Available online at www.jcsonline.in Journal of Current Science & Humanities
12 (3), 2024, 35-50

Impact Factor-2.05

A development of smart intrusion detection system using machine learning and deep learning approach

Aniket Yadneshwar Dixit [1], Dr. S. B. Thorat [2], Dr. Pritam R. Patil [3], Mr. Amol V. Suryawanshi [4]

[1] Research Scholar, School of Computational Sciences, SRTMU University, Nanded-M.H., India
[2] Director, [3,4]Assistant Professor,
SSBE Society, Institute of Technology & Management, Nanded-M.H., India

Abstract. Modern life depends heavily on networks, and cyber security is becoming a vibrant field of study. Because of the variety of complex, current assaults, developing an efficient intrusion detection system in a multi-attack categorization context is difficult. Because attackers may setup intrusive tactics and readily avoid the detection tools installed in a computer environment, intrusion detection systems require high-performance classification approaches. Furthermore, it is difficult to effectively detect all types of assaults using a single classifier. To put out a novel ensemble architecture that is capable of successfully identifying various assault types. According to the survey results, high-level accuracy was attained for the restored traffic, and both binary and multiclass classification accuracy are better than in earlier studies. Several researchers have concentrated on creating IDSs that utilize machine learning techniques in order to address the aforementioned issues. With a high degree of accuracy, machine learning techniques can automatically identify the key distinctions between normal and aberrant data. Furthermore, because machine learning techniques are very generalizable, they can potentially identify unidentified threats. We performed a thorough analysis of machine learning as well as deep learning methods applied to IDS construction in this study.

Keywords: 1. IDS: Intrusion Detection System, 2.FNN: Feed forward neural network,3. NIDS: Network Intrusion Detection System, 4. HIDS: Host Intrusion Detection System, 5. CNN: Convolutional Neural Network ,6. RNN: Recurrent Neural Network NSL-KDD database, GPU-Graphics Processing Unit ,7 DoS: Denial of service.

1 Introduction

One type of protection system that can identify unusual behavior is intrusion detection. "Any set of actions that attempt to compromise the integrity, confidentiality, or availability of a resource" is the definition of intrusion [3], [32]. IDSs are always evaluated from a security perspective as an additional line of protection. To further protect the systems from assaults, IDSs can be used in conjunction with other security measures including access control, authentication procedures, and encryption methods. IDSs are able to differentiate between legitimate and malicious activity by using patterns of benign traffic, typical behavior, or rules that define a particular attack [7], [32]. In contrast to traditional IDSs, which might not be as successful against contemporary sophisticated assaults, data mining—which is used to characterize knowledge discovery—can assist in the design and deployment of IDSs with im-

Available online at www.jcsonline.in Journal of Current Science & Humanities
12 (3), 2024, 35-50

Impact Factor-2.05

proved accuracy and resilient behavior, according to Dewa and Maglaras [8], [32]. "Low false-positive rate and high true positive rate" is a requirement for IDSs. A network's intruders can be divided into two categories: internal and external. (1) External intruder: An outsider who enters the network using a variety of attack vectors. (2) Internal intruder: There are many different kinds of internal intrusions, including dosing, masquerading, penetration, leakage, and malicious usage. IDSs might provide those attackers partial detection solutions. All of the above-mentioned intrusions would be detectable by an ideal intrusion detection system [4, 5, 6, 32]. Abuse detection: In this case, the system has to be provided specified patterns, and the actions or behaviors of the nodes are compared to established attack patterns. Anomaly detection: Rather than looking for specific attack patterns, this technique determines if the behavior of the nodes can be measured as normal or anomalous. The methodology primarily explains the genuine aspects of a "normal behavior," which are established by automated training. Research technique makes the process of conducting research easier and more efficient, producing the most knowledge with the least amount of time, money, and effort. The term "research design" refers to the meticulous preparation that goes into selecting the best strategies for gathering pertinent data, as well as the instruments and methodologies that will be employed to analyze the study's goals. In this paper, the approach taken to build Initially, the effectiveness of machine learning-based intrusion detection techniques will be evaluated using the intrusion benchmark dataset. The incursion benchmark dataset will then be split into two sections: the train dataset and the test dataset. Using test metrics including accuracy, precision, recall, and F1 score—performance indicators—it creates a model for attack detection. Tenser flow and the Graphics Processing Unit (GPU) will be used at the Google Collaboratory running Python 3 for testing. The effectiveness of deep learning and machine learning-based intrusion detection algorithms will be evaluated using NSL-KDD Network intrusion or infiltration is the biggest concern and issue in today's world of network communications. A major issue for system administrators is the rise in frequency of system assaults. In an effort to avoid system infiltration and guarantee system security and protection, a number of research initiatives are presently being conducted. A network can experience aggressive or passive intrusion. If the first line of defense in a security system, "Intrusion Prevention," is unable to stop incursions, the next line of defense, "Intrusion Detection," will take over. When they detect suspicious activity in a system, intrusion detection systems (IDSs) may provide any or all of the following information to other supporting systems. Intrusion Detection Systems (IDSs) provide some or all of the following data to other supporting systems in the event of a security incident: the intrusion's detection, the intrusion's location (such as a solitary node or district), the intrusion instance (such as date), the intrusion's activity (such as active or passive), the type of intrusion (such as wormhole, black hole, sinkhole, selective forwarding), and the layer where the intrusion takes place. WSNs have unique security objects as well.

