precision and recall and must be always higher in any threat detection model. The equation for calculating the F1-Score is given below.

$$F1 - Score = \frac{2 * Precision * Recall}{Precision + Recall}$$

The appropriateness of the proposed Feature selection is analyzed and put in comparison with standard models in terms of accuracy on the NSLKDD database. The accuracy comparison graph for the suggested ANN model and the conventional models is shown in Fig. 1. Upon detailed examination of the provided graph in Fig. 2, it can be noted that QDA models produce the lowest accuracy results, coming in at just 79.47%. MLP, LSTM, LDA, L-SVM, Q-SVM, AE, and DNN models follow with 81.4%, 81.43%, 83.17%, 83.65%, 83.65% 87%, and 91.5%, respectively. However, the suggested ANN-based threat detection model's accuracy result was found to be 94.635%, which is far higher than the results of any other model.

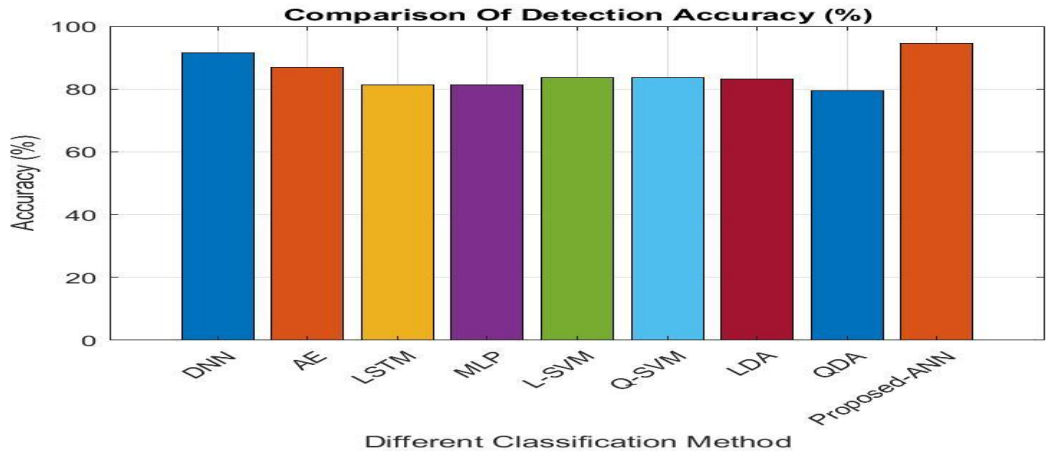
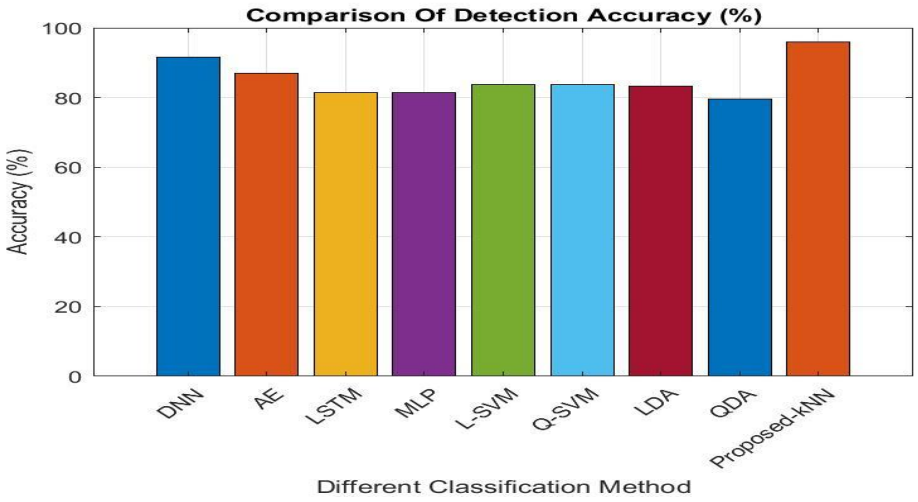


Figure 1: Analysis of the proposed ANN model's accuracy comparison using the NSLKDD dataset

On the NSLKDD database, the applicability of the suggested KNN scheme is also examined and its accuracy is compared with that of conventional models. Results from the comparison are displayed in Fig. 2. The 96.068% accuracy of the suggested KNN-based ID model is a strong indicator of its superiority in this graph. However, the accuracy ranged from 79.47% to 87% when the accuracy values were computed in QDA, MLP, LSTM, LDA, L-SVM, Q-SVM, AE, and DNN. This is much less than the accuracy found in the suggested model.