(1) Forward secrecy: once a node departs the network, it is unable to decipher any future secret communications.

(2) Backward secrecy: the inability of a joining node to decipher any secret communication that has already been sent.

Available online at www.jcsonline.in Journal of Current Science & Humanities
12 (3), 2024, 35-50

Impact Factor-2.05

(3) Survivability: provided a specific degree of service is provided in the event of breakdowns.
(4) Freshness: making sure that no attacker may replicate previous communications and that the data are current.
(5) Scalability: the capacity to support a big number of nodes.
(6) Efficiency: measured bounds for communication, processing, and storage on sensor nodes [1], [32]. To defend networks against intrusions by adversaries, the researchers devised a number of intrusion detection systems, or IDSs.

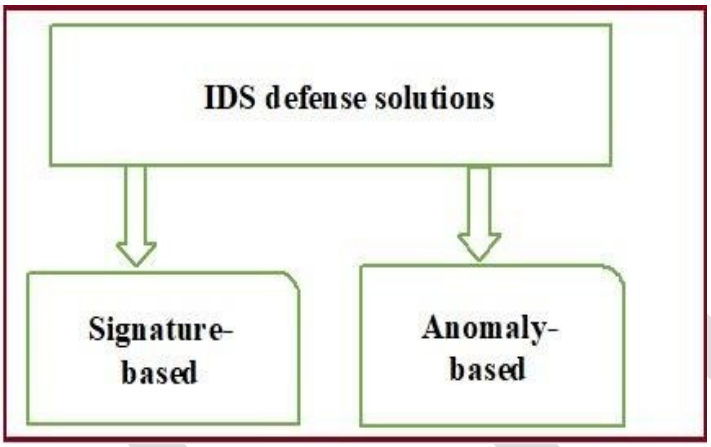

Fig. 1. Two main types of IDS by attack based

There are two categories for these IDS defensive solutions: anomaly-based and signature-based. While the latter uses methods like data mining, machine learning, deep learning, and statistical modeling to profile a statistical use model over time and classify data packets as normal or abnormal, the former depends on signs of known attack patterns.

2 Literature Review

An incremental learning method based on SVM as a classifier was proposed by Myint and Meesad [11]. This method reduces the number of steps required for computation, the complexity of the algorithm, the error set, and the amount of time needed continuously training the dataset by using SVM for Prediction. Using this strategy, the author assessed the system's performance using the KDD Cup99 dataset. 41 features of the incoming dataset may be predicted by the suggested system. A Random Forest classifier-based intrusion detection method was proposed by M. Nabila Farnaaz and Nabila Farnaaz A. Jabbar [12]. In this method, the author employed RF as an ensemble classifier, and the model performs better in categorizing assaults than other standard classifiers. The proposed model has a low false alarm rate and a high detection rate, making it effective. The author evaluated the model's performance using the NSL KDD

Available online at www.jcsonline.in Journal of Current Science & Humanities
12 (3), 2024, 35-50

Impact Factor-2.05

dataset. The STL-IDS assisted self-taught learning framework was presented by Majjed et al. as a successful deep learning strategy [13]. The suggested method may be applied to dimension reduction and feature learning. This technique shortens the testing and training periods, which increases the accuracy of SVM predictions. is reduced The suggested method enhances network intrusion detection. The evaluation of the intrusion detection decision tree was conducted by Sandhya Peddabachigari and colleagues [14]. The decision was used to assess intrusion detection using the 1998 DARPA dataset, and the accuracy of the system was better than that of traditional models. The results show reduced training and testing times as compared to the support vector machine. Wenchao Li and colleagues presented a novel intrusion detection method in WSN [16] that utilizes the K-nearest classification technique. By identifying anomalous behavior, the suggested approach is utilized to differentiate between normal and abnormal nodes. This method looks at the intrusion detection system's error rate and parameter selection. The efficiency of the suggested model is higher, and it operates quickly and with a high detection rate. A lightweight, energy-efficient system that uses mobile agents and the energy consumption of sensor nodes as a measure to identify intrusions is proposed by Michael Riecker et al. [19]. A linear regression model is utilized to predict energy usage. The suggested detection algorithm's accuracy is evaluated by the authors in a scenario that involves floods and a black hole assault. They also look at how walking techniques and the amount of the history affect detection times. They don't need audit data to be sent to a central location, and they don't need nodes to cooperate or watch their surroundings. Use a mobile agent instead, which gathers energy readings and notifies you if there are any abrupt changes. The practicality of using mobile IDS units In wireless sensor networks, it has been shown. Additionally, the authors showed that measuring energy usage is a suitable way to identify denial-of-service assaults. They used simulations to evaluate their suggested intrusion detection technique, and they were able to obtain excellent detection accuracy at a low false-positive rate. In order to increase the lifespan of WSNs, Mohammad Wazid et al. [20] suggested a secure intrusion detection method that makes use of K-means clustering. For a hybrid anomaly, the authors suggested a novel intrusion detection method called K-means, which automatically created attack patterns over training data in order to identify them. Using a WSN dataset that was created with the Opnet modeller and included a range of variables, including end-to-end latency, traffic transmitted, and traffic received, the authors assess the methodology. The network parameters' efault values are contained in the training dataset. The testing dataset, which includes both normal and aberrant network parameter values, is produced using an actual functioning model. The suggested technique, according to the authors, can identify two different kinds of malicious nodes: black hole and misdirection nodes, and it achieves a detection rate of 98.6% with a false positive rate of 1.2%, which is superior than equivalent methods that are already in use.