DOI: 10.48047/INTJECSE/V14I10.30 ISSN: 1308-5581 Vol 14, Issue 10, 2022

Fig.2 Analysis of the proposed KNN model's accuracy comparison using the NSLKDD dataset.

In a similar manner, the accuracy performance of the third classifier, or DT, is examined using the same dataset. The findings are shown in Fig. 3, where it can be seen that the value for the suggested DT model is 96.41%, which is marginally higher than the recommended KNN but greater than QDA, MLP, LSTM, LDA, L-SVM, Q-SVM, AE, and DNN models. The accuracy values obtained for both standard and proposed intrusion detection models displayed in Table II.

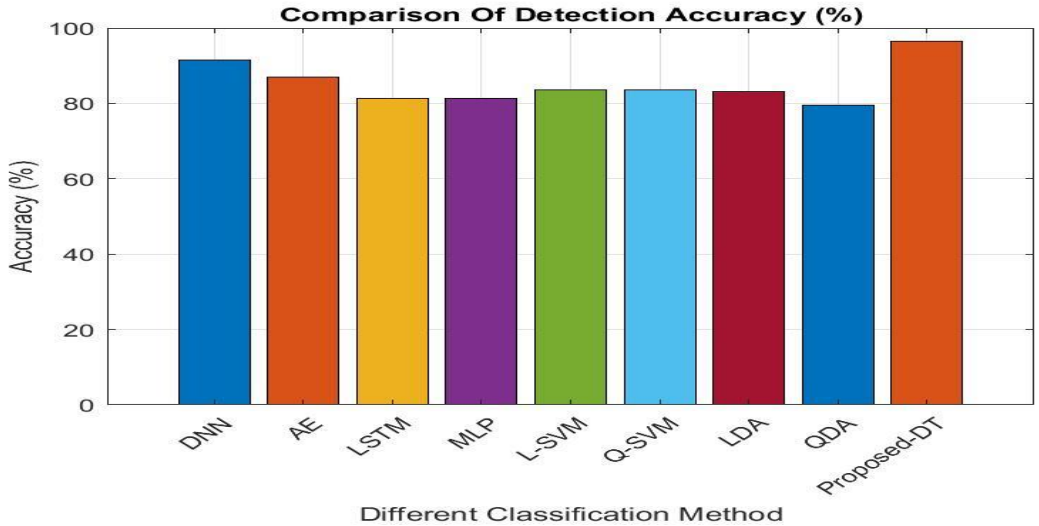


Fig.3 Analysis of the proposed DT model's accuracy comparison using the NSLKDD dataset.

Table II. The specific value of detection accuracy obtained for each model

Algorithms	**Accuracy %**
DNN	91.5
AE	87
LSTM	81.43
MLP	81.4
L-SVM	83.65
Q-SVM	83.65
LDA	83.17
QDA	79.47
PROPOSED-ANN	94.635
PROPOSED-KNN	96.068
PROPOSED -DT	96.401

As seen in Fig. 4, the precision values obtained from our technique (DT, KNN, and ANN) are subjected to an analysis and examination for efficacy. It shows the precision comparison graph in which the suggested ANN, KNN, and DT models had values of 96.581, 97.295, and 97.191 respectively. The suggested KNN model achieves the highest accuracy value at 98.041%, while the proposed DT model and the proposed ANN reach somewhat lower precision levels at 97.492% and 96.252%, respectively.

DOI: 10.48047/INTJECSE/V14I10.30 ISSN: 1308-5581 Vol 14, Issue 10, 2022

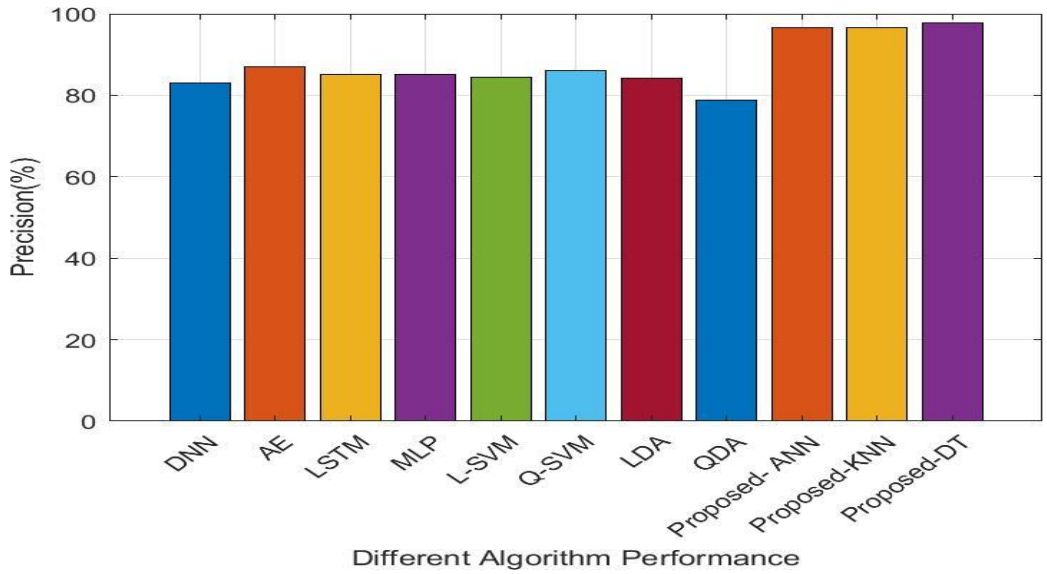


Fig. 4 A graph of precision comparison using the NSLKDD dataset.

Additionally, the F1-Score comparison between the proposed three ML models and the DL models analyses and validates their efficacy. The comparison graph showing the F1-score findings is shown in Fig. 5. It also shows that the F1-score values in the AE, LSTM, MLP, L-SVM, Q-SVM, LDA, and QDA models were only between 75-82 %. Conversely, the suggested KNN model had the highest F1-score value at 97.295 %, followed by the proposed DT model at 97.1915, and the proposed ANN model at 96.581%. Since the efficiency of a model is determined by its F1-Score, which needs to be as high as possible, the suggested KNN model outperforms the others based on these numbers.

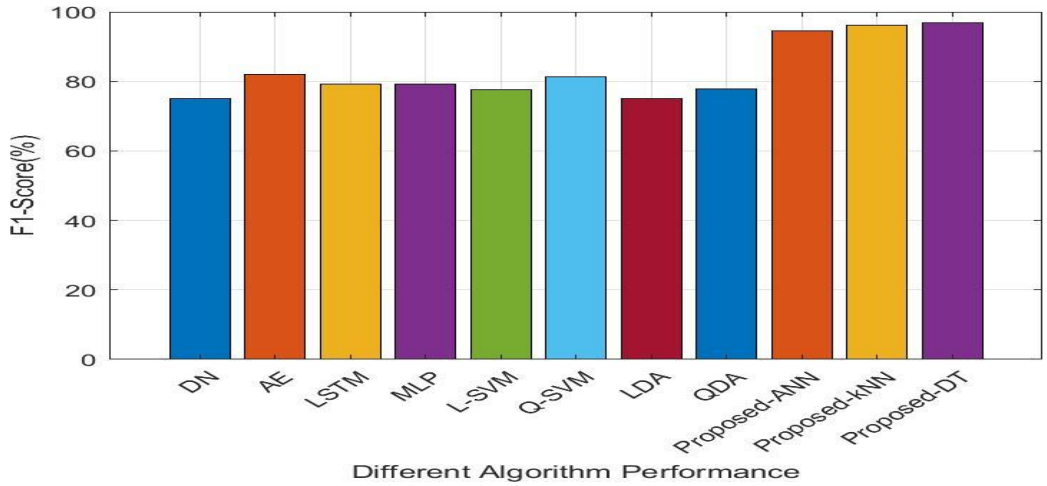


Fig. 5 A graph of F1-Score comparison using the NSLKDD dataset.

Furthermore, the performance of the proposed IDS models i.e., ANN, KNN, and DT models is observed and verified by comparing it with conventional DL models within the framework of Recall it came out to be 96.9%, 97.1%, and 97.3% as shown in Fig. 6. We captured the precise, F1-score, and Recall values in tabular form, which are displayed in Table III, in order to condense the values for all parameters on the NSLKDD dataset.