Available online at www.jcsonline.in Journal of Current Science & Humanities
12 (3), 2024, 35-50

Impact Factor-2.05

3 Methodology

In this research flowchart of proposed framework, we have experimental approach in a such a way that flowchart figure of proposed framework firstly we use benchmark dataset for intrusion to taste the performance of machine learning based intrusion detection approaches as well as deep learning after that we will divide the benchmark data set into section that is data set section.

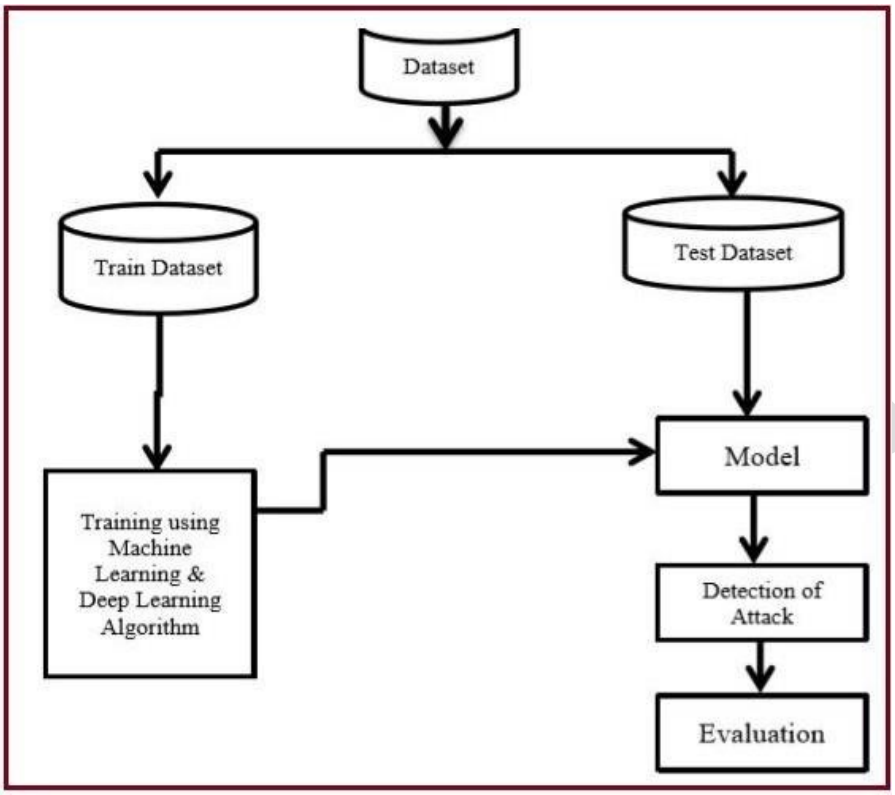

Fig. 2. Flowchart of Proposed Framework

In this we will use of 70% of data in it so has to train 70% of within machine learning algorithm as well as deep learning with this it generates a model for detection of attack now with the test data set is used to evaluate the attack where the model is used in appropriate and best fit or not from detection of attack working that it will generate and alert for it.

After that it will use and evolution parameter for testing how much efficiency of these model goes to generate with the help of test parameters like we will use indicators including precision recall F1 score and accuracy.

Available online at www.jcsonline.in Journal of Current Science & Humanities
12 (3), 2024, 35-50

Impact Factor-2.05

3.1 Intrusion Detection System (IDS)

Any improper or unauthorized activity within a network or system will be referred to as an "intrusion." A group of instruments, techniques, and materials called an intrusion detection system (IDS) are used to help identify, assess, distinguish, and characterize intrusions. [2]. One kind of protection system that recognizes anomalous behavior is intrusion detection. Intrusion may be described as "any set of actions that attempt to compromise the integrity, confidentiality, or availability of a resource" [3]. IDSs are always considered the second line of defense in terms of security. IDSs can be used in conjunction with other security measures like access control, authentication methods, and encryption techniques to better protect systems from assaults. utilizing safe traffic patterns, customary conduct, or established guidelines. External intruder: An outsider who uses a number of techniques to obtain access to the network. A hacked node that was formerly a network associate is known as an internal invader. IDS can identify both external and internal attackers; however, interior intruders are more challenging to identify. This is due to the fact that internal attackers possess the keying resources required to circumvent the security provided by authentication schemes. It is possible for there to be any kind of intrusion, including doS attacks, penetration attempts, masquerades, leaks, and malicious use.

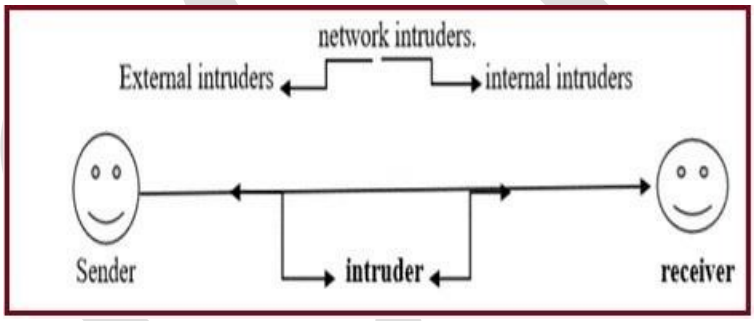

Fig. 3. Intrusion Working and types

For these kinds of assaults, IDSs might only offer a limited detection solution. All of the aforementioned intrusions would be detectable by the perfect intrusion detection system.[4], [5] Based on how they are deployed, intrusion detection systems (IDS) are divided into two categories: network-based IDS (NIDS) and host-based IDS (HIDS).One of the host's defenses against intrusions is the Host Intrusion Detection System (HIDS), which can pick up on modifications made to crucial system files, many unsuccessful efforts to gain access, odd memory allocations made by the host, strange CPU activity, and unusual I/O activity. HIDS does this by keeping an eye on how the host is using the scheme in real time or by looking at the host's log files. NIDS may listen to network communications and analyze a packet's payload, IP ad-

Available online at www.jcsonline.in Journal of Current Science & Humanities
12 (3), 2024, 35-50

Impact Factor-2.05

dresses, or ports in-depth or in real time. IDS can be categorized according on the methods used for detection. Three categories of intrusion detection systems exist: specific-based discovery, abuse-based detection, and abnormality-based detection.

1. Abuse detection: Here, the patterns need to be specified and supplied to the system, and node behaviors or activities are contrasted with established assault patterns. This method's drawbacks are that it can't identify new assaults and that creating attack patterns takes knowledge. This method has the drawback of drastically lowering system administration efficiency due to the network administrator's constant need to supply IDS agents with an up-to-date database.

2) Anomaly detection: Rather than looking for precise attack patterns, this method determines if the activity of the nodes can be measured as normal or anomalous. The methodology prime explains the genuine aspects of "normal behavior," which are detected via automated training. Any action that thereafter departs from these patterns is reported as an incursion. The IDS would have a high degree of confidence in identifying a sensor node as malicious if it did not behave in accordance with the specified guidelines of a given protocol; the accuracy of detection is impacted by the false-positive and false-negative alert judgments made by the IDS. This method's drawback is that it may cause the system to exhibit legitimate but concealed activity, which might lead to a high false alert rate.

3) Detection based on specifications: This approach focuses on identifying departures from typical behavior that are not specified by machine learning methods or training data, since it combines the objectives of misuse and anomaly detection mechanisms. Manual standards are used to specify what constitutes typical conduct, and actions are then carried out in compliance with these requirements. This approach's drawbacks are that it can't identify malicious activities that don't go against the established requirements of the IDS protocol and that all specifications have to be created manually, which takes time for people. Hybrid detection methods might arise from the occasional use of anomaly- and misuse-based detection strategies[1].

3.2 Machine Learning Approaches

1K-nearest-neighbors (KNN) technique uses similarity metrics to classify new objects. The Euclidean distance is a mathematical metric used to compare the similarity of several items. The KNN algorithm assigns the class with the highest frequency of occurrence to each test data point by examining the K-nearest training data points for each test data point. Thus, K is the number of training data points that are close to the test data point that we will use to determine the class. The K-Nearest Neighbors algorithm's steps are shown below.

Step 1: Determine K's value.

Step 2: Determine the distance between each training sample and the query instance.

Step 3: Verify that the closest neighbors supported the Kth minimal distance by sorting the distance in increasing order.

Step 4: Assign the prediction value of the query instance based on the majority of the class of nearest neighbors.

Available online at www.jcsonline.in Journal of Current Science & Humanities
12 (3), 2024, 35-50

Impact Factor-2.05

Vector Machine Support (SVM) Regression and classification are two uses for the SVM classifier. SVM uses a hyperplane to spit data into the data point in order to identify the class of the data point [28]. The data point that is closest to the classification border is referred to as a support vector, and the gap between the boundary and the nearest data point is known as the margin. When working with SVM, we must make the following two assumptions:
1) The margin needs to be as big as feasible
2) The most valuable data points are the support vectors, as they are the most likely to be misclassified. The working steps for SVM are as follows:
Steps 1: Determine the ideal hyperplane by maximizing margin.
Step 2: For nonlinearly separable issues, extend the definition from Step 1 by adding a penalty term for incorrect classifications.
Step 3: Use linear decision surfaces to map the data to a high-dimensional space where classification is simpler. rephrase the issue such that the data is implicitly mapped to this space.