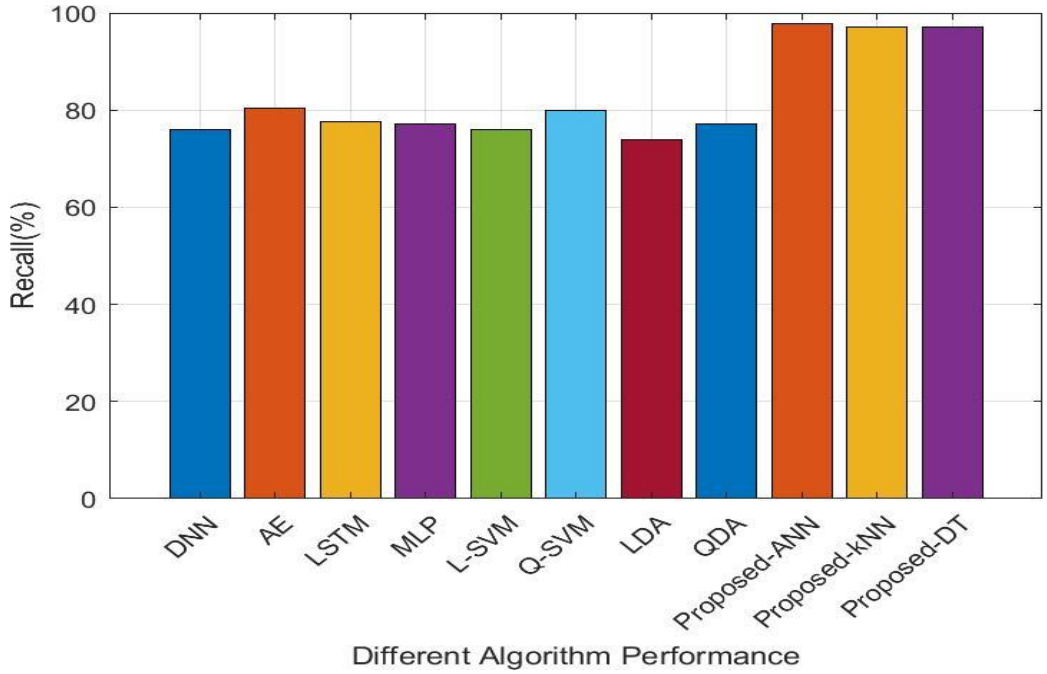


Fig. 6 A graph of Recall comparison using the NSLKDD dataset.

TABLE III Parameter Specific Value in the Proposed and Standard Models

Algorithms	**F1-score %**	**Precision %**	**Recall %**
DNN	75	83	76
AE	81.98	87	80.37
LSTM	79.24	85.13	77.70
MLP	79.24	85.03	77.13
L-SVM	77.54	84.32	76.06
Q-SVM	81.39	86.09	79.86
LDA	75.16	84.09	73.81
QDA	77.78	78.71	77.23
PROPOSED-ANN	96.581	96.252	96.913
PROPOSED-KNN	97.295	98.041	97.399
PROPOSED -DT	97.191	97.492	97.109

V. CONCLUSION

One of the challenges facing current network intrusion detection systems is handling massive amounts of data. Therefore, in order to achieve high detection accuracy with a low false alarm rate in the shortest amount of time, it becomes imperative to eliminate superfluous information and diminish its dimensionality by meticulously choosing the most important and relevant features. This paper emphasizes the significance of feature selection in IDS and assesses the performance of three ML algorithms i.e., ANN, KNN, and DT using the NSL-KDD intrusion detection dataset. To improve efficiency, the NSL-KDD dataset was first pre-processed to identify relevant features. Based on the analysis results, the three classifiers provided the highest detection accuracy rate (96.401%) for Decision Tree, the lowest accuracy rate (94.635%) for Artificial Neural Network, and KNN (96.068), which was somewhat lower than DT. According to empirical research, no single machine learning algorithm is capable of efficiently detecting every kind of attack. In the future, machine learning classifiers' accuracy rate can be raised and calculation times lowered by extracting pertinent features from the original dataset.