Decision tree is to represent the learnt function, decision tree learning is a technique for approximating discrete-valued target functions. Instances are categorized using decision trees by being sorted from the root of the tree to a leaf node, which indicates the instance's categorization. Every node in the tree indicates a test of a particular instance property, and every branch that descends from that node represents a potential value for that attribute. When classifying an instance, one tests the attribute that this node specifies at the root of the tree and then moves down the branch of the tree that corresponds to the attribute's value in the example. This process is then repeated for the sub tree rooted at the new node. The working steps of Decision Tree algorithm are given below.
Step 1: First, a mathematical metric such as information gain is utilized to determine which property in the dataset should be at the base of the tree.
Step 2: Next, separate the train dataset into smaller groups. When splitting, it's important to keep in mind that every subset should have data for every attribute with the same value.
Step 3: Finally, just carry out Steps 1 and 2 again on every subset until we locate leaf nodes in every branch of the tree.

Random forests are an ensemble learning technique for regression or classification that work by building many decision trees from the dataset by selecting "K" numbers of data points, then combining them to get a forecast that is more reliable and accurate. We make many forecasts for the decision tree of each "K" data point, and then we average them all. The steps for Random Forest algorithm are as follows:
Step 1: With the condition i << j, choose at random "i" features from all of the "j" characteristics.
Step 2: From the "i" characteristics, compute node "n" using the best split point notion.

Available online at www.jcsonline.in Journal of Current Science & Humanities
12 (3), 2024, 35-50

Impact Factor-2.05

Step 3: Once more, we must divide node "n" into daughter nodes using the best split idea.
Step 4: Continue from Step 1 through Step 3 until "1" nodes are reached.
Step 5: Construct a forest by going through Steps 1 through Step 4 "k" times to produce "k" trees.
Step 6: Predict the target by using test characteristics, applying the rules of each decision tree that is randomly constructed, and storing the anticipated target.
Step 7: Next, only ascertain the number of votes for every anticipated goal.
Step 8: At last, consider the high voted prediction target as a final prediction.

Naïve Bayes a group of classification algorithms based on Bayes' Theorem are known as naive Bayes classifiers. It is actually a family of algorithms rather than a single method, and they are all based on the same principle—that is, each pair of characteristics being categorized stands alone. Let's start by thinking about a dataset. The Naïve Bayes classifier, one of the most straightforward and efficient classification algorithms, facilitates the quick creation of machine learning models with quick prediction capabilities.

Logical Regression is for classification problems where the objective is to predict the likelihood that an instance belongs to a specific class or not, one supervised machine learning approach that is utilized. A procedure used in statistics to examine the connection between two data components is called logistic regression. The article examines the kinds, applications, and foundations of logistic regression. When using the sigmoid function, which accepts input as independent variables and outputs a probability value between 0 and 1, logistic regression is utilized for binary classification. As an illustration, there are two classes: Class 0 and Class 1. An input is classified as Class 1 or Class 0 if the logistic function value for it is larger than the threshold value of 0.5. Since it is a continuation of linear regression and is mostly applied to classification issues, it is known as regression.

3.3 Deep Learning Approaches

This section addresses the Deep Learning methodology. We have employed a convolutional neural network classifier to carry out deep learning. Context CNNs are a particular kind of artificial neural network that analyze data using the Perceptron machine learning algorithm [34]. CNN may be used for a variety of applications, including natural language processing and image processing. Fundamental: Below are the processes that a CNN classifier takes to operate. CNN consists of basically four phases. These steps are as follows:
Step 1 Convolution: Known as convolution filters, this is the first layer of CNN that takes in an input signal. One process type where the network attempts to identify an incoming signal by using prior knowledge is convolution. The flooding attack reference signal will be blended, or more accurately, convoluted, with the input signal if the input signal resembles a prior flooding attack that it has encountered. The resultant signal is then forwarded to the subsequent layer.

Available online at www.jcsonline.in Journal of Current Science & Humanities
12 (3), 2024, 35-50

Impact Factor-2.05

Step 2: Subsampling – This is the second CNN layer. It takes input from the convolution layer and smooths it out so that the filters are less sensitive to fluctuations and noise. We refer to the smoothing technique as subsampling.
Step 3: Activation: The third layer of CNN is responsible for regulating the flow of signals from one layer to the next, simulating the firing of neurons in the human brain. Once more, in this case, output signals that are highly correlated with previous references would activate more neurons, increasing the efficiency with which signals are conveyed for identification.
Step 4: Connectivity – This is the final, completely linked layer of CNN. Every neuron in this neuron's succeeding layers is related to the ones before it. Python is the programming language and WSN-DS is the dataset utilized in a CNN implementation. To get the findings, the CNN classifier's operational procedures are used. While floods and blackhole assaults are expected, the actual attack types were regular and blackhole, respectively. the CNN classification report, which identified TDMA, flooding, black hole, and gray hole assaults. CNN's accuracy is the average of all assaults and is higher than machine learning.

4 Experimental Results

To evaluate the effectiveness of machine learning-based intrusion detection techniques, we employ NSL-KDD. A selection of downloaded files available for scholars to use. The experiment uses TensorFlow and the Graphics Processing Unit (GPU) on Google Collaboratory running Python 3.

4.1 Dataset Description

Table 1. List of nsl-kdd Dataset files

Sr.No.	Dataset Files
1	KDDTrain+.ARFF
2	KDDTrain+.TXT
3	KDDTrain+_20Percent.ARFF
4	KDDTrain+_20Percent.TXT
5	KDDTest+.ARFF
6	KDDTest+.TXT
7	KDDTest-21.ARFF
8	KDDTest-21.TXT

To manage some of the KDD-99 dataset's inherent issues, the NSL-KDD dataset is suggested. Numerous statistical analyses have shown the intrinsic flaws in the KDD cup 99 datasets, which have impacted the detection accuracy of numerous IDS that researchers have modelled. The improved NSL-KDD data set [28] is an improved

Available online at www.jcsonline.in Journal of Current Science & Humanities
12 (3), 2024, 35-50

Impact Factor-2.05

version of the original. It includes all of the necessary entries for the whole KDD data collection. Compared to the original KDD dataset, the NSL-KDD dataset has the following improvements:

- In order for the classifiers to generate an unbiased result, redundant records are eliminated.
- Duplicate records are eliminated.
- The number of selected records is arranged as a percentage of records. (e.g., DDTrain+_20Percent.ARFF)
- There are enough records in the train and test data sets, which makes sense and allows for the execution of experiments on the entire set.
- The percentage of records in the original KDD data set is negatively correlated with the number of selected records from each challenging level group.

4.2 Performance Metrics

We employ the most crucial KPIs, such as accuracy (ACC), false alarm rate (FAR), and detection rate (DR). We may use the following Accuracy (ACC) to compute the performance metrics: It is a measure that shows what percentage of all the records in the testing set were correctly classified.

$$\text{Accuracy} = (TP+ TN)/ (TP+ FN+ TN+ FP)$$

Precision (P) is a metric that assesses actual performance between the locations, or within the required response space.

$$P = TP/ (TP + FP)$$

Recall (R) is a statistic used to determine how many true labels have been discarded for every accurate label, or how much of the predicted responses have been rejected.

$$R = TP/ (TP + FN)\ F1$$

Score (F) is the harmonic mean of the two matrices P and R.

$$F = (2 * P * R) / (P + R)$$

True positive (TP) It may be defined as anomaly occurrences that are appropriately classified as anomalies.
False positive (FP) It may be defined as typical occurrences that are mistakenly classified as abnormal.
True negative (TN) It is best described as typical circumstances that fall under the usual category.
False negatives (FN) are anomaly cases that are mistakenly classified as normal.

Available online at www.jcsonline.in Journal of Current Science & Humanities
12 (3), 2024, 35-50

Impact Factor-2.05

Table 2. Comparison of the proposed IDS framework with other machine learning-based IDS

Algorithm	Accuracy	Precision		Recall		F1-score	
		Attack	Normal	Attack	Normal	Attack	Normal
KNN	77.33	0.63	0.97	0.96	0.66	0.76	0.79
SVM	76.55	0.66	0.90	0.90	0.67	0.76	0.77
Decision Tree	72.05	0.62	0.86	0.85	0.63	0.72	0.73
Random Forest	72.73	0.54	0.98	0.97	0.62	0.69	0.76
Naïve Bayes	51.17	0.90	0.00	0.54	0.02	0.68	0.00
Logistic regression	55.03	0.71	0.34	0.59	0.47	0.64	0.39

Table 3. Classification result of Deep Learning approach

Deep learning accuracy	Precision	Recall	F1-Score
CNN	0.96	0.94	0.97

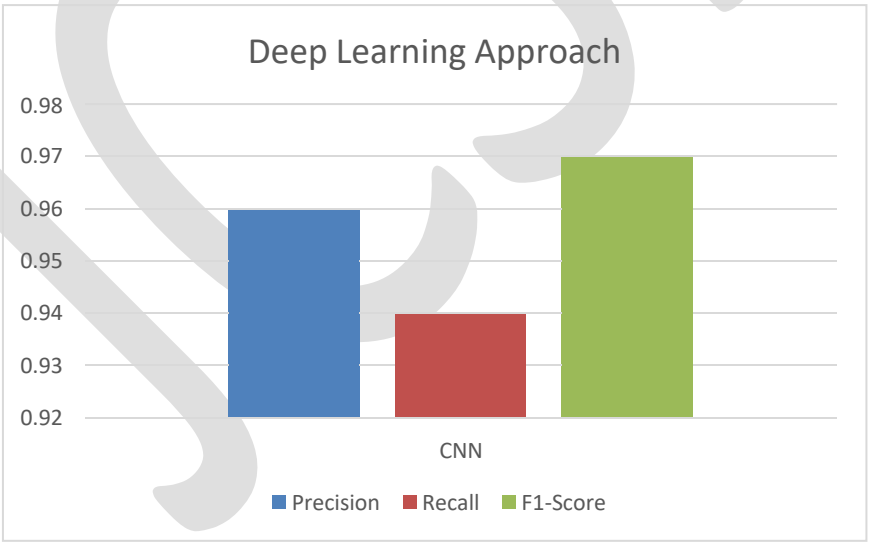

Fig. 3. Analysis of Deep Learning Approach

Available online at www.jcsonline.in Journal of Current Science & Humanities
12 (3), 2024, 35-50

Impact Factor-2.05

5 Conclusion

In this paper we have proposed a comparative study and performance analysis on intrusion detection system and its prevention system using machine learning based IDS with different machine learning classifier and one deep learning algorithm to comparison between machine learning and deep learning of the most important performance indicators like accuracy, precision, recall and F1-score for evaluating efficiency of both types of approach.