References

[1] Borges, L. M., Velez, F. J., & Lebres, A. S. (2014). Survey on the characterization and classification of wireless sensor network applications. *IEEE Communications Surveys & Tutorials*, *16*(4), 1860-1890.
[2] Rani, A., & Kumar, S. (2017, February). A survey of security in wireless sensor networks. In *2017 3rd International Conference on Computational Intelligence & Communication Technology (CICT)* (pp. 1-5). IEEE.
[3] Yang, Q., Zhu, X., Fu, H., & Che, X. (2015). Survey of security technologies on wireless sensor networks. *Journal of sensors*, *2015*.
[4] Padmavathi, D. G., & Shanmugapriya, M. (2009). A survey of attacks, security mechanisms and challenges in wireless sensor networks. *arXiv preprint arXiv:0909.0576*.
[5] Abduvaliyev, A., Pathan, A. S. K., Zhou, J., Roman, R., & Wong, W. C. (2013). On the vital areas of intrusion detection systems in wireless sensor networks. *IEEE Communications Surveys & Tutorials*, *15*(3), 1223-1237.
[6] Fuchsberger, A. (2005). Intrusion detection systems and intrusion prevention systems. *Information Security Technical Report*, *10*(3), 134-139.
[7] Farooqi, A. H., & Khan, F. A. (2009, December). Intrusion detection systems for wireless sensor networks: A survey. In *International Conference on Future Generation Communication and Networking* (pp. 234-241). Berlin, Heidelberg: Springer Berlin Heidelberg.
[8] Chaabouni, N., Mosbah, M., Zemmari, A., Sauvignac, C., & Faruki, P. (2019). Network intrusion detection for IoT security based on learning techniques. *IEEE Communications Surveys & Tutorials*, *21*(3), 2671-2701.
[9] Tahri, R., Balouki, Y., Jarrar, A., & Lasbahani, A. (2022). Intrusion Detection System Using machine learning Algorithms. In *ITM Web of Conferences* (Vol. 46, p. 02003). EDP Sciences.
[10] Thaseen, I. S., & Kumar, C. A. (2017). Intrusion detection model using fusion of chi-square feature selection and multi class SVM. *Journal of King Saud University-Computer and Information Sciences*, *29*(4), 462-472.
[11] Manzoor, I., & Kumar, N. (2017). A feature reduced intrusion detection system using ANN classifier. *Expert Systems with Applications*, *88*, 249-257.
[12] Ravale, U., Marathe, N., & Padiya, P. (2015). Feature selection based hybrid anomaly intrusion detection system using K means and RBF kernel function. Procedia Computer Science, 45(39), 428-435
[13] Dong, R. H., Yan, H. H., & Zhang, Q. Y. (2020). An Intrusion Detection Model for Wireless Sensor Network Based on Information Gain Ratio and Bagging Algorithm. IJ Network Security, 22(2), 218-230.
[14] S. Gurung, M. Kanti Ghose, and A. Subedi, "Deep Learning Approach on Network Intrusion Detection System using NSL-KDD Dataset," Int. J. Comput. Netw. Inf. Secur., vol. 11, no. 3, pp. 8–14, 2019, doi: 10.5815/ijcnis.2019.03.02
[15] Manimurugan, S., Majdi, A. Q., Mohmmed, M., Narmatha, C., & Varatharajan, R. (2020). Intrusion detection in networks using crow search optimization algorithm with adaptive neuro-fuzzy inference system. *Microprocessors and Microsystems*, *79*, 103261.
[16] F. H. Almasoudy, W. L. Al-yaseen, and A. K. Idrees, "ScienceDirect ScienceDirect Differential Evolution Wrapper Feature Selection for Intrusion Differential Evolution Wrapper Feature Selection for Intrusion Detection System Detection System," Procedia Comput. Sci., vol. 167, no. 2019, pp. 1230–1239, 2020, doi: 10.1016/j.procs.2020.03.438.
[17] Tang, T. A., Mhamdi, L., McLernon, D., Zaidi, S. A. R., & Ghogho, M. (2016, October). Deep learning approach for network intrusion detection in software defined networking. In *2016 international conference on wireless networks and mobile communications (WINCOM)* (pp. 258-263). IEEE.
[18] Ieracitano, C., Adeel, A., Morabito, F. C., & Hussain, A. (2020). A novel statistical analysis and autoencoder driven intelligent intrusion detection approach. *Neurocomputing*, *387*, 51-62.
[19] Ingre, B., & Yadav, A. (2015, January). Performance analysis of NSL-KDD dataset using ANN. In *2015 international conference on signal processing and communication engineering systems* (pp. 92-96). IEEE.

[20] Li, W., Yi, P., Wu, Y., Pan, L., & Li, J. (2014). A new intrusion detection system based on KNN classification algorithm in wireless sensor network. *Journal of Electrical and Computer Engineering, 2014*.