References

1. SumaiyaThaseen, J. SairaBanu, K. Lavanya, Muhammad Ghalib2, KumarAbhishek3.: An integrated intrusion detection system using correlation-based attribute selection and artificial neural network. John Wiley & Sons, Ltd, (2020).
2. Samrat Kumar Dey, Md. Raihan Uddin and Md. Mahbubur Rahman.: Chapter 41, Performance Analysis of SDN-Based Intrusion Detection Model with Feature Selection Approach. Springer Nature Singapore Pte Ltd. (2020).
3. Pankaj R. Chandre, Parikshit N. Mahalle and Gitanjali R. Shinde.: Deep Learning and Machine Learning Techniques for Intrusion Detection and Prevention in Wireless Sensor Networks: Comparative Study and Performance Analysis. Springer Nature Singapore Pte Ltd. (2020).
4. T. Tulasi Bhavani, M. Kameswara Rao and A. Manohar Reddy.: Network Intrusion Detection System Using Random Forest and Decision Tree Machine Learning Techniques., Springer Nature Singapore Pte Ltd. (2020)
5. Nicholas Lee, Shih Yin Ooi and Ying Han Pan.: A Sequential Approach to Network Intrusion Detection. Springer Nature Singapore Pte Ltd. (2020).
6. Mukaram Safaldin1, Mohammed Otair1, Laith Abualigah1.: Improved binary gray wolf optimizer and SVM for intrusion detection system in wireless sensor networks., springer (2020).
7. Mohamed Amine Ferrag, Leandros Maglaras, Sotiris Moschoyiannis, Helge Janicke.: Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study.Journal of Information Security and Applications, 50 (2020) .
8. Dewa Z, Maglaras L A.: Data mining and intrusion detection systems. Int. J. Adv. Comput. Sci. Appl. (2016).
9. Stewart B, Rosa L, Maglaras LA, Cruz TJ, Ferrag MA, Simões P, et al..: A novel intrusion detection mechanism for scada systems which automatically adapts to network topology changes.EAI Endorsed Trans. Ind. Netw. Intell. Syst. (2017).
10. Niyaz, Q., Sun, W., Javaid, A. Y., & Alam, M. 03–05.:A deep learning approach for network intrusion detection system., In BICT 2015, New York City, United States. (2015).

Available online at www.jcsonline.in Journal of Current Science & Humanities
12 (3), 2024, 35-50

Impact Factor-2.05

11. Myint, H. O., & Meesad, P. :Incremental Learning Algorithm based on Support Vector Machine with Mahalanobis distance (ISVMM) for Intrusion Prevention. IEEE 978-1-4244-3388 9/09/$25.00 ©(2009).
12. Farnaaz, N., & Jabbar, M. A. :Random forest modelling for network intrusion detection system. Procedia Computer Science, 89, 213–217 Elsevier (2016).
13. Al-Qatf, M., Lasheng, Y., Alhabib, M., & Al-Sabahi, K. :Deep learning approach combining sparse auto encoder with SVM for network intrusion detection.IEEE Access. https:// doi.org/10.1109/ACCESS.2018.2869577. (2018).
14. Peddabachigari, S., Abraham, A., & Thomas, J. :Intrusion detection systems using decision trees and support vector machines. International Journal of Advanced Networking and Applications, 07(04), 2828–2834. ISSN: 0975-0290. (2016).
15. Panda, M., & Patra, M. R. :Network intrusion detection using Naïve Bayes. IJCSNS International Journal of Computer Science and Network Security, 7(12) (2007).
16. Li, W., Yi, P., Wu, Y., Pan, L., & Li, J. :A new intrusion detection system based on KNN classification algorithm in WSN. Journal of Electrical and Computer Engineering, Hindawi Publishing Corporation. (2014).
17. Van, N. T., Thinh, T. N., & Sach, L. T. :An anomaly-based network intrusion detection system using deep learning. In 2017 International Conference on System Science and Engineering ICSSE. (2017).
18. Yang, Y., Zheng, K., Wu, C., Niu, X., Yang, Y. :Building an Effective Intrusion Detection System Using the Modified Density Peak Clustering Algorithm and Deep Belief Networks., Appl. Sci. 9, 238 (2019).
19. Michael Riecker, Sebastian Biedermann, Rachid El Bansarkhani and Matthias Hollick. :Lightweight energy consumption-based intrusion detection system for wireless sensor networks. International Journal of Information Security, vol. 14, no. 2, pp. 155-167,(2015).
20. Mohammad Wazid and Ashok Kumar Das. :An Efficient Hybrid Anomaly Detection Scheme Using K- Means Clustering for Wireless Sensor Networks, Wireless Personal Communications, vol for Wireless Sensor Networks.Wireless Personal Communications, vol. 90, no. 4, pp. 1971-2000, October (2016).
21. Ahmed Saeed, Ali Ahmadinia, Abbas Javed and Hadi Larijani. :Random Neural Network based Intelligent Intrusion Detection for Wireless Sensor Networks. In proceedings of International Conference on Computational Science, vol. 80, pp. 2372-2376, (2016).
22. Yassine Maleh, Abdellah Ezzati, Youssef Qasmaoui and Mohamed Mbida. :A Global Hybrid Intrusion Detection System for Wireless Sensor Networks. The fifth International Symposium on Frontiers in Ambient and Mobile Systems, vol. 52, pp. 1047-1052, (2015).
23. Hichem Sedjelmaci and Mohamed Feham. :Novel Hybrid Intrusion Detection System for Clustered Wireless Sensor Network", International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.4 July (2011).

Impact Factor-2.05

24. P. R. Chandre, P. N. Mahalle, and G. R. Shinde.:Deep Learning and Machine Learning Techniques for Intrusion Detection and Prevention in Wireless Sensor Networks: Comparative Study and Performance Analysis. Lecture Notes in Networks and Systems 82, https://doi.org/10.1007/978-981-13-9574-1_5.
25. Nicholas Lee, Shih Yin Ooi and Ying Han Pang. :A Sequential Approach to Network Intrusion Detection. Lecture Notes in Electrical Engineering 603, https://doi.org/10.1007/978- 981-15-0058-9_2.
26. Kishor Kumar Gulla, P. Viswanath, Suresh Babu Veluru, and R. Raja Kumar. :Machine Learning Based Intrusion Detection Techniques", Handbook of Computer Networks and Cyber Security, https://doi.org/10.1007/978-3-030-22277-2_35.
27. Tavallaee M, Bagheri E, Lu W, Ghorbani A. A. :A detailed analysis of the kdd cup 99 data set", In: 2009 IEEE Symposium on Computational Intelligence for Security and Defence Applications. IEEE; (2009).
28. Nsl kdd. https://www.unb.ca/cic/datasets/nsl.html
29. L. Dhanabal, and Dr. S.P. Shantharajah. :A Study on NSL-KDD Dataset for Intrusion Detection System Based on Classification Algorithms. international Journal of Advanced Research in Computer and Communication Engineering Vol. 4, Issue 6, June(2015).
30. Sapna S. Kaushik, Dr. Prof. P. R. Deshmukh. :Detection of Attacks in an Intrusion Detection System", International Journal of Computer Science and Information Techytre4wsnologies, Vol. 2 (3), (2011)
31. Opeyemi Osanaiye, Olayinka Ogundile, Folayo Aina, Ayodele Periola. :FEATURE SELECTION FOR INTRUSION DETECTION SYSTEM IN A CLUSTER-BASED HETEROGENEOUS WIRELESS SENSOR NETWORK.FACTA UNIVERSITATIS, Series: Electronics and Energetics Vol. 32, N o 2, June (2019).
32. Seema M.Shinde, Dr.Thorat S.B. , Miss.Tazeen Khan, Dr.PravinTamsekar . :Survey and performance analysis of Machine learning based Intrusion detection approaches in wireless sensor networks .IOSR Journal of Computer Engineering (IOSR-JCE), Volume 22, Issue 4, Ser. IIPP 06-13 (2020)
33. Rakesh Sharma, and Vijay Anant Athavale. :A Survey of Intrusion Detection Techniques and Architectures in Wireless Sensor Networks. Int. J. Advanced Networking and Applications, Volume: 10 Issue: 04 Pages: 3925-3937,(2019).
34. Bhattacherjee, A., Roy, S., Paul, S., Roy, P., Kausar, N., & Dey, N. :Classification approach for breast cancer detection using back propagation neural network: A study (pp. 210–221). IGI Global(2016).
35. Pankaj R. Chandre, Parikshit N. Mahalle and Gitanjali R. Shinde . :Deep Learning and Machine Learning Techniques for Intrusion Detection and Prevention in Wireless Sensor Networks: Comparative Study and Performance Analysis. Springer Nature Singapore Pte Ltd. (2020).
36. Seema M.Shinde, Dr.Thorat S.B. , Miss.Tazeen Khan, Dr. Pravin Tamsekar. : Survey and performance analysis of Machine learning based Intrusion de-

Impact Factor-2.05

tection approaches in wireless sensor networks .IOSR Journal of Computer Engineering (IOSR-JCE), Volume 22, Issue 4, Ser. IIPP 06-13 (2020).

37. Rakesh Sharma, and Vijay Anant Athavale. :A Survey of Intrusion Detection Techniques and Architectures in Wireless Sensor Networks. Int. J. Advanced Networking and Applications, Volume: 10 Issue: 04 Pages: 3925-3937,(2019).
38. Bhattacherjee, A., Roy, S., Paul, S., Roy, P., Kausar, N., & Dey, N. :Classification approach for breast cancer detection using back propagation neural network: A study (pp. 210–221). IGI Global (2016).
39. Pankaj R. Chandre, Parikshit N. Mahalle and Gitanjali R. Shinde . :Deep Learning and Machine Learning Techniques for Intrusion Detection and Prevention in Wireless Sensor Networks: Comparative Study and Performance Analysis. Springer Nature Singapore Pte Ltd. (2020).